MÉMO
N°08

LA DSP2 ET LES ENJEUX DE SÉCURITÉ

FÉDÉRATION BANCAIRE FRANÇAISE

- **En quoi consiste la DSP2 ?**
- **Quels sont les enjeux en termes de sécurité pour les données des clients et les systèmes de paiement ?**
- **Quelles sont les solutions pour garantir cette sécurité ?**
- **Quelles sont les modalités du passage à l'authentification forte ?**

01

QU'EST CE QUE LA DSP2 ?

Un nouveau cadre réglementaire

La directive (UE) 2015/2366 relative aux services de paiement dans le marché intérieur, dite DSP2, actualise le cadre réglementaire des paiements en Europe. Son objectif est de prendre en compte les évolutions technologiques, en permettant l'émergence de **« services de paiement numériques novateurs, sûrs et conviviaux ».**

54,8 

MILLIARDS
NOMBRE DE PAIEMENTS PAR CARTE EN EUROPE

Source : BCE, Payment Statistics, 2018 (hors Royaume-Uni, Slovaquie, Malte et Irlande)

La DPS2 s'applique depuis le **13 janvier 2018**. Elle impose que soient accessibles, gratuitement, les données des comptes de paiement des clients, dans le cadre de deux activités nouvelles :

- **le service d'information sur les comptes :** c'est un service d'agrégation de données fournissant au client titulaire de comptes de paiement, dans un ou plusieurs établissements, des informations consolidées ;
- **le service d'initiation de paiement :** il permet à un prestataire de services de paiement de transmettre un ordre de paiement, au nom et pour le compte du client, à l'établissement teneur de compte.

Innovation et sécurité

La DSP2 affiche deux ambitions : d'une part, favoriser l'innovation pour un marché européen des paiements compétitif ; d'autre part, renforcer le niveau de sécurité des paiements et la protection des clients.

Elle prévoit ainsi des obligations d'enregistrement (pour les agrégateurs) ou d'agrément (pour les initiateurs de paiement).

C'est l'Etat membre d'origine de ces nouveaux acteurs (le pays où ils ont leur siège statutaire) qui a en charge leur contrôle.

En France, ces nouveaux acteurs sont contrôlés par l'Autorité de contrôle prudentiel et de résolution (ACPR).

Vis-à-vis du client, le teneur de compte (donc la banque ou l'établissement de paiement où le client a son compte) a l'obligation, en cas de fraude opérée à partir d'une initiation de paiement, de rembourser le client. Ce **régime inédit de responsabilité** fait peser sur le teneur de compte le coût de la fraude, quelle qu'en soit l'origine, charge à lui de se retourner vers l'initiateur de paiement soumis à une obligation d'assurance.

02

PROTECTION DES DONNÉES ET DES SYSTÈMES : UN ENJEU MAJEUR

Un contexte de risques croissants

La directive elle-même insiste sur les risques nouveaux introduits par l'innovation et la multiplication des acteurs. Elle précise que **« ces dernières années ont vu croître les risques de sécurité liés aux paiements électroniques. Cela s'explique par la complexité technique croissante de ces paiements, leurs volumes toujours croissants à l'échelle mondiale et l'émergence de nouveaux types de services de paiement »**[(1)].

De plus, **« la sûreté et la sécurité des services de paiement sont vitales au bon fonctionnement du marché des services de paiement. Il convient dès lors de protéger de manière adéquate les utilisateurs contre ces risques. Les services de paiement sont essentiels au fonctionnement d'activités économiques et sociales vitales. »**[(1)]

Le nombre de cyberattaques a explosé entre le moment où la directive a été conçue et aujourd'hui. Cela constitue une préoccupation majeure pour les banques et les régulateurs.

32%

D'AUGMENTATION ANNUELLE DU NOMBRE DE CYBER-ATTAQUES EN 2018 EN FRANCE

Source : F-Secure - Mars 2019

(1) Considérant n°7 de la Directive

Un besoin vital de sécurité

L'enjeu est à la fois de protéger les données et les fonds que chacun confie à sa banque et de garantir la sécurité des opérations de paiement. La directive rappelle que l'absence de règles régissant le service d'initiation de paiement et l'absence de contrôle soulèvent **« de nombreuses questions juridiques, notamment en matière de protection des consommateurs, de sécurité et de responsabilité, ainsi que de concurrence et de protection des données, en particulier pour ce qui est de la protection des données de l'utilisateur de services de paiement conformément aux règles de l'Union en matière de protection des données »** et enfin que les **« nouvelles règles devraient donc répondre à ces questions »**[2].

En outre, **« La sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude »**[3].

La directive montre ainsi que la sécurité est une préoccupation majeure pour le législateur européen. En effet, il s'agit de maintenir la confiance de tous dans des systèmes de paiement, sans lesquels il n'y a pas de vie économique possible.

Chaque année les banques réalisent d'importants investissements pour maintenir un degré de sécurité élevé des systèmes et des infrastructures.

(2) Considérant n°29 de la Directive
(3) Considérant n°95 de la Directive

03

LE CHOIX DE LA SÉCURITÉ

De nouvelles normes de sécurité

Parce que l'enjeu de sécurité est vital, la DSP2, dans son article 98, a confié aux experts de l'Autorité bancaire européenne (ABE) le soin de définir les normes techniques de réglementation (RTS) concernant **l'authentification forte du client** pour les opérations de paiements et l'accès aux comptes de paiement en ligne. Ces normes, publiées au Journal Officiel de l'UE le 13 mars 2018[4], s'appliquent à compter du **14 septembre 2019**, soit 18 mois après leur publication comme prévu par la directive.

L'API : une solution partagée

Ces normes de sécurité (RTS) reposent sur **un mode d'accès ouvert à tous les acteurs, standardisé et sécurisé**. Les banques teneurs de comptes doivent ainsi mettre à disposition des agrégateurs et initiateurs de paiement une interface standardisée et sécurisée. Cette interface se substitue aux techniques de « web scraping », basées sur l'utilisation par les agrégateurs et initiateurs de paiement des identifiants et des mots de passe des clients, transmis par ces derniers sous leur seule responsabilité.

Une interface de type API (Application Programming Interface), bien connue dans le monde du marketing digital et de l'Internet, offre une réponse conforme aux exigences posées par la directive et les RTS, à la fois en termes d'égalité d'accès pour tous les acteurs et de sécurité pour les données des clients. Les banques, mais aussi les consommateurs au niveau européen (par la voix du Bureau européen des unions de consommateurs - BEUC) ainsi que bon nombre de nouvelles Fintechs qui arrivent sur le marché des paiements, soutiennent cette solution.

Ainsi, les banques françaises ont travaillé depuis quatre ans à la définition, au développement et à la mise en production d'API conformes aux exigences fixées par les RTS. **Ces solutions sont disponibles pour l'accès aux comptes des clients par les tiers de paiement.**

(4) Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017.

Passage progressif à l'authentification forte

Le 14 septembre 2019 marque **le début du passage à l'authentification forte des opérations de paiements et des modalités d'accès aux comptes de paiements**. En tant qu'experts de la sécurité des fonds et des données de leurs clients, les banques sont préparées à cette échéance. Elles se sont fortement mobilisées pour que la mise en œuvre se passe dans les meilleures conditions pour leurs clients et les e-commerçants.

- **Accès aux comptes de paiements en ligne** (banque en ligne, application mobile bancaire) : les textes prévoient qu'une authentification forte du client soit demandée a minima tous les 90 jours. Elle est mise en œuvre **de manière simple et progressive, avec un déploiement propre à chaque banque**. Les clients sont informés des évolutions par leurs banques.

- **Paiements des achats en ligne** : le mécanisme actuel pour authentifier le client continue d'être utilisé mais il est **remplacé progressivement par de nouvelles solutions d'authentification forte** que les banques proposent à leurs clients. Cette transition s'inscrit dans un planning de place élaboré par l'ensemble des acteurs de l'écosystème (réseaux cartes, e-commerçants, banques…) en lien avec les autorités nationales, et publié par l'Observatoire de la sécurité des moyens de paiement (OSMP).

04

NOS ENJEUX

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 européenne a fait le choix de la sécurité.

A l'instar de l'Autorité bancaire européenne (ABE), du Bureau européen des unions de consommateurs (BEUC), des autorités en charge des questions de cybersécurité, des associations bancaires européennes et des Fintechs désireuses d'entrer sur le marché, la Fédération bancaire française a toujours soutenu les API, seules solutions garantes d'une véritable sécurité dans l'environnement actuel de cyberattaques toujours plus nombreuses.

Fidèles à leurs valeurs d'innovation dans la sécurité et d'accompagnement de leurs clients, les banques ont développé des API pour l'accès aux comptes de paiements des clients par les agrégateurs et initiateurs de paiement (TPP). Ces interfaces sont en tests depuis de nombreux mois et disponibles en production. Elles sont prêtes, conformes à la DSP2 et aux normes de sécurité, et utilisables par les TPP. Elles garantissent la sécurité des données et des fonds des clients.

LE CALENDRIER

La directive DSP2 est applicable depuis le 13 janvier 2018 et les normes de sécurité à compter du 14 septembre 2019.

25 NOVEMBRE 2015

Adoption
de la DSP2

10 AOÛT 2017

Publication de l'ordonnance
de transposition en France

13 JANVIER 2018

Application
de la DPS2

13 MARS 2018

Publication des normes techniques
de réglementation (RTS) sur
l'authentification forte et la
communication sécurisée

18 MOIS

**Période transitoire :
les normes de sécurité
ne sont pas encore appliquées.**

14 SEPTEMBRE 2019

Application progressive
des normes de sécurité (RTS)
sur l'authentification forte

Glossaire

AGRÉGATEUR DE COMPTE Le service d'agrégation de données fournit au client titulaire de plusieurs comptes de paiement, dans un ou plusieurs établissements, des informations consolidées.

API ou **APPLICATION PROGRAMMING INTERFACE** L'API (Interface Applicative de Programmation) est un moyen efficace, standardisé et sécurisé, de faire communiquer entre elles deux applications.

AUTHENTIFICATION FORTE L'authentification forte, ou authentification à deux facteurs, combine l'utilisation de deux éléments parmi les trois catégories suivantes : quelque chose que l'on sait (mot de passe, code PIN), quelque chose que l'on possède (ordinateur, téléphone mobile), quelque chose que l'on est (empreinte digitale, rétine, voix).

INITIATEUR DE PAIEMENT Le service d'initiation de paiement permet à un prestataire de services de paiement de transmettre un ordre de paiement, au nom et pour le compte du client, à l'établissement teneur de compte.

RTS ou **REGULATORY TECHNICAL STANDARDS** Les normes techniques de réglementation fixent les règles sur l'authentification forte du client et la communication sécurisée.

TPP ou **THIRD PARTY PROVIDER** Les TPP ou tiers de paiement sont les agrégateurs de comptes ou initiateurs de paiement.

WEB SCRAPING Cette technique permet de récupérer le contenu d'une page web en vue d'en réutiliser le contenu.

18, RUE LA FAYETTE
75440 PARIS CEDEX 09
TÉL : 01 48 00 52 52

FBF.FR

@FBFFrance

Septembre 2019

Directrice de la publication :
Marie-Anne Barbat-Layani

FÉDÉRATION
BANCAIRE
FRANÇAISE