FÉDÉRATION BANCAIRE FRANÇAISE

Fiche de synthèse

SCA – Stratégie, Communication, Adhérents
Novembre 2017

REVISION DE LA DIRECTIVE SUR LES SERVICES DE PAIEMENT (DSP2)

La directive du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (dite DSP2) a été publiée au Journal officiel de l'UE le 23 décembre 2015. Elle entre en application à partir du 13 janvier 2018. Tout au long des débats européens, la profession bancaire s'est mobilisée pour que les nouveaux prestataires de services de paiement (« PSP tiers ») appliquent les mêmes règles de sécurité, de responsabilité et de transparence à l'égard du client que les établissements bancaires, afin de maintenir le niveau de confiance des clients et la sécurité des accès aux informations bancaires.

En vue de l'application de la DSP2, la FBF s'est notamment fortement investie sur le projet de normes techniques de réglementation de l'Autorité Bancaire Européenne (ABE) liées aux exigences requises en matière d'authentification forte du client et de communication sécurisée entre PSP tiers et PSP gestionnaires de compte. L'initiative de place visant à développer une API (Application Programming Interface) ouverte vient compléter ce dispositif.

Le 27 novembre 2017 la FBF a pris acte de la publication par la Commission européenne des normes techniques réglementaires (RTS). La solution API étant clairement retenue au niveau européen, il est nécessaire de réduire au maximum la période de transition et de mettre en oeuvre rapidement des API opérationnelles.

■ CONTEXTE

La directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (dite DSP2) vise à accroître l'efficacité du cadre législatif en vigueur, assurer une concurrence équitable entre tous les acteurs de paiement et intégrer les évolutions technologiques apparues sur le marché depuis la mise en œuvre de la DSP1. Elle abroge la directive 2007/64 du 13 novembre 2007 concernant les services de paiement dans le marché intérieur (DSP1). Ce texte poursuit deux objectifs principaux :

- adapter les règles existantes aux services de paiement électroniques (paiements par internet et paiements mobile), en établissant notamment un ensemble de règles visant à garantir un environnement plus sûr en matière de sécurité des paiements (authentification forte du client) ;
- mettre en place un cadre réglementaire propice à l'émergence de nouveaux acteurs (agrégateurs de comptes et initiateurs de paiement) et au développement de solutions de paiement innovantes.

Les dispositions de la DSP2 s'appliquent à partir du 13 janvier 2018, à l'exception de celles concernant les exigences relatives d'une part à une authentification forte du client, et d'autre part à une communication sécurisée entre PSP Tiers et PSP gestionnaires de compte. Ces dernières sont fixées dans les normes techniques de réglementation (RTS) élaborées par l'Autorité Bancaire Européenne.
Le projet de RTS sur l'authentification forte du client a été adopté par la Commission européenne le 27 novembre 2017. En l'absence d'objection du Conseil et du Parlement européen, ces normes s'appliqueront après une période de transition de 18 mois suivant leur publication au Journal officiel de l'Union européenne, soit bien

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

après l'entrée en application des dispositions de la DSP2. Ce décalage entre l'application de la DSP2 et celle des normes techniques présente un enjeu vital de sécurité.

En France, l'ordonnance n° 2017-1252 du 9 août 2017 transpose la directive DSP2 dans la partie législative du code monétaire et financier. Elle crée notamment deux nouveaux services de paiement (le service d'information sur les comptes et le service d'initiation de paiement) et une nouvelle catégorie de prestataires de services de paiement (les prestataires de services d'information sur les comptes). L'ordonnance est complétée au plan réglementaire par les décrets n° 2017-1313 et n° 2017-1314 du 31 août 2017 et les cinq arrêtés du 31 août 2017 (cf. textes de référence en fin de document).

■ IMPLICATIONS POUR LES ETABLISSEMENTS

>>> Champ d'application de la DSP2

Le texte s'applique aux prestataires de services de paiement (PSP) qui comprennent deux catégories :

- le **« PSP gestionnaire de compte »** qui fournit et gère des comptes de paiement ;
- le **« PSP tiers »** (Third Party Payment Services Providers - TPP) qui peut être :

- **un agrégateur** (en anglais AISP - Account Information Services Providers) : il propose aux clients des services en ligne d'information sur les comptes de paiement et leur permet de bénéficier, par exemple, d'une vision consolidée de l'ensemble de leurs comptes de paiement sur une seule interface ;
- **un initiateur de paiement** (en anglais PISP - Payment Initiation Services Providers) : intermédiaire entre le site internet du commerçant et la banque en ligne du payeur, il initie, à la demande de ce dernier, un ordre de paiement sur un compte détenu auprès d'un autre prestataire ;
- un **émetteur d'instruments de paiement** liés à une carte (en anglais Payment Service Provider issuing card-based payment instrument).

>>> Principales dispositions

▪ Tout client ayant un compte de paiement accessible en ligne peut utiliser les services de paiement proposés par **un prestataire de service de paiement agréé (initiateur de paiement) ou enregistré (agrégateur) auprès de l'autorité nationale compétente.** Une banque ne peut refuser l'accès au compte de paiement à un de ces prestataires que pour des raisons objectivement motivées ou documentées liées à un accès non autorisé ou frauduleux, refus qui devra être notifié immédiatement à la Banque de France.

▪ L'ensemble des prestataires de services de paiement devront adopter des technologies assurant une **authentification forte du client** lorsqu'elle est requise ; ils devront veiller à ce que les données de sécurité personnalisées de l'utilisateur soient transmises par des canaux sûrs et efficaces et qu'elles soient partagées uniquement avec l'émetteur de ces données ou l'utilisateur.

▪ **En cas d'opération de paiement non autorisé effectuée via un initiateur de paiement**, le client pourra s'adresser à son PSP gestionnaire de compte pour être remboursé immédiatement du montant de l'opération de paiement, au plus tard à la fin du premier jour ouvrable suivant (sauf soupçon de fraude) ; charge ensuite à l'initiateur de paiement responsable de l'opération non autorisée d'indemniser le PSP gestionnaire de compte, à sa demande.

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

- **Certaines activités de paiement restent exclues de la DSP2** (ce qui était déjà le cas dans la DSP1) : les services reposant sur des instruments de paiement qui ne peuvent être utilisés que de manière limitée, dans un réseau limité de prestataires ou pour acquérir un éventail très limité de biens ou de services (par exemple carte d'enseigne, titre restaurant…) et les opérations de paiement proposées par un opérateur de télécommunication à ses abonnés.

- Les **obligations d'information** dues aux clients sont étendues à toutes les opérations de paiement vers ou depuis des pays hors de l'Union européenne, y compris dans les devises de ces pays, en ce qui concerne la partie de l'opération de paiement effectuée dans l'Union européenne.

- La **prise de frais (surfacturation)** par le bénéficiaire d'un paiement est autorisée uniquement pour les instruments de paiement qui ne sont pas soumis au règlement (UE) 2015/751 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

- La **franchise supportée par le client** lorsqu'un paiement non autorisé lui est imputé sur son compte suite à l'utilisation d'un instrument de paiement volé ou perdu est **réduite à 50 euros** (au lieu de 150 euros dans le texte actuellement en vigueur de la DSP1).

>>> Elaboration des normes techniques de réglementation de l'ABE (RTS)

Le 23 février 2017, l'ABE soumet à la Commission européenne un projet de normes techniques de réglementation (RTS) sur les exigences relatives à l'authentification forte du client et à la communication sécurisée entre PSP tiers et PSP gestionnaires de compte. Ces RTS introduisent un cadre visant à assurer des approches technologiques communes pour les nouveaux prestataires de services de paiement ainsi qu'à renforcer la sécurité des paiements via l'authentification forte du client.

Dans ce premier projet, l'ABE prévoit que les PSP gestionnaires de compte doivent offrir un accès via une interface (une interface « dédiée » ou interface de l'utilisateur).

Le 26 mai 2017, la Commission européenne propose quatre amendements au projet de RTS de l'ABE dont un visant à imposer une « solution de repli » dans le cas où l'interface dédiée proposée par les banques ne serait pas disponible ou ne fonctionnerait pas correctement. Cet amendement permet aux PSP tiers de conserver, en partie, leur mode de fonctionnement actuel comme la **pratique de capture de données d'écran** (en anglais **« screen scraping »**), technique qui permet à un PSP tiers d'accéder aux services de banque en ligne du client en utilisant les identifiants-mots de passe du client. Dans son avis du 29 juin 2017, l'ABE exprime son désaccord avec cet amendement au motif que cela aurait un impact négatif sur le compromis et l'équilibre précédemment trouvés pour atteindre les différents objectifs concurrents de la directive DSP2.

Le 27 novembre 2017, la Commission européenne adopte les RTS sur l'authentification du client. Ces normes précisent que la pratique existante du « screen scraping » ne sera plus autorisée. Cependant, la Commission européenne maintient sa « solution de repli » lorsque l'interface de communication dédiée est indisponible ou si elle ne respecte pas les obligations applicables aux interfaces. La Commission propose que les banques puissent être exemptées de cette solution de secours à condition qu'elles élaborent une interface de communication dédiée (type API) entièrement fonctionnelle répondant aux critères de qualité définis par les RTS, sur décision des autorités nationales et après consultation de l'ABE.

Le Conseil et Parlement européen disposent de trois mois pour formuler des objections. A défaut d'objection dans les délais prévus, les normes seront publiées au Journal officiel de l'Union européenne. Cette publication est attendue début 2018. Les prestataires de services de paiement auront 18 mois pour mettre en œuvre ces RTS.

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

■ POSITION ET DEMARCHES DE LA PROFESSION BANCAIRE

La FBF approuve l'entrée de nouveaux acteurs de paiement dans le champ d'application de la directive DSP2 et l'objectif d'accroître la concurrence sur le marché des paiements. Pour la profession bancaire, le sujet majeur est **l'encadrement juridique des PSP tiers** qui agiront comme intermédiaires entre les banques et leurs clients. Ces nouveaux acteurs doivent se voir appliquer des **règles de sécurité, de responsabilité et de transparence** à l'égard du client identiques à celles auxquelles sont soumis les établissements bancaires. Il importe en effet que les **conditions d'accès aux informations du compte de paiement par ces acteurs soient clairement encadrées** afin de maintenir le niveau de confiance des clients dans leurs moyens de paiement et la sécurité des accès aux informations bancaires.

Pour la profession bancaire, le partage des identifiants et mots de passe de banque en ligne avec des PSP tiers va à l'encontre de l'objectif visé par la DSP2, c'est-à-dire de garantir aux consommateurs une protection accrue de leurs paiements et données bancaires.

La FBF regrette que le régime de responsabilités ne soit pas plus équitable entre les parties et que la banque porte les conséquences, y compris financières, des choix du client ou de manquement d'un PSP tiers au regard des exigences de sécurité. **Aucune profession n'est engagée au niveau de la responsabilité pour les activités du fait d'autrui.**

Contribution aux mesures de niveau 2 élaborées par l'ABE et calendrier d'application

En 2017, la profession bancaire a été appelée à se positionner sur un certain nombre d'éléments structurants, impactant notamment les infrastructures sécuritaires et techniques des établissements ainsi que les parcours client. **La FBF a ainsi répondu aux consultations de l'ABE (Autorité Bancaire Européenne) relatives aux mesures de niveau 2 sur les sujets suivants** : exigences relatives à une authentification forte du client et à une communication sécurisée ; déclaration des incidents opérationnels ou de sécurité majeurs ; mesures de sécurité pour les risques opérationnels et de sécurité des services de paiement ; registre électronique central de l'EBA ; assurance de responsabilité civile professionnelle des PSP tiers et reporting de la fraude liée aux moyens de paiement.

La profession bancaire a approuvé la proposition de RTS de l'ABE transmises à la Commission européenne le 23 février 2017, ainsi que celle mise à jour le 29 juin 2017.

La FBF a, par ailleurs, mené de multiples actions au niveau national et européen afin de demander **le maintien de l'approche sécuritaire stricte des normes proposées par l'ABE** et **un alignement du calendrier d'application de la directive DSP2 et de ces standards de sécurité**. Le 27 novembre 2017, la FBF a pris acte de la publication par la Commission européenne des normes techniques réglementaires (RTS) concernant la directive des services de paiement révisée (DSP2). En privilégiant les interfaces standardisées, ouvertes et sécurisées (API) comme solutions d'accès aux comptes de paiement par les agrégateurs et les initiateurs de paiement au sein de l'Union européenne, la Commission a fait le choix de la sécurité. Maintenant que la solution API est clairement retenue au niveau européen, il est nécessaire de réduire au maximum la période de transition et de mettre en oeuvre rapidement des API opérationnelles.

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

Elaboration d'une interface dédiée pour les PSP tiers

La FBF soutient pleinement la création d'un écosystème fiable et efficace d'interfaces interopérables (de type API) par les banques pour une communication fiable entre PSP tiers et banques. Pour la profession bancaire, l'élaboration d'une **interface de programmation applicative (API - *Application Programming Interface*) offre une réponse conforme aux exigences posées par la DSP2 et au projet de RTS, à la fois en termes d'égalité d'accès pour tous les acteurs et de sécurité pour les données des clients.** La solution API est également soutenue par les banques centrales nationales (dont la Banque de France), les autorités en charge de la sécurité (ANSSI en France, ENISA au niveau européen) et le Bureau européen des unions de consommateurs (BEUC).

La profession bancaire française a confié les travaux de spécifications techniques de l'API DSP2 à la société STET qui a publié le 13 juillet 2017 ces spécifications sur la base des fonctionnalités conformes aux exigences requises par la DSP2 et les RTS de l'ABE.

Transposition de la DSP2 en droit français

La FBF a participé activement à la concertation menée par la Direction Générale du Trésor en vue de la transposition de la DSP2 appliquée aux comptes de paiement. Dans le cadre de ces travaux sur l'ordonnance de transposition et les textes d'application (décrets et arrêtés), elle s'est, en particulier, opposée à toute sur-transposition en France.

TEXTES ET SITES DE REFERENCE

Textes français

- **Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014** relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumis au contrôle de l'Autorité de contrôle prudentiel et de résolution
- **Arrêté du 31 août 2017 modifiant l'arrêté du 20 mai 2015** portant réglementation prudentielle et comptable en matière bancaire et financière en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna
- **Arrêté du 31 août 2017 modifiant l'arrêté du 2 mai 2013** portant sur la réglementation prudentielle des établissements de monnaie électronique
- **Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009** portant sur la réglementation prudentielle des établissements de paiement
- **Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009** relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principales stipulations devant figurer dans les conventions de compte de dépôt et les contrats-cadres de services de paiement
- **Décrets n° 2017-1313 et n° 2017-1314 du 31 août 2017** portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur
- **Ordonnance n° 2017-1252 du 9 août 2017** portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP2)

Textes européens

- **Communiqué de la Commission européenne du 27 novembre 2017** : DSP2 : adoption des normes techniques de réglementation sur l'authentification du client
- **Orientations finales de l'ABE du 13 octobre 2017** sur les procédures de réclamation en cas d'infraction

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

présumée à la directive DSP2

- **Orientations finales de l'ABE du 27 juillet 2017** sur le reporting d'incidents majeurs (DSP2)
- **Orientations finales de l'ABE du 11 juillet 2017** sur l'information à fournir pour l'agrément des établissements de paiement et de monnaie électronique et pour l'enregistrement des agrégateurs (DSP2)
- **Orientations finales de l'ABE du 7 juillet 2017** sur les critères permettant de déterminer le montant minimal de l'assurance de responsabilité civile professionnelle ou de la garantie comparable (DSP2)
- **Avis de l'ABE du 29 juin 2017** sur l'intention de la Commission européenne d'approuver en partie et de modifier les projets de normes techniques réglementaires (RTS) sur l'authentification forte du client et la communication commune et sécurisée (DSP2)
- **Projet final de normes techniques réglementaires (RTS) de l'ABE du 23 février 2017** sur les exigences relatives à une authentification forte du client et à une communication commune et sécurisée (DSP2)
- **Directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015** concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE

Positions de la profession bancaire

- **Communiqué de presse de la FBF du 28 novembre 2017** : Mise en oeuvre de la DSP2 : le choix de la sécurité
- **Déclaration de la FBE du 27 novembre 2017** sur l'adoption par la Commission européenne des normes techniques de règlementation relatives au paiement en ligne
- **Projet d'orientations : réponse de la FBF du 27 octobre 2017** à la consultation de l'ABE sur les exigences en matière de déclaration de données statistiques relatives à la fraude
- **Réponse de la FBF du 9 août 2017** à la consultation sur le projet de position ACPR relative aux notions de réseau limité d'accepteurs et d'éventail limité de biens et services
- **Projet de normes techniques de règlementation et d'exécution : réponse de la FBF du 18 septembre 2017** à la consultation de l'ABE sur le registre électronique central de l'ABE
- **Projet d'orientations : réponse de la FBF du 28 juillet 2017** à la consultation de l'ABE sur les mesures de sécurité pour les risques opérationnels et de sécurité des services de paiement
- **Déclaration de la FBE du 2 juin 2017** sur la position de la Commission européenne relative au projet de normes techniques RTS de l'ABE dans le cadre de la DSP2
- **Communiqué de presse de la FBE du 16 mai 2017** : La FBE demande à la Commission européenne de soutenir l'interdiction de la capture de données d'écran (« screen scraping ») dans le cadre de la DSP2
- **Projet d'orientations : réponse de la FBF du 7 mars 2017** à la consultation de l'ABE sur la déclaration des incidents opérationnels ou de sécurité majeurs
- **Projet de normes techniques réglementaires : réponse complémentaire de la FBF du 19 janvier 2017** à la consultation de l'ABE sur les exigences relatives à une authentification forte du client et à une communication commune et sécurisée
- **Projet d'orientations : réponse de la FBF du 29 novembre 2016** à la consultation de l'ABE sur les critères permettant de déterminer le montant minimal de l'assurance de responsabilité civile professionnelle ou de la garantie comparable pour les prestataires de services d'initiation de paiement et de services d'information sur les comptes
- **Projet de normes techniques réglementaires : réponse de la FBF du 12 octobre 2016** à la consultation de l'ABE sur les exigences relatives à une authentification forte du client et à une communication commune et sécurisée
- **Orientations de la FBE du 14 septembre 2016** relatives à la mise en oeuvre de la directive révisée sur les services de paiement

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.

- **Réponse de la FBF du 13 avril 2016** aux questions complémentaires de l'ABE concernant le document de travail sur le futur projet de normes techniques réglementaires relatives aux procédures d'authentification forte du client et à une communication sécurisée
- **Communiqué de la FBF du 9 octobre 2015 :** Vote de la directive européenne sur les services de paiement (DSP2) : les banques françaises demandent des modalités de mise en oeuvre garantissant la sécurité des clients

La présente « fiche de synthèse FBF » destinée aux adhérents a été rédigée à des fins d'information.
Elle ne constitue pas une interprétation juridique de la part de la FBF et de ses instances.