SwissBanking

Juillet 2020

Open Banking

Etat des lieux pour la place financière suisse

Sommaire

Avant-propos

S'agissant de l'évolution future du secteur financier, l'open banking fait partie des sujets incontournables dans le monde entier. Les prescriptions réglementaires dans l'Union européenne (UE) ainsi que dans des pays hors d'Europe ont notamment donné un nouvel élan à la thématique. Dans ce cadre, l'open banking – à savoir des modèles d'affaires basés sur l'échange standardisé et sécurisé de données entre une banque et des prestataires tiers dignes de confiance – est souvent considéré comme une première étape en direction d'une économie de plateforme dans laquelle des données sont échangées entre secteurs et traitées avec une valeur ajoutée pour les clients, l'économie et la société.

Les banques jouent un rôle déterminant à cet égard. En raison de leur base de clientèle étendue et de la confiance qui leur est accordée, elles ont la chance de jouer un rôle de précurseur dans un écosystème intersectoriel. De plus, elles ont la possibilité de jouer un rôle important dans la définition de la protection des données, des règles pour l'utilisation éthique des données, des normes pour les interfaces et de l'infrastructure. La place financière suisse a ainsi une occasion unique de façonner l'écosystème financier du futur en collaboration avec les principaux acteurs.

Sous la direction de l'Association suisse des banquiers (ASB), un groupe de travail a élaboré le présent document. Il doit permettre de créer les conditions optimales pour faciliter la coopération entre les banques et les prestataires tiers et faire avancer la mise en œuvre de l'open banking en Suisse. Le thème de l'open banking est structuré du point de vue du secteur bancaire suisse et des règles de base sont définies pour les aspects juridiques pertinents.

Le présent document de l'ASB contient des recommandations qui ne sont pas juridiquement contraignantes et des analyses qui peuvent être utilisées pour la suite de la mise en œuvre des modèles d'affaires d'open banking. Le document ne prétend pas à l'exhaustivité. Il sera actualisé et complété si nécessaire en fonction des évolutions techniques et juridiques futures. La version la plus récente du document est publiée sur le site de l'ASB.

Auteurs dans l'ordre alphabétique

Matthias Häfner, Banque Valiant
Martin Hess, Association suisse des banquiers
Richard Hess, Association suisse des banquiers
Roger Huber, Banque Cantonale de Zurich
Friederich Kersting, PostFinance
Matthias Plattner, Julius Bär
Jürg Schär, UBS
Sven Siat, SIX
Cornelia Stengel, Swiss Fintech Innovations
Stephanie Wickihalder, Credit Suisse
Marco Wüst, Raiffeisen Suisse

Nous remercions tout particulièrement les experts externes pour leurs précieuses contributions sous forme de discussions et de compléments au document.

Executive Summary

L'Association suisse des banquiers (ASB) reconnaît que l'open banking recèle un fort potentiel pour la place financière suisse. Elle contribue donc activement aux conditions-cadres qui rendent possibles les modèles d'affaires correspondants et qui renforcent ainsi la compétitivité de la place financière suisse. Dans le même temps, il convient de s'assurer que la place financière continue de bénéficier d'un haut niveau de confiance y compris en cas d'ouverture des interfaces à des tiers. Il n'est pas pertinent de prendre des mesures réglementaires, par exemple en rendant obligatoire l'ouverture des interfaces. C'est à la libre concurrence, et en particulier aux besoins des clients, de déterminer les modalités de l'open banking en Suisse. Les banques doivent rester libres de décider si elles souhaitent coopérer avec des prestataires tiers et lesquels. Les trois points suivants sont déterminants pour une évolution positive à l'avenir:

1. Un positionnement stratégique clair

La collaboration avec différents prestataires tiers dans un écosystème d'open banking est avant tout une question stratégique. Les différents établissements doivent se demander de façon ciblée comment ils souhaitent gérer à l'avenir le traitement des données client et leur échange dans l'écosystème. Pour cela, chaque établissement doit adopter un positionnement clair dans le cadre de son offre propre et définir son rôle dans le développement de l'offre. Ce positionnement crée des bases solides pour le choix ultérieur de prestations et partenaires concrets.

2. Exigences juridiques dépendant de la situation

Grâce à l'approche d'économie de marché, il n'existe en Suisse actuellement aucune exigence réglementaire et juridique spécifique pour l'open banking. En principe, les banques peuvent ainsi déterminer librement avec qui elles souhaitent coopérer et donner accès à leurs interfaces. Cela permet de garantir que la collaboration entre la banque et le prestataire tiers repose sur des considérations économiques et des cas d'application concrets qui apportent une valeur ajoutée au client. Pour faire une évaluation juridique, il convient d'abord de différencier l'outsourcing de l'open banking. Cette distinction importante entraîne ensuite des exigences différentes. Dans le contexte de l'open banking, le type et l'intensité de l'interaction entre banque, prestataire tiers et client doivent être examinés. Plus la collaboration entre

la banque et le prestataire tiers dans l'open banking est étroite, plus un client comptera sur le fait que sa banque a contrôlé le prestataire tiers et assume une certaine responsabilité pour ses prestations. Par exemple, une commercialisation active est un indicateur d'une coopération étroite pour le client.

3. Standardisation des API pour chaque domaine spécialisé

La standardisation ouverte des interfaces (Application Programming Interface, API) est nécessaire pour assurer une parfaite coopération avec les tiers et des échanges de données sans erreurs. Pour les interfaces qui permettent d'accéder aux informations sur le compte et de livrer des paiements, il existe déjà des normes sur le marché suisse. Dans ce cadre, il est important de tenir compte des différents niveaux et de leur degré de standardisation. En effet, l'hétérogénéité est généralement source de complexité et de coûts plus élevés. A moyen terme, on peut donc s'attendre à ce que, pour chaque domaine spécialisé (information sur le compte, paiements, hypothèques, prévoyance, etc.), quelques normes voire souvent une seule norme s'imposent sur le marché.

1. L’open banking en Suisse

Moteurs de l’open banking

L’évolution des besoins des clients, les nouveaux acteurs, les nouvelles technologies sont autant de défis à relever pour les banques traditionnelles. Dans ce contexte, l’open banking est appelé à influencer et à transformer durablement le secteur bancaire. Dans un monde où la chaîne de création de valeur se fragmente de plus en plus et où de multiples prestataires de services financiers (banques, entreprises Fintech, néobanques, non-banques) proposent leurs services aux clients, on ne se demande plus si l’open banking s’imposera, mais sous quelle forme. La concurrence accrue et les exigences réglementaires jouent un rôle de catalyseur dans ce cadre.

En Suisse, la clientèle Entreprises reste au cœur de l’open banking. La palette d’offres est régulièrement étendue en fonction des besoins et du marché et peut aussi ouvrir des perspectives à la clientèle privée à l’avenir. L’émergence d'écosystèmes intersectoriels, dans lesquels le secteur financier peut jouer un rôle précieux, est étroitement liée à l’open banking.

Grâce à l’ouverture contrôlée d’interfaces standardisées, les clients bénéficient d’un rythme d’innovation soutenu et, dès lors, d’offres compétitives – dans un cadre à la fois très stable et fiable. L’intégration de logiciels de comptabilité, par exemple, permet à la clientèle Entreprises d’améliorer la planification de ses liquidités. Aussi bien la clientèle Entreprises que les clients privés peuvent profiter de l’interconnexion entre différents comptes ouverts auprès de divers prestataires qui leur donne une vue d’ensemble sur leur situation financière.

Pour les banques, la coopération avec des prestataires tiers au moyen d’interfaces standardisées génère des gains d’efficience ainsi que de nouvelles sources de revenus. L’open banking permet une meilleure expérience client en assurant la fluidité entre différentes offres. Grâce aux échanges mutuels de données, les banques ont davantage accès aux données de tiers, ce qui favorise l’offre de produits innovants. En outre, l’open banking leur donne l’opportunité de se positionner en tant

qu'acteur central ou prestataire d'une économie de plateforme et de diversifier leurs sources de revenus de manière efficace tout en élargissantla base de clientèle.

S'agissant des prestataires tiers comme les entreprises Fintech, l'open banking leur offre la possibilité de commercialiser leurs produits et services selon des modalités techniques et réglementaires simplifiées (p. ex. pas d'obligation d'obtenir une licence bancaire). En coopérant avec des prestataires de services financiers établis, ils ont accès à une solide base de clientèle, ce qui facilite le développement rapide des modèles d'affaires. L'inverse peut également être vrai.

Open banking ou outsourcing

L'open banking comporte trois éléments

L'ASB définit l'open banking comme un modèle d'affaires basé sur l'échange standardisé et sécurisé de données entre une banque et des prestataires tiers dignes de confiance ou d'autres prestataires de services financiers.

- **«Standardisé»:** la standardisation ouverte des interfaces est indispensable pour assurer une parfaite coopération avec les tiers et des échanges de données sans erreurs[1]. Elle devrait reposer dans la mesure du possible sur des normes reconnues sur le marché.
- **«Sécurisé»:** la confidentialité et la sécurité des données ne sauraient être garanties sans des dispositifs technologiques de sécurisation.
- **«Dignes de confiance»:** pour assurer l'intégrité du système, seuls doivent avoir accès à l'interface les tiers qui répondent à certains critères de qualité – en particulier des exigences techniques extrêmement strictes. Il revient toujours au client de décider s'il échange ses données. La banque se positionne en partenaire digne de confiance avec une offre adaptée de prestataires tiers et défend les intérêts de ses clients. Elle contribue ainsi à la sécurité et à la stabilité de la place financière suisse et montre pourquoi les clients peuvent continuer à accorder un haut niveau de confiance aux banques suisses.

1 Outre la coopération avec les tiers et la fragmentation de la chaîne de création de valeur, l'«open banking» est essentiel et constitue un moteur pour les offres «Software as a Service (SaaS)» dans le secteur financier. Seule la standardisation permet aux fabricants de logiciels et aux prestataires informatiques de proposer des solutions correspondantes aux prestataires de services financiers. Cet état de fait aura un impact significatif sur les architectures informatiques des prestataires de services financiers et renforcera la tendance à délaisser l'architecture monolithique au profit d'une architecture best-of-breed.

Différences économiques et juridiques par rapport à l'outsourcing

L'open banking et l'outsourcing sont étroitement liés, mais ne peuvent pas être utilisés comme synonymes. Dans la circulaire 2018/3, l'Autorité fédérale de surveillance des marchés financiers (FINMA) définit le terme d'«outsourcing» comme suit[2]:

> On parle d'outsourcing (externalisation) au sens de la circulaire lorsqu'une entreprise charge un prestataire de remplir, de manière indépendante et durable, tout ou partie d'une fonction essentielle à l'activité commerciale de l'entreprise.

L'open banking et l'outsourcing ont pour dénominateur commun le fait que des tiers sont impliqués. Il existe toutefois des différences du point de vue économique et juridique:

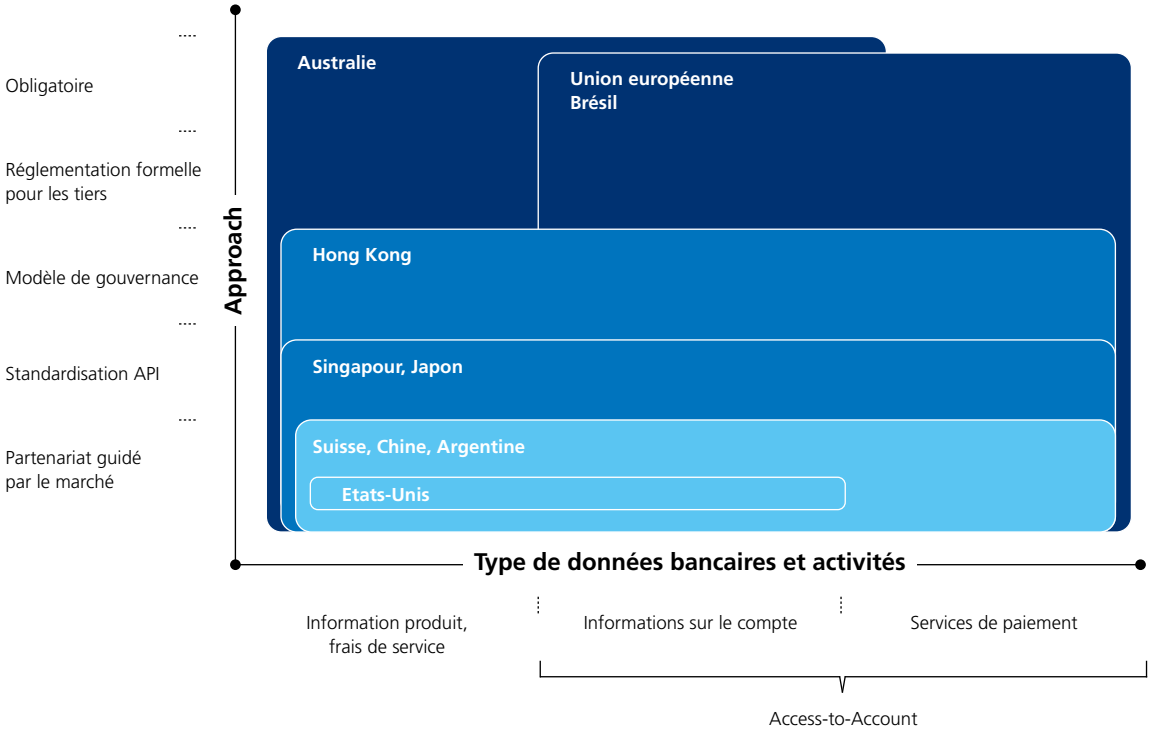
- Dans **l'outsourcing**, le tiers impliqué agit uniquement sur mandat, selon les instructions et dans l'intérêt de la banque donneur d'ordre. La banque donneur d'ordre contrôle obligatoirement la prestation fournie. La fonction externalisée fait partie de la chaîne de création de valeur du donneur d'ordre et est soumise à son obligation de diligence vis-à-vis du client.
- Dans le cas de **l'open banking**, le tiers impliqué n'agit pas sur mandat de la Banque, mais d'abord sur mandat et dans l'intérêt du client. Légitimé par le client, le tiers accède à une partie des données du client auprès de la banque ou reçoit celles-ci pour les traiter et offrir ainsi une valeur ajoutée au client. La banque n'a donc aucun contrôle sur la prestation fournie du tiers. Pour que l'obligation de diligence vis-à-vis du client incombe au tiers, la prestation de service d'open banking requiert le consentement du client.

2 Pour faire la distinction avec la définition du traitement de données de mandat selon la loi sur la protection des données (LPD), qui est plus large.

2. Développements internationaux

Au niveau international, les autorités de surveillance et les régulateurs ont pris diverses mesures pour définir les conditions-cadres de l'open banking. Les mesures diffèrent en ce qui concerne l'approche réglementaire ainsi que l'étendue et le type de données bancaires et activités qui sont soumis à l'échange de données réglementé (cf. figure 1).

Fig. 1: Comparaison des cadres d'open banking internationaux



Catégorie 1: Échange de données imposé
Catégorie 2: Échange de données encouragé
Catégorie 3: Approche basée sur le marché sans règles explicites pour l'échange de données

Source: ASB, basée sur Basel Committee on Banking Supervision (2019).
Report on open banking and application programming interfaces. https://www.bis.org/bcbs/publ/d486.pdf

En combinant ces approches, on peut distinguer quatre catégories principales.[3] A cet égard, la Suisse poursuit une approche basée sur le marché et se classe dans la catégorie 3.

- **Catégorie 1: échange de données imposé**
  Les banques sont tenues de transmettre aux tiers les données pour lesquelles le client a donné une autorisation. Les tiers doivent s'enregistrer auprès d'une autorité de surveillance ou de réglementation et sont généralement soumis à des contrôles stricts par des organismes publics.
  Exemples: Australie, Brésil, UE, Inde, Mexique, Afrique du Sud, Royaume-Uni.
- **Catégorie 2: échange de données encouragé**
  Les autorités ont promulgué des directives avec des normes et des spécifications techniques recommandées.
  Exemples: Hong Kong, Japon, Singapour, Corée du Sud.
- **Catégorie 3: approche basée sur le marché sans règles explicites pour l'échange de données**
  Aucune règle explicite ni directive qui exige ou interdit la transmission de données avec l'autorisation du client par les banques à des tiers.
  Exemples: Argentine, Chine, Suisse, Etats-Unis.
- **Catégorie 4: réglementation en cours d'examen[4]**
  Les juridictions qui introduisent actuellement des exigences réglementaires spécifiques ou réfléchissent activement à le faire.
  Exemples: Canada, Russie.

3 Basel Committee on Banking Supervision (2019). Report on open banking and application programming interfaces. https://www.bis.org/bcbs/publ/d486.pdf

4 Non représenté dans la figure 1.

3. Mise en place de conditions optimales

Conditions-cadres – liberté contractuelle et solutions fondées sur l'économie de marché

Selon l'approche d'économie de marché, il n'existe en Suisse actuellement aucune exigence réglementaire et juridique spécifique pour l'open banking. En principe, les banques peuvent ainsi déterminer librement avec qui elles souhaitent coopérer et donner accès à leurs interfaces. Cela permet de garantir que la collaboration entre la banque et le prestataire tiers repose sur des considérations économiques et des cas d'application concrets qui apportent une valeur ajoutée au client.

En particulier, il n'existe en Suisse aucune obligation pour les banques de partager les données de clients avec des prestataires tiers. L'accès automatisé aux interfaces est laissé à l'appréciation de la banque. Par conséquent, il n'existe à l'heure actuelle pas non plus d'obligation d'obtenir une licence et une autorisation prescrite par le régulateur pour les prestataires tiers, qui faciliterait ou remplacerait une vérification préalable de prestataires tiers.

Du point de vue de la banque, il est recommandé de soumettre préalablement les tiers éventuels à certaines clarifications. A cet égard, la forme de coopération entre la banque et le prestataire tiers est déterminante. Les approches et éléments concrets de contrôle des prestataires tiers sont traités plus en détail au chapitre 4.

Stratégie – positionnement clair

Positionnement clair d'une banque dans le cadre de l'offre
Pour une banque, l'objectif principal de l'open banking devrait être d'apporter une valeur ajoutée au client en élargissant sa propre offre avec des produits et prestations innovants. De telles offres sont caractérisées par le fait qu'elles:

- **sont élaborées en collaboration avec le tiers** Dans ce cadre, des entreprises Fintech ou d'autres prestataires établis (p. ex. des fabricants de systèmes de comptabilité) sont systématiquement intégrés au flux d'information et à l'offre proposés au client.
- **complètent l'offre bancaire classique.** Dans ce cadre, les données existantes de la banque sont affinées en relation avec des données de tiers afin de créer de nouvelles informations pour le client ou les lui présenter dans un nouveau contexte.

Pour cela, une banque doit développer une vision claire des offres qui doivent être placées et avec quelles valeurs ajoutées concrètes. En d'autres termes: il convient de s'assurer que l'open banking corresponde à la stratégie globale, u positionnement sur le marché et à la stratégie d'offre de la banque.

Pour mettre en œuvre l'open banking, il peut donc être utile pour la banque de se poser les questions fondamentales suivantes:

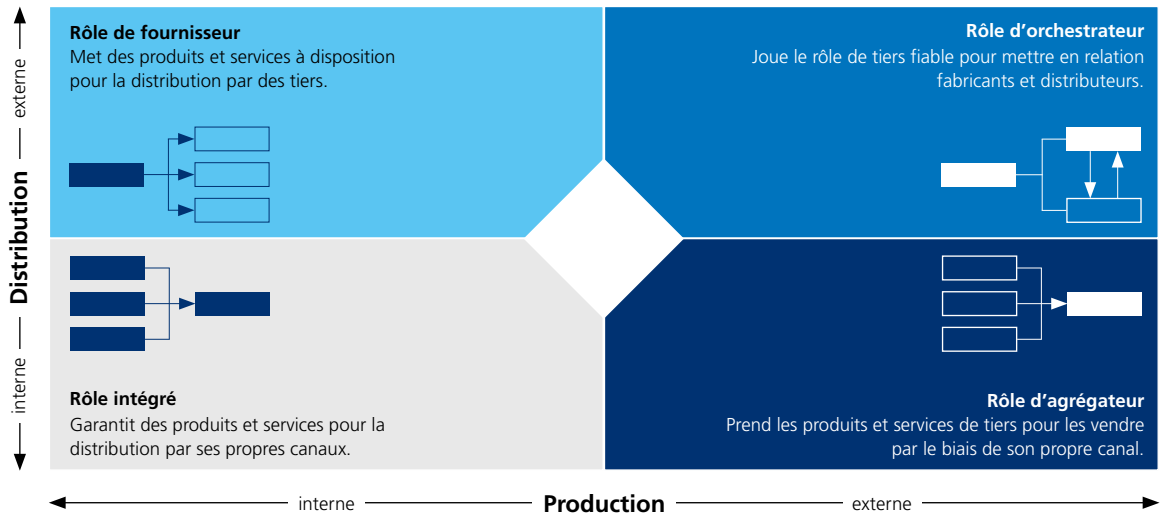
- Quels segments de clientèle cherche-t-on à atteindre avec l'offre d'open banking?
- Quelle stratégie d'offre poursuiton actuellement pour ces segments de clientèle?
- Quelles valeurs ajoutées et offres de produits sont offertes à ces segments de clientèle?
- Quel rôle jouent les anciennes «Non-Banking Added Values» (p. ex. programmes de fidélité, prestations de conseil dans le domaine fiscal, de la cybersécurité, prestations e-administration)?
- Quelles expériences client sont visées par le biais de quelles «User Journeys»?
- Quelle politique de prix est poursuivie (par segment)?

Le positionnement clair de l'open banking dans la stratégie d'offre d'une banque crée des bases solides pour le choix ultérieur nécessaire de partenaires et prestations concrets.

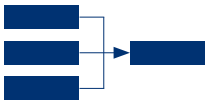
Clarification du propre rôle dans le développement de l'offre

Sur la base du positionnement stratégique de l'open banking dans le développement de l'offre, la banque doit décider quel rôle elle veut jouer dans la mise en œuvre. Pour cela, il existe quatre modèles de base que l'on peut caractériser de la manière suivante:

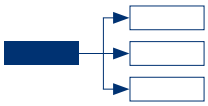
Fig. 2: Rôle possible des banques dans un écosystème d'open banking



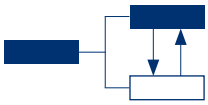
Source: ASB, basée sur Capgemini (2020). World FinTech Report.



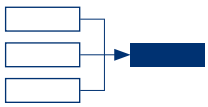
«Rôle intégré»: Traditionnellement, les banques (universelles) établies développent et produisent leurs produits et prestations en interne et les distribuent ensuite par le biais de leurs canaux. Cette approche intégrée a fait ses preuves au cours des décennies passées et généré une grande confiance et sécurité auprès des clients. Dans ce modèle, les banques contrôlent l'interface client. Certaines prestations peuvent également être reprises par des prestataires tiers par l'outsourcing. Pour rester compétitif à long terme dans ce modèle, de vastes compétences sont nécessaires – aussi bien dans la production que dans la distribution.



«Rôle de fournisseur»: Dans ce modèle, la banque prépare ses produits et prestations pour la distribution par des tiers. L'interface client final est contrôlée par divers prestataires tiers dans ce rôle. Pour rester compétitif à long terme dans ce modèle, une élaboration et une mise à disposition efficaces de produits et prestations sont nécessaires afin de diminuer le coût marginal par pièce (economies of scale).



«Rôle d'orchestrateur»: Dans ce modèle, la banque se présente comme une partie fiable pour mettre en relation les clients et les fabricants de produits. Dans ce cadre, elle peut toujours contrôler l'interface client. Pour rester compétitive à long terme dans ce modèle, la Banque doit être capable d'intégrer des offres de tiers dans sa propre palette d'offres (p. ex. e-banking).



«Rôle d'agrégateur»: Dans ce modèle, la banque prend les produits et prestations de tiers pour les vendre par le biais de ses propres canaux. L'interface client est l'atout principal. Pour rester compétitif à long terme dans ce modèle, des compétences best in class sont nécessaires dans le domaine UX/UI et de grandes compétences sont requises dans la prospection par le biais des canaux numériques.

Une banque peut aussi assumer plusieurs rôles simultanément (p. ex. modèle intégré avec approche fournisseur en aval). Par ailleurs, il est envisageable qu'une banque assume le rôle de fournisseur de plateforme. Elle met alors à disposition l'infrastructure correspondante et les informations pour les participants de l'écosystème.

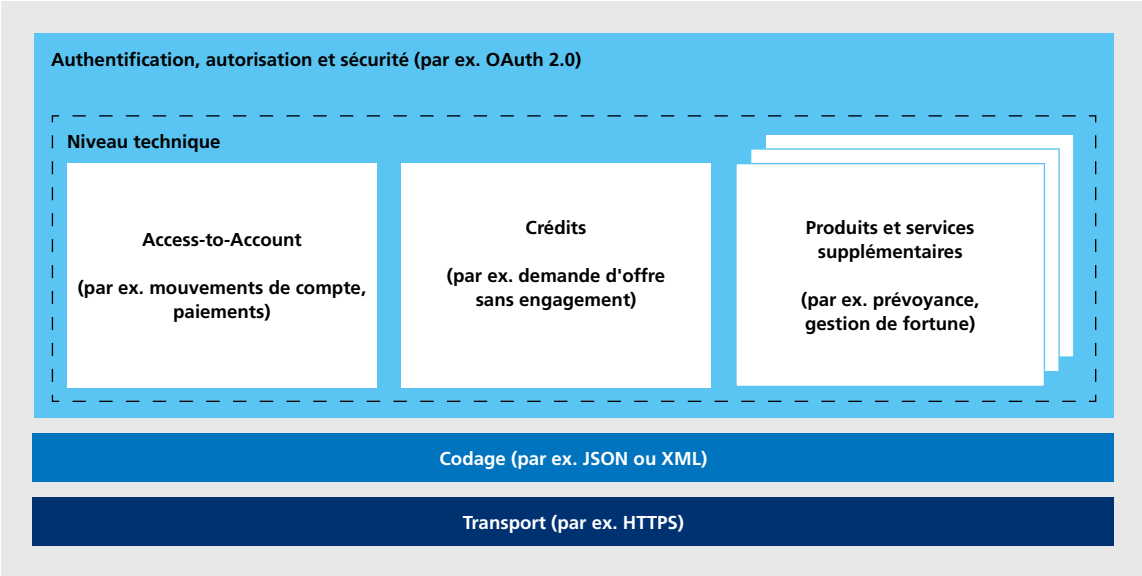
Pour que cela fonctionne, il faut obligatoirement que tous les acteurs nécessaires soient mis en réseau de manière systématique. Cela vaut en particulier dans la gestion de produits avec les flux d'informations liée au développement de l'open banking. La capacité d'évaluer rapidement le développement d'idées et d'offres, de sélectionner des partenaires adaptés et de les intégrer de manière ciblée est nécessaire pour une mise en œuvre réussie. La mise en place de ces compétences doit avoir lieu de manière ciblée et être soigneusement planifiée. Elle peut nécessiter des investissements dans de nouvelles ressources en personnel et technologiques. A cet égard, la coopération systématique avec des prestataires tiers établis, qui suivent étroitement le marché dans l'intérêt des banques et qui ont développé des connaissances sur les évolutions actuelles, les offres disponibles et leur succès sur le marché sur la base de leurs expériences lors de la construction d'une plateforme peut être utile.

Infrastructure – standardisation des API

Les différents niveaux de standardisation

En Suisse, les banques donnent déjà accès aux comptes et aux données de leurs clients de manière sélective et ouvrent des interfaces clients dans l'intérêt des deux parties. Toutefois, il n'existe aucune une obligation légale pour les banques. Pour poursuivre la discussion en vue de la standardisation d'interfaces et analyser les solutions possibles, il est important de comprendre les différents niveaux des interfaces et leur degré de standardisation.

Fig. 3: Représentation schématique des différents niveaux de normalisation des API



Source: ASB.

L'illustration présente différents niveaux qui sont utilisés pour l'échange de données par le biais d'API. Si l'on se représente la situation avec le cas de la transmission de données par voie postale, le niveau du transport serait assuré par la Poste. Celui-ci est en grande partie standardisé au niveau mondial. Le niveau du codage serait le format du papier, p. ex. DIN-A4. Celui-ci est également standardisé au niveau international. L'authentification et l'autorisation garantiraient que seul le destinataire correct puisse lire le contenu. Enfin, le contenu du document constitue le niveau technique. Les informations contenues dans le document et la manière dont elles sont traitées par le destinataire peut toutefois beaucoup varier en fonction du contexte du cas commercial.

La situation est comparable dans le monde numérique. Les niveaux du transport et du codage sont largement standardisés à l'échelle mondiale (p. ex. HTTPS[5], JSON[6], REST[7]). Pour l'autorisation, il existe aussi des normes telles que OAuth 2.0[8], sur lesquelles les solutions d'open banking suisses se basent également. Compte tenu des innombrables cas commerciaux au niveau technique, la standardisation dans ce domaine constitue le principal défi. Certains domaines spécialisés comme le trafic des paiements sont standardisés au niveau international (p. ex. avec la norme internationale de messagerie ISO 20022, dont la mise en œuvre en Suisse est de la responsabilité de SIX). Par contre, pour d'autres domaines, il n'existe que peu de normes adaptées, sur lesquelles les initiatives d'open banking peuvent s'appuyer. C'est notamment le cas pour les questions qui ont un «caractère très suisse» (p. ex. la prévoyance).

5 Hypertext Transfer Protocol Secure, en français «protocole de transfert hypertexte sécurisé»
6 JavaScript Object Notation
7 Representational State Transfer
8 Open Authorization 2.0

Fig. 4: Comparaison du degré de standardisation des différents niveaux de standardisation

Niveau	Question	«Analogie avec la Poste»	«Monde numérique»	Degré de standardisation
Technique	Quelles informations doivent être données où et comment?	Le contenu du document varie selon le contexte du cas commercial	par ex. Berlin Group NextGen-PSD2 XS2A, SFTI Common API, Swiss NextGen API	Dépend du domaine spécialisé
Authentification Autorisation Sécurité	Comment l'utilisateur est-il authentifié? Quels sont les droits de l'utilisateur?	P. ex. secret de la correspondance	P. ex. OAuth 2.0, Open IDConnect	Moyen (un groupe de flux définis et établis)
Codage	Dans quelle structure les données sont-elles transférées?	Format du papier P. ex. DIN-A4	P. ex. JSON, XML	Elevé
Transport	Comment les données sont-elles transmises?	Poste et autres prestataires	P. ex. HTTPS	Elevé

Source: ASB.

La standardisation nécessite une approche commune

Pour les interfaces qui permettent d'accéder aux informations sur le compte et de livrer des paiements, des normes existent déjà sur le marché. D'une manière générale, l'hétérogénéité engendre de la complexité et des coûts plus élevés. A moyen terme, on peut donc s'attendre à ce qu'une norme s'impose sur le marché pour chaque domaine spécialisé (information sur le compte, hypothèques, prévoyance, etc.).

Une standardisation ouverte est un préalable indispensable à un écosystème d'open banking plus exhaustif en Suisse. Elle permettrait aux différents acteurs du marché de s'adapter sans heurts, mais aussi d'échanger et d'exploiter les données en toute sécurité. Il est plus facile de faire converger les efforts de standardisation si toutes les parties prenantes poursuivent le même objectif, autrement dit si ces stakeholders ont des intérêts et des modèles d'affaires complémentaires.

Mais, concrètement, quels sont les aspects à prendre en compte pour mener à bien une standardisation?

Dans un premier temps, il convient d'identifier toutes les parties prenantes concernées, et notamment de cerner leurs attentes en termes d'avantages ainsi que leurs préoccupations. Dans chaque groupe, il faudrait mobiliser un nombre représentatif de personnalités de premier plan, sachant que cet engagement ne suppose pas nécessairement une participation active permanente. Collaborer dans le cadre d'un conseil consultatif ou en participant à un «sondage» ou à un «contrôle» peut également suffire.

L'organisation de l'initiative de standardisation est ensuite structurée en fonction des différents aspects pertinents dans l'open banking: outre l'aspect technologies de l'information, les exigences bancaires ainsi que les conditions-cadres juridiques et réglementaires entrent également en ligne de compte. Eu égard à ces différents points de vue, il ressort que l'initiative doit être structurée en groupes de travail assortis de priorités distinctes. Les diverses tâches doivent par conséquent être coordonnées sur cette base.

Trois stratégies de standardisation en Suisse

Les stratégies envisageables pour standardiser effectivement les API en Suisse sont au nombre de trois:

- Reprendre une norme existante (p. ex. Berlin Group NextGenPSD2 XS2A[9], Open Banking UK[10]).
- S'appuyer sur plusieurs normes en place pour élaborer une norme propre.
- Concevoir une norme suisse (en partant de zéro).

La première variante est moins appropriée car les spécificités suisses dans le domaine des systèmes de paiement ne sont pas représentées dans la mesure souhaitée par l'une des normes actuellement en place. La troisième variante prônant une conception autonome d'une norme suisse «en partant de zéro» est hautement complexe et ne saurait être efficace dès lors qu'il existe des normes

9 https://www.berlin-group.org/
10 https://www.openbanking.org.uk/

reconnues à l'échelle internationale. Il reste donc l'option d'élaborer une norme nationale sur la base des normes existantes et s'inspirant de celles-ci. Pour ce faire, des concepts sous-tendant les normes existantes peuvent être intégrés selon le principe best of all worlds et complétés par des spécificités suisses. Dans ce contexte, l'interopérabilité internationale est cruciale.

Initiatives de standardisation en Suisse

Dans le sillage de la visibilité croissante de l'open banking, diverses initiatives lancées en Suisse s'efforcent à présent de faire avancer la standardisation des interfaces et de développer une norme suisse pour les API. Les initiatives existantes se concentrent principalement sur l'élaboration d'une norme suisse des API sans toutefois s'attaquer à des problématiques spécifiques ayant trait aux conditions-cadres juridiques et réglementaires.

Par rapport aux initiatives de standardisation précédentes, les initiatives d'open banking actuelles diffèrent en particulier sur les points suivants:

- Les efforts de standardisation menés actuellement portent systématiquement sur des interfaces permettant aux banques de communiquer vers l'extérieur. Il s'agit toujours de services axés sur le client proposés directement ou par l'intermédiaire de tiers.
- Quant aux initiatives de standardisation antérieures, elles étaient généralement axées sur l'open banking en interne. La norme d'échange de messages ISO 20022 en est un exemple. Il s'agit d'une norme régissant l'échange de données, principalement entre les banques (ou entre les «systèmes back-end» orientés vers le client, tels que des progiciels de gestion intégrée aussi appelés systèmes ERP (Enterprise Resource Planning) et les banques). L'adoption de cette norme reconnue au sein du secteur des services financiers s'est généralisée à l'échelle internationale et en Suisse.

En règle générale, les initiatives existantes abordent d'abord les thèmes de l'accès aux comptes et des systèmes de paiement, car ceux-ci sont devenus davantage une priorité dans les discussions relatives à la DSP2 (voir glossaire). De ce fait, ces initiatives sont comparables en termes d'orientation initiale du contenu. En revanche, elles diffèrent considérablement en termes d'objectifs et de stratégies pour atteindre les objectifs.

D'une manière générale, les initiatives lancées en Suisse peuvent être classées dans les catégories suivantes:

- **Initiatives de standardisation et plateformes de connaissances:** ces initiatives se concentrent sur la création d'une norme ouverte pour les API en Suisse. Elles s'inspirent généralement des normes internationales existantes (p. ex., Berlin Group NextGenPSD2 XS2A) et les adaptent à la place financière suisse. Le but est avant tout de standardiser sur le plan technique. Les travaux du groupe de travail Common API de Swiss Fintech Innovations (SFTI) et l'initiative openbankingproject.ch en sont un exemple.
- **Plateformes et marchés:** ces initiatives visent à développer une solution globale et opérationnelle (p. ex. plateforme, marché des API) pour les participants à l'écosystème financier (p. ex. les banques, les prestataires tiers, les Fintech). Les solutions sont basées soit sur des normes ouvertes des initiatives de standardisation, soit sur des API individuelles et internes.[11] Cette catégorie comprend également les prestataires européens qui ont acquis de l'expérience dans le développement d'API et de marchés dans le cadre de DSP2, et qui élargissent à présent leur offre en Suisse.
- **Offres de fournisseurs de solutions technologiques:** la plupart des fournisseurs de logiciels bancaires de base en Suisse proposent leurs propres marchés et plateformes basés sur leurs propres normes d'API.[12]

Des synergies peuvent donc être trouvées entre les différentes initiatives lancées en Suisse, sachant qu'il existe aussi une certaine concurrence. Des échanges permanents se sont déjà mis en place entre ces initiatives afin de réduire conjointement le nombre d'API au minimum. L'ASB fait le trait d'union, intervenant à titre de médiateur et de coordinateur entre les différentes initiatives.

11 En voici des exemples actuels (état juin 2020): SIX b.Link Platform, Swisscom Open Banking Hub, inventx Open Finance Platform. En Suisse, le fournisseur central d'infrastructure SIX est actuellement le seul prestataire à couvrir trois aspects importants grâce à b.Link avec l'élaboration de normes, la construction d'une plateforme et une prise en charge des prestataires tiers par une technologie appropriée.

12 En voici des exemples actuels (état juin 2020): Finnova Open Platform, avaloq.one ou le système bancaire de base finstar de la banque Hypothekarbank Lenzburg

D'autres éléments sont développés en fonction des besoins

Les expériences réalisées sur des marchés plus en avance dans le développement de l'open banking montrent qu'à mesure que l'open banking s'adapte, d'autres éléments peuvent devenir pertinents pour favoriser le développement de l'écosystème. On peut supposer que ces éléments seront également développés et mis à disposition par les acteurs du marché en Suisse si la demande est suffisante. Il s'agit notamment de:

- **la gestion des différends (dispute management):** définition d'une approche uniforme et transparente en cas de conflits entre les parties impliquées dans l'écosystème d'open banking.
- **l'expérience client:** définition des lignes directrices pour une expérience client uniforme (p. ex. lors de l'octroi du consentement).
- **l'assurance qualité:** possibilités de voir, par exemple, la disponibilité des interfaces.

4. Quels sont les aspects juridiques que les banques doivent contrôler?

Exigences en fonction de la configuration

Dans le cadre du droit de surveillance, la banque doit toujours assurer une organisation adéquate en termes de modèle d'affaires et procéder à une gestion appropriée des risques. En outre, la loi sur la protection des données et le secret bancaire imposent également certaines exigences pour le partage des données clients. Afin de pouvoir déterminer les exigences juridiques qui s'appliquent dans une configuration d'open banking concret, il convient au préalable de faire la distinction entre l'outsourcing et l'open banking (voir p. 9 ci-dessus). Cette distinction importante est déjà fondamentale pour l'évaluation juridique.

Si le modèle d'open banking prévu n'est pas une externalisation (les règles générales prévues dans ce cas de figure s'appliquent), la nature et la fréquence des interactions entre la banque, le prestataire tiers et le client devront ensuite être examinées dans le domaine de l'open banking.

Plus la coopération entre la banque et les prestataires tiers dans le domaine de l'open banking est étroite, plus ces parties mettront la coopération commune en avant et la positionneront en conséquence auprès des clients, et plus un client aura tendance à se fier au fait que sa banque a contrôlé la qualité de ce prestataire tiers – qui est leur partenaire de coopération.

A l'inverse, il existe des configurations d'open banking dans lesquelles une banque transmet à un prestataire tiers les données d'un client uniquement à la demande de ce dernier. Ce prestataire tiers les prépare ensuite pour le client, lui offrant ainsi une valeur ajoutée. Plus la communication entre la banque et le prestataire tiers est fluide, moins les exigences seront sévères pour ce qui est des obligations de vérification.

Entre ces deux extrêmes, des configurations à des degrés différents sont concevables. Dans ce contexte, il convient de tenir compte en particulier de la possibilité qu'un open banking intervienne entre deux (ou plusieurs) banques.

Les exigences légales applicables à chaque configuration devront donc être analysées en détail. Dans tous les cas, la banque doit cependant clarifier en particulier les aspects suivants:

- Existence des **bases légales claires** et, le cas échéant, des **accords contractuels** régissant la collaboration et le flux de données entre clients et prestataires tiers.
- Respect des **aspects** fondamentaux **de la protection des données et de la sécurité des données:**
  - La protection des données joue également un rôle décisif, et à plus forte raison dans les configurations d'open banking, à divers titres: du fait des obligations légales de la banque et des prestataires tiers d'une part, mais aussi en lien avec la réputation des parties concernées, d'autre part – au final, il en va aussi de la réputation de la place financière dans son ensemble.
  - La législation sur la protection des données autorise dans tous les cas l'open banking, surtout si c'est le client qui prend l'initiative d'échanger ses données. Dans ce contexte, il est particulièrement important que le client sache en tout temps quelles données sont partagées avec des tiers.
  - En termes de sécurité des données, l'utilisation d'interfaces standardisées peut atténuer les risques en fournissant des modèles établis. En outre, il est recommandé d'adapter les interfaces pour qu'elles soient à la pointe de la technique. Il est par ailleurs conseillé de définir les processus applicables en cas de «fuite de données» avec le prestataire tiers afin que toutes les parties en présence puissent s'acquitter de leurs obligations en pareil cas et que le client soit protégé de la meilleure façon possible.
  - Les normes de sécurité sont «adéquates» et se fondent sur les derniers développements technologiques et les exigences réglementaires de la FINMA.
- Instaurer la **transparence** vis-à-vis du client.
  - Le client doit toujours être informé de ce qui arrive à ses données. Le consentement respectif au transfert de données doit être aussi précis que possible. Par ailleurs, le client doit autoriser l'échange de données de manière volontaire et en toute connaissance de cause.
  - Le client doit avoir de la transparence et le contrôle sur les conditions d'accès à ses données (p. ex. par le biais d'un tableau de bord lui garantissant un contrôle total).

A mesure que la coopération entre la banque et les prestataires tiers s'intensifie, on peut s'attendre à ce que les exigences en ce qui concerne les bases légales augmentent également. En pareil cas, les aspects suivants du droit de la surveillance pourraient entrer en ligne de compte:

- Contrôle du **respect des exigences réglementaires** (loi sur les services financiers LSFin, agréments obligatoires, etc.) par le prestataire tiers.
- Contrôle du **modèle d'affaires** (prévention de la fraude) par le prestataire tiers.
- Contrôle du **concept de protection des données** et de la sécurité des données chez le prestataire tiers.

A ce propos, il est important que la banque vérifie systématiquement si les exigences pertinentes s'appliquent au modèle d'affaires qu'elle a retenu, et si oui, dans quelle mesure, pour se conformer à ses obligations réglementaires en tout temps.

Contrôle des prestataires tiers

Si l'intensité de la coopération entre la banque et le prestataire tiers exige que la banque contrôle ce dernier (voir la section ci-dessus), ce contrôle peut revêtir plusieurs formes.

D'une manière générale, un établissement financier peut suivre l'une des trois approches suivantes:

- **Réalisation bilatérale de contrôles des prestataires tiers** dans le cadre desquels la banque définit un ensemble de critères en s'appuyant sur la réglementation. Tout prestataire tiers souhaitant accéder aux interfaces de la banque doit démontrer à l'établissement financier concerné que ces critères sont respectés dans le cadre du contrôle. Cette procédure, qui se répète à un rythme déterminé par l'établissement financier, permet de personnaliser le contrôle autant que possible en fonction des besoins de l'établissement financier en question. L'établissement financier peut fixer les critères de façon indépendante et mener à bien la procédure de contrôle en toute autonomie. Toutefois, cette forme de contrôle des prestataires tiers peut être la plus fastidieuse, aussi bien pour la banque que pour les prestataires tiers. De plus, cette procédure n'est évolutive dans une mesure très limitée puisque chaque prestataires tiers devrait réaliser un contrôle de prestataire tiers dans chaque établissement financier.
- **Contrôle de prestataire tiers uniforme assuré par une «Trusted Party»** garantissant la protection de la bonne foi en ce qui concerne les exigences personnelles et techniques et la forme de société. Cette approche nécessite la mise en place d'un «label» correspondant qui n'existe pas encore pour le marché suisse. Toutefois, à titre d'exemple, la procédure de SIX régissant le contrôle des participants à sa plateforme «b.Link» a le potentiel pour y parvenir. Elle a été définie en étroite coopération avec les banques et les prestataires tiers, garantissant ainsi la prise en compte de tous les critères de vérification essentiels du point de vue des banques. La procédure est appliquée pour les banques et les prestataires tiers. Elle comprend des contrôles sur la société et ses dispositifs techniques et équipements de sécurité. SIX mandate des auditeurs externes pour assurer le contrôle. SIX fonde sa décision de raccorder ou non un participant à la plateforme b.Link sur un rapport d'évaluation élaboré par l'auditeur à l'attention de SIX. Une fois le contrôle réussi, SIX exige une mise à jour annuelle sur les infor-

mations pertinentes. Le contrôle ne doit être effectué qu'une seule fois et est reconnu par tous les participants à la plateforme b.Link.

- **Appui de certifications existantes.** L'établissement financier pourrait également encourager l'obtention de certifications existantes telles que la certification ISO 27001 en vue du contrôle des prestataires tiers et du respect de l'obligation de diligence. Ces certifications permettent à un prestataire tiers de prouver qu'il se conforme aux processus et contrôles spécifiques. Il convient de noter que ces certifications n'ont pas été spécifiées spécialement pour l'open banking. De ce fait, elles ne livrent que des informations limitées à l'établissement financier quant au respect des critères de sécurité, telles que la conservation sécurisée des token qui leur donnent le droit d'accéder aux données des clients. Cette procédure semble être une variante efficace du fait de l'appui des normes internationales. Chaque établissement financier doit toutefois décider, en concertation avec son service de compliance interne, dans quelle mesure les certificats ISO pertinents suffisent afin que l'établissement financier puisse s'acquitter de son obligation de loyauté et de diligence lors du contrôle de prestataires tiers. Pour les prestataires tiers qui n'ont pas encore prétendu à une telle certification, les démarches nécessitent souvent de lourds investissements.

Conception du cadre contractuel

Si une coopération est instaurée entre une banque et un prestataire tiers, son cadre contractuel doit être défini. Contrairement à ce qui se passe en cas d'externalisation, les parties sont libres à cet égard dans un environnement d'open banking. Suivant le type et la fréquence des interactions entre la banque, le prestataire tiers et le client, différents accords contractuels sont nécessaires. Il convient ainsi de tenir compte des points suivants:

- **Règles régissant l'utilisation de l'échange de données:** quelles données sont échangées et dans quel but?
- **Protection des données:** comment la protection des données est-elle garantie en tout temps?
- **Droits et obligations liés à l'accès aux interfaces:** qui doit remplir quelles obligations envers le client afin d'obtenir la meilleure coordination possible entre les parties à cet égard?
- **Communication vis-à-vis du client:** comment garantir que le client sait en tout temps qui traite ses données où et quels risques pourraient en découler?
- **Règles s'appliquant à la gestion des incidents** quel est le processus à suivre lorsque l'intégrité des données utilisées est compromise?
- **Normes de sécurité:** quelles normes de sécurité sont appliquées?
- **Responsabilité:** qui doit remplir quelles obligations envers le client afin d'obtenir la meilleure coordination possible entre les parties à cet égard?
- **Règles pour le contrôle des prestataires tiers:** comment et à quelle fréquence les prestataires tiers sont-ils contrôlés?
- **Règles relatives à la gestion du déploiement de nouvelles versions, en particulier des déploiements critiques en termes de sécurité:** comment et à quelle fréquence les nouvelles versions sont-elles déployées?

Comme pour le contrôle des prestataires tiers, il existe plusieurs approches pour fixer le cadre contractuel:

- **Accords bilatéraux avec les prestataires tiers:** chaque établissement financier définit un accord contractuel réglementant l'accès à sa propre interface et le conclut avec chaque prestataire tiers. La banque dispose de la plus grande latitude pour personnaliser l'accord, sachant que cela nécessite d'importants efforts pour les prestataires tiers et l'établissement financier et conduit à une moindre évolutivité.
- **Définition et conclusion d'un contrat harmonisé dans la configuration de la plateforme:** une configuration contractuelle où chaque partie participe à une plateforme et n'a qu'à conclure un contrat avec l'opérateur de la plateforme à chaque fois, est gage d'évolutivité. C'est, par exemple, l'approche suivie par b.Link: chaque participant conclut un accord contractuel harmonisé avec le fournisseur de la plateforme et peut ainsi échanger des données avec d'autres participants à la plateforme.

Pour résumer, les parties impliquées dans les configurations d'open banking ont une grande liberté d'action, tant en termes de sélection de partenaires appropriés que de relations entre la banque et le prestataire tiers.

Glossaire

Terme	Définition
Access to Account (=XS2A)	Access to Account désigne l'accès aux comptes clients que les banques doivent octroyer en relation avec des prestataires tiers DSP2. Concrètement, des prestataires tiers bénéficient d'un «accès non discriminatoire» à des comptes clients par l'intermédiaire d'interfaces de programmation d'applications (API). Cet accès porte également sur les fonctions de base «Payment Initiation Service Provider» (PISP) et «Account Information Service Provider» (AISP).
Application Programming Interface (API)	Interface entre différents programmes qui a pour vocation de faciliter l'interaction entre les programmes grâce à un ensemble de règles et de spécifications.
Open API	Interface qui donne accès à des données basées sur une norme publique. Elle est également connue sous le nom d'API externe ou publique.
Données	D'un point de vue logique, les données sont des éléments d'une information qui peuvent également être traités par voie électronique.
DSP2 (Directive 2 sur les services de paiement)	La directive 2 sur les services de paiement (DSP2) est une réglementation de l'UE qui astreint entre autres les banques de l'UE à accorder un accès aux comptes bancaires à des prestataires tiers. La Suisse n'est pas tenue de transposer (directement ou indirectement) la DSP2 car elle n'est pas membre de l'UE ou de l'EEE et elle n'a pas d'obligation de le faire au titre des accords bilatéraux conclus avec l'UE.

Littérature d'accompagnement

Accenture (2018). It's Now Open Banking.

BCG (2018). Retail Banks Must Embrace Open Banking or Be Sidelined.

Basel Committee on Banking Supervision (2019). Report on open banking and application programming interfaces.

Capgemini (2020). World FinTech Report 2020.

Deloitte & Business Engineering Institute St. Gallen (2019). Ecosystems 2021 – what will the future bring? Shaping and positioning of the financial services industry. (Étude disponible seulement en allemand)

ndgit (2019). Open Banking APIs worldwide.

Institute of Financial Services Zug IFZ (2020). IFZ Fintech Study 2020.

Institute of Financial Services Zug IFZ (2019). IFZ Sourcing Studie 2019. (Étude disponible seulement en allemand)

McKinsey & Company (2019). The last pit stop? Time for bold late-cycle moves. McKinsey Global Banking Annual Review 2019.

McKinsey & Company (2017). Data sharing and open banking.

Open Data Institute & Fingleton Associates (2014). Data Sharing and Open Data for Banks.

SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Case postale 4182
CH-4002 Bâle

office@sba.ch
www.swissbanking.org