Ratgeber

Tink Open-Banking-Konnektivität Leitfaden

Was es braucht, um sich mit Open Banking APIs zu verbinden - und warum dies komplexer ist, als es zunächst scheint

tink
A Visa Solution

Auf den ersten Blick scheint die Einbindung einer Open Banking API ziemlich leicht zu sein. Seit die PSD2-Gesetzgebung 2018 in Kraft trat, sind ASPSPs in ganz Europa verpflichtet, freien Zugang zu Kundendaten über APIs zu gewähren. Und wenn Sie sich einmal mit der Bank oder dem Finanzinstitut verbunden haben, sollte diese Verbindung doch dauerhaft einwandfrei funktionieren. Oder etwa nicht?

Leider nein.

Was in dieser Gleichung übersehen wurde, ist, dass ASPSPs keine finanziellen Anreize für die Bereitstellung des Zugangs zu Daten über APIs erhalten. Dies mag für sie zwar eine langfristige Investition in die Idee und Vision eines offeneren Finanzsystems sein, aber es zahlt noch nicht die Rechnungen von heute. Das bedeutet, dass die ASPSPs-Teams, die für die Verwaltung dieser APIs zuständig sind, oft chronisch unterbesetzt sind.

Open-Banking-Plattformen wie Tink bilden daher einen wichtigen Teil dieses neuen Ökosystems. Sie arbeiten mit den ASPSPs zusammen, um ihre Verbindungen kontinuierlich zu überwachen, Fehler zu finden, Probleme zu melden und regelmäßig mit ihren Ingenieurteams zu kommunizieren. Eine operative und technische Herausforderung, die viel Zeit, Personal und Infrastruktur erfordert.

Dieser Leitfaden erklärt den gesamten Prozess und zeigt, warum es bei der Anbindung an eine Open-Banking-API um viel mehr geht, als nur die erste Verbindung herzustellen.

Was Sie in diesem Leitfaden finden

Was steckt wirklich hinter der Anbindung an Open Banking APIs?

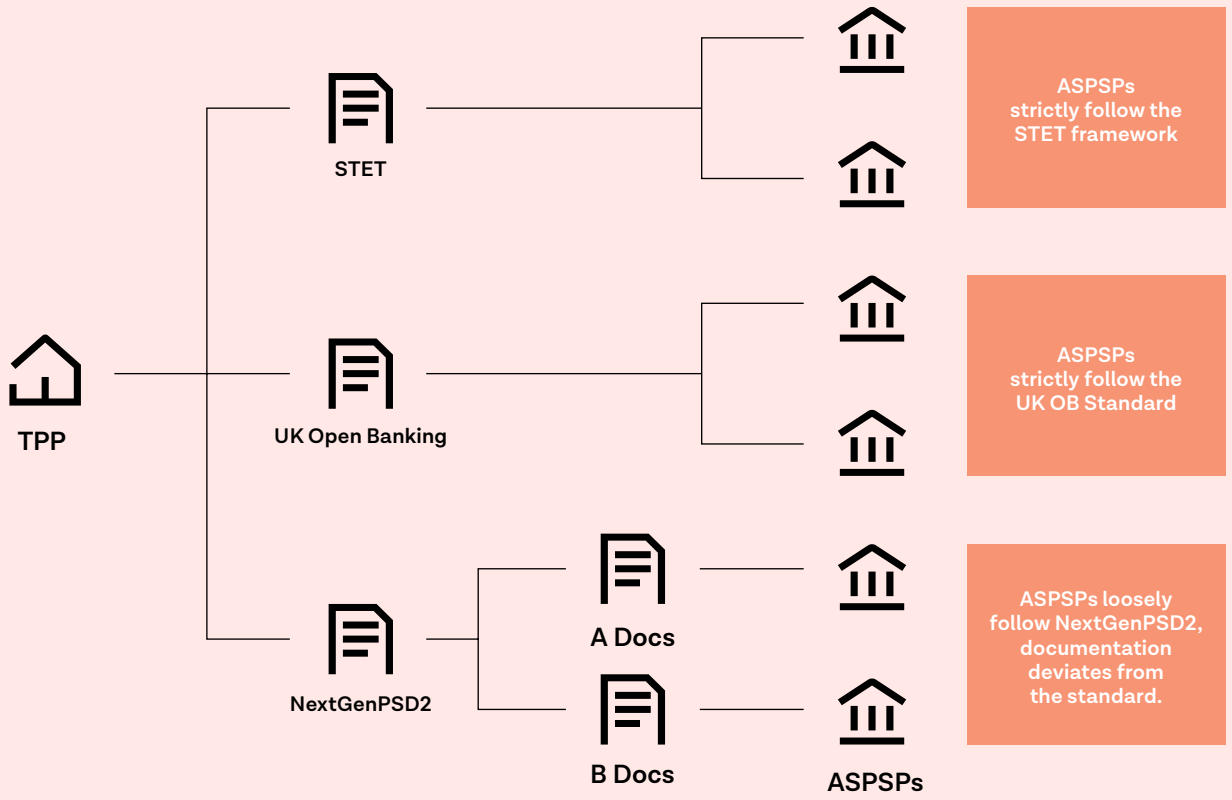
Der Aufbau von Verbindungen über mehrere Länder hinweg ist ein komplexes Unterfangen, das erhebliche Investitionen erfordert, insbesondere in Technik, Betrieb und Rechtssicherheit. Um dies übersichtlich darzustellen, werden wir das hypothetische Beispiel eines Drittanbieters (Third Party Povider, TPP) verwenden, der sich mit Dienstleistern in ganz Europa verbindet, die für Kunden Zahlungskonten unterhalten (sogenannte Account Servicing Payment Service Providers, ASPSPs). Anhand dieses Beispiels führen wir Sie durch den gesamten Prozess der Optimierung von Verbindungen zu Bank-APIs. Dabei ist die Verbindung zu einer Bank nur der erste Schritt der Wertschöpfungskette.

Mit einer Open Banking API verbinden

Verbindung mit Banken aufbauen

1.1 Europäische Standards verstehen

Die Anbindung an eine Open Banking-API erfordert ein umfassendes Verständnis der Standards, die von Banken in verschiedenen Ländern verwendet werden. In Westeuropa gibt es drei übergreifende Rahmenrichtlinien:



STET: Das STET PSD2 API-Framework wird hauptsächlich in Frankreich verwendet und ist strikter als das NextGenPSD2-Framework. Der Hauptunterschied liegt im Protokoll für die Signaturanforderung, mit dem validiert wird, dass die Informationen vom TPP nicht verändert wurden.

UK Open Banking: Der UK Open Banking Standard ist der am wenigsten flexible. Die meisten britischen ASPSPs folgen einer fast direkten Implementierung dieses Standards mit nur sehr kleinen Variationen. Dies ist der ausgereifteste Standard, da es ihn bereits seit 2018 gibt, er von Hunderten von TPPs gründlich getestet wurde und seine Entwicklung und Implementierung von der CMA und FCA überwacht wurde.

NextGenPSD2: Der NextGenPSD2 Access to Account (XS2A) Framework-Standard der Berlin Group bietet eine architektonische Sicht auf die API und ermöglicht eine flexible Implementierung, bei der ASPSPs die Möglichkeit haben, vom Standard abzuweichen und diesen nach ihren eigenen Anforderungen zu implementieren. Obwohl die Berlin Group von ASPSPs verlangt, Änderungswünsche an das Komitee des Frameworks zu richten, wird dies leider nur selten getan. Das hat zu einer starken Fragmentierung der Implementierung des Standards und einem hohen Maß an Varianz zwischen den Open Banking APIs geführt. Er ist das am häufigsten eingesetzte Framework in Europa.

1.2 Registrierung bei ASPSPs

Der zweite Schritt ist die Registrierung bei den ASPSPs. Das kann entweder durch manuelle oder dynamische Registrierungen erfolgen.

Manuelle Registrierungen erfordern eine Kommunikation zwischen dem TPP und dem ASPSP, zum Beispiel die Registrierung im Entwicklerportal, das Erstellen einer App oder das Hin- und Herschicken von E-Mails mit den ASPSPs, um Zugang zu erhalten. Dieser Prozess erfordert keine wertvolle Entwicklerzeit, kann aber je nach Bereitschaft der PSD2-API einige Tage bis Monate in Anspruch nehmen. Leider sind manuelle Registrierungen in Europa die Norm und nur etwa 15 % der europäischen ASPSPs bieten dynamische Registrierungen an.

Dynamische Registrierungen erfolgen über eine API und wenn sie korrekt durchgeführt werden, registriert der ASPSP den TPP automatisch. Die dynamische Registrierung erfordert eine große Anfangsinvestition, ist aber äußerst skalierbar und ermöglicht eine automatische Registrierung ohne weiteren Aufwand.

Tink hat beträchtliche Ressourcen in den Aufbau eines internen dynamischen Registrierungstools investiert, das uns ermöglicht unsere Kunden mit verschiedenen Registrierungs-APIs per Plug-and-Play fast sofort einzubinden.

1.3 Die Verbindung herstellen

In der Theorie ist der Prozess der Herstellung einer Verbindung relativ einfach, da der TPP die von der ASPSP veröffentlichte technische Anleitung befolgen muss. Die Realität kann jedoch wesentlich komplexer sein.

Die Anforderungen an die Anbindung an Open Banking APIs sind für jeden ASPSP und in jedem Land unterschiedlich. Einige ASPSPs sind relativ einfach anzubinden, während andere einen wesentlich mehr Aufwand erfordern.

Heutzutage sind die meisten Open-Banking-APIs glücklicherweise so weit ausgereift, dass wenig Aufwand erforderlich ist und die Anbindung sehr schnell erfolgen kann. Nichtsdestotrotz sollten TPPs einige Maßnahmen in Betracht ziehen:

- → Das Einrichten eines Kommunikationsteam, das sich mit dem ASPSP-Support in Verbindung setzt, wenn deren Dokumentation unklar oder veraltet ist.
- → Sich mit den technischen Spezifikationen vertraut amchen, sowohl mit den lokalen (spezifisch für ASPSP oder den Markt, z. B. API-Spezifikationen in Deutschland) als auch mit den allgemeinen (Standards, z. B. JWT-Methoden). Das wird Entwicklern helfen, die zugrundeliegenden Anforderungen der verwendeten Programme zu verstehen und Bugs schnell zu beheben.
- → Eine flexible Kernarchitektur entwerfen zur Unterstützung einer Vielzahl von ASPSP-Verbindungen. Die in Abschnitt 1.1 erwähnten technischen Standards bieten eine Grundlage dafür, wie die Open-Banking-APIs aussehen, aber die Einrichtung, um Zugriff auf das Konto zu erhalten, hängt vom ASPSP ab. Die zugrundeliegende Struktur ist extrem wichtig, da sich kleine Änderungen auf andere Verbindungen auswirken können, was zu fehlerhaften Ergebnissen führt.
- → TPPs sollten alle kryptografischen Methoden unterstützen, um den Aufwand für die Kunden zu minimieren und sie je nach dem vom ASPSP geforderten Standard zu verbinden. Zum Beispiel erfordert UK Open Banking 5 verschiedene kryptografische Methoden, die in allen ASPSPs weit verbreitet sind.
- → In die Schulung der Entwickler investieren und ihnen ein umfassendes Verständnis für die Standards, Systeme und Prozesse vermitteln. Die Menge an Programmcode, die zur Durchführung dieser Aufgaben benötigt wird, ist teuer und steigt mit jeder neuen Verbindung.

Tinks erster großer Kunde, der Open Banking-APIs verwendete, benötigte ein Team von fünf Entwicklern, die insgesamt sechs Monate lang die Plattform in einem einzigen Markt testeten und Bugs behoben. Wir haben über 1.500 E-Mails verschickt und dutzende Anfragen bei den Banken gestellt, bevor die Lösung einsatzbereit war.

Verbindung mit Banken aufrechterhalten

2.1 Die Verbindung prüfen und stabilisieren

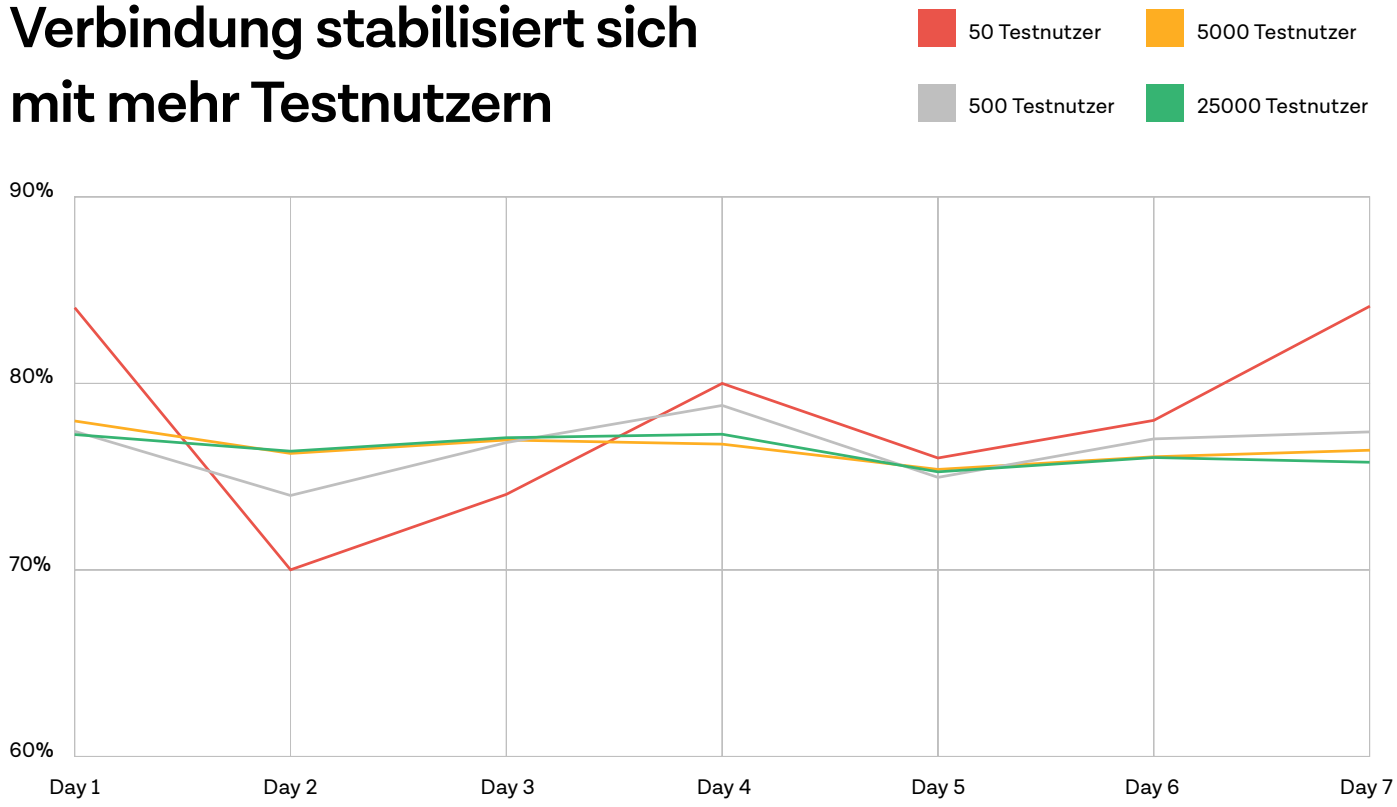
Sobald die Verbindungen aufgebaut sind, müssen eine Reihe von strengen Tests durchgeführt werden, um sicherzustellen, dass sie stabil laufen und richtig funktionieren. Ein typischer Testprozess würde folgendermaßen ablaufen:

1. Sie eröffnen Bankkonten bei jeder Bank eines Landes und testen die Verbindung mit echten Anmeldedaten. Entwickler bekommen so direktes Feedback aus Sicht des Endnutzers.
2. Nachdem die erste Testrunde abgeschlossen ist, führen Sie alle Prozesse bei denen zuvor Fehler aufgetreten sind mit einer größeren Anzahl von Benutzern durch.
3. Alle Endbenutzererfahrungen werden laufend aufgezeichnetsowie Informationen gesammelt, insbesondere dann, wenn ein Versuch fehlschlägt.

If a TPP plans to support a variety of use cases, it is important to have a large amount of traffic across several clients and use cases, as this will give a more comprehensive picture of how a connection is performing. For instance, testing a connection on a digitally-savvy customer base that is able to overcome obstacles during authentication could be falsely interpreted as a well-functioning connection with high conversion rates. In the real world, a lot of users may not be able to work their way around these same obstacles, leading to a big drop-off in conversion rates. This requires TPPs to think about the ways in which all types of customers may be impacted and how to guide them through the journey.

In the graph below, we use live data to illustrate the value of increasing the number of users to test connection stability. The red line shows the volatility of success rates when there are 50 users, while the green line shows a relatively stable success rate once traffic goes beyond 25000 users.

Die Erfolgsrate der Verbindung stabilisiert sich mit mehr Testnutzern



2.2 Tagesbetrieb

Der nächste Schritt besteht darin, sicherzustellen, dass die Verbindungen tagtäglich ordnungsgemäß funktionieren, sowie langfristig auftretende Probleme zu beheben. Um dies zu erreichen, sollten TPPs ein System einrichten, das die Qualität jeder Verbindung ständig misst, automatische Warnungen generiert, wenn Verbindungen nicht den Qualitätsstandards entsprechen, und Entwickler auf Abruf bereithält, die für solche Situationen geschult sind.

Warnmeldungen erfordern nicht immer sofortige Reaktionen oder sogar angepassten Programmcode, da gelegentlich ASPSPs-Dienste ausfallen. TPPs sollten jedoch darauf achten, jeden Vorfall und jedes Risiko zu identifizieren, ein klares Verständnis für die Grundursache des Problems zu haben und Kunden zu informieren, wenn nötig.

Der Betrieb einer Lösung über einen langen Zeitraum, mit ordnungsgemäßen Tests und täglichen Routinen ist ein nie endender Prozess und wird bei der Entscheidung für eine Eigenentwicklung oft unterschätzt.

Bei Tink haben wir ein umfassendes Alarmierungs- und Bereitschaftssystem aufgebaut, um mit den ständigen Veränderungen Schritt zu halten. Unser Alarmsystem hat eine Reihe von Prioritäten und Schwellenwerten, die den Schweregrad des Problems und die Anzahl der betroffenen Benutzer berücksichtigen. Sobald die Anzahl der Fehler den Schwellenwert überschreitet, wird eine Nachricht an das für die API verantwortliche Team weitergeleitet, um je nach Schwere des Problems eine Bewertung und Priorisierung vorzunehmen.

Service-Status-Seite auf Tink.com

Aggregationsdienste — Funktionsfähigkeit

Vor 90 Tagen — 99.92% Verfügbarkeit — Heute

Zahlungsdienste — Funktionsfähigkeit

Vor 90 Tagen — 99.86% Verfügbarkeit — Heute

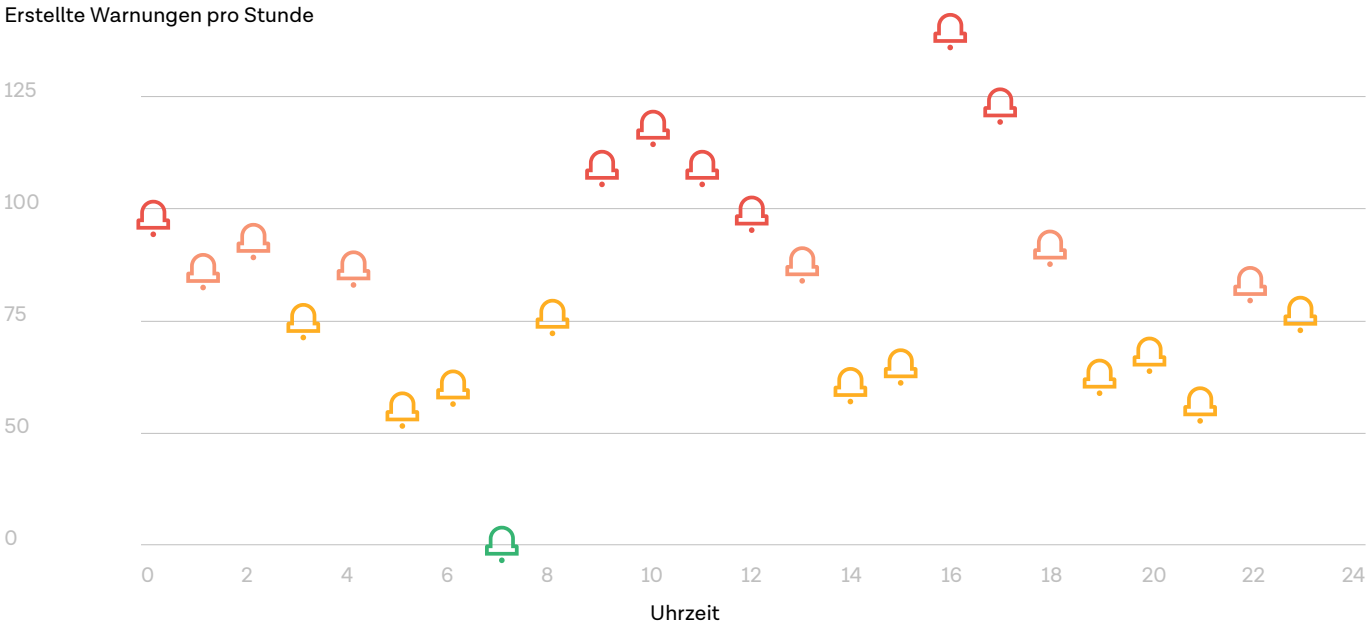
PFM-Dienste — Funktionsfähigkeit

Vor 90 Tagen — 100% Verfügbarkeit — Heute

Datenanreicherungsdienste — Funktionsfähigkeit

Vor 90 Tagen — 100% Verfügbarkeit — Heute

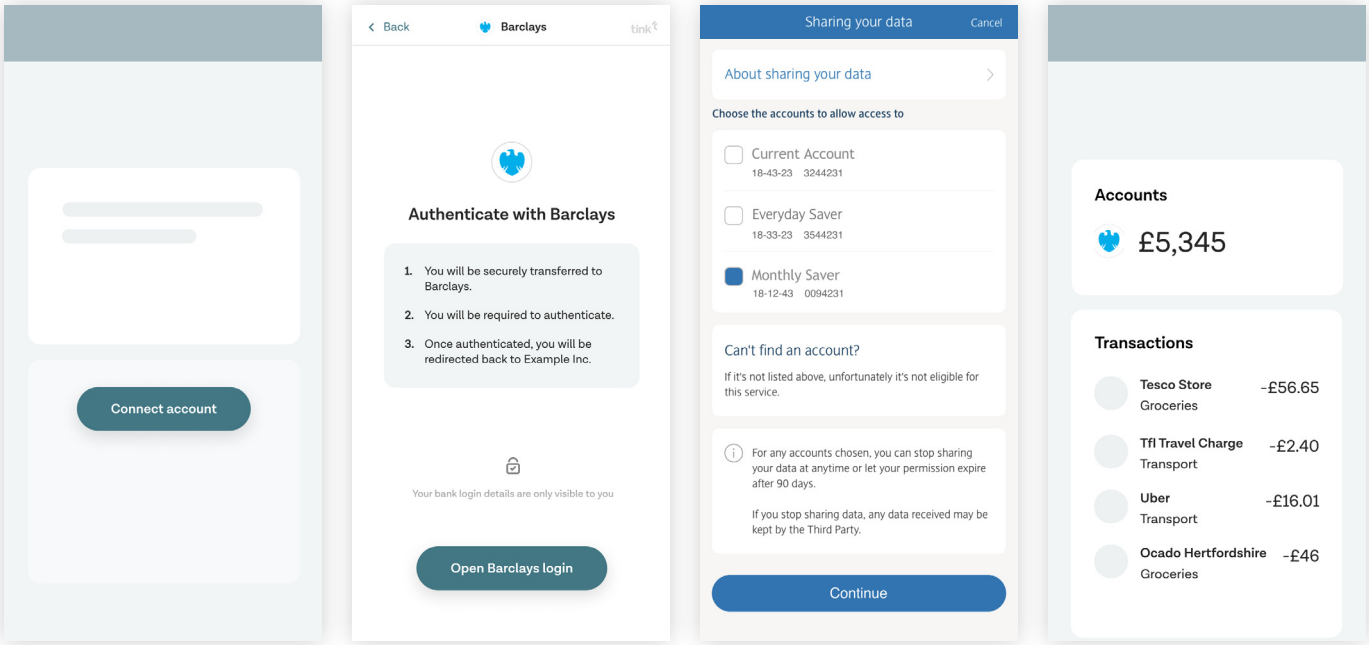
Dashboard für Warnungen



User Experience verbessern

All die Zeit und der Aufwand, die in den Aufbau und den Betrieb von Bankverbindungen investiert werden, führen zu dem alles entscheidenden Moment, an dem TPPs die Endbenutzer um die Zustimmung zum Zugriff auf ihre Bankkonten bitten. An dieser Stelle kommt die Benutzererfahrung ins Spiel. Die Bereitstellung einer guten UX erfordert eine Kombination aus operativem Wissen über Authentifizierungsabläufe, das Verstecken dieser Komplexität vor dem Endbenutzer und die Umwandlung in eine schöne, einfache und nahtlose Erfahrung.

Bei Tink tun wir das mit Tink Link, unserem Front-End-SDK zur Verwaltung und Optimierung der ASPSP-Authentifizierung.



Das Ziel ist es, sicherzustellen, dass Endbenutzer die Anforderungen der starken Kundenauthentifizierung (Strong Customer Authentication) erfüllen, die besagt, dass ein Benutzer sich durch zwei von drei Elementen identifizieren muss: Besitz (z. B. Smartphone), Wissen (z. B. Passwort) und Inhärenz (z. B. Biometrie). Für die meisten Endbenutzer mag das wie eine einfacher Anmeldeprozess aussehen. In der Realität existieren eine Menge an komplexen Vorgängen im Hintergrund, die von wichtigen Faktoren abhängen, wie z. B. Verbindungstyp, Gerätetyp, Länder und Sprachen und andere Variablen. Der vielleicht schwierigste Teil ist jedoch, dass viele Schritte außerhalb der Kontrolle eines TPPs liegen. Da es in der Branche keinen Konsens darüber gibt, wie ASPSPs die Benutzeridentität verifizieren sollten, müssen TPPs oft maßgeschneiderte Authentifizierungsabläufe erstellen, was zu einer unüberschaubaren Anzahl von Kombinationen führt, die berücksichtigt werden müssen. Typische Szenarien sind entkoppelte, eingebettete, Web- und App-Redirects.

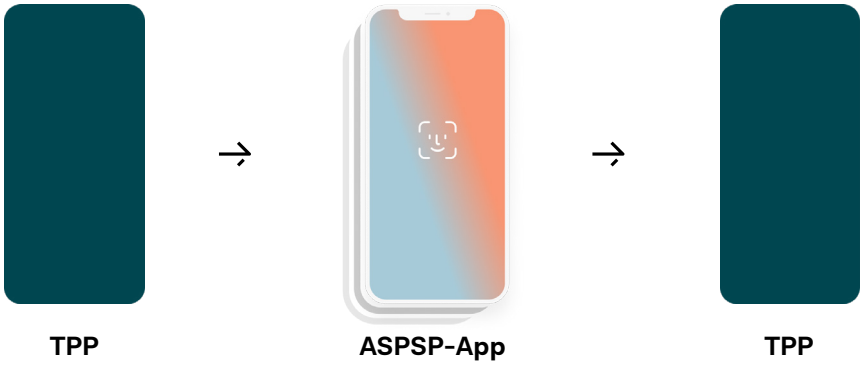
Häufige Authentifizierungsabläufe in Europa

Entkoppelt
(Schweden)

Eingebettet
(Deutschland)

Web-Umleitung
(Spanien, Italien)

App-Umleitung
(Großbritannien)



Anwendungsbeispiel

Um die Komplexität hinter der Verbesserung der Endbenutzererfahrung zu erklären, lassen Sie uns ein Beispiel eines Kunden nehmen, der mithilfe von Tink die manuellen Schritte im Onboarding-Prozess entfernen wollte. Die Verbesserung des Benutzer-Onboardings ist ein relativ etablierter Anwendungsfall im Open Banking, den wir schon für eine Reihe von Kunden durchgeführt haben.
Wir authentifizieren Nutzer, ermitteln Kontoinformationen, verbinden Bankkonten und voilà! Unsere Teams haben ein paar Monate mit der Integration verbracht, doch als wir sie implementiert hatten, waren wir überrascht, dass die Konversionsrate neuer Nutzer (Abschluss des gesamten Onboarding-Prozesses), enttäuschend niedrig war. Also haben wir die Daten angeguckt, um zu verstehen, wo das Problem lag.

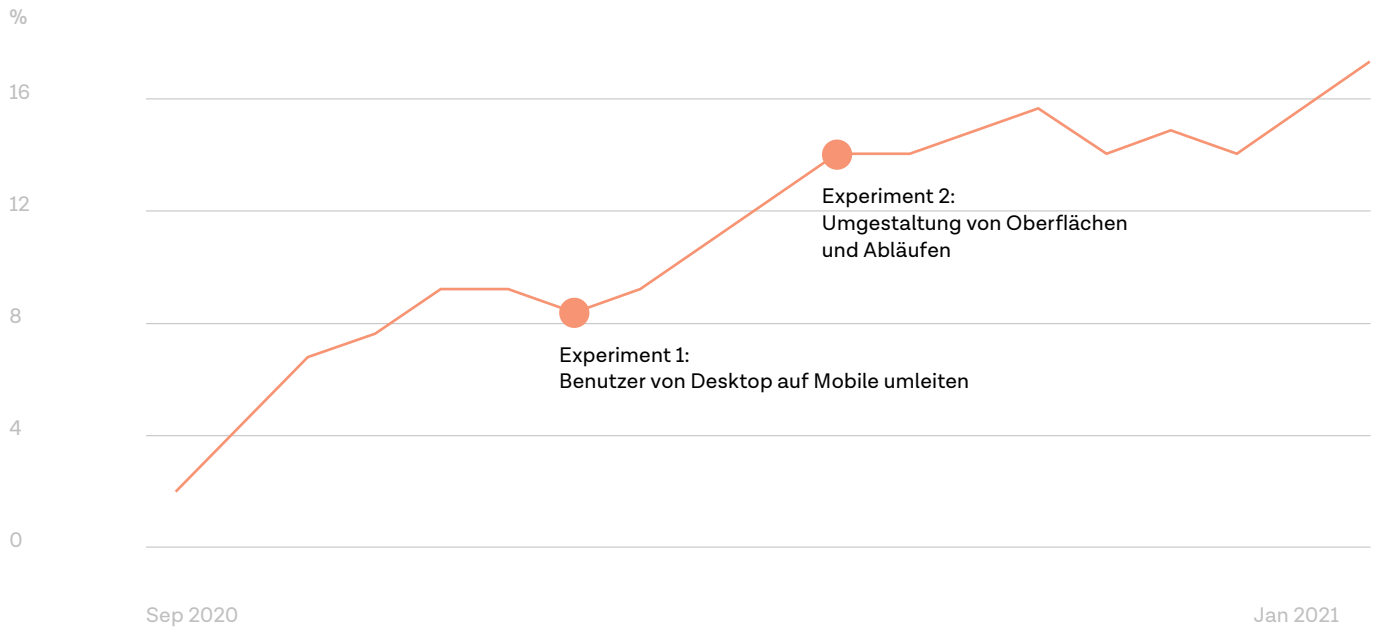
Interessanterweise entsprach die Konversionsrate mobiler Nutzer den internen Vorgaben. Der eigentliche Einbruch wurde durch den Authentifizierungsprozess auf einem Desktop-Computer verursacht. Das liegt daran, dass die meisten Finanzinstitute große Investitionen in die Verbesserung ihres mobilen Bankings getätigt haben, aber ihre Desktop-Anwendungen noch immer ziemlich schlecht sind.

Das Ergebnis war verständlicherweise eine sehr hohe Abbruchrate. Mit dieser wichtigen Erkenntnis begannen wir, Login-Flows für die verschiedenen Banken zu sammeln, Problemstellen zu ermitteln, Ideen zu deren Verbesserung zu entwickeln und Gespräche mit den relevanten Banken sowie den lokalen Aufsichtsbehördenzu führen. Nach mehreren Experimenten fanden wir heraus, dass die beste Lösung darin bestand, QR-Codes zu verwenden, um die Benutzer vom Desktop auf das Mobiltelefon umzuleiten, um den Authentifizierungsprozess abzuschließen und alle Hürden zu umgehen, die bei der Desktop-Authentifizierung vorhanden waren.

Der erste Durchlauf dieses neuen "QR-Code-Übergabebildschirms" wurde innerhalb weniger Tage eingeführt. Wir haben unserem Datenanalyseteam die Lösung präsentiert und auf ihr Urteil gewartet: Haben sich die Erfolgsraten verbessert? Die Ergebnisse waren ermutigend, entsprachen aber immer noch nicht unseren Erwartungen. Der nächste Schritt war Designer hinzuzuziehen. Unser Produktdesign-Team nahm mehrere Verbesserungen vor, reduzierte die Anzahl an QR-Codes und erstellte klareren Anweisungen für den Benutzer. Wir entfernten auch die Option für den Benutzer, zwischen dem Desktop- und dem mobilen Prozess zu wählen, und baten ihn, den Authentifizierungsprozess vollständig auf dem Smartphone abzuschließen.

Die Ergebnisse waren hervorragend: Diejenigen, die den QR-Code nutzten, wiesen eine um 62 % höhere Erfolgsquote auf, als denjenigen, die beim Desktop-Prozess blieben.

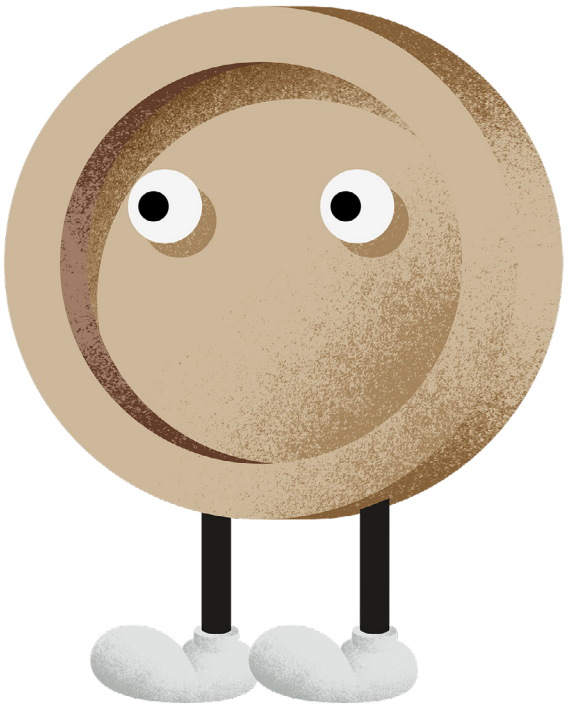
Relative prozentuale Verbesserung der Erfolgsrate



Dieses Beispiel verdeutlicht zwei Dinge:

→ Der Übergang vom physischen zum digitalen Banking ist chaotisch, erfordert ein tiefes Verständnis des Marktes und in vielen Fällen einzigartige Lösungen. Das klingt nicht sehr skalierbar, entspricht aber der aktuellen Situation.

→ Die Bedeutung von funktionsübergreifenden Disziplinen bei der Verbesserung des gesamten Benutzererlebnisses. Die Säulen einer solchen Verbesserung sind eine Mischung aus technischem und Design-Know-how, kombiniert mit einem datengesteuerten Ansatz zum Verständnis der Problempunkte, die die Benutzer erleben.



Die Branche voranbringen

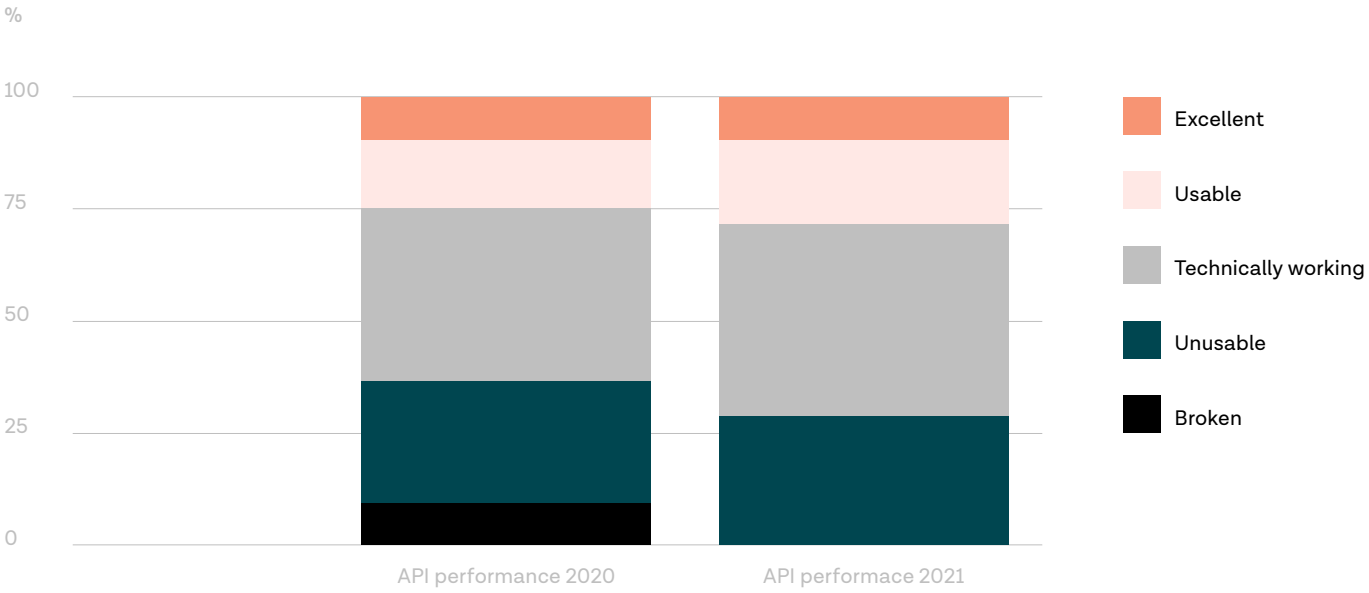
Die Branche voranbringen

Neben der technischen Seite des Aufbaus und der Optimierung von Verbindungen müssen TPPs auch ständig mit ASPSPs, Regulatoren und Finanzbehörden in Kontakt bleiben. Regulierungen wie PSD2 und RTS sind komplex, und TPPs spielen eine wertvolle Rolle dabei, die Branche voranzubringen, indem sie kurzfristige Probleme hervorheben, ASPSPs in die Pflicht nehmen, wenn Regulierungen nicht eingehalten werden, sowie die langfristige Vision von Open Banking im Blick behalten.

Kurzfristige Vision

Kurzfristig arbeiten TPPs mit ASPSPs zusammen, um Probleme zu lösen, die unmittelbare Auswirkungen haben, wie z. B. unerwartete Änderungen an APIs, fehlende Dokumentation, veraltete Testumgebungen und Serverausfälle ohne vorherige Kommunikation mit TPPs. In den meisten Fällen reicht die direkte Kommunikation mit ASPSPs aus, aber in Fällen, in denen keine Maßnahmen ergriffen werden, müssen TPPs die Probleme an die zuständigen Behörden weiterleiten.

Die gute Nachricht ist, dass diese anfänglichen Investitionen beginnen, wirklich Früchte zu tragen. In den letzten Jahren hat sich die API-Leistung unter den ASPSPs erheblich verbessert.



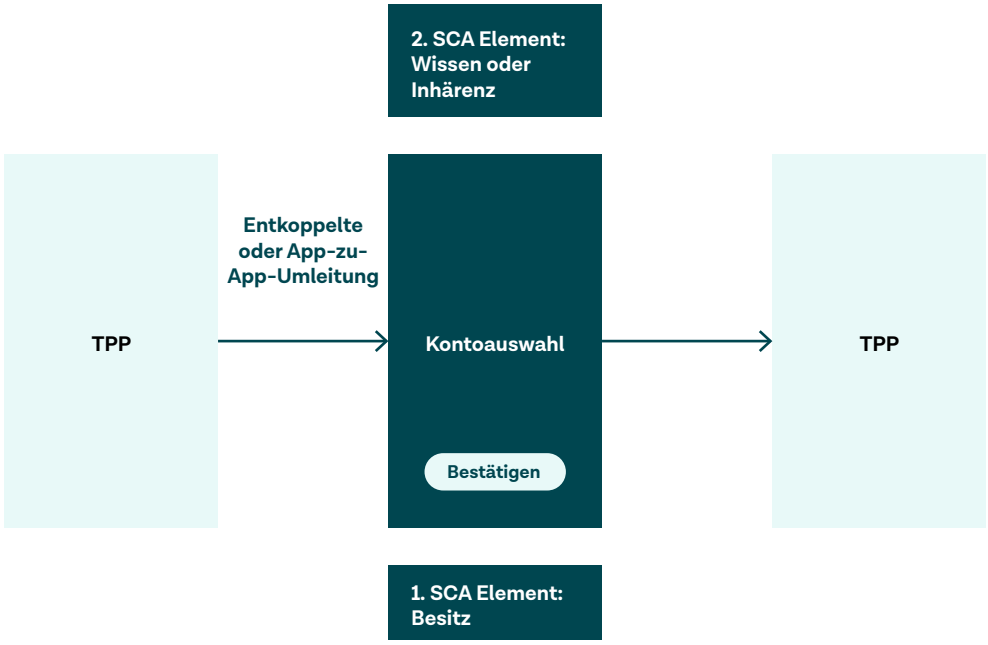
Die Abbildung oben zeigt den Status der PSD2-APIs von Großbanken in zwölf Ländern. Wir führen diese Bewertungen in regelmäßigen Abständen durch, um die neuesten Verbesserungen der API-Leistung zu messen.

- → **Unterbrochen:** Die PSD2-API ist nicht vorhanden oder funktioniert nicht.
- → **Unbenutzbar:** Die PSD2-API funktioniert, aber der Weg zur Authentifizierung ist für den Endbenutzer extrem umständlich, erfordert mehrere nicht-intuitive Schritte, mehrere SCAs und eine Web-Umleitung.
- → **Technisch funktionierend:** Die PSD2-API funktioniert, aber der Authentifizierungsprozess bietet keine App-zu-App-Umleitung und hat unnötige Fenster.
- → **Verwendbar:** Die PSD2-API ist nutzbar und bietet eine App-zu-App-Umleitung. Allerdings enthält der Authentifizierungsprozess immer noch unnötige Fenster.
- → **Ausgezeichnet:** Die PSD2-API bietet eine App-zu-App-Umleitung und hat keine unnötigen Bildschirme. Der Authentifizierungsprozess für die Benutzer ist optimiert.

Langfristige Vision

Die Anbindung an eine Bank-API um der Anbindung willen bedeutet sehr wenig, wenn die langfristige Vision einer kundenzentrierten, wettbewerbsfähigen und innovativen Finanzbranche in Debatten um Regulierung, Technologie und Prozesse untergeht. Dies erfordert, dass TPPs einen klaren Blick auf das Endkundenerlebnis haben und Zeit und Ressourcen in die Verwirklichung der Zukunft investieren.
Der beste Weg, dies zu tun, ist mithilfe von Daten. TPPs müssen eine Kultur etablieren, die beinhaltet, dass ständig getestet wird, Problemstellen, die bei der Verbindung mit einer API auftreten, ermittelt werden und Erkenntnisse und Daten mit den ASPSPs geteilt werden.

Die Verwendung objektiver, quantitativer Daten über die Auswirkungen eines unzureichenden Benutzererlebnisses macht es einfacher, konstruktive Gespräche mit ASPSPs und Regulierungsbehörden zu führen. Obwohl es sich hierbei um ein Gefangenendilemma handelt, bei dem ein TPP davon profitiert, dass jemand anderes die Lobbying-Investitionen tätigt, sind die langfristigen Auswirkungen besserer Prozesse und Endbenutzererfahrungen von großem Nutzen für die gesamte Branche. Zum Beispiel konzentriert sich ein großer Teil der Lobbyarbeit von Tink darauf, die folgende Abbildung zum Standard-Prozess in Europa zu machen.



- ✓ Alle Authentifizierungsverfahren werden vom ASPSP bereitgestellt (Art 30.2 der RTS)
- ✓ Der PSU wird auf die Authentifizierungs-App des ASPSP umgeleitet (Absatz 16.1 der EBA-Stellungnahme)
- ✓ Starke Kundenauthentifizierung (Strong Customer Authentication, SCA) erfüllt (Art 97 der PSD2)

Um die langfristige Vision von Open Banking zu beeinflussen, beteiligt sich Tink aktiv an Lobbygruppen und Fachverbänden wie ETPPA, PSD2 SIG, PayBelgium, Fintech Norway, UK Finance und der European Payments Association.

Fazit

Die wichtigste Erkenntnis ist wohl die, dass der Aufbau von Konnektivität eine langfristige strategische Investition ist. Die Branche bewegt sich sehr schnell. Um mit diesem Tempo Schritt zu halten, sind Fokus und gezielt eingesetzte Ressourcen erforderlich.

Mit Tink müssen Sie diesen Kraftakt jedoch nicht mehr alleine stemmen. Mit unserer Open-Banking-Plattform können Sie sich mit über 3.400 Banken und Instituten europaweit verbinden und erhalten angereicherte sowie kategorisierte Finanzdaten über eine zentrale API. Wir konzentrieren uns auf Konnektivität, damit Sie sich auf Innovation und intelligente Finanzdienstleistungen konzentrieren können.

Sie möchten mehr darüber erfahren, wie Sie auf Echtzeit-Finanzdaten zugreifen können?
Unsere Experten beantworten gerne Ihre Fragen - sprechen Sie uns einfach an:

partnerships@tink.com

tink.com