SOLUTION COLLECT

# 3-D Secure

Version du document 1.8

# Sommaire

# 1. INTRODUCTION

## 1.1. Qu'est-ce que 3-D Secure ?

3-D Secure est un protocole interbancaire permettant d'offrir un haut niveau de sécurité pour les paiements en ligne.

L'objectif du 3D Secure est de protéger les marchands en ligne contre les risques de fraude et de contestation du porteur.

- "**Visa Secure**" (remplace Verified by Visa) est le programme 3-D Secure de Visa
- "**Mastercard Identity check**" (remplace Mastercard Secure Code) est le nom du programme 3-D Secure de Mastercard
- "**Safekey**" est le programme 3-D Secure d'American Express
- "**CB Paiement sécurisé**" est le programme 3-D Secure de CB
- "**ProtectBuy**" est le programme 3-D Secure de Diners et Discover

Lyra Collect se charge de vous inscrire au programme 3-D Secure. Cet "enrôlement 3DS" consiste à déclarer votre site marchand auprès des réseaux CB, Diners,Visa, Mastercard et Amex.

Vous pouvez apposer sur votre site marchand les logos ci-dessus et ainsi en informer vos clients/usagers.



## 1.2. Fonctionnement du 3-D Secure

Lors du paiement, le protocole 3-D Secure implique l'authentification du porteur de la carte.

L'authentification se déroule après saisie des données de la carte et peut être réalisée :

- sans interaction du porteur ("frictionless"), auquel cas le porteur n'est pas explicitement invité à s'authentifier lors de son paiement ;
- avec interaction du porteur (authentification forte ou "challenge").

Chaque banque met en œuvre différentes méthodes d'authentification dans le cas d'une authentification forte. Exemple :

- l'authentification par application mobile ;

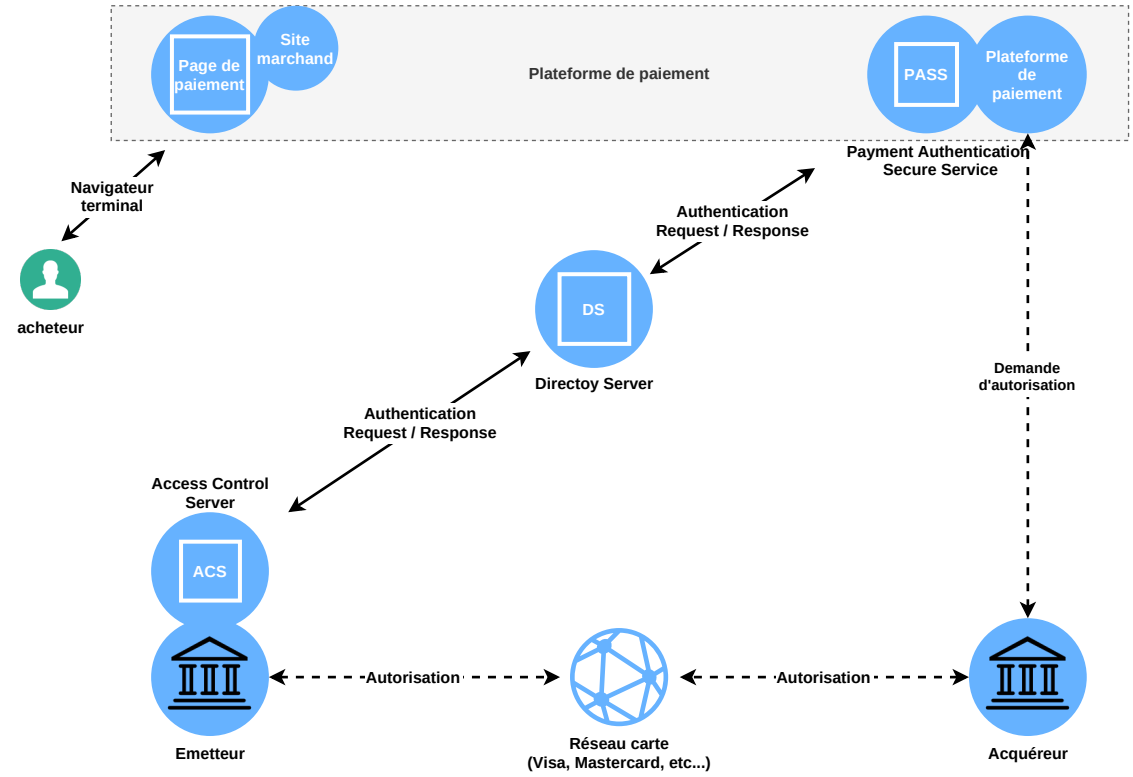
  L'acheteur reçoit une notification sur son smartphone et s'authentifie via l'application mobile de sa banque en saisissant un code secret ou grâce à ses données biométriques. Il confirme le paiement depuis l'application, puis retourne sur le site marchand.

- l'authentification par code de sécurité.

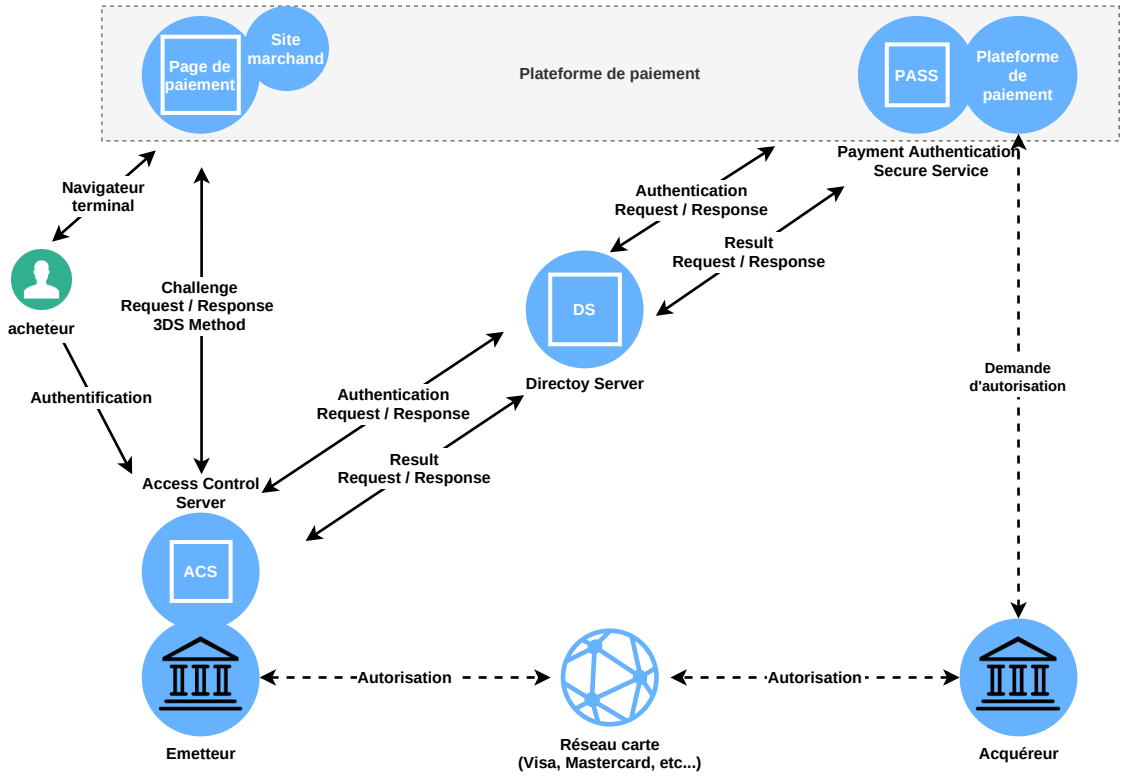
  L'acheteur reçoit un code à usage unique envoyé par SMS. Il renseigne ce code sur la page d'authentification afin de s'authentifier.

La plateforme de paiement se charge des échanges avec le serveur d'authentification de l'établissement bancaire du porteur et de récupérer le résultat pour finaliser le paiement.

**Cinématique Frictionless**



## Cinématique Challenge





# 2. 3DS2 : LE STANDARD D'AUTHENTIFICATION

La version 3-D Secure 2 (3DS2) augmente la sécurité des paiements mais aussi l'expérience utilisateur. Elle est basée sur une analyse de risques intelligente et dynamique. Elle permet de réduire le nombre d'abandons et les interactions avec l'acheteur.

Pour cela, une plus grande quantité d'information est utilisée par l'émetteur afin d'évaluer le risque de la transaction.

Si l'émetteur détermine que le niveau de risque de la transaction est faible, l'authentification se fait sans interaction de l'acheteur (***Frictionless***).

Dans le cas où l'émetteur évalue un risque élevé pour la transaction, une interaction de l'acheteur est nécessaire. On parle de ***Challenge***.

Durant ce challenge, l'acheteur doit répondre à, au moins, deux facteurs d'authentification. Cette méthode d'authentification s'appelle **SCA** (Strong Customer Authentication).

**SCA** impose que deux des trois différents facteurs d'authentification soient fournis :

- **Possession** : un objet que le client possède (comme le téléphone pour le paiement e-commerce ou la carte bancaire pour le paiement en magasin) ;
- **Connaissance** : donnée que seul le client connaît (comme un mot de passe) ;
- **Caractéristique personnelle** : élément biométrique caractérisant le client (comme une empreinte digitale, reconnaissance vocale ou reconnaissance faciale).

**SCA** est requise uniquement lorsque l'émetteur et l'acquéreur sont situés tous les deux dans l'Espace Economique Européen (EEE).

**SCA** n'est pas obligatoire sur les transactions réalisées avec une carte émise hors de l'EEE, ni si le marchand a souscrit un contrat avec un acquéreur hors de l'EEE, même si la carte est émise dans l'EEE (cas appelé "one-leg").

Les établissements émetteurs de carte déploient progressivement la méthode d'authentification dite forte à deux facteurs partout dans le monde.

Avec 3-D Secure v2 :

- l'**authentification en mode pop-in** remplace la redirection vers la page de l'ACS ;
- l'authentification est mieux adaptée pour les nouveaux canaux de paiement comme les **paiements in-app** et les **paiements via mobile**.

**Plus d'informations échangées entre les différents acteurs** :

Avec la 3DS2, les données partagées sont 10 fois plus nombreuses et peuvent être classées en 4 catégories :

- **Transaction & Données client** :

  Contient des informations obligatoires ou optionnelles récoltées depuis le parcours client sur le site marchand et depuis le détail de la transaction :

  - numéro de carte et date d'expiration ;
  - adresse de facturation ;
  - adresse de livraison ;
  - nom du marchand ;
  - URL du site marchand ;
  - pays ;
  - code MCC ;
  - BIN acquéreur ;
  - MID ;
  - montant ;
  - devise ;
  - type de transaction.

- **Données du marchand** :

  1. **Informations sur le risque marchand** :

     Données que seul le marchand est capable de vérifier à partir du détail de la commande et utilisées pour l'analyse de risques :

     - livraison à l'adresse de facturation ;
     - livraison en magasin ;
     - adresse e-mail de livraison ;
     - période de livraison ;
     - achat de carte-cadeaux ;
     - produits disponible ou pré commande ;
     - première commande ou non ;
     - score de l'analyse de risque effectuée par le marchand.

  2. **Informations sur le compte client du porteur** :

     Informations relatives aux détails ou à l'historique du compte client sur le site marchand :

     - date de création ;
     - date de modification ;
     - date du dernier changement de mot de passe ;
     - nombre de transactions ;
     - activité suspicieuse ;
     - etc.

- **Données sur l'équipement** :

  Informations spécifiques à l'équipement (navigateur / application native iOS / application native Android) :

  - adresse IP ;
  - langue ;
  - taille de l'écran ;
  - fuseau horaire ;
  - User-Agent ;
  - entêtes HTTP ;
  - modèle de l'équipement ;
  - nom de l'OS ;
  - version de l'OS ;
  - date et heure ;
  - résolution de l'écran ;
  - coordonnées GPS.

  En fonction du système d'exploitation, plusieurs dizaines d'informations pourront être exploitées (IMEI, fonts, Subscriber ID, etc.).

- **Données d'authentification** :

  1. **Authentification sur le site marchand** :

     Concerne l'authentification (non 3DS) de l'acheteur pour accéder au site marchand :

     - méthode d'authentification ;

- date et heure de connexion ;
- données d'authentification.

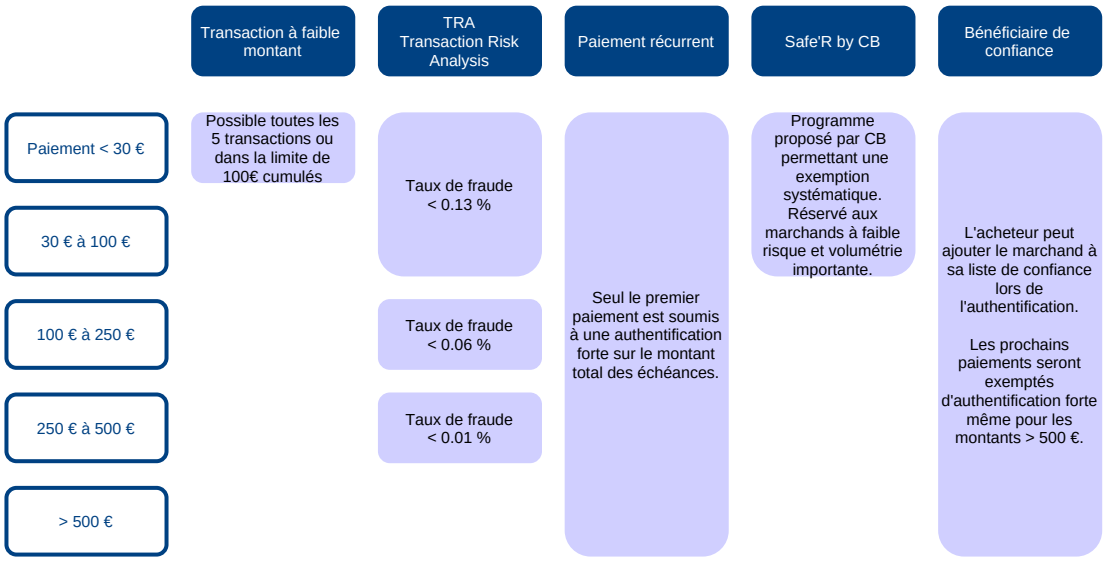
2. **Précédente authentification forte** :

   Données d'authentification 3DS issues d'une précédente transaction réalisée par le même porteur de carte avec le même moyen de paiement :

   - méthode d'authentification (frictionless ou challenge) ;
   - date et heure de l'authentification 3DS ;
   - données d'authentification (numéro de transaction ACS).

## 2.1. Les exemptions à l'authentification forte

La deuxième Directive sur les services de paiement (ou DSP2) impose l'authentification forte pour les paiements lorsque l'acheteur est présent lors de l'achat mais prévoit aussi des cas pour lesquels l'interaction avec l'acheteur (le challenge) n'est pas obligatoire. Pour bénéficier d'une authentification passive (frictionless), le paiement doit être éligible à une exemption. Voici les cas prévus par la DSP2 :




- Paiement récurrent : Seul le premier paiement est soumis à une authentification forte sur le montant total des échéances.
- Bénéficiaire de confiance : L'acheteur peut ajouter le marchand à sa liste de confiance lors de l'authentification. Les prochains paiements seront exemptés d'authentification forte même pour les montants > 500 €.

### 2.1.1. Transaction à faible montant

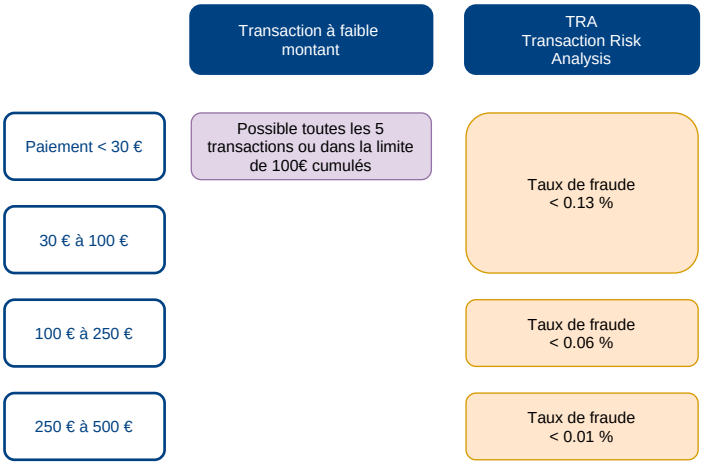
En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 €, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 €.Si le montant est supérieur à 30 €, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.

Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

Si la boutique ne dispose pas de l'option "Frictionless 3DS2", le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

### 2.1.2. Transaction Risk Analysis (TRA Acquéreur)




Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte si le montant est inférieur au seuil fixé par votre établissement financier. Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

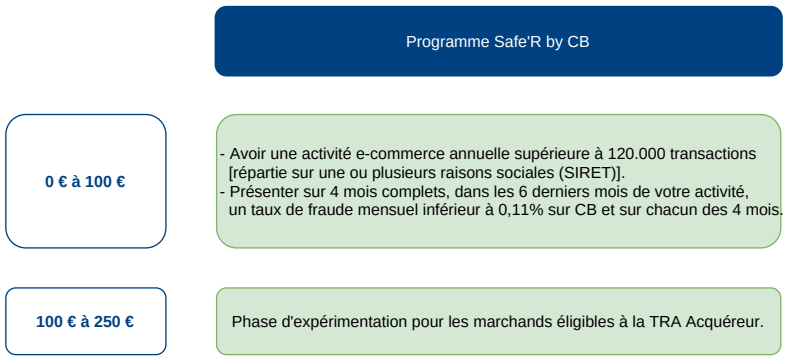
L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier.

### 2.1.3. Safe'R by CB

Certaines banques indiquent que le marchand doit pouvoir réaliser une demande d'authentification frictionless sans préciser de motif d'exemption particulier.

Pour répondre à ce besoin, CB propose le programme Safe'R by CB anciennement LRM (=Low Risk Merchant).

Ce programme Safe'R by CB est une exemption qui permet aux marchands détenteurs de contrats CB à faire du frictionless. Son objectif est de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Il permet de valoriser les investissements faits sur la lutte contre la fraude, en optimisant le taux de frictionless lorsque la réglementation le permet.




Jusque-là, le programme Safe'R by CB couvre jusqu'à 100 € pour une exemption systématique des bénéficiaires éligibles. Le GIE CB a démarré une expérimentation de la tranche 100 € à 250 €.

Dans les modalités de mise en œuvre de la tranche d'expérimentation de 100 € à 250 €, CB informe que pour bénéficier du frictionless avec application du programme Safe'R by CB, le marchand doit :

- avoir un contrat CB ;

- être éligible à la TRA acquéreur ;
- et transmettre les valeurs requises dans le flux 3-D Secure, selon les règles définies dans la plateforme.

Le programme Safe'R by CB s'applique sans date de fin pour les paiements compris entre 0-100 €.

Le bénéfice du programme sur la tranche 100-250 € est en phase d'expérimentation jusqu'au 30 septembre 2024 selon CB.

Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

Pour bénéficier du programme Safe'R by CB, vous devez contacter l'administration des ventes pour obtenir un accord explicite.

## 2.2. Les transactions non concernées par la SCA

Rappel

La **SCA** (Strong Customer Authentication) est une méthode d'authentification durant laquelle l'acheteur doit répondre à, au moins, deux facteurs d'authentification.

La deuxième Directive sur les services de paiement (ou DSP2) impose l'authentification forte mais décrit également les cas non concernés par cette authentification forte.

Il s'agit des cas suivants :

- **Les transactions initiées par le marchand (ou "MIT")**.

  Il s'agit des paiements réalisés sans la présence en ligne de l'acheteur (paiement par fichier, paiement par web services de serveur à serveur, duplication).

  Par exemple, lorsque le marchand gère lui même les récurrences dans le cas d'un abonnement à montant et dates d'échéance variables.

  L'authentification forte est néanmoins obligatoire lors de l'enregistrement du moyen de paiement et lors du premier paiement d'un abonnement ou d'un paiement en plusieurs fois.

- **Les paiements VAD (ou "MOTO" - Mail Order Telephone Order)**.

  Il s'agit d'achats initiés par courrier, e-mail ou téléphone et dont la saisie des données de la carte est réalisée par un opérateur.

- **Les transactions hors Espace Economique Européen (ou one-leg transactions)**.

  Paiements pour lesquels l'un des acteurs du paiement, l'acquéreur ou l'émetteur, se trouve hors de l'espace économique européen.

## 2.3. Exprimer un choix ou désactiver l’authentification

**En 3DS2, le marchand peut exprimer un choix.**

Dans le cadre de la DSP2, il n'est plus possible de désactiver l'authentification en 3DS2.

Le marchand peut, cependant, exprimer son choix quant à l'authentification du porteur.

On parle alors de "**préférence 3-D Secure**".

Parmi les choix disponibles, le marchand peut :

- demander une authentification forte, avec interaction du porteur (Challenge) ;
- demander une authentification sans interaction (Frictionless) s'il a l'option "Frictionless 3DS2" ;
- ne pas exprimer de choix et laisser l'émetteur décider (No Preference).

Par défaut, le choix "no preference" est appliqué.

Le choix du marchand s'effectue :

- soit depuis la requête de paiement ;
- soit au travers d'un module de paiement (Prestashop, Magento, etc. ) ;
- soit depuis le Back Office Expert s'il est habilité à accéder au module de risque avancé.

**Demande de frictionless**

Les marchands ayant souscrit une offre incluant l'option "Frictionless 3DS2" peuvent demander une exemption à l'authentification forte dans la requête de paiement.

L'option "Frictionless 3DS2" permet :

- d'exprimer une préférence quant au mode d'authentification ;
- de demander un paiement sans interaction du porteur (Frictionless).

L'acheteur n'a pas à s'authentifier si la demande est acceptée par l'émetteur, mais le marchand assure la responsabilité en cas d'impayé (pas de transfert de responsabilité à l'émetteur).

En Europe, le marchand peut demander une exemption à l'authentification forte, pour les transactions à faible montant en euro (inférieures à 30 EUR).

Toutes les transactions inférieures à 30 EUR ne sont pas systématiquement soumises à une authentification forte. D'autres exemptions existent comme l'application d'une TRA Acquéreur ou d'un bénéficiaire de confiance.

Pour les paiements réalisés dans une devise différente de l'euro, une demande d'authentification sans interaction (frictionless) est transmise à l'émetteur quel que soit le montant, si le marchand en fait la demande et s'il dispose de l'option "Frictionless 3DS2".

Les cas d'exemptions supportés sont :

- **Transactions à faible montant**

  En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 EUR, et dans la limite soit de 5 opérations successives ou d’un montant cumulé inférieur à 100 EUR.

  Si le montant est supérieur à 30 EUR, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

  Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.

  Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

- **Transactional Risk Analysis** (TRA Acquéreur)

  Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte si le montant est inférieur au seuil fixé par votre établissement financier.

  Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

  L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier.

- **Safe'R by CB**

  Le programme Safe'R by CB est une exemption qui permet aux marchands détenteurs de contrats CB à faire du frictionless. Son objectif est de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Il permet de valoriser les investissements faits sur la lutte contre la fraude, en optimisant le taux de frictionless lorsque la réglementation le permet.

  Jusque-là, le programme Safe'R by CB couvre jusqu'à 100 EUR pour une exemption systématique des bénéficiaires éligibles. Le GIE CB a démarré une expérimentation de la tranche 100 EUR à 250 EUR.

  Le programme Safe'R by CB s’applique sans date de fin pour les paiements compris entre 0-100 EUR.

  Le bénéfice du programme sur la tranche 100-250 EUR est en phase d’expérimentation jusqu’au 30 septembre 2024 selon CB.

La plateforme détermine automatiquement le motif d'exemption à transmettre à l'émetteur en fonction des options de votre boutique et du montant de la transaction.

## 2.4. Transfert de responsabilité

L'enrôlement du contrat à 3-D Secure permet de protéger le marchand contre le motif d'impayés "contestation du porteur".

Les transactions bénéficiant du transfert de responsabilité sont caractérisées :

- par la valorisation à **YES** du paramètre **vads_warranty_result** dans la réponse d'un paiement réalisé en mode redirection ;
- par la valorisation à **YES** du paramètre **liabilityShift** dans la réponse d'un paiement réalisé en mode embarqué ;
- par la valorisation de la rubrique **Transfert de responsabilité** à **OUI** dans Back Office Expert ;
- par la valorisation de la donnée **3D_LS** à **YES** dans le journal des transactions.

Dès lors que ces données sont renseignées à une toute autre valeur (**NO** ou **UNKNOWN** par exemple), la transaction ne bénéficie pas du transfert de responsabilité vers l'émetteur de la carte. .

L'enrôlement du contrat à 3-D Secure ne protège pas contre tous les motifs d'impayés et de fraude.

En complément, pour rentrer dans le périmètre de garantie 3-D Secure, la transaction doit avoir été réalisée par une carte éligible (réseau, zone géographique, produit), et sous des conditions bien définies.

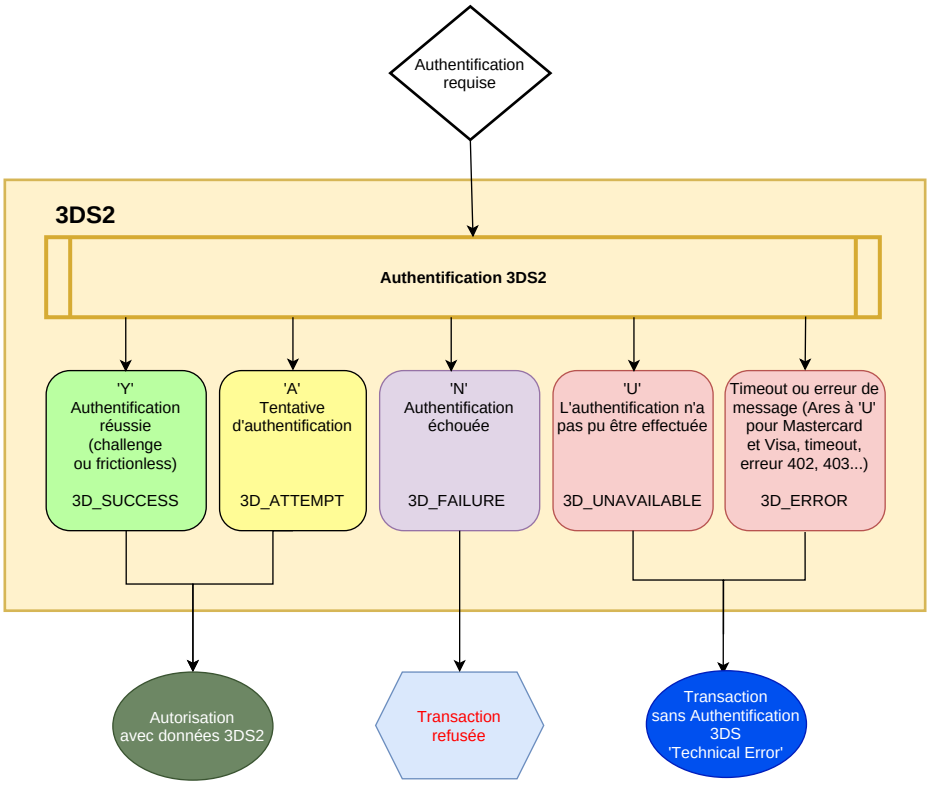
Le commerçant doit donc dans tous les cas rester vigilant en analysant les commandes de façon à ne pas expédier la marchandise en cas de suspicion de fraude. En effet, si le taux de fraude du marchand dépassait des standards définis par VISA et MASTERCARD, ces derniers pourraient d'autorité annuler la protection 3-D Secure.

**Par ailleurs, la protection 3-D Secure ne s'applique pas :**

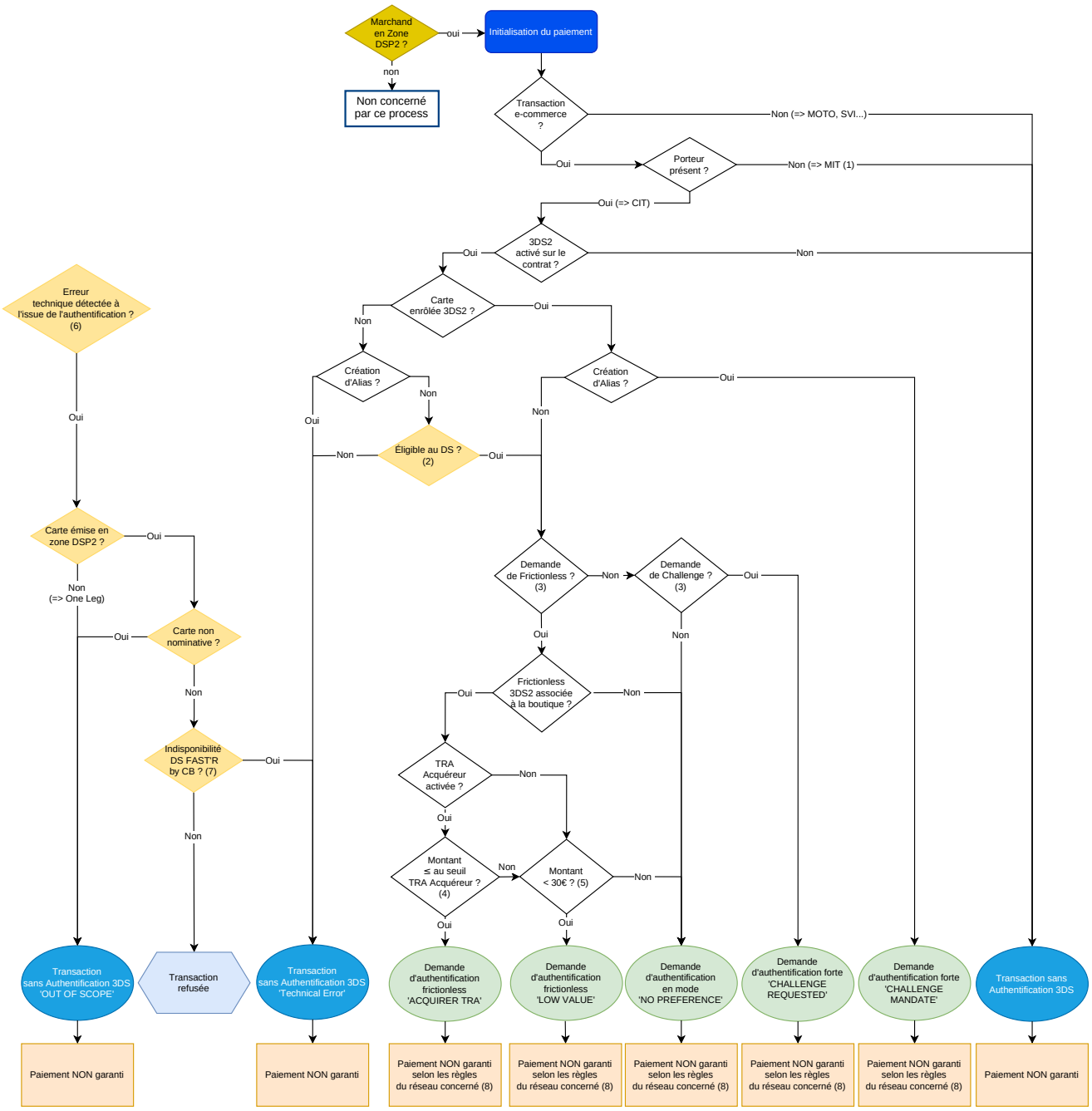
- aux paiements saisis manuellement par le marchand;
- aux transactions "dupliquées" par le marchand;
- aux paiements différés au-delà de la validité de l'autorisation (6 jours pour CB);
- aux diverses échéances des paiements en plusieurs fois, autres que la 1ère échéance ;
- aux paiements récurrents;
- aux paiements réalisés avec le service d'échange de fichiers.

## 2.5. Schéma de principe de l'authentification

Le schéma ci-dessous illustre le principe de l'authentification 3-D Secure 2 :



## 2.6. Diagramme décisionnel 3-D Secure





**Légende du diagramme**

*MIT (Merchant Initiated Transaction).*

*CIT (Client Initiated Transaction*).

*MOTO (Mail Order/Téléphone Order).*

*SVI (Serveur vocal interactif).*

*One leg transaction (paiements pour lesquels l'un des acteurs du paiement, l'acquéreur ou l'émetteur, ne se trouve pas dans l'espace économique européen.*

*Carte non nominative (par exemple carte cadeau).*

1. Hors paiement à l'expédition bénéficiant de la garantie de paiement dans les 30 jours pour un paiement CB.
2. Prise en charge de l'authentification par le *DS*. Visa et Mastercard ont chacun ses propres critères d'éligibilité. Par exemple, *Smart Authentication* pour Mastercard. Pas d'éligibilité au *DS* sur CB ou AMEX.
3. Demandes émises par le marchand.
4. Seuil défini sur le contrat du marchand par l'acquéreur. L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier. Contactez-nous une fois l'accord obtenu.L'option "TRA Acquéreur 3DS2" est activée sur la plateforme Lyra Collect.
5. Si la devise est différente de l'euro, le montant équivalent en euro sera pris en cas de conversion de devise. La règle sur la devise convertie sera appliquée.
6. Valorisé à 'U' pour Visa et Mastercard, et 402, 403, etc. Voir : Schéma de principe de l'authentification à la page 16
7. La transaction est refusée. Une autorisation est tentée si le retour d'authentification est 'U' ou '13'.
8. Garantie de paiement :
   - **Paiement non garanti** chez CB et Mastercard. Chez Visa, la garantie est possible selon les émetteurs (ACS).
   - **Paiement garanti** chez CB et Mastercard. Chez Visa, la garantie est possible selon les émetteurs (ACS).

# 3. RESTITUTION DES DONNÉES D'AUTHENTIFICATION DANS LE BACK OFFICE EXPERT

## 3.1. Consulter le résultat de l'authentification du porteur

Le détail de la transaction est consultable dans le Back Office Marchand. Un onglet **3-D Secure** (ou **SafeKey** pour les carte American Express) présente toutes informations nécessaires pour comprendre le résultat de l'authentification du porteur. Si l'onglet est absent, cela signifie que la transaction est non 3DS.

Dans la section **Récapitulatif** vous avez :

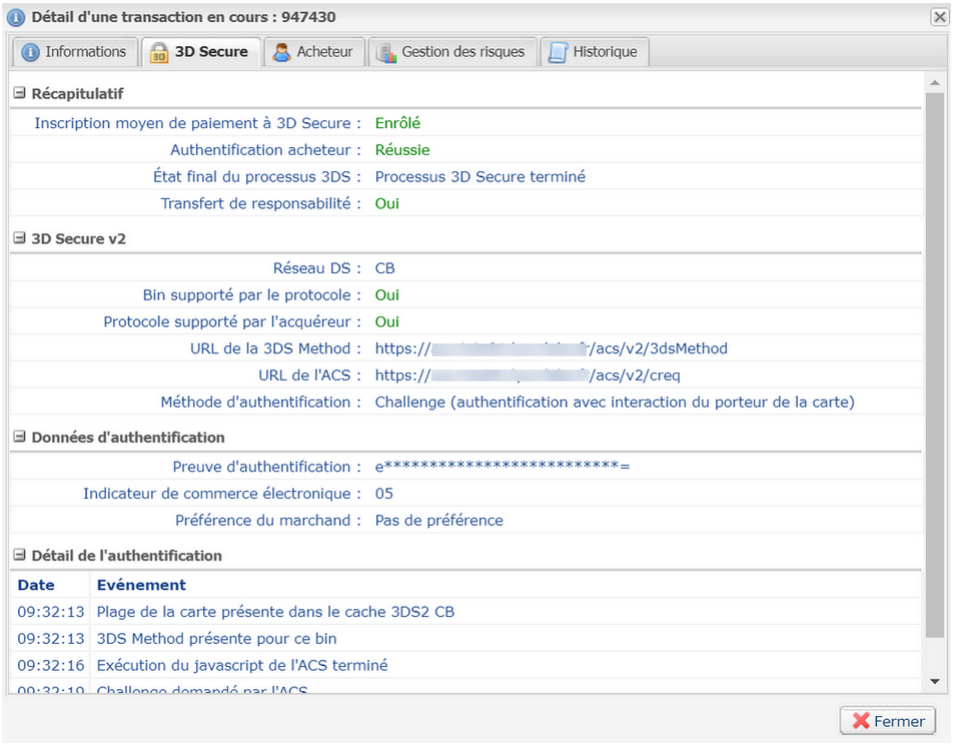
- le statut de l'inscription du moyen de paiement au programme 3-D Secure ;
- le statut de l'authentification du porteur ;
- l'état final du processus 3-D Secure ;
- le résultat du calcul du transfert de responsabilité.

Les autres rubriques donnent des informations techniques sur le processus d'authentification :

- **3-D Secure v2** : indique la méthode d'authentification du porteur (frictionless ou challenge) ;
- **Données d'authentification** : indique la préférence du marchand et la raison de l'erreur reçue du service d'authentification en 3DS2 ;
- **Détail de l'authentification** : liste les différents événements intervenus lors de l'authentification.

Les chapitres suivants vous aide à interpréter ces informations en fonction des différents cas d'usage.

### 3.1.1. Transaction avec authentification forte réussie




- **Récapitulatif** :

  Le moyen de paiement est enrôlé et l'acheteur s'est authentifié correctement sur le site d'authentification de sa banque (ACS).

  L'absence de point d'exclamation rouge sur les différents onglets, indique que le paiement est réussi.

  La rubrique Transfert de responsabilité est positionnée à **Oui**. Ainsi, en cas de fraude, les frais ne seront pas imputés au marchand.

- **Authentification** :

  Le réseau DS qui se charge de la sécurisation est présenté.

  Le *bin* du moyen de paiement supporte le protocole 3-D Secure v2.

  Le protocole 3-D Secure v2 est également supporté par l'acquéreur.

  Un challenge (authentification forte avec interaction) a été requis et réalisé avec succès pour la transaction.

- **Données d'authentification** :
  - Preuve d'authentification : la donnée sensible (CAVV, AEVV ou AAV) montrant la preuve de l'authentification du porteur par l'ACS est présente et masquée.
  - Indicateur de commerce électronique : l'acheteur s'est correctement authentifié. La valeur **05** indique une authentification réussie sur **CB**, **VISA** et **AMEX**. La valeur **02** indique une authentification réussie sur **MasterCard**.
  - Préférence du marchand : la valeur **Pas de préférence** indique que le marchand n'a pas exprimé de choix sur la méthode d'authentification.

- **Détail de l'authentification** :

  La chronologie des événements est affichée en détail pour un meilleur suivi en cas de besoin d'assistance technique.

### 3.1.2. Transaction avec authentification frictionless réussie

Vous avez deux cas de figure sur une transaction avec authentification frictionless réussie :

1. L'émetteur a reçu un choix "No Preference" ou "Challenge Requested". Il a évalué le risque de la transaction et a décidé qu'une authentification sans interaction était suffisante.


  - **Récapitulatif** :

    Le moyen de paiement est enrôlé et l'acheteur s'est authentifié correctement sur le site d'authentification de sa banque (ACS).

    L'absence de point d'exclamation rouge sur les différents onglets, indique que le paiement est réussi.

La rubrique Transfert de responsabilité est positionnée à **Oui**. Ainsi, en cas de fraude, les frais ne seront pas imputés au marchand.

- **Authentification** :

  Le réseau DS qui se charge de la sécurisation est présenté.

  Le *bin* du moyen de paiement supporte le protocole 3-D Secure v2.

  Le protocole 3-D Secure v2 est également supporté par l'acquéreur.

  Une authentification sans interaction du porteur (frictionless) a été accordée par la banque mais non demandée par le marchand.

  La transaction bénéficie du transfert de responsabilité.

- **Données d'authentification** :

  - Preuve d'authentification : la donnée sensible (CAVV, AEVV ou AAV) montrant la preuve de l'authentification du porteur par l'ACS est présente et masquée.
  - Indicateur de commerce électronique : l'acheteur s'est correctement authentifié. La valeur **05** indique une authentification réussie sur **CB**, **VISA** et **AMEX**. La valeur **02** indique une authentification réussie sur **MasterCard**.
  - Préférence du marchand : la valeur **Pas de préférence** indique que le marchand n'a pas exprimé de choix sur la méthode d'authentification.

- **Données d'authentification** :

  - Preuve d'authentification : la donnée sensible (CAVV, AEVV ou AAV) montrant la preuve de l'authentification du porteur par l'ACS est présente et masquée.
  - Indicateur de commerce électronique : l'acheteur s'est correctement authentifié. La valeur **05** indique une authentification réussie sur **CB**, **VISA** et **AMEX**. La valeur **02** indique une authentification réussie sur **MasterCard**.
  - Préférence du marchand : la valeur **Pas de préférence** indique que le marchand n'a pas exprimé de choix sur la méthode d'authentification.
  - Motif de l'exemption : donne la raison qui justifie une authentification sans interaction du porteur.

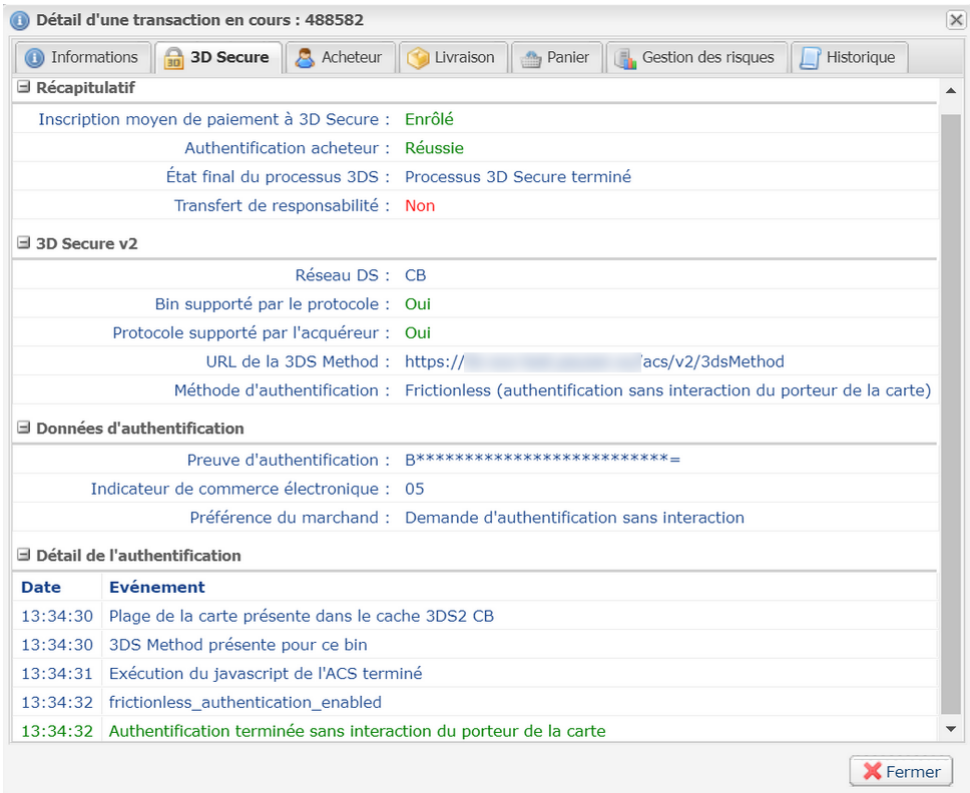
    Dans cet exemple, le motif est transmis par l'émetteur. Consultez la liste des exemptions.

- **Détail de l'authentification** :

  La chronologie des événements est affichée en détail pour un meilleur suivi en cas de besoin d'assistance technique.

2. Le marchand dispose de l'option "Frictionless 3DS2" et a demandé une authentification sans interaction du porteur. L'émetteur de la carte a accepté la demande.

   - **Récapitulatif** :




Le moyen de paiement est enrôlé et l'acheteur s'est authentifié correctement sur le site d'authentification de sa banque (ACS).

L'absence de point d'exclamation rouge sur les différents onglets, indique que le paiement est réussi.

La rubrique Transfert de responsabilité est positionnée à **Non**. Ainsi, en cas de fraude de l'acheteur, les frais sont à la charge du marchand.

- **Authentification** :

  Le réseau DS qui se charge de la sécurisation est présenté.

  Le *bin* du moyen de paiement supporte le protocole 3-D Secure v2.

  Le protocole 3-D Secure v2 est également supporté par l'acquéreur.

  Une authentification sans interaction du porteur est demandée par le marchand et la demande a été acceptée par la banque. Ce mode d'authentification est valable en 3DS2 sur un montant en euro inférieur à 30 EUR.

  La transaction ne bénéficie pas du transfert de responsabilité.

- **Données d'authentification** :

  - Preuve d'authentification : la donnée sensible (CAVV, AEVV ou AAV) montrant la preuve de l'authentification du porteur par l'ACS est présente et masquée.
  - Indicateur de commerce électronique : l'acheteur s'est correctement authentifié. La valeur **05** indique une authentification réussie sur **CB**, **VISA** et **AMEX**. La valeur **02** indique une authentification réussie sur **MasterCard**.
  - Préférence du marchand : dans cet exemple, le marchand a demandé une authentification sans interaction du porteur. En fonction des options de la boutique et des caractéristiques de la transaction, la plateforme a transmis la demande à l'émetteur.
  - Motif de l'exemption : donne la raison qui justifie une authentification sans interaction du porteur.

    Dans cet exemple, le motif est transmis par la plateforme de paiement. Consultez la liste des exemptions.

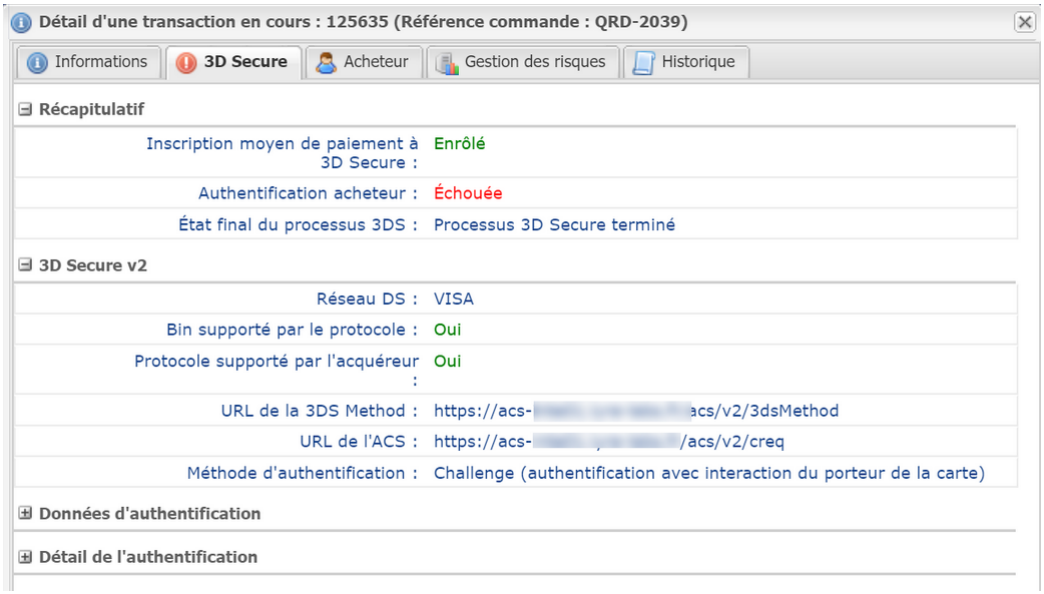
- **Détail de l'authentification** :

  La chronologie des événements est affichée en détail pour un meilleur suivi en cas de besoin d'assistance technique.

**Liste des motifs d'exemption** :

- Analyse de risque par l'émetteur ;
- Transaction Risk Analysis (TRA Acquéreur) ;
- Authentification forte déléguée à un tiers ;
- Transaction à faible montant ;
- Paiements récurrents fixes à durée déterminée ;
- Le marchand participe au programme Safe'R by CB ;
- Autre cas d'exemption ;
- Une erreur technique empêche l'authentification du porteur ;
- Bénéficiaires de confiance ;
- Automates de paiement ;
- Paiement par carte d'entreprise ;
- Transaction non concernée par la SCA (Strong Customer Authentication) ;
- Autre exemption reçue du DS.

### 3.1.3. Transaction avec authentification 3-D Secure en échec




Le point d'exclamation rouge à gauche du nom de l'onglet indique que la raison du refus est liée à l'authentification 3-D Secure.

Le moyen de paiement est enrôlé 3-D Secure et une authentification forte (challenge) était requise.

Le statut de l'authentification ("**Echouée**") indique que le porteur ne s'est pas authentifié correctement sur le site d'authentification de sa banque (ACS).

Exemple de motifs de refus :

- "39 : Refus 3-D Secure pour la transaction" : correspond à une mauvaise saisie du code d'authentification ; ce qui a entraîné le refus du paiement.

- "206 : 3-D Secure - Une erreur technique est survenue lors du processus" :

  Ce type d'erreur peut apparaître lorsque l'acheteur effectue sa transaction via un mobile avec une mémoire insuffisante. La transaction échoue lors de la phase d'authentification et l'ACS nous remet un message d'erreur visible dans le détail de la transaction.

Exemple : "Erreur reçue de l'ACS : TRANSACTION_DATA_NOT_VALID"

Détail de l'authentification

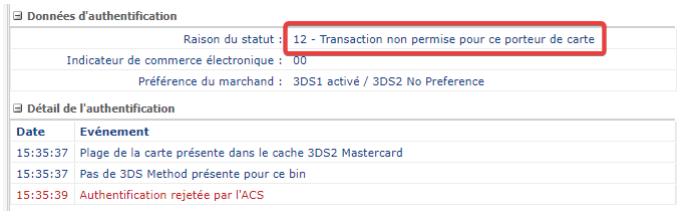
| Date | Evénement |
|---|---|
| 14:47:55 | Plage de la carte présente dans le cache 3DS2 CB |
| 14:47:55 | Pas de 3DS Method présente pour ce bin |
| 14:47:55 | Challenge imposé par l'ACS |
| 14:48:47 | Notification de fin d'authentification forte reçue (RREQ) |
| 14:48:47 | Réception du résultat de challenge (CRES) |
| 14:48:47 | Erreur reçue de l'ACS: TRANSACTION_DATA_NOT_VALID - C0000: A Session with acsTransID b77d5a47-b52d-4fb6-bc5c-5afd21cf46b6 has already been completed. - CReq message with this ACS Transaction ID has already been received and processed. |
| 14:48:48 | Authentification échouée |

- "207 : Refus de l'authentification par l'émetteur (Transaction non permise pour ce porteur de carte)" :

  Les serveurs d'authentification (ACS) ont rejeté l'authentification.

  L'acheteur doit demander à sa banque si la carte utilisée autorise des paiements avec authentification 3DS2 et/ou des paiements via un site e-commerce.

  Raison du statut : "12-Transaction non permise à ce porteur"



Données d'authentification

Raison du statut : 12 - Transaction non permise pour ce porteur de carte
Indicateur de commerce électronique : 00
Préférence du marchand : 3DS1 activé / 3DS2 No Preference

Détail de l'authentification

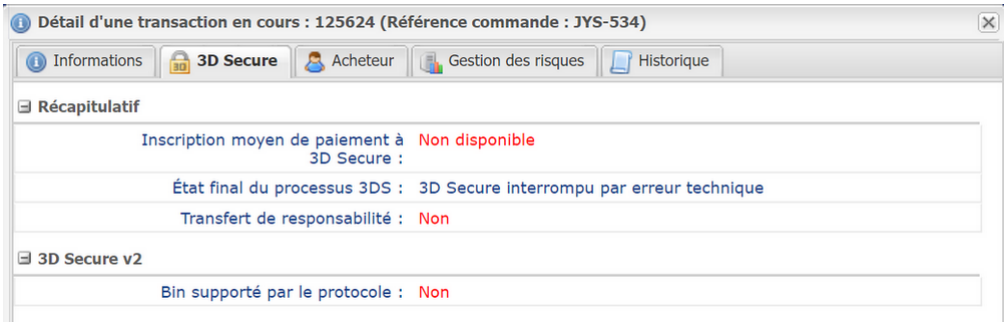
| Date | Evénement |
|---|---|
| 15:35:37 | Plage de la carte présente dans le cache 3DS2 Mastercard |
| 15:35:37 | Pas de 3DS Method présente pour ce bin |
| 15:35:39 | Authentification rejetée par l'ACS |

### 3.1.4. Transaction avec erreur technique durant l'authentification

Ce cas peut se produire lorsque :

- le statut de l'inscription du moyen de paiement est inconnu ;
- le statut d'authentification de l'acheteur est inconnu.

Exemple du cas "statut de l'inscription du moyen de paiement non disponible" :



Détail d'une transaction en cours : 125624 (Référence commande : JYS-534)

Informations | 3D Secure | Acheteur | Gestion des risques | Historique

Récapitulatif

| | |
|---|---|
| Inscription moyen de paiement à 3D Secure : | Non disponible |
| État final du processus 3DS : | 3D Secure interrompu par erreur technique |
| Transfert de responsabilité : | Non |

3D Secure v2

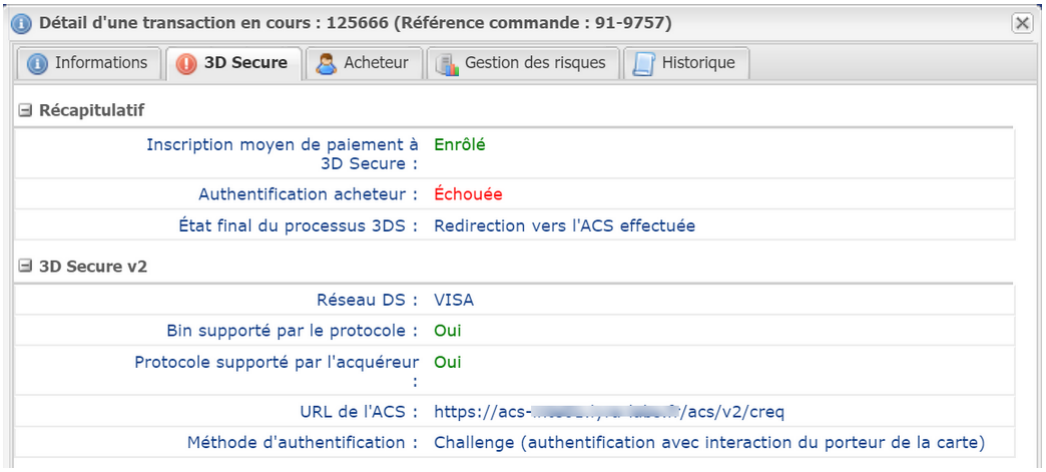
| | |
|---|---|
| Bin supporté par le protocole : | Non |

Dans ce cas de figure, une erreur est survenue lors de la vérification du statut de l'inscription du moyen de paiement.

Le processus 3-D Secure s'est arrêté prématurément.

Le paiement s'est poursuivi sans authentification du porteur. Conformément aux règles du réseau concerné, cela a entraîné la perte du transfert de responsabilité à l'émetteur.

### 3.1.5. Session de paiement expirée



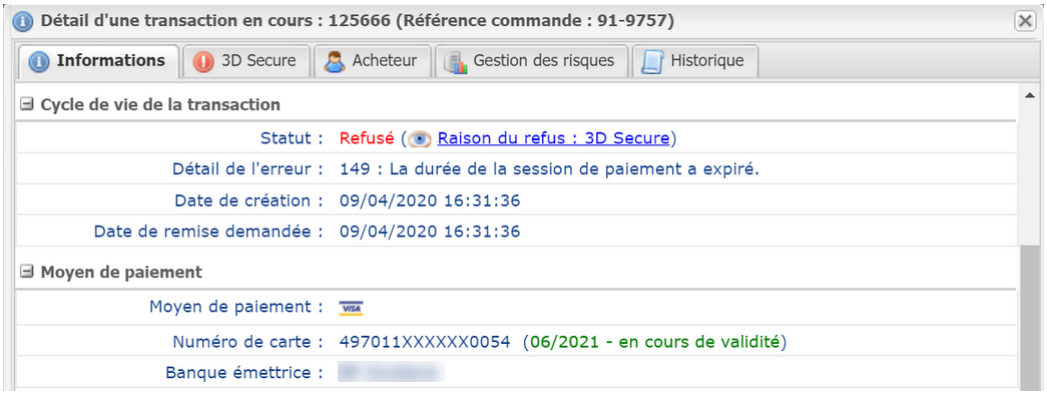

Le moyen de paiement est enrôlé 3-D Secure et une authentification forte (challenge) a été requise.

Le navigateur de l'acheteur a été redirigé vers le site d'authentification de sa banque (ACS).

L'URL du site d'authentification (ACS) est indiquée dans la section 3-D Secure correspondante au protocole utilisé pour l'authentification..

A ce stade, la plateforme de paiement reste en attente d'un retour du navigateur.

Au bout de 10 minutes sans réponse (durée de la session de paiement), le paiement est refusé pour motif "149 - session de paiement expirée".




Parmi les causes possibles :

- l'acheteur a mis trop de temps avant de procéder à l'authentification ;
- l'acheteur a fermé la fenêtre d'authentification ;
- l'acheteur n'a pas reçu le code d'authentification par SMS ;
- l'acheteur a installé un plugin sur son navigateur ou un antivirus qui empêche l'ouverture de la page de l'ACS ;
- la page de l'ACS ne s'est pas affichée car le serveur ACS est indisponible ;
- la page de l'ACS ne s'affiche pas correctement.

La plateforme de paiement n'est jamais en cause sur ces cas d'erreur. Elle ne gère pas les serveurs d'authentification des banques et n'est jamais en contact avec eux.

Seul le navigateur de l'acheteur interagit avec les serveurs d'authentification des banques.

## 3.2. Gestion de la préférence 3-D Secure dans les liens de paiement

Dans le cadre de la DSP2, le marchand peut exprimer son choix quant à l'authentification du porteur.

Pour plus d'informations, voir : Exprimer un choix ou désactiver l'authentification à la page 13.

La page de création d'un lien de paiement affiche une rubrique de paramétrage : **"Préférence 3-D Secure pour le paiement par carte"**.

Pour y avoir accès, votre boutique doit posséder au moins l'une des fonctions "Frictionless 3DS2".

Cette section est réduite par défaut. En la dépliant, vous pourrez modifier votre préférence 3-D Secure.

Il est recommandé de modifier la valeur par défaut avec prudence.

Une mauvaise préférence peut entraîner la perte du transfert de responsabilité à l'émetteur en cas d'impayé.

Par défaut, le choix de la préférence est délégué à l'émetteur de la carte (No Preference).

Les différentes combinaisons proposées dépendent des options de la boutique. Par exemple l'authentification sans interaction de l'acheteur (Frictionless) est proposée uniquement si la boutique dispose de l'option "Frictionless 3DS2".

Pour chaque préférence, une aide est disponible en cliquant sur le symbole "?".

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Ainsi, si vous avez demandé l'enregistrement du moyen de paiement, vous ne pourrez pas modifier la préférence 3-D Secure.

## 3.3. Gestion de la préférence 3-D Secure et gestion des risques

### 3.3.1. Comportement 3-D Secure par défaut

Si la carte est enrôlée 3D Secure v2, l'authentification est réalisée avec la préférence marchand "No preference". Dans ce cas, l'établissement bancaire émetteur décide du mode d'authentification le plus adapté en fonction des caractéristiques de la transaction.

Si la carte n'est pas enrôlée 3D Secure, il n'y a pas d'authentification préalable de l'acheteur et vous ne bénéficierez pas du transfert de responsabilité.

### 3.3.2. Présentation des actions

L'option **Gestion des risques avancée** donne accès à des actions spécifiques à l'authentification du porteur lors du paramétrage des règles :

| Action | Description |
|---|---|
| **Définir un mode d'authentification** | Cette action n'est disponible que si 3-D Secure v2 est activé sur au moins un des contrats associés à la boutique.<br>Elle permet de modifier le mode d'authentification par défaut (NO_PREFERENCE) appliqué lors du paiement.<br>Les choix disponibles dépendent des options de la boutique.<br>Si votre boutique dispose de l'option "Frictionless 3DS2" et est associée à un contrat 3DS2 activé, vous aurez le choix entre les modes d'authentification suivants :<br>• **Demande d'authentification avec interaction de l'acheteur (Challenge)**<br>• **Demande d'authentification sans interaction de l'acheteur (Frictionless)**<br>En choisissant le choix "Frictionless", l'authentification 3-D Secure v2 sera réalisée avec une préférence marchand forcée à Frictionless si une exemption s'applique (voir "Application des exemptions").<br>Pour plus d'informations, cliquez sur le "?" présent dans la colonne Aide. |

**Application des exemptions :**

Les cas d'exemptions supportés sont :

- **Transactions à faible montant**

  En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 EUR, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 EUR.

  Si le montant est supérieur à 30 EUR, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

  Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.

  Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

- **Transactional Risk Analysis** (TRA Acquéreur)

  Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte si le montant est inférieur au seuil fixé par votre établissement financier.

  Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier.

- **Safe'R by CB**

  Le programme Safe'R by CB est une exemption qui permet aux marchands détenteurs de contrats CB à faire du frictionless. Son objectif est de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Il permet de valoriser les investissements faits sur la lutte contre la fraude, en optimisant le taux de frictionless lorsque la réglementation le permet.

  Jusque-là, le programme Safe'R by CB couvre jusqu'à 100 EUR pour une exemption systématique des bénéficiaires éligibles. Le GIE CB a démarré une expérimentation de la tranche 100 EUR à 250 EUR.

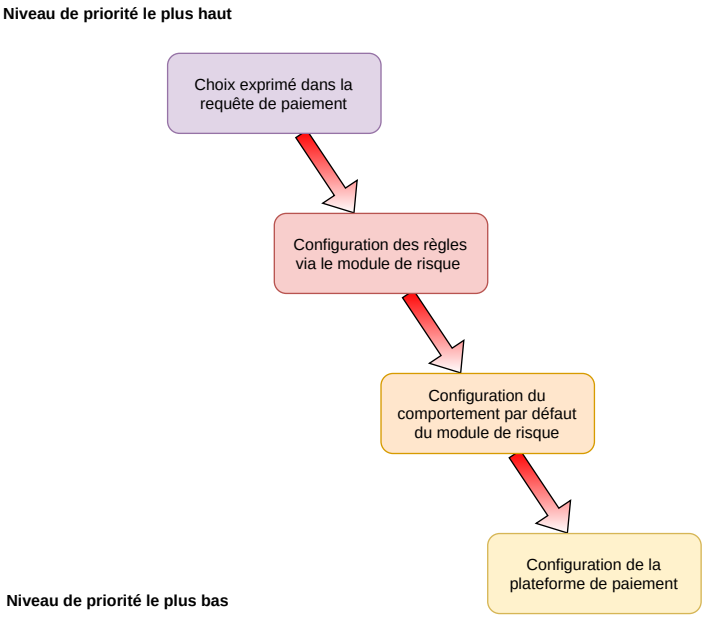
  Le programme Safe'R by CB s'applique sans date de fin pour les paiements compris entre 0-100 EUR.

  Le bénéfice du programme sur la tranche 100-250 EUR est en phase d'expérimentation jusqu'au 30 septembre 2024 selon CB.

- Pour les paiements réalisés en euro, si le montant est inférieur à 30€, une demande de frictionless est transmise à l'émetteur. **Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas d'impayé**.
- Pour les paiements réalisés en euro, si le montant est supérieur à 30€, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).
- Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur. **Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas d'impayé**.
- Si la boutique ne dispose pas de l'option "Frictionless 3DS2", le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

### 3.3.3. Priorité entre les différents moyens d'exprimer la préférence 3-D Secure

La préférence 3-D Secure peut être exprimée à plusieurs niveaux :




Le paramètre transmis dans la requête de paiement (**strongAuthentification** de l'API REST ou **vads_threeds_mpi** de l'API Formulaire) est prioritaire sur les décisions du module de gestion des risques.

Si le marchand n'exprime pas de souhait via la requête de paiement ou les règles de risque, alors la configuration de la plateforme de paiement est appliquée.

La préférence 3-D Secure est ignorée lorsque :

- le moyen de paiement utilisé est une Maestro,
- la plateforme de paiement réalise une nouvelle tentative de paiement après un refus soft decline,
- le marchand a demandé l'enregistrement du moyen de paiement.

# 4. UTILISATION DU FORMULAIRE EN REDIRECTION



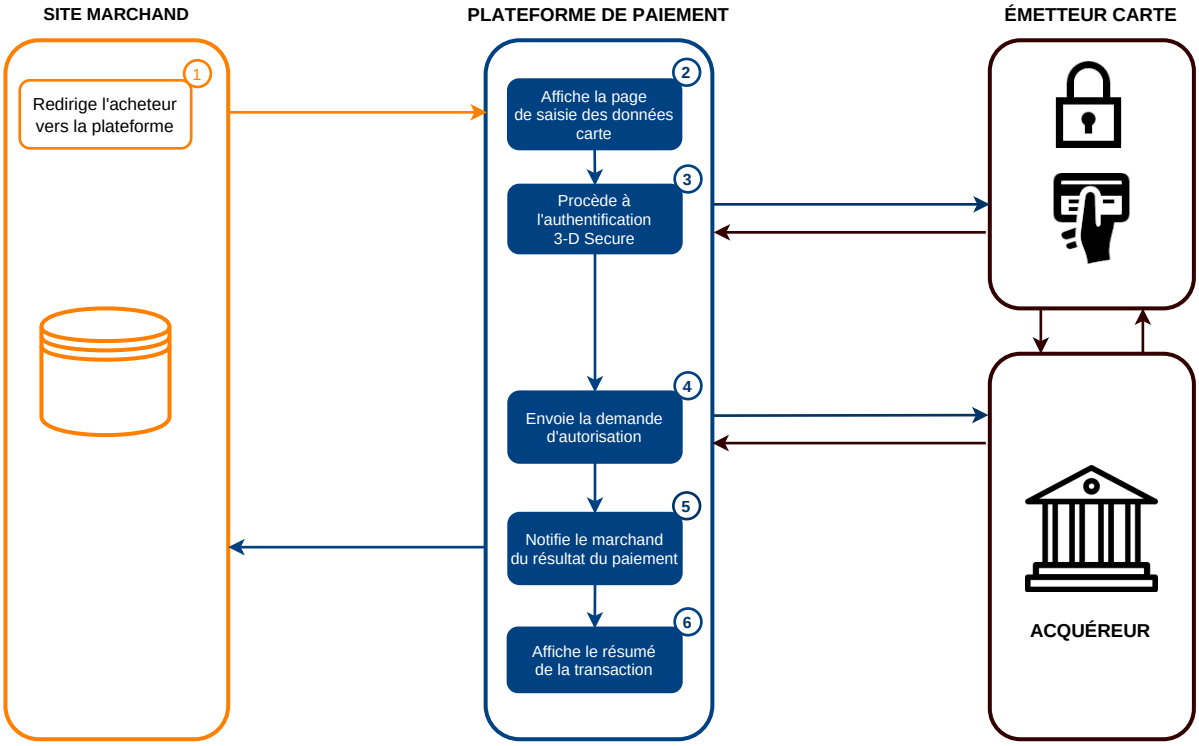
### Cas d'usage concernés

Ce chapitre s'applique pour les cas d'utilisation suivants :

- Paiement comptant avec saisie des données de la carte,
- Paiement en plusieurs fois,
- Enregistrement d'une carte (avec ou sans paiement, avec ou sans souscription à un abonnement),
- Paiement par alias.

### Cinématique

La cinématique ci-dessous s'applique aux paiements CB, VISA, MASTERCARD, AMEX.




1. Le site marchand redirige l'acheteur vers la plateforme de paiement en transmettant les données du paiement (montant, devise etc.).
2. La plateforme de paiement affiche la page de saisie des données carte.

   L'acheteur sélectionne son moyen de paiement et renseigne le numéro et la date d'expiration de sa carte.

   Si la carte possède un cryptogramme visuel, ce dernier doit obligatoirement être renseigné.
3. La plateforme de paiement procède à l'authentification 3-D Secure.
4. La plateforme de paiement réalise une demande d'autorisation auprès de l'acquéreur (la banque du marchand).
5. La plateforme de paiement notifie le site marchand du résultat du paiement.

6. En cas de succès, la plateforme de paiement affiche la page de résumé présentant les informations de la transaction.

   Si le paiement est refusé, la plateforme de paiement invite l'acheteur à tenter un nouveau paiement.

### Création du formulaire de paiement

### Analyse de la réponse

Le résultat de l'authentification 3-D Secure est transmis dans la notification de fin de paiement (IPN) et lorsque le navigateur de l'acheteur est redirigé vers le site marchand.

Voici la liste des champs décrivant l'authentification du porteur par cas d'usage :

| Cas d'usage | Champs retournés |
|---|---|
| Transaction avec authentification forte réussie. | • vads_threeds_enrolled = Y : Porteur enrôlé.<br>• vads_threeds_status = Y (Authentification réussie)<br>• vads_threeds_auth_type = CHALLENGE (Valeur retournée en 3DS1 et 3DS2).<br>• vads_threeds_eci = 5 (Visa ou AMEX) ou 02 (Mastercard).<br>• vads_warranty_result = YES : Transfert de responsabilité à l'émetteur possible en cas de contestation du porteur. |
| Transaction avec authentification frictionless réussie, le marchand dispose de l'option "Frictionless 3DS2" et a demandé une authentification sans interaction du porteur. | • vads_threeds_enrolled = Y : Porteur enrôlé.<br>• vads_threeds_status = Y : Authentification réussie.<br>• vads_threeds_auth_type = FRICTIONLESS.<br>• vads_threeds_eci = 5 (Visa ou AMEX) ou 02 (Mastercard).<br>• vads_warranty_result = NO : Pas de transfert de responsabilité à l'émetteur de la carte. |
| Transaction avec authentification frictionless réussie, le marchand n'a pas demandé une authentification sans interaction du porteur. | • vads_threeds_enrolled = Y : Porteur enrôlé.<br>• vads_threeds_status = Y : Authentification réussie.<br>• vads_threeds_auth_type = FRICTIONLESS.<br>• vads_threeds_eci = 5 (Visa ou AMEX) ou 02 (Mastercard).<br>• vads_warranty_result = YES : Transfert de responsabilité à l'émetteur possible en cas de contestation du porteur. |
| Transaction avec authentification 3-D Secure en échec. | • vads_threeds_enrolled = Y : Porteur enrôlé.<br>• vads_threeds_status = N : Erreur d'authentification.<br>• vads_threeds_auth_type = vide: l'acheteur ne s'est pas authentifié.<br>• vads_warranty_result = NO : Pas de transfert de responsabilité à l'émetteur de la carte.<br>• vads_threeds_eci = vide.<br>• vads_payment_error = 39 : Refus 3-D Secure pour la transaction. |
| Transaction avec erreur technique durant l'authentification. | • vads_threeds_enrolled = Y ou U : "Y" si porteur enrôlé, "U" si impossible de vérifier le statut d'enrôlement.<br>• vads_threeds_status = U : Authentification impossible ou vide.<br>• vads_threeds_auth_type = vide : l'acheteur ne s'est pas authentifié.<br>• vads_threeds_eci = 7(Visa ou AMEX) ou vide (Mastercard). |

| Cas d'usage | Champs retournés |
| --- | --- |
| | • vads_warranty_result = UNKNOWN : Transfert de responsabilité à l'émetteur non déterminable suite à une erreur technique.<br>• vads_payment_error =<br>  • en 3DS2 : 205, 206, 208 ou 213 : une erreur technique est survenue lors du processus.<br>  • en 3DS1 : 105 : Signature du message d'authentification invalide. |
| Session de paiement expirée. | • vads_threeds_enrolled = Y : Porteur enrôlé.<br>• vads_threeds_status = N : Erreur d'authentification.<br>• vads_threeds_auth_type = vide: l'acheteur ne s'est pas authentifié.<br>• vads_threeds_eci = vide.<br>• vads_warranty_result = vide : Le transfert de responsabilité est non applicable.<br>• vads_payment_error = 149 : Session expirée. L'acheteur a été redirigé vers l'ACS mais n'a pas finalisé l'authentification 3DS. |
| Carte non enrôlée. | • vads_threeds_enrolled = N : Porteur non enrôlé.<br>• vads_threeds_status = vide : Pas d'authentification.<br>• vads_threeds_auth_type = vide : Pas d'authentification.<br>• vads_threeds_eci = vide : Pas d'authentification.<br>• vads_warranty_result = NO : Pas de transfert de responsabilité à l'émetteur de la carte. |

## 4.1. Paiement en N fois

Une authentification forte sera toujours requise lors de la première échéance, quelle que soit la préférence du marchand.

Cette authentification portera sur le montant global c'est-à-dire la somme de toutes les échéances du paiement.

La demande d'authentification sur un paiement en N fois fait partie du dispositif réglementaire de la DSP2. Pensez à prévenir vos clients en amont avant qu'il ne procède au règlement.

## 4.2. Enregistrement d'une carte sans paiement

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte, quelle que soit la préférence du marchand.

Ainsi lorsque le marchand demande l'enregistrement d'une carte sans paiement (**vads_page_action = REGISTER**), la préférence du marchand est ignorée, qu'elle soit exprimée dans la requête (champ **vads_threeds_mpi**) ou depuis le Back Office Expert (module de gestion des risques avancée).

## 4.3. Paiement par alias

L'authentification forte est obligatoire quand le porteur est présent.

La demande de saisie du CVV est aussi obligatoire sur les boutiques de la zone d'application de la DSP2.

## 4.4. Préférence 3-D Secure

Le marchand peut exprimer son choix concernant l'authentification forte de l'acheteur en utilisant le champ vads_threeds_mpi.

La valeur transmise dans la requête de paiement est prioritaire aux règles de risque éventuellement définies par le marchand dans son Back Office Expert.

Voici comment l'utiliser :

| Cas d'utilisation | Valeurs | Description |
|---|---|---|
| **CHALLENGE** : avec interaction du porteur | **1** | **Déprécié**. |
| | **3** | **Challenge Requested (3DS Requestor Preference)** : permet de demander une authentification forte pour la transaction. |
| | **4** | **Challenge Requested (Mandate)** :permet d'indiquer que pour des raisons réglementaires, une authentification forte est requise pour la transaction. |
| **FRICTIONLESS** : sans interaction du porteur | **2*** | Permet de demander une exemption à l'authentification forte :<br>• Transactions à faible montant.<br>• Transaction Risk Analysis (TRA Acquéreur).<br>• Safe'R by CB.<br>Plus d'infos : Tableau des exemptions, ci-après. |
| Pas de préférence 3-D Secure | **0 ou absent ou vide** | Le choix de la préférence est délégué à l'émetteur de la carte. Si l'émetteur décide de réaliser une authentification sans interaction (frictionless), le paiement sera garanti. |
| | **5** | |

* **Tableau des exemptions** :

| Exemptions | Description |
|---|---|
| **Transactions à faible montant** | En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 EUR, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 EUR.<br>Si le montant est supérieur à 30 EUR, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).<br>Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.<br>Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.<br>Si la boutique ne dispose pas de l'option "Frictionless 3DS2", le choix de la préférence est délégué à l'émetteur de la carte ( No Preference). |
| **Transaction Risk Analysis (TRA Acquéreur)** | Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte lorsque le montant est inférieur au seuil fixé par votre établissement financier.<br>Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte. |

| Exemptions | Description |
| --- | --- |
| | L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier. |
| **Safe'R by CB** | CB propose le programme Safe'R by CB. Ce programme a pour objectif de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Vous pouvez demander une exemption à l'authentification forte :<br>• Si le montant est inférieur à 100 EUR, l'exemption est systématique pour les marchands éligibles.<br>• Si le montant est compris entre 100 EUR et 250 EUR, une expérimentation est en cours. Pour en bénéficier, le marchand doit :<br>  • Avoir un contrat CB.<br>  • Être éligible à la TRA acquéreur.<br>  • Transmettre les valeurs requises dans le flux 3-D Secure, selon les règles définies par la plateforme.<br>Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.<br>Pour bénéficier du programme Safe'R by CB, vous devez contacter l'administration des ventes pour obtenir un accord explicite. |

## 4.5. Champs permettant d'améliorer les chances de frictionless

Afin de permettre à l'émetteur de la carte de déterminer le risque d'une transaction, il est recommandé de transmettre un maximum d'informations lors du paiement.

Plus les émetteurs disposent d'informations sur les habitudes des porteurs de carte, plus ils sont à même de proposer une authentification sans interaction (frictionless).

Voir la liste ci-dessous :

| Nom / Description | Format / Valeurs |
|---|---|
| **vads_cust_address_number**<br>Numéro de rue - Adresse de facturation. | Format : ans..64 |
| **vads_cust_address2**<br>2ème ligne d'adresse - Adresse de facturation. | Format : ans..255 |
| **vads_cust_address**<br>1ère ligne d'adresse - Adresse de facturation. | Format : ans..255 |
| **vads_cust_cell_phone**<br>Numéro de téléphone mobile. | Format : an..32 |
| **vads_cust_city**<br>Ville - Adresse de facturation. | Format : an..128 |
| **vads_cust_email**<br>Adresse e-mail du porteur de carte. | Format : ans..150 |
| **vads_cust_national_id**<br>Identifiant national.<br>Permet d'identifier de façon unique chaque citoyen au sein d'un pays. | Format : ans..255 |
| **vads_cust_phone**<br>Numéro de téléphone. | Format : an..32 |
| **vads_cust_state**<br>Etat / Région - Adresse de facturation. | Format : ans..127 |
| **vads_cust_zip**<br>Code postal- Adresse de facturation. | Format : an..64 |
| **vads_ship_to_city**<br>Ville - Adresse de livraison. | Format : an..128 |
| **vads_ship_to_email**<br>Adresse e-mail de livraison dans le cas d'une commande e-ticket. | Format : an..128 |
| **vads_ship_to_type**<br>Type de transport | Format : enum<br>Valeurs pour 3DS2 :<br>• **RECLAIM_IN_SHOP** : Retrait de la marchandise en magasin.<br>• **RELAY_POINT** : Réseau de points de retrait tiers (Kiala, Alveol, etc).<br>• **RECLAIM_IN_STATION** : Retrait dans un aéroport, une garre ou une agence de voyage. |

| Nom / Description | Format / Valeurs |
|---|---|
| | • **PACKAGE_DELIVERY_COMPANY** : Livraison par transporteur (Colissimo, UPS, etc).<br>• **ETICKET** : Emission d'un billet électronique, téléchargement.<br>• **CARD_HOLDER_ADDRESS** : Livraison chez l'acheteur.<br>• **VERIFIED_ADDRESS** : Livraison à une adresse vérifiée (Adresse de livraison et de facturation identiques).<br>• **NOT_VERIFIED_ADDRESS** : Livraison à une adresse non vérifiée (Adresse de livraison et de facturation différentes).<br>• **SHIP_TO_STORE** : Livraison en magasin.<br>• **DIGITAL_GOOD** : Livraison digitale.<br>• **ETRAVEL_OR_ETICKET** : Billet électronique.<br>• **OTHER** : Autre.<br>• **PICKUP_POINT** : Retrait en point relais.<br>• **AUTOMATED_PICKUP_POINT** Retrait en point relais automatique. |
| **vads_ship_to_state**<br>Etat / Région - Adresse de livraison. | Format : ans..127 |
| **vads_ship_to_street2**<br>2ème ligne d'adresse - Adresse de livraison. | Format : ans..255 |
| **vads_ship_to_street**<br>1ère ligne d'adresse - Adresse de livraison. | Format : ans..255 |
| **vads_ship_to_speed**<br>Rapidité de livraison | Format : enum<br>Valeurs pour 3DS2 :<br>• **STANDARD** : Livraison standard.<br>• **EXPRESS** : Livraison en moins de 24 h.<br>• **PRIORITY**: Livraison prioritaire.<br>• **ELECTRONIC_DELIVERY** : Téléchargement électronique.<br>• **SAME_DAY_SHIPPING** : Livraison le même jour.<br>• **OVERNIGHT_SHIPPING** : Livraison de nuit.<br>• **TWO_DAYS_OR_MORE_SHIPPING** : Livraison 2 jours ou plus. |
| **vads_ship_to_zip**<br>Code postal - Adresse de livraison. | Format : ans..64 |

# 5. UTILISATION DU FORMULAIRE EMBARQUÉ

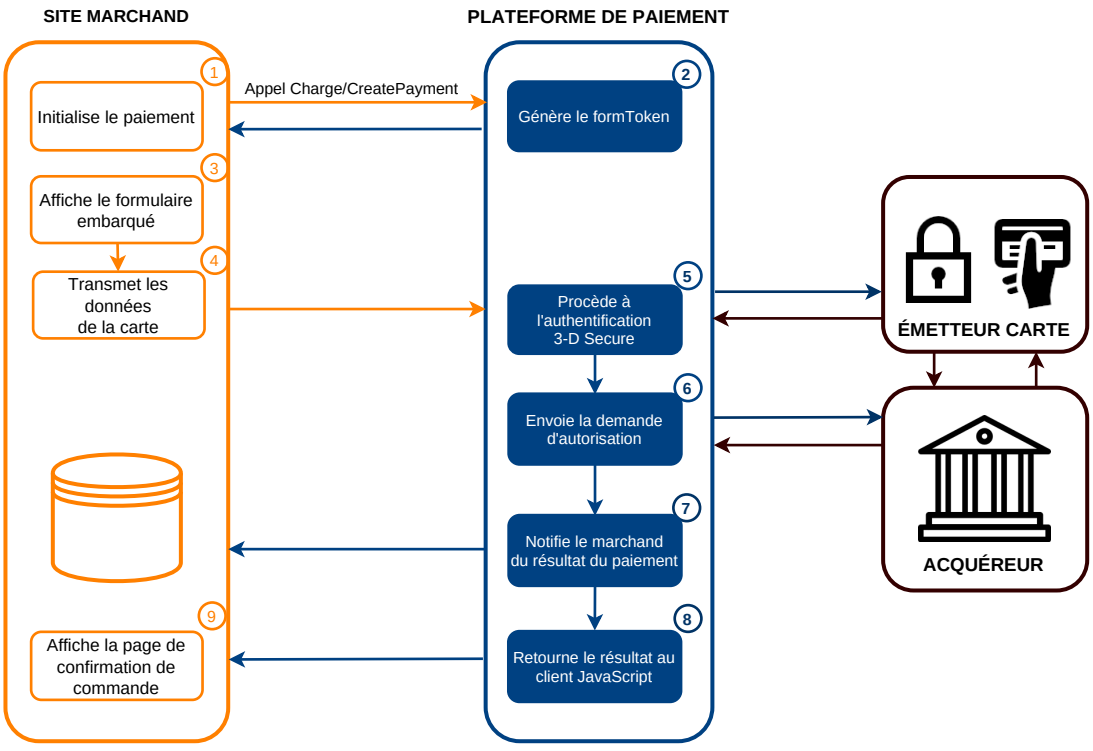


### Cas d'usage concernés

Ce chapitre s'applique pour les cas d'utilisation suivants :

- Paiement comptant avec saisie des données de la carte,
- Paiement par alias,
- Proposition d'enregistrement de la carte pendant le paiement,
- Enregistrement de la carte pendant le paiement,
- Enregistrement d'une carte dans un wallet acheteur (avec ou sans paiement).

### Cinématique



**Initialisation de la session de paiement**

Ce cas d'utilisation nécessite la création d'un formToken via un appel au Web Service **Charge/CreatePayment**.

**POST** **https://api.lyra.com/api-payment/V4/Charge/CreatePayment**

Aucun champ spécifique n'est nécessaire pour bénéficier de la protection 3-D Secure.

Utilisez les champs ci-dessous pour construire la requête :

| NOM | DESCRIPTION | REQUIS |
|---|---|---|
| **amount** | Montant pour lequel l'authentification est demandée. | Oui |
| **currency** | Code alphanumérique de la devise. | Oui |
| **orderId** | Référence de la commande.<br>**Ce champ est recommandé**. | Non |
| **formAction** | Type de comportement souhaité lors de la création de la transaction. | Non |
| **customer** | Objet contenant les données de l'acheteur. | Non |

Pour obtenir une description plus complète des champs à utiliser, testez le Web Service **Charge/CreatePayment** depuis notre playground.

En fonction du cas d'usage (c'est à dire de la valeur du champ formAction), une authentification forte peut être obligatoire. Dans ce cas, le champ strongAuthentication est ignoré.

| Cas d'usage | formAction | Authentification forte requise? |
|---|---|---|
| Paiement simple | PAYMENT | Le type d'authentification dépend de la décision de l'émetteur.<br>Pour les paiements en euro, le marchand peut demander une exemption à l'authentification forte si le montant est inférieur à 30€ et si la boutique possède l'option "Frictionless 3DS2".<br>Pour les paiements réalisés dans une autre devise, le marchand peut demander une authentification sans interaction du porteur si la boutique possède l'option "Frictionless 3DS2". |
| Paiement par alias | PAYMENT | Authentification forte et saisie du CVV requises. |
| Enregistrement de la carte pendant le paiement | REGISTER_PAY | Authentification forte requise. |
| Proposition d'enregistrement de la carte pendant le paiement | ASK_REGISTER_PAY | Authentification forte requise uniquement si l'acheteur accepte d'enregistrer son moyen de paiement.<br>Sinon, le comportement est identique à la valeur PAYMENT. |
| Paiement par wallet acheteur | CUSTOMERWALLET | Authentification forte requise uniquement si l'acheteur accepte d'enregistrer son moyen de paiement ou s'il utilise une carte déjà enregistrée.<br>Dans tous les autres cas, le comportement est identique à la valeur PAYMENT. |

Il est possible de transmettre des champs spécifiques pour :

- demander une exemption à l'authentification forte,
- favoriser une authentification sans interaction du porteur,
- débrayer l'authentification 3D Secure 1.

**Analyse de la réponse**

A la fin de l'opération, la plateforme retourne un objet `Payment` à l'URL de notification du site marchand et au client JavaScript.

Voici la liste des attributs décrivant, par cas d'usage, le résultat de l'authentification du porteur :

| Cas d'usage | Champs retournés |
|---|---|
| Transaction avec authentification forte réussie | • `authenticationResponse.value.status` = `SUCCESS` : Authentification réussie.<br>• `authenticationResponse.value.authenticationType` = `CHALLENGE` (Valeur retournée en 3DS1 et 3DS2).<br>• `authenticationResponse.value.commerceIndicator` = `5` (Visa ou AMEX) ou `02` (Mastercard).<br>• `authenticationResponse.value.extension.authenticationType` = `THREEDS_V1` ou `THREEDS_V2`.<br>• `transactionDetails.liabilityShift` = `YES` : Le paiement est garanti.<br>• `transactions.effectiveStrongAuthentication` = `ENABLED` : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification frictionless réussie, le marchand dispose de l'option "Frictionless 3DS2" et a demandé une authentification sans interaction du porteur | • `authenticationResponse.value.status` = `SUCCESS` : Authentification réussie.<br>• `authenticationResponse.value.authenticationType` = `FRICTIONLESS`.<br>• `authenticationResponse.value.commerceIndicator` = `5` (Visa ou AMEX) ou **02** (Mastercard).<br>• `authenticationResponse.value.extension.authenticationType` = `THREEDS_V2`.<br>• `transactionDetails.liabilityShift` = `NO` : Le paiement n'est pas garanti.<br>• `transactions.effectiveStrongAuthentication` = `ENABLED` : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification frictionless réussie, le marchand n'a pas demandé une authentification sans interaction du porteur | • `authenticationResponse.value.status` = `SUCCESS` : Authentification réussie.<br>• `authenticationResponse.value.authenticationType` = `FRICTIONLESS`.<br>• `authenticationResponse.value.commerceIndicator` = `5` (Visa ou AMEX) ou **02** (Mastercard).<br>• `authenticationResponse.value.extension.authenticationType` = `THREEDS_V2`.<br>• `transactionDetails.liabilityShift` = `YES` : Le paiement est garanti.<br>• `transactions.effectiveStrongAuthentication` = `ENABLED` : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification 3-D Secure en échec | • `authenticationResponse.value.status` = `FAILED` : Erreur d'authentification.<br>• `authenticationResponse.value.authenticationType` = `CHALLENGE`.<br>• `authenticationResponse.value.commerceIndicator` = null |

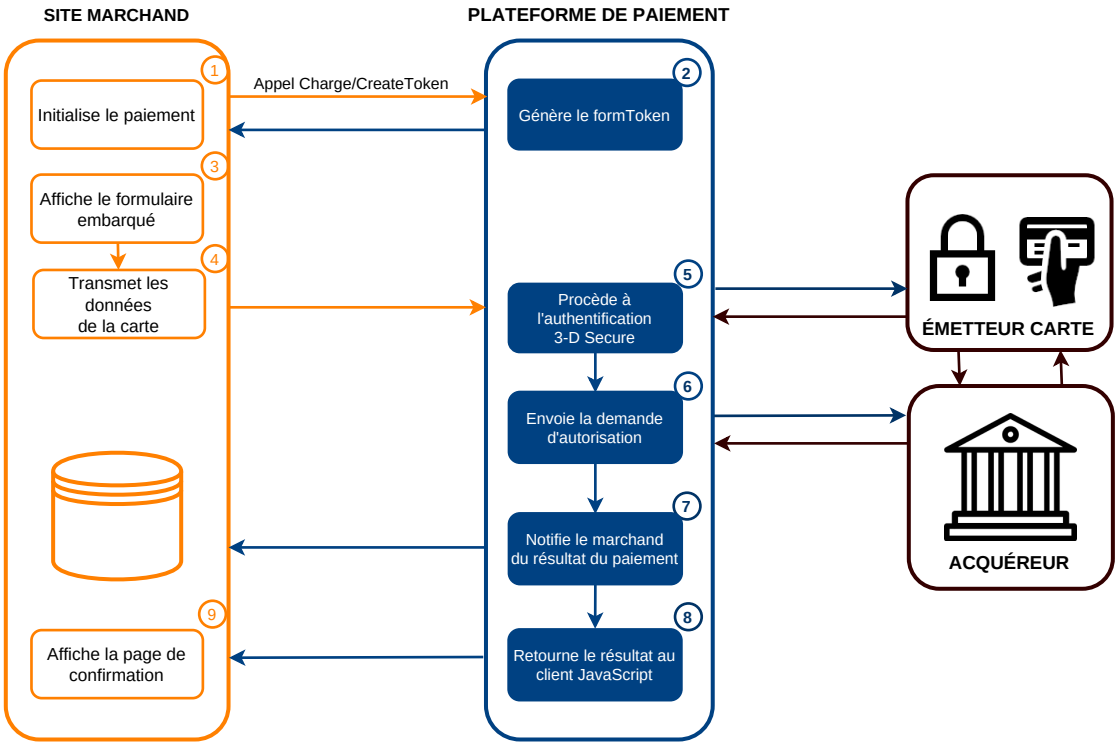
| Cas d'usage | Champs retournés |
| --- | --- |
| | • authenticationResponse.value.extension.authenticationType = THREEDS_V1 ou THREEDS_V2.<br>• authenticationResponse.value.reason.code = CARD_AUTHENTICATION_FAILED : Refus de l'authentification par l'émetteur.<br>• transactionDetails.liabilityShift = null : Le paiement n'est pas garanti.<br>• transactions.effectiveStrongAuthentication = DISABLED : l'authentification du porteur est en échec. |
| Carte non enrôlée | • authenticationResponse.value.status = NOT_ENROLLED : Porteur non enrôlé.<br>• authenticationResponse.value.authenticationType = null<br>• authenticationResponse.value.commerceIndicator = null<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V1.<br>• transactionDetails.liabilityShift = NO : Le paiement n'est pas garanti.<br>• transactions.effectiveStrongAuthentication = DISABLED : l'authentification du porteur est en échec. |

## 5.1. Enregistrement d'une carte sans paiement



### Cinématique




### Initialisation de la session de paiement

Ce cas d'utilisation nécessite la création d'un **formToken** via un appel au Web Service **Charge/CreateToken**.

**POST** **https://api.lyra.com/api-payment/V4/Charge/CreateToken**

Aucun champ spécifique n'est nécessaire pour bénéficier de la protection 3-D Secure.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte.

Le champ **strongAuthentication** est ignoré et une demande d'authentification forte est réalisée automatiquement.

### Analyse de la réponse

A la fin de l'opération, la plateforme retourne un objet **Payment** à l'URL de notification du site marchand et au client JavaScript.

Voici la liste des attributs décrivant, par cas d'usage, le résultat de l'authentification du porteur :

| Cas d'usage | Champs retournés |
|---|---|
| Transaction avec authentification forte réussie | • `authenticationResponse.value.status` = `SUCCESS` : Authentification réussie.<br>• `authenticationResponse.value.authenticationType` = `CHALLENGE` (Valeur retournée en 3DS1 et 3DS2). |

| Cas d'usage | Champs retournés |
| --- | --- |
| | • authenticationResponse.value.commerceIndicator = 5 (Visa ou AMEX) ou 02 (Mastercard).<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V1 ou THREEDS_V2.<br>• transactionDetails.liabilityShift = YES : Le paiement est garanti.<br>• transactions.effectiveStrongAuthentication = ENABLED : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification frictionless réussie, le marchand dispose de l'option "Frictionless 3DS2" et a demandé une authentification sans interaction du porteur | • authenticationResponse.value.status = SUCCESS : Authentification réussie.<br>• authenticationResponse.value.authenticationType = FRICTIONLESS.<br>• authenticationResponse.value.commerceIndicator = 5 (Visa ou AMEX) ou **02** (Mastercard).<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V2.<br>• transactionDetails.liabilityShift = NO : Le paiement n'est pas garanti.<br>• transactions.effectiveStrongAuthentication = ENABLED : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification frictionless réussie, le marchand n'a pas demandé une authentification sans interaction du porteur | • authenticationResponse.value.status = SUCCESS : Authentification réussie.<br>• authenticationResponse.value.authenticationType = FRICTIONLESS.<br>• authenticationResponse.value.commerceIndicator = 5 (Visa ou AMEX) ou **02** (Mastercard).<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V2.<br>• transactionDetails.liabilityShift = YES : Le paiement est garanti.<br>• transactions.effectiveStrongAuthentication = ENABLED : Le porteur s'est authentifié avec succès. |
| Transaction avec authentification 3-D Secure en échec | • authenticationResponse.value.status = FAILED : Erreur d'authentification.<br>• authenticationResponse.value.authenticationType = CHALLENGE.<br>• authenticationResponse.value.commerceIndicator = null<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V1 ou THREEDS_V2.<br>• authenticationResponse.value.reason.code = CARD_AUTHENTICATION_FAILED : Refus de l'authentification par l'émetteur.<br>• transactionDetails.liabilityShift = null : Le paiement n'est pas garanti.<br>• transactions.effectiveStrongAuthentication = DISABLED : l'authentification du porteur est en échec. |
| Carte non enrôlée | • authenticationResponse.value.status = NOT_ENROLLED : Porteur non enrôlé.<br>• authenticationResponse.value.authenticationType = null<br>• authenticationResponse.value.commerceIndicator = null<br>• authenticationResponse.value.extension.authenticationType = THREEDS_V1. |

| Cas d'usage | Champs retournés |
|---|---|
| | • transactionDetails.liabilityShift = NO : Le paiement n'est pas garanti.<br>• transactions.effectiveStrongAuthentication = DISABLED : l'authentification du porteur est en échec. |

## 5.2. Préférence 3-D Secure

Le marchand peut exprimer son choix concernant l'authentification forte de l'acheteur en utilisant le champ **strongAuthentication**.

La valeur transmise dans la requête de paiement est prioritaire aux règles de risque éventuellement définies par le marchand dans son Back Office Expert.

Voici comment l'utiliser :

| Cas d'utilisation | Valeurs | Description |
|---|---|---|
| **CHALLENGE** : Avec interaction du porteur | **ENABLED** | **Déprécié** . |
| | **CHALLENGE_REQUESTED** | **3DS Requestor Preference**. Permet de demander une authentification forte pour la transaction. |
| | **CHALLENGE_MANDATE** | **Challenge request mandate**. Permet d'indiquer que pour des raisons réglementaires, une authentification forte est requise pour la transaction. |
| **FRICTIONLESS** : Sans interaction du porteur. | **DISABLED**<br>Option "Frictionless 3DS2" obligatoire | Permet de demander **une exemption** à l'authentification forte :<br>• Transactions à faible montant<br>• Transactional Risk Analysis (TRA Acquéreur)<br>• Safe'R by CB<br>Plus d'infos : Tableau des exemptions. |
| Pas de préférence 3-D Secure | **AUTO** | Le choix de la préférence est délégué à l'émetteur de la carte. Si l'émetteur décide de réaliser une authentification sans interaction (frictionless), le paiement sera garanti. |
| | **NO_PREFERENCE** | |

**Tableau des exemptions** (valeur 2)

| Exemptions | Description |
|---|---|
| **Transactions à faible montant** | En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 €, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 €.<br>Si le montant est supérieur à 30 €, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).<br>Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.<br>Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.<br>Si la boutique ne dispose pas de l'option "Frictionless 3DS2", le choix de la préférence est délégué à l'émetteur de la carte ( No Preference). |

| Exemptions | Description |
| --- | --- |
| **Transactional Risk Analysis (TRA Acquéreur)** | Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte si le montant est inférieur au seuil fixé par votre établissement financier.<br>**Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte**.<br>L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier. |
| **Safe'R by CB** | CB propose le programme Safe'R by CB. Ce programme a pour objectif de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Vous pouvez demander **une exemption** à l'authentification forte :<br>• Si le montant est inférieur à 100 €, l'exemption est systématique pour les marchands éligibles.<br>• Si le montant est compris entre 100 € et 250 €, une expérimentation est en cours. Pour en bénéficier, le marchand doit :<br>  • Avoir un contrat CB.<br>  • Etre éligible à la TRA acquéreur.<br>  • Transmettre les valeurs requises dans le flux 3-D Secure, selon les règles définies par la plateforme.<br>**Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte**. |

## 5.3. Champs permettant d'améliorer les chances de frictionless

Afin de permettre à l'émetteur de la carte de déterminer le risque d'une transaction, il est recommandé de transmettre un maximum d'informations lors du paiement.

Plus les émetteurs disposent d'informations sur les habitudes des porteurs de carte, plus ils sont à même de proposer une authentification sans interaction (frictionless).

Voir la liste ci-dessous :

| Nom / Description | Format / Valeurs |
|---|---|
| **customer.email**<br>Adresse e-mail de l'acheteur | Format : String \| Longueur maximale : 150<br>Exemple : sample@example.com |
| **customer.billingDetails.identityCode**<br>Identifiant national. Permet d'identifier de façon unique chaque citoyen au sein d'un pays. | Format : String \| Longueur maximale : 150 |
| **customer.billingDetails.streetNumber**<br>Numéro de rue de l'adresse de facturation | Format : String \| Longueur maximale : 5 |
| **customer.billingDetails.address**<br>Adresse postale | Format : String \| Longueur maximale : 255 |
| **customer.billingDetails.address2**<br>Deuxième ligne d'adresse | Format : String \| Longueur maximale : 255 |
| **customer.billingDetails.zipCode**<br>Code postal | Format : String \| Longueur maximale : 64 |
| **customer.billingDetails.city**<br>Ville | Format : String \| Longueur maximale : 128 |
| **customer.billingDetails.state**<br>Etat / Région | Format : String \| Longueur maximale : 127 |
| **customer.billingDetails.country**<br>Code pays suivant la norme ISO 3166 alpha-2 | Format : String \| Longueur maximale : 2<br>Exemple : ES |
| **customer.billingDetails.phoneNumber**<br>Numéro de téléphone. | Format : String \| Longueur maximale : 32 |
| **customer.billingDetails.cellPhoneNumber**<br>Numéro de téléphone mobile | Format : String \| Longueur maximale : 32 |
| **customer.shippingDetails.address**<br>Adresse postale | Format : String \| Longueur maximale : 255 |
| **customer.shippingDetails.address2**<br>Deuxième ligne d'adresse | Format : String \| Longueur maximale : 255 |
| **customer.shippingDetails.zipCode**<br>Code postal | Format : String \| Longueur maximale : 64 |
| **customer.shippingDetails.city**<br>Ville | Format : String \| Longueur maximale : 128 |
| **customer.shippingDetails.state**<br>Etat / Région | Format : String \| Longueur maximale : 127 |

| Nom / Description | Format / Valeurs |
| --- | --- |
| **customer.shippingDetails.country**<br>Code pays suivant la norme ISO 3166 alpha-2 | Format : String \| Longueur maximale : 255<br>Exemple : FR |
| **customer.shippingDetails.shippingMethod**<br>Mode de livraison. | Format : String \| Longueur maximale : 24<br>Exemple : RECLAIM_IN_SHOP |
| **customer.shippingDetails.shippingSpeed**<br>Délai de livraison. | Format : String \| Longueur maximale : 8<br>Exemple : EXPRESS |

# 6. UTILISATION DES WEB SERVICES REST

Les Web Services REST permettent de gérer la préférence 3-D Secure :

- dans les requêtes de création d'ordres de paiement (voir : Web Services Ordre de paiement)
- dans les requêtes de création de paiement pour les marchands certifiées PCI-DSS (voir : Authentification intégrée au paiement).

La préférence 3-D Secure est transmise par le marchand via le champ `strongAuthentication`.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte, quelle que soit la préférence 3-D Secure.

Le champ `strongAuthentication` est donc ignoré dans les requêtes de création d'alias (`Charge/CreateToken` et `PCI/Charge/CreateToken`).

# 7. QUESTIONS FRÉQUENTES

## 7.1. Comment augmenter le taux de frictionless en 3-D Secure ?

Afin de permettre à l'émetteur de la carte de déterminer le risque d'une transaction, il est recommandé de transmettre un maximum d'informations lors du paiement.

Plus les émetteurs disposent d'informations sur les habitudes des porteurs de carte, plus ils sont à même de proposer une authentification sans interaction (frictionless).

L'utilisation de ces champs est optionnelle. Dans tous les cas, c'est la banque émettrice qui décide si une authentification forte doit être réalisée.

Consultez la liste des champs correspondante à votre implémentation :

- Mode redirection
- Mode embarqué

## 7.2. Est-ce que l'authentification 3-D Secure est systématique dans le parcours client ?

Dans le cadre des obligations réglementaires de la Directive des Services de Paiement n°2 (DSP2), l'authentification forte doit être généralisée sur l'ensemble des sites e-commerce qui réalisent des encaissements en ligne (internet ou application mobile) par carte bancaire.

Cependant, certains paiements pourront être exemptés, et ainsi être réalisés sans authentification forte du porteur (mode frictionless), s'ils sont éligibles aux exemptions définies par la DSP2 (exemples : faible montant, analyse de risques émetteurs (TRA émetteurs), analyse de risque acquéreurs (TRA acquéreurs), bénéficiaire de confiance, ...). Voir Les exemptions à l'authentification forte à la page 9 pour plus d'informations.

La mise en œuvre opérationnelle de ces cas d'exemption se fait progressivement selon le calendrier établi entre l'Observatoire de la sécurité des moyens de paiement (OSMP) de la Banque de France et les parties prenantes.

L'établissement émetteur de la carte, dans le cas de paiement en ligne, pourra refuser l'absence d'authentification 3-D Secure.

Il demandera une authentification du porteur s'il détecte, par exemple, une situation non habituelle (paiement depuis un autre équipement, paiement depuis un pays étranger, etc.).

## 7.3. Bénéficier des exemptions à authentification forte pour mes clients

Si votre boutique dispose de l'option "Frictionless 3DS2" , vous avez la possibilité[1] de demander une exemption au principe d'authentification forte. Cela concerne les transactions d'un montant inférieur à 30 €, et dans la limite soit de cinq (5) opérations successives ou d'un montant cumulé inférieur à 100 €.

Les cas d'exemptions supportés sont :

- **Transactions à faible montant**

  En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 EUR, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 EUR.

[1] Possibilité soumise à l'accord préalable de votre établissement financier.

Si le montant est supérieur à 30 EUR, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte ( No Preference).

Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur.

Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

- **Transactional Risk Analysis** (TRA Acquéreur)

  Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte si le montant est inférieur au seuil fixé par votre établissement financier.

  Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

  L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier.

- **Safe'R by CB**

  Le programme Safe'R by CB est une exemption qui permet aux marchands détenteurs de contrats CB à faire du frictionless. Son objectif est de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Il permet de valoriser les investissements faits sur la lutte contre la fraude, en optimisant le taux de frictionless lorsque la réglementation le permet.

  Jusque-là, le programme Safe'R by CB couvre jusqu'à 100 EUR pour une exemption systématique des bénéficiaires éligibles. Le GIE CB a démarré une expérimentation de la tranche 100 EUR à 250 EUR.

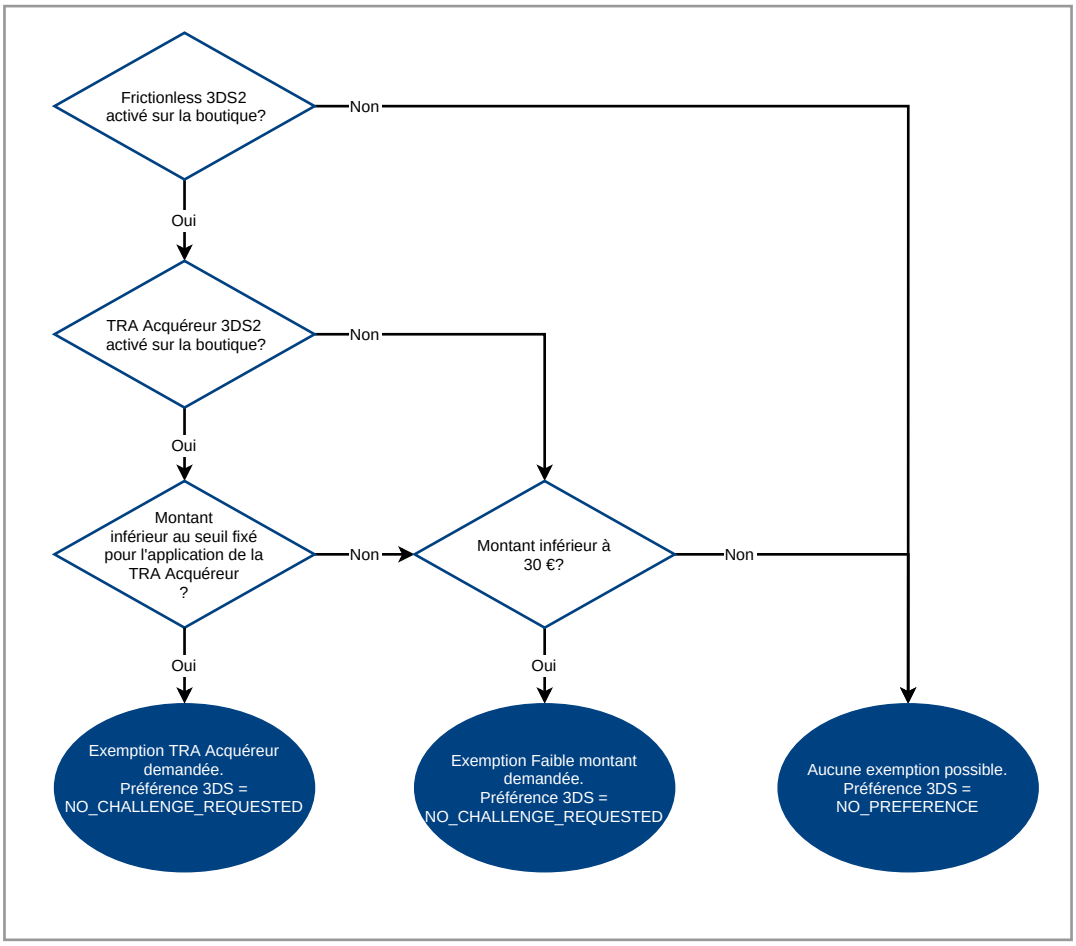
  Le programme Safe'R by CB s'applique sans date de fin pour les paiements compris entre 0-100 EUR.

  Le bénéfice du programme sur la tranche 100-250 EUR est en phase d'expérimentation jusqu'au 30 septembre 2024 selon CB.

En pratique, vous paramétrez cette règle d'exemption au niveau de votre formulaire de paiement (champ "**vads_threeds_mpi**" ou "**strongAthentication**" selon l'API utilisée).

La plateforme détermine automatiquement le motif d'exemption à transmettre à l'émetteur, selon la règle de priorité suivante :




En définitive, c'est la banque de votre client (la "banque émettrice") qui décide d'accorder une exemption d'authentification à son client.

> Si la banque émettrice accorde une exemption d'authentification que vous avez demandée, vous ne bénéficiez pas du transfert de responsabilité à l'émetteur. La banque émettrice sera en droit d'émettre un impayé en cas de contestation de la transaction par le porteur de la carte.

*email courriel*

## 7.4. Avantages et opportunités du 3-D Secure

Les réseaux CB, Visa et Mastercard ont mis en place le programme 3-D Secure v2 pour fluidifier davantage le parcours client et renforcer la sécurité des transactions.

Les apports majeurs de 3-D Secure v2 sont :

- un parcours client plus fluide et plus intégré, notamment pour les applications mobiles ;
- de nouvelles méthodes d'authentification pour les porteurs de carte ;
- la gestion des exemptions et du *frictionless* (petits montants, bénéficiaire de confiance, suivi du taux de fraude, etc.).

Son déploiement a nécessité des évolutions sur toute la chaîne monétique (sites internet, prestataires d'Acceptation Technique, réseaux de transport de données, Banque Commerçant, Banque Porteur).

**L'authentification en mode *Pop In*.**

Le principe de redirection vers une page d'authentification non-responsive, qui était source d'abandon du paiement, a été revu. L'authentification est désormais faite en mode "*Pop In*" (fenêtre qui s'ouvre sur le navigateur de l'acheteur).

Il est possible d'indiquer au serveur d'authentification la taille de l'écran de l'acheteur. La fenêtre *Pop in* s'adapte alors à la taille de la page du navigateur, améliorant ainsi l'expérience utilisateur notamment sur les équipements mobiles (si le serveur d'authentification de l'émetteur sait exploiter les paramètres de taille d'écran).

***Frictionless* : une authentification sans interaction systématique de l'acheteur**

Le protocole 3-D Secure v2 permet d'échanger de nouvelles données entre le marchand et l'émetteur (la banque du porteur de la carte).

Ainsi, l'analyse de ces données enrichies permettra à l'émetteur de décider :

- soit de déclencher une authentification forte du porteur, c'est-à-dire demander à l'acheteur de saisir des données complémentaires ;

  Les méthodes d'authentification forte sont du ressort de l'émetteur de la carte et évoluent vers des solutions de type "**biométrie**" et/ou connexion à sa "**banque en ligne**" pour éliminer à terme les codes à usage unique envoyés par SMS (non reconnus pour leur fiabilité maximale).

- soit de finaliser le processus de paiement sans interaction de l'acheteur. Ce mécanisme est appelé "*frictionless*".

Les objectifs sont de transformer un maximum de paiements sans authentification du porteur afin de fluidifier le parcours client, de réduire la fraude et par conséquent vos taux d'impayés.

L'objectif des réseaux carte est d'obtenir à terme 85 % des paiements sans authentification du porteur tout en maintenant le transfert de responsabilité.

## 7.5. Pourquoi mes clients sont obligés de s'authentifier même en frictionless ?

Pour bénéficier d'une authentification passive (frictionless), le paiement doit être éligible à une exemption.

Si le montant de la transaction est supérieur à 30 EUR, elle n'est pas éligible à l'exemption "Transaction à faible montant".

Par conséquent, sans l'option "Frictionless 3DS2" ou si le montant est supérieur à 30 EUR, le choix de la préférence est délégué à l'émetteur de la carte.

Si vous disposez de l'option "Frictionless 3DS2" et que la transaction est éligible à l'exemption "Transaction à faible montant", l'émetteur peut décider qu'une authentification forte est nécessaire, même si vous avez demandé une authentification frictionless.

## 7.6. Comment puis-je bloquer une transaction non garantie ?

Une transaction non garantie est une transaction pour laquelle le porteur de carte ne peut pas transférer la responsabilité d'un impayé pour le motif "contestation du porteur" vers le marchand.

L'enrôlement du contrat à 3-D Secure permet de protéger le marchand contre ce motif d'impayés "contestation du porteur".

Cependant, certains types de transactions ne bénéficient pas de cette garantie (voir le diagramme décisionnel pour mieux les identifier).

Grâce à l'option **Gestion des risques avancée**, vous pouvez bloquer ce type de transactions. Pour cela :

1. Connectez-vous à votre Back Office : https://secure.lyra.com/portal/.
2. Cliquez sur **Autres actions** et connectez-vous à votre Back Office expert.
3. Sélectionnez le menu **Paramétrage** > **Gestion des risques** > [libellé de votre boutique].

   Si vous ne voyez pas le menu **Gestion des risques**, c'est que votre compte utilisateur n'est pas habilité à faire ce paramétrage ou alors vous ne bénéficiez pas du module. Rapprochez-vous d'une personne ayant un compte utilisateur habilité ou contactez l'administration des ventes.
4. Cliquez sur **Créer une nouvelle règle**.
5. Utilisez le moteur de recherche pour trouver le contrôle "Transfert de responsabilité".

6. Sélectionnez le contrôle puis cliquez sur **Suivant**.
7. Saisissez le **montant minimum** qui déclenchera la règle sur la transaction. Sélectionnez la devise si nécessaire.
8. Sélectionnez **Refuser** dans la liste des actions.

   Toutes les transactions concernées par ce paramétrage seront refusées.

   Vous avez la possibilité de **Recevoir une alerte**. L'alerte vous permet par exemple, de mettre en attente le processus de livraison le temps que des vérifications puissent être réalisées sur la transaction.

   Il est également possible de choisir **Valider manuellement**. Cette action vous permet de bloquer temporairement la remise du paiement le temps de vérifier la transaction et décider si vous souhaitez la valider ou l'annuler.

   Si vous ajoutez plusieurs actions, sachez que l'action **Refuser** est prioritaire sur l'action **Valider manuellement**. Cette dernière, elle, peut se cumuler avec l'action **Recevoir une alerte**

## 7.7. C’est quoi le Soft Decline ?

Avec l'application de la DSP2, les émetteurs peuvent refuser la transaction si l'authentification 3-D Secure n'a pas été réalisée. Ce comportement s'appelle "Soft Decline".

Le "Soft Decline" s'applique également aux transactions en frictionless selon les souhaits de l'émetteur (par exemple. l'émetteur ou l'acquéreur peut refuser à l'étape d'autorisation s'il ne souhaite pas de frictionless sur la transaction).

Pour réduire le nombre de paiements refusés, lorsque l'émetteur refuse une transaction en "Soft Decline", la plateforme de paiement réalise automatiquement une nouvelle tentative de paiement mais cette fois en "challenge mandate". L'acheteur n’a pas à saisir ses données de carte une nouvelle fois. Le processus est transparent pour l'acheteur.

**Quels sont les réseaux concernés ?**

Tous les acquéreurs qui font de l'acquisition en euro dans la zone d'application de la DSP2 sont concernés.

La plateforme de paiement gère le "Soft Decline" sur les réseaux suivants :

- CB
- AMEXGLOBAL (American Express)
- GATECONEX (Elavon Europe)
- GICC (acquéreurs Concardis, Six payments, VR Pay)

Les codes retour autorisation correspondants :

| Réseau | Code retour autorisation |
|---|---|
| CB | 81 |
| AMEXGLOBAL | 130 |
| GATECONEX | 110 |
| GICC | 65 |