Directive européenne sur les services de paiement (DSP2)

HSBC

Nourrir vos ambitions

Adoptée en 2007 et mise en œuvre en 2009, la directive sur les services de paiement (DSP1) visait à créer un marché unique des paiements dans l'Union européenne et à établir les bases de l'espace unique de paiements en euros (SEPA). Son principal objectif était de rendre les paiements transfrontaliers aussi faciles, peu coûteux et sûrs que les paiements nationaux.

Au fur et à mesure que l'économie numérique se développait, de nouveaux services ont commencé à apparaître – des services qui dépassaient la portée de DSP1.

Pour répondre à ces avancées technologiques une nouvelle Directive a été rédigée : la DSP2. Des premiers éléments sont entrés en application en janvier 2018.

Le 14 septembre 2019, la deuxième vague des dispositions de la DSP2 entrera en vigueur dans l'ensemble de l'Espace Economique Européen (« EEE »).

Elle vise à :

- Permettre à des prestataires (PISP et AISP) d'offrir de nouveaux services d'agrégation d'information sur les comptes et d'initiation de paiement en assurant la protection des données financières des clients concernés.
- Renforcer le niveau de sécurité de vos paiements et assurer une meilleure protection de vos données. C'est le concept de l'authentification forte qui sera plus fréquent

Qu'est ce qu'un AISP ?

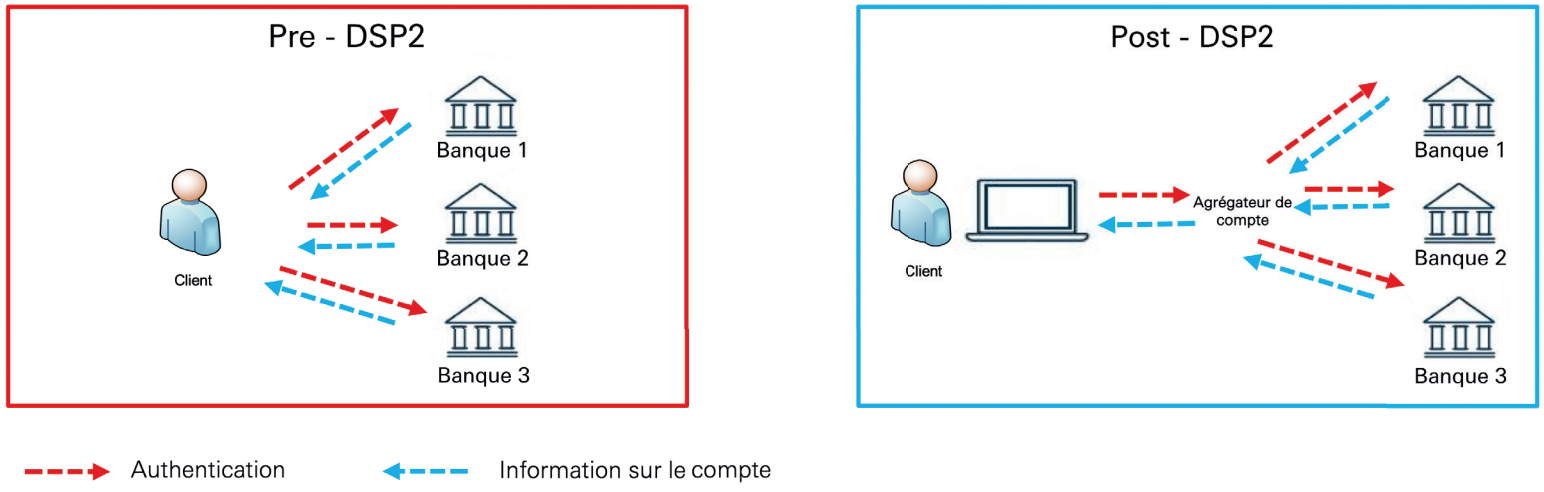
Un agrégateur ou AISP (Account Information Service Provider) offre à un client un portail unique consolidant les informations sur les comptes qu'il possède dans différentes banques et affiche le solde et le détail des opérations liées à ces comptes. Ce service nécessite le consentement du client pour chacun des comptes intégrés dans le service d'agrégation.

L'agrégation se limite aux seuls comptes de paiements tenus dans les différentes banques de l'EEE.

Dans le cadre de la DSP2, un AISP doit :

- Etre enregistré auprès de son régulateur local et être déclaré par ce dernier dans chaque pays européen où il désire opérer.
- Fournir des services uniquement sur **consentement explicite du client**.
- S'identifier auprès de l'établissement bancaire, gestionnaire du compte du client (ASPSP) et communiquer de façon sécurisée avec l'ASPSP et le client.
- Ne pas utiliser ou stocker des données à des fins autres que la réalisation du service d'information explicitement demandé par le client, conformément aux règles de protection des données.

Schéma AISP



Qu'est ce qu'un PISP ?

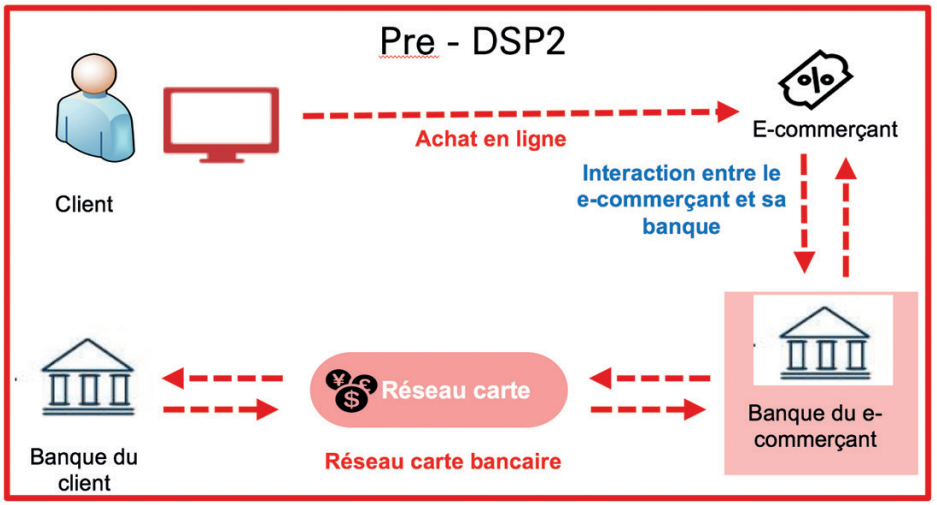
Un initiateur de paiement ou PISP (Payment Initiation Services Provider) est un prestataire fournissant à ses clients un service d'initiation de paiement (virement).

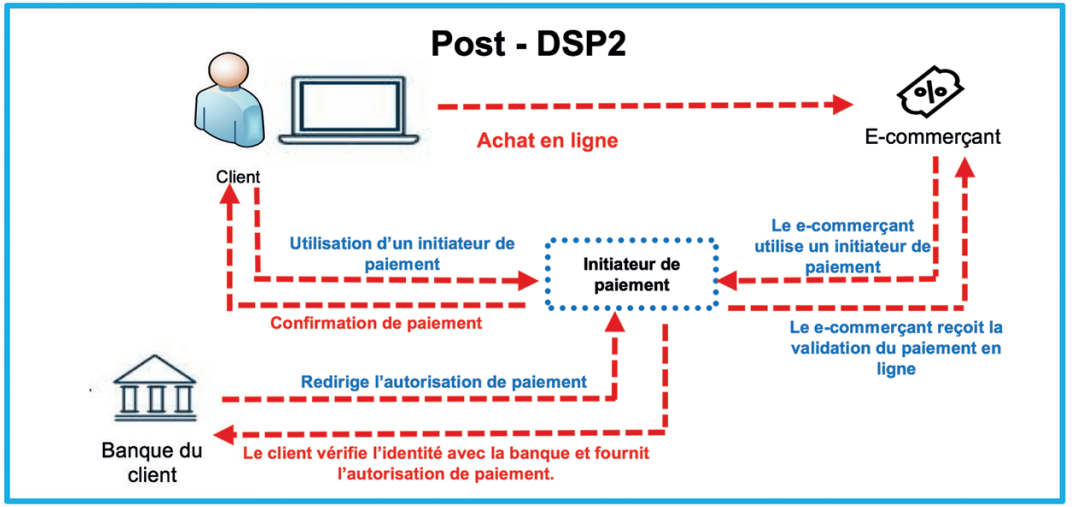
À NOTER
L'établissement bancaire reste responsable de l'exécution de l'ordre de paiement.

Dans le cadre de la DSP2, un PISP doit :

- Etre agréé dans son pays / territoire d'origine et obtenir un agrément de chaque pays européen où il désire opérer.
- Ne pas détenir les fonds du payeur mais seulement initier les paiements dans le cadre de la disposition du service d'initiation de paiement.
- S'assurer que toute autre information sur le client est seulement fournie au bénéficiaire et seulement avec le **consentement explicite du client**.
- S'assurer que chaque fois qu'un paiement est initié, les communications entre toutes les parties sont menées d'une manière sûre.
- Ne pas demander au client toute donnée autre que celles qui sont nécessaires pour fournir le service d'initiation de paiement.
- Ne pas utiliser ou stocker des données à des fins autres que la mise à disposition de l'initiation du paiement telle que demandé explicitement par le payeur.
- Ne pas modifier le montant, le bénéficiaire ou toute autre caractéristique de l'ordre de paiement.

Schéma PISP





Qu'est ce que l'authentification forte ?

L'authentification forte ou Strong Customer Authentification (SCA) qui sera généralisée le 14 septembre 2019 a pour objectif de réduire les cas de fraude et de renforcer la sécurité en introduisant l'authentification à deux facteurs pour l'accès à la banque en ligne ou lors des paiements électroniques.

L'authentification forte implique l'usage de « deux éléments ou plus appartenant aux catégories » suivantes :

Connaissance	Possession	Inhérence
Une information que seul l'utilisateur (et le PSP teneur de compte) connait Exemples : code confidentiel, mot de passe ou information personnelle avec longueur et complexité adéquate	Un objet que seul l'utilisateur possède, qui peut être reconnu sans risque d'erreur par le PSP teneur de compte et difficile à copier/contrefaire Exemples : smartphone, carte bancaire, montre ou objet connecté	Une caractéristique propre à l'utilisateur (empreinte biométrique) Exemples : empreinte digitale, reconnaissance faciale, biométrique comportementale

Quand l'authentification forte est-elle requise ?

- Lors de l'accès à la banque en ligne la première fois puis tous les 90 jours à compter de la dernière authentification forte (même pour une simple consultation). Elle nécessite l'utilisation soit du boitier « Secure Key » soit de la « Secure Key » mobile.
- Lors d'un achat en ligne avec une carte de paiement, elle sera requise plus souvent pour finaliser la transaction en toute sécurité
- Lors de paiements sans contact, la saisie du code confidentiel de la carte pourra être plus fréquente (selon les usages du porteur de la carte)

Rappel sur l’authentification forte sur la banque en ligne avec le boitier Secure Key

Rappel sur l'authentification forte sur la banque en ligne avec la Secure Key Mobile (1/2)

Rappel sur l'authentification forte sur la banque en ligne avec la Secure Key Mobile (2/2)

Lexique

Acronyme	Description
AISP	Account Information Service Provider ou **Prestataire de Services d'information sur les comptes**
API	Application Programming Interface est **une interface d'échange de données.** Les API sont mises à disposition sur une plateforme d'API management qui permet la gestion du cycle de vie de l'API, le contrôle des accès des applications qui consomment les API et le suivi de leur utilisation
ASPSP	Account servicing payment services providers ou **Prestataire de services de paiement gestionnaire de compte**
DSP	Directive sur les Services de Paiement
EBA	European Banking Authority ou **Autorité Bancaire Européenne**
ECB	European Central bank ou **Banque Centrale Européenne**
PISP	Payment Initiation Service Provider ou **Prestataire de Services d'Initiation de Paiement**
PSD	Payment Services Directive
PSP	Payment service provider ou **Prestataire de service de paiement** (e.g. HSBC)
PSU	Payment service users ou **Utilisateur d'un service de paiement**
RTS	Regulatory Technical Standards ou **Normes de Règlementation Technique**
TPP	Third party payment provider (Payment initiation services and/or Account information services)

HSBC Continental Europe
Société Anonyme au capital de 491 155 980 euros - SIREN 775 670 284 RCS PARIS
Siège Social : 38 Avenue Kléber - 75116 Paris. Banque et intermédiaire en assurance immatriculé auprès de l'ORIAS
(Organisme pour le Registre des Intermédiaires en Assurance - www.orias.fr) sous le n° 07 005 894 - 12/2020