Guide Tink

La connectivité open banking

Ce que nécessite la connexion aux APIs open banking - et pourquoi ce n'est pas aussi simple qu'il y paraît

tink
A Visa Solution

En apparence, se connecter à une API open banking peut paraître assez simple. Depuis l'entrée en vigueur de la DSP2 en 2018, tous les ASPSP en Europe sont tenus de fournir un accès gratuit aux données clients via des APIs. La connexion, une fois effectuée auprès d'une banque ou d'une institution financière, devrait être maintenue sans accroc indéfiniment. Vraiment ?

Et bien non.

Un élément très simple manque à cette équation : les ASPSP ne reçoivent pas d'argent pour fournir l'accès aux données via les API. Cet investissement à long terme est certes en phase avec l'idée et la vision d'un système financier plus ouvert, mais, dans l'immédiat, il ne paie pas les factures. Conséquence : les équipes des ASPSP chargées de gérer ces API sont souvent en sous-effectif.

Les plateformes open banking comme Tink constituent un rouage important de ce nouvel écosystème. Elles collaborent avec les ASPSP pour surveiller en permanence leurs connexions, trouver les bugs, signaler les problèmes et communiquer régulièrement avec leurs équipes d'ingénieurs. Ce défi, tant opérationnel que technique, nécessite des investissements considérables en temps, en personnel et en infrastructure.

Ce guide retrace l'ensemble du processus et explique pourquoi la connexion à une API open banking va bien au-delà du raccordement initial.

Ce que vous trouverez dans ce guide

Que signifie réellement se connecter aux APIs Open Banking ?

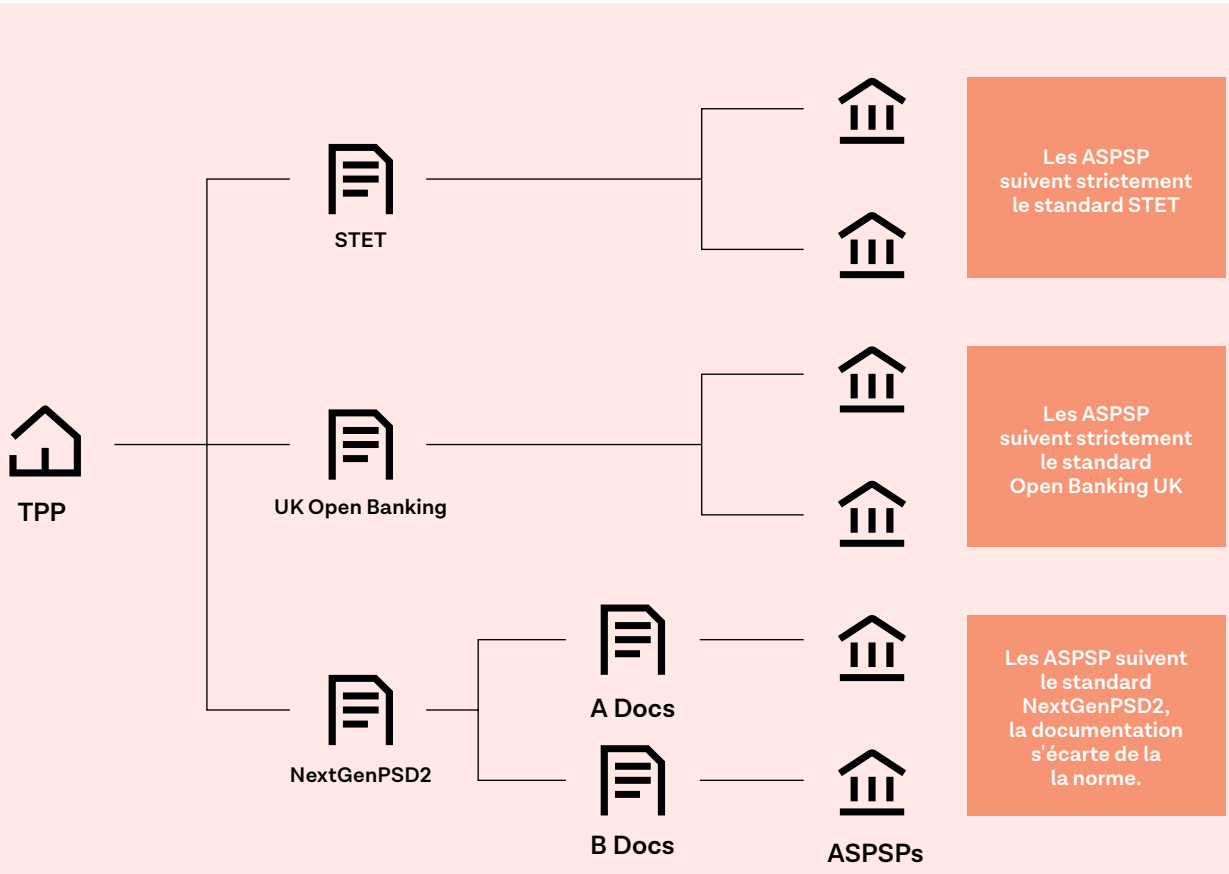
La mise en place de connexions dans plusieurs pays est une entreprise complexe qui nécessite des investissements significatifs, notamment aux plans technique, opérationnel et juridique. Pour l'illustrer, prenons l'exemple d'un fournisseur tiers (TPP) se connectant à des services de paiement gestionnaire de compte (ASPSP) à travers l'Europe. Le schéma ci-dessous représente l'intégralité du processus d'optimisation des connexions aux APIs bancaires, la connexion à une banque n'étant que la première étape de la chaîne de valeur.

Se connecter à une API Open Banking

Établir des connexions avec les banques

1.1 Comprendre les standards européens

La connexion à une API open banking nécessite une connaissance avancée des normes utilisées par les banques dans différents pays. En Europe, il existe trois principaux standards :



STET : Le standard STET DSP2 API, principalement utilisé en France, est plus contraignant que le standard NextGenPSD2. La principale différence réside dans le protocole de demande d'authentification, utilisé pour confirmer la non altération des informations par un TPP.

UK Open Banking : Le standard Open Banking UK se présente comme le moins flexible, la plupart des ASPSP britanniques adoptant quasi-directement sa mise en oeuvre, avec de très petits ajustements. Il s'agit du standard le plus mature, créé depuis 2018 et testé soigneusement par des centaines de TPP, tandis que son développement et son implémentation ont été surveillés par la CMA (Competition and Markets Authority) et la FCA (Financial Conduct Authority).

NextGenPSD2 : Le standard NextGenPSD2 Access to Account (XS2A) du Berlin Group permet d'accéder à l'architecture de l'API et à une mise en œuvre flexible. Les ASPSP ont ici la possibilité de s'écarter du standard et de l'implémenter selon leurs propres exigences. The Berlin Group exige des ASPSP qu'ils soumettent les demandes de changement au comité qui régit le standard, ce qu'ils font pourtant rarement. En résultent une importante disparité entre mises en œuvre du standard et un fort degré de divergence entre les API open banking. Il s'agit du standard le plus couramment adopté en Europe.

1.2 S'enregistrer auprès des ASPSP

La deuxième étape consiste à s'enregistrer auprès des ASPSP, via un enrôlement manuel ou dynamique.

Les enrôlements manuels nécessitent une communication entre le TPP et l'ASPSP, comme l'enregistrement sur le portail des développeurs, la création d'une application ou l'envoi d'emails aux ASPSP pour obtenir un accès. Ce processus n'est pas chronophage pour les développeurs, mais peut prendre de quelques jours à plusieurs mois, en fonction du niveau de maturité de l'API DSP2. Malheureusement, les enrôlements manuels sont la norme en Europe et environ 15 % seulement des ASPSP européens proposent des enregistrements dynamiques.

Les enregistrements dynamiques sont effectués par le biais d'une API et, si le procédé est réalisé correctement, l'ASPSP répertorie automatiquement le TPP. L'enregistrement dynamique nécessite un investissement initial important, mais il est facile à reproduire, permettant des inscriptions automatiques sans aucun travail supplémentaire.

Tink a investi des ressources significatives dans le développement d'outils internes d'enregistrements dynamiques qui nous permettent un accès direct à différentes APIs d'enrôlements et de connecter quasi-instantanément nos clients.

1.3 Etablir la connexion

En théorie, le processus permettant d'établir une connexion est relativement simple, car il exige que le TPP suive la documentation publiée par l'ASPSP. La réalité, cependant, peut être beaucoup plus complexe.

Les défis à relever pour se connecter aux APIs Open Banking sont différents selon l'ASPSP et le pays. La connexion à certains ASPSP est relativement facile, tandis que d'autres nécessitent un investissement en temps plus conséquent .

Heureusement, la plupart des APIs Open Banking ont aujourd'hui atteint un niveau de maturité tel que ce type d'investissement n'est plus nécessaire et que la connexion peut se faire beaucoup plus rapidement. Néanmoins, voici quelques mesures que les TPP devraient envisager :

→ Mettre en place une équipe de liaison avec la structure de soutien des ASPSPs lorsque la documentation n'est pas claire ou obsolète

→ Se familiariser avec les spécificités techniques, à la fois locales (propres à l'ASPSP ou au marché, par exemple celles des APIs au Royaume-Uni) et à échelle globale (avec des standards plus répandus, par exemple la méthode d'authentification JWT). Les développeurs pourront ainsi mieux comprendre les exigences sous-jacentes des programmes utilisés et résoudre rapidement les bugs.

→ Concevoir une architecture centrale flexible pour prendre en charge une variété de connexions ASPSP. Les standards techniques mentionnés à la section 1.1 sont le socle des APIs Open Banking, mais la configuration permettant d'accéder au compte dépend de l'ASPSP. La structure sous-jacente est fondamentale, de légères modifications pouvant impacter d'autres connexions entraînant ainsi de possibles ruptures de transmission.

→ Prendre en charge l'ensemble des méthodes cryptographiques afin de minimiser les frictions pour les utilisateurs et les plugger en fonction du standard exigé par chaque ASPSP. Par exemple, Open Banking UK exige 5 méthodes cryptographiques différentes et largement utilisées par les ASPSP.

→ Investir dans la formation des développeurs et leur donner les clefs d'une parfaite compréhension des normes, systèmes et processus. Les ressources nécessaires pour effectuer ces tâches en programmation sont coûteuses et augmentent (à quelle vitesse?) avec chaque nouvelle connexion.

Pour son premier grand client utilisant des APIs Open Banking, Tink a déployé une équipe de 5 développeurs, testant et remédiant aux bugs sur l'ensemble de la plateforme, sur un seul marché et pendant 6 mois au total. Nous avons échangé plus de 1500 e-mails et généré des dizaines de tickets avec les banques avant que la solution ne soit prête à être utilisée.

Faire fonctionner la solution

2.1 Tester et stabiliser les connexions

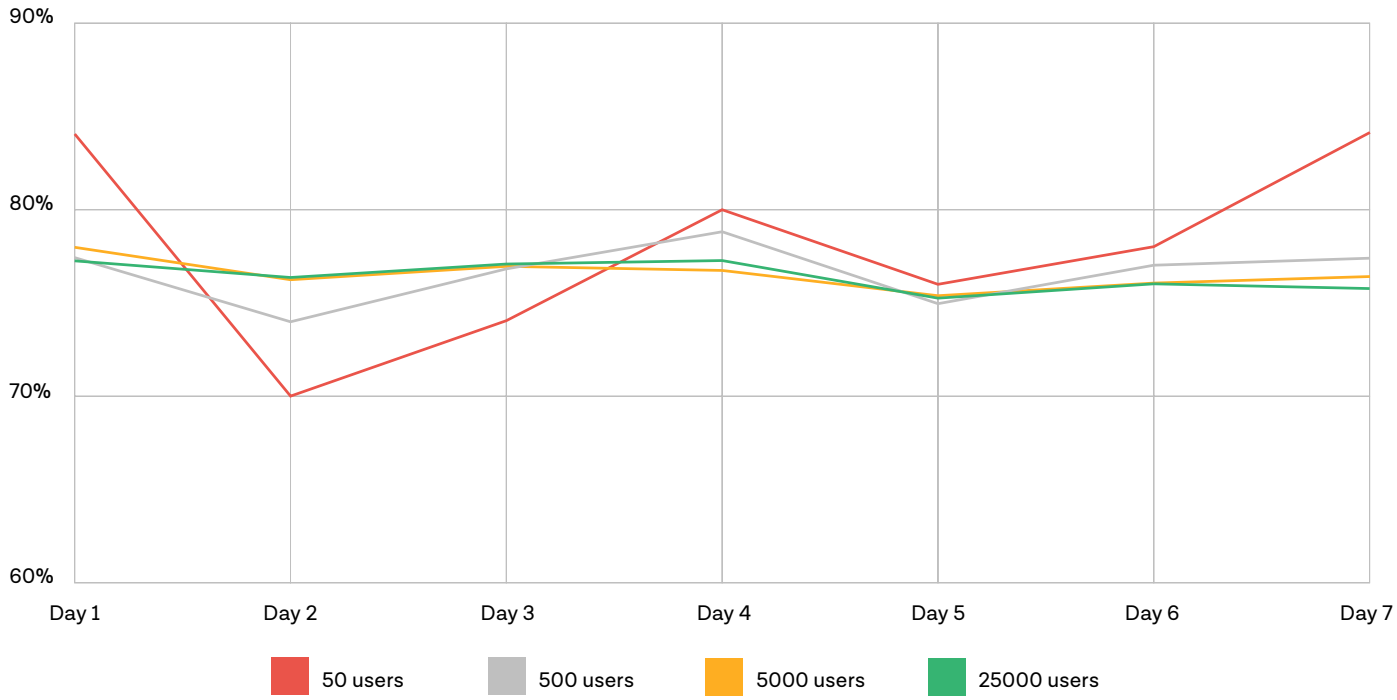
Une fois les connexions établies, elles doivent passer une série de tests rigoureux pour s'assurer de leur stabilité et de leur bon fonctionnement. Voici un processus de test type :

1. Ouvrir des comptes bancaires dans l'ensemble des banques d'un pays, tester les connexions dans des conditions réelles d'identification et fournir aux développeurs un rapport sur leurs tests de l'expérience utilisateur.
2. Examiner tous les cas particuliers avec un grand nombre d'utilisateurs (une fois cette première phase de tests terminée)
3. Enregistrer l'ensemble des parcours utilisateurs finaux et collecter les preuves d'erreurs en cas d'échec du test.

Si un TPP prévoit de gérer plusieurs cas d'usages, il est nécessaire de disposer d'un volume important de clients différents et d'utilisations variées, afin d'offrir une image exhaustive des performances d'une connexion. Ainsi, le fait de tester une connexion sur des clients familiers du numérique, dépassant les désagréments rencontrés lors d'un processus d'authentification, pourrait être faussement interprété comme une connexion qui fonctionne bien, avec des taux de conversion élevés. En réalité, nombreux sont les utilisateurs ne pouvant pas surmonter ces mêmes obstacles, ce qui entraîne une forte baisse des taux de conversion. Les TPP doivent donc réfléchir à la manière dont tous les types de clients peuvent être affectés et à la façon de les guider tout au long de leur parcours.

Sur le graphique ci-dessous, nous utilisons des données réelles pour illustrer l'intérêt d'augmenter le nombre d'utilisateurs afin de tester la stabilité d'une connexion. La ligne rouge montre la volatilité des taux de réussite lorsqu'il y a 50 utilisateurs, tandis que la ligne verte montre un taux de réussite relativement stable dès que le trafic dépasse 25000 utilisateurs.

Le taux de réussite d'une connexion se stabilise dès que le nombre d'utilisateurs augmente



2.2 Faire fonctionner au quotidien

L'étape suivante consiste à s'assurer que les connexions fonctionnent correctement au quotidien et à résoudre les problèmes qui surviennent sur le long terme.
Pour ce faire, les TPP doivent mettre en place un système permettant de mesurer en permanence la qualité de chaque connexion, de générer des alertes automatiques lorsque les connexions ne répondent pas aux standards de qualité et de disposer de développeurs d'astreinte formés pour répondre à de telles situations.

Les alertes ne nécessitent pas toujours une attention immédiate, ni d'intervenir avec du code, car il arrive que les services des ASPSP soient hors service. Cependant, les TPP doivent s'assurer d'identifier chaque incident ou risque, de remonter à l'origine du problème et d'informer les clients si nécessaire.

Faire fonctionner une solution sur le long terme nécessite de veiller constamment à effectuer des tests appropriés et des procédures quotidiennes ; cette réalité est souvent sous-estimée lorsqu'une décision est prise d'internaliser le développement des connexions.

Chez Tink, nous avons mis en place un système complet d'alertes et d'astreintes pour suivre les changements incessants. Notre système d'alertes définit une série de priorités et des seuils qui tiennent compte de la gravité du problème et du nombre d'utilisateurs touchés. Dès que le nombre d'erreurs franchit le seuil, un message est acheminé à l'équipe responsable de l'API pour qu'elle l'évalue et lui donne la priorité en fonction de la gravité du problème.

Etat des services sur Tink.com

Services d'agrégation — Opérationnel

90 jours plus tôt — 99.92% Temps de fonctionnement — Aujourd'hui

Services de paiement — Opérationnel

90 jours plus tôt — 99.86% Temps de fonctionnement — Aujourd'hui

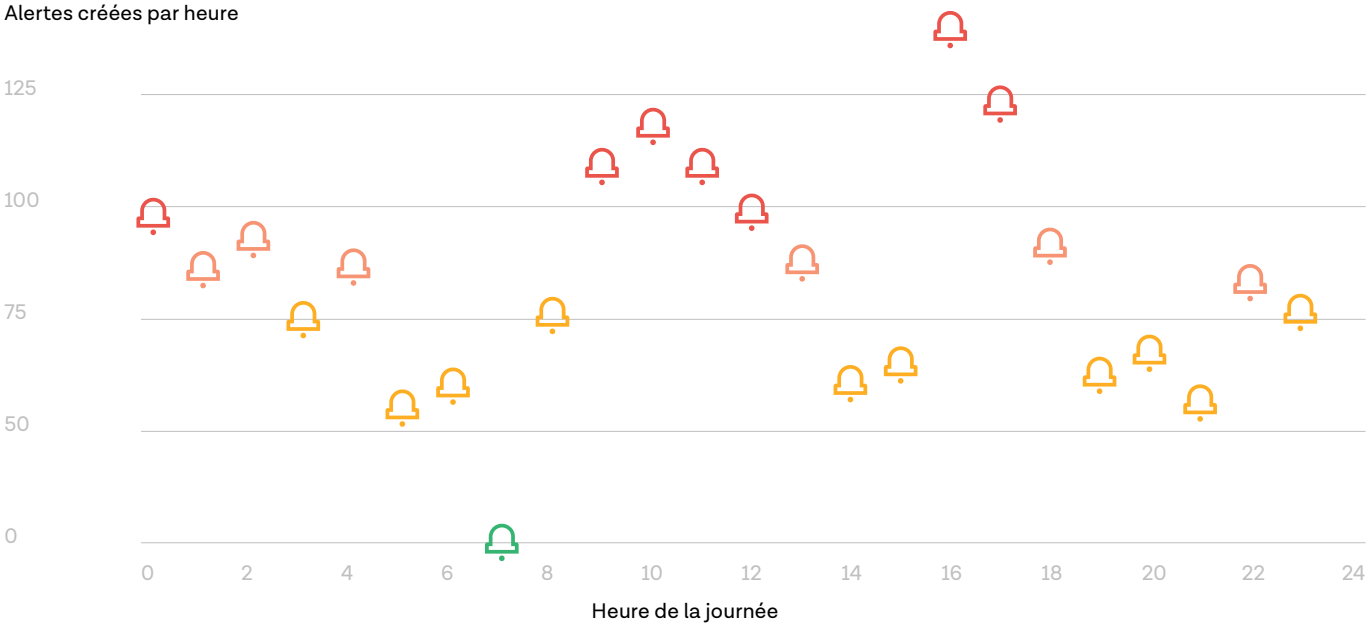
Services PFM — Opérationnel

90 jours plus tôt — 100% Temps de fonctionnement — Aujourd'hui

Services d'enrichissement des données — Opérationnel

90 jours plus tôt — 100% Temps de fonctionnement — Aujourd'hui

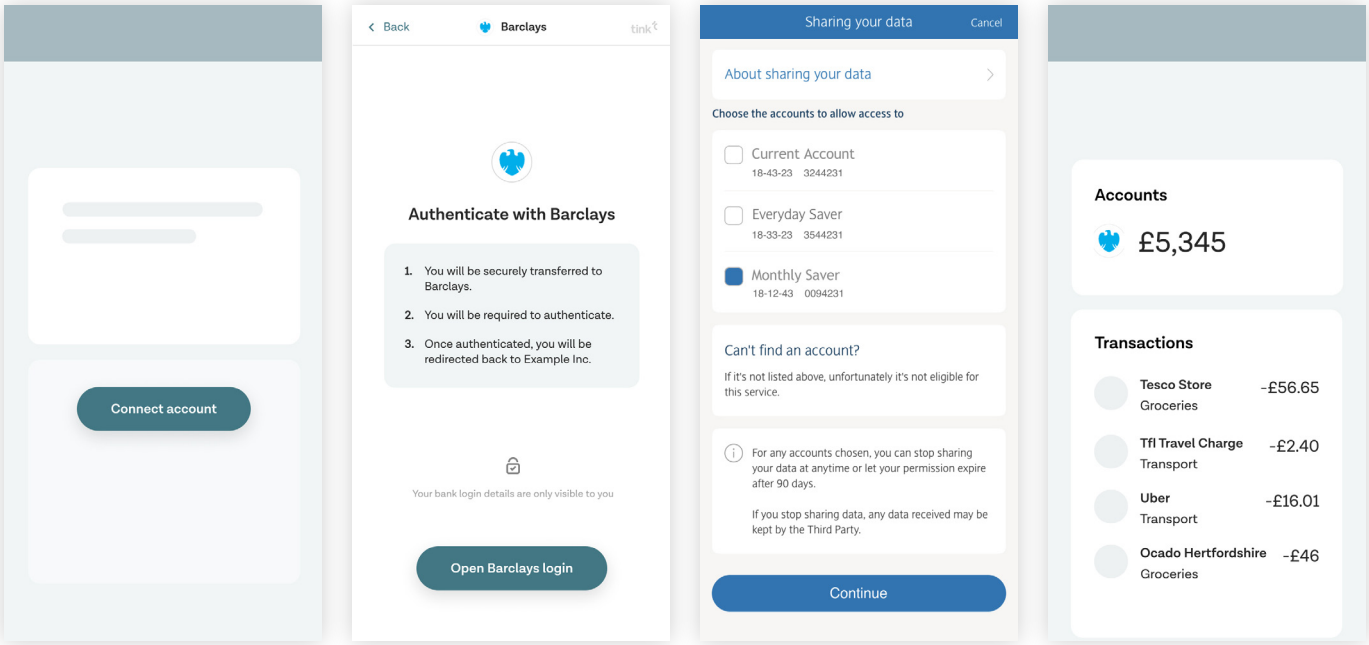
Tableau de bord des alertes



Améliorer l’expérience utilisateur

Tout le temps et les efforts consacrés à la mise en place et au bon fonctionnement des connexions bancaires aboutissent à ce moment si important, celui où les TPP demandent aux utilisateurs finaux leur consentement pour accéder à leurs comptes bancaires. C'est ici que l'expérience utilisateur entre en jeu. Une bonne UX est la combinaison d'une connaissance opérationnelle des flux d'authentification, d'une capacité à masquer cette complexité à l'utilisateur final et à la transformer en un parcours simple et transparent.

Chez Tink, nous parvenons à cette UX grâce à Tink Link, notre front-end SDK, qui gère et optimise l'authentification ASPSP.



L'objectif est de s'assurer que les utilisateurs finaux remplissent les exigences liées à l'authentification forte, stipulant qu'un utilisateur doit s'identifier via deux de ces trois procédés : la possession (par exemple, le téléphone), la connaissance (par exemple, le mot de passe) et l'inhérence (par exemple, la biométrie). Pour la plupart des utilisateurs finaux, cela peut ressembler à une simple succession d'écrans de connexion. Il existe en réalité beaucoup de paramètres complexes en arrière-plan, comme le type de connexion, le type d'appareil, le pays et la langue, entre autres variables. Le plus grand défi réside peut-être dans les nombreuses étapes du parcours de l'utilisateur qui échappent au contrôle du TPP. En effet, en raison de l'absence de consensus au sein du secteur sur la manière dont les ASPSP devraient vérifier l'identité des utilisateurs, les TPP doivent souvent construire des flux d'authentification sur mesure, ce qui crée un nombre impressionnant de configurations potentielles.

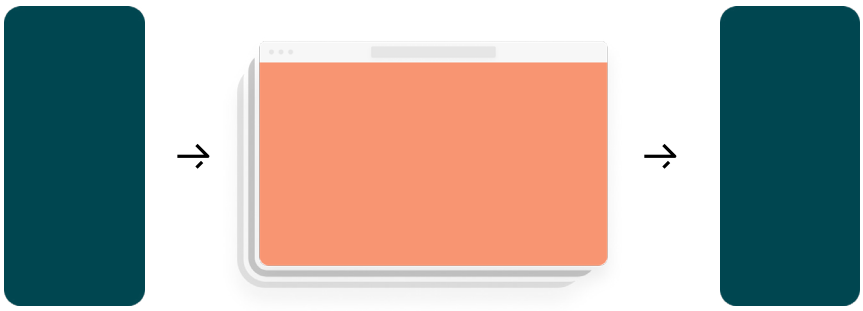
Les scénarios types incluent les redirections découplées, intégrées, web et app.

Les flux d'authentification courants en Europe

Découplé
(Suède)

Intégré
(Allemagne)

Redirection Web
(Espagne, Italie)



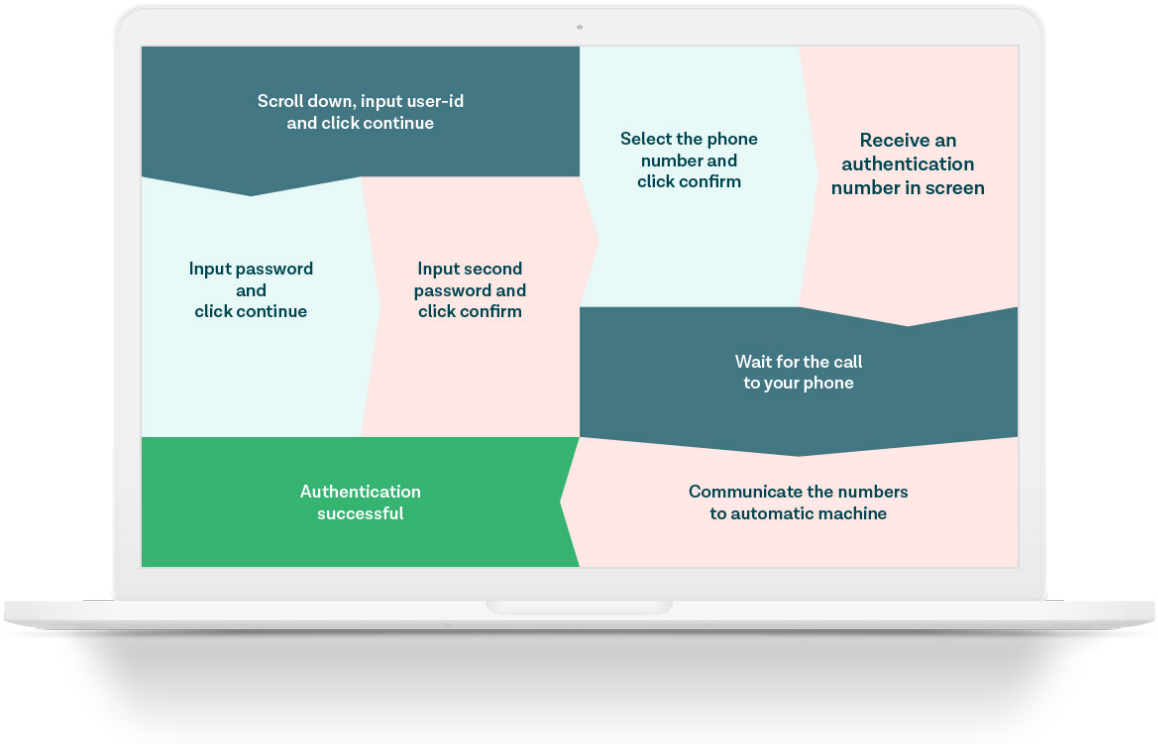
Redirection vers Application
(Royaume-Uni, France*)

*banques principales

Etude de cas

Pour illustrer le processus complexe qui se cache derrière l'amélioration de l'expérience client, prenons l'exemple récent d'un client qui souhaitait supprimer des étapes manuelles lors du parcours de connexion. L'amélioration de l'onboarding des utilisateurs est un cas d'usage bien connu de l'open banking et nous l'avons déjà mis en place pour un certain nombre de clients. Nous authentifions les utilisateurs, récupérons leurs informations de compte, connectons les comptes bancaires et la chose est faite ! Nos équipes ont passé quelques mois sur le travail d'intégration mais lorsque celui-ci fut terminé, nous avons été surpris de constater que le taux de conversion des nouveaux utilisateurs finissant l'ensemble du processus d'onboarding était décevant. Nous avons donc commencé à creuser dans les données pour comprendre ce qui se passait.

De manière surprenante, le taux de conversion des utilisateurs mobiles terminant de bout en bout la procédure d'onboarding correspondait à nos benchmarks. La raison du décrochage : l'utilisation d'un ordinateur pour commencer et terminer le parcours d'authentification. En effet, la plupart des institutions financières au Royaume-Uni ont réalisé des investissements importants pour améliorer leurs parcours bancaires mobiles, mais ceux des ordinateurs demeurent encore assez médiocres.



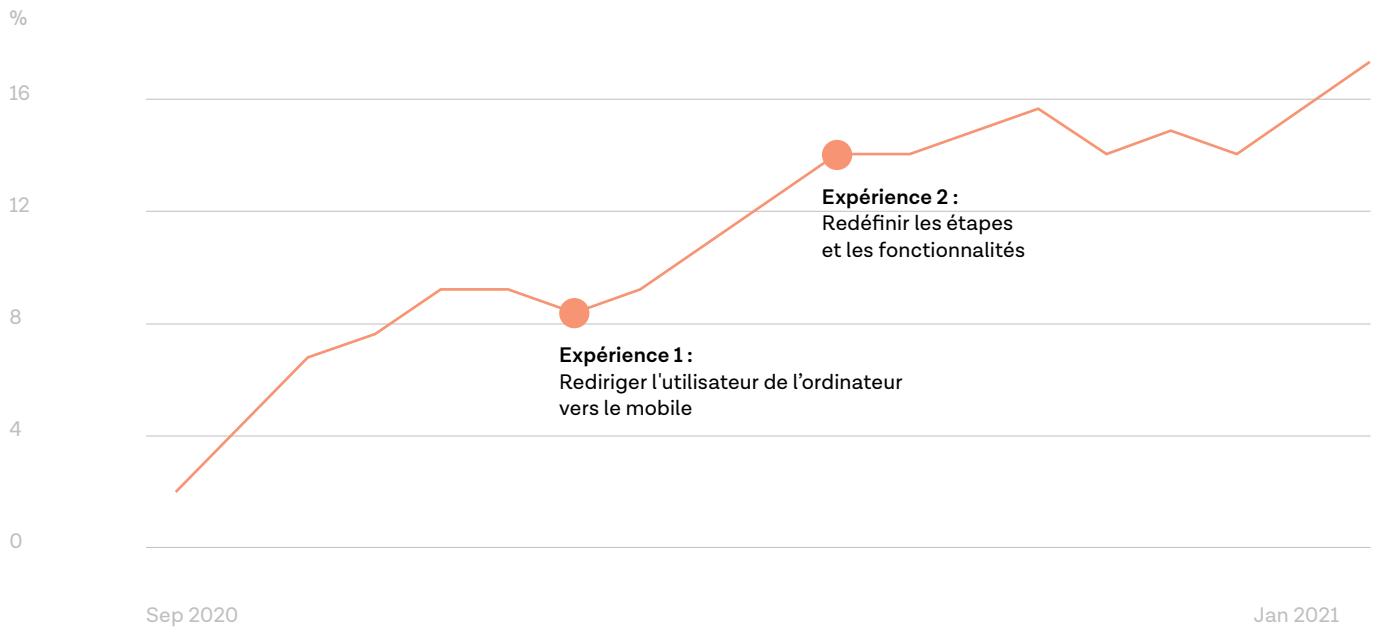
Résultat : un taux d'abandon très élevé. Éclairés par ces données instructives, nous avons commencé à rassembler les parcours de connexions de chaque banque du pays, à identifier les points de friction, à chercher les axes d'améliorations et à engager des discussions avec les banques concernées ainsi qu'avec le groupe de travail britannique l'OBIE (Open Banking Implementation Entity).

Après plusieurs essais, nous avons constaté que la meilleure solution était d'utiliser des QR codes pour rediriger les utilisateurs d'ordinateur vers leur mobile afin de compléter le processus d'authentification et contourner tous les obstacles qui étaient présents dans le parcours du bureau.

La première étape de ce nouveau parcours basé sur les QR codes a été déployée en quelques jours. Nous avons réuni notre équipe de data analyst et attendu leur verdict : les taux de réussite se sont-ils améliorés ? Les résultats étaient encourageants, mais ne répondaient toujours pas à nos attentes. L'étape suivante consistait à faire appel à des designers. Notre équipe produit a apporté plusieurs améliorations, de la réduction de la densité du QR code à la demande d'instructions plus claires à l'utilisateur. Nous avons également supprimé l'option permettant à l'utilisateur de choisir entre un parcours sur ordinateur et un parcours sur mobile et lui avons demandé d'effectuer le processus d'authentification entièrement sur son téléphone.

Les résultats furent époustouflants ! Les utilisateurs du QR code ont augmenté leur taux de réussite de 62% par rapport à ceux utilisant toujours leur ordinateur.

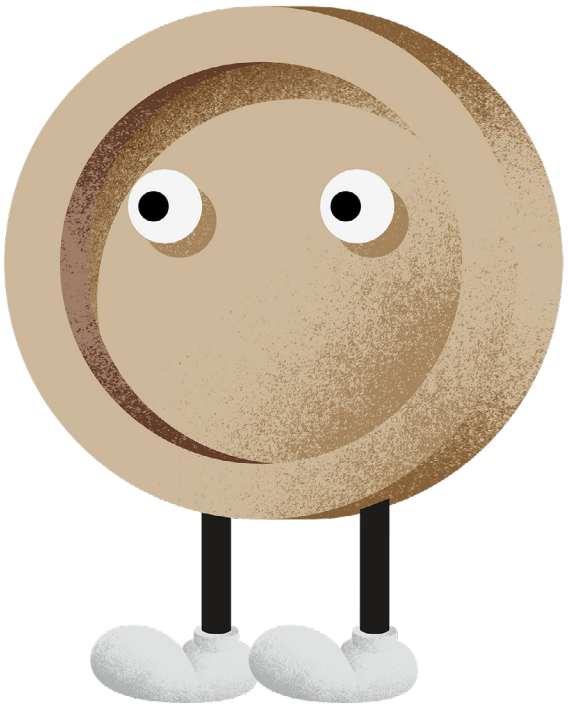
Evolution du taux moyen de réussite du parcours de bout en bout (en %)



Cet exemple met en évidence deux choses :

→ **Sur le secteur :** La transition de la banque traditionnelle vers la banque numérique est encore désordonnée, nécessite une compréhension approfondie du marché et, dans de nombreux cas, des solutions ad hoc. Même si cela semble un peu réducteur, c'est là où nous en sommes pour le moment.

→ **Sur l'UX :** L'importance des disciplines transversales pour améliorer l'expérience globale de l'utilisateur. Les piliers d'une telle amélioration sont un mélange d'expertise technique et de design, combiné à une approche fondée sur la donnée pour identifier les points de frictions que rencontrent l'utilisateur.



Amener le secteur plus loin

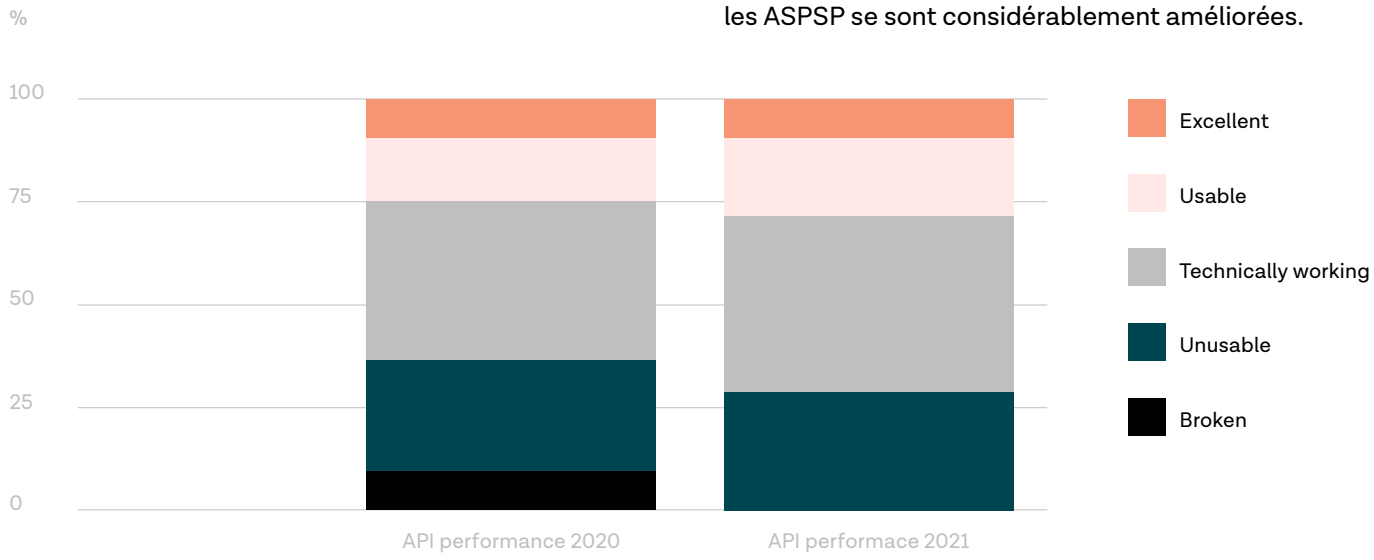
Faire avancer l'industrie

Outre l'aspect technique de développement et d'optimisation des connexions, les TPP doivent également maintenir un lien constant avec les ASPSP, les régulateurs et les autorités financières. Les réglementations telles que la DSP2 et les RTS sont complexes, et les TPP jouent un rôle essentiel pour faire avancer le secteur en soulignant les problèmes à court terme, mettant les ASPSP face à leur responsabilité lorsque les réglementations ne sont pas respectées. Parallèlement, les TPP doivent rester concentrés sur la vision à long terme de l'open banking.

A court terme

À court terme, les TPP collaborent avec les ASPSP pour résoudre les problèmes à conséquence immédiate, comme des modifications inattendues des API, de la documentation manquante, des environnements de test obsolètes et les temps d'arrêt des serveurs non communiqués préalablement aux TPP. Dans la plupart des cas, une communication directe avec les ASPSP suffit ; lorsqu' aucune mesure n'est prise, les TPP doivent faire remonter les problèmes auprès des autorités compétentes.

Bonne nouvelle, les investissements initiaux commencent à porter réellement leurs fruits ; au cours des dernières années, les performances des API parmi les ASPSP se sont considérablement améliorées.



Le graphe ci-dessus montre l'état des API PSD2 des principales banques dans 12 pays. Nous effectuons ces évaluations périodiquement pour mesurer les dernières améliorations des performances des API.

→ En panne : L'API DSP2 est inexistante ou ne fonctionne pas.

→ Inutilisable : L'API PSD2 fonctionne mais le parcours d'authentification est extrêmement laborieux pour l'utilisateur final, nécessite plusieurs étapes non intuitives, de multiples SCA (Strong Customer Authentification) et une redirection web.

→ Techniquement fonctionnel : L'API DSP2 fonctionne mais le parcours d'authentification n'offre pas de redirection app-to-app et comporte des étapes inutiles.

→ Utilisable : L'API DSP2 est utilisable et offre une redirection app-to-app. Cependant, le flow d'authentification contient encore des étapes inutiles.

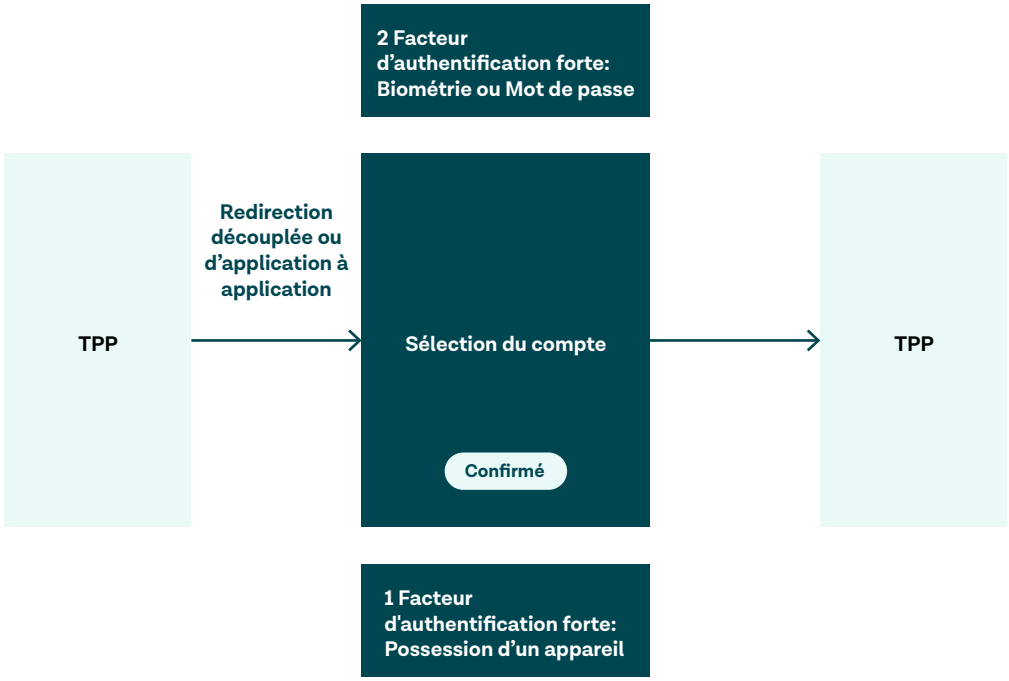
→ Excellent : L'API DSP2 offre une redirection app-to-app et ne comporte pas d'étapes inutiles. Les écrans sont optimisés pour permettre à l'utilisateur de s'authentifier rapidement.

Vision à long terme

Se connecter à une API bancaire pour le principe n'a pas beaucoup de sens ; la promesse à long terme d'une industrie financière davantage centrée sur le client, plus compétitive et plus innovante ne doit pas se perdre dans des débats de réglementation, de technologie et de processus.

Pour les TPP, il est essentiel d'avoir une vision claire de l'expérience de l'utilisateur final, et d'investir du temps et des ressources pour transformer cette promesse en réalité. Le meilleur moyen d'y parvenir est d'utiliser les données. Les TPP doivent créer une culture de tests constants, qui répertorie les obstacles rencontrés lors de la connexion à une API, et de partage des idées et des données avec l'ASPSP.

L'utilisation de données objectives et quantitatives prouvant un flux d'utilisateur inférieurs à la normale permet d'engager plus facilement des conversations constructives avec les ASPSP et les régulateurs. L'industrie progresse aussi grâce aux démarches des différents acteurs en matière de régulation, les implications à long terme de meilleurs user-flows et de l'expérience de l'utilisateur final sont d'un grand bénéfice pour l'ensemble du secteur. Par exemple, une grande partie des efforts de lobbying de Tink s'appuie sur le graphe ci-dessous représentant le flux d'utilisateur standard en Europe.



- ✓ Toutes les procédures d'authentification sont fournies par l'ASPSP (art 30.2 des RTS)
- ✓ Le PSU (Payment Service User) est redirigé vers l'application d'authentification de l'ASPSP (paragraphe 16.1 de l'avis rendu par l'EBA)
- ✓ Authentification forte de l'utilisateur accomplie (Art 97 de la DSP2)

Pour contribuer à la vision long terme de l'open banking, Tink participe activement à des groupes d'influence et associations professionnelles comme l'ACPR, l'ETPPA, PSD2 SIG, PayBelgium, Fintech Norway, UK Finance et l'European Payments Association.

Conclusion

S'il y a une chose à retenir de l'expérience de Tink, c'est que le choix de développer des connexions open banking doit être considéré comme un investissement stratégique à long terme. L'industrie évolue très rapidement, et suivre le rythme du changement nécessite d'y consacrer des ressources spécifiquement dédiées.

Avec Tink, vous évitez le gros du travail. Notre plateforme open banking vous permet de vous connecter à plus de 3 400 banques et institutions financières à travers l'Europe et d'obtenir des données financières enrichies et catégorisées - via une seule API. Nous nous concentrons sur la connectivité pour vous permettre de vous concentrer sur l'innovation et le développement de services financiers à forte valeur ajoutée.

Curieux d'en savoir plus sur la manière d'accéder en temps réel aux données financières ? Nos experts sont toujours ravis de répondre à vos questions via :

partnerships@tink.com

tink.com