3D Secure 2.0 - Se mettre en conformité avec la DSP2

Contenu

- 3D Secure 2.0 - Se mettre en conformité avec la DSP2
- 3DSV2 - Comment intégrer
- 3DSV2 - Comment ça marche
- 3DSv2 - Glossaire
- 3DSV2 - Intégration : cas d'usage
- 3DSV2 - Les fonctionnalités
- 3DSV2 - Périmètre d'application des RTS SCA

Qu'est-ce que la DSP2 ?

La nouvelle Directive sur les Services de Paiement (DSP2) initiée par la Commission Européenne est appliquée depuis le 13/01/2018

Objectif : Renforcer la sécurisation des paiements à distance

L'Autorité Bancaire Européenne (ABE) a élaboré des mesures d'exécution nommées **Regulatory Technical Standards (RTS) qui entreront en application le 14/09/2019.**

La DSP2 rendra obligatoire l'authentification SCA (Strong Customer Authentication) ou authentification à deux facteurs pour les transaction en VAD.

> Le 3DS V2 est l'outil de mise en conformité de la DSP 2 pour tous les marchands. Payline vous facilite l'intégration. Suivez les étapes ici.

Qu'est-ce qu'une authentification forte SCA ?

Pour renforcer la protection des acheteurs lors de paiements à distance, la DSP2 rend obligatoire l'authentification SCA (Strong Customer Authentication), aussi appelée « authentification à deux facteurs ».

Une authentification forte de l'acheteur nécessite la vérification d'au moins deux facteurs parmi les 3 suivants :

- Connaissance : ce que l'acheteur sait (PIN, mot de passe) ;
- Possession : ce que l'acheteur possède (carte, mobile, token) ;
- Inhérence : ce que l'acheteur est (empreinte digitale, reconnaissance faciale, iris).

qui sont **indépendants** l'un de l'autre en ce sens que la compromission de l'un n'entraine pas la compromission de l'autre.

Bien que non reconnue comme une méthode d'authentification forte par l'autorité bancaire européenne, le SMS-OTP sera encore utilisé le temps que de nouvelles méthodes (biométrie par exemple) prennent le relais.

Cette méthode adoptée massivement par les acheteurs, a contribué à faire baisser significativement les taux de fraude pour les paiements carte en e-commerce. Elle est actuellement la plus répandue chez les banques (86%).

Quels sont les impacts pour votre activité ?

La DSP2 s'applique aux banques et non aux marchands, cela signifie que les banques émettrices qui accepteront des transactions non conformes s'exposent à être hors la loi.

Toutes les transactions ne sont pas soumises aux RTS (voir les cas **hors scope** et les **exemptions**), le champ d'application des RTS est décrit dans l'article suivant. Périmètre d'application des RTS SCA

- Dans le cas d'une transaction hors scope, l'authentification forte n'est pas requise.
- Si une transaction rentre dans le périmètre d'une exemption, l'authentification forte est optionnelle et le choix d'authentifier fortement est entre les mains de la banque de l'acheteur .
- Si une transaction ne rentre pas dans le périmètre d'une exemption, l'authentification forte est obligatoire.

Une authentification forte impacte le parcours utilisateur et le taux d'acceptation en particulier sur mobile, il convient donc de la déclencher que pour les transactions risquées.

Les objectifs pour le marchand sont par conséquent :

- **la mise en conformité afin d'éviter des transactions en refus ;**
- **la conservation d'une expérience utilisateur optimale ;**
- **la réduction de la fraude.**

Nous vous fournissons les outils qui vous permettront d'atteindre ces objectifs.

3DS V2

Les règles décrivant la SCA sont techniquement neutres et n'imposent aucune méthode particulière.

Le protocole 3DS V2 fournit un mécanisme qui permet de réaliser une authentification forte en conformité avec la DSP2.

Le principal avantage de 3DS est de transférer la responsabilité de la fraude éventuelle du commerçant à l'émetteur de la carte (liability shift), ce qui réduit les impayés.

Néanmoins, de nombreux commerçants n'utilisent pas la solution 3DS à cause des pertes de taux de conversion et des coûts de service.

Pour rappel les principaux inconvénients de la version 3D-Secure 1.0 :

- La cinématique peut être compliquée ou déroutante pour un titulaire de carte, ce qui entraîne une conversion plus faible (problème des paniers abandonnés) ;
- 3-D Secure 1.0 ne s'adapte pas bien aux appareils mobiles ;
- manque d'intégration transparente avec les outils de paiement modernes tels que les wallets ;
- ensemble limité de méthodes d'authentification possibles, dont certaines sont obsolètes et dangereuses (date de naissance) ;
- capacité très limitée de l'autorisation sans friction basée sur du scoring.

Évolutions majeures de la nouvelle spécification de 3-D Secure 2.0

Fonctionnalité	Bénéfice
Authentification Basée sur les risques (RBA)	Permet une authentification passive sans challenge du porteur de la carte (mode frictionless) pour une majorité de transactions.

Gestion du risque orientée données	Utilisation de plusieurs données incluant les caractéristiques du device, les informations du compte du porteur et de sa localisation, afin de fournir une évaluation du risque suffisamment fine permettant ainsi de réduire le recours à une authentification forte du porteur.
Support natif des dispositifs mobiles	Conçu pour supporter les workflows e-commerce natifs et web fournissant ainsi une expérience fluide sur l'application mobile commerçant quel que soit le device (achat In-App).
Intégration souple dans le parcours client du marchand	Permet au marchand d'embarquer l'authentification dans le tunnel d' achat, maintenant ainsi une expérience utilisateur cohérente.
Support de la biométrie et d' autres méthodes	Réduit les frictions au niveau de l'expérience utilisateur.
Flags dans les messages afin de supporter les dérogations liées à la DSP2	Permet aux marchands et aux acquéreurs de préciser aux émetteurs quand ils souhaitent appliquer une exemption et prendre la responsabilité de la transaction.

La plus grande différence avec 3DS 1.0 réside dans le flux « frictionless » qui permet à l'émetteur d'approuver une transaction sans interaction du titulaire de la carte sur la base d'une authentification basée sur les risques effectuée dans l'ACS.

Grâce à ces évolutions, les banques des acheteurs auront accès à un plus grand nombre d' informations leur permettant d'affiner le scoring d'aide à la décision pour le déclenchement d'une authentification forte (ou non / frictionless).

3DS 2.0 permet de résoudre plusieurs problèmes techniques de 3DS v1.0. Comme une optimisation des parcours acheteurs, rendant le processus de paiement plus aisé pour les achats sur navigateur et inapp, l'introduction d'un flux d'authentification sans friction et une sécurité renforcée.

L'authentification 3DS V1 restera possible jusqu'à la fin 2020. A partir de 2021, toutes les authentifications 3DS devront utiliser la version 2 .

Comment être conforme à la DSP2 ?

La méthode d'authentification 3DSecure répondra aux exigences des RTS - SCA à partir du 14/09/2019.

Il faut cependant distinguer les cas suivants:

- Cas 1 : 3DS systématique

  Un marchand réalisant actuellement une authentification 3DS V1 de manière systématique sera en conformité avec la DSP2.

- Cas 2 : 3DS sélectif

  Un marchand réalisant actuellement une authentification 3DS V1 de manière sélective s'expose à un refus de la banque de l'acheteur pour les transactions non 3DS.

- Cas 3 : pas d'authentification réalisée

  Un marchand ne réalisant actuellement aucune authentification s'expose à un refus de la banque de l'acheteur pour toutes ses transactions.

Nous vous recommandons dans tous les cas d'envisager dès à présent une migration vers le protocole 3DS V2 afin d'être prêt à bénéficier de ses avantages et notamment du frictionless.

Afin d'intégrer le protocole 3DS V2, veuillez consulter l'article suivant 3DSv2 - Comment intégrer

Pages associées

- 3D Secure 2.0 - Se mettre en conformité avec la DSP2
- 3DSv2 - Augmenter le frictionless
- 3DSV2 - Cloture d'un dossier PLBS
- 3DSV2 - Comment intégrer
- 3DSV2 - Comment ça marche
- 3DSV2 - Direct Interface - JSON container format
- 3DSv2 - Exemption acquéreur
- 3DSv2 - Exigences Visa
- 3DSv2 - Glossaire
- 3DSV2 - Indicateur de transfert de responsabilité
- 3DSV2 - Interface Directe - Ajout Modification de données carte (card on file)
- 3DSV2 - Interface Directe - Commande avec expédition pendant la garantie de l'autorisation
- 3DSV2 - Interface Directe - Paiements pour la Location de Biens et Services
- 3DSV2 - Interface Directe - Paiements récurrents
- 3DSV2 - Interface Directe - Pré-commande ou expedition tardive