

3D Secure - Une authentification forte pour des paiements sécurisés

La **DSP2 (Directive sur les services de paiement version 2)** est une directive européenne visant à encourager l'innovation, améliorer la protection des consommateurs et renforcer la sécurité des services de paiement. La réglementation **RTS (Standards Réglementaires et Techniques)** liée à la DSP2 impose l'utilisation du processus d'authentification pour l'ensemble des paiements e-commerce initiés par le porteur de carte. L'objectif est de répondre aux exigences de l'authentification forte du client (**Strong Customer Authentication - SCA**) pour minimiser le risque pour le commerçant tout en simplifiant et fluidifiant le parcours des utilisateurs.

Glossaire autour du 3DSV2

Authentification Forte / Strong Customer Authentication (SCA)

L'authentification forte du porteur (client) est une exigence réglementaire introduite dans le cadre de la DSP2. Lors d'un paiement en ligne, une authentification forte à 2 facteurs peut être demandée au porteur de la carte de paiement, permettant de confirmer que la personne effectuant le paiement est bien le titulaire de la carte.

Une authentification est considérée comme forte lorsqu'elle réunit deux des trois facteurs d'authentification suivants :

- **Un élément connu du porteur** (un mot de passe, un code secret, etc.)
- **Un élément possédé par le porteur** (téléphone mobile via l'application de la banque, une carte bancaire, etc.)
- **Une caractéristique biométrique** (une empreinte digitale, la reconnaissance vocale, etc.)

Frictionless

Le marchand a la possibilité de demander une exemption d'authentification du porteur lors du paiement en ligne. La décision finale est laissée à la banque émettrice.

Lors d'une transaction "frictionless", une authentification passive du porteur est effectuée, sans aucune action de sa part. En résumé, il s'agit d'un processus qui réduit l'intervention de l'acheteur au cours du processus de paiement.

En cas de transaction frictionless, le transfert de responsabilité dépend de la marque de la carte. Pour plus de détails, consultez notre documentation sur le **Transfert de Responsabilité et Matrices 3D-Secure**.

Préférences du Marchand : no Preference / challenge / mandate

Le commerçant peut solliciter l'émetteur pour demander ou non une exemption d'authentification forte. Plusieurs choix se présentent à lui :

- **Le commerçant ne prend aucune action (no preference)** : Le choix d'exemption est laissé à l'émetteur.
- **Le commerçant demande une authentification forte (challenge)** :
 - **Obligatoire (mandate)** : L'émetteur doit authentifier l'acheteur (par exemple pour la première transaction d'un abonnement).
 - **Préférentielle (request)** : Le commerçant souhaite authentifier l'acheteur. Le choix final reste à l'émetteur.
- **Le commerçant demande une exemption d'authentification forte (no Challenge - Frictionless)** : L'émetteur va accepter ou non la demande du commerçant selon les informations transmises par celui-ci (données à transmettre).

Le transfert de responsabilité dépend du choix du commerçant et de la marque de la carte. Pour plus de détails, consultez notre documentation sur le **Transfert de Responsabilité et Matrices 3D-Secure**.

Soft Decline

En cas de transaction réalisée sans SCA (Authentification forte 3DS), les émetteurs peuvent répondre par des **Soft Decline**. Cela signifie que la demande d'autorisation de transaction est refusée par l'émetteur, cependant, la même transaction peut être initiée à nouveau. La principale raison pour laquelle des Soft Decline apparaissent dans le contexte de 3D Secure est que les émetteurs n'acceptent pas les exemptions de SCA demandées par le commerçant lorsqu'il demande un paiement sans que l'authentification soit réalisée au préalable.

Avec la fonctionnalité de gestion automatisée des Soft Decline, basée sur la configuration, la plateforme **Axepta BNP Paribas** réagira à la réponse de Soft Decline en redémarrant automatiquement le paiement en forçant l'authentification forte. La plateforme **Axepta BNP Paribas** activera ensuite automatiquement un nouveau paiement au nom du commerçant et inclura le flux 3-D Secure.

Important :

- Du point de vue de l'utilisateur, les clients ne remarqueront aucune différence et n'auront pas besoin de saisir à nouveau leurs données de carte de crédit. Le processus entier est géré par la plateforme **Axepta BNP Paribas**.
- Veuillez noter que cette solution n'est pas disponible pour les intégrations serveur-à-serveur, car la plateforme **Axepta BNP Paribas** n'a pas le client (navigateur) sous contrôle pour débiter le processus 3-D Secure. Pour l'intégration serveur-à-serveur, le commerçant est responsable de réactiver le paiement avec le flux 3-D Secure et, surtout, de forcer la SCA via le paramètre JSON disponible **threeDSPolicy (challengePreference = mandateChallenge)**.

Transactions Non Concernées par la SCA

Dans le cadre de cette nouvelle réglementation, certains cas de paiements peuvent bénéficier d'exemption à l'authentification forte du client :

- **Les paiements récurrents (transactions MIT - Merchant Initiated Transactions)** : Le paiement initial nécessite une authentification forte, cependant les paiements suivants seront exemptés. Dans le cas d'un changement de montant de l'abonnement, l'acheteur devra de nouveau passer par une procédure d'authentification forte.
- **Les transactions MoTo (Mail Orders and Telephone Orders)** : Ce type de transaction n'est pas considéré comme un paiement électronique.

Les Exemptions

Le marchand peut demander une exemption d'authentification pour certaines transactions soumises à l'authentification forte :

- **Les transactions à faible montant (inférieur à 30€)** : Les banques doivent toutefois demander une authentification si l'exemption a été utilisée cinq fois depuis la dernière authentification réussie du titulaire de la carte ou si la somme des paiements exemptés précédemment dépasse 100 €.
- **Les transactions à faible risque (TRA : Transaction Risk Analysis)** : Une dérogation à l'obligation d'authentification forte peut être accordée. Pour cela, il faut l'accord préalable de l'acquéreur (sur la base d'une analyse de risque en temps réel de chaque opération).

Favoriser les Paiements 'Frictionless'

Plusieurs paramètres peuvent être ajoutés à la requête de paiement afin de favoriser les paiements frictionless. Pour plus de détails, [consultez notre documentation](#) sur les **Paiements 'Frictionless' et Exemptions**.