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 paiements ?**
- **Quelles sont les solutions pour garantir cette sécurité ?**

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 ».**

59,6 

MILLIARDS
DE PAIEMENT PAR CARTE
EN EUROPE

source : BCE, Payment Statistics, 2016

La DPS2 s'appliquera à compter du **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). Ils interviennent aujourd'hui, via la technique du « web scraping », sans aucun encadrement réglementaire et sous la seule responsabilité des clients qui leur ont donné accès à leurs comptes en leur communiquant leurs identifiants et mots de passe.

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 seront 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) aura 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

Nouvelles activités, nouveaux risques

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. »**

Un contexte de risques croissants

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.

35%

D'AUGMENTATION DU NOMBRE DE CYBER-ATTAQUES EN UN AN EN FRANCE

Source : Global Security Mag - octobre 2017- Baromètre RGPD

(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 paiements. La directive rappelle que l'absence actuelle 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].

Le texte de 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

Des normes de sécurité indispensables

Parce que l'enjeu de sécurité est vital, la DSP2, dans son article 98, a prévu de confier aux experts de l'Autorité bancaire européenne (ABE) le soin de définir les normes techniques de réglementation (RTS) concernant l'authentification forte du client et la communication sécurisée entre les prestataires de services de paiement. Les prescriptions de sécurité de l'ABE ont été transmises à la Commission européenne le 23 février 2017.

La Commission européenne a adopté les RTS le 27 novembre 2017 ; reste au Parlement européen et au Conseil à les ratifier.

Ces normes reposent sur un mode d'accès ouvert à tous les acteurs, standardisé et sécurisé. Les banques teneuses de comptes devront ainsi mettre à disposition des agrégateurs et initiateurs de paiement une interface. Cette interface standardisée et sécurisée doit se substituer aux techniques actuelles de « web scraping », basées sur l'utilisation par les agrégateurs et initiateurs de paiement des identifiants et des mots de passe des clients.

L'authentification forte, ou authentification à deux facteurs, combine l'utilisation de deux éléments parmi les trois catégories : 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).

API : une solution partagée

Une interface de type API (Application Programming Interface), bien connue dans le monde du marketing digital et de l'Internet, offre ainsi une réponse conforme aux exigences posées par la directive et les normes techniques de réglementation, 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 fintech qui arrivent sur le marché des paiements, soutiennent cette solution.

Pourtant, la Commission européenne, sous la pression de certains acteurs déjà bien installés sur le marché de l'agrégation et de l'initiation de paiement et soucieux de protéger leur marché, a souhaité permettre que la technique, non-sécurisée, du web scraping puisse perdurer dans certains cas. Les banques y sont opposées, y compris comme solution de repli.

Les normes de sécurité ne pourront pas être appliquées en même temps que la directive en janvier 2018.

Les RTS ne s'appliqueront que 18 mois après leur publication, comme prévu par la directive elle-même.

L'INCOHÉRENCE DU CALENDRIER

Une directive qui s'applique le 13 janvier 2018 mais des normes de sécurité qui ne s'appliqueront pas avant mi-2019 au plus tôt.

25 NOVEMBRE 2015
Adoption de la DSP2

12 JANVIER 2016
Entrée en vigueur de la DSP2

23 FÉVRIER 2017
Publication par l'ABE d'un projet denormes techniques de réglementation (RTS) sur l'authentification forte et la communication sécurisée

24 MAI 2017
Proposition de la Commission européenne (CE)

29 JUIN 2017
2ème proposition de l'ABE

10 AOÛT 2017
Publication de l'ordonnance de transposition

27 NOVEMBRE 2017
Adoption des RTS par la CE et envoi au Parlement et Conseil européens pour ratification

13 JANVIER 2018
Application de la DPS2

?
Publication des RTS

MI 2019, AU PLUS TÔT
Application des RTS

18 MOIS
Période transitoire risquée : les normes de sécurité ne seront pas encore appliquées.

04

NOS ENJEUX

La Fédération bancaire française a pris acte de l'adoption, le 27 novembre 2017, par la Commission européenne des normes techniques réglementaires (RTS) concernant la Directive des services de paiement (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.

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 FBF a toujours soutenu les API, seules solutions garantes d'une véritable sécurité dans l'environnement actuel de cyberattaques toujours plus nombreuses.

L'actualité des derniers mois vient nous rappeler que le nombre de cyberattaques, toujours plus puissantes, se multiplie. Les API offrent une réponse sécurisée et leur reconnaissance par la Commission européenne est une bonne nouvelle pour tous. Les banques françaises déploieront cette solution courant 2018.

MARIE-ANNE BARBAT-LAYANI
DIRECTRICE GÉNÉRALE DE LA FBF
communiqué de presse
du 28 novembre 2017

Glossaire

API Application Programming Interface (Interface Applicative de Programmation). L'API est un moyen efficace, standardisé et sécurisé, de faire communiquer entre elles deux applications.

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.

AUTHENTIFICATION FORTE ou authentification à deux facteurs, combine l'utilisation de deux éléments parmi les trois catégories : 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 Regulatory Technical Standards : normes techniques de réglementation sur l'authentification forte du client et la communication sécurisée.

TPP Third Party Provider : agrégateurs de comptes ou initiateurs de paiement.

WEB SCRAPING Technique qui 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

Achevé de rédiger en décembre 2017

FÉDÉRATION
BANCAIRE
FRANÇAISE