DSP2 & OPEN API :

Menaces et opportunités pour le secteur bancaire

…En route vers l'Open-Banking ?

www.galitt.com

Sommaire

A PROPOS DE CE DOCUMENT & REMERCIEMENTS 4

A PROPOS DE DS AVOCATS 7

A PROPOS DE GALITT 8

CONTEXTE 9

GLOSSAIRE DE L'API ECONOMY 10

UN NOUVEAU CADRE JURIDIQUE REFLET D'UN ECOSYSTEME EMERGENT 13

1.1 Le cadre juridique 14
1.1.1 Quelques définitions autour de la DSP2 14
1.1.2 Droit d'accès 15
1.2 Le nouvel écosystème issu de la DSP2 19
1.2.1 Le rôle d'AISP (Account Information Service Provider) 19
1.2.2 Le rôle de PISP (Payment Initiation Service Provider) 21
1.2.3 Le rôle de CBPII (Card-based Payment Instrument Issuer) 23
1.2.4 Des services de paiement 25

ENJEU CLE : SECURISER ET STANDARDISER LES ECHANGES DU NOUVEL ECOSYSTEME 27

2.1 Le « web scraping » comme technique de récupération des données 28
2.1.1 Une technique utilisée actuellement par les TPP… 28
2.1.2 …Mais qui pose toutefois problème 28
2.2 Les RTS définitifs : articuler concurrence et sécurité 31
2.2.1 Agréer les TPP comme prestataires de services de paiement 31
2.2.2 Utiliser des certifics conformes au Règlement eIDAS 32
2.2.3 Authentifier le client de façon forte 32
2.2.4 Standards et protocoles ouverts de communication sécurisée 34
2.3 Les API comme réponse au défi d'échanges de données sécurisés et standardisés 34
2.3.1 Le principe des API 35
2.3.2 La standardisation des API, indispensable pour un modèle en rupture 40

STET 45

BERLIN GROUP 49

L'OPEN BANKING UK : UN PRECURSEUR 50

AUTRES INITIATIVES NATIONALES D'API COMMUNES 51

UN TOURNANT STRATEGIQUE POUR LE MONDE BANCAIRE 55

3.1 Rachats et entrées au capital de Fintechs : une stratégie adoptée par les banques françaises 56
3.2 Ouverture des SI bancaire et émergence de l'API economy 58
3.3 Des données bancaires suscitant les convoi- tises d'acteurs hors écosystème bancaire 64

CONCLUSION 69

ANNEXE 71

A propos de ce document & remerciements

La société Galitt, spécialisée dans les paiements, et la société d'avocats DS Avocats ont uni leurs compétences pour la rédaction d'un livre blanc sur l'Open Banking et les enjeux en France de la seconde Directive sur les Services de Paiements (Directive 2015/2366), dite DSP2, qui a remplacé depuis le 13 janvier 2018 dans le Code monétaire et financier la DSP1 de 2009 (Directive 2007/64/CE).

Pour leur participation et expertise, nous tenons à remercier vivement :

Clément Coeurdeuil : *Président et co-fondateur de Budget Insight*

Clément Coeurdeuil est ingénieur de l'Ecole Centrale Paris diplômé en 2012, il est spécialisé dans les systèmes d'information. Passionné d'entrepreneuriat, il a cofondé Budget Insight avec Romain Bignon en 2012, leader français de l'agrégation de données financières et de l'initiation de paiement.

Budget Insight fournit des services d'agrégation de comptes (au travers de l'appli Budgea) et met aussi à disposition des API permettant aux banques et autres institutions financières d'améliorer leur offre de services. Egalement agréée comme PSP d'initiation de paiement, la Fintech est implantée en France et au Luxembourg et connectée à plus de 300 établissements financiers. Plusieurs centaines de milliers d'entreprises et de particuliers utilisent quotidiennement ses services.

Sébastien Taveau : *Chief Developer chez Early Warning*

Sébastien Taveau est Chief Technologist chez Early Warning, où il supervise les opérations de technologie et d'innovation pour les solutions de paiement P2P. Fort d'une expérience de plus de vingt ans des technologies de paiement mobile, il se définit comme un résolveur de puzzle et un observateur d'horizon. Sébastien Taveau est un expert reconnu sur l'Open API, avec de nombreux articles et interventions sur CNN, The Wall Street Journal, The Huffington Post, Mashables, Reuters, Forbes, Dark Reading, Digital Transactions, Newsweek…

Early Warning est une société spécialisée dans les technologies de paiement mobile. Créée il y a 25 ans par Wachovia, JPMorgan Chase, Bank of America, BB&T Corporation et Wells Fargo, Early Warning est au cœur de l'actualité avec le lancement de Zelle

Hervé Robache : *Responsable Normes et Standards chez STET*

Hervé Robache est responsable Normes et Standards chez STET, qu'il a rejoint peu après sa création, en 2005. Avec plus d'une vingtaine d'années d'expérience dans le domaine de la compensation interbancaire, Hervé a notamment participé à la conception et au développement de la plateforme de compensation CORE de STET. Il se retrouve désormais au cœur des enjeux de l'Open Banking, ayant en charge l'animation de l'initiative STET en termes d'API DSP2 et la coordination des travaux avec les autres initiatives européennes (Berlin Group, Open Banking UK) ainsi que la participation aux travaux menés par l'ISO de standardisation des API ISO20022.

STET, fondé par 6 groupes bancaires français, est un acteur majeur du processing multi instrument de paiement (paiement carte, virement, prélèvement, instant payment, chèque, etc.) sur le marché européen. Ses principales missions recouvre la compensation nationale des opérations de paiement de détail nationales, en France et en Belgique, ainsi que le routage instantané des demandes d'autorisation monétiques, via son réseau dédié e-rsb.

A propos de DS Avocats

Créé en 1972 à Paris, le cabinet DS Avocats a développé son savoir-faire au bénéfice des entreprises et des collectivités publiques. Cette double culture du public et du privé est un atout et constitue la signature du cabinet.

DS Avocats compte aujourd'hui près de 400 professionnels, répartis dans 26 bureaux à travers le monde, qui interviennent tant en conseil qu'en contentieux.

Parmi l'ensemble de ses spécialités, le cabinet DS Avocats a développé une expertise reconnue en matière de Banque & Finance avec des équipes spécialisées en matière de financements mais également dans le domaine de la Fintech, de la Banque Digitale et de la Crypto-Finance.

Le Pôle Fintech, Banque Digitale et Crypto-Finance couvre tous les aspects transactionnels, y compris les opérations d'acquisition, rapprochements, accords de coopération, externalisation et aspects fiscaux.

Contacts :

Thibault Verbiest : Avocat associé
+33 6 25 44 12 71
verbiest@dsavocats.com

Frédéric Bellanca : Avocat associé
+33 1 53 64 50 00
bellanca@dsavocats.com

A propos de Galitt

Référence dans le secteur des paiements et des transactions électroniques, Galitt est leader en Europe dans l'ensemble de ses activités et dans le monde pour ses outils de tests et son expertise dans les technologies innovantes.

Galitt propose un ensemble de métiers et de savoir-faire complémentaires et reconnus pour assister ses clients sur tout le cycle de vie des projets et sur la totalité des composants de la chaine de valeur du paiement. Sa dimension lui permet d'appréhender des projets d'envergure, tout en conservant la réactivité, l'encadrement et les motivations d'une structure à taille humaine.

Galitt est la référence dans la mise en œuvre de technologies de paiement les plus avancées et la définition des architectures de demain.

L'offre de Galitt s'organise autour de 5 Business Units :

- Les experts de **Payment Consulting** et leurs approches innovantes éclairent les choix stratégiques des décideurs ;
- Les consultants de **Payment Services** assistent les clients dans la mise en œuvre de leurs projets de paiement ;
- Les équipes de **Testing Solutions** développent des logiciels de test et participent aux phases d'industrialisation des tests ou de certification des solutions ;
- Les collaborateurs de **Payment Solutions** développent et opèrent des applications monétiques et transactionnelles à forte valeur ajoutée ;
- Les formateurs de **Payment Education** relayent l'expertise et le métier de Galitt lors de séminaires de formation.

Galitt est une société du groupe Sopra Steria. En 2017, elle a réalisé un chiffre d'affaires de 31,1 millions d'euros et employait 260 personnes.

Pour en savoir plus sur Galitt, rendez-vous sur notre site Internet : www.galitt.com

Contact Galitt Payment Consulting :
Rémi Gitzinger
Directeur Exécutif
+33 6 20 66 77 40
r.gitzinger@galitt.com

Contexte

Entrée en vigueur le 13 janvier 2018 en Europe, la seconde Directive sur les Services de Paiement dans le Marché Intérieur (DSP2) ouvre la voie à une nouvelle notion : l'Open Banking. Désormais, la liberté des clients à disposer de leurs données bancaires amène les banques à les mettre à disposition d'établissements financiers tiers, au travers d'interfaces de programmation (API), avec pour objectif majeur de stimuler la concurrence et l'innovation dans le secteur.
Cette ouverture des données bancaires, et leur accès par ces établissements tiers régulés, soulèvent de nombreuses interrogations et controverses, en France et en Europe, objet d'analyses détaillées dans ce livre blanc.

Problématique

La DSP2, comment organiser le droit d'accès et quels impacts sur l'écosystème bancaire ?

La première partie de ce livre blanc décrit les effets de la révolution juridique portée par la DSP2 sur le contrôle des données bancaires de paiement. Dans une deuxième partie est présenté le nouvel écosystème qui s'est préparé en Europe, dressant les conséquences opérationnelles et techniques. Enfin, la troisième partie dessine les enjeux pour l'écosystème bancaire, à la lumière d'initiatives de marché au succès déjà significatif.
Le livre blanc récapitule les échéances majeures de la DSP2 encore à venir. En effet, la mi-mars 2018 a vu la parution très attendue de Regulatory Technical Standards (RTS, Normes Réglementaires Techniques). Ce « décret d'application » de la DSP2, portant sur l'authentification forte et sur les échanges sécurisés avec les tiers, lance le compte à rebours de l'ouverture des SI de paiement. Fixant également de nouvelles règles pour authentifier le client, ce texte complète la Directive - sans transposition requise - et ouvre l'ère d'une économie des paiements plus collaborative.

Glossaire de l'API economy

- **API** (Application Programming Interface ou accès par protocole informatique) : ensemble normalisé de fonctions informatiques, méthodes ou classes organisant l'accès d'une application tierce à des services, ressources ou données internes. Conçues pour un usage simplifié et une intégration aisée par les développeurs informatiques tiers, ces interfaces sont en outre sécurisées, évolutives et réutilisables ;

- **EBA** (European Banking Authority ou Autorité Bancaire Européenne) : autorité de l'UE indépendante, chargée d'harmoniser la surveillance prudentielle du secteur bancaire et sa règlementation technique, auteur des RTS et Guidelines ;

- **Open API** : API exposée, c'est-à-dire mise à disposition de tiers externes à la structure. Cette interface organise leur accès à des données et/ou services identifiés et documentés ;

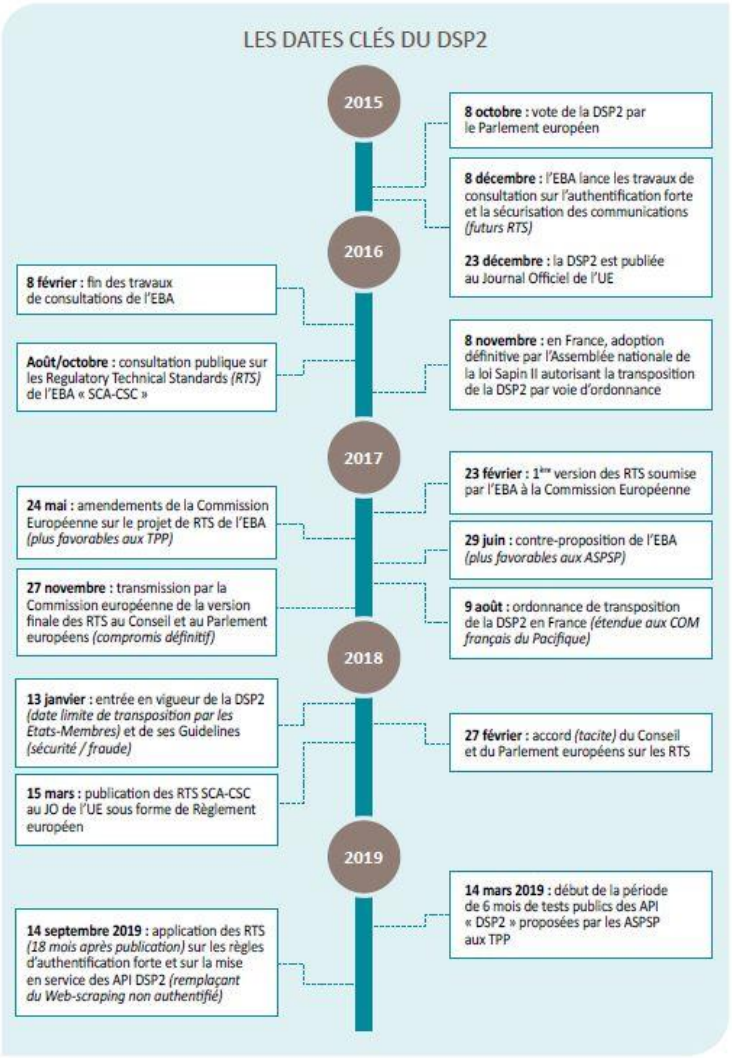
- **Open Banking** : stratégie bancaire s'appuyant sur la transparence des données bancaires pour fournir des Open API permettant à des tiers financiers d'enrichir leurs propres offres et en retour celles de la banque ;

- **Open data** : ouverture des données d'un système interne d'information afin qu'elles soient librement accessibles, utilisables et reproductibles par tous, sans restrictions de droits d'auteurs, de brevets ou d'autres mécanismes de contrôle. Elles permettent aux développeurs d'applications d'offrir des services innovants, voire mis à jour en temps réel ;

- **PSP** (Prestataire de service de paiement) : terme légal désignant les divers statuts d'établissements financiers autorisés à offrir des services de paiement. Il regroupe les établissements de crédit (banque, société de crédit à la consommation), les établissements de paiement (EP), les établissements de

monnaie électronique et, à présent, les prestataires d'information sur les comptes ;

- **RTS** (Regulatory Technical Standards ou Normes Réglementaires Techniques) : ensemble d'exigences détaillées par l'Autorité Bancaire Européenne, en collaboration avec la BCE (Banque Centrale Européenne) et les banques centrales nationales. Divers RTS sont prévus par la directive pour en harmoniser la mise en œuvre opérationnelle. Ceux renforçant l'authentification forte et la sécurité des échanges entre les PSP ont été amendés par la Commission Européenne le 27 novembre 2017 (en tant qu'acte délégué) et publiés le 13 mars 2018.


LES DATES CLÉS DU DSP2
2015
8 octobre : vote de la DSP2 par le Parlement européen
8 décembre : l'EBA lance les travaux de consultation sur l'authentification forte et la sécurisation des communications (futurs RTS)
23 décembre : la DSP2 est publiée au Journal Officiel de l'UE
2016
8 février : fin des travaux de consultations de l'EBA
Août/octobre : consultation publique sur les Regulatory Technical Standards (RTS) de l'EBA « SCA-CSC »
8 novembre : en France, adoption définitive par l'Assemblée nationale de la loi Sapin II autorisant la transposition de la DSP2 par voie d'ordonnance
2017
23 février : 1ère version des RTS soumise par l'EBA à la Commission Européenne
24 mai : amendements de la Commission Européenne sur le projet de RTS de l'EBA (plus favorables aux TPP)
29 juin : contre-proposition de l'EBA (plus favorables aux ASPSP)
27 novembre : transmission par la Commission européenne de la version finale des RTS au Conseil et au Parlement européens (compromis définitif)
9 août : ordonnance de transposition de la DSP2 en France (étendue aux COM français du Pacifique)
2018
13 janvier : entrée en vigueur de la DSP2 (date limite de transposition par les Etats-Membres) et de ses Guidelines (sécurité / fraude)
27 février : accord (tacite) du Conseil et du Parlement européens sur les RTS
15 mars : publication des RTS SCA-CSC au JO de l'UE sous forme de Règlement européen
2019
14 mars 2019 : début de la période de 6 mois de tests publics des API « DSP2 » proposées par les ASPSP aux TPP
14 septembre 2019 : application des RTS (18 mois après publication) sur les règles d'authentification forte et sur la mise en service des API DSP2 (remplaçant du Web-scraping non authentifié)

1

Un nouveau cadre juridique reflet d'un écosystème émergent

1.1 Le cadre juridique

1.1.1 Quelques définitions autour de la DSP2

- **PSU** (Payment Service User ou Utilisateur d'un service de paiement) : utilisateur particulier ou professionnel titulaire d'un ou de plusieurs comptes de paiement (compte courant) et/ou utilisateur d'un service de paiement ;

- **ASPSP** (Account Servicing Payment Service Provider ou Prestataire de services de paiement teneur de compte) : prestataire au sein duquel un client (PSU), détient un ou plusieurs comptes et/ou au sein duquel le PSU initie des paiements. Chaque ASPSP doit posséder le statut d'Établissement de Paiement (EP)1 avec, si nécessaire, le passeport lui permettant d'exercer dans d'autres pays de l'UE. Les établissements de crédit, de monnaie électronique et les établissements de paiement déjà agréés sont considérés comme ASPSP ;

Précision - Etablissement de Paiement (EP) : créés par la Directive sur les Services de Paiement (DSP1) de 2009, ils ont rejoint les établissements de crédit (banques, sociétés financières), jusque-là seuls admis à fournir des services de paiement. Avec le développement du paiement en ligne, de nouveaux acteurs, de taille plus petite, ont aisément pu rendre le paysage plus concurrentiel. Le statut d'EP est délivré par l'autorité financière du pays dans lequel il a ses opérations principales ; en France, il s'agit de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), liée à la Banque de France. L'obtention et la conservation d'un agrément suit une procédure rigoureuse afin d'apporter des garanties fortes aux utilisateurs des services de paiements.

- **TPP** (Third Party Provider ou PSP Tiers) : prestataire agréé pouvant initier des paiements à la demande du payeur, sans détenir les fonds et à partir de comptes qu'il ne gère pas, et offrir des informations consolidées sur ces comptes ;

Il comprend les deux catégories de prestataires suivants :

[1] ***ACPR** : Définition Etablissement de paiement*

- **PISP** (Payment Initiation Service Provider ou Prestataire de Services d'Initiation de Paiement) : prestataire proposant un service qui consiste à initier un ordre de paiement à la demande d'un PSU à partir d'un compte bancaire détenu par un ASPSP

- **AISP** (Account Information Service Provider ou Prestataire de Services d'Information sur les Comptes) : prestataire fournissant un service de consolidation des informations relatives à un ou plusieurs comptes détenus par un PSU auprès d'un ou plusieurs ASPSP ;

- **CBPII** (Card-based Payment Instrument Issuer ou Emetteur d'instrument de paiement lié à une carte[2]) : prestataire émettant une carte, ou une solution similaire en ligne (ex. : Wallet, compte prépayé), rattachée à un compte tiers qu'il débite auprès d'un ASPSP, et pour laquelle cet émetteur tiers pourra désormais demander à l'ASPSP, au moment de chaque transaction, de lui confirmer la disponibilité du montant - sans réservation ou garantie par de l'ASPSP, qui répond par oui ou par non.

Sans conteste, la principale innovation de la DSP2, et celle qui fait le plus débat, est la reconnaissance de ces trois nouveaux services de paiement qui permettent à un tiers de s'intermédier entre un utilisateur et son ASPSP.

Ces nouveaux prestataires de paiement bénéficient de conditions d'exercice allégées et d'exigences prudentielles assouplies par rapport aux ASPSP. Ces nouveaux prestataires doivent toutefois, comme les autres établissements de paiement, faire l'objet d'un agrément (d'un simple enregistrement déclaratif, pour le service d'information sur les comptes) et être couverts par une assurance en responsabilité civile professionnelle équivalente sur les territoires où ils fournissent leurs services, dont le montant minimal est défini par les Guidelines (Orientations) de l'EBA du 7 juillet 2017.

1.1.2 Droit d'accès

Les articles 65, 66 et 67 de la DSP2 ont instauré d'une part, un droit d'accès au compte de paiement pour les prestataires de services d'initiation de paiement (« PISP ») et d'autre part, un droit d'accès aux données du compte de paiement pour

[2] *Parfois abrégé en CISP = Card-Issuing service provider*

les prestataires de services d'information sur les comptes (« AISP ») et pour les émetteurs d'instruments de paiement liés à une carte (« CBPII »).

Ces droits d'accès sont assortis d'un certain nombre de garanties :

1. La limitation aux seuls comptes de paiement accessibles en ligne;

2. L'exigence d'un consentement explicite donné par l'utilisateur des services de paiement à la communication de ses données ;

3. La non-détention de fonds du payeur par les PISPs ;

4. L'inaccessibilité des données de sécurité personnalisées (données d'authentification ou credentials) à des tiers et leur transmission à l'utilisateur et à l'émetteur au moyen de canaux sûrs et efficaces ;

5.
6. La communication de manière sécurisée avec le seul prestataire de service de paiement teneur du compte (« ASPSP »), les TPP, le payeur et le bénéficiaire, conformément aux RTS ;
7. L'absence de modification par les PISP des caractéristiques de l'opération (montant, bénéficiaire, etc.) ;
8. La limitation de l'accès des AISP aux seules informations provenant des comptes de paiement désignés et des opérations de paiement associées ;

9. L'absence de stockage par les PISP des données de paiement sensibles concernant l'utilisateur de services de paiement, qu'il faut entendre comme « des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude » excluant - mais seulement vis-à-vis de l'activité des PISP et AISP - le nom du titulaire du compte et le numéro de compte ;

10. L'absence de demande de communication par les AISP de ces données de paiement sensibles liées à des comptes de paiement ;

11. La limitation des données pouvant être demandées à l'utilisateur de services de paiement à celles uniquement nécessaires pour fournir le service d'initiation de paiement ou le service d'information sur les comptes ;

12. L'utilisation, la consultation et le stockage des données aux seules fins de fournir le service d'initiation de paiement ou le service d'information sur les comptes ;

13. La faculté pour les ASPSP de refuser l'accès des PISP et des AISP à un compte de paiement pour des raisons objectivement motivées et documentées auprès du régulateur, liées à un accès non autorisé ou frauduleux.

Ces nouveaux acteurs, leur offre de services et leur intégration au sein de la chaîne de paiement sont décrits et analysés dans cette seconde partie. Un éclairage relatif aux incidences techniques liées aux partages des données des banques sera également apporté.

TRANSPOSITION DE LA DSP2 : DES COMPTES D'EPARGNE ET DE CREDIT OBJETS DE DEBATS EN FRANCE

Dans une première étape, le 8 février 2018, l'Assemblée nationale a adopté le projet de loi ratifiant l'ordonnance n°2017-1252 du 9 août 2017 portant transposition de la DSP2.

Lors de l'examen au Sénat, le 22 mars 2018, des amendements ont été adoptés, concernant le champ d'application initial de la DSP2 qui ne s'étend qu'aux comptes de paiement ou de dépôts à vue. Les sénateurs ont proposé de prévoir que les procédures d'accès authentifié s'adressent à l'ensemble des comptes de paiement,

d'épargne et de crédit, soulignant que « 80 % des comptes connectés aujourd'hui ne sont pas des comptes de paiement mais des comptes épargne, des comptes de crédit, des produits d'assurance-vie ».

Cette extension rejoint le point de vue défendu par les banques allemandes proactives sur l'application extensive de la DSP2. A titre d'exemple, la banque allemande HypoVereinsbank avait ouvert ses données de ses clients à la Fintech MoneyMap. Plutôt que de s'opposer à l'accès aux données permis par la DSP2, les banques allemandes ont préféré la signature de partenariats avec des Fintechs destinés à apporter de nouveaux services aux clients des banques.

Après un premier échec, la commission mixte paritaire dédiée a abouti le 27 juin 2018 à un projet commun, adopté en dernière lecture par l'Assemblée Nationale le 5 juillet 2018. Ce projet de loi commun, adopté à son tour le 25 juillet 2018 par le Sénat, ne comprend plus l'amendement sur la contrainte d'accès authentifié pour les comptes d'épargne et de crédit. Ce type de compte sort donc, in extremis et pour le moment, du périmètre de transposition de la DSP2 en France.

1.2 Le nouvel écosystème issu de la DSP2

La DSP2 vise à encadrer de nouveaux acteurs de paiements en sus de l'écosystème des établissements de paiements et des banques.

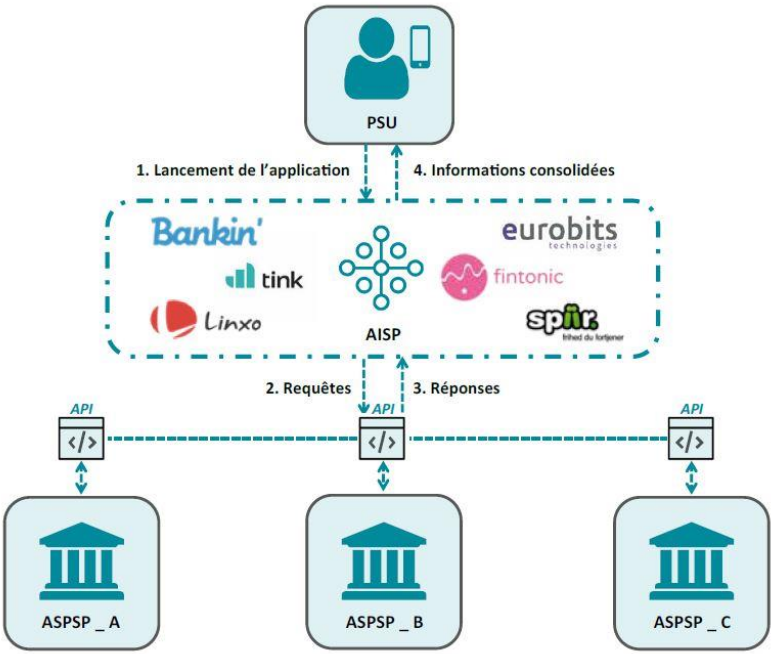
Précision - « Fintech » : combinaison des termes « finance » et « technologie », il s'agit d'une startup innovante qui utilise la technologie pour repenser et proposer des services financiers et bancaires à moindre coût pour le client final. Les Fintechs se spécialisent par activités : crowdfunding, monnaies virtuelles, applications mobiles, paiements électroniques, robot-conseillers, e

Le positionnement de chacun de ces acteurs et les fonctions qu'ils couvrent dans la chaîne de valeur des paiements sont présentés ci-dessous.

1.2.1 Le rôle d'AISP (Account Information Service Provider)

Les AISP offrent à leurs clients (PSU) la possibilité d'agréger leurs différents comptes détenus dans plusieurs établissements (ASPSP), au sein d'une même application offrant une vision consolidée de leurs données.
Le service d'agrégation prévu par la directive est le suivant : après avoir obtenu le consentement du client, l'agrégateur va se connecter aux différents ASPSP détenant les informations du client (PSU), au travers d'une interface dédiée.

FONCTIONNEMENT D'UN AISP PRÉVU PAR LA DSP2



Après avoir récupéré les données de compte auprès de chaque ASPSP, l'application analyse les données recueillies et les restitue dans une interface ergonomique présentant une situation agrégée des comptes.

Deux agrégateurs dominent actuellement le marché en France, Linxo et Bankin'. La première société créée en 2010 comptabilise actuellement 900 000 utilisateurs, et fait office d'outsider. La seconde, Bankin', est une Fintech parisienne comptant aujourd'hui 1,3 million d'utilisateurs sur quatre pays européens. Une autre start-up s'est démarquée en France : Fiduceo, rachetée en 2015 par Boursorama, la banque en ligne filiale de la Société Générale.

D'autres agrégateurs se sont également largement développés en Europe. Les principaux, Tink en Suède, Spiir au Danemark ou encore Fintonic et

Euro-bits en Espagne, comptent plusieurs centaines de milliers d'utilisateurs chacun.

Afin de se démarquer, ces plateformes développent d'autres services à valeur ajoutée, comme la gestion des finances personnelles (analyses de dépenses ou coaching financier), ou encore la gestion documentaire (factures, notes de frais…). Le client est au cœur de leur stratégie, privilégiant la facilité de leur expérience utilisateur grâce à des services innovants et intuitifs.

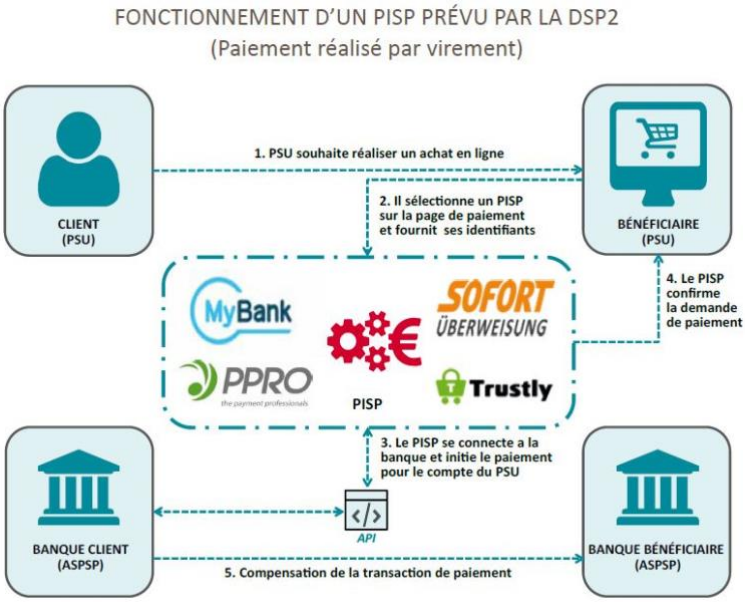
1.2.2 Le rôle de PISP (Payment Initiation Service Provider)

Les initiateurs de paiement interviennent en particulier sur le marché de l'e-commerce. Un e-commerçant peut élargir au virement sa palette de paiements acceptés, en intégrant l'offre de ces tiers au côté des marques de cartes de paiement et des méthodes prépayées : CB / Visa / Mastercard / American Express ou encore PayPal. Au moment du règlement, les clients (PSU) pourront alors choisir d'utiliser un PISP, dont l'offre se veut simple, donc souvent sans obligation d'inscription en amont de la transaction. Le client PSU doit simplement autoriser le PISP à accéder à son compte en renseignant ses identifiants de connexion à la banque en ligne. Dans le cadre de la DSP2, ce procédé repose sur un virement, au bénéfice de l'e-commerçant.

Les offres des PISP s'orientent majoritairement vers les pays où l'usage de la carte bancaire est moins répandu. Les PISP ont ainsi une position bien établie dans le nord de l'Europe, notamment en Allemagne avec Sofort (une entreprise du groupe suédois Klarna), ou encore en Suède avec Trustly.

De la même manière que les agrégateurs, ces applications peuvent se coupler à d'autres fonctionnalités pour proposer des services plus élaborés.

Trustly donne ainsi à ses clients une vision sur le solde de leurs différents comptes disponibles (épargne ou compte courant) et leur permet de choisir lequel sera utilisé pour le paiement. Son offre couvre aujourd'hui l'ensemble des banques suédoises, danoises, finlandaises et espagnoles. Trustly élargit actuellement son réseau autour des plateformes de jeux, des marketplaces et également des services de transfert d'argent.



Avec la création de la société Sofort en Allemagne en 2005 et du retentissement de son nouveau service de virement en ligne, le marché des paiements en Europe s'est retrouvé dans une situation inédite.
En Allemagne tout d'abord, les banques ne pouvant empêcher Sofort de se connecter à leurs interfaces, elles en ont contesté la légitimité auprès du régulateur, alléguant un risque lié à un accès total aux comptes de leurs clients.

Au niveau européen, dans l'objectif de Single Euro Payment Area (SEPA), cet acteur innovant a été perçu par le législateur, notamment la Commission Européenne, comme capable de stimuler la concurrence dans les services de paiement, avec ce type d'offre efficace et peu coûteuse.

Avec la DSP2, la Commission Européenne a, en conséquence, choisi de favoriser ce type d'entrepreneur innovant, voire disruptif. Elle libéralise donc de façon poussée le cadre réglementaire, tout en sécurisant les échanges de données entre

ces TPP et les teneurs de compte, au travers de nouveaux standards et protocoles de communication.

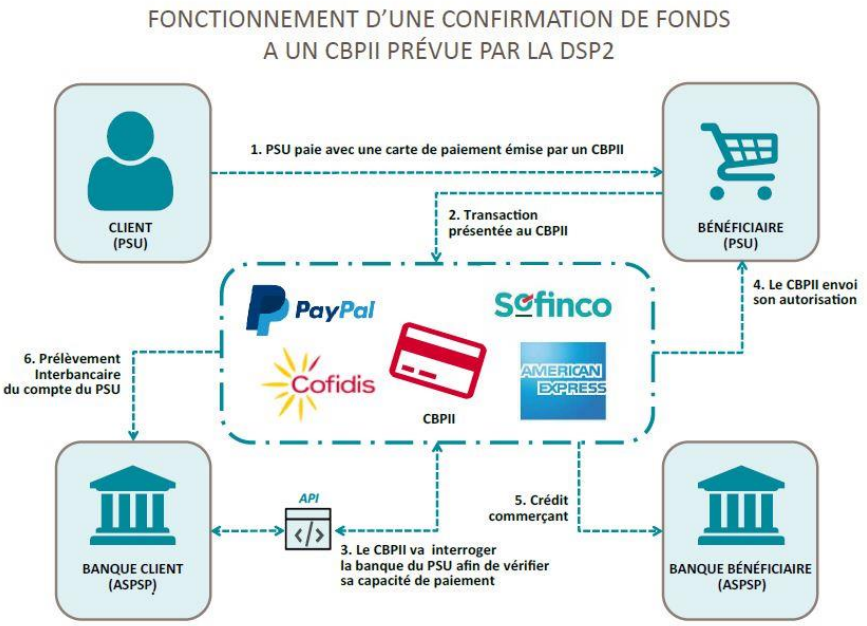
Nombre de ces TPP opèrent déjà, aux côtés de Sofort : nous présentons ci-après leur mode opératoire actuel, appelé « web scraping », ainsi que celui qui le remplacera obligatoirement, avec les Open API requises par la DSP2.

1.2.3 Le rôle de CBPII (Card-based Payment Instrument Issuer)

Outre l'officialisation de ces deux nouveaux services de paiement, la DSP2 permet désormais aux PISP et aux émetteurs d'instruments de paiement adossés à des comptes de paiement d'interroger directement les ASPSP. En temps réel, ils obtiendront confirmation de la disponibilité du montant d'une transaction sur le compte lié à (débité par) l'instrument de paiement. Dans son opinion sur la mise en œuvre des RTS, l'EBA accorde en effet aussi ce service aux initiateurs de paiement (PISP).

Le Card-based Payment Instrument Issuer (CBPII) bénéficie de ce nouveau service de confirmation de fonds, qu'il émette une carte de crédit à la consommation, un compte prépayé rechargeable ou une carte à débit différé de type T&E (Travel and Entertainment). En pratique, il s'agit d'un compte dont l'encours de transactions est soldé périodiquement par débit d'un compte courant détenu chez un ASPSP. Pour chaque paiement avec la carte du CBPII, celui-ci vient, a posteriori, prélever les fonds sur le compte courant externe détenu par le PSU, indiqué au TPP lors de sa souscription (IBAN), sur base d'un mandat de prélèvement (SDD).
Ce type d'acteur existe depuis de nombreuses années sur le marché de la carte de paiement. Des acteurs internationaux comme American Express, Paypal, ou en France, tels que Cofidis ou Sofinco auront accès à ce rôle de CBPII.

Le nouveau service de confirmation de fonds à l'émetteur tiers, formalisé par la DSP2, permet au CBPII de s'assurer qu'à l'instant de la transaction, les fonds sont bien disponibles sur le compte de l'ASPSP, en interrogeant directement ce dernier. Elle donne donc à cet émetteur une nouvelle donnée informative, utile par exemple pour gérer les impayés et la fraude. En revanche, cette vérification d'un montant ne vaut pas réservation de fonds : si à l'instant de la transaction, les fonds sont disponibles, rien ne garantit leur couverture à échéance. Il ne s'agit que d'une information pouvant renforcer la gestion du risque du CBPII. Celui-ci garde la main sur la décision d'autoriser ou non une transaction.



1.2.4 Des services de paiement

Certains TPP proposent d'ores et déjà la combinaison de ces nouveaux services de paiement dans le but d'offrir des services à valeur ajoutée au PSU.

Ainsi de nombreux établissements, qu'ils s'agissent de banques de réseau (Société Générale), banques en lignes (Boursorama), ou TPP (Bankin, Linxo), offrent depuis 2017 la possibilité, outre la consultation agrégée des comptes désignés du PSU, d'initier des virements à partir d'autres comptes en restant sur leur application ou leur espace client. L'utilisateur a la possibilité de mener de bout en bout la gestion de ses comptes sans s'y connecter un à un. Après leur consultation via l'agrégation, il peut, s'il a besoin de les équilibrer, transférer une somme via le service d'initiation de paiement.

Les modalités concrètes diffèrent selon les établissements : certains ne proposent que la possibilité d'effectuer des virements internes (compte à compte), quand d'autres permettent aussi des virements externes, sous réserve d'avoir validé au préalable le RIB bénéficiaire dans la banque en ligne du compte donneur d'ordre.

Un service de plus dans une expérience client « frictionless » est de proposer un service de gestion de trésorerie automatisée pour particuliers : l'agrégation offrant une vue d'ensemble des comptes du client, paramétrer l'initiation de paiement permet d'optimiser les fonds disponibles entre comptes. Cette allocation se déclencherait sur des critères définis par le client, par exemple :

- en virant automatiquement sur un compte d'épargne un montant maximisé en fonction du reliquat disponible en fin de mois sur un compte ;

- ou, afin d'éviter tout découvert, en générant un virement depuis un compte excédentaire dès l'atteinte d'un seuil plancher (fixé par l'utilisateur) sur le compte principal.

Ce service de gestion de trésorerie s'appuie sur les opportunités créées par la DSP2. Il est tout aussi pertinent pour les entreprises, particulièrement les moins grandes qui, à ce jour, ne bénéficient pas de ce type de service (cash-pooling) que la plupart des banques réservent à leurs grands comptes.

Enjeu clé : sécuriser et standardiser les échanges du nouvel écosystème

2.1 Le « web scraping » comme technique de récupération des données

2.1.1 Une technique utilisée actuellement par les TPP…

La plupart des AISP et certains PISP utilisent la technique dite du « web scraping » pour fonctionner. Elle consiste à extraire le contenu de sites Web, via un script ou un programme qui va lire le code html, dans le but de le transformer pour permettre son utilisation dans un autre contexte. Cette technique est celle utilisée, par exemple, par les sites de comparateurs de prix (trivago.fr, liligo.com...).

Dans le cas présent, un TPP, va demander à son client (PSU) les identifiants de connexion à la banque en ligne de son ASPSP. Il va ensuite les intégrer dans un programme qui, comme un robot, simulera la connexion à la place du client. Il va ensuite récupérer au sein de cette page l'ensemble des informations nécessaires à son fonctionnement, de façon ponctuelle (initiation de virement) ou périodique (consultation de comptes).

2.1.2 …Mais qui pose toutefois problème

- **Pour l' ASPSP** : un robot qui passe continuellement sur sa page Internet peut ralentir son fonctionnement. En cas de nombreuses connexions simultanées, ce mode opératoire peut provoquer une attaque par déni de services (un trop grand nombre de requêtes que le serveur ne peut prendre en charge, conduisant alors à un arrêt de service) ;

- **Pour le TPP** : ce mode nécessite de configurer autant de robots qu'il y a d'ASPSP, dans la mesure où les sites ne sont pas standards, d'où un temps de programmation important et un travail risquant d'être obsolète si l'ASPSP modifie sa page ;

- **Pour le PSU** : en donnant son consentement à un TPP, le PSU donne accès à la totalité des informations contenues dans sa banque en ligne. Bien que les services proposés soient légitimes et que les PSP garantissent la confidentialité des données, ils sont aujourd'hui dans la capacité de récupérer l'ensemble des informations détenues sur les comptes des clients : soldes,

- virements, prélèvements, et toutes les métadonnées liées (lieu, date, heure, commerce, montant, montant du loyer,

- remboursements, emprunts, opérateur téléphonique, assurances, salaire, rembour- sements médicaux, habitudes de consommation, etc.) ;

- **Pour les trois acteurs** : le problème majeur de la technique du web scraping réside dans le partage de responsabilité et le principe de la preuve. Prenons le cas d'une fraude, par exemple, sur un virement initié depuis le compte d'un PSU à son insu. Puisqu'il a donné ses identifiants bancaires et son consentement à un TPP, il peut être difficile de déterminer la chaîne de responsabilité : le PSU lui-même, le TPP ou l'ASPSP ?

LE REGIME DE LA RESPONSABILITE DE LA DSP2

L'une des pierres d'achoppement de la DSP2 concerne le régime de responsabilité institué entre les acteurs de la chaine de paiement.
Les articles 73 et 90 font porter aux teneurs de comptes (« ASPSP ») la responsabilité envers les utilisateurs en cas d'opération de paiement non autorisée, non exécutée ou mal exécutée, alors même qu'elle a été initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement (« PISP »). En outre, l'article 74 protège le donneur d'ordre de toute responsabilité financière, à la charge de son établissement financier, lorsque celui-ci n'a pas authentifié le client de manière forte.

La DSP2 a toutefois prévu un certain nombre de garanties :

1. une présomption de responsabilité du PISP (à lui de prouver à l'ASPSP que la défaillance ou l'incident ne lui sont pas dus) ;
2. un droit de remboursement à la première demande de l'ASPSP contre le PISP ;
3. le droit pour l'ASPSP de vérifier en amont que le PISP satisfait bien les conditions posées par la DSP2 ;
4. et, à défaut, le transfert au PISP de l'obligation de rembourser l'utilisateur qui ne respecte pas les conditions posées par la DSP2.

Cependant, la directive n'impose pas la contractualisation entre parties : un PISP peut accéder aux comptes du simple fait de la DSP2.

Sollicitée par les grandes banques de détail, la Banque de France a réaffirmé au printemps 2018 que la responsabilité de l'authentification forte incombe à l'ASPSP, en tant qu'établissement du payeur. Il est donc libre d'en déterminer les modalités, ainsi que la fréquence. Ce contrôle doit toutefois respecter un parcours convivial pour le client (PSU), sans gêner l'expérience d'usage avec un TPP[3].

[3] *Défini, par la Banque de France, comme n'imposant pas au client (PSU) plus de 5 étapes hors de l'environnement du TPP*

2.2 Les RTS définitifs : articuler concurrence et sécurité

La version initiale des RTS, soumise en février 2017 par l'EBA selon le mandat de l'art. 97 DSP2, avait été amendée par la Commission Européenne le 24 mai suivant, dans un sens plus favorable aux TPP. Après les contre-propositions de l'EBA, fin juin 2017, puis une longue recherche de compromis, la Commission a remis fin novembre 2017 la version finale des RTS au Conseil et au Parlement européens. En l'absence d'objection, ces RTS ont été publiés au Journal Officiel de l'UE le 13 mars 2018, sous forme de Règlement Européen (Cf. Dates clés de la DSP2).
Bien que directement applicables, ces RTS feront en France l'objet de précisions ultérieures, un décret d'application étant désormais prévu par la ratification de la transposition de la DSP2. Il portera sur les modalités d'échanges entre ASPSP et TPP.

2.2.1 Agréer les TPP comme prestataires de services de paiement

La première condition d'accès aux comptes est l'obligation, pour tous les AISP et PISP, d'obtenir un agrément d'établissement de paiement (a minima) auprès des autorités nationales, qui étudient ainsi la fiabilité des services proposés. Cette procédure d'agrément est complète pour les PISP, mais allégée pour les AISP (déclaration avec accord tacite). En France, ce régulateur reste l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), présidée par la Banque de France.

2.2.2 Utiliser des certifics conformes au Règlement eIDAS[4]

Le Règlement européen eIDAS (électronic IDentification And trust Services) du 1er juillet 2016 vise « un climat de confiance dans l'environnement en ligne » en fournissant un cadre européen intersectoriel complet pour des transactions électroniques sécurisées, fiables et simplifiées entre citoyens et entreprises.

Pour l'accès aux comptes, l'usage de certificats conformes eIDAS sert à authentifier les ASPSP, les AISP et les PISP. Ils s'appuieront sur les autorités de certification reconnues, qui garantiront l'authenticité de l'agrément de chaque établissement et son rôle.

2.2.3 Authentifier le client de façon forte

La DSP2 impose le principe d'authentifier de manière forte le client dans toute situation de paiement exposée au risque de fraude, et notamment l'accès aux comptes de paiement en ligne et les transactions de paiement électroniques.

Cette authentification forte requiert au minimum deux facteurs faisant partie d'au moins deux des catégories suivantes :

- **Connaissance** : ce que seul le client connaît (ex. : code PIN, information privée) ;
- **Inhérence** : ce que le client est (ex. : élément biométrique, comme l'empreinte digitale) ;
- **Possession** : ce que seul le client détient (ex. : carte de paiement sécurisée, ligne téléphonique ou compte mail où est reçu un OTP, adresse où est reçu un courrier).

En outre, l'authentification forte génère une donnée unique propre à la transaction, véhiculée de bout en bout : le « code d'authentification[5] » .

[4] *ANSSI : présentation du Règlement européen eIDAS*

[5] *Ce « code d'authentification » résultant de l'authentification, il diffère d'un éventuel code servant à l'établir, au titre d'un des facteurs forts requis. C'est un identifiant véhiculé dans la transaction, accepté une seule fois par l'ét. du payeur (ASPSP). En outre, pour les paiements à distance, ce code est « dynamiquement*

Avec ces deux exigences, l'authentification est conduite par l'ASPSP, qui porte le risque. Avant toute opération, il doit vérifier l'agrément et le rôle du TPP. Pour autant, il doit s'abstenir de contrôler systématiquement le consentement du client. Il lui appartient donc de définir, dans ses API, une politique de sécurité client (critères de SCA) non discriminante, c'est-à-dire qui ne fasse pas obstacle à l'activité des TPP.

En outre, le TPP doit, s'il le souhaite, pouvoir s'appuyer sur les procédures d'authentification de l'ASPSP via ses API.

Les RTS finaux prévoient 9 cas (facultatifs) d'exemption à l'authentification forte. Parmi les options applicables aux parcours d'API via des TPP[6], citons les exemples suivants.

- L'exemption en cas de consultation des informations sur les comptes s'applique :
  - s'il ne s'agit pas d'une première connexion au service de l'ASPSP via ce TPP, et que cette connexion est réalisée dans un délai de 90 jours après la dernière connexion authentifiée ;
  - si le service de consultation est limité à des informations qualifiées de non sensibles (le nom, le numéro de compte et l'historique des transactions sur les 90 derniers jours[7]) ;
- L'exemption pour les transactions à distance de petit montant s'applique à des opérations de moins de 30 euros, sans que le cumul depuis la dernière authentification forte n'excède :
  - soit 100 euros ;
  - soit 5 transactions (le choix entre les deux étant à la main de l'établissement du payeur) ;

lié » au montant et au bénéficiaire de la transaction.

6 *D'autres cas d'exemptions des RTS sont résumés en annexe. Dans tous les cas, seul l'établissement du payeur décide d'utiliser l'une ou l'autre des exemptions applicables.*

7 *L'ASPSP doit tenir un compteur de 90 jours distinct pour chacun des accès d'un même client (direct, via AISP1, via AISP2… etc.), sans tenir compte du canal d'accès (mobile / Web / autre…)*

- L'exemption au titre des bénéficiaires de confiance s'applique à tout paiement dont le destinataire a préalablement été listé par le client auprès de l'ASPSP, sous SCA. La Banque de France a décidé que le PISP aura accès en écriture à cette liste.

2.2.4 Standards et protocoles ouverts de communication sécurisée

Les ASPSP doivent mettre à disposition des TPP une interface dédiée pour leur communiquer, de façon sécurisée, les informations et ressources nécessaires pour les services de paiement CBPII, PISP et AISP[8]. L'EBA laisse ouverte la mise en œuvre technique sous les conditions suivantes :

- Avoir les mêmes fonctionnalités qu'en accès direct du client (c'est-à-dire qu'en banque en ligne), avec le même niveau de performances et de disponibilités ;

- Organiser les échanges de données sécurisés, via des standards de communication ouverts et universels, tels que les messages financiers automatisés de bout en bout de la norme ISO 200229;

- Ne pas se borner à l'utilisation de standards génériques d'Internet comme HTTP, HTTPS, TLS et SSL, qui n'offrent pas les garanties de sécurité suffisantes aux échanges de données financières.

2.3 Les API comme réponse au défi d'échanges de données sécurisés et standardisés

8 *Cf. articles 97(5), 65(2)c, 66(3)b et 67(2)b de la DSP2*

9 *ISO 20022 : Universal financial industry message scheme, norme ouverte de messages pour opérations de paiement, change, titres ou financement d'exportations*

2.3.1 Le principe des API

Le concept d'API est bien antérieur à la DSP2. Même si le texte de la directive et des RTS ne mentionnent pas la notion d'API en tant que telle, et que l'EBA se contente de lister des exigences techniques, les API apparaissent comme la solution la plus adéquate pour prendre en compte l'ensemble des exigences mentionnées précédemment.

INTERVIEW

Sébastien Taveau - Chief Developer chez Early Warning
Afin d'apporter un éclairage sur les notions d'API et d'Open API, nous avons fait appel à Sébastien Taveau, Technologist chez Early Warning.

Galitt : pourriez-vous définir ce que le terme « API » signifie selon vous ?

Sébastien Taveau : une API est un moyen structuré pour exposer des services ou des données à des tierces parties via une passerelle contrôlée et sécurisée. Dans l'absolu, il s'agit ni plus ni moins que d'une logique de questions-réponses.
Ainsi dans le cas d'un agrégateur de données (AISP), il enverra depuis son application une requête demandant de récupérer des données définies. Cette requête va transiter via une passerelle, l'API, qui va interroger le service en question au sein de l'ASPSP afin de récupérer les données. Les données transiteront en retour par cette passerelle vers l'application de l'AISP, qui les compilera (Cf. Schéma p.16).

ILLUSTRATION D'UNE API

Sébastien Taveau : il existe plusieurs types d'API, dont les principales sont :

- **API Privées** : il s'agit d'une intégration 1:1. Dans ce cas, l'API a été conçue pour un partenaire spécifique et ne sera utilisable que par celui-ci. Les API privées sont très généralement utilisées pour le partage de données sensibles présentant des risques pour les parties (listes noires, données personnelles…) ;

- **API Publiques** : ce sont les API les plus largement répandues, ne présentant pas de sensibilité particulière. Nous pouvons mentionner le cas de l'API de Google Maps ou celle des fils d'actualité de Twitter par exemple. Une inscription est encouragée, pas nécessaire ;

- **API Ouvertes ou (Open API)** : ce sont des API conçues pour un public plus large que celui des API privées. Elles exigent de la part du TPP d'accepter les

termes et conditions d'utilisation et nécessitent un processus de garantie et de sécurité via un enrôlement d'authentification « OAuth ». L'inscription est nécessaire pour utiliser ce service. Dans le cadre fourni par la DSP2, les Open API sont celles qui correspondent le mieux aux attentes concernant le recours à des interfaces dédiées, car elles permettent à l'ASPSP de contrôler les utilisateurs qui se connecteront afin de venir récupérer des données.

Un autre élément important à noter est que certaines API sont génératrices de revenus tandis que d'autres n'apportent pas de forte valeur ajoutée (utilisées pour la diffusion de contenu media gratuit ou comme service d'accroche, mais sans perspective économique sur ces API).

Par exemple, les API publiques ne sont pas orientées pour générer du profit, mais il est important de mentionner que le coût de maintien et l'ajout de données, pour tout type d'API, ont un impact financier non négligeable. Le business model réside alors dans l'utilisation des API à grande échelle ainsi que dans la pollinisation croisée avec d'autres API, ou au travers de services payants sous-jacents à l'utilisation d'une API. Il est envisageable de regrouper plusieurs fonctionnalités en fonction de la capacité de mappage des API.

Galitt : quels sont les avantages liés à l'Open API ?

Sébastien Taveau : les API et plus particulièrement les Open API offrent une grande flexibilité car elles permettent de maintenir une couche de sécurité tout en forçant l'administrateur à penser aux usages qui pourront être faits par les tierces parties.

Je compare souvent une API ouverte à un objet dans une boite en verre trempé : on peut voir l'objet, on peut secouer cette boite, mais on ne peut pas le toucher.

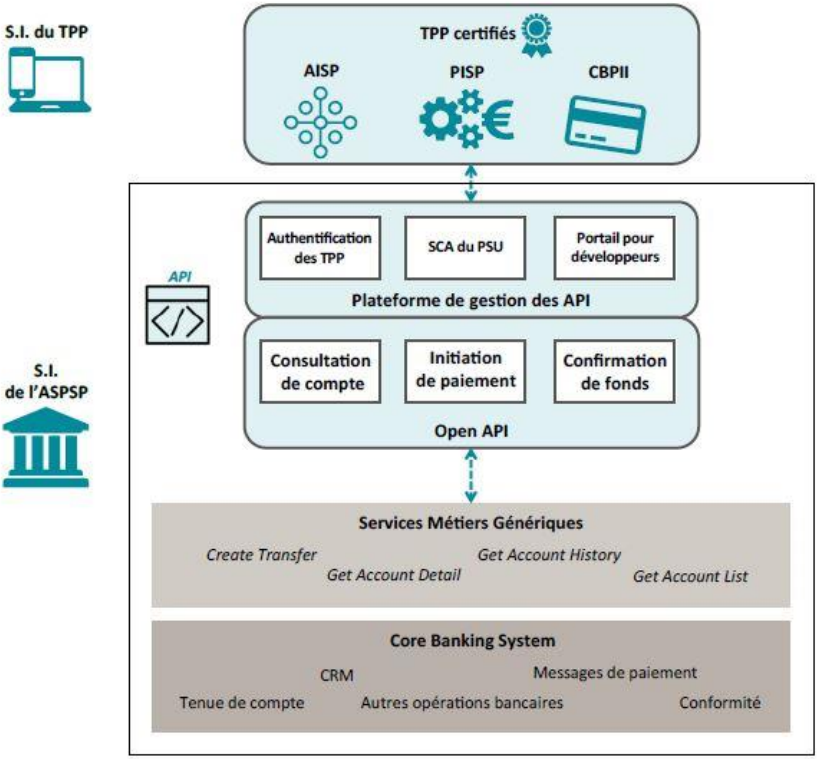
Une API comme nous avons pu le voir est un ensemble d'appels prédéfinis accédant à un service via une passerelle. Cette dernière apparait comme le point critique en termes de sécurité dans la mesure où le TPP, au travers de l'API, va directement interroger le SI des ASPSP.

Il est techniquement facile de construire dans le mécanisme un moyen de verrouiller la communication si un problème est détecté. De plus, avec l'Open API, l'authentification OAuth est obligatoire, ce qui limite encore davantage le risque. OAuth n'est pas un protocole d'authentification, mais un protocole de délégation

d'autorisation, ainsi il permet d'autoriser une application à utiliser une API sécurisée pour le compte d'un utilisateur. Il s'agira donc d'une couche de sécurité supplémentaire en plus de celle représentée par l'authentification forte. Encore une fois, l'analogie de l'objet dans du verre trempé est très parlante. De plus la réponse fournie par l'API est la seule chose que le TPP peut collecter ce qui est primordial.

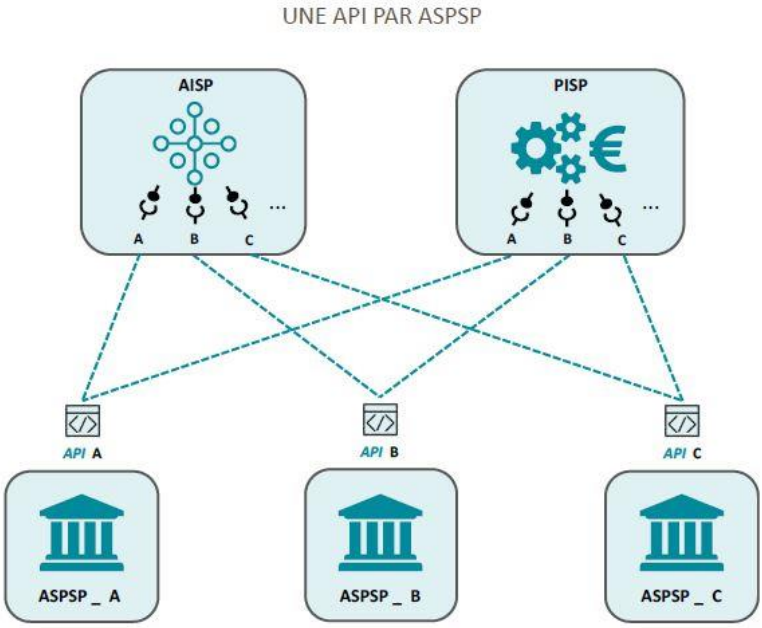
Pour résumer cette partie, on constate que la directive va entièrement bouleverser les relations entre les acteurs tant en matière juridique que technique.
L'impact majeur de ces innovations concerne aujourd'hui la banque à proprement parler. Dans les paragraphes suivants sont analysées les différentes possibilités qui s'offrent aujourd'hui et les initiatives observables.

LES API DANS LE CAS DE L'OPEN BANKING VISENT
À FACILITER L'INTERFAÇAGE ENTRE ASPSP ET TPP
(Architecture d'interfaçage par API pour l'Open Banking)



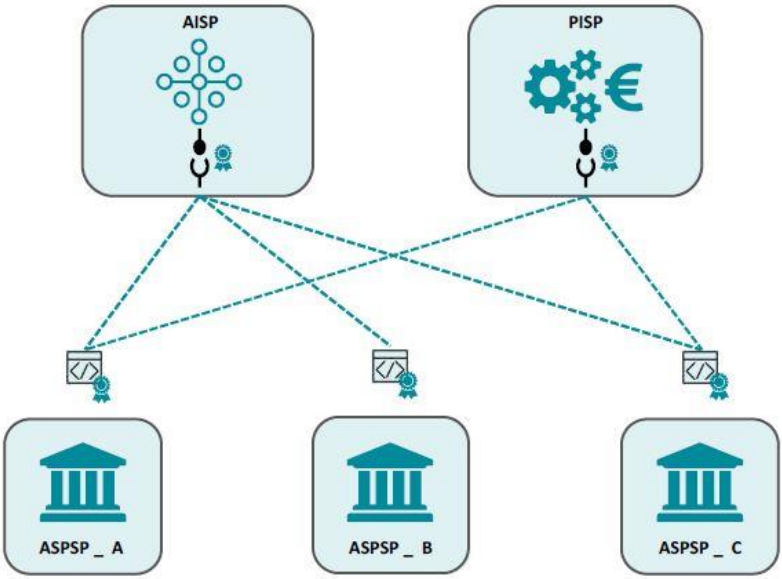
2.3.2 La standardisation des API, indispensable pour un modèle en rupture

La standardisation est un élément fondamental du déploiement d'un modèle en rupture. Pour fonctionner, les TPP doivent se connecter au travers d'une interface sécurisée, dans l'absolu des API, fournies par les ASPSP, afin de récupérer les informations nécessaires.
Le schéma ci-dessous illustre la mise en place d'API par les ASPSP pour le compte des TPP.



Ce schéma montre que pour se connecter à une banque A, les TPP (AISP ou PISP), doivent identifier le moyen technique pour permettre à leurs applications de se connecter à l'API de l'ASPSP_A pour interpréter les données fournies. Cette opération de développement est à répéter pour chaque d'ASPSP. Les TPP doivent donc être en capacité de gérer de nouvelles complexités techniques relatives à la variété des programmations d'API et à celle des données hiérarchisées.

ILLUSTRATION D'UNE API UNIVERSELLE



Dans ce schéma, les TPP et les ASPSP utilisent les mêmes standards de communication. Ainsi chaque API est identique, une seule programmation est désormais nécessaire. La standardisation facilite la relation entre les acteurs. Allant plus loin dans la démarche, la volonté au travers de ce projet est d'ouvrir la voie de l'Open Banking. La banque devient une plateforme modulaire où les acteurs interagissent au travers d'API.

Ce principe de « bank-as-a-platform » est présenté au travers du cas d'usage de SolarisBank détaillé page suivante.

SOLARISBANK, LA BANQUE DE DEMAIN ?

SolarisBank a été créée en 2015 par le groupe financier allemand FinLeap. Se voulant la première banque 100 % digitale, elle a obtenu sa licence bancaire auprès du régulateur financier allemand BAFin en neuf mois.
Axant sa stratégie vers les jeunes entreprises, SolarisBank opère avec un business model B2B2C qui est typiquement celui de l'Open Banking. Sa plateforme en marque blanche permet aux Fintechs de fournir leurs services bancaires, à la carte. Le client peut alors interagir directement afin de créer son environnement bancaire avec les applications qui l'intéressent.

La banque agit ainsi comme une boite à outils modulaires au travers de son API. Sont disponibles des services de tenue de compte, de paiement de détail, de cartes de crédit, d'octroi de crédit en temps réel et de tiers de confiance. Lors d'un nouveau tour de table en mars 2018, Solaris a réuni à son capital Visa, BBVA et ABN Amro. Ayant conquis 60 clients entreprises, elle en vise 100 fin 2018.

« Nos services sont comme des briques Lego : nos partenaires peuvent choisir les briques dont ils ont besoin et assembler des solutions personnalisées pour répondre à leurs propres attentes. Ils accèdent aux services de Solaris Platform via notre API. L'intégration simple leur permet de se concentrer sur leurs métiers. De plus, nos services sécurisés garantissent la confidentialité de leurs données. »
Andreas Bittner : Member of the Board and Founder, SolarisBank[10]

solarisBank

[10] *SolarisBank : Présentation de la société*

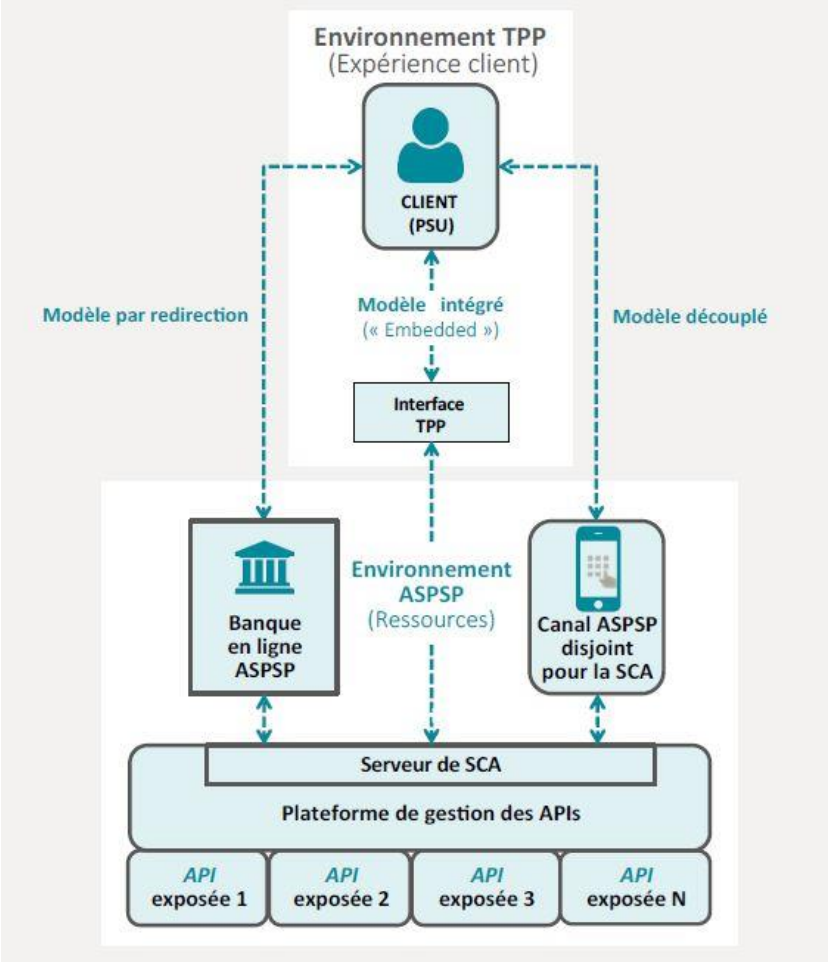
En résumé, il est possible d'utiliser cette plateforme en marque blanche pour créer sa propre banque. SolarisBank conserve les fonctions clés de la banque telles que la base de données clients, l'émission de cartes, la gestion des comptes bancaires, la conformité, la gestion des risques etc. Elle fait cependant intervenir différents acteurs pour implémenter chacune de ces briques.

Dans le modèle de banque plateforme, les banques se placent au centre d'une nouvelle économie dans laquelle les API sont sources de revenus et permettent d'adresser plus efficacement les besoins hétérogènes des clients.
SolarisBank n'est pas la première à proposer ce genre de modèle. La pionnière dans le domaine est Fidor Bank, rachetée par le groupe BPCE.

L'intérêt évident de la standardisation a d'ailleurs mené à plusieurs initiatives de place en Europe, visant à mutualiser et harmoniser un socle d'API « DSP2 ». Un point crucial de chaque spécification d'API définie par ces initiatives concerne les modalités de mise en œuvre de l'authentification forte du client (PSU).

MODELES DE MISE EN ŒUVRE DE L'AUTHENTIFICATION FORTE

Contrainte spécifiée dans les RTS de la DSP2 sur l'authentification forte et les normes de communication ouvertes, communes et sécurisées, l'authentification du client a convergé sur trois cinématiques ou parcours clients.



STET

La **STET** est l'opérateur du système de règlement et compensation (CSM) en France et, à ce titre, acteur majeur du traitement des transactions de détail en Europe.

Mandatée par ses actionnaires (La Banque Postale, BNP Paribas, BPCE, le Groupe Crédit Agricole, Crédit Mutuel-CIC, Société Générale, CB Investments), la STET a rendu publique, dès juillet 2017, des spécifications d'API destinées aux établissements se conformant à la DSP2.

Néanmoins, la version finale des RTS, adoptée par la Commission Européenne fin novembre 2017, a remis en cause leur conception, l'article 32.3 des RTS interdisant à l'ASPSP d'imposer aux TPP son interface d'authentification pour identifier leurs clients.

Ce modèle de redirection, systématique dans la version STET initiale, a évolué vers une approche multiple, en 3 modèles, qui permet aux TPP d'avoir la main sur le process d'authentification du PSU. Cette mise à jour (version 1.3) a été publiée le 10 avril 2018[11].

[11] *Depuis, à la demande du régulateur, la spécification STET devra s'enrichir, dans une version prévue en septembre. Principales évolutions : accès à tous les types de virements disponibles en banque à distance (récurrents, multiples, différés), avec leur option d'annulation ; accès des AISP à l'encours d'opérations carte à débit différé ; accès des AISP en lecture seule aux listes de bénéficiaires de confiance, et en écriture seule pour les PISP, avec vérification de la présence d'un bénéficiaire (cette évolution a été transmise pour avis à l'EBA).*

INTERVIEW

Hervé Robache - Responsable Normes et Standards chez STET

La STET a publié en avril 2018 la version 1.3 des spécifications françaises d'API « DSP2 », l'occasion alors d'échanger avec Hervé Robache, Responsable Normes et Standards chez STET, en charge de ce projet.

Galitt : quelles sont les parties prenantes de ce projet d'API standardisées DSP2 ?

Hervé Robache : outre les actionnaires de la STET[12], sont aussi impliqués la Banque de France, la Caisse des dépôts et des consignations, le Crédit Mutuel Arkéa et HSBC France. Les groupes de travail se sont également ouverts à l'Office de Coordination Bancaire et Financière (OCBF) et à des banques luxembourgeoises comme la BNL ou Raiffeisen Luxembourg.
Nous sommes par ailleurs étroitement en contact avec d'autres initiatives de standardisation d'API DSP2 en Europe.

Galitt : quelles sont vos relations avec ces autres initiatives ?

Hervé Robache : des travaux de convergence avec le Berlin Group ont été initiés à la demande de nos actionnaires : les premiers résultats de ces travaux sont intégrés dans la mise à jour de l'API DSP2 de la STET d'avril 2018 et le seront dans une mise à jour à venir côté Berlin Group.

Des contacts ont aussi lieu avec les initiatives de standardisation britannique et polonaise. Dans le cas de UK Open Banking, plusieurs rencontres ont lieu, même si l'initiative britannique reste un cas à part, du fait du Brexit mais aussi d'un périmètre plus large et plus prescriptif que celui de la DSP2.

12 *Voir plus loin § « Standardisation des API » (pour mémoire : La Banque Postale, BNP Paribas, BPCE, Groupe Crédit Agricole, Crédit Mutuel-CIC, Société Générale, CB Investments).*

Concernant l'initiative polonaise, un premier échange a eu lieu au printemps. Il n'y a en revanche encore rien à ce jour avec la Slovaquie et la République Tchèque.

Ces travaux de convergence sont jugés bienvenus par les autorités Européennes, ainsi que par les représentants du commerce et des consommateurs.

Galitt : en résumé, quelles sont les principales mises à jour dans la nouvelle version d'API DSP2 de la STET ?

Hervé Robache : la version finale des RTS adoptée par la Commission Européenne nous a conduit à proposer deux nouvelles cinématiques d'authentification forte du PSU par l'ASPSP, qui coïncident désormais avec celles du Berlin Group. En particulier, la cinématique « intégrée » (Embedded approach) permet au TPP de saisir, dans son environnement utilisateur, l'identifiant du PSU et l'élément d'authentification forte attendu, pour les transmettre à l'ASPSP. Sur ce point, la spécification STET préconise d'éviter le recours à un mot de passe statique afin d'éviter les risques liés au re-jeu possible d'éléments d'authentification.

Autre changement structurant, la gestion des consentements du PSU pour l'accès à ses différents comptes peut désormais être proposée autant par l'ASPSP que par le TPP.

Ont aussi été prises en compte de nombreuses suggestions, émises notamment par des banques, des TPP, des processeurs et les travaux menés avec le groupe de travail SWIFT en charge de la norme ISO 20022.
Y figurent enfin naturellement les acquis des travaux de convergence avec le Berlin Group (cf. ci-dessous).

Galitt : quels sont les premiers acquis de la convergence avec le Berlin Group ? A l'inverse, y a-t-il des éléments plus délicats à faire avancer ?

Hervé Robache : nous menons ensemble deux chantiers de convergence : sécuritaire et technique. Sur la sécurité, un grand pas a été franchi en adoptant,

on l'a vu, les trois mêmes cinématiques d'authentification forte (redirection, découplage, intégration).

Toutefois, les approches diffèrent notablement sur la gestion des droits d'accès - nos spécifications se basent sur le protocole standard OAuth 2.0, tandis que le Berlin Group n'utilise ce même protocole que de façon optionnelle, en complément d'une solution spécifiquement conçue.

D'un point de vue technique, l'écart entre STET et Berlin Group est très variable selon le type de service opéré par le TPP. Pour l'AISP, les structures et formats sont identiques à presque 100 %. Pour le PISP, la divergence est significative : les données en entrée sont plus nombreuses côté STET ; en revanche, le Berlin Group distingue 5 « produits de paiement » (du fait des spécificités des marchés nationaux représentés en son sein). A mi-chemin, on a la confirmation de fonds, pour qui les fonctions définies sont similaires, mais dont la structure de données diverge encore.

On parle ici des noms de balises, des structures de blocs de données échangées (requêtes, restitutions). En effet, nous avions opté pour refléter autant que possible, dans notre formatage JSON, la méthodologie ISO 20022 telle qu'utilisée pour les messages SEPA et certaines divergences persistent à ce niveau avec les spécifications du Berlin Group. Par exemple, dans la spécification STET, le PSU est identifié en tant que débiteur dans le corps de la demande de paiement (équivalent du Debtor présent dans le message ISO 20222 SEPA), alors que cette même information est plutôt localisée en en-tête (header HTTP) dans les spécifications du Berlin Group.

Galitt : quelles sont les prochaines étapes pour la STET avant de voir ses spécifications d'API adoptées par les teneurs de compte ?

Hervé Robache : nous poursuivons les travaux de convergence avec le Berlin Group en vue de publier une API unifiée dès 2019.

En parallèle, l'API STET a aussi été étudiée par l'API Evaluation Group européen. Assistée par 30 experts techniques du secteur, répartis en sous-groupes dédiés à

chaque initiative d'API, cette instance (voir encart 7) propose à l'EBA une méthode pour évaluer la conformité aux RTS d'un jeu d'API DSP2. Pour l'heure, huit premiers critères ont été définis, que les spécifications STET semblent à première vue respecter. Ces recommandations, à destination des régulateurs, en charge notamment des exemptions de solution de secours (fallback), resteront non contraignantes. En France, le régulateur s'appuiera, par ailleurs, sur un forum national de banques et de TPP.

Berlin Group

Depuis 2006, le Berlin Group[13] propose des standards pour les échanges entre systèmes de paiement européens, élaborés par les principaux acteurs monétiques d'Europe (schemes cartes et grands processeurs principalement).

En 2017, il a investi le domaine de l'accès aux comptes DSP2 avec l'initiative NextGenPSD2, définie par 43 acteurs bancaires du paiement, avec un objectif de standard à l'échelle paneuropéenne.

Publiées le 8 février 2018, ses spécifications d'API détaillent l'accès aux comptes (XS2A) par les TPP (PISP, AISP, CBPII) pour les 3 services DSP2 (initiation de paiement, consultation des comptes, validation de disponibilité de fonds), tout en supportant des services additionnels que mettraient en place les ASPSP via cette interface.

L'originalité de l'approche Berlin Group est d'offrir trois options pour authentifier le client (PSU) selon les règles d'authentification forte (SCA) fixées par les RTS. Chaque ASPSP devra indiquer aux TPP le(s) modèle(s) retenu(s) dans la conception des API qu'il mettra à leur disposition :

- Un modèle de redirection, où le TPP redirige le PSU vers le mécanisme de la banque à distance de l'ASPSP pour authentifier le PSU ;

[13] *Dans les spécifications STET de l'API PIS, l'interface de paiement simplifiée propose un seul produit de paiement. Une piste de convergence pourrait être de l'ajouter aux côtés des cinq prévus dans celles du Berlin Group*

- Un modèle découplé, pour lequel l'authentification forte passe par un canal disjoint (application mobile de l'ASPSP, ou appareil tiers[14]), mais toujours maîtrisé par l'ASPSP (c'est donc une variante du modèle par redirection) ;
- Un modèle intégré (« embedded »), où l'authentification du PSU s'initie au travers de l'interface du TPP, qui recueille et transfère, sous sa responsabilité, les identifiants et éléments d'authentification bancaires, et en reçoit la confirmation (réussite/échec).

L'Open Banking UK : un précurseur

Le Royaume-Uni s'est saisi du sujet des Open API il y a déjà plusieurs années. Dès 2015 en effet, le gouvernement britannique a, pour stimuler la concurrence par les nouveaux entrants, mis en évidence un besoin évident de partage de données depuis les banques jusqu'aux Fintechs et à leurs clients communs entreprises.

Anticipant la DSP2, le Département britannique du Trésor a créé en septembre 2015 l'Open Banking Working Group. Ce groupe de travail a regroupé les différents acteurs de l'écosystème (banques, entreprises du secteur, associations de consommateurs, instituts de recherche) et publié l'Open Banking Standard[15], un guide de normalisation pour le formatage, le partage et l'utilisation des données dans l'industrie bancaire.

Dans le sillage de ces travaux, l'Open Banking Implementation Enti-ty (OBIE) est créée en 2016 par l'Autorité des Marchés et de la Concurrence (CMA), qui en prend par ailleurs la direction. L'OBIE, financée par les 9 principales banques du pays[16] a pour objectif de déployer l'Open Banking au Royaume-Uni. En juillet 2017, elle a ainsi publié des spécifications d'API pour fournir un standard sur le contenu minimal des services d'Open Banking britanniques.

[14] *par exemple, un « hardware token » ou générateur de mots de passe à usage unique.*

[15] *Open Banking Standard*

[16] *Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group, Santander.*

3 principales spécifications d'API ont été formalisées par l'OBIE, complétées par des « guidelines » :

- API Open data, avec laquelle un établissement met à disposition de tiers des informations sur ses services et produits, afin que ces derniers développent des applications mobiles et/ou web pour leurs clients s'appuyant sur ces ressources publiées ;
- API Open Banking Read, permettant à un établissement de donner accès aux AISP à l'information des comptes du PSU, ainsi que l'historique de transactions du PSU (sous réserve d'un accord préalable du PSU) ;
- API Open Banking Write, par laquelle un établissement donne la possibilité aux PISP d'initier un paiement pour le compte d'un PSU (sous réserve d'un accord préalable du PSU).

Par ailleurs, l'OBIE encadre le déploiement de ces API par les neufs banques qui s'étaient engagées sur leur mise en service au 13 janvier 2018.

A l'issue d'une période complémentaire[17], puis de 3 mois de tests conclus avec succès, les TPP, autorisés par la Financial Conduct Authority (FCA), offriront à partir de septembre 2018 à leurs clients des services d'agrégation/consultation fondés sur les spécifications développées par l'OBIE.

Les services d'initiation de paiement font, eux, encore l'objet de tests, avec des dates de livraison s'échelonnant entre mars et septembre 2019[18].

Autres initiatives nationales d'API communes

Enfin, à l'instar du Royaume-Uni ou de la France, la Pologne, la Tchéquie et la Slovaquie ont aussi défini des spécifications d'API de place à destination de leurs membres, via leurs associations bancaires respectives : ZBP, CˇBA et SBA.

[17] *Au 13 janvier 2018, 6 de ces 9 banques n'avaient pu tenir leurs engagements : Bank of Ireland, Barclays, HSBC, RBS, Santander, Nationwide. Chacune a négocié un délai de mise en oeuvre, publié au journal officiel par le Trésor.*

[18] *La feuille de route de déploiement des API Open Banking a été revue par l'OBIE en juillet 2018.*

L'API EVALUATION GROUP

L'API Evaluation Group est une instance indépendante d'une vingtaine de représentants des acteurs du marché, réunis depuis janvier 2018, à l'issue des travaux de l'ERPB sur l'initiation de paiement (PIS Working Group).
Y participent des représentants des principales parties prenantes : TPP, ASPSP (avec la Fédération Bancaire Européenne, le Groupement Européen des Caisses d'Epargne, l'Association Européenne des Banques Coopératives) et PSU (EuroCommerce, Ecommerce Europe, Bureau Européen des Unions de Consommateurs), ainsi qu'un représentant de l'E-Money Association (EMA) et un représentant de la Fédération Européennes des Etablissements de Paiement (PIF).

Son objectif est d'établir une liste de critères objectifs de conformité vis-à-vis de la DSP2 et des RTS sur l'authentification forte et les normes de communication ouvertes, communes et sécurisées (voir annexe), et d'étudier chaque initiative d'API à l'aune de ces critères.
Elles feront office de guides, tant pour les organismes développant ces spécifications, et pour les établissements qui les mettront en œuvre, que pour les Autorités Nationales Compétentes (ANC), les régulateurs.

INTERVIEW

Clément Cœurdeuil - Président et co-fondateur de Budget Insight

Pour donner la vision d'un TPP, directement impacté par les interfaces à venir, nous avons fait appel à Clément Coeurdeuil, Président de l'agrégateur Budget Insight, et expert auprès de l'API Evaluation Group, un groupe multi-partite réuni par l'EPC à la demande de la Commission Européenne.

Galitt : peut-on déjà avoir une idée des critères qui serviront pour juger si une API est conforme aux exigences DSP2 des RTS ?

Clément Cœurdeuil : certainement, d'autant que je suis rapporteur sur la dernière version des spécifications d'API de la STET. A l'échelle européenne, l'API

Evaluation Group de la Commission n'a pas encore publié de version finale des critères d'évaluation.

En France, j'ai présenté au CNPS les conclusions de notre travail d'analyse lors d'une réunion avec la Banque de France, où Budget Insight représente les TPP avec Bankin et Linxo. Y sont décrites 9 demandes d'évolution, déclinées ensuite en 14 critères, afin de reprendre les fonctionnalités métiers correspondant aux exigences des RTS. Ces demandes d'évolution sont en cours de débat au sein du Groupe, qui produira ses décisions finales courant 2018.

De notre point de vue, les RTS sont tout à fait clairs sur le fait que les banques teneurs de compte ne doivent ni contrôler le consentement du client (PSU) vérifié par le TPP, ni apporter d'obstacles à l'activité des TPP. Or, dans les spécifications de la STET, élaborées sans concertation avec les TPP, le souci sécuritaire, bien que légitime, semble aussi un prétexte pour faire obstacle à nos connexions. De par la réglementation applicable aux TPP, ces barrières pour des raisons de sécurités sont abusives.

Galitt : quels exemples objectifs pouvez-vous citer ?

Clément Cœurdeuil : pour commencer, selon notre analyse des textes et des usages actuels, les trois options d'authentification forte du client (SCA) ne présentent pas les mêmes niveaux de fluidité / de contrainte sur le parcours client. Le mode « Redirect » est beaucoup plus impactant que le mode « Embedded ». C'est notamment le cas sur le service d'information sur les comptes, avec authentification forte (SCA) tous les 90 jours.

Cela ajoute une contrainte sur une responsabilité - sécuriser la prestation pour le client - que les TPP assument déjà, en direct. En outre, les TPP sont désormais agréés et contrôlés par l'ACPR. Ils appliquent les textes DSP2, et appliqueront demain les RTS, comme les banques !

Autre exemple : la STET ne précise pas les moyens d'accéder à la liste des bénéficiaires que le client a déjà enregistrée sur son espace de banque à distance. Cette limitation oblige donc le TPP à être moins disant par rapport à ce que son client peut faire en direct avec sa banque. Or nous avons lancé le pilote d'un

service de P2P : en partenariat avec la solution de Wallet prépayé de Lydia, nos clients peuvent virer des fonds vers un bénéficiaire enregistré sur un compte que nous agrégeons.
Aujourd'hui, le web scraping nous permet en effet, de récupérer l'IBAN du compte, et le client valide toute la transaction. Demain, cette donnée ne sera pas mise à disposition par une API DSP2 reposant sur la norme STET.

Constatant ces restrictions, le rapport du sous-groupe de travail sur l'API STET inclut donc une version amendée des spécifications STET, conforme aux RTS dans la mesure où elle permet un iso-fonctionnement entre offres TPP et banque à distance.

Galitt : comment, selon vous, fonctionnera la solution de repli (fall-back), prévue par les RTS en cas de défaillance[19] des API d'accès aux comptes ?

Clément Cœurdeuil : je pense que, dans une situation d'urgence, où il s'agit d'assurer la continuité d'activité d'établissements régulés comme le nôtre, il faudra rester pragmatique. L'obligation est que les teneurs de comptes puissent nous identifier : nous leur confirmerons donc les adresses IP de nos robots, de préférence en amont de tout incident.
D'ailleurs, la plupart d'entre eux les connaissent déjà (sinon, ils nous bloqueraient) ! A posteriori, ils vérifieront l'agrément et le rôle (AISP, PISP…). Selon les textes, les TPP ne sont tenus de présenter leur certificat numérique d'agrément que pour le fonctionnement nominal de l'API.

Galitt : comment devraient être évaluées les API avant et pendant les six mois préalables de tests (de mars à septembre 2019, NDLR) ?

19 *Sauf exemption par le régulateur, chaque teneur de compte devra en permanence être en mesure de permettre aux TPP de revenir au web scraping en cas d'urgence, à la condition, pour les TPP, de s'identifier auprès de lui.*

Clément Cœurdeuil : les TPP sont prêts à se connecter aux API pour les tester dès que la documentation sur la connexion et leur utilisation sont publiées par les teneurs de compte, et que leurs environnements de tests sont disponibles !

3

Un tournant stratégique pour le monde bancaire

En France comme ailleurs en Europe, les acteurs bancaires ont investi le champ de l'Open Banking avec des stratégies qui peuvent parfois varier. De la collaboration ouverte au rachat, en passant par la monétisation de services au-delà du minimum réglementaire (consultation, initiation), les relations avec les TPP viennent bouleverser les business models traditionnels des banques.

Parmi ces stratégies, deux semblent se démarquer :

- La première consiste à s'appuyer sur l'écosystème des Fintechs, au travers de rachats et partenariats, pour rapidement proposer des services innovants à ses clients, tout en gardant le contrôle de leur image et de leur relation client ;

- La seconde, d'une dimension plus ambitieuse, vise à embrasser l'Open Banking en donnant l'accès à des tiers, via des API, aux produits et services de l'établissement bancaire.

3.1 Rachats et entrées au capital de Fintechs : une stratégie adoptée par les banques françaises

Comme nous l'avons déjà présenté dans l'encart 2 sur SolarisBank, le groupe BPCE a annoncé en juillet 2016 le rachat de Fidor Bank. Cette action s'inscrit dans le plan stratégique du groupe « Grandir Autrement ».

L'objectif est annoncé : renforcer et accentuer la transformation digitale de la banque.

Fidor Bank, créée en 2009 à Munich, est la première néo-banque entièrement digitale. Comme SolarisBank, elle s'inscrit sur le modèle en rupture où l'Open Banking est mis en avant. Pour Fidor Bank, l'entrée d'un actionnaire important à son capital lui offre les moyens de poursuivre et d'accélérer sa stratégie offensive, résolument tournée vers l'innovation et le client. En effet, cette entité est orientée vers les particuliers, à l'inverse de SolarisBank, qui cible les professionnels.

Fidor Bank s'appuie sur une communauté de plus de 500 000 membres, dont plus de 200 000 sont clients, encouragés à participer à la stratégie de la banque en

contribuant à définir des services supplémentaires ou des changements sur l'offre existante. La communauté, à la façon d'un réseau social, partage ses conseils, y compris lorsqu'ils portent sur les produits de banques concurrentes. Les membres actifs sont d'ailleurs financièrement récompensés.

BPCE compte s'appuyer sur cet actif stratégique pour lancer de nouvelles offres. Alors qu'en Algérie, le groupe mutualiste a annoncé lancer l'application Banxy, néobanque qui reprend le socle technologique de Fidor, un lancement est aussi prévu en France, mais sur un périmètre semble-t-il restreint. En effet, l'offre française ne sera pas, au moins dans un premier temps, sous licence bancaire.

Les banques françaises se sont, ces dernières années, particulièrement intéressées aux startups proposant des services d'agrégation de compte. Au point que ce type de service fait désormais partie intégrante du paysage bancaire français.

Crédit Mutuel Arkéa et Crédit Agricole sont devenus actionnaires de Linxo respectivement depuis 2012 et 2015. Les banques en ligne de ces deux établissements bancaires, Fortunéo et BforBank, ont ainsi passé des partenariats avec Linxo pour permettre à leurs clients de profiter des services de l'agrégateur.

HSBC France, sans entrer au capital de la Fintech française, s'est aussi rapproché de Linxo, en octobre 2016, en concluant un partenariat afin d'offrir à ses clients la technologie et le service de cet agrégateur en marque blanche[20], leur offrant ainsi la possibilité de les aider à mieux gérer leurs finances personnelles.

Autre exemple, le Crédit du Nord, a lancé en octobre 2016 son agrégateur de services baptisé « Synthèse multibanque », en s'appuyant sur la technologie développée par Fiduceo[21]. La filiale de la Société Générale a récemment étoffé son offre depuis février 2018, avec l'agrégation de factures, « Synthèse Multidoc », par intégration d'e-factures. Dès mars 2017, la Société Générale France a elle-même lancé son service d'agrégation de comptes, qui s'appuie aussi sur la technologie de Fiduceo.

[20] *Linxo : communiqué de presse sur le partenariat avec HSBC France*

[21] *Startup rachetée, rappelons-le, par Boursorama, banque du groupe Société Générale.*

Les autres grandes banques françaises ne sont pas en reste : BNP Paribas a ajouté la fonctionnalité d'agrégation de comptes externes en collaborant avec Budget Insight, alors que, du côté du Crédit Agricole, ce service n'est plus l'apanage des clients BforBank, puisque désormais les clients Crédit Agricole en bénéficient via l'application Ma Banque.

3.2 Ouverture des SI bancaire et émergence de l'API economy

L'ouverture du S.I. bancaire permet aux banques d'ajouter à leur cœur applicatif (Core Banking Solution, CBS) des services construits par des partenaires Fintechs ou même banques, via les Interfaces de Programmation Applicatives (API), qui apportent des fonctionnalités de plus en plus riches. Exemple récent de ces banques qui multiplient les API, la DBS Bank de Singapour, qui en revendiquait 155 lors du lancement officiel de sa plateforme d'API, en novembre 2017, grâce à une cinquantaine de collaborations avec des tiers.

En France, plusieurs initiatives se distinguent, concrétisées ou à venir.

Par la singularité de sa démarche, inédite à l'époque, le Crédit Agricole fait figure d'acteur majeur de l'Open Banking en France, et plus généralement de l'open innovation. Son API « Simone » permet, depuis 2012, à des développeurs externes d'enrichir les fonctionnalités de son application bancaire.

Le principe est simple : la banque fournit au travers de cette API un kit de développement logiciel sécurisant l'accès aux données bancaires de ses clients. Allant plus loin dans la démarche, elle a anticipé les risques de vol de données, en assumant l'entière responsabilité juridique en cas de fraude ou de vol.

Cette initiative a été une première mondiale.

La banque a par la suite créé son propre appstore, le « CAstore », afin de permettre aux développeurs, appelés « Les Digiculteurs » de proposer leurs applications aux clients de la banque. Pour en bénéficier, les clients paient un montant forfaitaire selon l'offre à laquelle ils ont souscrit : pass Découverte (utilisation de 1 à 10 applications par mois), ou pass Premium (usage illimité des applications disponibles). Les fonds récoltés sont utilisés pour entretenir la plateforme, la part restante revenant aux développeurs.

La plateforme connait aujourd'hui un franc succès et le Crédit Agricole organise régulièrement des hackathons dans le but de stimuler l'innovation au travers de concours thématiques. Le caractère innovant du dispositif s'est fait remarquer à plusieurs reprises, comme dans le rapport du World Economic Forum d'août 2017 sur la disruption dans les services financiers[22].

LA BANQUE RESPONSABLE DE SON APP STORE ?

22 *World Economic Forum Beyond Fintech : A Pragmatic Assessment Of Disruptive Potential In Financial Services*

Que se passerait-il si l'une des applications était contraire à la loi ? La banque serait-elle responsable d'une application illégale développée par un tiers et éditée via son app store ?
La réponse est donnée par la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 200423, applicable à toutes les communications au public en ligne, y compris les « app stores » fournis par des banques.
La LCEN distingue deux types d'acteurs : l'éditeur de contenu, qui engage automatiquement sa responsabilité ; et l'hébergeur, qui ne peut voir sa responsabilité engagée que s'il n'a pas agi promptement pour retirer tout contenu illicite à compter du moment où ledit caractère lui a été notifié. En application de la LCEN, la banque devrait être considérée comme éditeur des applications disponibles si elle effectue une validation de ces dernières avant mise à disposition au public. Dans le cas contraire, elle devrait être considérée comme simple hébergeur des applications.

Dans une démarche plus orientée Open Banking, BPCE devrait prochainement lancer une place de marché de services financiers basée sur la fourniture d'API. Au-delà des services réglementaires DSP2, la plateforme devrait mettre à disposition des API facilitant l'accès aux produits et services d'entités du Groupe BPCE.

La Société Générale s'apprête à adopter la même approche, le lancement d'une place de marché de même nature étant programmé pour la fin d'année 2018 ou le début d'année 2019.

Ces API additionnelles sont notamment destinées aux néo-banques souhaitant étoffer leur offre de services.

Il s'agit du business model adopté par la néo-banque Starling. La banque mobile britannique, créée en 2014 construit sa « place de marché bancaire » mobile par intégration d'applications tierces. Ses API permettent d'assembler les services existants pour une expérience utilisateur attractive, à un coût et un time-to-market moindres qu'en les développant un à un.

23 *Legifrance : Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*

En plus de la mise à disposition d'un compte courant rémunéré et d'instruments de paiement, l'offre aux particuliers adjoint l'épargne, le cashback et la collecte de points de fidélité commerciaux via le paiement, en passant par la dématérialisation du détails des achats (pour remplacer les reçus papier). En février 2018, Starling Bank s'est connectée à BACS, le CSM britannique de compensation des virements et prélèvements, après avoir déjà adhéré à Faster Payment UK (virements de masse en temps réel) et à Transferwise, qui rivalise avec SWIFT sur les transferts à l'international.

Depuis fin avril 2018 s'ajoute une offre aux entreprises, avec la gratuité pour les TPE (moins de 10 salariés et moins de 2 millions d'euros de CA/an).

Ce type de démarche, visant à mettre à disposition une bibliothèque d'API, est l'opportunité de générer de nouveaux revenus. En effet, si l'usage des API DSP2 doit être gratuit, l'accès à d'autres données ou types de services bancaires par des tiers, via des API, peut être monétisé. Cette nouvelle tendance, désignée sous le terme d'API economy, offre donc des perspectives démultipliées d'augmenter attractivité et rentabilité.
Outre les gains générés par cette monétisation, des API bien pensées peuvent avoir des effets bénéfiques indirects, comme l'amélioration de la notoriété, ou l'enrichissement d'une offre grâce à l'usage et aux apports par des partenaires utilisateurs de l'API.

BBVA, banque espagnole qui compte 10 millions de clients, dont 4 millions sur ses canaux numériques, a été la première grande banque européenne à miser sur cette stratégie. Le 24 mai 2017, elle a lancé sa plateforme « API_Market ».

Cette initiative s'est nourrie d'une année de tests, avec 1500 entreprises et développeurs, destinée à co-construire la politique de sécurité avec, au cœur du dispositif, l'authentification forte du client. Son modèle économique repose sur une rétribution directe par les partenaires utilisateurs des API. Ils ont au préalable la possibilité de les tester gratuitement dans un environnement dédié.

La plateforme API Market[24] met désormais à disposition 10 API pour le marché espagnol, dont quatre également disponibles pour le marché américain et deux pour le marché mexicain. BBVA annonce avoir convaincu plusieurs grands groupes espagnols, ainsi que quelques Fintechs.

INTERVIEW

Clément Coeurdeuil - Président et co-fondateur de Budget Insight

Sur les ambitions innovatrices d'un TPP, nous avons fait appel à Clément Coeurdeuil, Président de l'agrégateur Budget Insight.

Galitt : pour tous les autres types de comptes que de paiement, le web scraping restera non régulé, donc autorisé. Comment ferez-vous ? Si des API bancaires permettent d'y accéder aussi, serez-vous disposés à payer pour ? De même, d'ailleurs, que pour des services « premium », hors DSP2, sur les comptes de paiement ?

Clément Coeurdeuil : le RGPD[25] permet au client (PSU) de disposer à tout moment des données collectées sur lui par ses fournisseurs. En matière bancaire, il peut donc les mettre à disposition de tiers, comme un TPP. Avec son consentement éclairé, celui-ci peut donc web scraper les autres types de comptes de ce client, hors DSP2.

Si l'API du teneur de comptes y donne aussi accès, de manière payante, le prix ne devra pas être discriminant : il devra se situer dans la moyenne des prix pratiqués par tous les ASPSP de l'EEE, à un niveau acceptable, c'est-à-dire en lien avec les coûts d'infrastructure interbancaire et de gestion de compte.

En tant qu'agrégateur de compte, nous y avons d'ailleurs économiquement intérêt. Le web scraping nous coûte, et de plus en plus. Chez Budget Insight,

[24] *BBVA : API Market*

[25] *Règlement Général européen sur la Protection des Données (GDPR en anglais), renforçant les droits des consommateurs sur leurs données personnelles et leur portabilité, en vigueur depuis le 25 mai 2018 (n° UE 2016/679).*

depuis notre fondation en 2014, nous avons constaté que la charge pour intégrer un nouvel établissement bancaire dans notre outil de web scraping est passée de trois à cinq jours par site de banque en ligne. C'est plus encore par application bancaire mobile, mais leur S.I. plus stable s'avère requérir moins de suivi/adaptions chez nous.

Galitt : quelle est votre stratégie d'innovation ?

Clément Coeurdeuil : nous souhaitons porter le paiement au sein des nouveaux usages en forte croissance, de manière intuitive et sans couture. Je pense notamment aux applications de dialogue en temps réel, ou « chat ».
En partenariat avec leur opérateur, type WhatsApp, un algorithme d'intelligence artificielle pourra détecter, dans les conversations, un besoin de paiement entre particuliers. Une offre contextuelle apparaît alors, avec accord de l'utilisateur, pour le mener vers l'opération correspondante, dans l'environnement d'un partenaire. L'initiation d'un virement peut ainsi être suscitée par un échange parlant d'un pot commun, une addition ou facture à se partager…

L'opérateur de l'application de dialogue / réseau social maîtrise son expérience client. A lui d'y déceler des besoins récurrents, et les contextes propices, puis de solliciter un professionnel agréé pour intégrer une offre de paiement, ou bien d'autres services financiers : placement, (micro) financement…

Galitt : rien que dans le domaine de la finance personnelle, le potentiel est immense et le besoin d'API multiple. Comment concilier ces métiers régulés et l'univers spontané des échanges en temps réel ?

Clément Coeurdeuil : la réponse repose en partie sur ce que j'appelle le chaînage des API. Les spécialistes de chaque métier financier identifié exposent leur(s) API, correspondant ou contribuant au besoin identifié. Un module de gestion d'API les interconnecte et les orchestre, selon l'attente du client, pour les combiner au besoin.
Celui-ci ayant donné son accord, le module peut faire communiquer les données connues de chaque API.
Au lieu d'outils dédiés de langage naturel, comme on voit sur nombre de sites institutionnels, où le client doit faire la démarche de se rendre, le but est de brancher des actions financières là où les besoins naissent, là où ils sont formulés.

Galitt : pour les banques teneurs de compte, c'est l'opportunité d'un nouveau et puissant canal de distribution de leurs services financiers ?

Clément Coeurdeuil : oui, en effet ! En Europe d'ailleurs, les grands teneurs de compte sont déjà devenus agrégateurs de comptes (AISP). C'est à un tel point qu'on peut déjà prédire la disparition de la « 2nde banque ». S'appuyer sur ce type de partenariat avec des TPP leur permettra de profiter des marchés naissants et de l'innovation des Fintechs.

3.3 Des données bancaires suscitant les convoi- tises d'acteurs hors écosystème bancaire

Trois typologies d'acteurs tiers s'intéressent également de près aux données bancaires.

Les premiers sont les assureurs, qui voient dans la DSP2 la possibilité de devenir des établissements de paiement et de proposer à leurs clients mutualistes des possibilités d'agréger leurs comptes. En France, la MAIF a lancé son service d'agrégation de comptes bancaires baptisé « Nestor », conçu en marque blanche avec la technologie de Linxo. Sont couverts 140 établissements teneurs de comptes. Une version premium sur abonnement, « Nestor + », permet d'ajouter une anticipation de dépense, appuyée sur l'historique des derniers mois, ainsi que des analyses et synthèses personnalisées.

« Le digital entraîne un abaissement généralisé des barrières à l'entrée. Partant de ce constat, nous sommes défensifs sur notre cœur de métier, mais rien ne nous interdit d'être offensifs sur des métiers qui ne sont pas les nôtres ».
Pascal Demurger, Directeur Général de la MAIF[26].

Les seconds acteurs sont les opérateurs téléphoniques. Pour exemple, le lancement d'Orange Bank fin 2017 marque la volonté de l'opérateur de proposer lui-même des services bancaires à ses clients. Orange est de surcroît entré au capital de Groupama Banque via une prise de participation majoritaire. Objectif : 2 millions de clients à terme.

[26] *L'offre d'agrégation MAIF, article des Echos*

Enfin, les derniers et plus menaçants concernent les GAFA (Google, Apple, Facebook et Amazon). Ces géants du web, au cœur de la gestion des données, et de ce que l'on appelle plus largement le Big Data, affirment leur ambition de bousculer les acteurs bancaires traditionnels du marché. Leur avantage comparatif face aux banques réside dans l'image souvent privilégiée qu'en ont leurs clients, construite sur une expérience utilisateur réputée performante. Leur arrivée sur ce marché des services financiers témoigne de leur volonté d'acquérir tout type de données pour une connaissance client toujours plus poussée.

Les catalogues produits d'Apple et de Google comportent chacun un Wallet de paiement mobile, respectivement disponibles pour tous les détenteurs d'iPhone et de smartphone Android. Apple continue de le déployer, sur une vingtaine de pays désormais, tandis que Google semble désormais faire de Google Pay une priorité, à en juger par la place accordée à ce service lors du dernier évènement annuel Google I/O. L'accent est mis sur le multicanal, et évidemment sur l'expérience client, avant, pendant, et après l'achat.

Apple a, en fin d'année 2017, ajouté un service de paiement Peer to Peer (P2P) directement intégré dans la messagerie iMessage, imitant ainsi Facebook, qui, dès 2015, avait dévoilé Messenger Payments.

Amazon apparaît comme le GAFA le plus actif sur le marché des services financiers : en témoignent la variété de services lancés depuis quelques années. Citons notamment Amazon Cash, offre de dépôt d'espèces permettant d'alimenter son compte en ligne, Amazon Lending, offre de crédit à destination des PME, Amazon Store Card, une carte de crédit privative offrant des facilités de paiement, ou encore Amazon Rewards Visa Signature Card, une carte de crédit émise par Chase, lancée en 2017.

Le poids des GAFA ne doit pas occulter la présence des géants du web chinois sur le marché des services financiers, tel qu'Alibaba. La firme de Jack Ma propose, au travers de sa filiale Ant Financial, le Wallet mobile Alipay, et a lancé dès 2015 une banque en ligne, MYbank.

L'enjeu pour ces acteurs est immense : pouvoir contrôler l'ensemble de la chaine de valeur, et rendre le parcours client plus fluide, mais surtout intensifier leur cœur de métier sur la collecte des données et ainsi pouvoir connaitre plus facilement leurs utilisateurs et leurs habitudes. Ils restent pour l'heure discrets,

mais inutile de souligner que leur force de frappe financière leur permettrait d'absorber aisément les Fintechs tirant le meilleur parti de la DSP2.

Notons que certains acteurs et services de paiement peuvent ne pas être appréhendés par la DSP2. En effet, la DSP2 procède, à l'instar de la DSP1, par listes exhaustives tant pour les catégories de prestataires de services de paiement, que pour la liste des opérations considérées comme des services de paiement. Il suffit alors qu'un nouveau moyen de paiement apparaisse pour ne pas être régulé, n'étant pas catégorisé dans la DSP2. En opérant de tels choix qualitatifs et technologiques, la DSP2 exclurait de son champ d'application de nouvelles activités de paiement qui se retrouvent dans le même vide juridique dans lequel se trouvaient les initiateurs de paiement et agrégateurs de compte.

Pour les banques, le risque à court terme se situe dans une désintermédiation par ces acteurs disruptifs de leur relation client. A plus long terme, une concurrence plus directe pourrait s'installer, permise et facilitée par l'Open Banking.

Opportunités ou menaces, cela dépendra avant tout du positionnement stratégique et des moyens qui y sont alloués en ce moment même. Dans les deux cas, la DSP2 ouvre la voie d'une nouvelle ère bancaire.

DONNEES PERSONNELLES : COMMENT CONCILIER RGPD ET DSP2 ?

La DSP2 et le Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD »), en vigueur depuis le 25 mai 2018, constituent deux réformes majeures de l'année 2018. Il convient alors d'aborder l'application combinée de ces deux textes et de s'interroger sur leur cohérence.

D'une part, la DSP2 prône une ouverture des systèmes d'information bancaires aux agrégateurs de comptes et aux initiateurs de paiements et, d'autre part, le RGPD impose un cadre strict aux entreprises traitant des données à caractère personnel de clients européens.

Les deux textes semblent afficher des philosophies et objectifs antagonistes car la DSP2 considère le partage des données comme essentiel au respect de la concurrence du secteur bancaire, tandis que le RGPD donne au citoyen le contrôle du traitement, de l'utilisation de ses données à caractère personnel pour en assurer

une protection maximale. Pourtant, en approfondissant l'analyse, ces deux textes apparaissent plutôt complémentaires.

Une difficulté de conciliation des deux textes porterait sur la notion de consentement de l'utilisateur.

La DSP2 permet en effet à des tiers, prestataires, distincts du teneur de compte, d'accéder aux comptes bancaires de l'utilisateur et donc ouvre l'accès à ces tiers aux données à caractère personnel qui ont été recueillies. Ainsi l'article 94 (2) de la DSP2 prévoit un consentement explicite de nature contractuelle[27] entre l'utilisateur et le prestataire des services de paiement.

Parallèlement, en application de l'article 6 du RGPD, le traitement des données n'est licite que dans la mesure où au moins une des six conditions proposées est remplie :

1. Consentement de la personne pour une ou plusieurs finalités spécifiques ;
2. Traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
3. Traitement nécessaire au respect d'une obligation légale par le responsable du traitement ;
4. Traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
5. Traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique par le responsable du traitement ;
6. Traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement.

[27] *Article 94 (2) DSP2 : « Les prestataires de services de paiement n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement explicite de l'utilisateur de services de paiement ».*

Interprétés à la lumière du RGPD, les termes traitant du consentement au sein de la DSP2 impliquent qu'en formant un contrat avec un prestataire de service de paiement, les personnes concernées doivent être pleinement conscientes des finalités pour lesquelles leurs données personnelles seront traitées et devront expressément accepter une telle clause. Par conséquent, de telles clauses devront nécessairement être clairement distinguées des autres clauses s'insérant dans le contrat de prestation.

Le concept de consentement explicite prévu par l'article 94 (2) de la DSP2 est par conséquent une condition supplémentaire (de nature contractuelle) qui se distingue du consentement explicite du RGPD.

La DSP2, bien que plus restrictive sur les conditions de traitement des données à caractère personnel, n'entre pas en contradiction avec le RGPD.

Les dispositions issues de la DSP2 prévoyant le recueil du consentement explicite de l'utilisateur comme seule base légale au recueil des données à caractère personnel, sont donc bien plus restrictives, mais pas moins compatibles, avec les cas envisagés par le RGPD.

En effet, en ne prévoyant comme base légale au traitement des données, qu'un seul cas, à savoir celui du consentement, la DSP2 exclut les cinq autres possibilités énumérées par le RGPD. En application de la DSP2, le traitement des données ne peut pas se fonder sur la seule exécution du contrat

Conclusion

Sommes-nous à l'aube d'un open data bancaire ?

La DSP2 s'inscrit dans le mouvement de l'open data bancaire, déjà initié par le service de mobilité bancaire et au travers de la loi du 7 octobre 2016 pour une République numérique. Cette dernière a en effet consacré un droit à la portabilité permettant aux consommateurs de récupérer leurs données auprès de leurs prestataires de services numériques et de les transférer auprès d'autres prestataires. Ce droit a depuis été renforcé par le Règlement Européen de protection générale des données (RGPD), entré en application le 25 mai 2018.

L'essor des services en ligne des banques a logiquement fait du secteur bancaire un terrain d'application pertinent de ce nouveau cadre réglementaire. Depuis le 25 mai 2018, ce droit à la portabilité permet en effet au consommateur, notamment de services bancaires en ligne, de récupérer l'ensemble de ses fichiers ou données de consommation liées à des transactions. A ce titre, les fournisseurs des services en ligne doivent prendre toutes les mesures nécessaires, notamment en termes d'interface de programmation et de transmission des informations nécessaires au changement de prestataire.

Ceci confirme une nouvelle fois l'intérêt des API.

Au travers de ce livre blanc, les API et plus particulièrement les Open API apparaissent comme une réelle alternative au web scraping et un point d'équilibre entre sécurité et innovation. Toutefois, il reste encore un chemin important à parcourir pour parvenir à une standardisation des API et de la structure des données, permettant une interopérabilité entre les services dans l'écosystème européen.

On constate que les banques françaises, après avoir été à l'origine réticentes, ont parfaitement compris l'enjeu et l'opportunité de

développer des projets dans ce domaine. Elles ont aussi été inspirées par certaines banques européennes, comme SolarisBank et Fidor Bank qui ont ouvert la voie vers l'Open Banking en Europe.

Mais jusqu'où ce mouvement ira-t-il ? Jusqu'à une banalisation de la donnée bancaire, jusqu'ici sanctuarisée par une tradition du secret et de la sécurité ? Il est en tous cas vital pour le secteur bancaire de mesurer les évolutions en cours. Au lieu de subir les assauts de nouveaux entrants, souvent plus agiles, il est nécessaire de se positionner au centre du jeu, par une définition équilibrée et responsable des conditions d'accès aux comptes bancaires. Et en créant les conditions d'un nouvel écosystème créateur de valeur

ANNEXE

Les 9 cas d'exemption à la SCA

- En consultation des informations sur les comptes (article 10) :
  - s'il ne s'agit pas d'une première connexion à l'ASPSP via ce TPP, et que moins de 90 jours se sont écoulés depuis la dernière connexion authentifiée ;
  - s'il se limite à des informations qualifiées de « non sensibles » (nom, numéro de compte, historique des transactions sur les 90 derniers jours) ;
- En paiement sans contact de moins de 50 euros et soit en dessous d'un cumul de 150 euros, soit dans la limite de 5 transactions sans contact consécutives depuis la dernière authentification forte (art. 11) ;
- En paiement électronique à distance pour des montants de moins de 30 euros, et soit en dessous d'un cumul de 150 euros, soit dans la limite de 5 transactions électroniques à distance consécutives depuis la dernière authentification forte (art. 16) ;
- Les paiements sur automate dans le transport et les parkings (art. 12) ;
- Les paiements à l'adresse de bénéficiaires de confiance, la création ou l'amendement de cette liste (que le PSU peut mettre à jour sur son espace client) étant elle-même sujette à authentification forte (art. 13) ;
- Les transactions récurrentes, sous réserves que le montant des transactions successives soit identique et qu'elles soient adressées au même bénéficiaire, la première de la série restant soumise à authentification forte (art. 14) ;
- Virements entre comptes d'une même personne physique ou morale, à condition que ces comptes soient détenus par le même ASPSP (art. 15) ;

- Les paiements basés sur des protocoles et processus sécurisés et dédiés à des transactions entre personnes morales, sous réserve que la méthode en question soit jugée par l'autorité nationale compétente comme offrant un niveau de sécurité conforme à la DSP2 (art. 17) ;

- Les paiements électroniques à distance, si la transaction est qualifiée par le PSP comme peu risquée (Transaction Risk Analysis ou TRA). Cette exemption est conditionnée à un taux de fraude du PSP pour ce type de paiement (lié à une carte, ou par virement) inférieur à un niveau de référence des RTS, lequel varie selon le montant selon des seuils de dérogation (Exemption Threshold Value) définis au tableau ci-dessous. De plus, l'analyse de risque menée en temps réel par le PSP doit n'avoir détecté aucun élément inhabituel ou anormal lié au paiement : montant anormal, localisation du payeur inhabituelle ou risquée, similitude avec un scénario de fraude connu, informations inhabituelles concernant le canal utilisé pour le paiement… (art. 18).

Seuil de dérogation	Taux de fraude de référence :	
	Paiements électroniques à distance liés à une carte	Virements électroniques à distance
500 euros	0,01%	0,005%
250 euros	0,06%	0,010%
100 euros	0,13%	0,015%

A propos des auteurs

Thibault Verbiest - *DS Avocats - Avocat associé*

Avocat au barreau de Paris et de Bruxelles, et ancien entrepreneur, Thibault Verbiest dispose d'une expérience approfondie notamment en propriété intellectuelle, et dans le secteur des technologies, des médias et des télécommunications. Il conseille les clients de notre société dans des opérations variées, allant de la dématérialisation des services bancaires et financiers, à la transformation digitale des entreprises, en passant par les fusions & acquisitions dans le domaine technologique. Il assiste également nos clients sur certains dossiers de contentieux, notamment en propriété intellectuelle ou en responsabilité liée à la cyber sécurité.

Frédéric Bellanca - *DS Avocats - Avocat associé*

Avocat au barreau de Paris, Frédéric Bellanca encadre une équipe spécialisée en réglementation bancaire, financière et boursière au profit d'institutions financières, Fintechs et groupes industriels français et étrangers. Il intervient en matière de conseil et de contentieux financiers complexes, tant devant les juridictions de droit commun que l'AMF et l'ACPR.

Diane Richebourg - *DS Avocats (avocate collaboratrice)*

Diane Richebourg est avocate au sein du département Banque Finance du cabinet DS Avocats et intervient sur l'ensemble des problématiques bancaires et financières ainsi qu'en matière de Fintech et crypto-finance.

Emmanuel Caron - *Galitt - Payment Consulting*

Emmanuel est Practice Manager au sein de Galitt Payment Consulting, en charge plus particulièrement des thématiques réglementaire et économique. Depuis 20 ans, Emmanuel travaille sur l'évolution des systèmes de paiement, que ce soit en monétique ou sur les flux paiement (SCT, SDD, Instant Payment). Son parcours l'a conduit à piloter des missions sur la refonte de systèmes monétiques, l'équilibre économique des systèmes de paiement, et sur l'impact du cadre réglementaire européen. Son expertise repose notamment sur une connaissance approfondie des marchés cartes et paiement en Europe.

Guillaume de LONGEAUX - *Galitt - Payment Consulting*

Trilingue, et avec 20 ans dans les paiements de détail, Guillaume a rejoint Galitt en 2017 comme Manager, pour y développer l'expertise en flux et cash management (instant payment, transferts SWIFT et SCT, prélèvements SDD). Il intervient également sur les projets de conformité réglementaire des paiements : dérégulation (DSP2), antiblanchiment, sanctions/embargos. Diplômé de Sciences Po Paris, Guillaume y anime aussi les formations européennes, tant sur les flux que sur la monétique et ses déclinaisons en Europe.

Gwendal BOEDEC - *Galitt - Payment Consulting*

Diplômé de Sciences Po Rennes et de l'Ecole de Guerre Economique (EGE), Gwendal est actuellement Consultant au sein de la Business Unit Payment Consulting de Galitt, travaillant principalement sur des sujets liés aux innovations et à la réglementation dans le secteur du paiement.

Plusieurs collaborateurs de Galitt sont intervenus sur le projet:

Gérard de Moura : *Directeur Général Délégué*

Stéphane Dubois : *Practice Manager*

François Flouriot : *Practice Manager*

Vincent Mesnier : *Directeur Exécutif - Testing Solutions*

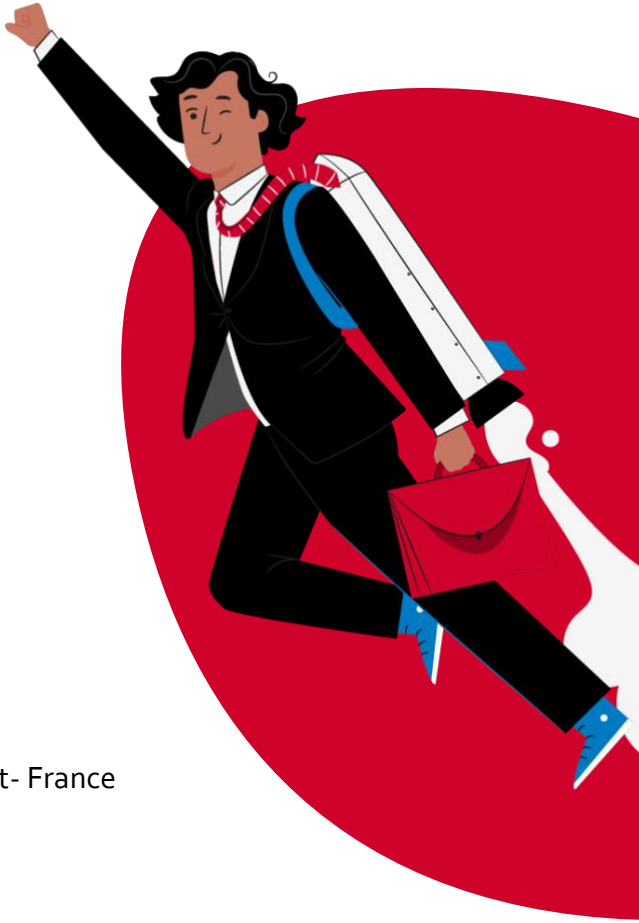
Paul Noel : *Consultant*

Isabelle Pujadas : *Directrice de la communication*

Gérard Tchakgarian : *Président*

Diane Walch : *Business Develo*

Rendre les paiements simples, efficaces et sûrs, dans la vie de tous les jours.



galitt
a Sopra Steria company

17 route de la Reine
92100 Boulogne-Billancourt- France
Tél. : +33 1 77 70 28 00
contact@galitt.com
www.galitt.com