Par Christophe Jacomin,
avocat associé,
LPA-CGR avocats

Directive sur les services de paiement : API et authentification forte, où en sont les banques françaises ?

L'objectif de la directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dite «DSP 2», qui est entrée en vigueur en droit français le 13 janvier 2018, est d'intégrer toutes les méthodes de paiement dans un seul cadre réglementaire et de lever les obstacles à l'entrée sur le marché des nouveaux fournisseurs de services de paiement.

La DSP 2 doit permettre d'accompagner les nombreuses évolutions technologiques dans les services de paiement en favorisant l'innovation et la croissance du commerce électronique tout en renforçant la sécurité des paiements.

La DSP 2 prévoit ainsi notamment :

– l'accès non discriminatoire aux systèmes de paiement pour tout prestataire de services de paiement ;

– l'ouverture non discriminatoire de comptes bancaires pour tout prestataire de services de paiement ;

– la modernisation et le renforcement des règles de sécurité des opérations de paiement.

La DSP 2 a donc consacré de nouveaux acteurs tels que ceux proposant des services d'agrégation d'information et d'initiation de paiement. Afin de protéger les consommateurs, la DSP 2 a également instauré un mécanisme d'authentification forte pour renforcer la sécurité des opérations de paiement en ligne. Ces mesures devaient être mises en œuvre le 14 septembre 2019. Mais cette date n'a pas pu être respectée.

1. Prestataires de services d'information sur les comptes et d'initiation de paiement et Application Programming Interface (API)

Les prestataires de services d'information sur les comptes (PSIC) (article L. 522-1 du Code monétaire et financier (CMF)) sont ceux fournissant un service d'information consolidée sur les comptes de paiement détenus par l'utilisateur auprès des prestataires de services de paiement (PSP). Ces informations sont accessibles via des interfaces en ligne qui permet à l'uti-

Pour permettre aux PSIP d'initier les paiements de leurs clients ou aux PSIC de fournir des services d'information consolidée, la DSP 2 a ainsi imposé aux PSP gestionnaires de comptes de concevoir ce que l'on appelle des Open Application Programming Interfaces (API).

lisateur d'avoir une vue d'ensemble de sa situation financière à un moment donné. Ces prestataires ne sont soumis qu'à une procédure d'enregistrement auprès de l'Autorité de contrôle prudentiel et de résolution (ACPR).

La DSP 2 a également instauré un service d'initiation de paiement fourni par des prestataires de services d'initiation de paiement (PSIP). Ces prestataires exercent dans le cadre du commerce électronique, selon la DSP 2 (considérant 27), «en établissant une passerelle logicielle entre le site internet du commerçant et la plateforme de banque en ligne du prestataire de services de paiement gestionnaire de compte du payeur en vue d'initier des paiements par l'internet sur la base d'un virement». Ils «initient un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de service de paiement». L'intervention d'un PSIP modifie le schéma de la transaction. Une fois sur le portail du commerçant lui proposant diverses modalités de paiement (ex. : paiement par carte/Paypal), le payeur choisit de recourir aux services de son PSIP. Le commerçant (aussi bénéficiaire de la transaction) transmet l'ordre de paiement au PSIP du payeur, lequel initie le paiement sur la base d'un virement : le PSP du bénéficiaire n'a pas à transmettre l'ordre de paiement du payeur au PSP du payeur.

Pour permettre aux PSIP d'initier les paiements de leurs clients ou aux PSIC de fournir des services d'information consolidée, la DSP 2 a ainsi imposé aux PSP gestionnaires de comptes de concevoir ce que l'on appelle des Open Application Programming Interfaces (API). Leur objet est de permettre aux PSIP ou aux PSIC, sans discrimination, d'accéder au compte de paiement de leurs clients afin de fournir les services d'initiation de paiement ou d'informations concernés. Auparavant, ces prestataires, dont le statut n'était pas encore consacré, avaient recours à la technique du web-scrapping qui consistait à utiliser les identifiants et mots de passe de leurs clients afin d'accéder aux comptes de paiement auprès des prestataires gestionnaires de compte et est donc contraire aux prescriptions de la DSP 2 en matière de protection des données de sécurité personnalisées.

Ces API devaient être mises en œuvre au plus tard le 14 septembre 2019, date limite d'obtention d'une exemption de mécanisme d'urgence pour les PSP ayant décidé la mise en place d'une API. Seulement six banques françaises ont été exemptées à ce jour par l'ACPR dont un seul grand groupe bancaire, le Crédit Agricole, ce qui indique que ces banques ont pu tester de façon concluante pendant au moins trois mois leurs API avec des PSIC ou PSIP tiers. Il semble donc bien y avoir un retard important des PSP français dans la mise en production opérationnelle des API au profit des PSCIC et PSIP tiers. En conséquence, il semblerait que les autorités bancaires françaises entendent donner un délai de quelques mois supplémentaires aux banques françaises pour continuer à s'adapter et rendre leurs API parfaitement exploitables.

Les banques européennes ne s'estimant pas encore prêtes et craignant un impact négatif sur l'e-commerce et des problématiques de gestion ont demandé via la Fédération bancaire européenne à l'Autorité bancaire européenne (ABE) un report de la fin de la periode de transition initial prévue le 14 septembre dernier.

2. Mécanisme d'authentification forte

Les obligations de la DSP 2 d'authentification forte ont fait l'objet d'une période de transition qui devait prendre fin le 14 septembre 2019. Les banques européennes ne s'estimant pas encore prêtes et craignant un impact négatif sur l'e-commerce et des problématiques de gestion ont demandé via la Fédération bancaire européenne à l'Autorité bancaire européenne (ABE) un report de cette date.

Dans ses opinions relatives à l'authentification forte publiées le 21 juin 2019, l'ABE a ainsi permis aux autorités bancaires européennes compétentes d'accorder du temps supplémentaire aux PSP pour se conformer effectivement aux obligations d'authentification forte.

A l'instar de ce qui se passe en Allemagne et au Royaume-Uni, l'Observatoire de la sécurité des moyens de paiement, placé sous la tutelle de la Banque de France, a ainsi indiqué qu'elle faisait usage de cette liberté en accordant un délai supplémentaire de trois ans pour une mise une pleine conformité des PSP aux obligations d'authentification forte, soit 2022. Mais en quoi consiste cette authentification forte ?

2.1. Définition

L'authentification forte d'une transaction est requise par l'article 97 de la DSP 2. La définition de l'authentification forte est donnée en deux temps par la directive.

Elle définit l'authentification comme une «procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur».

L'authentification forte consiste alors en une authentification reposant «sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession" (quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification».

Jusqu'à présent, les paiements par carte sur internet étaient authentifiés, après fourniture par le titulaire de la carte de son numéro de carte bancaire et de son cryptogramme, par l'envoi d'un SMS sur le téléphone du payeur contenant un code d'authentification que celui-ci devait renseigner. Ce système, dit du 3D-secure (de première génération), a été analysé par

l'ABE comme une authentification à un facteur, reposant sur l'élément «possession». L'authentification forte introduit un second facteur d'authentification, certains étant d'ores et déjà proposés par l'ABE.

Les deux facteurs utilisés aux fins d'authentification doivent être indépendants l'un de l'autre de sorte que la «compromission d'un des éléments ne remet pas en question la fiabilité des autres» (art. 9 règlement délégué (UE) 2018/389 du 27 novembre 2017). Cette indépendance des facteurs est assurée par des dispositifs techniques mis en place par le PSP qui procède à l'authentification, le PSP du payeur.

L'authentification forte génère un code d'authentification selon l'article 4 du règlement délégué. Ce code doit notamment permettre, dans le cadre des opérations de paiements électroniques à distance, d'établir un lien dynamique (considérant n° 4 : «L'établissement d'un lien dynamique est possible grâce à la génération de codes d'authentification, qui fait l'objet d'une série d'exigences strictes en matière de sécurité») entre l'authentification forte, l'opération, son montant et son bénéficiaire. A ce titre, ce code informe le payeur du montant de l'opération. La transmission de ce code au payeur est encadrée par des mesures de sécurité et des garanties de confidentialité (art. 22 du règlement délégué).

L'authentification forte consiste en une authentification reposant «sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession" (quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants.

2.2. Champ d'application et exceptions

L'authentification forte du client est requise dans trois cas, lorsque le payeur :

– accède à son compte de paiement ;
– initie une opération de paiement électronique ; ou
– exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

L'opération soumise à authentification forte est donc initiée par le payeur à distance, de manière électronique. Cette notion est entendue au sens large : elle comprend à la fois les paiements qui sont effectués par virements, pour l'exécution desquels le payeur transmet directement l'ordre de paiement à son PSP (y compris donc les opérations initiées par un PSIP) ; et les paiements par carte, qui consistent pour le payeur à donner un ordre de paiement au bénéficiaire (le commerçant), lequel transmettra cet ordre à son PSP. Les opérations de paiement réalisées par prélèvement ne requièrent pas l'authentification forte du payeur.

Le règlement délégué prévoit toutefois plusieurs cas d'exception dans lesquels les PSP sont autorisées à ne pas satisfaire à l'obligation d'authentification forte du client lors d'une transaction en ligne :

– paiements sans contact au point de vente lorsque le montant de la transaction ne dépasse pas 50 euros, ou un montant cumulé de 150 euros s'il y a eu une multitude de paiements sans contact depuis la dernière authentification forte. A l'inverse du paiement où le payeur introduit sa carte dans le terminal de paiement du commerçant (point of sale), le paiement sans contact constitue une opération de paiement à distance, ce qui explique cette exclusion ;
– paiements aux automates de paiement aux fins de régler des frais de transport ou de parking ;
– paiements aux bénéficiaires de confiance. Une des nouveautés introduites par la DSP 2 est la possibilité pour le payeur de fournir une liste de bénéficiaires de confiance. L'authentification est nécessaire pour créer ou modifier la liste ;
– virements à soi-même (de compte à compte) ;
– paiements dont le montant de la transaction individuelle ne dépasse pas 30 euros, ou 100 euros s'il y a eu plusieurs opérations de faible valeur depuis la dernière authentification forte du payeur.

La dernière exception est la plus intéressante : «les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance que le prestataire de services de paiement considère comme présentant un faible niveau de risque» (art. 18 du règlement délégué). Le recours à cette exception est conditionné.

Afin que les PSP puissent déterminer le risque que la transaction présente, l'article 95 de la DSP 2 leur impose d'établir un «cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité, liés aux services de paiement qu'ils fournissent» et qu'ils notifient aux autorités de contrôle tout incident relatif à la sécurité des opérations auxquelles ils participent (art. 96 DSP 2). Ces PSP sont donc tenus par des obligations de monitoring. Ces derniers doivent notamment établir des statistiques de fraude relatives aux services de paiement qu'ils fournissent. La première condition tient à ce que les statistiques de fraude du PSP qui souhaite mettre en œuvre cette exception soient inférieures ou égales aux taux de référence publiés en annexe du règlement délégué. Ces taux varient selon le montant de la transaction et le type de transaction (virement ou opération par carte à distance). En tout état de cause, les transactions dont le montant est supérieur à 500 euros ne peuvent être exemptées sur ce fondement.

Ce critère de nature quantitative est un prérequis à la mise en œuvre de l'exception. Celui-ci doit satisfaire à cette condition s'il décide de ne pas déclencher l'authentification), mais en outre, les PSP doivent se fonder sur des critères qualitatifs (art. 18 § 2 c et § 3 du règlement délégué) pour déterminer le risque de la transaction. Ces critères qualitatifs sont des indicateurs inhérents à la personne du payeur (ex. : les habitudes de dépenses antérieures du payeur). Les PSP doivent procéder en temps réel à l'analyse de la transaction en tenant compte de ces indicateurs.

2.3. Charge de l'authentification forte

L'article 97 de la DSP 2 ne précise pas explicitement à quel PSP incombe de procéder à l'authentification forte du payeur. Il y a lieu de distinguer, ici, le PSP du bénéficiaire, qui déclenche l'authentification forte du client, et le PSP du payeur, qui y procède. S'agissant d'une opération réalisée par virement, la question ne semble pas poser de difficulté particulière.

Afin que les PSP puissent déterminer le risque que la transaction présente, l'article 95 de la DSP 2 leur impose d'établir un «cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité, liés aux services

Le payeur transmet un ordre de virement à son PSP qui, sous réserve des exceptions prévues dans le règlement délégué, initie et procède à l'authentification forte de son client avant de transmettre les fonds au PSP du bénéficiaire du virement. L'authentification forte s'applique ainsi aux opérations initiées par un PSIP, mais l'authentification forte est réalisée selon la procédure du PSP gestionnaire de compte du payeur.

En ce qui concerne les opérations de paiement par carte, la charge de déclencher l'authentification forte du client devrait reposer sur le PSP du bénéficiaire (la plupart du temps, un PSP offrant un service d'acquisition de services de paiement). Il redirige le payeur vers son PSP afin qu'il procède à l'authentification.

La distinction entre le PSP qui déclenche le processus d'authentification forte (PSP du bénéficiaire) et le PSP qui y procède explique aussi le point de vue de l'ABE concernant les transactions dites one-leg, c'est-à-dire dont l'un des PSP est situé en dehors de l'Espace économique européen (EEE). On comprend que, dans le cadre d'une transaction one-leg, le fait que le PSP du payeur soit situé en dehors de l'EEE exclut la transaction du champ de l'authentification forte : le PSP non européen du payeur ayant fourni la carte utilisée dans la transaction n'est pas soumis aux dispositions de la DSP 2, et le PSP du bénéficiaire européen n'a pas à procéder à l'authentification forte du payeur bien qu'il doive faire les efforts raisonnables pour déterminer l'utilisation légitime du moyen de paiement concerné.

Au total, les principaux PSP français que sont les établissements de crédit français vont devoir investir encore massivement dans le développement de leurs systèmes informatiques, voire profondément innover, afin de s'adapter aux nouveaux défis et services technologiques et se conformer à l'ensemble des dispositions de la DSP 2. ■