Gestion des transactions

Manuel d'utilisation du Back Office

Version du document 2.11

Sommaire

1. HISTORIQUE DU DOCUMENT.....4

2. SE CONNECTER AU BACK OFFICE MARCHAND.....5

3. AFFICHER LE TABLEAU DE BORD.....6

4. VISUALISER LES TRANSACTIONS.....8

5. PERSONNALISER L'AFFICHAGE DE LA TABLE DES TRANSACTIONS.....9

6. RECHERCHER UNE TRANSACTION EN COURS.....11

7. RECHERCHER UNE TRANSACTION REMISÉE.....13

8. CONSULTER LE DÉTAIL D'UNE TRANSACTION.....15
- 8.1. Consulter les caractéristiques du paiement.....17
- 8.2. Consulter le détail d'un paiement en N fois.....18
- 8.3. Consulter le résultat de l'authentification 3D Secure.....19
  - 8.3.1. Transaction avec authentification forte réussie.....19
  - 8.3.2. Transaction avec authentification frictionless réussie.....20
  - 8.3.3. Transaction avec authentification 3D Secure en échec.....23
  - 8.3.4. Transaction avec erreur technique durant l'authentification.....24
  - 8.3.5. Session de paiement expirée.....25
- 8.4. Consulter le résultat de l'authentification American Express SafeKey.....26
- 8.5. Consulter les informations sur l'acheteur.....27
- 8.6. Consulter les informations du sous-marchand.....28
- 8.7. Consulter les informations de livraison.....29
- 8.8. Consulter le détail du panier.....30
- 8.9. Consulter les informations Extras.....31
- 8.10. Consulter les contrôles effectués sur la transaction.....32
- 8.11. Consulter l'historique de la transaction.....33

9. RÉALISER UNE OPÉRATION SUR VOS TRANSACTIONS.....34
- 9.1. Valider une transaction.....34
- 9.2. Annuler une ou plusieurs transactions.....35
- 9.3. Modifier une transaction.....36
- 9.4. Dupliquer une transaction.....37
- 9.5. Rembourser une transaction.....38
- 9.6. Rapprocher manuellement.....39
- 9.7. Editer la référence d'une commande.....39
- 9.8. Créer un alias depuis une transaction.....40
- 9.9. Télécharger le ticket de paiement.....42
- 9.10. Envoyer un ordre de paiement à partir d'une transaction refusée.....43

10. RENVOYER MANUELLEMENT UNE NOTIFICATION.....44
- 10.1. Renvoyer une notification de fin de paiement (IPN).....44
- 10.2. Renvoyer l'e-mail de confirmation de paiement au marchand.....45
- 10.3. Renvoyer l'e-mail de confirmation de paiement à l'acheteur.....45

11. DURÉE DE RÉTENTION DES TRANSACTIONS.....46

12. CYCLE DE VIE DES TRANSACTIONS.....47
- 12.1. Paiement comptant immédiat.....47
  - 12.1.1. Validation automatique.....47
  - 12.1.2. Validation manuelle.....48

12.2. Paiement comptant différé....50
12.2.1. Validation automatique....50
12.2.2. Validation manuelle....51
12.3. Paiement en plusieurs fois.... 52
12.3.1. Validation automatique....52
12.3.2. Validation manuelle....53
12.4. Le service "Autorisations anticipées".... 54
12.5. Durée de validité d'une demande d'autorisation.... 55

13. OBTENIR DE L'AIDE.... 56

1. HISTORIQUE DU DOCUMENT

Version	Auteur	Date	Commentaire
2.11	OSB (Océanienne de Service Bancaire)	07/02/2024	• Mise à jour du chapitre *Rembourser une transaction* • Mise à jour du chapitre *Rechercher une transaction en cours* • Mise à jour du chapitre *Rechercher une transaction remisée* • Mise à jour du chapitre *Consulter les informations sur l'acheteur* • Mise à jour de la structure du document
2.10	OSB (Océanienne de Service Bancaire)	30/03/2023	• Mise à jour des chapitres dans *Cycle de vie des transactions* • Mise à jour du chapitre *Transaction avec authentification 3D Secure en échec*
2.9	OSB (Océanienne de Service Bancaire)	23/01/2023	• Modification du chapitre *Rembourser une transaction*.

2. SE CONNECTER AU BACK OFFICE MARCHAND

Votre Back Office est accessible sur :

https://secure.osb.pf/vads-merchant/

1. Saisissez votre nom d'utilisateur.

   Vos identifiants de connexion (nom d'utilisateur et mot de passe) vous ont été communiqués dans un e-mail ayant pour objet **Identifiants de connexion - [nom de votre boutique]**.

2. Saisissez votre mot de passe.

   Vos identifiants de connexion (nom d'utilisateur et mot de passe) vous ont été communiqués dans un e-mail ayant pour objet **Identifiants de connexion - [nom de votre boutique]**.

3. Cliquez sur **Valider**.

   Le compte de l'utilisateur est bloqué au bout de 3 saisies erronées du mot de passe. Si votre compte est bloqué, cliquez sur **Mot de passe oublié ou compte bloqué** pour le réinitialiser.

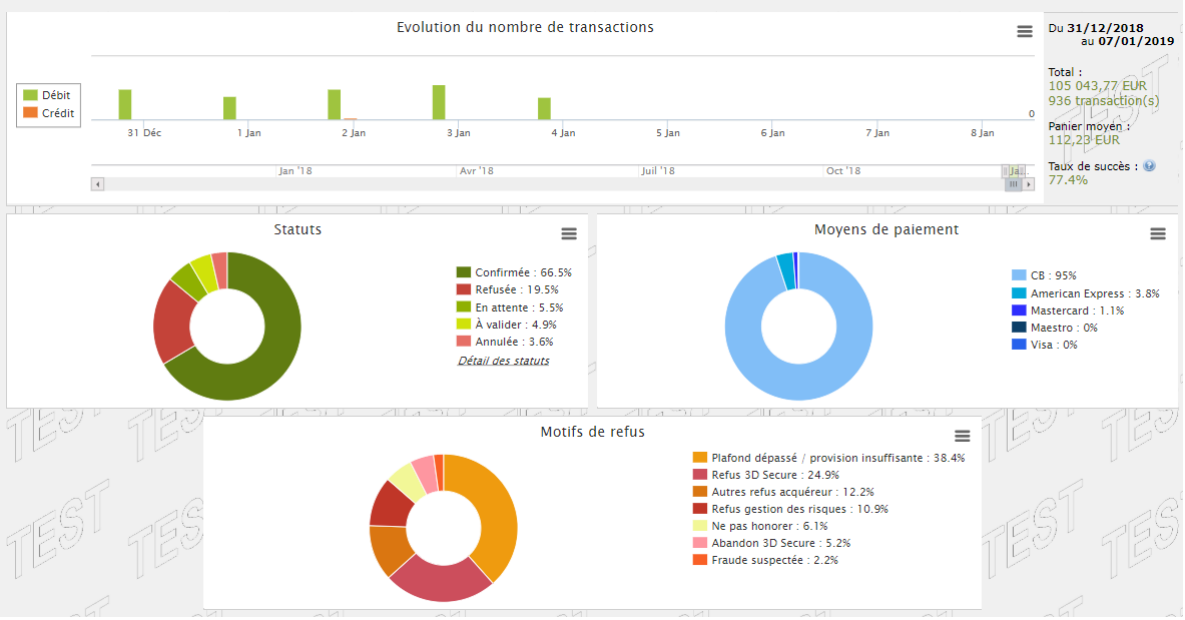
> Le mot de passe d'un utilisateur a une durée de validité de 90 jours. Au-delà de cette durée, l'utilisateur doit le modifier en se connectant à son compte.

3. AFFICHER LE TABLEAU DE BORD

L'accès au **Tableau de bord** nécessite un paramétrage. Si votre Back Office Marchand n'affiche pas le menu **Tableau de bord**, veuillez contacter votre conseiller clientèle.

Pour afficher le tableau de bord, cliquez sur le menu **Gestion** > **Tableau de bord**

La page des graphes s'affiche.



Les boutiques choisies dans cet exemple de tableau de bord sont en **mono devise** mais ces graphes fonctionnent également en **multi devises**.

4 types de données sont analysés :

- **L'évolution du nombre de transactions et/ou du chiffre d'affaires.**

  Les graphes sont en forme d'histogramme. Les données sont analysées et comparées sur une période donnée.

  L'utilisateur peut, à tout moment, passer le curseur sur une période pour afficher en infobulle les montants et/ou le nombre de transactions analysés dans cette période.

- **Les différents statuts des paiements effectués.**

  Les graphes sont en forme d'anneau. Les données sont analysées et comparées en temps réel sur la période choisie.

  L'utilisateur peut, à tout moment, passer le curseur sur un statut de paiement pour afficher en infobulle les montants et le nombre de transactions concernés.

  Les différents statuts analysés sont :

  - Annulée
  - A valider
  - Confirmée
  - Échec
  - En attente
  - Refusée

- **Les différents moyens de paiement utilisés lors des transactions.**

Les graphes sont en forme d'anneau. Les données sont analysées et comparées en temps réel sur la période choisie.

L'utilisateur peut, à tout moment, passer le curseur sur un moyen de paiement pour afficher en infobulle le montant et le nombre de transactions effectués avec ce moyen de paiement.

- **Les différents motifs de refus.**

  Les graphes sont en forme d'anneau. Les données sont analysées et comparées en temps réel sur la période choisie.

  L'utilisateur peut, à tout moment, passer le curseur sur un motif de refus pour afficher en infobulle les montants et le nombre de transactions concernés par ce refus.

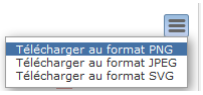
  Les différentes catégories de motifs de refus analysées sont :

  - Abandon 3D Secure
  - Autres refus acquéreur
  - Carte invalide
  - Carte perdue ou volée
  - Erreur de configuration
  - Fraude suspectée
  - Ne pas honorer
  - Plafond dépassé / provision insuffisante
  - Refus 3D Secure
  - Refus gestion des risques
  - Transaction non permise

L'utilisateur peut, à tout moment, appliquer des filtres dans un graphe en cliquant sur un ou plusieurs éléments de sa légende.

Exemple : dans cette copie d'écran, l'utilisateur souhaite ne pas analyser les transactions effectuées par **Mastercard**. Il clique sur le moyen de paiement pour le mettre à zéro (**0**) et l'exclure de l'analyse. Il lui suffit de cliquer à nouveau sur le moyen de paiement pour le réintégrer dans le graphe.

L'utilisateur a la possibilité de télécharger chaque graphe en format PNG, JPEG ou SVG.
Il suffit de cliquer sur l'icône de téléchargement et de choisir son format.



4. VISUALISER LES TRANSACTIONS

Depuis le menu **Gestion**, le marchand a accès aux transactions réelles et aux transactions de TEST.

Remarque :

Suivant ses droits d'accès, les transactions de TEST (exemple : profil développeur) et/ou les transactions réelles (exemple : profil comptable) peuvent s'afficher.

L'interface se décompose comme suit :

- **Le tableau de bord**

  Historique du chiffre d'affaire.

- **L'outil de recherche**

  - Transactions en cours

  Permet de rechercher toutes les transactions qui n'ont pas encore été capturées (par exemple, les transactions expirées, refusées, en attente d'autorisation, à valider, pré-autorisées, en attente de remise, etc...).

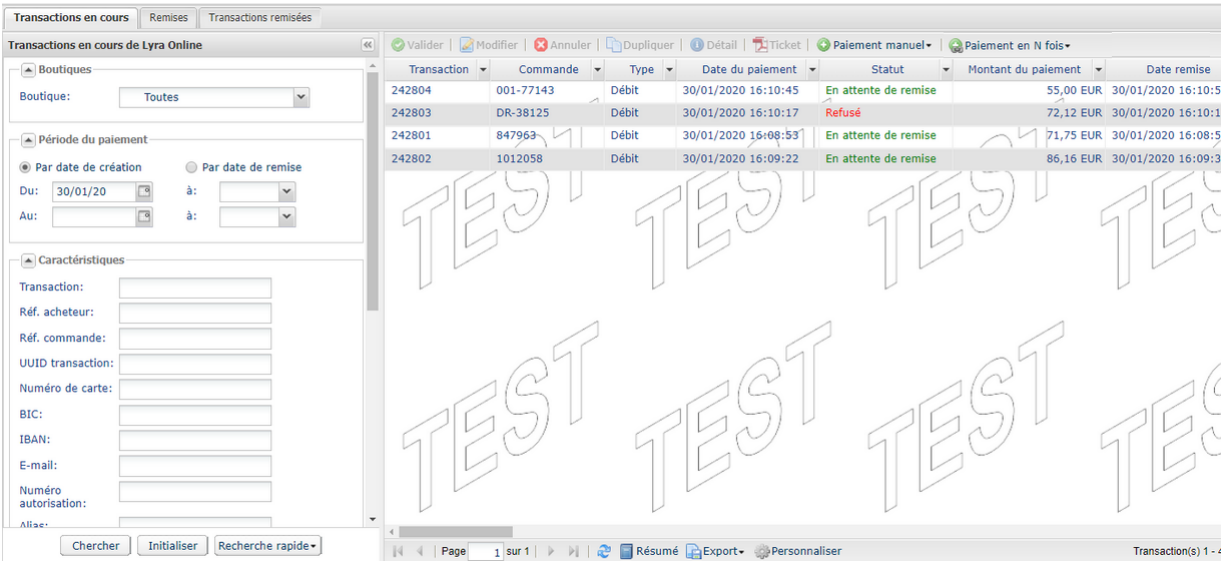
  - Remises

  Permet de rechercher toutes les remises par contrat acquéreur.

  - Transactions remisées

  Permet de rechercher toutes les transactions remisées chez l'acquéreur.

- **Le panneau de visualisation des transactions**



Par défaut l'interface affiche le contenu de l'onglet **Transactions en cours**. Il liste toutes les transactions de la journée. Les anciennes transactions sont accessibles via la recherche.

Si vous souhaitez visualiser les paiements remis en banque, cliquez sur l'onglet **Transactions remisées**.

Vous avez toujours la possibilité de faire des exports à tout moment..

5. PERSONNALISER L'AFFICHAGE DE LA TABLE DES TRANSACTIONS

Vous avez la possibilité de modifier l'affichage par défaut de la page des transactions en cours ou remisées en ajoutant, supprimant ou en modifiant l'ordre des colonnes.

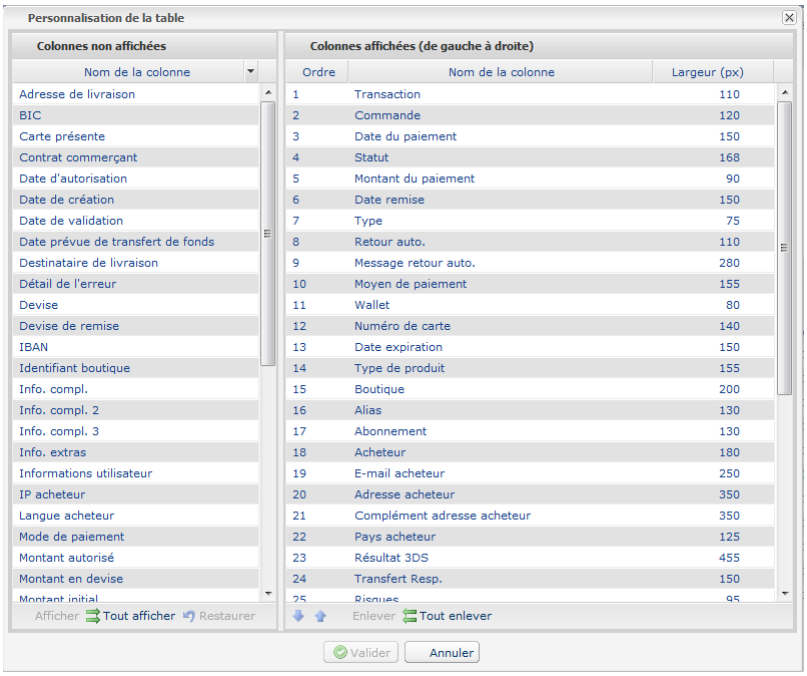
Le nouvel agencement sera utilisé pour :

- les exports de transactions
- la génération des journaux de transactions

Pour modifier l'affichage des colonnes

1. Sélectionnez l'onglet de votre choix
2. En bas de page, cliquez sur **Personnaliser**

   Le fenêtre suivante s'affiche.



Pour afficher une colonne :

1. Sélectionnez la colonne dans la zone **Colonnes non affichées**.
2. Cliquez sur le bouton **Afficher** ou faites un glisser-déposer vers **Colonnes affichées**.

Pour supprimer une colonne :

1. Sélectionnez la colonne dans la zone **Colonnes affichées**.
2. Cliquez sur le bouton **Enlever** ou faites un glisser-déposer vers **Colonnes non affichées**.

Pour déplacer une colonne :

Sélectionnez la colonne dans la zone **Colonnes affichées**.

Cliquez sur le bouton ou jusqu'à la position désirée.

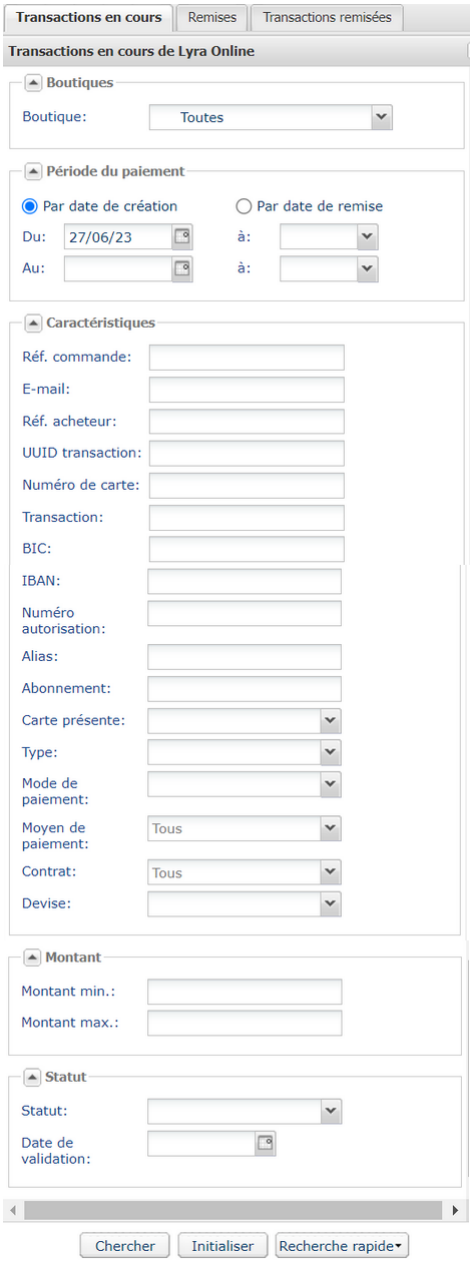
Cliquez sur **Valider** pour enregistrer vos modifications.

Le tableau suivant vous donne la signification des différentes icônes de la fenêtre **Personnalisation de la table**. Vous pouvez les utiliser pour faciliter votre personnalisation.

Icône	Description	Icône	Description
	Déplacer le champ sélectionné vers le bas		Déplacer ce champ sélectionné vers le haut
	Afficher toutes les colonnes		Enlever toutes les colonnes
	Afficher la (les) colonne(s) sélectionnée(s)		Enlever la (les) colonne(s) sélectionnée(s)
	Restaurer l'affichage par défaut avant les modifications.		

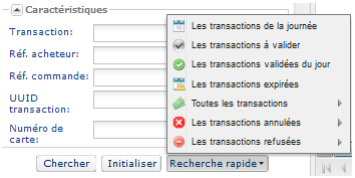
Tableau 1 : Tableau des icônes servant à personnaliser l'affichage

6. RECHERCHER UNE TRANSACTION EN COURS



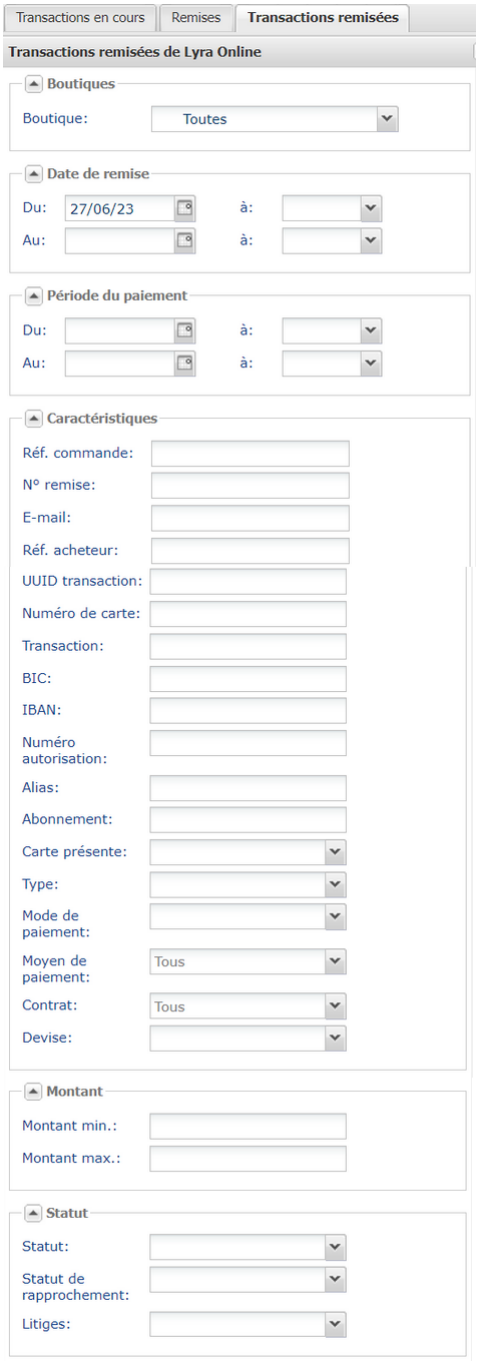
Depuis l'outil de recherche :

1. Sélectionnez l'onglet **Transactions en cours**.
2. Renseignez vos critères de recherche.
   Les critères de recherche sont multiples. Il n'y a pas de restriction sur le nombre de critères. Toutefois, plus les critères sont nombreux plus le temps de réponse devient long. Si le délai de réponse est trop long, le marchand est invité à restreindre sa plage de recherche.
   Les critères sont les suivants :
   - Boutique (par défaut toutes)
   - Plage de date / heure de création
   - Plage de date / heure de remise en banque
   - Référence de commande marchand (fourni par le marchand dans le formulaire)
   - Adresse e-mail de l'acheteur
   - Référence acheteur (code client fourni par le marchand)
   - UUID (référence unique de paiement générée par la plateforme de paiement et renvoyée au site marchand à la fin du paiement)
   - Numéro de carte de paiement, BIC ou IBAN
   - Numéro de transaction
   - Numéro d'autorisation
   - Alias (Identifiant acheteur ou RUM)
   - Référence de l'abonnement associé à l'alias
   - La présence de carte
   - Type d'opération:
     - **débit**: crédit en faveur du marchand,
     - **crédit**: crédit en faveur de l'acheteur,
     - **vérification**: opération permettant de vérifier la validité d'une carte. Ne donne jamais lieu à un débit ou à un crédit.
     - **pré-autorisation**
   - Mode de paiement
     - Paiement simple
     - Paiement en plusieurs fois
     - etc.
   - Moyen de paiement (une restriction de la recherche au moyen de paiement utilisé)
   - Contrat (permet une restriction de la recherche au contrat marchand ou au wallet)
   - Montant (permet de définir une plage de montants)
   - Statut de l'opération (permet une restriction de la recherche au statut de la transaction)
3. Cliquez sur le bouton **Chercher**.
   La plateforme de paiement met également à disposition une liste de recherches rapides :



Les résultats sont affichés dans le panneau de visualisation des transactions.

7. RECHERCHER UNE TRANSACTION REMISÉE



1. Sélectionnez l'onglet **Transactions remisées**.
2. Renseignez vos critères de recherche.
   Les critères de recherche sont multiples. Il n'y a pas de restriction sur le nombre de critères. Toutefois, plus les critères sont nombreux plus le temps de réponse devient long. Si le délai de réponse est trop long, le marchand est invité à restreindre sa plage de recherche.
   Les critères sont les suivants :
   - Boutique (par défaut toutes)
   - Plage de date / heure de remise en banque
   - Plage de date / heure de création
   - Référence de commande (fournie par le marchand)
   - Numéro de remise
   - Adresse e-mail de l'acheteur
   - Référence acheteur (code client fourni par le marchand)
   - UUID (référence unique de paiement générée par la plateforme de paiement et renvoyée au site marchand à la fin du paiement)
   - Numéro de carte de paiement, BIC ou IBAN
   - Numéro d'autorisation
   - Alias (Identifiant acheteur ou RUM)
   - Numéro de transaction
   - Référence de l'abonnement associé à l'alias
   - Type d'opération:
     - **débit**: crédit en faveur du marchand,
     - **crédit**: crédit en faveur de l'acheteur,
     - **vérification**: opération permettant de vérifier la validité d'une carte. Ne donne jamais lieu à un débit ou à un crédit.
     - **pré-autorisation**
   - Mode de paiement
     - Paiement simple
     - Paiement en plusieurs fois
     - etc.
   - Moyen de paiement (une restriction de la recherche au moyen de paiement utilisé)
   - Contrat (permet une restriction de la recherche au contrat marchand ou au wallet)
   - Devise
   - Montant (permet de définir une plage de montants)
   - Statut de l'opération
   - Statut de rapprochement
   - Litige (permet d'identifier les transactions impayées)
3. Cliquez sur le bouton **Chercher**.

Les résultats sont affichés dans le panneau de visualisation des transactions.

8. CONSULTER LE DÉTAIL D'UNE TRANSACTION

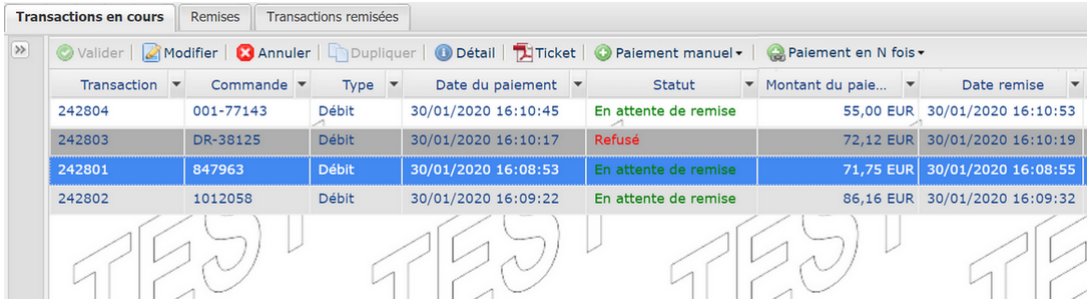


Image 1 : Liste des transactions en cours

Pour consulter le détail d'une transaction, double-cliquez sur la ligne concernée.

Image 2 : Exemple d'onglets dans le détail de la transaction

Dans le détail de la transaction, il y a autant d'onglets que d'informations transmises dans le formulaire.

La présence d'un point d'exclamation rouge à gauche du nom d'un onglet indique que la raison du refus du paiement est liée aux informations présentées dans cet onglet.

Les principaux onglets affichés:

- **Informations**

  Affiche les caractéristiques du paiement.

- **Authentification**

  Le nom de l'onglet authentification varie en fonction du type d'authentification :

  - 3D Secure
  - etc.

- **Acheteur**

  Affiche les données personnelles de l'acheteur.

- **Historique**

  Affiche l'historique des opérations intervenues sur la transaction.

Les onglets complémentaires :

- **Extra**

  Affiche les informations additionnelles que le marchand peut envoyer dans sa demande de paiement.

- **Livraison**

  Cet onglet s'affiche si et seulement si le marchand transmet les informations sur l'adresse de livraison à la plateforme de paiement (imposé par certains moyens de paiement).

- **Panier**

  Cet onglet s'affiche si et seulement si le marchand transmet le contenu du panier à la plateforme de paiement.

- **Gestion des risques**

  Cet onglet s'affiche si et seulement si le marchand a souscrit à l'option **Contrôle de risque**.

- **Tentatives multiples**

  Cet onglet s'affiche si et seulement si l'acheteur a fait plusieurs tentatives de paiement. Il donne le tableau de toutes ses tentatives.

  La ligne en gras correspondant à la transaction courante.

  Par double clic sur une ligne du tableau on bascule sur le détail de la tentative de paiement correspondante.

- **Paiement en N fois**

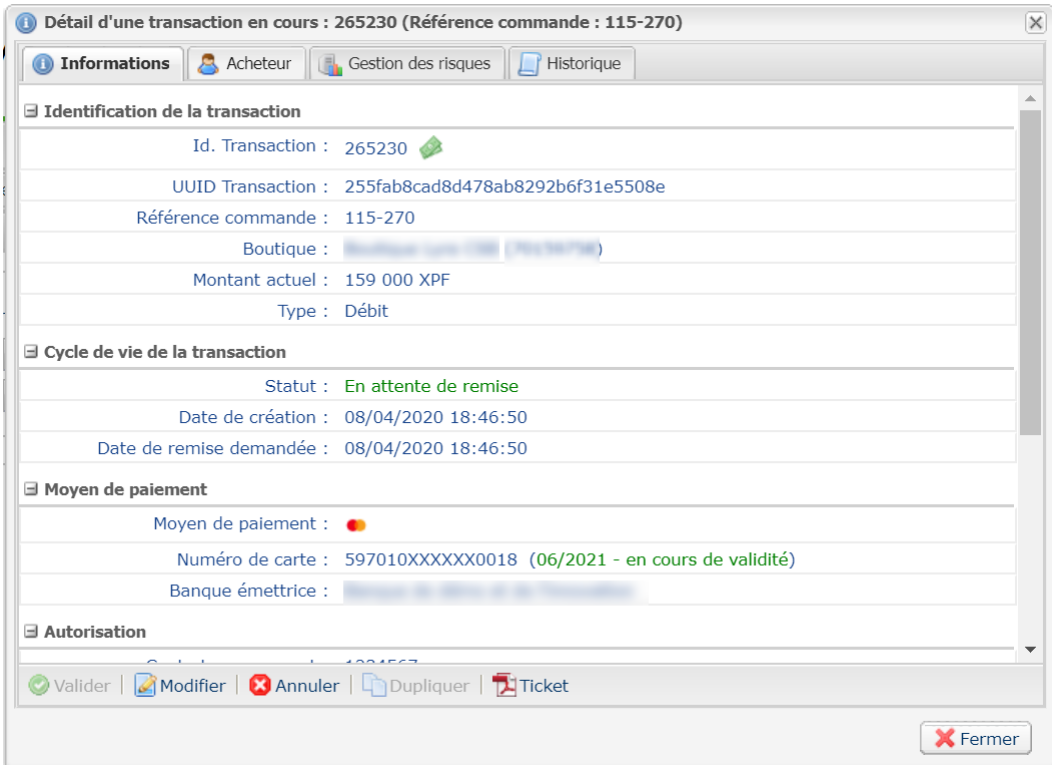
  Cet onglet s'affiche si et seulement si l'acheteur a réalisé un paiement en plusieurs fois. Il donne le tableau de toutes les échéances.

  La ligne en gras correspond à la transaction courante.

  Par double clic sur une ligne du tableau on bascule sur le détail de l'échéance correspondante.

8.1. Consulter les caractéristiques du paiement

Les caractéristiques du paiement sont affichées par défaut.



L'onglet **Informations** donne les informations suivantes :

- Identification de la transaction et l'UUID

  Affiche le numéro de transaction unique généré par la plateforme de paiement, la référence de la commande du marchand si celle-ci est transmise, le nom de la boutique, l'identifiant de la boutique, le montant actuel, la devise de la transaction et le type d'opération (débit ou crédit).

- Information sur le cycle de vie de la transaction

  Affiche le statut actuel de la transaction, la date de création de la transaction (peut être différente de la date d'autorisation), la date de remise en banque demandée et le statut de rapprochement si la transaction est déjà dans l'état **Transaction remise à l'acquéreur**.

- Moyen de paiement

  Affiche les informations sur le moyen de paiement utilisé.

- Information sur les données de l'autorisation

  Quel que soit le moyen de paiement utilisé, le code retour acquéreur est restitué sans altération (important pour les acquéreurs privatifs et étrangers). Les informations affichées sont les suivantes : le contrat acquéreur qui a été utilisé pour l'autorisation (peut être surchargé par le formulaire ou peut être surchargé si des règles de déliassage (On-Us) s'appliquent), le numéro d'autorisation, les informations sur la prise d'empreinte si une préautorisation a été faite, la date et heure de l'autorisation.

- Données techniques

  Affiche le statut de l'url de notification instantanée (IPN) et la clé générée par la plateforme de paiement validant l'intégrité des données retournées.

- Informations source

  Affiche la version du navigateur utilisé, la version du module de paiement si ce dernier est restitué, la version de la solution e-commerce utilisée et la source du paiement (e-commerce, Back Office, Web Services avec la version utilisée).

8.2. Consulter le détail d'un paiement en N fois

Un paiement est dit "en plusieurs fois" dès lors que l'acheteur est débité du montant de son achat en plusieurs échéances.

Si la demande d'autorisation (ou de renseignement) est acceptée le jour de la commande, une transaction est créée pour chaque échéance du paiement en N fois.

Dans le cas contraire, une seule transaction refusée est créée. L'onglet **Historique** de la transaction indique alors le nombre d'échéances initialement prévues.

L'onglet **Paiement en N fois** n'apparaît donc que sur ce type de transaction.

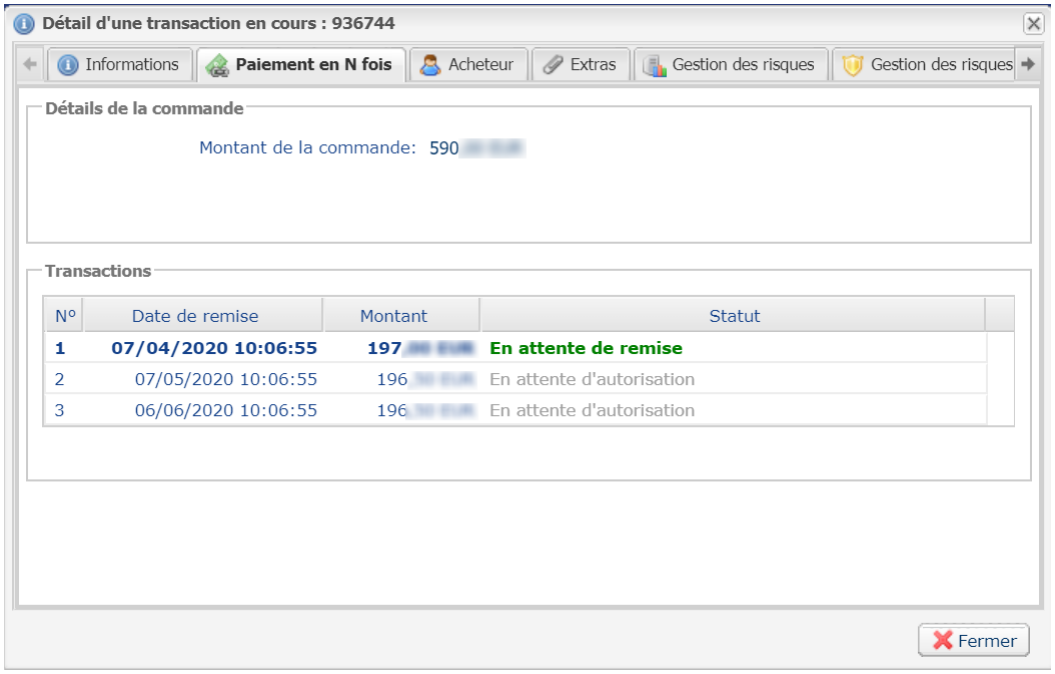


Image 3 : Exemple d'onglet Paiement en plusieurs fois

Un paiement en N fois n'est pas un crédit, mais une facilité de paiement proposée par le marchand.

Le marchand assume seul le risque d'impayé sur les différentes échéances.

La première échéance peut faire l'objet d'une authentification forte et bénéficier d'une garantie de paiement.

Ce n'est pas le cas des échéances suivantes.

En cliquant sur l'onglet **Paiement en N fois**, vous trouverez les informations suivantes:

- Le montant total de la commande,
- L'échéancier détaillant le nombre d'échéances, le montant de chaque échéance, les dates d'échéance et le statut des transactions associées.

  La ligne en surbrillance indique de quelle échéance vous consultez actuellement le détail.

En double-cliquant sur une échéance, vous ouvrez le détail de la transaction associée.

8.3. Consulter le résultat de l'authentification 3D Secure

Cliquez sur l'onglet **3D Secure**.

Dans la section **Récapitulatif** vous avez :

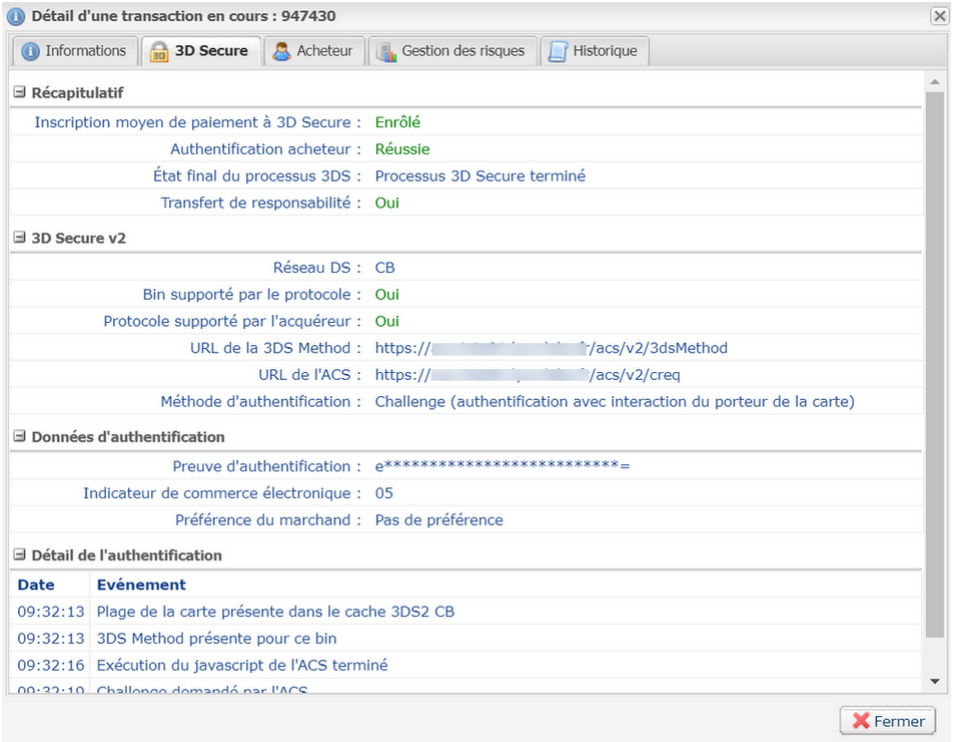
- le statut de l'inscription du moyen de paiement au programme 3D Secure ;
- le statut de l'authentification du porteur ;
- l'état final du processus 3D Secure ;
- le résultat du calcul du transfert de responsabilité.

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

- **3D 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.

8.3.1. 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 3D Secure v2.

Le protocole 3D 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.

8.3.2. 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 3D Secure v2.

  Le protocole 3D 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.

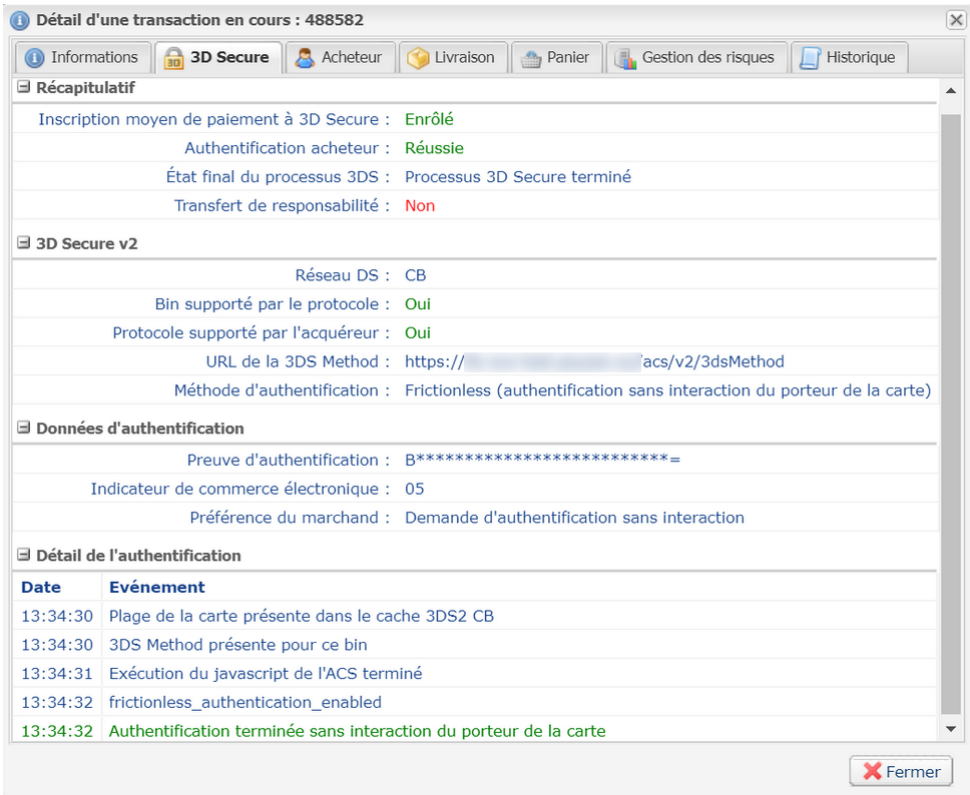
    Dans cet exemple, le motif est transmis par l'émetteur. *Consultez la liste des exemptions*.

- **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 3D Secure v2.

  Le protocole 3D 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 €.

  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*.

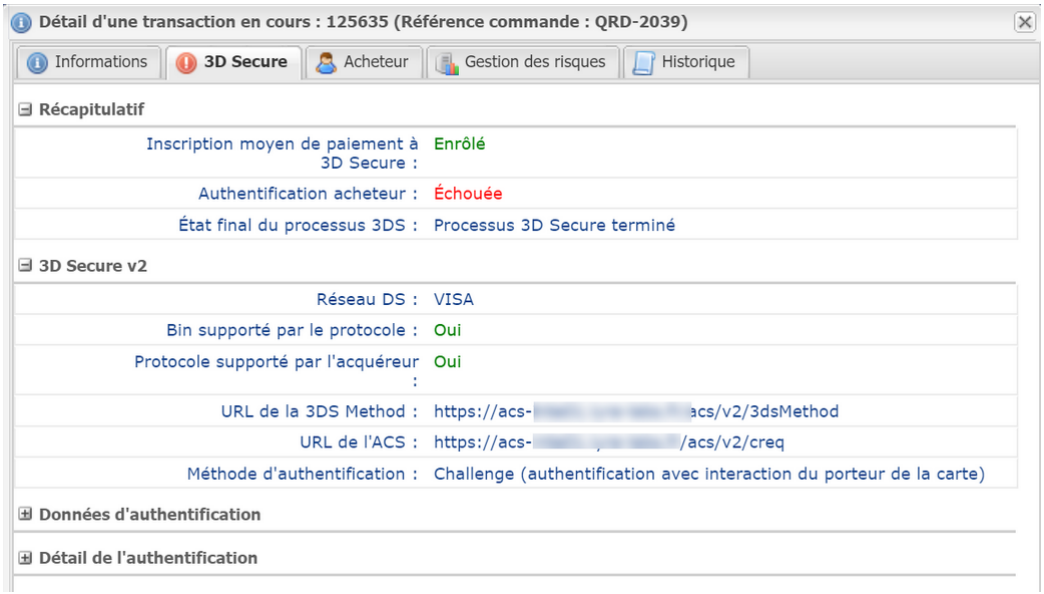
- **Détail de l'authentification** :

  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 ;
- Analyse de risque par l'acquéreur ;
- Authentification forte déléguée à un tiers ;
- Transaction à faible montant ;
- Paiements récurrents fixes à durée déterminée ;
- Le commerçant participe au programme Low Risk Merchant de 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.

8.3.3. Transaction avec authentification 3D 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 3D Secure.

Le moyen de paiement est enrôlé 3D 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 3D Secure pour la transaction" : correspond à une mauvaise saisie du code d'authentification ; ce qui a entraîné le refus du paiement.

- "206 : 3D 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

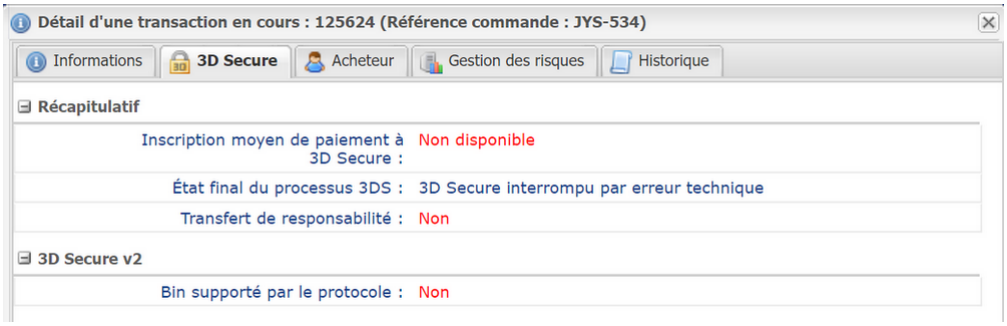
Date	Evénement
15:35:37	Plage de la carte présente dans le cache 3DS2 Mastercard
15:35:37	Pas de 3DS Method présente pour ce bin
15:35:39	Authentification rejetée par l'ACS

8.3.4. 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

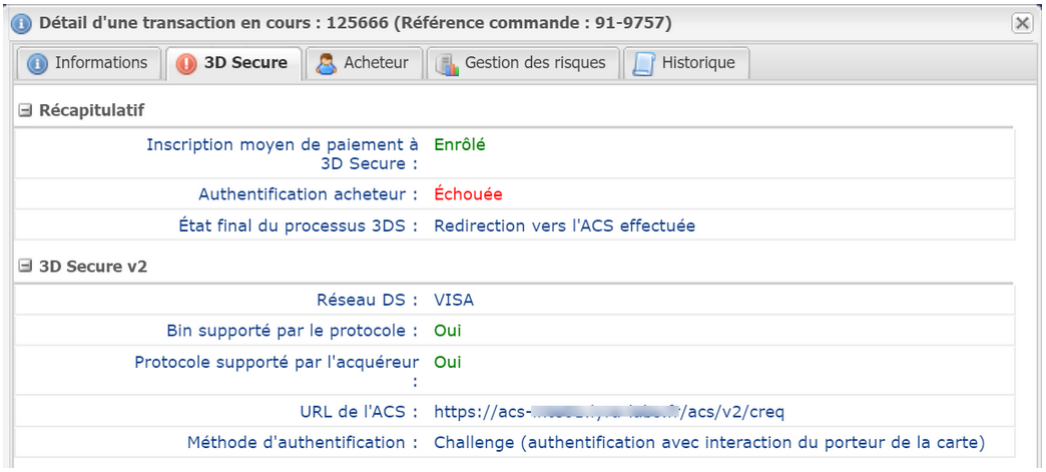
Bin supporté par le protocole :	Non

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

Le processus 3D 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.

8.3.5. Session de paiement expirée



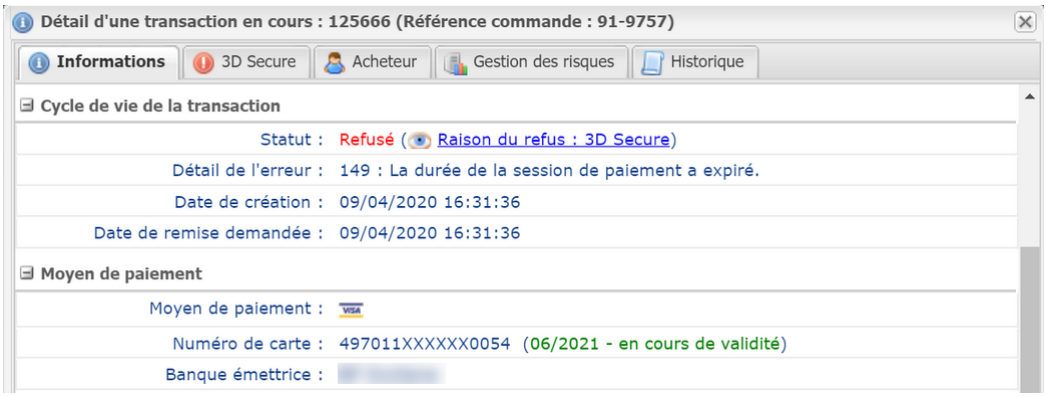
Le moyen de paiement est enrôlé 3D Secure et une authentification forte (challenge) a été requise.

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 3D 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.

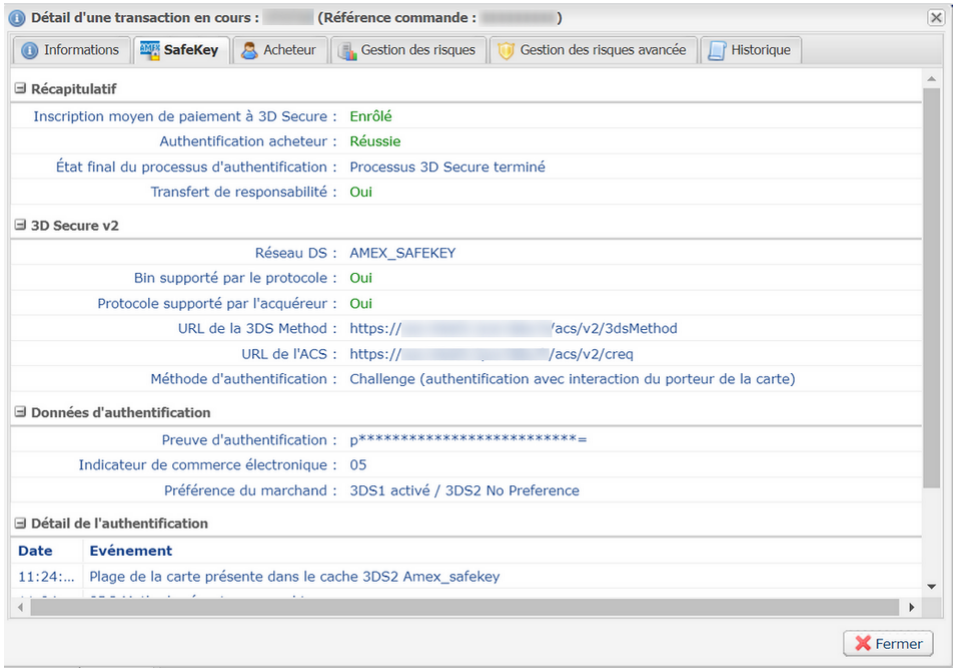
Seul le navigateur de l'acheteur interagit avec les serveurs d'authentification des banques.

8.4. Consulter le résultat de l'authentification American Express SafeKey

American Express SafeKey se base sur la technologie 3D Secure pour authentifier le porteur durant les paiements en ligne.

L'interprétation des informations de l'onglet SafeKey est identique à celle présentée dans le chapitre *Consulter le résultat de l'authentification 3D Secure à la page 19*.

Cliquez sur l'onglet **SafeKey**.



Dans la section **Récapitulatif** vous trouverez :

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

Les autres sections vous donnent des informations techniques sur le processus d'authentification, utiles en cas de demande de support :

- **3D Secure v2** : Indique notamment la méthode d'authentification du porteur (frictionless ou challenge).
- **Données d'authentification** : Indique notamment la préférence du marchand en 3DS2, le motif du refus si transmis par l'ACS, ou la validité du message contenant le résultat de l'authentification du porteur (PaRes) en 3DS1.
- **Détail de l'authentification** : Liste les différents événements intervenus lors de l'authentification.

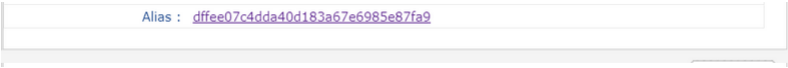
Pour plus d'informations, consulter le chapitre *Consulter le résultat de l'authentification 3D Secure à la page 19*.

8.5. Consulter les informations sur l'acheteur

Les informations sur l'acheteur sont accessibles depuis l'onglet **Acheteur**.

Cet onglet vous informe sur :

- l'adresse IP à partir de laquelle l'acheteur a fait son achat,
- le pays qui héberge l'adresse IP,
- la civilité de l'acheteur*,
- le type de client (particulier ou société)*,
- la référence de l'acheteur dans le système d'information du marchand*,
- les données personnelles de l'acheteur (nom complet, identifiant national, adresse, numéro de téléphone, etc.)*,
- la langue de l'acheteur utilisée pour afficher la page de paiement et les e-mails de confirmation de paiement,
- la raison sociale s'il s'agit d'un professionnel*,
- l'alias du moyen de paiement le cas échéant*.

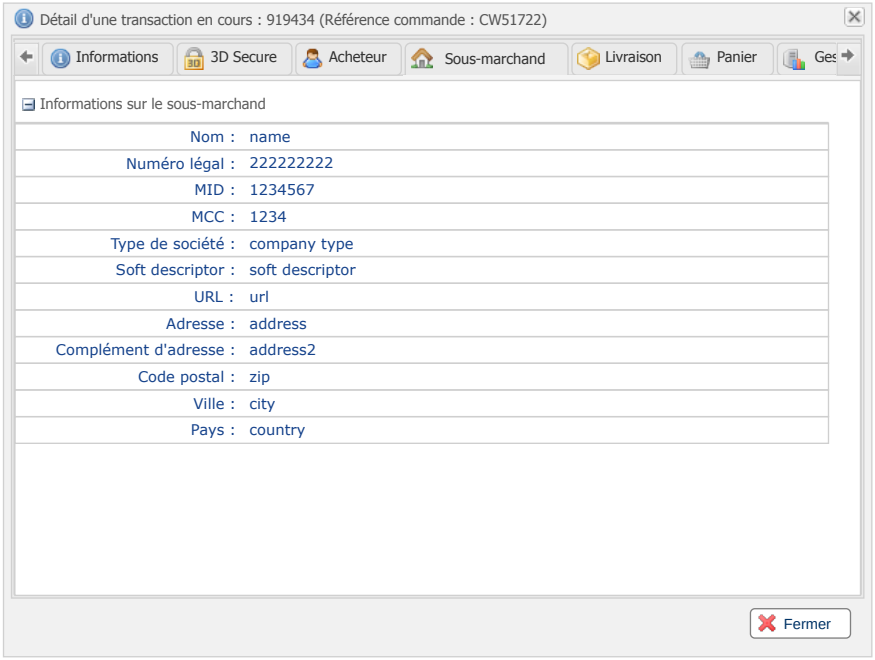


  - Vous pouvez cliquer sur l'alias pour afficher le détail de cet alias.

*Uniquement si le marchand a transmis les informations dans sa requête de paiement.

8.6. Consulter les informations du sous-marchand

Les informations du sous-marchand transmises dans la requête de paiement sont accessibles depuis l'onglet **Sous-marchand**.



8.7. Consulter les informations de livraison

Cet onglet est présent uniquement si le marchand a transmis au moins une donnée de livraison dans sa requête de paiement.

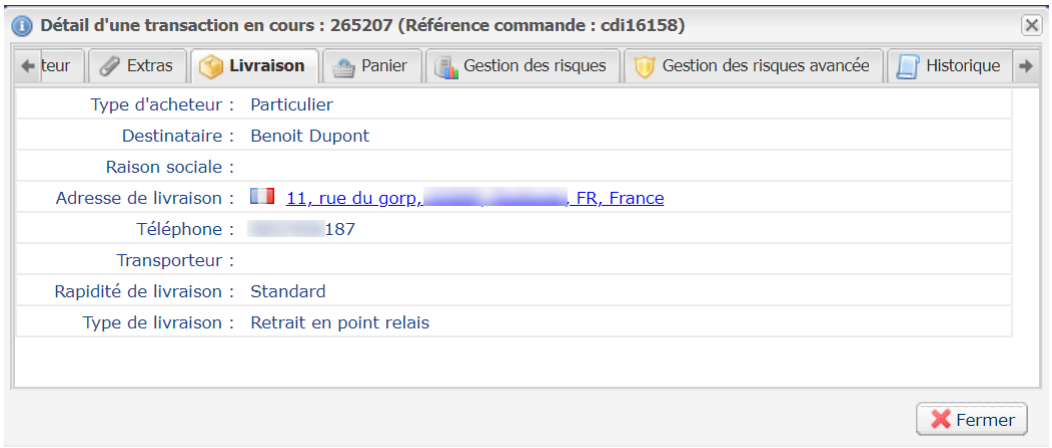


Image 4 : Exemple d'onglet Livraison

Cet onglet vous informe sur :

- le type de client (particulier ou société),
- le destinataire,
- la raison sociale en cas de livraison en point-relais ou magasin,
- le nom et prénom en cas de livraison à domicile,
- l'adresse de livraison,
- le numéro de téléphone du contact,
- le nom du transporteur,
- la rapidité delivraison,
- le type de livraison.

8.8. Consulter le détail du panier

Cet onglet est présent uniquement si le marchand a transmis au moins une information sur le contenu du panier dans sa requête de paiement.

Image 5 : Exemple d'onglet Détail du panier

Pour chaque article présent dans le panier, vous trouverez:

- Sa référence
- sa dénomination
- son prix
- sa quantité
- sa catégorie
- la montant de la TVA

8.9. Consulter les informations Extras

Image 6 : Exemple d'onglet Extras

L'onglet **Extras** est présent uniquement:

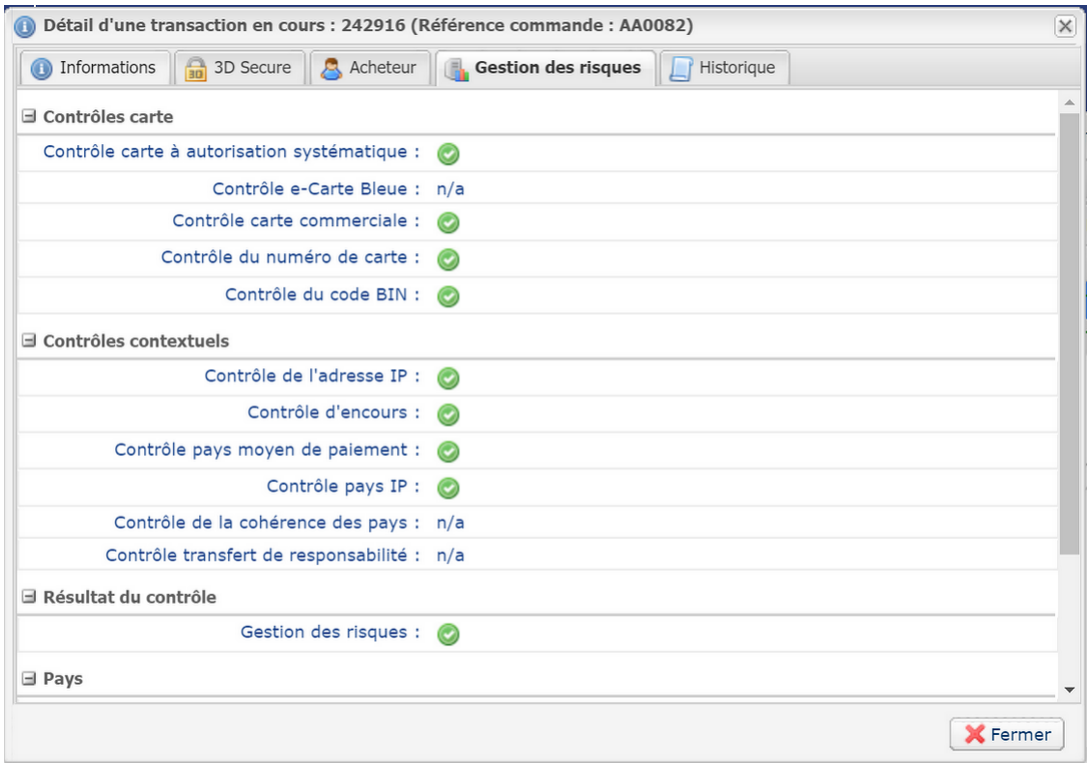
- si au moins une information complémentaire décrivant la commande a été transmise dans la requête de paiement:
  - via les champs vads_order_info, vads_order_info2, vads_order_info3 de l'API Formulaire.
  - via les attributs orderInfo, orderInfo2, orderInfo3 de l'objet metadata de l'API REST.
- si au moins un champ personnalisé a été transmis dans la requête de paiement
  - vads_ext_info_xxxx de l'API Formulaire.
  - via les metadata de l'API REST.

8.10. Consulter les contrôles effectués sur la transaction

Cet onglet est présent uniquement si vous avez souscrit au service *Gestion des risques*.

Par défaut, tous les contrôles sont désactivés. Tous les contrôles sont à paramétrer boutique par boutique (Paramétrage > Gestion des risques).

Pour consulter les contrôles effectués sur la transaction, affichez l'onglet **Gestion des risques**.



Les contrôles sont classés par rubriques (Contrôles carte, contrôles contextuels, pays, etc.)

Pour chaque contrôle, le résultat peut être:

- **n/a**: contrôle non réalisé ou non applicable,
- **icône verte**: contrôle passé avec succès – aucune alerte déclenchée,
- **icône jaune**: déclenchement d'une alerte,
- **icône rouge**: échec d'un contrôle.

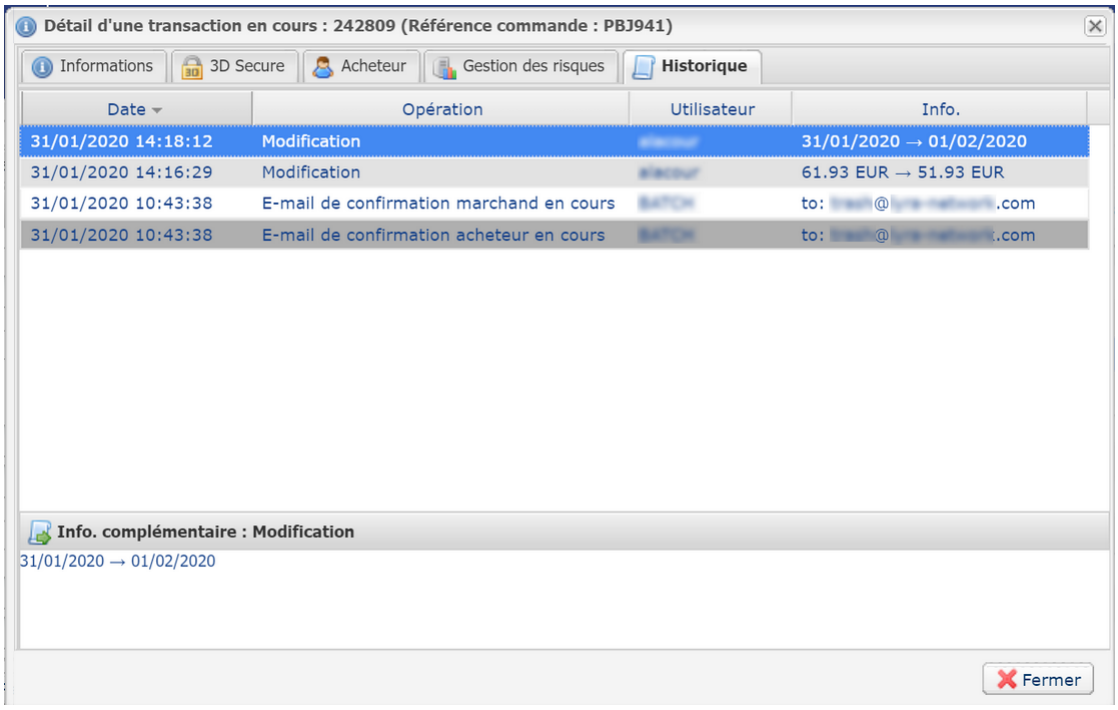
La section **Résultat du contrôle** vous donne le résultat global des contrôles:

- **n/a**: intégralité des contrôles non réalisés ou non applicables,
- **icône verte**: intégralité des contrôles passés avec succès – aucune alerte déclenchée,
- **icône jaune**: déclenchement d'une ou plusieurs alertes,
- **icône rouge**: échec d'un ou plusieurs contrôles.

En cas d'échec d'un ou plusieurs contrôles, le paiement est refusé et un point d'exclamation rouge est présent dans le libellé de l'onglet.

8.11. Consulter l'historique de la transaction

Pour consulter l'historique des opérations effectuées sur la transaction, affichez l'onglet **Historique**.



Tous les événements sont listés avec le maximum de détail possible.

- Toute mise à jour sur la transaction (date de remise, montant, annulation, remboursement, ...)
- Historique de l'envoi d'e-mail marchand et accusé de réception
- Historique de l'envoi d'e-mail acheteur et accusé de réception
- Historique des appels URL de notification à la fin du paiement

  Sont enregistrés la date et heure d'appel, le temps de traitement de l'IPN côté site marchand, et les 200 premiers octets lus sur l'interface de connexion (socket) du site marchand.
- Information sur l'heure de remise en banque et le numéro de remise associé s'il existe.

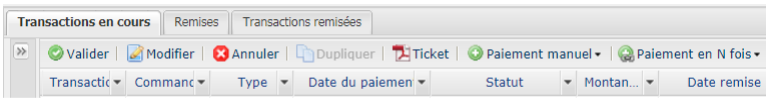
9. RÉALISER UNE OPÉRATION SUR VOS TRANSACTIONS

La liste des opérations autorisées sur une transaction dépend de son statut (et des droits de l'utilisateur).

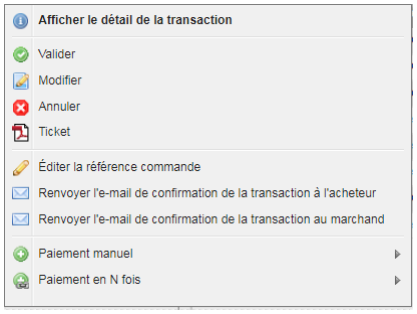
Cette liste varie selon que vous vous placiez dans l'onglet **Transactions en cours** ou dans l'onglet **Transactions remisées**.

La liste des opérations autorisées est accessible:

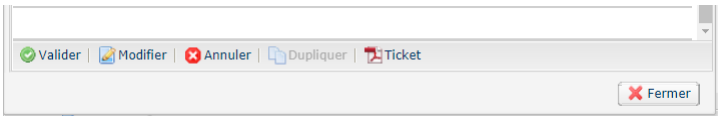
- par la barre de menu,



- par clic droit,



- en bas de la fenêtre de **Détail de la transaction**.



9.1. Valider une transaction

Cette opération permet d'indiquer que la transaction peut être remisée à la date de présentation retenue.

Seules les transactions ayant l'un des statuts suivants peuvent être validées :

- **À valider**
- **À valider et autoriser**

Pour valider une transaction:

1. Cliquez sur l'onglet **Transactions en cours**
2. Sélectionnez la transaction.
3. Cliquez sur **Valider**.

Une fois la transaction validée, le statut devient "**En attente de remise**" ou "**En attente d'autorisation**" en fonction du statut initial de la transaction.

Même s'il n'est pas validé avant la date de remise prévue, le paiement restera dans l'état À valider jusqu'à expiration de l'autorisation.

Dans l'intervalle vous pourrez donc toujours le valider et/ou le modifier même si la date de remise initiale est dépassée.

Cas des paiements en N fois créés en mode de validation manuelle:

Quand un utilisateur valide la première échéance, une fenêtre s'affiche pour demander la confirmation de la validation et lui proposer une validation simultanée de toutes les échéances restantes.

Lors de chaque validation d'échéance, et tant que l'utilisateur n'a pas validé toutes les échéances restantes, cette validation simultanée des échéances restantes est proposée

9.2. Annuler une ou plusieurs transactions

Cette opération permet d'annuler totalement la transaction avant le débit effectif.

Elle ne permet pas d'annulation partielle. Si vous souhaitez annuler partiellement une transaction, consultez le chapitre *Modifier une transaction*.

En fonction de l'acquéreur, l'annulation est possible :

- avant que la date de remise ne soit atteinte (notamment sur le réseau CB),
- après la date de remise, tant que la transaction n'est pas compensée.

L'annulation ne sera pas proposée si le processus de remise est déjà démarré. Dans ce cas vous devrez procéder à un remboursement.

Lorsqu'une demande d'annulation est acceptée, le statut de la transaction passe à **Annulé** (CANCELLED).

Il est impossible d'annuler une demande d'annulation.

Demande de redressement (reversal)

Si l'acquéreur le supporte, lorsque le marchand annule une transaction, la plateforme de paiement demande automatiquement l'annulation de la demande d'autorisation.

Si l'émetteur de la carte accepte la demande, le plafond d'autorisation de la carte du porteur est restauré.

Dans le cas contraire ou si l'acquéreur ne supporte pas le redressement, la transaction est annulée et le plafond de la carte est restauré lors de l'expiration de la demande d'autorisation.

Si une demande de redressement est réalisée lors de l'annulation, l'information est visible dans le détail de la transaction (onglet Historique).

Pour demander l'annulation d'une transaction :

- Placez-vous dans l'onglet **Transactions en cours** pour annuler une transaction en cours.

1. Sélectionnez la transaction.
2. Cliquez sur **Annuler**.

   Un message de confirmation d'annulation s'affiche.
3. Cliquez sur **Oui** pour confirmer l'annulation de la transaction ou sur **Non** pour annuler votre action.

Un message d'erreur peut apparaître si l'annulation de la transaction n'est pas possible. Dans ce cas, suivez les instructions indiquées par le message.

Cas des paiements en N fois:

En cas d'annulation d'une transaction avec plusieurs échéances, vous avez la possibilité d'annuler uniquement la transaction sélectionnée ou d'annuler toutes les échéances associées. Il suffit de cocher "**Annuler toutes les échéances des paiements en n fois**".

Annulation multiples

Il est possible d'annuler plusieurs transactions en même temps :

1. Sélectionnez l'ensemble des transactions à annuler.

   *Utilisez la touche **Ctrl** et le **clic gauche** pour sélectionner plusieurs transactions.*

2. Cliquez sur **Annuler** et confirmez votre choix.

Le statut des transactions passera à **Annulé**.

9.3. Modifier une transaction

L'opération **Modifier** est disponible lorsque la transaction possède un des statuts suivant :

- A valider
- A valider et autoriser
- En attente d'autorisation
- En attente de remise

Cette action permet de modifier le montant et la date de remise en banque en respectant les contraintes suivantes:

- le montant modifié ne peut être supérieur au montant initial
- lorsque la transaction n'a pas encore été autorisée, la date de remise peut être positionnée à n'importe quelle date comprise entre la date du jour et la date de remise spécifiée par le marchand lors du paiement.

  Une demande d'autorisation sera automatiquement déclenchée si la date de remise choisie est comprise entre la date du jour et la date de fin de validité d'une demande d'autorisation (Ex: 7 jours pour Visa).
- lorsque la transaction a déjà été autorisée, la date de remise en banque ne peut être supérieure à la date de validité de l'autorisation (Ex: 7 jours pour Visa)
- le type de carte autorise la modification du montant ou de la date de remise.

Pour modifier une transaction :

1. Sélectionnez la transaction.

2. Cliquez sur **Modifier**.

   La boîte de dialogue **Modification d'une transaction** s'affiche.

   *Il est possible de valider les transactions ayant un statut **A valider** ou **A valider et autoriser**, en cochant la case **Valider la transaction**.*

3. Renseignez le nouveau montant.

Pour rappel, le nouveau montant doit être inférieur au montant initial.

4. Renseignez la date de remise.

   Le calendrier proposera la plage autorisée pour la date de remise. La plage est calculée en fonction de la durée de validitée de l'autorisation. Cette durée dépend du moyen de paiement et du réseau sur lequel a été réalisée la demande d'autorisation (ex: 7 jours pour Visa).

5. Cliquez sur **Valider**.

Une fois la transaction modifée:

- le montant du paiement correspond au montant modifié,
- le montant initial correspond au montant avant modification.

9.4. Dupliquer une transaction

Cette fonction permet de créer une nouvelle transaction ayant exactement les mêmes caractéristiques (n ° de carte notamment) que la transaction qui a servi de base à la duplication.

Une transaction dupliquée possède les mêmes caractéristiques que toutes les autres transactions, en particulier, elle peut être à son tour dupliquée.

Lors de la duplication d'une transaction, une nouvelle demande d'autorisation est effectuée avec le numéro de carte correspondant à la transaction d'origine. Cette transaction ne possède pas de garantie de paiement.

Le ticket de paiement sera envoyé à l'acheteur si l'e-mail existe sur la transaction d'origine et si la règle de notification associée à l'envoi d'un e-mail à l'acheteur est active.

Les transactions pouvant faire l'objet d'une duplication doivent posséder un des statuts suivants :

- Remisé
- Expiré
- Annulé
- Refusé

La duplication de transactions refusées, réalisées avec des cartes Mastercard (Mastercard, Maestro, Mastercard Debit), est interdite lorsque le motif du refus est compris dans la liste ci-dessous :

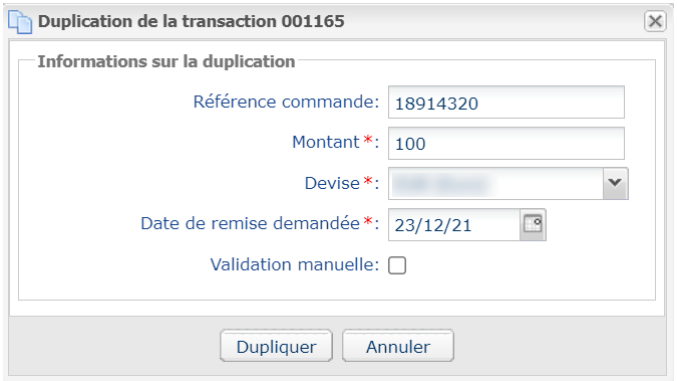
- 04 - Conserver la carte
- 14 - Numéro de porteur invalide
- 15 - Émetteur de carte inconnu
- 41 - Carte perdue
- 43 - Carte volée
- 54 - Date de validité de la carte dépassée

Pour dupliquer une transaction :

1. Sélectionnez la transaction.

2. Cliquez sur **Dupliquer**.

La boîte de dialogue **Duplication de la transaction** s'affiche. L'ensemble des champs est pré renseigné.



Vous pouvez modifier :

- La référence de la commande.
- Le montant.
- La devise.

  Si la devise sélectionnée n'est pas supportée le message suivant s'affiche : ***Devise non supportée pour ce contrat et/ou cette boutique***.
- La date de remise demandée.

  Elle ne peut être antérieure à la date de modification de la transaction.
- Le mode de validation en (dé)cochant **Validation manuelle** si vous le souhaitez.

3. Cliquez sur **Dupliquer** pour continuer ou sur **Annuler** pour annuler la duplication.

La transaction est affichée dans l'onglet **Transactions en cours**.

9.5. Rembourser une transaction

Cette opération permet de re-créditer le compte d'un client suite à une transaction.

Le compte d'un client est crédité du montant remboursé, le compte du marchand est débité de ce même montant.

Le remboursement est disponible uniquement sur les transactions remisées. En fonction de l'acquéreur, il est possible de rembourser une partie ou la totalité d'un montant d'une transaction.

Le délai de remboursement suivant la date du paiement initial dépend également de l'acquéreur ou du réseau.

Par exemple :

- Jusqu'à expiration de la carte sur le réseau CB. Le remboursement sur une carte expirée est interdit.

Pour plus d'informations, consultez la documentation de référence du moyen de paiement concerné.

Cas du refus d'un remboursement :

Un dispositif appelé **credit online** a récemment été mis en place. Ce dispositif intègre une demande d'autorisation systématique auprès de la banque de l'acheteur à chaque demande de remboursement.

Vous pouvez ainsi savoir si le remboursement est accepté et, dans le cas contraire, la raison du blocage.

En cas de refus lors de la demande d'autorisation, la banque de l'acheteur nous renvoie un motif que nous vous présentons.

Pour le réseau CB, nous indiquons le code et le motif du refus renvoyés par la banque de l' acheteur. Si la demande de remboursement s'effectue depuis le Back Office Marchand, un message d'avertissement s'affiche en plus, pour informer que l'établissement financier de l'acheteur est à l'origine de ce refus pour des raisons qui lui sont propres.

Par exemple, si la demande de remboursement se fait sur une carte en opposition, le code et le motif du refus peut être "59 : suspicion de fraude" pour certains acquéreurs. Voir : *la liste des codes de retour spécifiques* au réseau CB pour plus de détails.

Vous devez alors rembourser votre acheteur **par un autre moyen de paiement** (chèque, virement, etc.).

1. Placez-vous dans l'onglet **Transactions remisées**.
2. Sélectionnez la transaction.
3. Cliquez sur **Effectuer un remboursement**. La boîte de dialogue **Remboursement de la transaction** s'affiche.

Exemple de remboursement total

Exemple de remboursement partiel

4. Renseignez le montant que vous souhaitez rembourser. Le champ de saisie apparaît si le remboursement partiel est possible.
5. Cliquez sur **Effectuer le remboursement**. Le détail de cette opération s'affiche.

9.6. Rapprocher manuellement

Cette opération permet de rapprocher manuellement les paiements d'un marchand depuis un extrait de compte.

1. Depuis l'onglet **Transactions remisées**, recherchez la transaction concernée.
2. Effectuez un clic droit sur la transaction.
3. Sélectionnez **Rapprocher manuellement**.
4. Cliquez sur **Oui** pour confirmer le rapprochement manuel de la transaction sélectionnée.
   La boîte de dialogue **Commentaire** s'affiche.
5. Saisissez un commentaire pour ce rapprochement.
6. Cliquez sur **OK**.

Le statut de rapprochement de la transaction devient **Rapproché**.

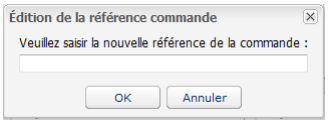
9.7. Editer la référence d'une commande

Cette opération permet au marchand de changer la référence de commande.

Pour éditer la référence commande d'une transaction :

1. Effectuez un clic droit sur la transaction.

2. Sélectionnez **Éditer la référence de la commande**.



3. Saisissez la nouvelle référence de la commande.

4. Cliquez sur **OK**.

9.8. Créer un alias depuis une transaction

Cette action permet à l'utilisateur de créer un alias du moyen de paiement utilisé pour le paiement.

Cette action est autorisée uniquement si le statut de la transaction d'origine est :

- accepté
- à valider
- en attente de remise
- présenté
- remise en cours.

Le moyen de paiement utilisé dans la transaction d'origine doit :

- supporter le paiement par alias,
- être supporté par un contrat non résilié et associé à la boutique.

La création d'un alias donne lieu à la création d'une transaction de type **VERIFICATION** et à l'envoi des notifications suivantes (si le marchand a activé les règles correspondantes) :

- URL de notification sur une opération provenant du Back Office,
- E-mail de confirmation d'une création d'alias à destination du marchand
- E-mail de confirmation d'une création d'alias à destination de l'acheteur

Une ligne d'historique sera ajoutée dans le détail de la transaction d'origine afin de tracer l'opération.

Pour créer un alias :

1. Effectuez un clic droit sur la transaction.

2. Sélectionnez **Créer un alias depuis cette transaction**.

   L'assistant de création d'un alias s'affiche.

3. Saisissez l'adresse **E-mail acheteur**.

4. Un alias (token) est généré par défaut dans le champ **Identifiant alias**. Vous pouvez cliquer sur le bouton **Générer un nouvel identifiant** si vous le souhaitez.

   Vous avez aussi la possibilité de renseigner votre propre alias. Il faut, cependant, veiller à son unicité.

5. Si vous le souhaitez, vous pouvez sélectionner la devise utilisée lors de la vérification du moyen de paiement.

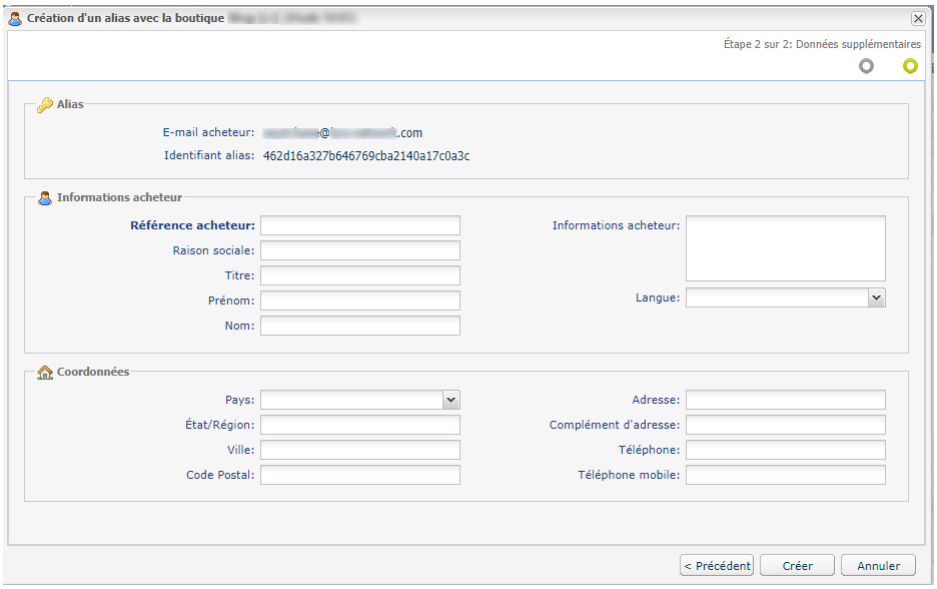
   Ce choix est utile lorsque vous possédez un contrat multi-devises associé à plusieurs boutiques, chacune ne supportant qu'une seule devise.

Il sera toujours possible d'utiliser l'alias pour réaliser des paiements dans n'importe quelle devise supportée par le contrat.

6. Cliquez sur **Suivant**.

   La page de saisie des données de l'acheteur s'affiche.

   La rubrique **Alias** vous rappelle l'e-mail saisi- ainsi que l'alias créé.



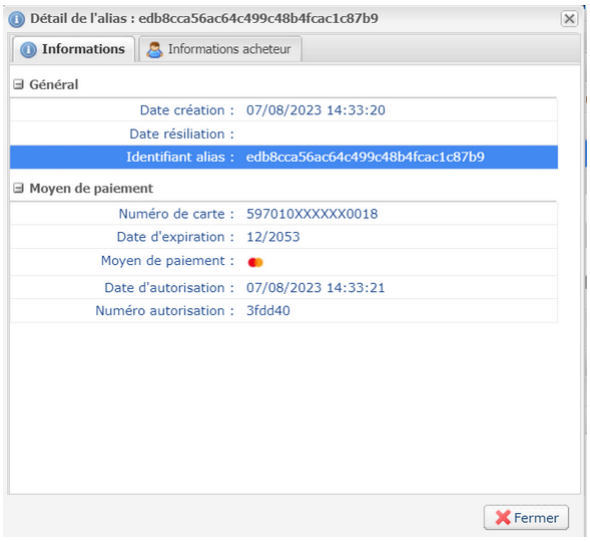
7. Renseignez les informations sur l'acheteur.

   Ces informations sont utiles pour mieux identifier l'acheteur.

   Les champs précédés d'un astérisque (*) sont obligatoires.

8. Cliquez sur **Créer** pour terminer.

Si tous les contrôles du moyen de paiement ont abouti avec succès, la fenêtre de détail de l'alias est affichée.



On y retrouve notamment l'**Identifiant alias**. Il correspond à l'alias nouvellement créé. Ce dernier pourra être utilisé ultérieurement pour effectuer une autre opération bancaire dans votre (ou vos) boutique(s).

> *L'alias (token) ne sera pas créé si la demande d'autorisation ou de renseignement est refusée.*

9.9. Télécharger le ticket de paiement

Le ticket de paiement est une preuve de la transaction liant le marchand à l'acheteur et peut être présenté en cas de contestation ou de demande de renseignement auprès de l'émetteur ou de l'acquéreur.

Vous pouvez télécharger le ticket d'une transaction au format PDF.

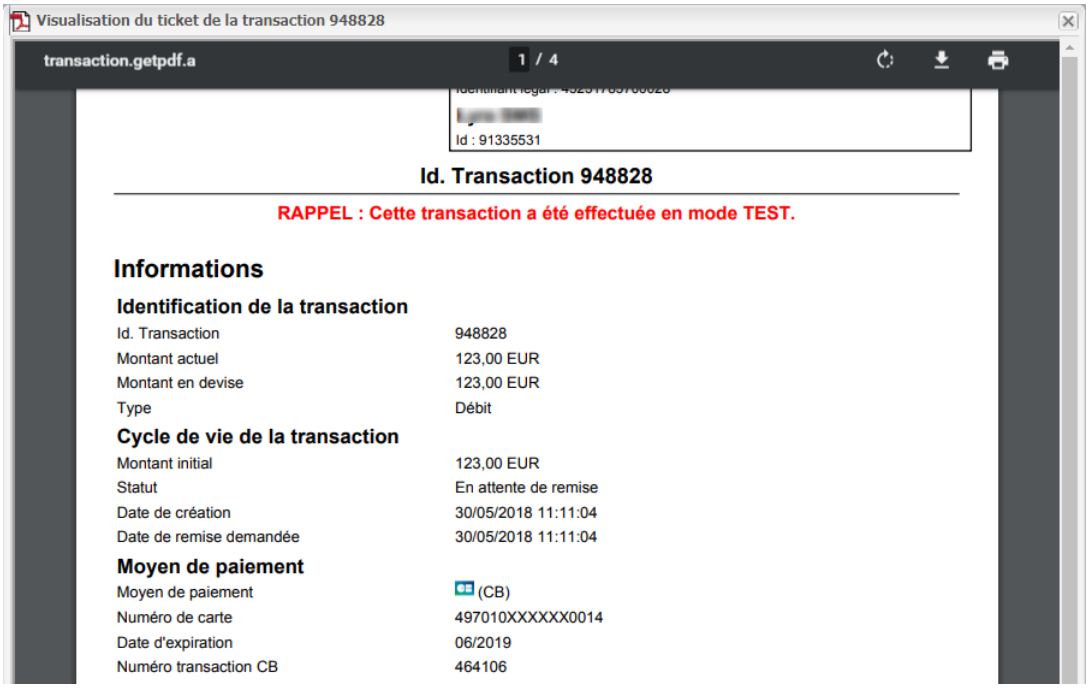
Cette opération est disponible sur les **transactions en cours** et sur les **transactions remisées** :

1. Recherchez et sélectionnez la transaction.
2. Cliquez sur **Ticket**

   La page de **choix des pages à imprimer** s'affiche.

   Les choix proposés dépendent des onglets disponibles sur la transaction.

3. Cochez les données à imprimer.
4. Cliquez sur **Visualiser PDF** pour visualiser les informations avant téléchargement.



5. Cliquez sur **Télécharger** pour imprimer ou enregistrer le document.

9.10. Envoyer un ordre de paiement à partir d'une transaction refusée

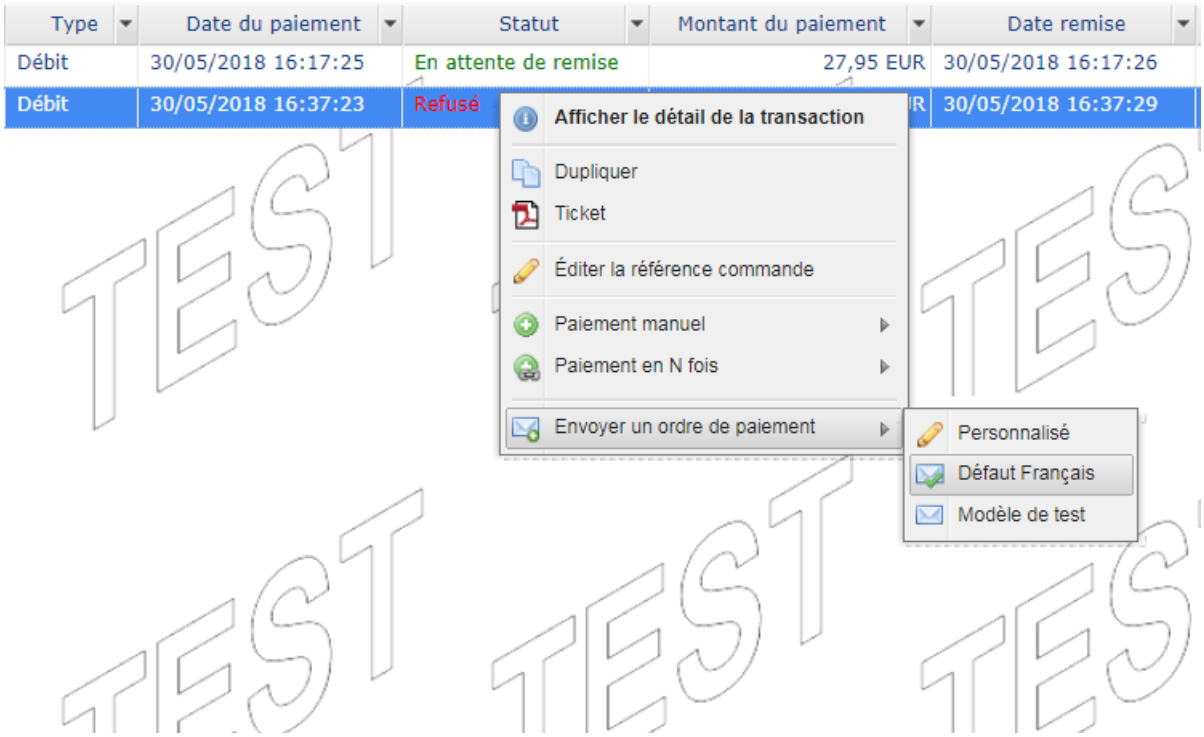
Suite à un paiement refusé, vous avez la possibilité d'envoyer à votre acheteur un ordre de paiement à partir du paiement refusé.

Lors de cette deuxième tentative, l'acheteur aura, par exemple, la possibilité de changer de moyen de paiement.

Remarque

Pour utiliser cette fonctionnalité, votre offre doit inclure le paiement par e-mail.

1. Depuis l'onglet **Transaction en cours**
2. Sélectionnez la transaction refusée.
3. Faites un clic droit sur la transaction refusée.



4. Sélectionnez le sous menu **Envoyer un ordre de paiement**

   Plusieurs possibilités dans le choix du modèle de l'e-mail :

   - le modèle d'e-mail par **Défaut** vous permet un envoi sans personnalisation et dans la langue du Back Office Marchand.
   - le modèle **Personnalisé** vous permet d'aller vers l'éditeur d'ordre de paiement par e-mail et de personnaliser votre e-mail (objet, texte, durée de validité, 3DS sélectif sur l'ordre).
   - les autres modèles vous permettent d'envoyer directement l'e-mail en sélectionnant juste le nom du modèle.

   L'envoi de l'e-mail est immédiat sans passer par l'éditeur d'ordre de paiement mail si vous sélectionnez un modèle. Une page de confirmation s'affiche.

5. Confirmez l'envoi de l'e-mail en cliquant sur **Oui**.

Votre acheteur recevra un ordre de paiement avec le même montant déjà refusé. Il lui suffit de suivre le lien pour reprendre le paiement.

10. RENVOYER MANUELLEMENT UNE NOTIFICATION

Le marchand peut renvoyer manuellement une notification à partir d'une transaction présente dans la grille des transactions (en cours ou remisées).

10.1. Renvoyer une notification de fin de paiement (IPN)

Cette fonctionnalité permet de renvoyer manuellement une notification de fin de paiement vers l'URL de notification de la boutique.

Cette procédure est utile lorsque la notification initiale s'est terminée en erreur, quelle que soit la règle qui a été déclenchée.

Pour utiliser cette fonctionnalité le marchand doit avoir configuré la règle de notification URL de notification à la fin du paiement.

L'option Exécuter l'URL de notification n'est pas disponible dans le menu contextuel si vous n'avez pas configuré la règle de notification de fin de paiement ou si votre compte utilisateur n'est pas habilité à réaliser cette action.

1. Depuis la grille des transactions, recherchez la transaction pour laquelle vous souhaitez renvoyer la notification.

2. Effectuez un clic droit sur la transaction et sélectionnez **Exécuter l'URL de notification**.

   Un message vous informe de la bonne exécution de cette commande si votre application est à nouveau disponible.

   Vous pourrez, dans tous les cas, visualiser le résultat de votre action dans l'historique des événements de la transaction et éventuellement analyser les messages d'erreur si le problème persiste.

Spécificités de l'exécution manuelle

Lors du déclenchement manuel d'une IPN, certains champs ne seront pas envoyés ou auront une valeur différente.

Exemples de champs non disponibles / non enregistrés en base de données :

- **vads_page_action**
- **vads_payment_config**
- **vads_action_mode**

Exemples de champs envoyés avec des valeurs différentes :

- **vads_url_check_src**

  Sera valorisé à **BO** dans le cas d'un rejeu manuel.
- **vads_trans_status**

  Le statut de la transaction pourra être différent entre l'appel initial et le rejeu.
- **vads_hash**
- **signature**

10.2. Renvoyer l'e-mail de confirmation de paiement au marchand

Pour renvoyer l'e-mail de confirmation de la transaction au marchand, le marchand doit avoir au préalable configuré la règle E-mail de confirmation de paiement à destination du marchand.

1. Depuis la grille des transactions, recherchez la transaction pour laquelle vous souhaitez renvoyer l'e-mail de confirmation de paiement.
2. Effectuez un clic droit sur la transaction et cliquez sur **Renvoyer l'e-mail de confirmation de la transaction au marchand**.

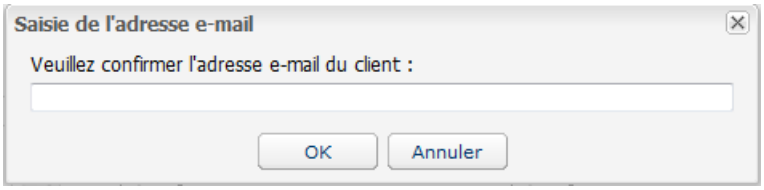
   Un message de confirmation d'envoi apparait.
3. Cliquez sur **OK**.

10.3. Renvoyer l'e-mail de confirmation de paiement à l'acheteur

Pour renvoyer l'e-mail de confirmation de paiement à l'acheteur en cas de non réception ou en cas de correction de l'adresse e-mail :

1. Depuis la grille des transactions, recherchez la transaction pour laquelle vous souhaitez renvoyer l'e-mail de confirmation à l'acheteur.
2. Effectuez un clic droit sur la transaction et cliquez sur **Renvoyer l'e-mail de confirmation de la transaction à l'acheteur**.

   La boîte de dialogue pour saisir l'adresse e-mail de l'acheteur s'affiche.

   Le champ de saisie est prérempli avec l'adresse e-mail de l'acheteur enregistrée dans la transaction.
3. Saisissez une autre adresse e-mail si nécessaire.
4. Cliquez sur **OK**.

11. DURÉE DE RÉTENTION DES TRANSACTIONS

Les transactions sont conservées dans le Back Office Marchand pendant une durée limitée.

- En Mode TEST, chaque transaction est conservée pendant une durée de 30 jours à partir de la date de la transaction. Elle sera automatiquement effacée après la date limite.
- En Mode PRODUCTION, la règle de conservation des transactions est établie selon la norme PCI-DSS. Chaque transaction est conservée pendant 15 mois à partir de la date de la transaction. Elle sera automatiquement effacée après la date limite.

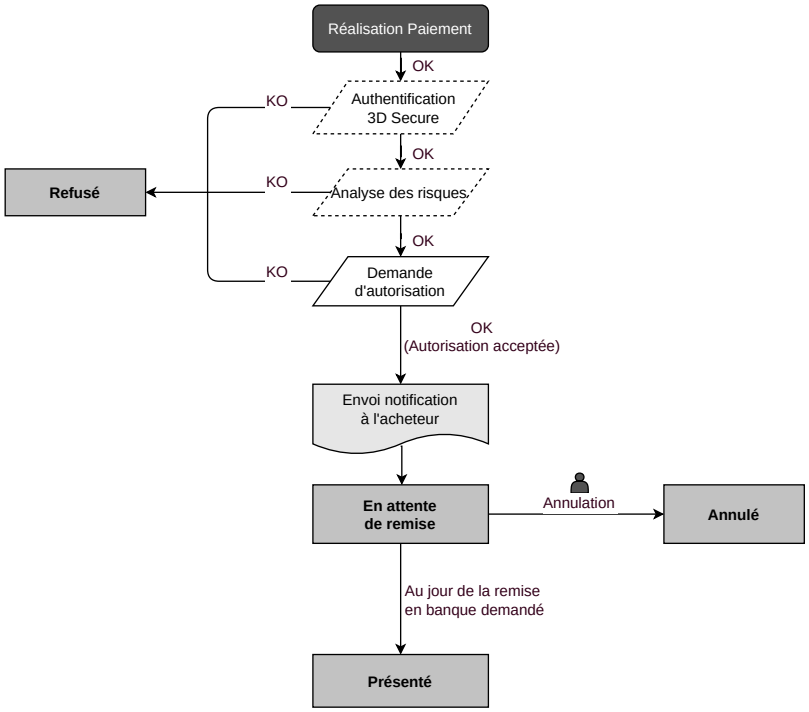
12. CYCLE DE VIE DES TRANSACTIONS

Dans tous les schémas suivants, la légende suivante est adoptée :

Action du marchand nécessaire - manuelle (Back Office Marchand) ou automatique (Web Services)

12.1. Paiement comptant immédiat

12.1.1. Validation automatique



Suite à la demande de paiement, plusieurs contrôles sont automatiquement mis en oeuvre :

- L'authentification 3D Secure.
- Différents contrôles réalisés par la plateforme de paiement (ceux-ci incluent potentiellement les contrôles locaux, les règles de risques configurées par le marchand) ou par un analyseur de risque externe.
- Une demande d'autorisation est également effectuée auprès de la banque de l'acheteur, le jour même de la date de paiement, quelle que soit la date de remise en banque demandée.

Si l'un de ces contrôles échoue, la demande de paiement n'est pas acceptée. L'acheteur est informé du refus à l'écran. Dans le Back Office Marchand, la transaction est consultable avec le statut **Refusé**.

Dans le cas contraire, la transaction prend le statut **En attente de remise**.

L'acheteur est informé de l'acceptation de sa demande de paiement et est destinataire d'un e-mail de confirmation.

La transaction partira automatiquement en remise le jour demandé par le marchand et prendra le statut **Présenté**. Le statut **Présenté** est définitif.

Une fois la remise effectuée, la compensation de la transaction sur le compte du marchand dépend des délais de traitements interbancaires.

Dans l'attente de cette remise, le marchand peut modifier la date de remise ainsi que le montant (modification du montant uniquement à la baisse, ce cas correspond à une livraison partielle par le marchand).

Si nécessaire, il peut également annuler la transaction : celle-ci prend alors le statut **Annulé**.

12.1.2. Validation manuelle

Suite à la demande de paiement, des contrôles sont automatiquement mis en oeuvre :

- L'authentification 3D Secure.
- Différents contrôles réalisés par la plateforme de paiement (ceux-ci incluent potentiellement les contrôles locaux, les règles de risques configurées par le marchand) ou par un analyseur de risque externe.
- Une demande d'autorisation est effectuée auprès de la banque de l'acheteur.

Si l'un de ces contrôles échoue, la demande de paiement n'est pas acceptée. L'acheteur est informé du refus à l'écran. Dans le Back Office Marchand, la transaction est consultable avec le statut **Refusé**.

Dans le cas contraire le paiement est accepté et la transaction est consultable dans le Back Office Marchand avec le statut **À valider**.

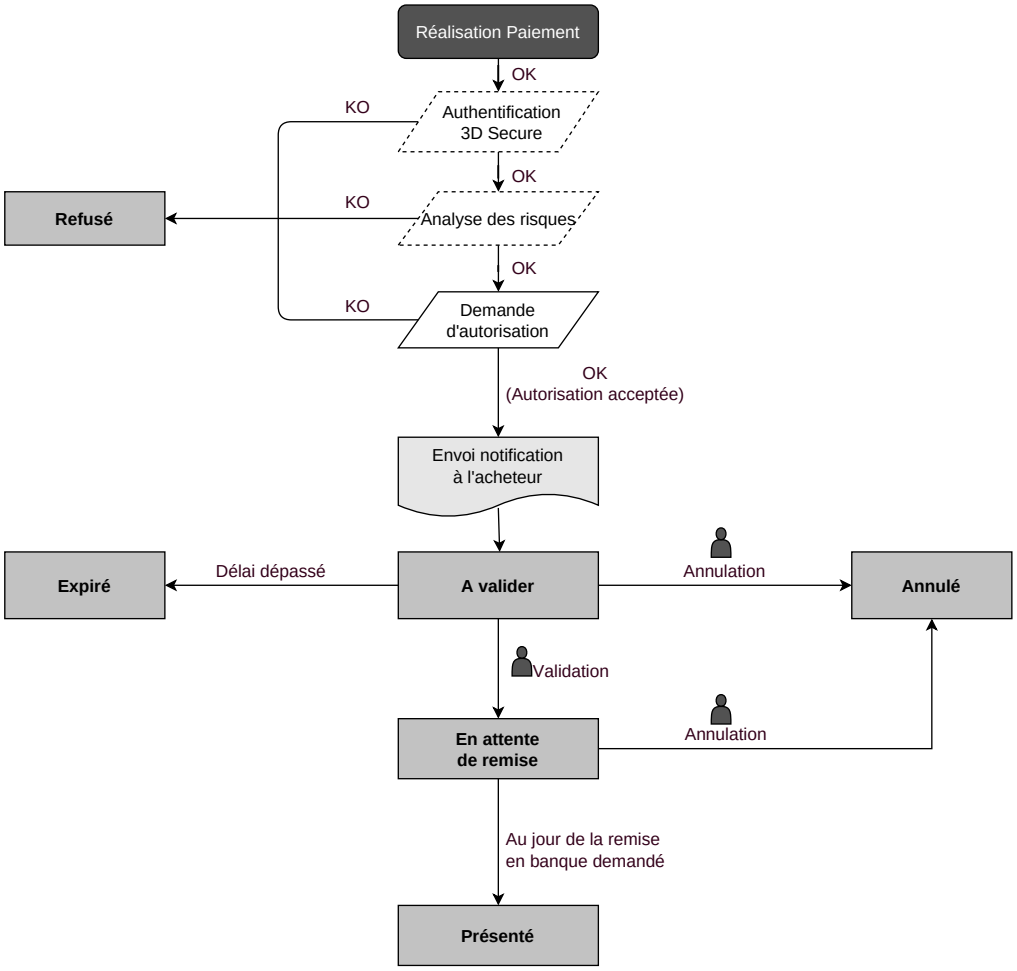
Le marchand doit alors obligatoirement valider la transaction avant la date d'expiration de la demande d'autorisation. Dans le cas contraire, la transaction prend le statut **Expiré** et ne peut plus être remise en banque.

Dès lors qu'une transaction est validée, elle passe en statut **En attente de remise**.

La transaction partira automatiquement en remise le jour demandé par le marchand et prendra le statut **Présenté**. Le statut **Présenté** est définitif.

Une fois la remise effectuée, la compensation de la transaction sur le compte du marchand dépend des délais de traitements interbancaires.

Le marchand peut également annuler la transaction si nécessaire. La transaction prend alors le statut **Annulé**.


Réalisation Paiement
OK
Authentification
3D Secure
KO
OK
Analyse des risques
KO
Refusé
OK
Demande
d'autorisation
KO
OK
(Autorisation acceptée)
Envoi notification
à l'acheteur
A valider
Délai dépassé
Expiré
Annulation
Annulé
Validation
En attente
de remise
Annulation
Au jour de la remise
en banque demandé
Présenté

12.2. Paiement comptant différé

12.2.1. Validation automatique

Délai de remise inférieur à la durée de validité de l'autorisation

(voir diagramme cycle de vie d'une transaction de paiement comptant immédiat).

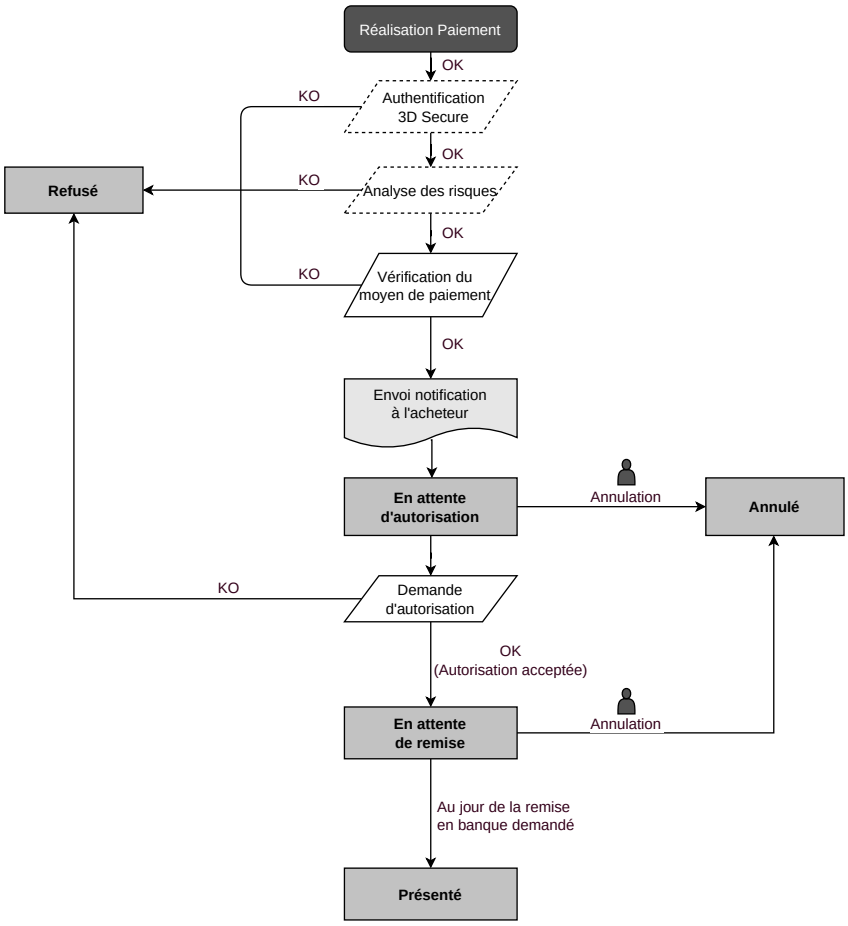
Délai de remise supérieur à la durée de validité de l'autorisation

Toute transaction de paiement comptant différé réalisée avec le mode de validation automatique, et dont la demande de vérification a été réalisée avec succès, est consultable dans le Back Office Marchand avec le statut **En attente d'autorisation**.

La demande d'autorisation est automatiquement effectuée :

- fonctionnement par défaut : la veille de la date de remise en banque souhaitée,
- fonctionnement avec autorisation anticipée : selon le moyen de paiement sélectionné, à J-Δ avant la date de remise en banque souhaitée (voir chapitre *Le service "Autorisations anticipées"* à la page 54).

Le diagramme suivant résume les différents statuts d'un paiement différé :



12.2.2. Validation manuelle

Délai de remise inférieur à la durée de validité de l'autorisation

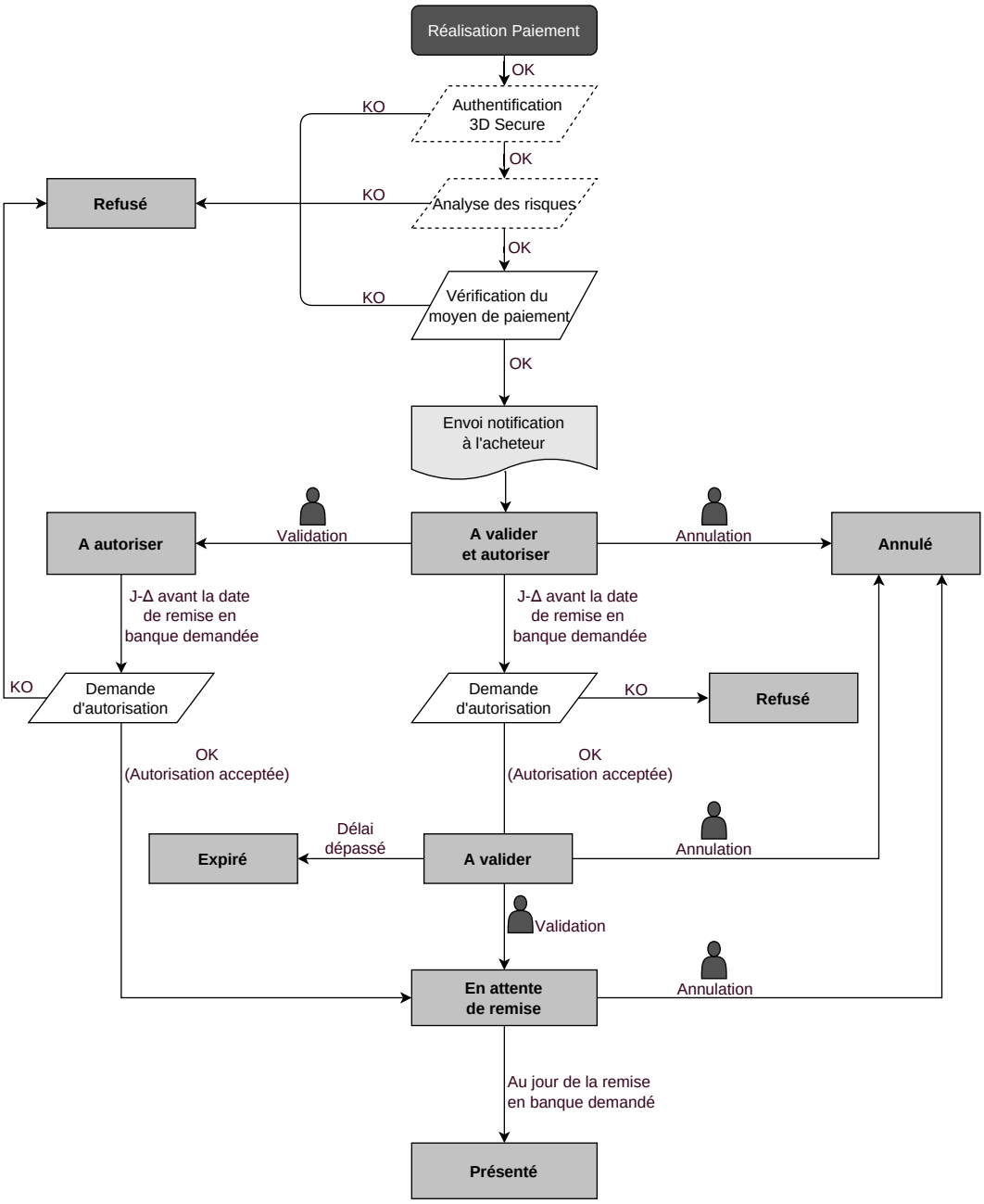
(voir diagramme cycle de vie d'une transaction de paiement comptant immédiat).

Délai de remise supérieur à la durée de validité de l'autorisation

Toute transaction de paiement comptant différé réalisée avec le mode de validation manuelle et dont la demande d'autorisation à 100 XPF (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été réalisée avec succès, est consultable dans le Back Office Marchand avec le statut **À valider et autoriser**.

La demande d'autorisation est automatiquement effectuée le jour de la remise en banque demandé, sous réserve que le marchand ait précédemment validé la transaction.

Dans l'attente de la remise, le marchand peut annuler la transaction ou en modifier le montant et/ou la date de remise en banque. Ces transactions suivent le diagramme d'état suivant :



12.3. Paiement en plusieurs fois

12.3.1. Validation automatique

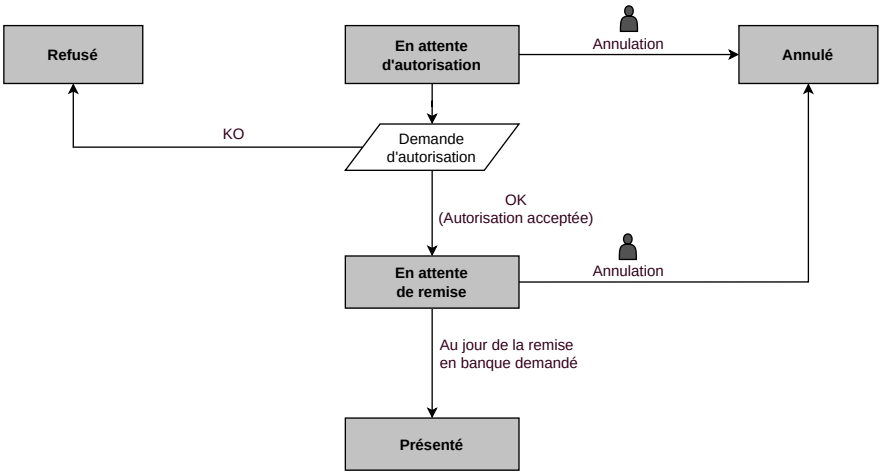
La première échéance du paiement en plusieurs fois se comportera exactement comme une transaction de paiement comptant immédiat ou une transaction de paiement différé selon sa date de remise en banque.

Les échéances suivantes sont par défaut positionnées en statut **En attente d'autorisation**. La banque de l'acheteur pourra refuser la demande d'autorisation. La plateforme de paiement informe alors le marchand du refus de la transaction par e-mail.

Les demandes d'autorisation des échéances suivantes sont automatiquement effectuées comme une transaction de paiement différé, donc avec deux dates possibles :

- fonctionnement par défaut : la veille de la date de remise en banque souhaitée,
- fonctionnement avec autorisation anticipée : selon le moyen de paiement sélectionné, à J-Δ avant la date de remise en banque souhaitée (voir chapitre *Le service "Autorisations anticipées"* à la page 54).

Les échéances ultérieures suivent le diagramme d'état suivant (cas d'une demande d'autorisation non rejouée) :



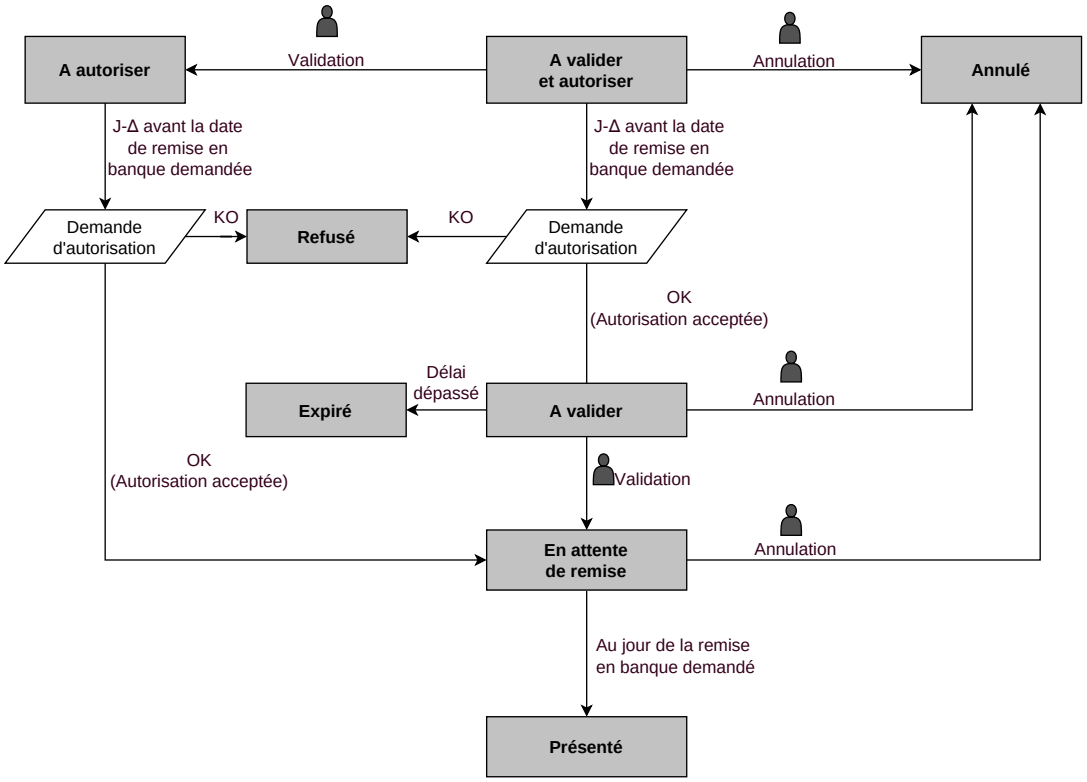
L'annulation d'une échéance n'implique en aucun cas l'annulation des échéances suivantes restant à remettre en banque.

12.3.2. Validation manuelle

La première échéance du paiement en plusieurs fois se comportera exactement comme une transaction de paiement comptant immédiat ou une transaction de paiement différé, selon la date de remise en banque demandée.

Les échéances suivantes sont par défaut positionnées en statut **À valider et autoriser** tant que la première échéance n'aura pas été validée par le marchand. Leur bonne fin n'est pas garantie pour le marchand. En effet, la banque de l'acheteur peut refuser la demande d'autorisation.

La validation de la 1ère échéance vaut validation de toutes les échéances suivantes. Par contre, l'annulation d'une échéance ne vaut pas annulation des échéances ultérieures.



12.4. Le service "Autorisations anticipées"

Ce service permet le déclenchement de l'autorisation à J-Δ (voir *durée de validité d'une autorisation* pour chaque moyen de paiement) avant la date de remise en banque souhaitée.

En cas de refus, exclusivement pour un motif non frauduleux, par la banque émettrice, un processus réitère automatiquement les demandes d'autorisation, et ce jusqu'à 2 jours avant la date de remise en banque souhaitée.

Le marchand peut à tout moment annuler la transaction ou en modifier le montant (à la baisse uniquement) et/ou la date de remise.

Ce processus s'applique :

- aux paiements récurrents
- aux paiements différés
- aux échéances autres que la première, pour un paiement en plusieurs fois.

En cas de refus pour un motif frauduleux la transaction est considérée comme définitivement refusée.

Ci dessous la liste des motifs frauduleux qui ne permettent pas le rejeu de l'autorisation.

Réseau	Codes retour autorisation	Libellé
CB / AMEX	03	Accepteur invalide
	04	Conserver la carte
	05	Ne pas honorer
	07	Conserver la carte, conditions spéciales
	12	Transaction invalide
	13	Montant invalide
	14	Numéro de porteur invalide
	15	Emetteur de carte inconnu
	31	Identifiant de l'organisme acquéreur inconnu
	33	Date de validité de la carte dépassée
	34	Suspicion de fraude
	41	Carte perdue
	43	Carte volée
	54	Date de validité de la carte dépassée
	56	Carte absente du fichier
	57	Transaction non permise à ce porteur
	59	Transaction non permise à ce porteur
	63	Règles de sécurité non respectée
	76	Porteur déjà en opposition, ancien enregistrement conservé
	80	Le paiement sans contact n'est pas admis par l'émetteur
	81	Le paiement non sécurisé n'est pas admis par l'émetteur
	82	Révocation paiement récurrent pour la carte chez le commerçant ou pour le MCC et la carte
	83	Révocation tous paiements récurrents pour la carte

Contactez votre conseiller clientèle si vous souhaitez activer les autorisations anticipées.

12.5. Durée de validité d'une demande d'autorisation

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
AMEX	American Express	AMEX	7
CB	CB	CB	7
CB	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	7
CB	Maestro	MAESTRO	30
CB	Mastercard	MASTERCARD	7
CB	Visa	VISA	7
CB	Visa Electron	VISA_ELECTRON	7
CB	VPay	VPAY	7
DINERS	Diners Club	DINERS	3
DINERS	Discover	DISCOVER	5
JCB	JCB	JCB	7
MC_CB2A	Maestro	MAESTRO	30
MC_CB2A	Mastercard	MASTERCARD	7
OSB_PRIV	Carte privative HOA (Banque de Polynésie)	PRV_BDP	7
OSB_PRIV	Carte privative Tiare (Banque de Tahiti)	PRV_BDT	7
OSB_PRIV	Carte privative MARARA	PRV_OPT	7
OSB_PRIV	Carte privative Smart Card (BRED Bank Vanuatu)	PRV_SMART_CARD	7
OSB_PRIV	Carte privative Socredo (Banque Socredo)	PRV_SOC	7
VISA_CB2A	Visa	VISA	7
VISA_CB2A	Visa Electron	VISA_ELECTRON	7
VISA_CB2A	VPay	VPAY	7

13. OBTENIR DE L'AIDE

Vous cherchez de l'aide ? Consultez notre FAQ :

https://secure.osb.pf/doc/fr-FR/faq/faq-homepage.html

Pour toute question technique ou demande d'assistance, nos services sont disponibles

- du lundi au vendredi de 07 h 00 à 17 h 00
- le samedi de 08 h 00 à 12 h 00

par téléphone au :	(689) 40 46 09 09 (Tarification de ce numéro : coût d'un appel local depuis un poste fixe.)
par e-mail :	*support@osb.pf*

et via votre Back Office Marchand, menu **Aide** > **Contacter le support**

Pour faciliter le traitement de vos demandes, il vous sera demandé de communiquer votre identifiant de boutique (numéro à 8 chiffres).

Cette information est disponible dans l'e-mail d'inscription de votre boutique ou dans le Back Office Marchand (menu **Paramétrage** > **Boutique** > **Configuration**).

