IMPACTS DE LA DIRECTIVE EUROPEENNE PSD2

an atos company

Worldline

TABLE DES MATIÈRES

01 Introduction

Ce document a pour but d'exposer aux commerçants utilisant les services de paiement de Worldline les implications de la directive européenne PSD2.

Il contient une présentation générale de ce qu'est la directive PSD2 et des implications spécifiques pour les commerçants offrant des services de paiement de proximité (dans le magasin) ou à distance (e-Commerce). Dans ce contexte, les évolutions des règles des schémas de paiement induites par cette nouvelle directive sont prises en compte et mentionnées si utiles.

Le document précise également les mesures que Worldline demande aux commerçants de prendre afin d'être prêts par rapport à la directive PSD2 et aux nouvelles règles des schémas de paiement.

02 Contexte réglementaire

2.1 PSD2 et EBA RTS

La directive sur les services de paiement (UE) 2015/2366 révisée, appelée PSD2, est entrée en vigueur le 13 janvier 2018.

Plusieurs éléments de cette réglementation ont un impact pour les commerçants. L'un des objectifs les plus importants de la nouvelle directive concerne la protection du client payeur à travers quelques règles : son information, son consentement et son authentification forte (obligatoire en B2C).

L'Autorité Bancaire Européenne (EBA) a précisé certaines exigences de la directive à travers des spécifications techniques (RTS), notamment celles relative à l'authentification forte (SCA) du porteur de carte qui sera applicable à partir du 14 septembre 2019.

2.2 Couverture géographique

La directive PSD2 s'applique à toutes les transactions de paiement au sein de l'Espace Economique Européen (EEE/EEA en anglais), c'est-à-dire l'Union Européenne, Royaume-Uni inclus (au minimum jusqu'au Brexit), la Norvège, le Liechtenstein et l'Islande.

En ce qui concerne l'authentification forte du porteur de carte (SCA), celle-ci s'applique lorsque l'acquéreur et l'émetteur sont situés dans l'EEA. En revanche, si l'un d'eux se situe hors de l'EEA, elle n'est plus obligatoire. Par exemple, un commerçant dont l'acquéreur est Worldline Belgique doit permettre une authentification forte pour un porteur de carte dont la banque est localisée en France, mais pas nécessairement pour un acheteur dont la banque est localisée aux Etats-Unis, en Suisse ou en Chine. Dans le cas particulier d'un porteur de carte dont la banque est localisée au Royaume-Uni, l'authentification forte est obligatoire au minimum jusqu'à la mise en application du Brexit.

2.3 Les obligations depuis mi-janvier 2018

De nouvelles règles doivent être mises en œuvre depuis janvier 2018 ; elles concernent principalement l'information et le consentement du payeur.

L'information du payeur
Le payeur doit être informé des conditions de son acte de paiement. Cela concerne, par exemple,

- le délai final d'exécution du paiement (par exemple, dans le cas d'un paiement à la livraison),
- le montant pré-autorisé ou réservé lors d'une réservation (par exemple, lors du check-in dans un hôtel ou lors de l'achat d'essence sur un distributeur automatique de carburant, où le montant final de la transaction n'est pas connu à l'avance),
- les frais de change ou le taux de change,
- ou encore les frais supplémentaires (surcharging) ou les réductions liées à l'utilisation d'un moyen de paiement, quand ceci est autorisé par l'Etat où exerce le commerçant.

Pour les transactions, lorsque Worldline n'est pas en mesure d'informer le consommateur (par exemple, sur Internet quand la page de paiement n'est pas présentée par Worldline) ou lorsque l'information n'est pas connue de Worldline (par exemple, date de livraison, frais de change quand ceux-ci sont calculés par le commerçant, surcharging), c'est au commerçant lui-même d'informer le consommateur (éventuellement via son PSP).

Le consentement du payeur
Le payeur doit donner un consentement explicite à chaque transaction de paiement ou de pré-autorisation en sa présence. Pour une transaction de proximité en mode contact, le consentement est matérialisé, par exemple, par l'introduction du code secret ou l'insertion de la carte après visualisation du montant (ex. sur automate de péage autoroutier). Pour une transaction de proximité en mode sans contact, la présentation de la carte à proximité du terminal après visualisation du montant équivaut au consentement du porteur. Dans le cas de la vente sur internet, ceci peut être fait en invitant le porteur de carte à approuver les données de la transaction en cliquant sur un bouton.

2.4 L'obligation d'authentification forte à compter de septembre 2019

L'authentification forte du porteur de carte (SCA) vise à réduire les taux de fraude. Elle sera obligatoire à compter du 14 septembre 2019 lorsqu'un porteur de carte initie un paiement électronique, pour le montant exact du paiement, pour le montant pré-autorisé en cas de réservation, pour la totalité d'une série de paiements (sachant que dans ce cas, tout changement des conditions, nécessitera une nouvelle authentification).

Qu'est-ce que l'authentification forte ?

L'utilisateur doit utiliser deux facteurs d'authentification parmi les trois suivants :
- Ce qu'il sait (mot de passe, code PIN) – connaissance
- Ce qu'il possède (une carte, un téléphone mobile) – possession
- Ce qu'il est (biométrie, ex : empreinte digitale, scan de l'iris) – inhérence

L'authentification forte du porteur s'applique tant au paiement de proximité qu'au paiement à distance. Par exemple, sur un terminal de paiement, l'insertion d'une carte à puce et la saisie d'un code secret sont considérées comme une méthode d'authentification forte.

Dans le cadre du paiement à distance, l'utilisation d'un mot de passe statique pour une authentification vis-à-vis de la banque du porteur n'est pas considérée comme étant une authentification forte. Par contre, l'usage d'un équipement capable de générer un code d'authentification dynamique spécifique à chaque transaction ou d'un smartphone couplé à une reconnaissance faciale ou de l'empreinte digitale est considéré comme une authentification forte.
Il est attendu que les banques généralisent à terme le déploiement de méthodes conviviales d'authentification par biométrie (par exemple, empreinte digitale, reconnaissance faciale) sur le smartphone du client, ce qui devrait aider à une plus grande acceptation de ces mécanismes par les consommateurs.

La PSD2 a défini également des cas où l'authentification forte du porteur de carte ne s'applique pas :
- Lorsque la banque du payeur (l'émetteur) ou du payé (l'acquéreur) se situe hors de l'EEA,
- Lorsque le paiement est initié par le payé (par exemple : un prélèvement/direct debit/ domiciliation)
- Aux paiements sur support papier (chèques, TIP)
- A la vente-à-distance par courrier ou par téléphone.
- Lorsqu'une exemption définie par le RTS SCA peut s'appliquer, par exemple dans le cadre du paiement sur automate relatif au transport (ex : péage autoroutier) ou au parking.

Il est important de noter que les exceptions au procédé d'authentification forte ne sont pas obligatoires.

Rappelons que les exemptions ne sont pas systématiques et que même si les conditions d'exemption sont remplies, la décision finale revient à l'émetteur (la banque du payeur) qui peut l'accorder ou non en fonction de ses propres critères (capacité technique à la gérer, risque de fraude, modalités convenues avec le porteur de carte, ...).

2.5 Le rôle des schémas de paiement

Les acquéreurs de transactions par carte de paiement (ex. Worldline) et les émetteurs de cartes de paiement se doivent de respecter :
- La loi en vigueur (ex. PSD2)
- Les règles des schémas de paiement des cartes dont ils proposent les services à leurs clients, qui par principe doivent être conformes aux exigences des législateurs ou régulateurs.

A titre d'exemple, le RTS prévoit une exemption pour du paiement de proximité sans contact, avec des montants plafonds à respecter. Un schéma de paiement peut décider d'imposer des règles plus restrictives à ses membres. De même, un émetteur peut aussi décider, pour des raisons qui lui sont propres, de mettre en œuvre des solutions plus contraignantes, par exemple dans ce cas, des plafonds plus faibles que ceux imposés par le schéma de paiement, ceux-ci ne pouvant pas dépasser ceux fixés par le RTS. Ceci peut avoir pour conséquence que le commerçant pourrait constater des comportements différents des cartes de ses clients (par exemple, telle carte acceptée sans code secret pour une transaction sans contact de 45€, alors qu'une autre carte demande le code secret pour ce même montant).

2.6 Les différents types d'exemptions d'authentification forte

2.6.1 Exemptions d'authentification forte pour des paiements de proximité

Le RTS prévoit 2 possibilités d'exemption pour des paiements de proximité, en plus de celles définies ci-avant :
- Pour des transactions sans contact de petit montant ;
- Pour des transactions relatives au transport ou au parking sur automate de paiement

L'exemption pour transaction sans contact peut être invoquée :
- Si le montant de la transaction est inférieur à 50€ ;
- Si depuis la dernière transaction avec authentification forte du porteur, le montant maximum de transactions sans contact, quel que soit le marchand, ou le nombre de transactions sans contact ne dépasse pas un plafond (critères de vélocité) défini par le RTS (max 150 € ou 5 transactions, au choix de l'émetteur qui peut également abaisser ces plafonds).

Seul l'émetteur peut valider les critères de vélocité. Dès lors, sur le terminal de paiement, la transaction sans contact pourra être initiée sans demande d'introduction du code secret, mais l'émetteur pourrait devoir la refuser ou demander l'introduction du code secret sur le terminal, selon le résultat de la validation des critères de vélocité.

2.6.2 Exemptions d'authentification forte pour des paiements à distance

Le RTS prévoit 5 possibilités d'exemption pour des paiements à distance (e/commerce), en plus de celles définies ci-avant (§2.4) :
- Bénéficiaires de confiance ou White-Listing
- Transactions récurrentes
- Transactions de petit montant
- Corporate payments
- Analyse de risque transactionnel

Bénéficiaire de confiance ou White-Listing
Le white-listing est la possibilité pour un porteur de carte de désigner, auprès de l'émetteur de sa carte, en général sa banque, un marchand dans lequel il a confiance et pour lequel il ne souhaite pas réaliser une authentification forte lors de l'exécution de transactions à distance, pour autant que cela réponde aux critères de sécurité établis par la banque.

Les schémas de paiement internationaux recommandent aux émetteurs de carte (les banques) de prévoir, lors de la phase d'authentification du porteur auprès de sa banque durant l'exécution d'une transaction 3D Secure, d'ajouter une case à cocher dans laquelle le payeur peut demander d'intégrer le marchand dans sa liste de bénéficiaires de confiance (la white liste).
Les schémas de paiement envisagent que le marchand puisse être informé, en réponse à l'exécution de la transaction, qu'il se trouvait dans la white-liste du consommateur.

La règlementation prévoit également que le porteur puisse, à tout moment, retirer un commerçant de sa liste de bénéficiaires de confiance, ce qui se fera très certainement depuis la banque en ligne.

L'exemption pour bénéficiaire de confiance (White List) est certainement la méthode la plus simple pour un commerçant de bénéficier de l'exemption d'authentification forte. Elle repose cependant sur :
- La confiance accordée par les consommateurs au commerçant,
- L'information du payeur par le commerçant pour l'encourager à l'inscrire dans la liste blanche,
- La capacité de la banque à gérer les listes blanches et la facilité d'inscription,
- Et à la banque du consommateur qui décide, in fine, d'accorder ou de refuser l'exemption pour chaque transaction.

Transactions récurrentes
Une exemption d'authentification forte s'applique pour les séries de transactions à distance d'un même montant vers un même bénéficiaire. Cependant, une authentification forte est requise pour la première transaction (le contrat) ou à chaque modification des conditions de la série.

Transactions de petit montant
L'exemption d'authentification forte pour transaction à distance de petit montant peut être invoquée :
- Si le montant de la transaction est inférieur à 30€ ;
- Si depuis la dernière transaction avec authentification forte du porteur, le montant maximum de transactions de transactions de petit montant à distance, quel que soit le marchand, ou le nombre de transactions de petit montant à distance ne dépasse pas un plafond (critères de vélocité) défini par le RTS SCA (max 100 € ou 5 transactions, au choix de l'émetteur qui peut également abaisser ces plafonds).

Seul l'émetteur peut valider les critères de vélocité. Dès lors, il est recommandé d'exécuter la transaction de façon à permettre à l'émetteur de décider s'il peut appliquer ou non l'exemption, et si ce n'est pas le cas, d'initier alors une session d'authentification forte avec le porteur de carte.

Les paiements « Secure Corporate »
Des exemptions sont valables aussi pour les paiements initiés par les entreprises avec débit du compte de l'entreprise (par exemple, cartes logées, comptes centralisés et cartes virtuelles). En revanche, les cartes corporate (avec débit du compte bancaire de l'employé selon conditions particulières) sont assimilées à des transactions B2C et ne font pas l'objet de dérogations particulières.

Exemption pour analyse de risque transactionnel (TRA)
L'exemption d'authentification forte pour transaction à distance dénommée « analyse de risque » peut être invoquée par l'acquéreur (pour le compte du commerçant) et par l'émetteur lorsque les deux conditions suivantes sont remplies :
1. Que la transaction soit déclarée sûre (par exemple, pas d'infection du poste de l'utilisateur par un malware, pas de dépenses anormales du payeur, localisation du payeur, historique des transactions,...)
2. Que le taux de fraude (pour les transactions à distance) de l'établissement de paiement (et non du marchand ou de son PSP) soit en dessous de plafonds prédéterminés :
   - 0,13% si le montant de la transaction est inférieur à 100 euros
   - 0,06% si le montant de la transaction est inférieur à 250 euros
   - 0,01% si le montant de la transaction est inférieur à 500 euros
   - Exemption non applicable pour les transactions de plus de 500 euros

Comme nous le verrons plus loin, il est recommandé d'initier la transaction en mode 3D Secure afin de permettre soit au commerçant qu'il souhaite bénéficier de cette exemption, soit à l'émetteur d'appliquer de lui-même l'exemption s'il remplit les conditions et le juge approprié pour son client, le porteur de carte.

03 La prise en compte de PSD2 par les schémas de paiement

Caractéristiques de 3D Secure 2.0

Les schémas de paiement internationaux ont défini, au sein d'EMVco, leur organisme de standardisation, une évolution majeure de la spécification 3D Secure, appelée 3DS 2.0, utilisée pour le paiement à distance. 3DS 2.0 a pour but principal de réduire la fraude des paiements à distance tout en augmentant fortement la convivialité pour le porteur de carte, notamment en fournissant à l'émetteur plus d'informations sur le contexte de la transaction afin de permettre à ce dernier de décider s'il convient ou non de procéder à une authentification forte du porteur de carte, ou encore en standardisant le processus d'authentification du porteur depuis son smartphone.

Cette nouvelle version apporte principalement les avantages suivants :

- La logique d'échange d'informations entre le PSP du commerçant et l'émetteur est adaptée et enrichie afin de fournir à l'émetteur un nombre plus élevé d'informations contextuelles relatives à la transaction en cours, ceci afin de lui permettre d'affiner son estimation de risque et dès lors de décider s'il peut ne pas procéder à une authentification forte du porteur de carte, pour autant qu'il réponde aux conditions d'exemption.
- Une intégration dans les applications mobiles permettant une expérience utilisateur plus conviviale depuis son smartphone. Ainsi, l'intégration optimisée de 3D-secure peut permettre :
  - L'initiation de l'authentification au travers de l'application (mode embedded) : c'est-à-dire que le composant 3D-secure du commerçant et l'application dialogue directement avec le moyen d'authentification, sans qu'il y ait besoin que le payeur soit redirigé sur le site web de l'émetteur (par exemple, pour un achat in-app, l'application pourrait déclencher une vérification de l'empreinte digitale, tenant lieu d'authentification 3D-secure, à condition que l'émetteur le permette).
  - L'initiation via une redirection sur une application bancaire installée sur le smartphone, et non plus via une redirection sur une page web ; où depuis l'application bancaire, via un code confidentiel ou une authentification biométrique, le processus 3D serait réalisé – à condition que l'émetteur le permette.
- Une authentification possible via un canal différent de celui de l'acte d'achat (mode out-of-band ou decoupled). Dans le cas d'achats sur console de jeu, sur un smartspeaker, voire même pour de la vente au téléphone, 3D-Secure 2.0 permet de déclencher l'authentification via un autre canal (par exemple sur l'application bancaire du smartphone, réveillée via une alerte). A la rigueur, un achat in-app sur smartphone peut faire l'objet d'une authentification out-of-band sur le même smartphone, ce qui reviendrait à une redirection sur l'application bancaire. On peut envisager aussi, qu'un achat sur internet classique depuis son PC, fasse l'objet d'une authentification out-of-band sur smartphone, sans redirection du browser du payeur vers la banque du payeur. Bien entendu, à condition que l'émetteur mette en œuvre cette authentification et que le payeur soit équipé.

Déploiement de 3D Secure 2.0 et coexistence avec 3D Secure 1.0

Le déploiement de 3D Secure 2.0 est exigé par les schémas de paiement Visa et Mastercard.
Cependant, comme nous le verrons ci-dessous, il est recommandé que le PSP du marchand supporte tant 3DS 1.0 que 3D 2.0 jusqu'à la mise hors service de 3DS 1.0 actuellement planifié fin 2020 pour Visa et Mastercard.

En ce qui concerne les autres schémas de paiement carte :

- Cartes Bancaires : 3DS 2.0 sera lancé courant 2019 avec migration progressive
- Bancontact : 3DS 1.0 est déjà obligatoire, la migration vers 3DS 2.0 se fera prochainement (planning à confirmer)
- American Express : il est nécessaire d'intégrer 3D-Secure 1.0 puis d'y rajouter 3D-Secure 2.0
- Diners : l'intégration 3D-Secure 1.0 est recommandée selon l'origine des porteurs
- JCB, UnionPay, Diners/Discover network : l'origine extra-européenne des cartes émises permet une exemption d'authentification forte
- Pour les autres solutions privatives : voyez auprès d'eux les impacts possibles de la directive PSD2 sur leurs services de paiement.

Les nouvelles règles de transfert de responsabilité

Les règles de transfert de responsabilité entre émetteur et acquéreur en cas d'impayé vont changer avec l'introduction de la PSD2, la nouvelle version de 3D Secure et la capacité du marchand à demander une exemption d'authentification forte dans le premier message échangé entre lui (ou son prestataire d'acceptation technique, communément appelé PSP) et l'émetteur. Les règles peuvent légèrement différer selon les schémas.

Dans la mesure où le commerçant permet à l'émetteur de faire une authentification forte, le marchand est dégagé de sa responsabilité, que l'émetteur procède ou non à une authentification forte du porteur de carte, selon le type d'exemption qu'il peut invoquer (ex. White Listing, TRA coté émetteur, transaction de petit montant).

Si volontairement le commerçant ne permet pas à l'émetteur de réaliser une authentification forte (par exemple en n'initiant pas la transaction en mode 3D Secure), le marchand supportera le risque de fraude.

Par ailleurs, si le commerçant initie une transaction en mode 3D Secure et invoque l'exemption d'authentification forte pour analyse de risque (TRA) et si l'émetteur accepte cette demande sans forcer une authentification forte du porteur, l'acquéreur sera responsable en cas de fraude.

Par exemple, lors d'une transaction initiée en 3D-Secure 2.0, l'émetteur pourra décider de ne pas procéder à une authentification forte du consommateur, s'il peut invoquer l'une des exemptions (white listing, TRA coté émetteur, transaction de petit montant). Dans ces cas, l'émetteur est responsable.

Dès que les règles des schémas seront finalisées, des informations complémentaires seront partagées.

04 Aspects à prendre en considération par les commerçants

Les obligations d'information du consommateur et d'obtention de son consentement sont applicables depuis janvier 2018.

Les obligations d'authentification forte du porteur de carte doivent être mises en œuvre pour le 14 septembre 2019.

4.1 Paiements de proximité

Comme expliqué précédemment, deux cas d'exemption ont été prévus pour du paiement de proximité, à savoir les transactions sans contact de petit montant et les transactions relatives au transport et parking sur automate. Dans tous les autres cas, une authentification forte du porteur de carte doit être exécutée.

Un terminal acceptant les transactions sans contact pourrait dès lors ne pas être équipé d'un PINpad.
Cependant, il est recommandé d'utiliser un terminal avec PINpad, d'une part, s'il accepte également des transactions en mode contact, et d'autre part, parce qu'il se peut que durant l'exécution d'une transaction sans contact, l'émetteur demande l'authentification forte, par exemple sur base des calculs de vélocité.

Un opérateur de services de transport ou de parking pourra décider d'installer des terminaux de paiement sans PINpad (et donc ne permettant pas d'introduire un code secret). Cependant, comme l'exemption est une option, il se pourrait que dans certains cas l'émetteur souhaite une authentification forte. Actuellement il paraît raisonnable d'envisager un terminal sans PINpad sur un péage autoroutier ou sur un horodateur de rue ; par contre sur un automate de parking privé, il pourrait être utile d'envisager un terminal avec PINpad.

4.2 Paiements à distance

Comme expliqué précédemment, cinq cas d'exemption d'authentification forte sont prévus dans le contexte de paiements à distance : bénéficiaires de confiance ou White-Listing, transactions récurrentes, transactions de petit montant, corporate payments, analyse de risque transactionnel. Dans tous les autres cas, une authentification forte du porteur de carte doit être exécutée.

Comme expliqué également ci-dessus, les schémas de paiement imposent le déploiement de 3DS 2.0 comme solution technique dans le cadre de transactions à distance. Ils considèrent que cela permettra de réduire significativement la fraude, tout en n'impactant pas le taux de conversion, la solution 3DS 2.0 devant permettre à l'émetteur de ne pas systématiquement effectuer une authentification forte du porteur de carte.

Dans la période de déploiement de 3DS 2.0, il est fortement recommandé que le PSP du commerçant supporte tant 3DS 1.0 que 3DS 2.0, ceci afin de profiter du transfert de responsabilité indépendamment de la solution supportée par l'émetteur durant la période de transition.

En résumé, en tant que commerçant proposant des paiements à distance, assurez-vous que votre PSP ait rendu opérationnel 3DS 1.0 et si possible 3DS 2.0 pour le 13 septembre 2019.

Les commerçants n'ayant pas encore implémenté 3D Secure doivent envisager de revoir l'expérience d'achat du consommateur et s'assurer que l'authentification forte s'intègre parfaitement dans le processus de vente.

Les commerçants peuvent également envisager de faire appel aux exemptions d'authentification forte autorisées par la PSD2. Comme nous le verrons ci-dessous, dans la plupart des cas, cela passe cependant par l'initiation de la transaction en mode 3D Secure.

Les commerçants qui actuellement n'utilisent pas systématiquement 3D Secure pour toutes les transactions (par exemple : activation de 3D Secure pour les ventes risquées de haut montant ou lorsque le porteur est situé dans un pays à risque, mais pas pour les autres transactions), ce mode de fonctionnement devra être revu pour tenir compte de l'obligation d'authentification forte et des cas d'exemption autorisés (voir ci-dessus).

Exemption pour bénéficiaire de confiance ou White-Listing
La décision d'utilisation de l'exemption est prise par l'émetteur (et non par le marchand, son PSP ou l'acquéreur). Le commerçant peut inciter le consommateur à le mettre dans la liste des bénéficiaires de confiance.

La transaction doit être initiée en mode 3D Secure. Si l'émetteur supporte ce mode d'exemption, il pourra l'appliquer si le commerçant se trouve déjà dans la liste des bénéficiaires. Si ne n'est pas le cas, une authentification forte est requise. (Il est prévu que les émetteurs permettent l'inscription en white-liste lors de l'authentification forte associée à une transaction.)

Exemption pour transactions récurrentes
La première transaction (le contrat) doit être réalisée avec authentification forte (en 3D Secure).
Les transactions suivantes peuvent être exemptées d'authentification forte sans utilisation de 3D Secure, auquel cas certains émetteurs pourraient malgré tout la rejeter.

Exemption pour transaction de petit montant
La décision d'utilisation de l'exemption est prise par l'émetteur (sur base du montant de la transaction, des conditions de vélocité et de la stratégie de l'émetteur vis-à-vis de son client porteur de carte).

La transaction doit être initiée en mode 3D Secure, l'émetteur décidera de procéder ou non à l'authentification forte du porteur de carte.

Exemption pour analyse de risque transactionnel
La transaction doit être initiée en mode 3D Secure. Un flag doit être positionné afin d'informer l'émetteur que le commerçant souhaite bénéficier de cette exemption. Si l'émetteur accède à la demande du marchand, sans procéder à une authentification forte du porteur de carte, l'acquéreur devient responsable en cas de fraude.

Cette exemption peut aussi être appliquée par l'émetteur de la carte de paiement sans requête du commerçant. Dans ce cas l'émetteur devient responsable en cas de fraude.

05 Exemples de mise en œuvre de transactions particulières

Wallets

Dans le cas de wallets tiers ayant un accord d'authentification par délégation de l'émetteur (exemple, Paylib pour Cartes Bancaires, Bancontact mobile), l'authentification forte est gérée par le gestionnaire de ce wallet (en délégation de l'émetteur), avec également la possibilité d'invocation des exemptions d'authentification forte.

Dans le cas d'un wallet marchand (stockage des identifiants de la carte sur le site marchand) ou des wallets tiers n'ayant pas un accord d'authentification par délégation de l'émetteur, la transaction de paiement fera l'objet d'une authentification forte 3D-Secure comme toute transaction faite à l'aide d'une carte non stockée dans un wallet marchand, tout en pouvant bénéficier des règles d'exemptions.

Apple Pay, Samsung Pay

Ces moyens de paiement, mis à disposition sur le smartphone du porteur de carte et couplés à une méthode d'authentification forte de type biométrique, reconnue par l'émetteur de la carte de paiement, sont utilisables aussi bien dans un contexte de proximité, en mode sans contact, que pour des paiements à distance lorsqu'ils sont intégrés dans un site e-commerce.

Ne négligez pas d'intégrer ces moyens de paiement, qui se débouclent sur des transactions carte (Visa, Mastercard, American Express, Cartes Bancaires) et sont possibles avec votre acquéreur Worldline. Les fabricants de terminaux mobiles y ont vu une opportunité et lanceront des opérations de communication adaptée.

Exemples de transactions à distance et recommandations de traitement

Ci-dessous sont listées des transactions communément effectuées par les commerçants.
Il est à noter que les schémas vont adapter leurs protocoles pour le traitement de types particuliers de transactions.
Tout n'est pas encore totalement défini.

Ci-dessous, sont décrites quelques règles générales.
A ces règles sont aussi applicables les exemptions que les commerçants peuvent essayer de faire jouer.

Paiement unitaire

Exemple : J'achète un produit sur un site web de e-commerce. Le produit est disponible immédiatement pour livraison dans la journée. Le paiement est exécuté aujourd'hui.
Paiement initié par : le payeur
Règle : Authentification forte avec exemption possible.

Paiement différé (avec montant égal ou inférieur au montant initial ; dont le montant n'est pas connu à l'avance)

Exemple : J'achète plusieurs produits sur un site web de e-commerce. Tous les produits ne sont pas disponibles pour une livraison immédiate. Je consens à l'ordre de paiement que le marchand ne réalisera qu'à l'envoi de la marchandise. Si un ou plusieurs produits sont manquants, le montant final de la transaction sera diminué d'autant et inférieur au montant consenti.

Paiement initié par : le payeur
Règle : Authentification forte avec exemption possible pour le montent consenti (la somme globale). Paiement sur le montant final de la transaction.

Paiements fractionnés – paiements échelonnés, abonnements sans tacite reconduction

Exemple : Lorsqu'une vente fait l'objet de plusieurs livraisons, et de débouclages à chaque envoi, l'utilisateur ayant consenti la totalité de la transaction.
Autre exemple : Paiement en trois fois sans frais
Autre exemple : abonnement à un magazine pour une durée inférieure à un an.

Paiement initié par : le payeur
Règle : Authentification forte pour le montant global pendant la session d'achat et plusieurs transactions de paiement (avec référence à l'autorisation initiale pour les paiements subséquents, avec ou sans autorisation supplémentaire, selon les règles des schémas). Dans le cas de transactions de petits montants, le commerçant peut aussi essayer de faire jouer l'exemption pour petit montant à chaque transaction.

Série de paiements à montants fixes

Exemple : abonnement de type « musique en ligne », « vidéo à la demande »
Paiement initié par : le payeur pour la première transaction et par le marchand pour les transactions suivantes.
Règle : Authentification forte pour la première transaction, mais pas pour les suivantes. Si un produit ou un service additionnel est comptabilisé lors de la première transaction (par exemple : frais de mise en service), alors l'authentification forte du client doit intégrer le montant total de la transaction la plus élevée (en l'occurrence, la première). Dans le cas de petits montants, le commerçant peut aussi essayer de faire jouer l'exemption pour petit montant à chaque transaction.

Paiements 1-Clic

Exemple : Paiement en 1-clic à partir d'une application commerçant ou d'un wallet commerçant et pour lequel le consommateur a fait l'objet d'une authentification par le commerçant.
Initié par : le payeur ou le marchand (selon les différents cas décrits ci-dessus)
Règle : la connaissance parfait du client par le commerçant ne change en rien les règles décrites ci-dessus et l'authentification forte s'applique selon les cas. Cependant, de par sa préinscription dans le wallet, le commerçant peut faire jouer l'exemption pour les bénéficiaires de confiance. Ainsi, l'achat d'un livre auprès d'une librairie en ligne, est une transaction initiée par le payeur et doit faire l'objet d'une authentification forte ou d'une exemption.
L'inscription (ou le renouvellement) du client dans le wallet fait aussi partie des cas entrants dans le champ d'application de l'authentification forte.

Les transactions initiées par les marchands

Une note à paraitre de l'Autorité Bancaire Européenne doit préciser et confirmer la notion de « Merchant Initiated Transactions », ce qui permettra ou non de lever des incertitudes quant aux modalités de traitement de certaines transactions spécifiques.

Transactions initiées par le payeur ou par le marchand?

Selon les RTS (spécifications techniques liées à la DSP2), seules les opérations initiées par le payeur entrent dans le champ d'application : « Toute opération de paiement ou toute série d'opérations de paiement ayant fait l'objet d'un consentement ad hoc du client pour un montant global maximum déterminé ».

Sur cette base, certains schémas de paiement estiment que les opérations initiées par le commerçant, ne doivent pas faire l'objet d'une authentification forte, ce qui provoquerait une distorsion de concurrence avec le prélèvement.

Cela concerne entre autre, les achats de biens et services dont le montant ne peut être ni déterminé, ni estimé par le commerçant ou les transactions dans le consentement du payeur ne peut être recueilli. En revanche, le mandat initial ou les changements liés aux modalités de paiement devront faire l'objet d'une authentification forte

L'EBA n'a pas encore confirmé que les transactions carte initiées par les commerçants, sans intervention du payeur sont hors du scope de l'authentification forte.

Un exemple : le paiement de factures

Exemple : paiement d'une facture d'électricité dont le montant varie en fonction de la consommation.
Paiement initié par : le marchant
Règle : la première transaction serait faite avec authentification forte, les suivantes sans. Certains schémas conseillent même de réaliser la première transaction avec le montant maximal qui pourrait être atteint pour les transactions suivantes.

Cas particuliers

Il y a tout un ensemble de cas particuliers en fonctions de cas d'usage métiers très spécifiques.
Quelques exemples :

- les VTC, dont le montant de la course n'est pas connu à l'avance,
- l'hôtellerie, où des sommes additionnelles peuvent être réglées (petit-déjeuner), après le paiement de la chambre, la location, où des frais peuvent être appliqués pour le nettoyage, le plein d'essence, ou l'application de franchises,
- l'hôtellerie ou la location, où le client peut ne passer au comptoir pour régler sa note finale (par exemple, en dehors des heures d'ouverture),
- les paniers multi-marchands, dans le cas des marketplaces ou des agences de voyage, et pouvant déclencher de multiples transactions, directement par les bénéficiaires finaux,
- les cas où des augmentations de prix (si les conditions de livraison ont changé, si un produit a été remplacé par un autre avec accord du client),
- le no-show quand un client ayant commandé un service, ne se présente pas ou n'est pas en mesure de réceptionner ce service.

Il existe des possibilités techniques permettant aux commerçants de réaliser ces transactions :

- en s'appuyant sur la notion de transactions initiées par le commerçant, si celles-ci sont acceptées par l'EBA,
- en effectuant une authentification forte, dite out-of-band ou decoupled,
- en effectuant une première authentification d'un montant bien supérieur au montant maximal possible,
- en recommandant très fortement au consommateur d'inscrire le commerçant en liste de bénéficiaires de confiance.

06 Résumé des actions

1. Intégrez avant le 14 septembre 2019 3D-Secure 1.0 sur votre site internet, auprès de votre prestataire d'acceptation technique ; nécessaire pour être en conformité et vous assurer de ne perdre aucune transaction. Assurez-vous aussi d'être bien enregistré auprès de votre acquéreur Worldline.
2. Migrez vers 3D-Secure 2.0 courant 2019 pour bénéficier des exemptions et d'une meilleure intégration avec votre site mobile, tout en conservant 3D-Secure 1.0 pour traiter les cas des émetteurs par encore prêts sur 3D-Secure 2.0.
3. Demandez à votre acquéreur Worldline d'être enregistré dans le programme 3D-Secure 2.0 (même si vous êtes déjà dans le programme 3D-Secure 1.0)
4. Dans le cas où vous initiez une transaction 3D-Secure 2.0 et que l'émetteur ne le supporte pas, assurez-vous de pouvoir vous replier sur la version 1.0.
5. Améliorez l'analyse de risque de l'émetteur pour bénéficier plus facilement d'une exemption en partageant les données porteur (mail, adresses de facturation et livraison, téléphone, etc...) via votre PSP et 3D-Secure 2.0.
6. N'oubliez pas d'intégrer les nouveaux logos 3D-Secure des différents schémas sur vos pages Web. Pensez à intégrer le nouveau logo Mastercard Identity Check.
7. Repensez l'expérience d'achat et de paiement en fonction de ces nouvelles obligations d'authentification, et plus particulièrement pour les ventes sur mobile.
8. Ayez un nom simple, unique et qui vous identifie parfaitement afin d'optimiser votre reconnaissance par les porteurs dans les white-listes.
9. Pour les paiements récurrents, une authentification forte est nécessaire pour le premier. Pour les paiements suivants, exécutez le process 3D-Secure en vous référant à la première authentification, de sorte qu'il ne soit pas demandé au porteur de se ré-authentifier.
10. Dans le cas de paiements récurrents à montants variables, où le montant n'est pas connu à l'avance, pour lesquels vous authentifiez le porteur pour un montant plus élevé que la (ou les) transaction(s), informez-le et rassurez-le.
11. N'oubliez pas d'initier une authentification forte même dans le cas où le paiement sera déclenché par le marchand à une date ultérieure.
12. Le montant authentifié doit toujours être supérieur ou égal au montant de l'autorisation ou de la somme des autorisations dans le cas de paiements fractionnés.

07 Glossaire

Autorité Bancaire Européenne (ABE)
Créée en 2010, autorité de supervision du système financier européen.

DSP2
La Directive européenne (2015/2366/UE) sur les Services de Paiement 2ème version

Paiement fractionné (split payment)
Transaction de paiement faisant l'objet de plusieurs opérations de débit du consommateur en fonction des livraisons successives des biens achetés.

Regulatory Technical Standards (RTS)
Normes techniques réglementaires publiées par l'Autorité Bancaire Européenne associées à la DSP2.

Strong Customer Authentification (SCA)
Authentification forte du client