

Note de Synthèse – Le nouveau *Scheme* SPAA



*A l'heure où la première version du Rulebook du nouveau *Scheme* SEPA Payment Account Access (SPAA) vient d'être publiée, il nous paraît essentiel de revenir sur son origine et sur les ambitions qu'il porte, avant de tenter d'éclairer si ce *scheme* répond effectivement aux objectifs cruciaux que sont l'Initiation de paiement et l'Open Banking. Le SPAA leur permettra-t-il de prendre leur essor en balayant les critiques de l'Autorité Bancaire Européenne (ABE) sur les interfaces d'accès aux comptes (API) de la Directive des Services de paiement (DSP2) ?*

D'où vient le SPAA

La révision de la DSP2 avait instauré l'obligation pour les établissements gestionnaires de comptes de mettre à disposition des interfaces d'accès aux comptes de paiement à des prestataires tiers de service de paiement (*Third Party Providers* ou TPP). En effet, la DSP2 prévoyait la possibilité pour les clients des comptes accessibles en ligne d'utiliser les services de paiement proposés par un TPP (initiateur de paiement ou agrégateur), sous réserve que ce dernier ait été agréé auprès de l'autorité nationale compétente.

Ces services de paiement doivent préférentiellement s'articuler sur des interfaces sécurisées dédiées de type API (*Application Programming Interfaces*) où le prestataire tiers doit être authentifié par certificat au lieu et place des techniques plus problématiques de *web-scraping*. Les RTS (*Regulatory Technical Standards*) proposées par l'EBA et ratifiées par la Commission européenne encadrent par ailleurs les mesures de sécurité devant être mises en œuvre. La

conception détaillée et l'implémentation technique de ces interfaces ont concrètement été laissées à l'initiative des acteurs du marché afin de privilégier l'innovation.

Plusieurs APIs ont donc été spécifiées et proposées par différents groupes de travail. Les plus connues sont celles d'Open Banking UK, de STET et du Berlin Group, qui coexistent toutefois avec d'autres, dont des interfaces « propriétaires », développées spécifiquement par certains établissements ou par d'autres communautés (Pologne, Slovaquie, République Tchèque...).

- Du fait des disparités du marché européen et des différences d'appréciation des régulateurs nationaux, le périmètre des API mises en œuvre s'est avéré variable d'un pays à l'autre. Par ailleurs, les différents standards d'API peuvent différer en fonction de choix d'architecture technique ou fonctionnelle. Pour illustrer cela synthétiquement : en France STET a proposé un standard d'application de la DSP2 pour les comptes de paiement, les spécifications publiées décrivant la structure des appels et des réponses du standard API. Outre-Manche, l'OPEN BANKING UK, qui avait commencé avant tous les autres, a convergé vers la DSP2 en proposant à travers l'*OPEN BANKING IMPLEMENTATION ENTITY (OBIE)*¹ un standard d'API ouverte incluant les cartes de crédit prépayées et e-wallets. Du côté de l'Allemagne, le BERLIN Group a établi le *NextGenDSP2* qui encadre le fonctionnement de l'Open Banking DSP2 tout en laissant libre de créer des structures d'API différentes.

En conséquence, malgré tout le travail accompli pour la mise en place de telles interfaces et les tentatives de convergences, les TPP déplorent avec insistance un manque d'harmonisation qui les entrave dans leur activité. Poussé par leur lobbying, l'*Euro Retail Payments Board* (ERPB) avait commencé à se saisir de la question d'un standard d'API en publiant un rapport en juin 2021. Toutefois, peu de clarifications supplémentaires étaient ressorties de cette synthèse.

C'est dans ce contexte, à la croisée des travaux de l'ERPB sur le paiement instantané, un autre chantier européen, qu'a émergé l'idée de confier à l'*European Payment Council* (EPC) la préparation d'un *Scheme Payment SEPA Account Access* (SPAA) à même d'étendre la palette de service des API DSP2 du marché pour poser les premières pierres d'une société ouverte de la donnée financière en proposant un modèle incitatif.

Retour sur les étapes d'élaboration du SPAA

Les principales étapes de l'élaboration du SPAA ont été :

- Octobre 2021 - Réunion de lancement du groupe multipartite SPAA (SPAA MSG) qui est chargé d'élaborer la portée du SPAA, les lignes directrices prioritaires et son plan de développement ; puis deuxième réunion de SPAA MSG sur la clarification des objectifs détaillés du futur régime de SPAA.

¹ OBEI, de nom commercial *Open Banking Limited*. Entreprise créée en 2016 par les 9 plus grandes banques britanniques pour développer un standard commun, il sera prochainement remplacé par un organisme adapté à la nouvelle phase de développement de l'open banking au Royaume Uni, dite de « maturité »

- Novembre 2021 – Finalisation de la phase préparatoire, le Board de l'EPC accepte l'invitation de l'ERPБ de prendre en charge la définition et la gestion d'un nouveau *Scheme* permettant l'accès aux comptes de paiement SEPA (SPAA). Cette définition doit toutefois se limiter à la publication d'un RULEBOOK, le détail d'implémentation des spécifications étant laissé aux différents acteurs du marché (cf. infra).
- Janvier 2022 : Première session d'introduction du SPAA avec un calendrier des actions du SPAA MSG sur une base de réunions mensuelles.
- Février 2022 : Le MSG SPAA décide d'orienter ses travaux sur deux axes :
 - Le chantier SPAA API (SPAA API WB), qui a pour objectif de développer des « exigences minimales d'API » permettant de viser l'harmonisation et l'interopérabilité paneuropéennes
 - Le chantier SPAA Business conditions (SPAA BC WB), telles que définies dans le rapport de juin 2021 du Groupe de travail ERPБ sur un schéma SEPA API Access, dont l'objectif est d'explorer et d'identifier les éléments éligibles à une rémunération et comment les participants au SPAA pourraient les échanger tout en apportant des avantages potentiels pour leurs clients.
- Du 13 juin 2022 au 12 septembre 2022 : Période de consultation publique sur le draft du RULEBOOK.
- 30 novembre 2022 : Publication du RULEBOOK V1.0 validé par l'EPC.

Objectifs du SPAA

Ce nouveau *Scheme* SPAA définit les interactions entre les établissements gestionnaires de comptes (nommés ASPSP selon la terminologie DSP2 mais *Asset Holders* selon la terminologie du SPAA²) et des prestataires tiers (les TPP selon la terminologie DSP2 mais *Asset brokers* selon la terminologie du SPAA). Les interactions des *Assets Brokers* ou des *Assets Holders* avec leurs utilisateurs respectifs (marchands, consommateurs...) ne sont, quant à elles, pas dans le périmètre du *Scheme* SPAA.

L'adhésion des différents acteurs à ce nouveau *Scheme* SPAA reste **optionnelle**.

Le SPAA MSG a rassemblé les besoins identifiés et les a approfondis pour définir :

- Des activités d'Initiation de paiement (*Transaction Assets*),
- Des activités d'information sur les comptes (*Data Assets*),
- Des services à valeur ajoutée pouvant intervenir en complément des précédents.

² Cette différence de terminologie s'explique par la volonté des promoteurs du SPAA d'étendre le champ du schéma au-delà du domaine des paiements

Le SPAA MSG ne s'étant engagé que sur la seule fourniture du RULEBOOK, l'implémentation détaillée est donc laissée aux acteurs du marché, notamment les éditeurs actuels des standards d'API DSP2. Le Berlin Group, au travers de son projet Open-Finance avait d'ores et déjà anticipé ce travail.

Le SPAA MSG définit également les exigences opérationnelles, les modalités de gouvernance et un jeu minimum de fonctionnalités, sous la forme d'un « *Minimum Viable Product* » (MVP), que chaque participant devra mettre en œuvre s'il décide d'adhérer au *Scheme* SPAA.

Parallèlement, comme pour tout *scheme*, il est nécessaire d'établir un cadre pour la juste répartition de la valeur et du risque entre les acteurs. Il est notamment question de permettre une rémunération par les *Assets Brokers* de l'accès et de l'utilisation des services qui seront proposés par les *Assets Holders*. Néanmoins la définition précise de ce cadre de rémunération reste un chantier en cours important.

La volonté d'étendre le Panel de services

Au-delà du socle de service pour les paiements requis par la DSP2, le *Scheme* SPAA décline tout un ensemble de services d'initiation de paiement, s'étendant du simple « *One off payment* » instantané ou planifié, à des modalités plus sophistiquées :

- Paiements à de multiples bénéficiaires
- Paiements programmés sur plusieurs dates
- Paiements à exécution dynamique
- Paiements récurrents
- Paiements récurrents à exécution dynamique
- ...

L'autre nouveauté apportée par le SPAA concerne les services complémentaires à valeur ajoutée. Parmi ces services, celui qui permettra, sous la forme d'un mécanisme (garantie, réservation de fonds...) à l'*Asset Broker* d'avoir l'assurance de l'exécution d'un paiement.

Cette gamme de services constitue autant d'options facturables.

API Berlin Group & API STET vs SPAA

Parallèlement, les travaux entre les groupes de travail de STET et du Berlin Group se sont poursuivis en vue d'atteindre une solution commune.

Où en est-on après plusieurs années de travail ?

Sur le volet agrégation de comptes, les deux standards d'API sont quasiment sur la même ligne avec des structures de données très similaires.

En revanche sur le volet initiation de paiement, l'architecture fonctionnelle des deux standards est très différente pour un périmètre fonctionnel similaire. Par exemple, si STET

privilégie un point d'entrée API unique prenant en charge toutes les modalités d'initiation de paiements, le BERLIN GROUP définit autant de points d'entrée API que de modalités d'initiation de paiement, c'est à dire des APIs dédiées par produit.

D'autres choix opérés par les deux initiatives sont également divergents :

- Mécanisme d'autorisation
- Gestion du consentement détaillé sur les comptes à consulter
- Prise en charge des approches d'authentification forte
- ...

Le SPAA et les responsabilités de chaque acteur

Rappelons d'abord que le SPAA, pour l'initiation de paiement, ne recouvre pas l'exécution du paiement en tant que tel mais uniquement les échanges de messages qui permettent sa préparation. L'exécution du paiement reste sous la responsabilité de l'établissement gestionnaire de compte.

Ensuite, la DSP2 encadre déjà beaucoup de volets liés aux responsabilités.

Enfin, le RGPD, Règlement Général de Protection des Données personnelles régit la gestion du consentement client et le risque de divulgation d'informations sensibles avec la surveillance attentive des acteurs par les différentes autorités compétentes.

Ceci étant posé, le SPAA reprend globalement les principes encadrés par la DSP2 et certaines précisions sont à venir.

- La gestion du risque lié au paiement se situe entre les TPP d'une part et les établissements gestionnaires de comptes, d'autre part. Les API DSP2 permettent leur collaboration par la mise en commun de certaines informations, ce que nous retrouvons dans le *Rulebook* du SPAA.
- L'authentification forte du client (*Strong Customer Authentication* ou SCA), encadrée par la DSP2 dans les relations contractuelles entre les acteurs, est reprise par le SPAA comme étant de la responsabilité des établissements gestionnaires de comptes (*Asset Holders*), les TPP (*Asset Brokers*) pouvant toutefois recevoir cette responsabilité via une délégation soumise à un accord bilatéral. Cela ne va pas plus loin pour le moment, mais une consultation sur ce chapitre SCA est actuellement organisée par l'EPC.
- Concernant le risque de fraude, les API DSP2 permettent la collaboration des acteurs par la mise en commun de certaines informations, ce que nous retrouvons dans le *Rulebook* du SPAA. Ce dernier indique aussi que la responsabilité des contrôles anti-fraude est partagée entre *Asset Holders* et *Asset Brokers*. Un dispositif de demande d'annulation du paiement est prévu (*Cancellation Request from Asset Broker to Asset Holder*) afin de permettre au TPP de réagir en cas de détection de fraude de son côté.

Cependant, en présence de multiples acteurs, si le montant s'avère débité à l'issue d'une fraude, les litiges potentiels peuvent être complexes : qui rembourse (ou pas) le consommateur lésé par la fraude ? La consultation à venir devrait introduire en partie ce sujet sensible en lien avec la révision de la DSP2 (future DSP 3).

Le SPAA et la Directive des Services de Paiement

Dans la longue note de l'EBA du 23 juin 2022 - *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market* - sur les modifications souhaitées dans le cadre de la révision de la DSP2, deux propositions pourraient impacter le *Rulebook* du SPAA :

- La volonté de soumettre les *Schemes* à un contrôle de supervision pour s'assurer qu'ils reposent bien sur des systèmes suffisamment sécurisés ;
- La proposition d'imposer à travers la future DSP3 un standard d'API :
 - DSP2 (Basic) & *Premium* qui émane des acteurs financiers : ces deux composantes de l'API sont justement compatibles avec (i) le contenu du *Rulebook* et (ii) le fait que le standard émane bien des acteurs financiers, représentés par l'EPC ;
 - Une meilleure ligne de démarcation entre les fonctionnalités attendues de l'API *Basic* et ce qui pourrait être dans l'API *Premium*, étant précisé que l'éventuelle ouverture de la DSP3 au-delà des « comptes de paiement »³ impactera nécessairement la ligne de démarcation actuelle du *Rulebook* ;
 - Le *Rulebook* devra suivre des exigences (*guidance*) dictées par l'EBA/Autorités de supervision, notamment afin que (i) la supervision en soit facilitée (ii) le coût d'accessibilité des API DSP2 soit moindre pour les TPP ; sur cette proposition, le *Rulebook* du SPAA *Scheme* serait donc potentiellement impacté par une position de l'EBA sur certains de ses aspects, sans qu'on puisse savoir à ce stade quel type de position pourrait être adopté et imposer une V2 au projet de *Rulebook* ;
 - L'adhésion à ce standard européen deviendrait donc obligatoire pour les acteurs financiers concernés, étant précisé qu'aujourd'hui les participants ne sont pas tous agréés en tant que PSP (ce qui explique d'ailleurs pourquoi l'EPC a pu choisir les expressions d'*Asset Broker* et *Asset Holder*, puisqu'elles peuvent impliquer des personnes qui ne sont pas respectivement des TPP et des ASPSP) ;

³ Une des recommandations de l'ABE est d'étendre l'Open Banking à l'Open Finance

- Il est bien reconnu que l'API *Premium* ne serait pas gratuite, ce qui est également compatible avec le projet de *Rulebook* SPAA dont l'EPC indique qu'elle publiera en 2023 les « *Business Conditions* » ;
- La question du RGPD est certainement sous-évaluée dans le *Rulebook* ; l'EBA entend que l'initiative commune d'API standardisée soit claire sur la responsabilité des acteurs lorsqu'ils échangent des données personnelles ;
- L'EBA considère que l'émergence d'une API unique (standard) participerait à l'émergence de l'Open Finance.

Par ailleurs, le *Rulebook* renvoie à certains principes de la DSP2, ce compris le sujet de l'authentification forte et ses dispenses des RTS. Si les points visés évoluent à la faveur de la DSP3, le *Rulebook* devra également faire évoluer ses références aux textes et leurs principes. Par exemple, si la DSP3 consacre l'ouverture à l'Open Finance, le *Rulebook* devra faire évoluer ses participants au-delà du cercle des PSP (ou de ceux qui peuvent aujourd'hui l'être sans agrément). Sur ce point toutefois, l'EBA semble indiquer que l'Open Finance pourrait intervenir à la faveur d'un texte autonome (avec naturellement un impact sur la DSP2/3).

Enfin, une lecture rapide du rapport de l'ERP de 2021 à l'origine de l'initiative de l'EPC tend à conclure qu'à la parution de son avis sur la DSP3 (juin 2022), l'EBA était consciente de l'évolution attendue de l'EPC même si ce n'est pas explicite ; le *Rulebook* semble ainsi s'inscrire dans le sens de l'évolution attendue par la DSP3.

Conclusion

Le *Scheme* SPAA s'appuie sur les investissements réalisés dans le cadre de la DSP2. Il est conforme à la législation de l'Union européenne (UE), soutenu par les institutions européennes concernées et développé en collaboration avec l'ensemble des acteurs du marché.

Ce *Scheme* SPAA pourrait par ailleurs amorcer la transition du marché européen vers une « société des données ouvertes », bien au-delà des paiements. Si sa mise en œuvre est bien menée, elle constituera une opportunité en termes d'innovations autour d'expériences client inédites et en termes de nouvelles sources de revenus pour les acteurs du marché.

Les solutions actuelles du marché vont s'adapter au SPAA et probablement peu se préoccuper de convergence, l'usage et le marché ayant consacré jusqu'à présent une coexistence plutôt qu'une trajectoire de convergence complète.

Côté gestion du risque lié au paiement, la consultation à venir devrait préciser les choses, toutefois il faudra du temps aux différents acteurs pour collaborer suffisamment étroitement sur ce sujet.

Nous suivrons attentivement les prochains jalons du SPAA MSG :

- Du 16 décembre 2022 au 15 mars 2023 : Période de consultation publique sur *l'usage de la SCA (Strong Customer Authentication)*. Le résultat sera intégré à une version révisée du premier *rulebook SPAA*
- 30 Novembre 2023 : date d'application du SPAA RULEBOOK V1.0 révisé
- Q2 2023 *SPAA scheme default business conditions publication - Revised version of the first scheme rulebook publication & Second version of the API Security Framework (covering SPAA scheme related specifications) publication*

*

* *

« Avis de France Payments Forum – Groupe de travail RED⁴ »

Le SPAA tient compte des critiques de l'EBA pour permettre aux 2 objectifs de la DSP2, l'Initiation de paiement et l'Open Banking, de prendre leur essor. Toutefois, le *scheme* pourrait être amené à évoluer à la faveur de la future DSP3.

Le *scheme* lève les limitations des APIs DPS2 à la fois du périmètre des API (par exemple extension du périmètre initial des comptes de paiement aux autres types de comptes, par exemple les comptes épargne) et de l'absence d'un mécanisme de rémunération des acteurs pour permettre une meilleure adoption et constituer une incitation à investir.

Mais le *scheme* SPAA n'éclaire pas toutes les questions techniques liées au déploiement et à l'utilisation des API DSP2.

Côté mise en œuvre donc, on ne peut s'empêcher de souligner qu'une année semble bien court pour l'application du SPAA par tous les acteurs ; la gouvernance de l'ERBP, la mobilisation de tous les acteurs et des instances de chaque pays seront essentielles pour surmonter les difficultés avant d'aboutir à l'harmonisation attendue. Le *scheme* n'étant pas obligatoire, on peut penser que seule la perspective de générer des revenus peut motiver les *Assets Holders* et les *Assets Brokers*.

En synthèse, tous les écosystèmes nationaux sont embarqués dans la stratégie européenne des paiements de détail. Les rôles sont taillés pour chaque acteur mais les scripts ne sont pas écrits en détail, et chacun cherche comment tirer son épingle du jeu.

Lorsque l'on considère l'entièreté du scénario, on s'aperçoit que les grands gagnants du nouveau *Scheme* SPAA pourraient être les marchands/commerçants pour qui le paiement initié selon les APIs représenterait une alternative intéressante aux solutions de paiement par carte des *schemes* internationaux. Pour leur part, les *Asset Brokers*, en jeunes premiers du système pourraient espérer, par la mise à disposition de solutions intégrées et performantes, des sources de revenus. Les banques, en qualité d'*Asset Holders*, pourraient quant à elles envisager, au moins en partie, la rentabilisation de leurs investissements effectués sur la DSP2 et sur le *Scheme* SPAA, par la facturation de ces nouveaux services.

Et le consommateur dans tout cela ? Son parcours client devrait être plus attractif, mais ce qui présentera réellement un atout clé, et constituera une incitation concrète pour le client à payer selon le *Scheme* d'initiation SPAA n'est pas encore flagrant et devra être notamment parfaitement articulé avec le virement instantané. Un *scheme* ne peut être réellement performant que s'il couvre au-delà des règles opérationnelles, les questions liées au modèle économique (ce qui sera le cas ici), aux risques, à la conformité, et s'il inclut une stratégie marketing. **Par conséquent, il reste encore du chemin à faire pour parvenir à l'aboutissement du SPAA.**

⁴ GT RED (Règles, Évolutions, Déploiements) : concerne essentiellement les flux de paiement