Compte-rendu du Séminaire du 3 avril 2018

DSP2 et sécurité de la chaîne de paiement : progrès ou nouveaux risques ?

Marie Agnès NICOLET - Regulation Partners

La seconde directive sur les services de paiement consacre de nouveaux usages et des avancées techniques, rehausse les exigences de sécurité et crée de nouveaux acteurs : les prestataires de services d'information sur les comptes (PSIC) et les prestataires de services d'initiation de paiement (PSIP). Ces nouvelles prestations nécessitent d'avoir accès aux comptes bancaires, ce qui pose la question de la sécurité des opérations.

Ces prestataires (PSP) sont soumis à des obligations, dont l'authentification forte du client. L'authentification est réputée forte quand deux éléments au moins appartenant aux catégories connaissance (mot de passe, code…), possession (token, téléphone portable...), inhérence (empreinte digitale…) sont réunis.

Les standards techniques réglementaires précisent les cas où l'authentification forte n'est pas requise, notamment celui où la banque du payeur peut se prévaloir d'un taux de fraude légale inférieur à un certain seuil.

En France, la directive européenne a été transposée par une ordonnance du 9 août 2017, un décret et cinq arrêtés. L'ordonnance précise les conditions d'exercice des établissements de paiement, qui vont dans le sens d'un renforcement des droits des utilisateurs et des exigences de sécurité. L'arrêté du 31 août 2017 traite des obligations d'information des prestataires de services de paiement à l'égard de leurs clients et éclaire la notion d'incident de sécurité (les incidents majeurs doivent être notifiés à l'Autorité de contrôle prudentiel et de résolution - ACPR).

En France, l'agrément des prestataires de services par l'ACPR garantit un niveau de sécurité élevé. Il n'est pas certain qu'il en soit de même à propos d'acteurs ayant reçu un agrément dans certains pays de l'Union européenne et exerçant, en France par exemple, en vertu du passeport européen. Une supervision commune est ainsi hautement souhaitable.

Emmanuelle Assouan – Banque de France

La France, qui se situe à l'avant-garde en matière de sécurité des paiements, a été un élément moteur dans l'adoption de l'authentification forte, une notion qui existait dans l'hexagone avant la DSP révisée, dans le domaine de la carte bancaire (des solutions avaient été présentées dès 2008 : SMS, carte virtuelle, lecteur de carte individuel…et aujourd'hui, 98 % des porteurs de carte bancaire disposent d'un procédé d'authentification forte).

En matière de paiement à distance, le taux de fraude se situait à 0,199 % en 2016 (dernière donnée connue). Il y a encore des marges de manœuvre à la baisse.

La DSP 2 n'est pas prescriptive quant aux modalités techniques de l'authentification forte.

En ce qui concerne l'agrément (PSIP) ou l'enregistrement (PSIC) des prestataires de services, la Banque de France est compétente pour ce qui est des aspects sécuritaires. Une fois l'agrément obtenu, la Banque de France opère un contrôle dans le temps sur la base des rapports de contrôle interne.

Dans les dispositifs de sécurité introduits par la DSP 2 figurent les interfaces sécurisées (API ou Application Programming Interface), qui devront s'interposer entre la banque et les prestataires de services de paiement tiers à compter de septembre 2019, et dont la généralisation mettra fin à la pratique du web scrapping (extraction du contenu d'un site). On se trouvera donc durant les dix-huit prochains mois dans une situation porteuse de risques. Des discussions, en cours, devraient déboucher sur l'adoption d'une API de place.

Certains enjeux de sécurité ne sont pas couverts par la DSP 2 : les comptes d'épargne et d'assurance-vie, des instruments scripturaux comme le chèque, le prélèvement et la signature du mandat SDD, qui constitue une part significative des paiements scripturaux en France (pas d'authentification forte).

Jean-Claude Huyssen - ACPR

La DSP 2 vise à une meilleure harmonisation des paiements dans l'Union européenne, notamment au travers des exigences à l'encontre des six types d'acteurs (dont cinq existaient au sens de la première DSP).

Les établissements de paiement sont soumis aux exigences les plus élevées : capital minimum, fonds propres pour certains services, protection des fonds, lutte contre le blanchiment d'argent, assurance

responsabilité civile pour certaines activités, avis de la Banque de France sur la sécurité. Les établissements dont le volume de paiement n'excède pas 3 millions par mois bénéficient d'un agrément simplifié.

Sont exemptés d'agrément des fournisseurs de services (VTC, livraison de repas…) travaillant pour un réseau limité d'accepteurs ou pour l'acquisition d'un éventail limité de biens et services (ces notions sont précisées par la position 2017P-01 de l'ACPR). Les opérateurs de télécommunication sont exemptés dans le cadre de dons, services numériques ou tickets électroniques payés par leurs clients, sous réserve de ne pas dépasser certains seuils.

L'harmonisation européenne passe aussi par le renforcement des pouvoirs de l'Autorité bancaire européenne (ABE). L'ABE publiera un registre des établissements de paiement, sera compétente pour régler les différends entre autorités nationales, préparera les textes d'application manquants et rédigera des orientations (guidelines).

La DSP 2, par ailleurs, favorise l'innovation (initiation de paiement, agrégation) sans sacrifier la sécurité. Ces deux prestations sont soumises à des exigences en matière de capital, de contrôle interne, de lutte contre le blanchiment d'argent, ou encore de responsabilité civile (opérations de paiement non autorisées, pas ou mal exécutées, accès non autorisé ou frauduleux aux données des comptes de paiement…). Les prestataires sont en outre contrôlés, sur pièces et sur place, peuvent être frappés de mesures contraignantes, voire de suspension ou de retrait d'agrément. Ils sont enfin tenus de procéder à des notifications préalables (nomination d'un dirigeant effectif, changement de forme juridique, prise de contrôle…).

Fabrice Denèle - Natixis Payment Solutions

Les banques, qui demeurent responsables en dernier ressort dans le domaine des paiements, ont œuvré dans deux directions à l'occasion de l'élaboration de la DSP 2 : ne pas être en retard par rapport aux avancées techniques et ne pas scléroser le parcours du client ; lutter contre ce que l'on ne peut admettre, par exemple la pratique du web scraping (les banques ont milité dès avant la DSP 2 pour le développement des API, ce qui se traduira de facto par la disparition du web scraping).

Plusieurs failles de sécurité demeurent : i) le registre européen des prestataires (publié par l'Autorité bancaire européenne) n'est pas en temps réel : une banque ne peut pas être certaine que tel prestataire est agréé ii) il n'existe pas de procédure de résolution des conflits entre les banques et les prestataires

(initiateurs, agrégateurs) iii) en matière d'authentification forte, la DSP 2 a-t-elle anticipé les nouveaux standards EMV (Europay Mastercard Visa) ? iv) le mandat SDD ouvre la voie à de nouveaux types de fraude s'il n'y a pas de dispositif d'authentification forte adapté v) dans le cadre du paiement instantané européen, le remplacement de l'Iban par un numéro de téléphone peut créer une situation alarmante s'il n'est pas fait usage de tokens vi) en matière de protection des données personnelles, le niveau de connaissance des consommateurs est très faible.

Avec la DSP 2, on a peut-être créé des brèches dans la sécurité en allant trop vite. Est-on certain, par ailleurs, que les nouveaux acteurs sachent exactement le ou les services qu'ils souhaitent proposer ?

Valérie Pozzo di Borgo – EY Société d'Avocats

On assiste, notamment avec la DSP 2 et le règlement général sur la protection des données (RGPD), à l'émergence d'un droit de la digitalisation. Les deux textes ont des objectifs communs : i) étendre le champ d'application territoriale ii) favoriser la circulation des données personnelles bancaires (les données bancaires sont des données personnelles au sens du RGPD) iii) protéger le consentement du client iv) renforcer la sécurité v) favoriser la dématérialisation des relations contractuelles.

La présence de ces deux textes pose la question de l'articulation du droit des personnes, en matière d'information, de gestion du consentement (le consentement est exprès dans les deux textes) et d'exercice de ces droits.

Directive et règlement convergent pour ce qui est de la sécurité (mesures, notifications).

D'autres textes traitent de la sécurité des paiements électroniques : i) le décret du 18 septembre 2017 relatif à la présomption de fiabilité de la signature électronique ii) l'ordonnance du 4 octobre 2017 relative à la dématérialisation des relations contractuelles dans le secteur financier iii) la décision 2017-09 de l'ACPR à propos de l'obligation d'information précontractuelle et contractuelle.

Bertrand Pineau - FEVAD

Pour les paiements à distance, outre les deux éléments sur trois (possession, connaissance, inhérence) caractérisant l'authentification forte, la DSP 2 impose l'établissement d'un lien entre les éléments d'authentification et les données de transaction (montant, bénéficiaire).

Les transactions peuvent être exemptées d'authentification forte sous quatre motifs principaux : petits montants, en deçà d'un certain seuil de fraude, paiement récurrent, bénéficiaires de confiance. Mais le périmètre des exemptions n'est pas encore tout à fait délimité au regard des standards techniques réglementaires existants.

A l'heure actuelle, l'utilisation fréquente du 3D Secure est limitée à quelques cas de paiement via browser (navigateur) : paiement invité, paiement à partir d'un espace client, et plus rarement paiement par wallet du commerçant ou par wallet tiers.

Les paiements par carte bancaire à distance déclenchés par le commerçant sont fortement menacés par les standards techniques réglementaires, en dehors des paiements récurrents à montants fixes. L'impact sur le taux de transformation pourrait donc être fort en présence de paiements uniques (en fin de prestation, paiement de facture complémentaire (location de véhicules), paiement no show) et en présence de paiements récurrents concernant des montants variables (abonnement à montant variable, paiements échelonnés avec remboursement, paiement à la livraison).

Damien Guermonprez - Lemonway

Lemonway, l'un des premiers établissements de paiement agréé par l'Autorité de contrôle prudentiel et de résolution et qui peut exercer partout dans l'Union européenne grâce au passeport européen, s'est spécialisé dans le collecte pour compte de tiers. La société fournit des services aux plates-formes de crowfunding (qui ne peuvent pas collecter les fonds directement et doivent cantonner les fonds reçus), aux places de marché et au commerce en ligne. Lemonway fournit des services de paiement et effectue pour le compte de ses clients les diligences liées aux obligations de connaissance du client (KYC).

Les limites de la mise en œuvre de la DSP 2 sont nombreuses. On a par exemple affaire à une Union européenne à deux vitesses s'agissant du degré d'exigence des autorités de contrôle : de nombreux nouveaux acteurs des paiements se font agréés à Malte, à Chypre, à Gibraltar…Comment l'ACPR peut-elle contrôler ces acteurs ? Les approches des autorités de contrôle diffèrent selon les pays : au Royaume-Uni par exemple, le superviseur délègue beaucoup aux banques ; en Italie, seules les banques peuvent servir les plates-formes de crowdfunding equity. En matière de connaissance du client (KYC), les règles et pratiques varient sensiblement d'un pays à l'autre.

Les recommandations de Lemonway : i) mutualiser les listes noires ii) mettre à la disposition des établissements de paiement et des établissements de monnaie électronique les fichiers accessibles aux banques (Ficoba) iii) développer l'intelligence artificielle et l'utiliser dans le cadre de la lutte contre la fraude.

Clément Coeurdeuil - Budget Insight

Budget Insight effectue la collecte sécurisée de données (données d'identification, données bancaires et de placement, données de transfert) auprès de plus de cent partenaires, banques et compagnies d'assurance. Pour le client, il s'agit, au travers d'une API, de pouvoir en disposer en temps réel, sans changer d'environnement. Les services vont de la comptabilité en temps réel au conseil en temps réel, en passant par le financement en quelques secondes.

On se dirige vers une très forte segmentation de la chaîne de valeur (les banques ne sont plus les seules à pouvoir offrir un service bancaire) et l'on assiste à l'émergence de nouveaux modèles d'affaires comme le cash back.

Renaud Gruchet - Pradeo

Si les applications sont plutôt bien faites du point de la sécurité, ce n'est pas le cas du terminal qui les héberge : le téléphone portable est le maillon faible de la sécurité. C'est le constat de base de Pradeo, qui développe des dispositifs permettant de tester la robustesse des applications et de développer l'autoprotection des applications face à une menace (par blocage, par dégradation de certaines fonctions…). Il existe de nombreuses applications malveillantes, dont certaines peuvent être pilotées par des quasi amateurs, capables d'intercepter les informations sensibles.

Les applications consultables à partir des téléphones portables contiennent de très nombreuses informations sensibles, dont, par exemple, des identifiants et mots de passe. D'après un sondage réalisé pour le compte de Pradeo, une personne sur deux a déjà enregistré des identifiants, mots de passe ou copies de documents d'identité sur son téléphone portable professionnel et 43 % des informations relatives à des comptes ou cartes bancaires.