

3DSV2 - Comment ça marche

Contenu

- [Le principe](#)
 - [Le traitement d'authentification](#)
 - [1. Hors périmètre](#)
 - [2. Exemptions](#)
 - [3. Frictionless](#)
 - [4. Challenge](#)
 - [Pages associées](#)
-

Le principe

Cette page vous permet de guider les commerçants Payline à évoluer en 3DS version 2.0

3D Secure version 2.0

Pour renforcer la protection des acheteurs lors de paiements à distance (online), la directive européenne DSP2 rend obligatoire l'authentification SCA (Strong Customer Authentication) de l'acheteur pour tout paiement électronique qu'il initie.

Ce traitement permet l'échange de données avec le commerçant et l'émetteur afin que ce dernier décide de l'authentification. Dorénavant plus le commerçant envoie de données au moment de l'authentification, plus les paiements ont des chances d'être autorisés. Ce traitement s'adresse aux commerçants qui ne réalisent pas d'authentification 3DS systématique, néanmoins les commerçants qui souhaitent profiter de ce traitement 3DS v2 et transmettre les données acheteurs pourront bénéficier d'un meilleur taux d'acceptation.

La directive sur les Services de Paiement (DSP2) impose l'application de nouvelles normes à appliquer (Regulatory Technical Standards (RTS)) dont une authentification forte (Strong Customer Authentication SCA) lors de paiement en ligne : c'est à dire authentification à 2 facteurs.

En décembre 2020, le 3DS 1.0 ne sera plus supporté.

Chaque transaction 3DS initiée sur Payline devra être transmise à l'ACS (serveur authentification du porteur) par l'intermédiaire du MPI, avec un maximum d'informations concernant le porteur et sa commande pour permettre à l'ACS de décider si une authentification forte (avec challenge) est requise ou non (friction less).

Rappel du 3D Secure

3D Secure est un protocole d'authentification fourni par les systèmes de cartes de crédit.

Le marchand peut demander un mot de passe au consommateur pour confirmer le paiement. Cette procédure permet d'authentifier le consommateur comme étant le porteur de la carte utilisée pour le paiement. Elle permet de renforcer la sécurité et de [transférer la responsabilité](#) au consommateur de la carte en cas d'impayé.

L'authentification se fait en deux étapes :

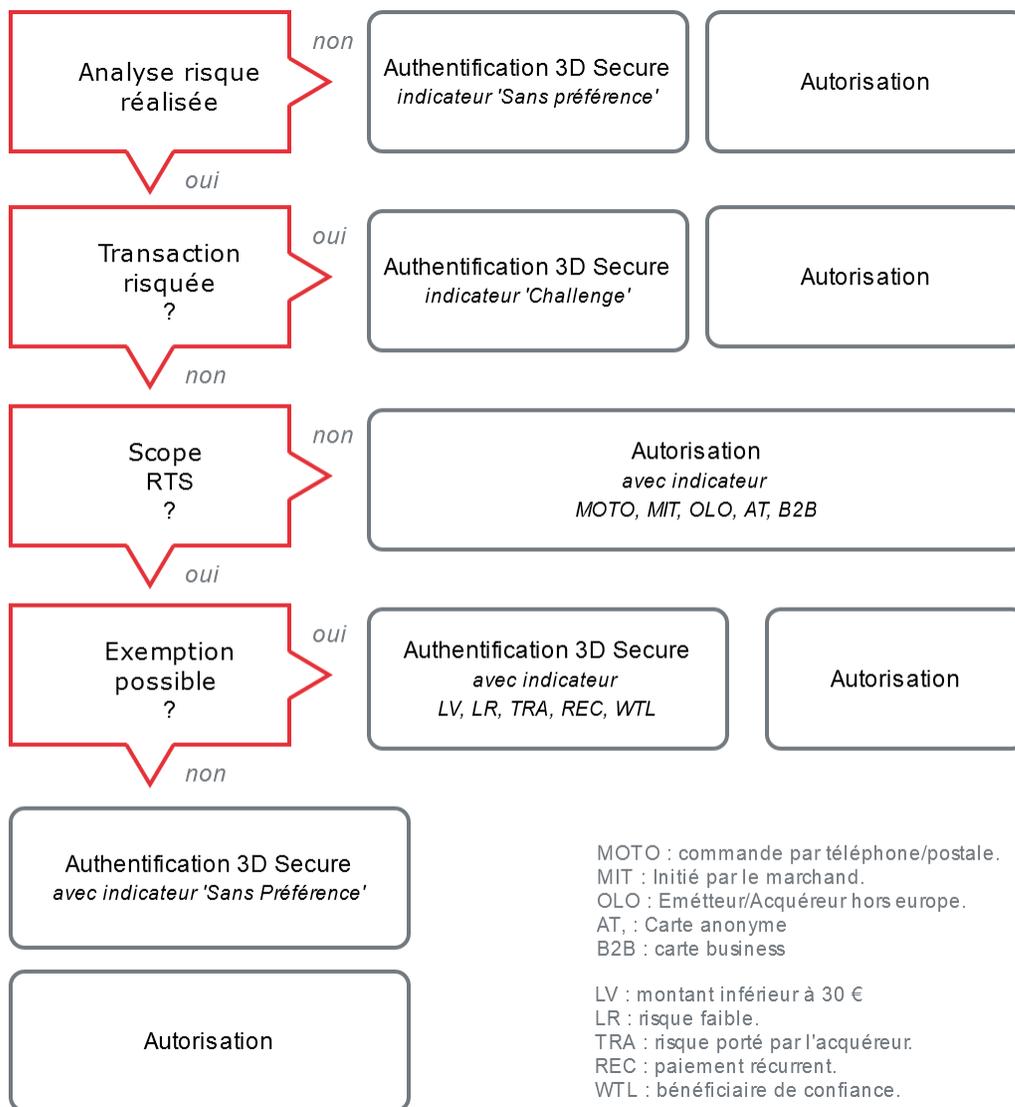
- vérification de l'enrôlement de la carte au système 3D Secure ;
- demande d'authentification du consommateur.

La mise en place de 3D Secure doit permettre aux e-marchands de réduire le montant de leurs impayés dus à la fraude, mais cette procédure réduit également le taux des paiements acceptés.

Principe du 3DS V1 : [consulter la page pour plus d'information](#).

Le traitement d'authentification

Le commerçant initie une demande de paiement et la banque de l'acheteur va l'authentifier de manière plus sur si les transactions sont dans le périmètre 3DSv2 et si elles ne sont pas exemptées.



1. Hors périmètre

La directive n'impose pas l'authentification forte (SCA) à ces types de transactions. Pour ces transactions, le marchand est responsable en cas de fraude.

1. Commande par paiement postal et téléphone (MOTO) ;
2. Transaction initiée par le marchand (MIT) ;
3. Transaction avec acquéreur ou émetteur hors europe (OneLeg) ;
4. Transaction anonyme (Prepaid);
5. Transaction B2B (Business).

2. Exemptions

Pour permettre une meilleure expérience utilisateur, la directive prévoit les exemptions suivantes. Si une demande d'exemption est acceptée, le marchand est responsable en cas de fraude.

1. Montant < 30 € (LOWVALUE)
2. Risque faible / TRA
3. Paiement récurrent (REC)
4. Bénéficiaire de confiance (WHISTELIST)

3. Frictionless

Le commerçant pourra demander un traitement Frictionless pour éviter l'authentification basé sur un scoring ou l'envoi de données supplémentaires afin de bien identifier l'acheteur.

Plus d'information : [3DSv2 - Augmenter le frictionless](#)

4. Challenge

Vous pouvez également challenger la demande de paiement en excluant ou en demandant l'authentification de l'acheteur. La banque de l'acheteur pourra valider ou vous demandez de refaire une demande de paiement avec authentification.

Réaliser un [verifyEnrollment](#) avec l'objet [Object - threeDSInfo](#) en indiquant les [Codes - ChallengeInd](#)

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 expédition tardive](#)