WAVESTONE

SÉCURITÉ DES OPÉRATIONS FINANCIÈRES EN LIGNE EN 2020 :

QUELS SONT LES APPORTS DE LA DSP2 ?

Dans un monde toujours plus connecté, les opérations financières en ligne, de la consultation aux paiements, sont en constante augmentation : plus d'1,5 milliards de personnes ont réalisé un paiement sur internet dans le monde en 2017 et plus de 2 milliards sont attendues en 2019. En France, le paiement mobile concerne plus de 6 personnes sur 10 pour un usage régulier.

Cet engouement invite les acteurs historiques et de nouvelles fintechs à se positionner sur le marché des services bancaires en ligne. De nombreuses solutions se déploient aujourd'hui à grande échelle, nécessitant une réglementation adaptée.

CONTACT

Michel GIRIER
michel.girier@wavestone.com

LA DSP2 ET LES ACTEURS FINANCIERS

La DSP2, Directive sur les services de paiements 2, s'inscrit dans l'évolution des transactions électroniques. Elle est une nouvelle étape dans la normalisation des échanges financiers après la DSP1 et en parallèle des travaux OpenBanking au Royaume-Uni.

Avec l'évolution du nombre d'acteurs sur le marché, les solutions mises en œuvre pour l'authentification des utilisateurs et la sécurisation des opérations financières se mul-

tiplient. Ces solutions peuvent s'appuyer sur des moyens d'échange reconnus comme sécurisés (EBICS, Swift…) mais elles ne sont pas les plus aptes à répondre à un besoin de plus en plus important d'accès aux données en temps réel.

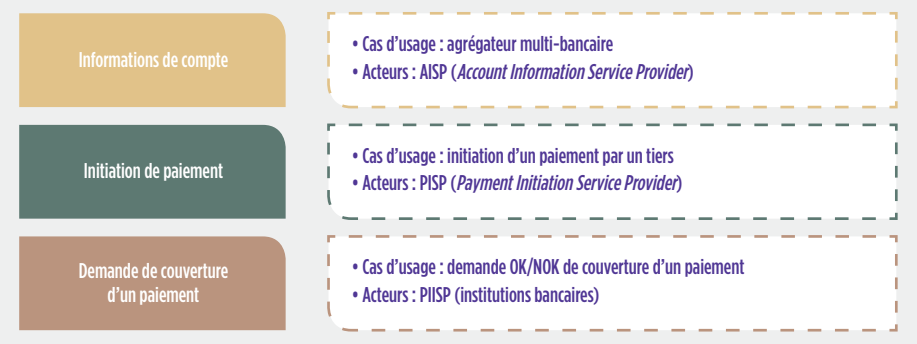
Le but de cette directive est d'apporter un cadre réglementaire aux banques et aux acteurs non-bancaires tout en favorisant la concurrence.

Pour cela, la directive circonscrit les prestations réalisées par les acteurs des services de paiements en trois services :

- Le Service d'Information sur les Comptes (*Account Information Service* ou AIS) consiste en l'affichage et l'agrégation des données de solde et des transactions des comptes de paiement.
- L'Initiation de Paiement (*Payment Initiation Service* ou PIS) consiste en la transmission d'un ordre de paiement pour le compte d'un payeur, à son établissement teneur de compte.
- L'Émission d'Instruments de Paiement (*Payment Issuer Instrument Service* ou PIIS) met à la disposition des utilisateurs des moyens de paiement.

Elle impose aux fournisseurs (*Provider*) de ces services un ensemble de règles et d'obligations à remplir. À la condition que ces règles soient appliquées, les AISP, PISP et PIISP auront la possibilité d'accéder gratuitement aux données sur les comptes de paiement de l'utilisateur dans leur établissement teneur de comptes (*Account Servicing Payment Service Provider* ou ASPSP).

Les services du périmètre de la DSP2



L'APPORT SÉCURITAIRE DE LA DSP2

Pour offrir la possibilité d'accéder aux données des établissements teneur de compte (les banques), la directive impose à ces dernières d'exposer de nouvelles interfaces répondant à un ensemble de mesures de sécurité et permettant la réalisation de ces services.

Sous l'impulsion de plusieurs groupes de travail (en particulier le STET et le Berlin Group), la solution retenue est la construction d'API exposant les services des ASPSP, à l'aide des standards Open API adoptés par les géants du Web. En particulier, d'un point de vue sécurité, les standards retenus sont OAuth2 et OpenID Connect.

Identification et authentification des acteurs

En réponse au fonctionnement actuel des agrégateurs, une des mesures d'importance de la directive est l'obligation pour les acteurs bancaires de s'identifier et de s'authentifier entre eux pour réaliser toute opération liée aux comptes de paiement.

En effet, en l'absence d'interface adéquate, les agrégateurs fonctionnent actuellement par *web scraping* qui consiste à simuler la navigation d'un utilisateur sur sa banque en ligne, en rejouant ses secrets de connexion. Cette méthode comporte trois défauts principaux :

- l'agrégateur client n'est pas formellement identifié, empêchant l'établissement teneur de comptes de déterminer s'il s'agit d'un acteur légitime ou non,
- les secrets de connexion de l'utilisateur sont transmis et connus par un acteur tiers et ne sont pas gardés confidentiels par l'utilisateur,
- la traçabilité des opérations n'est pas assurée car il est impossible d'établir la preuve d'origine d'une requête. Plus particulièrement, la granularité d'accès aux services utilisés et informations consultées par un acteur tiers n'est pas possible.

La directive (articles 66 et 67) oblige donc tous les acteurs, notamment AISP et PISP à s'identifier et s'authentifier pour consommer les services. Un consensus s'est établi autour de la réalisation d'une authentification mutuelle par certificat lors de l'établissement de toutes les communications entre un fournisseur de service (TPP) et un établissement teneur de compte (ASPSP).

Renforcement de l'authentification de l'utilisateur

Elément récurrent dans la directive et au cœur de l'un des *Regulatory Technical Standards* définis par l'ABE (Autorité bancaire Européenne), l'authentification renforcée des utilisateurs est une des mesures structurantes de cette directive.

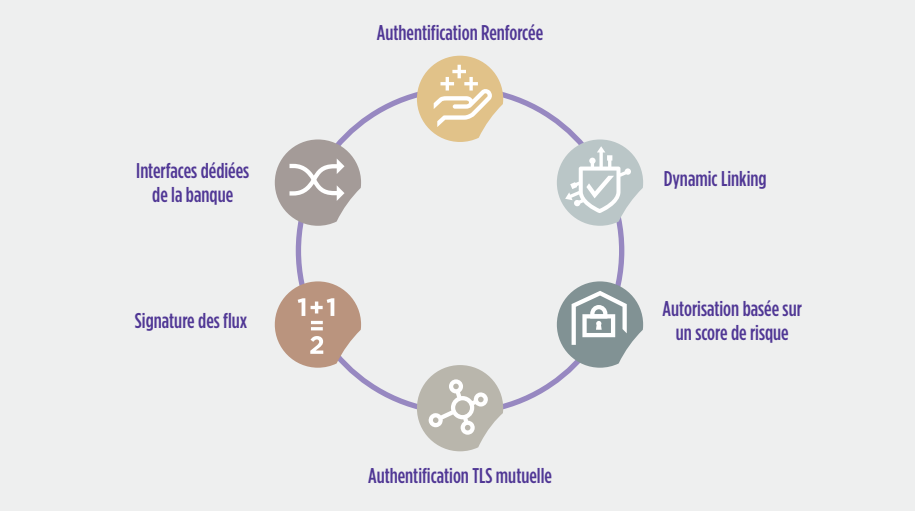
Aujourd'hui, les solutions s'appuient principalement sur l'utilisation d'un mot de passe (rejouable et sujet au phishing) et sur l'OTP SMS (présentant des risques d'interception) pour l'authentification renforcée. Ces deux méthodes sont très répandues mais présentent des failles de sécurité et sont parfois coûteuses. Les nouveaux services de paiement mobile permettent aussi une identification par l'adresse e-mail ou par le numéro de mobile, non connu de la banque.

Les RTS visent à sécuriser cette authentification de l'utilisateur par la définition d'une authentification renforcée (« Strong Customer Authentication » ou SCA) comme une authentification à deux facteurs indépendants, c'est-à-dire que la compromission de l'un n'entraîne pas la compromission du second. La directive impose que l'établissement teneur de compte fournisse les moyens de réaliser cette authentification renforcée, et que chacun des deux facteurs soit sécurisé sur toute la chaîne de transmission.

Les solutions envisagées pour répondre à ce besoin sont de plusieurs natures :

- Le mot de passe reste un facteur principal aujourd'hui, à condition d'être accompagné d'un second facteur pour l'authentification renforcée.
- Les solutions matérielles, plus sures, présentent l'inconvénient d'un coût supplémentaire : token d'authentification physique, clé ou dispositif FIDO U2F…

Exigences sécuritaires de la DSP2



/ Les solutions logicielles sur smartphone sont en développement constant : notification in-app, token d'authentification logicielle, biométrie à l'aide des capteurs du device, MobileConnect…

Le lien dynamique, *dynamic linking*

Dans le cas particulier des transactions de paiement, la directive impose qu'un code unique soit généré pour permettre aux acteurs de la transaction d'être, à tout moment du processus d'authentification et d'autorisation, en mesure de retrouver les caractéristiques de la transaction. En particulier, l'utilisateur doit être conscient, durant la totalité du processus, du montant et du bénéficiaire de la transaction qu'il autorise.

Cette mesure est similaire à ce qui est déjà réalisé dans certains cas de paiement en ligne. L'utilisateur est en effet notifié par SMS avec le code OTP correspondant à une transaction unique, de son montant et de l'origine de la demande. Elle généralise donc cet usage et l'impose en condition pour toute transaction de paiement.

Les exemptions à l'authentification forte

Dans la définition du besoin d'authentification forte et les exigences sur la *Strong Customer Authentication*, la DSP2 essaie également de maintenir un équilibre avec l'ergonomie de la navigation pour les utilisateurs des services. Pour cela, elle prévoit des cas où les fournisseurs de services de paiement peuvent choisir d'exempter leurs utilisateurs de la réalisation d'une authentification forte.

Les conditions en place pour réaliser ces exemptions sont précisément décrites dans les RTS, notamment suivant les modes de paiement de l'utilisateur. Il est ensuite de la responsabilité des fournisseurs de service de paiement de déterminer, à l'aide d'un score de risque, si une exemption doit être appliquée ou non.

LES LIMITES DE LA DSP2

La DSP2 est un nouveau jalon dans le renforcement de la sécurité sur les services de paiement. Elle apporte des mesures adaptées aux besoins et à la multiplication des acteurs numériques. Dans l'état cependant, elle comporte des limitations qui réduisent la portée des mécanismes de sécurité.

La limitation du périmètre aux seuls comptes de paiement

La DSP2, en tant que directive sur les services de paiement régit les opérations en ligne des acteurs de ces services uniquement sur les périmètres concernés qui sont les comptes intervenant dans les opérations de paiements.

Dans les faits cependant, les acteurs, et en particulier les agrégateurs, réalisent aujourd'hui des opérations sur l'ensemble des comptes des utilisateurs, notamment leurs comptes d'épargne. Un des enjeux de ces agrégateurs étant de fournir des services à valeur ajoutée touchant à l'ensemble de l'activité de l'utilisateur sur ses comptes : comptes courants, comptes d'épargnes, chèque, cartes, crédits, plan en actions,…

En réglementant uniquement sur l'accès aux comptes de paiement, la commission européenne et l'ABE mettent en lumière le fonctionnement des agrégateurs (rejeu des secrets de connexion utilisateurs) sans fournir une solution à l'ensemble des problématiques des échanges entre ces acteurs non bancaires (agrégateurs) et les banques.

Dans l'intérêt du développement des agrégateurs, des solutions devront donc être actées pour élargir cette législation. Par ailleurs, les travaux engagés par les banques dans le cadre de la DSP2 les ayant amenées à construire l'architecture nécessaire à l'exposition de services sur internet, une évolution de ces services à plus des comptes et à plus de services utilisateurs est probablement à venir.

Incompatibilité avec les standards existants

Contrairement à l'initiative OpenBanking UK, basé sur le standard reconnu du groupe de travail Financial API, au sein de la fondation OpenID, les nouveaux services offerts par les banques dans le cadre de la DSP2 se fondent sur des exigences réglementaires plutôt que sur des standards de sécurité établis.

Consentement utilisateur

Le consentement utilisateur est un bon exemple de cet éloignement entre le standard, ici OpenID Connect, et la réglementation.

La directive implique que le consentement de l'utilisateur à l'utilisation d'un ou plusieurs comptes pour un agrégateur :

/ doit être recueilli par le TPP (donc l'application qui va consommer les API),

/ doit être appliqué et vérifié par l'ASPSP (hébergeant les API).

Ceci est réalisé à rebours du standard OpenID Connect (implémenté dans le cadre de OpenBanking UK), dans lequel le consentement doit être recueilli par le service hébergeant les données et les API.

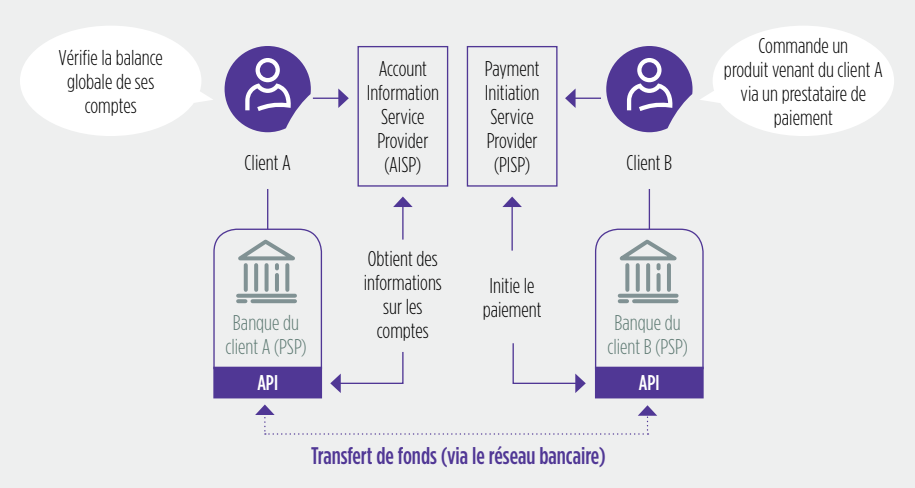
Cinématique *authorization code*

Mise en œuvre pour l'usage des AISP, la cinématique *authorization code* requiert une redirection de l'utilisateur de l'AISP vers le service d'authentification et de consentement de l'ASPSP, puis en retour une nouvelle redirection vers l'application de l'AISP.

Cette redirection peut être considérée comme un obstacle à l'utilisation des services comme le mentionne en exemple l'article 32 des RTS. En conséquence elle peut s'avérer illégale et des travaux sont en cours pour trouver des alternatives conformes ou non aux standards OAuth2.

L'acceptation de l'usage de cette cinématique pour les besoins de la DSP2 relève alors de chaque autorité nationale, ce qui a pour effet de limiter l'uniformisation européenne de ces interfaces. Actuellement, en France, l'ACPR a validé l'usage de cette redirection.

Les acteurs de la DSP2 en scène



CONCLUSION

Dans un environnement numérique en constante mutation, la DSP2 prend le parti de favoriser le développement des acteurs intermédiaires de services de paiement, pour mieux standardiser les échanges et apporter une meilleure ergonomie de navigation des utilisateurs et une meilleure sécurité des transactions.

Elle comporte des apports importants sur des sujets de sécurité, qui imposent des évolutions des SI bancaires : l'ouverture des services sur internet et le changement des moyens d'authentification sont en particulier un sujet compliqué pour les banques historiques.

Néanmoins, elle laisse en suspens d'autres usages dont la législation devra suivre, en particulier sur le périmètre des services hors comptes de paiement, pour lesquels les chantiers initiés par la DSP2 est une opportunité pour l'ouverture de l'accès à ces services de façon sécurisée.

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement, début 2016, de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods).

Dans un monde où savoir se transformer est la clé du succès, l'ambition de Wavestone est d'apporter à ses clients des réponses uniques sur le marché, en les éclairant et les guidant dans leurs décisions les plus stratégiques.

Wavestone rassemble 2 500 collaborateurs présents sur 4 continents. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

2018 I © WAVESTONE