CENTRE DE DROIT
BANCAIRE ET FINANCIER

FinTech

Courte introduction à l'open banking

Par Jeremy Bacharach le 9 avril 2020

Un nouveau terme a récemment fait son entrée dans la grande famille du jargon financier. Il a pour lui le chic de l'anglais et une petite connotation utopique : l'*open banking*. L'oxymore saute immédiatement aux yeux. Comment diable le « *banking* », bastion traditionnel de la discrétion et de la confidence, pourrait-il se marier avec l'*openness* ? C'est pourtant le projet porté par ses partisans, qui ont réussi l'exploit de rendre l'*open banking* non seulement possible, mais *obligatoire* pour les banques et autres établissements offrant des comptes de paiement dans l'Union européenne.

Le problème fondamental auquel l'*open banking* cherche à apporter une solution est le suivant : comment le client d'une banque peut-il octroyer à des prestataires de service tiers un certain accès à son compte bancaire ? En d'autres termes, comment faire en sorte qu'il soit possible, pour ce client, d'habiliter de tels prestataires à interagir avec son compte ? On pense essentiellement à deux cas de figure :

- le client souhaite qu'un prestataire de services puisse avoir accès à diverses données relatives à son compte bancaire, telles que le solde ou les dernières transactions ;
- le client souhaite habiliter le prestataire à transmettre à la banque des ordres de paiement pour son compte.

Rendons les choses plus concrètes. Imaginons une application – il en existe – qui permette à ses utilisateurs de gérer leurs dépenses ou de créer des budgets. Dans l'idéal, cette application devrait pouvoir afficher les informations relatives aux comptes bancaires et aux comptes de cartes de ses utilisateurs. Cela n'est possible qu'en ayant accès aux informations bancaires du client. Prenons un autre exemple : les applications de paiement, telles que Twint. Ces applications permettent à leurs utilisateurs d'effectuer des versements instantanés depuis leurs comptes bancaires, sans toutefois qu'ils n'aient à se connecter à leur plateforme e-banking. Les clients habilitent donc ce « tiers » à transmettre des ordres de paiement à leurs banques, qui consentent à les traiter.

Cette problématique appelle deux sous-questions.

La première est de nature technique. Par quels moyens la communication entre les banques et les prestataires de services devrait-elle se dérouler ? Comment, d'un point de vue strictement technique, les banques et les prestataires de services devraient-ils communiquer ? Il existe deux grandes méthodes permettant à cette communication d'avoir lieu.

La première consiste en l'utilisation, par le prestataire de services, des identifiants e-banking du client. On parle alors de *screen scraping* ou de *reverse engineering*. Dans cette hypothèse, le prestataire de services utilise les identifiants e-banking pour avoir accès à toutes les informations du compte et pour effectuer les opérations ordonnées par le client. Cette méthode, parfois utilisée à l'étranger, a peu cours en Suisse, les Helvètes étant particulièrement attachés à la protection de leurs données bancaires. Elle pose en tout état d'évidents problèmes de sécurité informatique et de confidentialité.

La seconde méthode, plus avancée, est celle des *Application programming interfaces* ou API (prononcez « éille-pi-aille »). En bref, les APIs constituent des canaux de communication entre l'infrastructure informatique du prestataire de services et l'infrastructure informatique de la banque. Ces canaux sont digitaux et automatisés. Une fois un système d'API mis en place et le consentement du client recueilli, le prestataire de services peut obtenir de la banque des informations précises et ciblées, de même que lui faire parvenir des ordres de virement. La communication se fait ainsi directement entre les prestataires et les banques, sur la base d'un protocole et d'un langage informatiques définis à l'avance.

L'*open banking* n'est rien d'autre que la mise en place d'API par les banques, rendant possible l'accès à leurs données et à leurs opérations par des prestataires de services tiers.

Les avantages pour les clients et les prestataires de services sont clairs. Les clients gardent le contrôle de leurs données bancaires et peuvent choisir quelles informations sont, ou non, transmises. Les prestataires ont accès de manière facilitée au *back-end* des banques. Pour les banques, cependant, la mise en place d'une solution API est particulièrement coûteuse et complexe. Elles doivent rendre leurs infrastructures existantes compatibles avec la transmission d'informations à des tiers ou encore s'assurer qu'elles n'ouvrent aucune porte d'entrée aux pirates. Mais il y a pire : elles perdent leur monopole sur les données de leurs clients et leurs opérations bancaires. Ces facteurs, combinés avec l'absence d'une réelle demande pour l'*open banking* de la part des consommateurs, ont mené à une situation où peu de banques ont jugé l'aventure utile ou rentable.

Cela nous mène à la seconde sous-question : quel doit être le rôle de l'Etat ?

Pour l'Union européenne, la réponse ne fait l'ombre d'aucun doute : il appartient à l'Etat d'*imposer* aux banques de mettre en place des systèmes d'API permettant aux prestataires de services d'obtenir des informations sur des comptes ou d'initier des paiements. Cette obligation est désormais consacrée par les art. 66 et 67 de la 2e Directive sur les services de paiement (DSP2 ou PSD2, Directive 2015/2366) et 30 ss du Règlement technique y relatif (RTS, Règlement délégué 2018/389). Ces textes sont désormais en vigueur. Le lecteur est invité à faire l'expérience instructive qui consiste à taper sur Google le nom de sa banque européenne préférée avec le terme « API ». Il arrivera alors sur la page internet dédiée au système API de cette banque.

La situation en Suisse est plus… suisse. L'Association suisse des banquiers a réitéré à deux reprises déjà son opposition de principe à toute obligation pour ses membres de mettre en place un système d'API. La place est donc laissée aux initiatives privées : Twint, au premier plan, mais également SIX, Swisscom, ou les projets Common API et OpenBankingProject. Pour leur part, le Parlement, la FINMA et le Département fédéral des finances brillent par leur silence. La relation particulière – déjà évoquée – que les Suisses ont avec leurs informations

bancaires est sans doute pour beaucoup dans cette politique du laissez-faire. A une époque d'uniformisation grandissante des règles juridiques, les technologies de pointe témoignent donc d'une réalité souvent oubliée, mais connue depuis Montesquieu, à savoir que les lois découlent avant tout des « mœurs et manières » de leurs assujettis !

Liens utiles :

Bank for International Settlements/Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, novembre 2019, https://www.bis.org/bcbs/publ/d486.pdf

Emmenegger Susan/Miescher Caroline, Legal and regulatory framework in the context of open banking in Switzerland, https://www.openbankingproject.ch/media/1110/191004_legal-and-regulatory.pd

European Banking Authority, EBA working group on APIs under PSD2, https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2

Pour un aperçu des abbréviations utilisées dans le monde de l'*open banking* : European Banking Authority, Final Report on final draft RTS and ITS on EBA Register under PSD2 (EBA-RTS-2017-10) (EBA-ITS-2017-07), 13 décembre 2017, p. 3

Reproduction autorisée avec la référence suivante: Jeremy Bacharach, Courte introduction à l'open banking, publié le 9 avril 2020 par le Centre de droit bancaire et financier, https://cdbf.ch/fr/1124/