ABE/GL/2014/12_Rev1

19 décembre 2014

Orientations finales

sur la sécurité des paiements sur internet

Table des matières

Orientations sur la sécurité des paiements sur internet

Statut des présentes orientations

Le présent document contient des orientations émises conformément à l'article 16 du règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (le «règlement de l'ABE»). Conformément à l'article 16, paragraphe 3, du règlement ABE, les autorités compétentes et les établissements financiers doivent tout mettre en œuvre pour respecter ces orientations.

Les orientations exposent l'opinion de l'ABE concernant les pratiques de surveillance appropriées au sein du système européen de surveillance financière ou les modalités d'application de la législation de l'Union dans un domaine particulier. L'ABE attend dès lors de l'ensemble des autorités compétentes et établissements financiers auxquels les orientations s'adressent qu'ils s'y conforment. L'ABE demande à toutes les autorités compétentes auxquelles s'adressent ces orientations de les respecter. Les autorités compétentes concernées par les orientations doivent s'y conformer en les intégrant dans leurs pratiques de surveillance, selon les modalités qu'elles estiment appropriées (en modifiant leur cadre juridique ou leurs procédures de surveillance, par exemple).

Obligation de notification

Conformément à l'article 16, paragraphe 3, du règlement instituant l'ABE, les autorités compétentes doivent notifier avant le 5 mai 2015 à l'ABE si elles respectent ou entendent respecter les présentes orientations ou communiquent, dans le cas contraire, les motifs de leur non-respect. En l'absence de toute notification dans ce délai, les autorités compétentes seront considérées par l'ABE comme ne les respectant pas. Les notifications doivent être transmises en envoyant le formulaire fourni à la section 5 à l'adresse compliance@eba.europa.eu sous la référence: EBA/GL/2014/12. Les notifications doivent être envoyées par des personnes habilitées à rendre compte de ce respect au nom des autorités compétentes qu'elles représentent.

Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3, du règlement de l'ABE.

Titre I – Champ d'application et définitions

Champ d'application

1. Les présentes orientations établissent un ensemble d'exigences minimales en ce qui concerne la sécurité des paiements sur internet. Elles s'appuient sur les règles de la directive 2007/64/CE [1] («directive sur les services de paiement», DSP) concernant les exigences en matière d'information pour les services de paiement et les obligations des prestataires de services de paiement (PSP) pour la fourniture de services de paiement. En outre, l'article 10, paragraphe 4, de la directive prévoit que les établissements de paiement doivent disposer d'un solide dispositif de gouvernance d'entreprise et de mécanismes adéquats de contrôle interne.

2. Les orientations s'appliquent à la fourniture de services de paiement proposés sur internet par les PSP définis à l'article premier de la directive.

3. Les orientations sont destinées aux établissements financiers définis à l'article 4, paragraphe 1, du règlement (UE) n° 1093/2010, ainsi qu'aux autorités compétentes définies à l'article 4, paragraphe 2, du règlement (UE) n° 1093/2010. Les autorités compétentes dans les 28 États membres de l'Union européenne doivent garantir l'application, sous leur surveillance, des présentes orientations par les PSP définis à l'article premier de la DSP.

4. En outre, les autorités compétentes peuvent décider d'exiger que les PSP déclarent à l'autorité compétente qu'ils se conforment aux orientations.

5. Les présentes orientations n'affectent pas la validité des recommandations de la Banque centrale européenne en matière de sécurité des paiements sur internet (le «rapport»).[2] Le rapport continue notamment de constituer le document sur la base duquel les banques centrales doivent, dans le cadre de leur fonction de surveillance des systèmes et des instruments de paiement, évaluer la conformité en ce qui concerne la sécurité des paiements sur internet.

6. Les orientations représentent des attentes minimales. Elles sont sans préjudice de la responsabilité des PSP de suivre et d'évaluer les risques inhérents à leurs opérations de paiement, de définir leurs propres politiques de sécurité détaillées et de mettre en œuvre des mesures adéquates de sécurité, d'urgence, de gestion des incidents et de continuité des activités proportionnelles aux risques inhérents aux services de paiement fournis.

---

1 Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, JO L 319, du 05.12.2007,

2 http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

7. L'objectif des orientations est de définir des exigences minimales communes pour les services de paiement sur internet énumérés ci-dessous, indépendamment du dispositif d'accès utilisé :

   - [cartes] l'exécution de paiements par carte sur internet, y compris les paiements par carte virtuelle, ainsi que l'enregistrement des données de paiement par carte à utiliser dans des «solutions de portefeuille électronique»;

   - [virements] l'exécution de virements sur internet;

   - [mandat électronique] l'émission, la signature et la modification de mandats électroniques de prélèvement;

   - [monnaie électronique] le transfert de monnaie électronique entre deux comptes en monnaie électronique sur internet.

8. Lorsque les orientations indiquent un résultat, celui-ci peut être atteint par différents moyens. Outre les exigences énoncées ci-dessous, les présentes orientations fournissent également des exemples de bonnes pratiques (annexe 1), que les PSP sont encouragés à adopter, sans pour autant y être tenus.

9. Si la fourniture de services et d'instruments de paiement est proposée au moyen d'un système de paiement (par exemple, systèmes de paiement par carte, systèmes de virements, systèmes de prélèvements, etc.), les autorités compétentes et la banque centrale pertinente exerçant une fonction de surveillance des instruments de paiement doivent coopérer afin de garantir une application cohérente des orientations par les acteurs responsables du fonctionnement du système.

10. Les intégrateurs de paiement[3] proposant des services d'initiation de paiement sont considérés soit comme acquéreurs de services de paiement sur internet (et donc comme PSP) soit comme fournisseurs externes de services techniques aux systèmes concernés ou aux PSP. Dans ce dernier cas, les intégrateurs de paiement doivent être contractuellement tenus de respecter les orientations.

11. Sont exclus du champ d'application des orientations :

   - les autres services sur internet fournis par un PSP au moyen de son site internet de paiement (par exemple courtage en ligne, contrats en ligne);

   - les paiements où l'instruction est donnée par courrier, téléphone, messagerie vocale ou à l'aide d'une technologie reposant sur des SMS;

[3] Les intégrateurs de paiement fournissent au bénéficiaire (c'est-à-dire le commerçant en ligne) une interface normalisée avec les services d'initiation de paiement fournis par les PSP.

- les paiements mobiles autres que les paiements reposant sur un navigateur internet;

- les virements où un tiers de paiement a accès au compte de paiement du client;

- les opérations de paiement effectuées par une entreprise au moyen de réseaux spécialisés;

- les paiements par carte en utilisant des cartes, physiques ou virtuelles, prépayées anonymes et non rechargeables, lorsqu' il n'existe pas de relation continue entre l'émetteur et le titulaire de la carte;

- la compensation et le règlement d'opérations de paiement.

Définitions

12. Aux fins des présentes orientations, outre les définitions énoncées dans la DSP, les définitions suivantes s'appliquent :

- *Authentification*: une procédure permettant au PSP de vérifier l'identité d'un client.

- *Authentification forte du client*: aux fins des présentes orientations, une procédure reposant sur l'utilisation de deux éléments ou plus parmi les suivants – appartenant aux catégories connaissance, possession et inhérence: i) quelque chose que seul l'utilisateur connaît, par exemple, un mot de passe fixe, un code, un numéro d'identification personnel ; ii) quelque chose que seul l'utilisateur possède, par exemple un jeton (*«token»*), une carte à puce, un téléphone mobile ; iii) une propriété de l'utilisateur, par exemple une caractéristique biométrique, telle qu'une empreinte digitale. En outre, les éléments sélectionnés doivent être mutuellement indépendants, à savoir la compromission de l'un d'entre eux ne doit pas entraîner la compromission des autres. Au moins un des éléments doit être non réutilisable et non reproductible (excepté en ce qui concerne l'inhérence), ainsi que non susceptible d'être volé subrepticement sur internet. La procédure d'authentification forte doit être conçue de sorte à protéger la confidentialité des données de l'authentification.

- *Autorisation*: une procédure qui vérifie si un client ou un PSP est autorisé à effectuer une certaine action, par exemple transférer des fonds ou avoir accès à des données sensibles.

- *Données d'authentification*: les informations — généralement confidentielles — fournies par un client ou un PSP aux fins de l'authentification. Les justificatifs d'identité peuvent également inclure la possession d'un instrument physique contenant les informations (par exemple un générateur de mot de passe unique, une carte à puce) ou quelque chose que l'utilisateur mémorise ou représente (telles que des caractéristiques biométriques).

- *Incident de sécurité de paiement majeur*: un incident ayant ou susceptible d'avoir une incidence importante sur la sécurité, l'intégrité ou la continuité des systèmes relatifs aux paiements du PSP et/ou la sécurité de données de paiement sensibles ou de fonds. L'évaluation de l'importance doit tenir compte du nombre de clients potentiellement touchés, du montant sur lequel porte le risque, et de l'incidence sur d'autres PSP ou sur d'autres infrastructures de paiement.

- *Analyse du risque inhérent à l'opération*: évaluation du risque associé à une opération spécifique en tenant compte de critères tels que, par exemple, le profil des paiements du client (comportement), la valeur de l'opération concernée, le type de produit et le profil du bénéficiaire.

- *Carte virtuelle*: une solution de paiement par carte reposant sur la création d'un numéro de carte temporaire et alternatif qui peut être utilisé pour effectuer des achats sur internet. La période de validité de ce numéro de carte est réduite et son usage est limité et soumis à un plafond.

- *Solutions de portefeuille électronique*: solutions permettant à un client d'enregistrer des données se rapportant à un ou plusieurs instruments de paiement afin d'effectuer des paiements avec plusieurs commerçants en ligne.

Titre II – Orientations sur la sécurité des paiements sur internet

Environnement général de contrôle et de sécurité

Gouvernance d'entreprise

1. Les PSP doivent mettre en œuvre et réexaminer régulièrement une politique de sécurité formalisée concernant leurs services de paiement sur internet.

   1.1 La politique de sécurité doit être dûment documentée et régulièrement réexaminée (conformément à l'orientation 2.4) et approuvée par la direction générale. Elle doit définir les objectifs de sécurité et l'appétence au risque.

   1.2 La politique de sécurité doit définir les rôles et les responsabilités, y compris la fonction de gestion du risque avec une ligne hiérarchique directe au niveau de l'organe de direction, et les lignes hiérarchiques pour les services de paiement sur internet fournis, y compris la gestion des données de paiement sensibles en ce qui concerne l'évaluation, le contrôle et l'atténuation des risques.

Évaluation des risques

2. Les PSP doivent conduire et documenter des évaluations des risques exhaustives en ce qui concerne la sécurité des paiements sur internet et les services associés, tant avant la mise en place de ce(s) service(s)que régulièrement par la suite.

   2.1 Au moyen de leur fonction de gestion du risque, les PSP doivent conduire et documenter des évaluations de risques détaillées concernant les paiements sur internet et les services associés. Les PSP doivent apprécier les résultats du suivi continu des menaces pour la sécurité des services de paiement sur internet qu'ils proposent ou qu'ils ont l'intention de proposer, en tenant compte: i) des solutions technologiques qu'ils utilisent, ii) des services sous-traités à des fournisseurs externes, et iii) de l'environnement technique des clients. Les PSP doivent tenir compte des risques associés aux plates-formes technologiques sélectionnées, à l'architecture de l'application, aux techniques et aux routines de programmation tant de leur côté[4] que du côté de leurs clients,[5] ainsi que des résultats du processus de suivi des incidents de sécurité (voir orientation 3).

   2.2 Sur cette base, les PSP doivent déterminer si et dans quelle mesure il y a lieu de modifier les mesures de sécurité existantes, les technologies utilisées et les procédures ou services proposés. Les PSP doivent tenir compte du temps nécessaire pour mettre

[4] Tels que la sensibilité du système au piratage de sessions de paiement, à l'injection code SQL, aux attaques de type XSS, aux débordements de la mémoire tampon etc.

[5] Tels que les risques associés à l'utilisation d'applications multimédia, de modules d'extension de navigateur, de cadres, de liens externes etc.

en œuvre les modifications (y compris le déploiement chez les clients) et adopter les mesures provisoires appropriées afin de minimiser les incidents de sécurité et la fraude, ainsi que les éventuels effets perturbateurs.

2.3 L'évaluation des risques doit tenir compte de la nécessité de protéger et de sécuriser les données de paiement sensibles.

2.4 Les PSP doivent réexaminer les scénarios de risque et les mesures de sécurité existantes à la suite d'incidents majeurs affectant leur services, avant une modification importante de l'infrastructure ou des procédures et lorsque de nouvelles menaces sont recensées par leurs activités de suivi des risques. En outre, l'évaluation des risques doit être soumise à un réexamen général au moins une fois par an. Les résultats des évaluations et des réexamens des risques doivent être présentés à la direction générale pour approbation.

Suivi et déclaration des incidents

3. Les PSP doivent assurer de manière cohérente et intégrée le suivi, le traitement et la gestion des suites à donner aux incidents de sécurité, y compris les plaintes des clients en matière de sécurité. Les PSP doivent mettre en place une procédure pour déclarer de tels incidents à la direction et, en cas d'incidents de sécurité de paiement majeurs, aux autorités compétentes.

3.1 Les PSP doivent mettre en place un processus leur permettant de suivre, de traiter et de donner suite aux incidents de sécurité et aux plaintes des clients relatives à la sécurité et de déclarer de tels incidents à la direction.

3.2 Les PSP doivent disposer d'une procédure leur permettant de notifier immédiatement les autorités compétentes (à savoir, autorités de surveillance et de protection des données), le cas échéant, en cas d'incidents de sécurité de paiement majeurs concernant les services de paiement fournis.

3.3 Les PSP doivent disposer d'une procédure leur permettant de coopérer avec les autorités judiciaires pertinentes en cas d'incidents de sécurité de paiement majeurs, y compris la compromission de données.

3.4 Les PSP acquéreurs doivent exiger par voie contractuelle que les commerçants en ligne qui stockent, traitent ou transmettent des données de paiement sensibles coopèrent en cas d'incidents de sécurité de paiement majeurs, y compris la compromission de données, tant avec eux qu'avec les autorités judiciaires pertinentes. Si un PSP constate qu'un commerçant en ligne ne coopère pas comme prévu par le contrat, il doit prendre des mesures pour faire respecter cet engagement contractuel ou résilier le contrat.

Contrôle et atténuation des risques

4. Les PSP doivent mettre en œuvre des mesures de sécurité conformément à leurs politiques de sécurité respectives afin d'atténuer les risques recensés. Ces mesures doivent incorporer des couches multiples de défense de la sécurité, où la défaillance d'une couche de défense est rattrapée par la couche de défense suivante («défense en profondeur»).

4.1 Lorsqu'ils conçoivent, élaborent et maintiennent des services de paiement sur internet, les PSP doivent accorder une attention particulière à la séparation adéquate des fonctions dans les environnements des technologies de l'information (TI) (par exemple séparation des environnements de développement, de test et de production) et à l'application appropriée du principe de séparation des privilèges comme base d'une gestion solide des identités et des accès.[6]

4.2 Les PSP doivent mettre en place des solutions de sécurité appropriées pour protéger les réseaux, les sites internet, les serveurs et les liens de communication contre des abus ou des attaques. Les PSP doivent retirer toute fonction superflue des serveurs afin de les protéger (durcissement) et de supprimer ou de réduire les vulnérabilités des applications en risque. L'accès aux données et aux ressources nécessaires par les applications diverses doivent être maintenus au strict minimum conformément au principe du moindre privilège. Afin de limiter l'utilisation de sites internet falsifiés (imitant les sites authentiques des PSP), les sites proposant des services de paiement en ligne doivent être authentifiés par certificats établis au nom du PSP ou par d'autres méthodes d'authentification similaires.

4.3 Les PSP doivent disposer de processus appropriés afin de suivre, de poursuivre et de limiter les accès: i) aux données sensibles de paiement et ii) aux ressources logiques et physiques critiques, telles que les réseaux, les systèmes, les bases de données, les modules de sécurité, etc. Les PSP doivent constituer, stocker et analyser des fichiers historiques et des pistes d'audit appropriés.

4.4 Lorsqu'ils conçoivent,[7] élaborent et maintiennent des services de paiement sur internet, les PSP doivent veiller à ce que la minimisation des données[8] soit une composante essentielle de la fonctionnalité principale: la collecte, l'acheminement, le traitement, le stockage et/ou l'archivage, et la visualisation de données sensibles de paiement doivent être maintenus au strict minimum.

4.5 Les mesures de sécurité pour les services de paiement sur internet doivent être évaluées sous le contrôle de la fonction de gestion du risque afin de garantir leur solidité et leur efficacité. Toutes les modifications doivent être soumises à une

6 «Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job*job.* «» (Saltzer, J.H. [1974], 'Protection and the Control of Information Sharing in Multics', Communications of the ACM, Vol. 17, No 7, p. 388.)..

7 De la privacité à la conception

8 La minimisation des données fait référence à la politique consistant à collecter la plus petite quantité d'informations personnelles nécessaire pour réaliser une fonction spécifique.

procédure officielle de gestion des modifications garantissant que les modifications sont dûment planifiées, évaluées, documentées et autorisées. Sur la base des modifications effectuées et des menaces pour la sécurité observées, les évaluations doivent être répétées régulièrement et inclure des scénarios d'attaques potentielles pertinentes et connues.

4.6 Les mesures de sécurité des PSP pour les services de paiement sur internet doivent être périodiquement contrôlées afin de garantir leur solidité et leur efficacité. La mise en œuvre et le fonctionnement des services de paiement sur internet doivent également faire l'objet de contrôles. La fréquence et le centre d'attention de ces contrôles doivent tenir compte des risques de sécurité et être proportionnels à ceux-ci. Les contrôles doivent être réalisés par des experts fiables et indépendants (internes ou externes). Ces experts ne doivent pas participer de quelque manière que ce soit à l'élaboration, à la mise en œuvre ou à la gestion opérationnelle des services de paiement sur internet fournis.

4.7 Lorsque les PSP sous-traitent des fonctions associées à la sécurité des services de paiement sur internet, les contrats doivent inclure des dispositions exigeant le respect des principes et des orientations énoncés dans les présentes orientations.

4.8 Les PSP proposant des services d'acquisition doivent exiger, par contrat, que les commerçants en ligne qui manient (à savoir, stockent, traitent ou transmettent) des données de paiement sensibles mettent en œuvre des mesures de sécurité dans leur infrastructure TI, conformément aux orientations 4.1 à 4.7, afin d'éviter le vol de ces données sensibles de paiement dans leur systèmes. Si un PSP se rend compte qu'un commerçant en ligne n'a pas mis en place les mesures de sécurité prévues, il doit prendre des mesures pour faire respecter cet engagement contractuel ou résilier le contrat.

Traçabilité

5. Les PSP doivent mettre en place des processus garantissant que toutes les opérations, ainsi que la cinématique du mandat électronique, sont dûment tracées.

5.1 Les PSP doivent veiller à ce que leurs services incorporent des mécanismes de sécurité pour l'enregistrement de données détaillées des opérations et des mandats électroniques, y compris le numéro d'ordre de l'opération, l'horodatage des données des opérations, les modifications de paramètres ainsi que l'accès aux données des opérations et des mandats électroniques.

5.2 Les PSP doivent utiliser des fichiers-journaux permettant de tracer tout ajout, toute modification ou tout effacement des données des opérations ou des mandats électroniques.

5.3 Les PSP doivent soumettre à requêtes et analyser les données des opérations et des mandats électroniques et s'assurer de disposer d'instruments pour analyser les fichiers-journaux. Les applications correspondantes ne doivent être disponibles utilisables que par le personnel autorisé.

Mesures de contrôle et de sécurité spécifiques pour les paiements sur internet

Identification initiale du client, informations

6. Les clients doivent être dûment identifiés conformément à la réglementation européenne en matière de lutte anti-blanchiment[9] et confirmer leur volonté de procéder à des paiements sur internet en utilisant les services avant que l'accès à de tels services leur soit accordé. Les PSP doivent fournir au client des informations adéquates «préalables», «régulières» ou, le cas échéant, «ad hoc» concernant les exigences nécessaires (par exemple, équipement, procédures) pour réaliser des opérations sécurisées de paiement sur internet et les risques inhérents.

6.1 Les PSP doivent s'assurer que le client a bien été soumis aux procédures de vigilance à l'égard de la clientèle et qu'il a fourni des documents d'identité adéquats[10] et des informations pertinentes avant d'obtenir accès aux services de paiement sur internet.[11]

6.2 Les PSP doivent veiller à ce que les informations préalables[12] fournies au client contiennent des détails spécifiques concernant les services de paiement sur internet. Ces informations doivent inclure, selon le cas:

- des informations claires sur les éventuelles exigences en matière d'équipement du client, de logiciel ou d'autres outils nécessaires (par exemple un logiciel antivirus, un pare-feu);

- des consignes sur l'utilisation appropriée et sécurisée des données d'authentification;

9 Par exemple la directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme. JO L 309, du 25.11.2005, pp. 15-36. Voir également la directive de la Commission 2006/70/CE du 1er août 2006 portant mesures de mise en œuvre de la directive 2005/60/CE du Parlement européen et du Conseil pour ce qui concerne la définition des «personnes politiquement exposées» et les conditions techniques de l'application d'obligations simplifiées de vigilance à l'égard de la clientèle ainsi que de l'exemption au motif d'une activité financière exercée à titre occasionnel ou à une échelle très limitée. JO L 214, du 4.8.2006, pp. 29-34.

10 Par exemple un passeport, une carte d'identité nationale ou une signature électronique avancée.

11 Le processus d'identification du client est sans préjudice des éventuelles dérogations prévues par la réglementation en matière de lutte anti-blanchiment en vigueur. Les PSP ne sont pas tenus d'appliquer une procédure distincte d'identification du client pour les services de paiement sur internet, à condition qu'une telle identification du client ait déjà été réalisée, par exemple pour d'autres services existants relatifs aux paiements ou pour l'ouverture d'un compte.

12 Ces informations complètent l'article 42 de la DSP spécifiant les informations que les PSP doivent fournir à l'utilisateur du service de paiement avant la conclusion d'un accord relatif à la fourniture de services de paiement.

- une description des étapes de la procédure à suivre par le client pour initier et autoriser une opération de paiement et/ou obtenir des informations, y compris les conséquences de chaque action;

- des consignes sur l'utilisation appropriée et sécurisée de tout matériel ou logiciel fourni au client;

- les procédures à suivre en cas de perte ou de vol des données d'authentification ou du matériel ou du logiciel du client utilisés pour entrer en communication avec le système ou effectuer des opérations;

- les procédures à suivre en cas d'abus détecté ou soupçonné;

- une description des responsabilités et des engagements respectifs du PSP et du client concernant l'utilisation du service de paiement sur internet.

6.3 Les PSP doivent veiller à ce que le contrat-cadre conclu avec le client spécifie que le PSP peut bloquer une opération spécifique ou l'instrument de paiement[13] sur la base de considérations de sécurité. Il doit spécifier la méthode et les conditions de la notification du client et comment le client peut contacter le PSP pour obtenir le déblocage de l'opération de paiement sur internet ou du service, conformément à la DSP.

[13] Voir l'article 55 de la DSP sur les limitations de l'utilisation des instruments de paiement.

Authentification forte du client

7. L'initiation de paiements sur internet, ainsi que l'accès aux données sensibles de paiement, doivent être protégés par une authentification forte du client. Les PSP doivent mettre en place une procédure d'authentification forte du client conformément à la définition prévue par les présentes orientations.

   7.1 [virement/mandat électronique/monnaie électronique] Les PSP doivent procéder à une authentification forte du client pour l'autorisation des opérations de paiement sur internet du client (y compris des virements groupés) et pour l'émission ou la modification de mandats électroniques de prélèvement. Or, les PSP peuvent envisager d'adopter des mesures alternatives d'authentification du client pour:

   - les paiements en émission vers des bénéficiaires de confiance figurant dans des listes blanches préalablement établies pour ce client;
   - les opérations entre deux comptes du même client détenus auprès du même PSP;
   - les virements au sein du même PSP justifiés par une analyse du risque inhérent à l'opération;
   - les paiements de faibles montants tels que visés dans la DSP.[14]

   7.2 L'accès aux données sensibles de paiement ou leur modification (y compris la création et la modification des listes blanches) exigent une authentification forte du client. Si un PSP ne propose que des services purement consultatifs, n'affichant pas d'informations sensibles concernant le client ou le paiement, telles que les données de paiement d'une carte qui pourraient facilement être utilisées de manière abusive à des fins de fraude, le PSP peut adapter ses exigences d'authentification sur la base de son évaluation des risques.

   7.3 [cartes] Pour les opérations effectuées par carte, tous les PSP émetteurs de cartes doivent rendre possible l'authentification forte du titulaire de la carte. Toutes les cartes émises doivent être techniquement prêtes (enregistrées) à être utilisées suite à l'authentification forte de leurs titulaires.

   7.4 [cartes] Les PSP proposant des services d'acquisition doivent faciliter la mise en œuvre de technologies permettant à l'émetteur de procéder à une authentification forte du titulaire de la carte pour les systèmes de paiement par carte auxquels participe l'acquéreur.

   7.5 [cartes] Les PSP proposant des services d'acquisition doivent exiger que leurs commerçants en ligne favorisent des solutions permettant à l'émetteur de procéder à

[14] Voir la définition des instruments de paiement relatifs à des montants faibles prévue à l'article 34, paragraphe 1, et à l'article 53, paragraphe 1, de la DSP.

une authentification forte du titulaire de la carte pour les opérations effectuées par carte sur internet. L'utilisation de mesures d'authentification alternatives peut être envisagée pour des catégories prédéfinies d'opérations à faible risque, par exemple sur la base d'une analyse du risque inhérent à l'opération, ou pour des opérations concernant des paiements de faibles montants tels que prévus par la DSP.

7.6 [cartes] Pour les systèmes de paiement par carte acceptés par le service, les fournisseurs de solutions de portefeuille électronique doivent exiger une authentification forte de la part de l'émetteur lorsque le titulaire légitime enregistre pour la première fois les données de la carte.

7.7 Les fournisseurs de solutions de portefeuille électronique doivent favoriser une authentification forte du client lorsque les clients entrent en communication avec les services de paiement par portefeuille électronique ou effectuent des opérations par carte sur internet. L'utilisation de mesures d'authentification alternatives peut être envisagée pour des catégories prédéfinies d'opérations à faible risque, par exemple sur la base d'une analyse du risque inhérent à l'opération, ou pour des opérations concernant des paiements relatifs à de faibles montants, tels que prévus par la DSP.

7.8 [cartes] Pour les cartes virtuelles, l'enregistrement initial doit être effectué dans le cadre d'un environnement sûr et de confiance.[15] Une authentification forte du client doit être exigée pour le processus de génération des données de la carte virtuelle si la carte est émise dans l'environnement internet.

7.9 Les PSP doivent s'assurer qu'une authentification bilatérale appropriée est bien mise en œuvre lorsqu'ils communiquent avec des commerçants en ligne aux fins d'initier des paiements sur internet et d'avoir accès à des données sensibles de paiement.

Demande et fourniture d'outils d'authentification et/ou logiciel livré au client

8. Les PSP doivent veiller à ce que la demande de la part du client et la fourniture initiale des outils d'authentification requis pour utiliser le service de paiement sur internet et/ou la livraison au client du logiciel relatif aux paiements sont effectuées de manière sécurisée.

8.1 La demande et la fourniture d'outils d'authentification et/ou le logiciel relatif aux paiements livré au client doivent répondre aux exigences suivantes:

[15] Les environnements relevant de la responsabilité du PSP et assurant l'authentification adéquate du client et du PSP proposant le service et la protection des informations confidentielles/sensibles incluent : i) les locaux du PSP ; ii) la banque en ligne ou autre site internet sécurisé, par exemple si le AG propose des caractéristiques de sécurité comparables, entre autres, comme prévu à l'orientation 4 ; ou iii) les services de guichet automatique de banque (GAB). (En cas de GAB, une authentification forte du client est requise. Une telle authentification est généralement fournie par puce et code PIN ou puce et données biométriques).

- les procédures associées doivent être appliquées dans un environnement sûr et de confiance tout en tenant compte des risques éventuels découlant de dispositifs que le PSP ne contrôle pas;

- des procédures efficaces et sécurisées doivent être mises en place pour la remise des données d'authentification, du logiciel relatif aux paiements et de tous les dispositifs personnalisés relatifs au paiement sur internet. Le logiciel livré par internet doit également comporter la signature numérique du PSP afin de permettre au client de vérifier qu'il est authentique et qu'il n'a pas été altéré;

- [cartes] pour les opérations effectuées par carte, le client doit avoir la possibilité de s'inscrire dans le dispositif d'authentification forte indépendamment d'un achat spécifique sur internet. Si l'activation est proposée pendant la réalisation des achats en ligne, elle doit être effectuée en redirigeant le client vers un environnement sûr et de confiance.

8.2 [cartes] Les émetteurs doivent encourager activement leurs titulaires de cartes à s'inscrire dans leurs dispositifs d'authentification forte et à ne permettre à leurs titulaires de cartes de contourner une telle inscription que dans des cas exceptionnels et limités en nombre, si cela est justifié par le risque inhérent à l'opération spécifique effectuée par carte.

Tentatives de connexion, délais d'expiration des sessions, validité de l'authentification

9. Les PSP doivent limiter le nombre de tentatives de connexion ou d'authentification, définir des règles pour les délais d'expiration des sessions de services de paiement sur internet et fixer des limites à la durée de validité de l'authentification.

9.1 Lorsqu'un mot de passe à usage unique est utilisé à des fins d'authentification, les PSP doivent veiller à ce que le délai de validité du mot de passe soit limité au strict minimum.

9.2 Les PSP doivent définir le nombre maximal d'échecs de connexion de connexion ou d'authentification suite auxquelles l'accès au service de paiement sur internet est (provisoirement ou définitivement) suspendu. Ils doivent mettre en place une procédure sécurisée pour réactiver les services de paiement sur internet suspendus.

9.3 Les PSP doivent définir la période maximale à l'issue de laquelle les sessions inactives de services de paiement sur internet sont automatiquement fermées.

Suivi des opérations

10. Les mécanismes de suivi des opérations conçus pour prévenir, détecter et bloquer les opérations de paiement frauduleuses doivent être activés avant l'autorisation du paiement par le PSP; les opérations suspectes ou à risque élevé doivent faire l'objet d'une procédure

spécifique de criblage et d'évaluation. Des mécanismes équivalents de surveillance et d'autorisation doivent également être mis en place lors de l'émission des mandats électroniques.

10.1 Les PSP doivent utiliser des systèmes de détection et de prévention de la fraude pour détecter les opérations suspectes avant que le PSP n'autorise définitivement les opérations ou les mandats électroniques. Ces systèmes doivent reposer par exemple sur des règles paramétrées (telles que des listes noires de données de cartes compromises ou volées), et utiliser des outils de détection des comportements anormaux concernant le client ou le dispositif d'accès du client (tel un changement d'adresse *Internet Protocol* [IP][16] ou de plage IP pendant la session du service de paiement internet, détecté parfois par un contrôle de géolocalisation IP,[17] des catégories atypiques de commerçants en ligne pour un client spécifique ou des données d'opération inhabituelles, etc.). De tels systèmes doivent également être en mesure de détecter des signes d'infection par un logiciel malveillant pendant la session (par exemple, à l'aide d'outils permettant de déterminer si l'interlocuteur est un homme ou une machine) et des scénarios de fraude connus. Tout en respectant la réglementation pertinente en matière de protection des données, l'étendue, la complexité et l'adaptabilité des solutions de suivi doivent être proportionnelles au résultat de l'évaluation du risque.

10.2 Les PSP acquéreurs doivent mettre en place des systèmes de détection et de prévention des fraudes afin de suivre les activités des commerçants en ligne.

10.3 Les PSP doivent conduire toute procédure de criblage et d'évaluation des opérations dans un délai approprié afin de ne pas retarder indûment l'initiation et/ou l'exécution du service de paiement concerné.

10.4 Si le PSP décide, conformément à sa politique en matière de risques, de suspendre une opération de paiement qui a été identifiée comme potentiellement frauduleuse, le PSP doit maintenir la suspension pendant une période aussi brève que possible jusqu'à ce que les questions de sécurité aient été traitées.

Protection de données sensibles de paiement

11. Les données sensibles de paiement doivent être protégées lorsqu'elles sont stockées, traitées ou transmises.

11.1 Toutes les données utilisées afin d'identifier et d'authentifier les clients (par exemple, au moment de l'entrée en communication, lorsqu'ils initient des paiements sur internet ou lorsqu'ils émettent, modifient ou annulent des mandats électroniques),

[16] Une adresse IP est un code numérique unique identifiant chaque ordinateur connecté à internet.

[17] Un contrôle de géolocalisation IP vérifie si le pays d'émission correspond à l'adresse IP à partir de laquelle l'utilisateur initie l'opération.

ainsi que l'interface client (PSP ou site internet d'un commerçant en ligne), doivent être dûment protégées contre les risque de vol, et d'accès non autorisés ou de modification.

11.2 Lorsqu'ils échangent des données sensibles de paiement par internet, les PSP doivent s'assurer de l'application d'un chiffrement sécurisé de bout en bout[18] entre les parties communicantes pendant toute la durée de la session de communication concernée, afin de protéger la confidentialité et l'intégrité des données, en utilisant des techniques de chiffrement robustes et largement reconnues.

11.3 Les PSP proposant des services d'acquisition doivent encourager leurs commerçants en ligne à ne pas stocker de données sensibles de paiement. Si les commerçants en ligne manient, à savoir conservent, traitent ou transmettent des données sensibles de paiement, les PSP concernés doivent exiger, par contrat, que les commerçants en ligne mettent en place les mesures nécessaires pour protéger ces données. Les PSP doivent effectuer des contrôles réguliers, et si un PSP se rend compte qu'un commerçant en ligne maniant des données sensibles de paiement n'a pas mis en place les mesures de sécurité requises, il doit prendre des mesures pour faire respecter cet engagement contractuel ou résilier le contrat.

[18] Le chiffrement de bout en bout est un chiffrement effectué à l'intérieur du ou au niveau du système source, associé à un chiffrement effectué uniquement à l'intérieur du ou au niveau du système de destination. ETSI EN 302 109 V1.1.1. (2003-06).

Sensibilisation et éducation du client et communication avec le client

Éducation du client et communication avec le client

12. Les PSP doivent fournir aide et orientation aux clients, lorsque cela est nécessaire, en ce qui concerne l'utilisation sécurisée des services de paiement sur internet. Les PSP doivent communiquer avec leurs clients et les rassurer quant à l'authenticité des messages qu'ils reçoivent.

12.1 Les PSP doivent fournir à tout le moins un canal sécurisé[19] pour les communications régulières avec les clients concernant l'utilisation correcte et sécurisée du service de paiement sur internet. Les PSP doivent informer les clients de l'existence de ce canal et expliquer que tout message de la part du PSP reçu par d'autres moyens, tel que le courrier électronique, concernant l'utilisation correcte et sécurisée du service de paiement sur internet, n'est pas fiable. Le PSP doit expliquer:

- la procédure à appliquer par les clients souhaitant déclarer au PSP des paiements (suspectés) frauduleux, des incidents suspects ou des anomalies pendant la session des services de paiement sur internet et/ou les éventuelles tentatives d'ingénierie sociale[20];
- les étapes suivantes, à savoir comment le PSP répondra au client;
- comment le PSP informera le client des opérations (potentiellement) frauduleuses ou de leur non-initiation ou avertira le client des attaques survenues [par exemple, courriels de hameçonnage («*phishing*»)].

12.2 Les PSP doivent maintenir les clients informés, au moyen du canal sécurisé, des actualisations des procédures de sécurité concernant les services de paiement sur internet. Les éventuelles alertes concernant des risques émergents significatifs (par exemple des avertissements à propos d'ingénierie sociale) doivent également être données au moyen du canal sécurisé.

12.3 Les PSP doivent proposer une assistance à la clientèle pour toutes questions, plaintes, demandes de soutien et notifications d'anomalies ou d'incidents concernant les services de paiement sur internet et les services associés, et les clients doivent être dûment informés des modalités d'utilisation de cette aide.

12.4 Les PSP doivent lancer des programmes d'éducation et de sensibilisation des clients conçus de sorte à garantir que les clients comprennent, au minimum, la nécessité:

---

19 Tel qu'une boîte aux lettres spécialisée sur le site internet du PSP ou un site internet sécurisé.

20 Dans ce cadre, ingénierie sociale signifie les techniques de manipulation des individus afin d'obtenir des informations (par exemple, par courriel ou appels téléphoniques), ou d'extraction d'informations des réseaux sociaux à des fins de fraude ou afin d'obtenir un accès non autorisé à un ordinateur ou à un réseau.

- de protéger leurs mots de passe, leurs jetons («*tokens*») de sécurité, leurs informations personnelles et autres données confidentielles;

- de gérer dûment la sécurité de leur dispositif personnel (par exemple l'ordinateur) en installant et en actualisant les composantes de sécurité (antivirus, pare-feu, correctifs de sécurité);

- de tenir compte des menaces et risques significatifs liés au téléchargement de logiciels sur internet, si le client ne peut pas être raisonnablement certain que le logiciel est authentique et qu'il n'a pas été altéré;

- d'utiliser le site authentique de paiement sur internet du PSP.

12.5 Les PSP acquéreurs doivent exiger que les commerçants en ligne distinguent clairement les processus relatifs aux paiements du magasin virtuel afin de permettre aux clients de se rendre compte plus facilement qu'ils communiquent avec le PSP et non pas avec le bénéficiaire (par exemple en redirigeant le client et en ouvrant une fenêtre distincte afin que le processus de paiement ne soit pas affiché dans une fenêtre du commerçant en ligne).

Notifications, fixation de limites

13. Les PSP doivent fixer des limites pour les services de paiement sur internet et peuvent proposer à leurs clients des options pour limiter davantage les risques à l'intérieur de ces limites. Ils peuvent également fournir des services d'avertissement et de gestion du profil des clients.

13.1 Afin de fournir des services de paiement sur internet à un client, les PSP doivent fixer des limites[21] applicables à ces services (par exemple un montant maximal pour chaque paiement individuel ou un montant cumulé au cours d'une certaine période) et doivent informer leurs clients en conséquence. Les PSP doivent permettre aux clients de mettre hors service la fonctionnalité de paiement sur internet.

Accès du client aux informations sur le statut de l'initiation et de l'exécution du paiement

14. Les PSP doivent confirmer à leurs clients l'initiation du paiement et fournir aux clients en temps utile les informations nécessaires pour vérifier qu'une opération de paiement a été correctement ouverte et/ou exécutée.

14.1 [virement/mandat électronique] Les PSP doivent fournir aux clients un dispositif fonctionnant presque en temps réel leur permettant de vérifier le statut de l'exécution

[21] Ces limites peuvent s'appliquer globalement (c'est-à-dire à tous les instruments de paiement permettant d'effectuer des paiements sur internet) ou individuellement.

des opérations ainsi que les soldes des comptes à tout moment [22] dans un environnement sûr et de confiance.

14.2 Les éventuels relevés électroniques détaillés doivent être mis à disposition dans un environnement sûr et de confiance. Si les PSP informent leurs clients de la disponibilité de relevés électroniques (par exemple, régulièrement, lorsqu'un relevé électronique périodique a été émis sur une base ad hoc après l'exécution d'une opération) au moyen d'un canal alternatif, tel que SMS, courriel ou lettre, les données sensibles de paiement ne doivent pas être incluses dans ces communications ou, si elles le sont, elles doivent être masquées.

Titre III – Dispositions finales et mise en œuvre

15. Les présentes orientations s'appliquent à partir du 01.08.2015.

[22] Exception faite de la non-disponibilité exceptionnelle du dispositif pour motif d'entretien technique ou en raison d'incidents majeurs.

Annexe 1: Exemples de bonnes pratiques

Outre les exigences énoncées ci-dessus, dans les présentes orientations sont décrites quelques bonnes pratiques que les PSP et les acteurs des marchés pertinents sont encouragés à adopter, sans pour autant y être tenus. Afin de faciliter les références, les chapitres auxquels s'appliquent ces bonnes pratiques sont explicitement indiqués.

Environnement général de contrôle et de sécurité

Gouvernance d'entreprise

BP 1: La politique de sécurité peut être définie dans un document spécifique.

Contrôle et atténuation des risques

BP 2: Les PSP peuvent fournir des outils de sécurité (par exemple, dispositifs et/ou navigateurs personnalisés dûment sécurisés) pour protéger l'interface client contre l'emploi illicite ou les attaques (par exemple, attaques de type «man in the browser» - homme dans le navigateur).

Traçabilité

BP 3: Les PSP proposant des services d'acquisition peuvent exiger, par contrat, que les commerçants en ligne stockant des informations de paiement mettent en place des processus adéquats favorisant la traçabilité.

Mesures de contrôle et de sécurité spécifiques pour les paiements sur internet

Identification initiale du client, informations

BP4: Le client peut signer un contrat de service spécifique relatif à la réalisation d'opérations de paiement sur internet qui remplacerait les conditions incluses dans un contrat de service plus général conclu avec le PSP.

BP5: Les PSP peuvent également veiller à fournir à leurs clients, sur une base continue ou, le cas échéant, de manière ponctuelle, et par des moyens appropriés (par exemple des brochures, des pages de sites internet), des instructions claires et simples expliquant leurs responsabilités en ce qui concerne l'utilisation sécurisée du service.

Authentification forte du client

BP6: [cartes] Les commerçants en ligne peuvent favoriser une authentification forte du titulaire de la carte par l'émetteur pour les opérations effectuées par carte sur internet.

BP7: Pour la commodité des clients, les PSP peuvent envisager d'utiliser un outil unique d'authentification forte du client pour l'ensemble des services de paiement sur internet. Cela pourrait favoriser l'acceptation de la solution par les clients et faciliter sa bonne utilisation.

BP8: L'authentification forte du client peut inclure des éléments liant l'authentification à un montant et à un bénéficiaire spécifiques. Cela pourrait renforcer le degré de certitude des clients lorsqu'ils autorisent des paiements. La solution technologique permettant de lier les données d'authentification forte aux données de l'opération doit être inviolable.

Protection de données de paiement sensibles

BP 9: Il est souhaitable que les commerçants en ligne maniant des données sensibles de paiement dispensent une formation appropriée à leur personnel chargé de la gestion du risque de fraude et mettent régulièrement à jour cette formation afin de garantir que son contenu demeure pertinent dans un environnement de sécurité dynamique.

Éducation du client et communication avec le client

BP 10: Il est souhaitable que les PSP proposant des services d'acquisition organisent des programmes de formation sur la prévention de la fraude à l'attention de leurs commerçants en ligne.

Notifications, fixation de imites

BP 11: Dans le cadre des limites fixées, les PSP peuvent fournir à leurs clients la possibilité de gérer les limites des services de paiement sur internet dans un environnement sûr et de confiance.

BP 12: Les PSP peuvent mettre en œuvre des alertes à l'attention de leurs clients, par exemple par appel téléphonique ou SMS, en cas d'opérations de paiement suspectes ou à risque élevé sur la base de leurs politiques de gestion du risque.

BP 13: Les PSP peuvent permettre aux clients de spécifier des règles générales personnalisées comme paramètres de leur comportement en ce qui concerne les paiements sur internet et les services associés, par exemple qu'ils n'initieront des paiements qu'à partir de pays spécifiques et que les paiements initiés à partir d'autres lieux devront être bloqués ou qu'ils peuvent inclure des bénéficiaires spécifiques dans des listes blanches ou des listes noires.