MECANISMES DE TRAITEMENT DES FLUX DE PAIEMENT DU E-COMMERCE EN CAS DE DEFAUT DES INFRASTRUCTURES OU DES DISPOSITIFS D'AUTHENTIFICATION

La 2ème directive sur les services de paiement prévoit un recours systématique à l'authentification forte du payeur lors d'un paiement initié en ligne, sauf cas d'exemption dûment justifié. À cet égard, le plan de migration de Place validé par l'Observatoire prévoit en cible l'utilisation généralisée du protocole 3D-Secure, notamment sous sa version 2 qui permet au commerçant de choisir entre demande d'authentification forte et demande d'exemption.

Cette utilisation plus systématique du protocole 3D-Secure rend le secteur du e-commerce dépendant du bon fonctionnement des infrastructures d'authentification, notamment les serveurs d'authentification des banques (ACS / *Authentication Control Servers*) et les serveurs de routage des flux 3D-Secure mis en place par les schemes (DS / *Directory Servers*). Ces infrastructures ayant pris une dimension systémique pour le e-commerce, il s'agit d'assurer la capacité pour les marchands à poursuivre leurs opérations en cas de défaillance d'un des maillons de la chaine d'authentification.

À cet effet, il est proposé aux membres du GT migration de valider la mise en œuvre des mesures de continuité ci-dessous, visant respectivement les ACS des banques et les DS des *schemes*. Il est attendu des acteurs de marché que ces mécanismes soient implémentés dès que possible, et pleinement opérationnels au plus tard au 1er trimestre 2021.

A – PRINCIPES COMMUNS APPLICABLES EN CAS D'INCIDENT

La survenance d'un incident affectant les infrastructures et dispositifs d'authentification, quelle qu'en soit l'origine, doit entrainer sans délai la mise en œuvre des diligences suivantes (et ce même dans l'hypothèse où les mécanismes présentés ci-après ne pourraient pas être activés) :

- **La suspension du mécanisme d'émission de message de *soft decline* par les établissements émetteurs** : si le niveau de risque d'une transaction donnée est jugé trop élevé, la banque doit alors privilégier l'émission d'un message de *hard decline* ;

- L**'évaluation du degré de criticité de l'incident, afin d'assurer le cas échéant la notification d'incident majeur à l'autorité compétente en la matière** (au titre de la DSP2 pour les PSP et/ou au titre du cadre de surveillance de l'Eurosystème pour les *schemes*).

31, RUE CROIX-DES-PETITS-CHAMPS – 75049 PARIS CEDEX 01
CODE COURRIER : 11-2324 – TÉL : 01 42 92 96 13 – TÉLÉCOPIE : 01 42 92 31 74

B - MÉCANISMES DE TRAITEMENT EN CAS D'INCIDENT AFFECTANT LE DOMAINE « ÉMETTEUR »

Du côté des émetteurs des cartes, les ACS sont chargés de traiter les flux d'authentification 3D-Secure en provenance des e-commerçants, et donc de procéder soit à l'authentification forte du payeur, soit de valider le recours à une exemption. En cas d'incident affectant les ACS ou un autre composant du domaine 3D-Secure émetteur, les demandes d'authentification restent sans réponse au niveau des émetteurs, et sont ainsi mises en échec ; par ailleurs, en cas d'indisponibilité de la solution d'authentification forte, le porteur ne peut pas finaliser sa transaction.

1. Incident affectant les infrastructures du domaine émetteur

Afin d'assurer la capacité des commerçants à émettre des transactions en cas de défaillance d'un ACS ou d'un autre composant du domaine émetteur, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau du *scheme* :

- En cas d'absence de réponse de l'ACS après un délai prédéfini (*timeout* strictement encadré par les règles du *scheme*), le *scheme* qui traite la transaction est invité à se substituer à l'ACS par l'émission d'un cryptogramme d'authentification, quel que soit le contexte de la transaction (montant, score de risque, transfert de responsabilité);
- Cette émission doit être assortie d'un indicateur permettant à l'émetteur d'identifier qu'il s'agit d'une transaction bénéficiant du mécanisme de *fallback* émetteur ;
- De façon optionnelle et comme pour toute autre transaction, le *scheme* peut accompagner cette réémission d'informations à valeur ajoutée : niveau de risque, éligibilité de la transaction à une exemption d'authentification forte…

Au niveau des serveurs d'autorisation (SAE) des banques émettrices :

- Évaluation du niveau de risque de la transaction en *fallback* émetteur et validation le cas échéant de la transaction même si elle n'est pas éligible à une exemption ; cette évaluation devra prendre en compte le cas échéant les implications futures de l'opération (en cas d'initiation de série d'opérations récurrentes ou de mandat de MIT par exemple) ;
- Les transactions issues du mécanisme de *fallback* émetteur ne doivent donner lieu à aucune émission de *soft decline* : si le niveau de risque est jugé trop élevé, la banque doit émettre un message de *hard decline* ;
- Les transactions autorisées non exemptées d'authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement ;
- Les conditions du transfert de responsabilité restent inchangées selon les règles du *scheme*.

Les établissements émetteurs sont tenus :

(i) de veiller à la bonne utilisation de ce mécanisme par les *schemes* afin d'assurer qu'il ne soit pas mis en œuvre en dehors des plages d'indisponibilité de leur ACS,

(ii) d'accepter de manière proportionnée aux risques les demandes d'autorisation.

(iii) d'évaluer la criticité de l'incident au regard des critères établis par l'Autorité bancaire européenne (EBA/GL/2017/10) et le cas échéant le notifier comme incident opérationnel ou de sécurité majeur à la Banque de France et à l'Autorité de contrôle prudentiel et de résolution (ACPR)[1]

[1] Les incidents opérationnels et de sécurité majeurs des prestataires de services de paiement doivent être notifiés au titre de l'article L.521-10 du code monétaire et financier, mettant en application les critères des orientations de l'Autorité bancaire européenne (EBA/GL/2017/10). Les notifications sont à transmettre par le biais d'une interface sécurisée dédiée, conformément aux orientations de l'Autorité Bancaire Européenne en la matière. Les PSP sont invités à transmettre toute demande de documentation par courriel à l'adresse suivante : 2323-NOTIFICATIONS-UT@banque-france.fr

De leur côté, les *schemes* mettent en place une surveillance des taux de réponse des émetteurs sur les transactions bénéficiant du mécanisme de *fallback* émetteur.

2. Incident affectant les solutions d'authentification forte de l'émetteur

Afin d'assurer la capacité des porteurs à s'authentifier pour valider leurs transactions en cas d'indisponibilité de leur solution d 'authentification, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau des serveurs d'authentification (ACS) des banques émettrices :
- Activation d'un dispositif d'authentification de secours, relevant potentiellement de l'authentification simple (de type SMS-OTP) en cas d'indisponibilité d'une solution d'authentification forte alternative ;
- Les transactions n'ayant pas fait l'objet d'une authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement ;
- Du point de vue des règles de responsabilité applicables, la transaction doit être considérée comme fortement authentifiée du point de vue des *schemes*.

Les établissements émetteurs sont tenus de veiller à la bonne utilisation de ce mécanisme, afin d'assurer (i) qu'il est mis en œuvre de façon diligente en cas d'incident identifié et (ii) qu'il ne soit pas utilisé en dehors des plages d'indisponibilité des solutions d'authentification forte.

La nature de l'incident sur les solutions d'authentification forte de l'émetteur est également susceptible de faire l'objet d'une notification à la Banque de France et à l'ACPR au titre des incidents majeurs.

C - MÉCANISMES DE TRAITEMENT EN CAS D'INCIDENT AFFECTANT LE DOMAINE « ACCEPTEUR »

Du côté des *schemes*, les *Directory Servers* sont chargés de router les flux de paiement 3D-Secure en provenance des e-commerçants vers les ACS des banques émettrices. En cas d'incident affectant les DS ou la *gateway* d'accès, les paiements 3D-Secure ne peuvent être réalisés.

Afin d'assurer la capacité des commerçants à émettre des transactions en cas de défaillance d'un *Directory Server* ou *de leur gateway d'accès*, l'Observatoire recommande la mise en place des mécanismes suivants :

Au niveau du *scheme* :
- Mise en place d'un indicateur permettant d'identifier les demandes d'autorisation bénéficiant du mécanisme de *fallback* accepteur.

Au niveau des commerçants :
- Sous réserve de faisabilité au regard du règlement IFR (notamment en cas d'absence de sélection active de la marque par le consommateur), bascule sur le deuxième *scheme* si la carte est co-badgée ;
- En cas d'incapacité à émettre une transaction via 3D-Secure, émission de la transaction directement en autorisation en l'identifiant comme relevant du mécanisme de *fallback* accepteur.

Au niveau des serveurs d'autorisation (SAE) des banques émettrices :
- Évaluation du niveau de risque de la transaction en *fallback* accepteur et validation le cas échéant de la transaction même si elle n'est pas éligible à une exemption ; cette évaluation devra prendre en compte le cas échéant les implications futures de l'opération (en cas d'initiation de série d'opérations récurrentes ou de mandat de MIT par exemple) ;
- Les transactions issues du mécanisme de *fallback* accepteur ne doivent donner lieu à aucune émission de *soft decline* : si le niveau de risque est jugé trop élevé, la banque doit émettre un message de *hard decline* ;

- Les transactions autorisées non exemptées d'authentification forte doivent être déclarées comme non authentifiées pour motif « Autre » dans la cartographie semestrielle des flux de paiement.

Les établissements acquéreurs sont tenus de veiller à la bonne utilisation de ce mécanisme par leurs commerçants, afin d'assurer qu'il ne soit pas mis en œuvre en dehors des plages d'indisponibilité des *Directory Servers* ou de leurs *gateways* d'accès.

De leur côté, les établissements émetteurs sont tenus d'accepter de manière proportionnée aux risques les demandes d'autorisation.

Enfin, les *schemes* mettent en place une surveillance du taux d'utilisation de ce dispositif côté acquéreur et des taux de réponse des émetteurs. Ils sont également tenus de notifier à l'Eurosystème, le cas échéant via la Banque de France comme surveillant principal, les incidents majeurs affectant leurs infrastructures dans le cadre du « *Major incident reporting framework for payment schemes and retail payment systems* » (2018).