BANQUE DE FRANCE

EUROSYSTÈME

RÉFÉRENTIEL DE SÉCURITÉ DES INTERFACES D'ACCÈS AUX COMPTES DE PAIEMENT

FÉVRIER 2019

Table des matières

1 INTRODUCTION

La fourniture de nouveaux services de paiement (initiation de paiement, information sur les comptes), ainsi que le service permettant la confirmation de la disponibilité des fonds, issus de la transposition de la directive (UE) 2015/2366 concernant les services de paiement dans le marché intérieur (DSP 2) nécessite qu'un prestataire de services de paiement (dit « tiers ») accède à des comptes de paiement et à leurs informations gérés par d'autres prestataires de services de paiement (dit « gestionnaires de comptes »).

Ces activités étant jugées risquées en matière de lutte contre la fraude, la DSP 2, le règlement délégué (UE) 2018/389 ainsi que le décret n°2018-1228 du 24 décembre 2018 encadrent la fourniture de ces services.

Lors de la transposition de cette directive en droit français par l'ordonnance n°2017-1252 du 9 août 2017, les principes de fourniture de ces services ont été codifiés dans la partie législative du code monétaire et financier dans une nouvelle section 13 intitulée « Modalités d'accès aux comptes de paiement » du chapitre III du Titre III du Livre 1er. Le décret n°2018-1228 du 24 décembre 2018 a été codifié dans la partie réglementaire du code monétaire et financier dans une nouvelle section 12 intitulée « Modalités d'accès aux comptes de paiement » du chapitre III du Titre III du Livre 1er.

La Banque de France s'est vue confier la mission de s'assurer de la sécurité de l'accès aux comptes de paiement et à leurs informations ainsi que de s'assurer de la pertinence des normes applicables en la matière (*cf.* article L. 521-8 du code monétaire et financier). Pour l'exercice de cette mission, la Banque de France se fait communiquer, par les prestataires de services de paiement ou par toute personne intéressée, les informations utiles concernant l'accès aux systèmes de paiement et à leurs informations ainsi qu'à tous les dispositifs techniques qui y sont associés. Si elle estime que les conditions d'accès à un compte de paiement présentent des garanties de sécurité insuffisantes, elle peut recommander à un prestataire de service de paiement de prendre toutes mesures destinées à y remédier. Si ces recommandations n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations du prestataire de service de paiement, décider de formuler un avis négatif publié au Journal officiel.

Les articles 30 à 36 du règlement délégué (UE) 2018/389 précisent les exigences spécifiques relatives aux normes ouvertes communes et sécurisées de communication prévues à l'article 98 de la DSP2 afin que les prestataires de services de paiement fournissant les services d'initiation de paiement et d'information sur les comptes ainsi que les émetteurs d'instruments de paiement liés à une carte, puissent communiquer avec les utilisateurs de services de paiement et les prestataires de services de paiement gestionnaires de comptes.

Le « Référentiel de sécurité des interfaces d'accès aux comptes de paiement » (RSIAC) a pour objet de préciser les objectifs de sécurité des interfaces d'accès au sens des articles 30 à 36 du règlement délégué (UE) 2018/389. Conformément à l'article D. 113-10 du code monétaire et financier, l'évaluation de la conformité d'une interface dédiée lancée par un prestataire de service de paiement gestionnaire de comptes au RSIAC est effectuée par un centre d'évaluation agréé par l'Agence nationale de la sécurité des systèmes d'information.

Le rapport d'évaluation est destiné à la Banque de France pour s'assurer de la sécurité de l'interface d'accès.

Pour toute information complémentaire concernant le référentiel de sécurité des interfaces d'accès aux comptes de paiement, veuillez contacter 2323-SURV-UT@banque-france.fr.

2 PÉRIMÈTRE

Les objectifs de sécurité présentés dans le RSIAC s'appliquent à tous les prestataires de services de paiement qui mettent à disposition une interface dédiée exemptée de mesures d'urgences au sens de l'article 33.6 du règlement délégué (UE) 2018/389 (*cf.* article D. 133-10 du code monétaire et financier).

Le RSIAC s'adresse aux prestataires de services de paiement établis sur le territoire de la France et agréés par l'Autorité de contrôle prudentiel et de résolution, ou dont le dossier d'agrément est en cours de traitement et qui effectuent des test d'utilisation de l'interface dédiée.

Les objectifs de sécurité sont formulés de façon à être indépendants des techniques employées pour leur mise en œuvre et doivent être considérés comme un minimum requis pour la sécurité de l'accès aux comptes de paiement par des prestataires de services de paiement tiers. Ces objectifs pourront faire l'objet d'une révision en fonction d'une révision du règlement délégué (UE) 2018/389.

Les prestataires de services de paiement doivent s'attacher à intégrer les objectifs de sécurité à l'ensemble des processus liés à la fourniture des services d'information sur les comptes, d'initiation de paiement ou de confirmation de la disponibilité des fonds.

En application de l'article 237 de l'arrêté du 3 novembre 2014, un prestataire de services de paiement qui externalise des prestations de service demeure pleinement responsable de toutes les obligations qui lui incombent. Le prestataire de service de paiement doit alors s'assurer que les mesures mises en place par ses prestataires et opérateurs techniques, au titre de la fourniture des services d'initiation de paiement, d'information sur les comptes ou de confirmation de la disponibilité des fonds, sont conformes aux objectifs de sécurité énoncés dans le présent référentiel.

Les objectifs de sécurité n'ont pas vocation à traiter :

- les exigences en matière de performance et de disponibilité de l'interface d'accès prévues par le règlement délégué (UE) 2018/389, dont le contrôle relève de la compétence de l'Autorité de contrôle prudentiel et de résolution ;
- des obligations spécifiques des prestataires de services de paiement assujettis en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, qui relèvent de dispositions légales et réglementaires particulières.

3 MISE EN ŒUVRE

Le RSIAC présente sept objectifs de sécurité s'appliquant à l'ensemble des opérations nécessaire à la fourniture des services d'initiation de paiement, d'information sur les comptes ou de vérification de la disponibilité des fonds.

La vérification du respect de la mise en œuvre de ces objectifs est assurée par la Banque de France, conformément au mandat qui lui a été confié par l'article L. 521-8 du code monétaire et financier.

À cette fin, conformément au 5° de l'article D. 133-10 du code monétaire et financier, le rapport d'évaluation à la conformité aux objectifs du RSIAC fait partie du dossier de demande d'exemption de mesures d'urgence prévu au 6 de l'article 33 du règlement délégué (UE) 2018/389. Le rapport d'évaluation est utilisé par la Banque de France pour délivrer à l'Autorité de contrôle prudentiel et de résolution un avis sur la sécurité de l'interface dédiée.

4 OBJECTIFS DE SÉCURITÉ

4.1 Objectif de sécurité 1 : Gouvernance et organisation

Compte tenu des interactions entre les prestataires de services gestionnaires de comptes, les prestataires de services de paiement fournissant le service d'information sur les comptes, les prestataires de paiement fournissant le service d'initiation de paiement, la sécurité globale est conditionnée par une coopération réelle entre les acteurs. À partir de ce fondement, la gouvernance de la sécurité vise à assurer que les mesures de sécurité sont en place, optimales et appropriées.

EXG 1.1. La politique de gouvernance des interfaces d'accès (dénommées ci-après interfaces de programmation applicative, ou API) est formalisée par les prestataires de services gestionnaires de comptes et régulièrement actualisée. Elle définit le cycle de vie ainsi que la politique de sécurité globale de ces API.

EXG 1.2. Le cycle de vie d'une API définit au minimum les phases suivantes : développement, test, publication et maintenance. La sécurisation est une activité transverse à toutes les phases du cycle de vie et doit être prise en compte dès la conception.

EXG 1.3. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que la politique de gestion des versions multiples d'API en production, la durée de support de ces différentes versions et leur décommissionnement soient clairement formalisés.

4.2 Objectif de sécurité 2 : Évaluation des risques

La gestion de la sécurité repose sur l'identification des ressources à protéger associée à une analyse des risques encourus ainsi qu'à la mise en place de mesures organisationnelles, techniques et procédurales en vue d'assurer cette protection. Elle prévoit une évaluation périodique des mesures déployées en vue de leur efficacité.

EXG 2.1. Les prestataires de services de paiement gestionnaires de comptes conduisent et documentent une évaluation de l'ensemble des risques associés à la sécurité des ressources tout au long de leur cycle de vie. Cette évaluation, qui inclut l'identification des risques majeurs, est régulièrement actualisée.

EXG 2.2. Les prestataires de services de paiement gestionnaires de comptes exercent une activité de veille qui leur permet d'adapter les protections dont bénéficient leurs ressources en fonction de l'évolution des techniques de cyberattaque et de fraude, afin que les mesures de protection demeurent en permanence pertinentes.

4.3 Objectif de sécurité 3 : Contrôle et encadrement des risques

Les prestataires de services de paiement gestionnaires de comptes doivent mettre en œuvre des mesures de sécurité adéquates en vue d'encadrer les risques identifiés.

EXG 3.1. Les prestataires de services de paiement gestionnaires de comptes s'assurent de la mise en œuvre de mesures de sécurité adaptées à la nature et l'importance des risques identifiés et vérifient que ces mesures :

a. sont sous la supervision de l'entité en charge des fonctions de contrôle permanent ;

b. sont testées par le responsable de la sécurité afin de valider leur robustesse, leur efficacité (dispositif de contrôle permanent) et leur conformité ;

c. font régulièrement l'objet d'une procédure de mise à jour.

4.4 Objectif de sécurité 4 : Identification

Les prestataires de services de paiement fournissant le service d'information sur les comptes, les prestataires de services de paiement fournissant le service d'initiation de paiement et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte sont en mesure de s'identifier auprès du prestataire de services de paiement gestionnaire du compte.

EXG 4.1. Les prestataires de services de paiement gestionnaires de comptes s'assurent que les certificats des prestataires de services de paiement tiers soient des certificats qualifiés au sens du règlement (UE) n° 910/2014.

EXG 4.2. Les prestataires de services de paiement gestionnaires de comptes s'assurent que les prestataires de services de paiement tiers utilisent un certificat qualifié d'authentification de site internet pour sécuriser la couche de transport et un certificat qualifié de cachet électronique pour signer électroniquement le contenu des messages échangés.

EXG 4.3. Les prestataires de services de paiement gestionnaires de comptes sont en mesure de vérifier la validité en cours des agréments des prestataires de services de paiement tiers.

EXG 4.4. Les prestataires de services de paiement gestionnaires de comptes sont en mesure de vérifier la validité en cours des certificats qualifiés présentés par les prestataires de services de paiement tiers.

EXG 4.5. Les prestataires de services de paiement gestionnaires de comptes rendent l'ensemble des procédures d'authentification proposées aux utilisateurs de services de paiement utilisable par les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement aux fins de l'authentification des utilisateurs de services de paiement.

EXG 4.6. Les prestataires de services de paiement gestionnaires de comptes sont en capacité de commencer l'authentification forte sur la requête d'un prestataire de services d'initiation de paiement ou d'un prestataire de services d'information sur les comptes qui a préalablement recueilli le consentement de l'utilisateur.

4.5 Objectif de sécurité 5 : Sécurité des flux et des sessions de communication

Les prestataires de services de paiement veillent à ce que les risques que la communication soit déviée vers des tiers non autorisés dans le cadre d'applications mobiles, ou d'autres interfaces pour utilisateurs de services de paiement, proposant des services de paiement électronique soient efficacement réduits.

EXG 5.1. Les prestataires de services de paiement gestionnaire de comptes disposent de moyens de sécuriser les flux de communication au niveau de la couche application du modèle OSI (Open Systems Interconnection).

EXG 5.2. Les prestataires de services de paiement gestionnaire de comptes disposent de moyens de supervision des flux et d'alerte afin de détecter un incident. Toutes les données transitant par les flux de communication sont soumises systématiquement à une analyse de contenu à la recherche de codes malveillants.

EXG 5.3. Lors de l'échange de données, un chiffrement sécurisé doit être utilisé entre les prestataires de services de paiement gestionnaires de comptes et les prestataires de services de paiement tiers tout au long de la session de communication.

EXG 5.4. Les prestataires de services de paiement gestionnaire de comptes mettent en place une protection conforme à l'état de l'art contre des attaques de type déni de service.

EXG 5.5. Les prestataires de services de paiement gestionnaires de comptes s'assurent que le protocole de communication d'échange avec les prestataires de services de paiement tiers permette de sécuriser les transferts de données au niveau de la couche transport du modèle OSI.

EXG 5.6. Les solutions dont dépend le déploiement de la solution de chiffrement sécurisé sont tenues à jour.

EXG 5.7. Les prestataires de service de paiement gestionnaires de comptes garantissent l'intégrité et la confidentialité des données de sécurité personnalisées et des codes d'authentification qui transitent par les flux de communication ou qui sont stockés dans l'infrastructure technique de leurs systèmes d'information.

EXG 5.8. Les sessions de communication entre le prestataire de services de paiement gestionnaire du compte, le prestataire de services d'information sur les comptes, le prestataire de services d'initiation de paiement et tout utilisateur de services de paiement concerné sont établies et maintenues tout au long de l'authentification.

4.6 Objectif de sécurité 6 : Traçabilité

Les prestataires de services de paiement mettent en place des procédures qui garantissent que l'ensemble des opérations de paiement et des autres interactions avec l'utilisateur de services de paiement, avec d'autres prestataires de services de paiement et avec d'autres entités, dans le cadre de la fourniture du service de paiement, sont traçables, afin que l'ensemble des événements en rapport avec l'opération électronique durant ses différentes phases soient connus a posteriori.

EXG 6.1. Les prestataires de services de paiement veillent à ce que toute session de communication avec l'utilisateur de services de paiement, y compris des commerçants, d'autres prestataires de services de paiement et d'autres entités, s'appuie sur chacun des éléments suivants:

a. un identifiant unique, non prédictible, de la session;

b. des mécanismes de sécurité pour l'enregistrement détaillé de l'opération, y compris le numéro de l'opération, les horodatages et toutes les données pertinentes de l'opération;

c. des horodatages qui sont fondés sur un système unifié de représentation du temps et qui sont synchronisés conformément à un signal horaire officiel.

EXG 6.2. Les cas d'erreur et événements imprévus au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information sont traçables et contiennent toutes les données pertinentes à des fins d'audits.

EXG 6.3. En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information, le prestataire de services de paiement gestionnaire du compte envoie un message de notification au prestataire de services d'initiation de paiement ou au prestataire de services d'information sur les comptes et au prestataire de services de paiement qui émet des instruments de paiement liés à une carte, en indiquant les raisons de l'erreur ou de l'événement imprévu.

4.7 Objectif de sécurité 7 : Interopérabilité

EXG 7.1. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leurs interfaces d'accès suivent des normes de communication publiées par des organisations européennes ou internationales de normalisation.

EXG 7.2. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que les spécifications techniques des interfaces d'accès fassent l'objet d'une documentation mentionnant une série de routines, de protocoles et d'outils dont les prestataires de services de paiement fournissant le service d'initiation de paiement, les prestataires de services de paiement fournissant le service d'information sur les comptes et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte, ont besoin pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes des prestataires de services de paiement gestionnaires de comptes.