Backoffice AXEPTA

- Objectif de ce document
- Préambule
- Presentation du backoffice
- Gestion des transactions
  - Transactions
  - Détails des opérations (remboursement, annulation, capture..)
  - Fichier de réconciliation (Settlement file)
  - Création de transaction
  - Fichiers Batch
- Tableau de bord
  - Chiffres clés
  - Analyse des operations
  - Statut des transactions
  - Analyse des tendances
  - Analyse par pays
- Lutte contre la Fraude
  - Listes noires
  - Listes noires SecurePay
  - Listes blanches
  - Listes blanches SecurePay
- Gestion des utilisateurs
  - Les droits d'accès (divisés en groupes) :
  - Créer un nouvel utilisateur :
  - Consulter la liste des utilisateurs :
  - Consulter le Journal d'activités
- Gestion des clés
  - Données d'accès disponibles
  - Actions disponibles sur les clés
  - Renouveler une clé API REST principale
  - Rotation sans interruption avec les clés secondaires
  - Révoquer une clé API REST
  - Renouveler une clé HMAC
- Contacter le Support technique

Objectif de ce document

Ce document présente le backoffice AXEPTA et décrit ses différentes fonctionnalités.

Préambule

En souscrivant à la solution AXEPTA BNP Paribas, chaque commerçant aura accès au backoffice AXEPTA. Un accès en tant que « super-administrateur » est automatiquement créé à un contact défini par le commerçant et mentionné dans le formulaire de souscription. Un super-administrateur aura donc tous les droits dont le droit de créer d'autres utilisateurs et de leurs attribuer des droits également (la liste exhaustive sera présentée par la suite).

Un commerçant peut avoir accès à un ou plusieurs MIDs (Merchant IDs).

Un MID (merchant ID) permet d'identifier une boutique (que ce soit une boutique en ligne ou en proximité).

Il existe 3 types de MIDs :

- MasterMID: Permet d'avoir une vue globale de l'activité du commerçant sur les différentes boutiques qu'il possède. Le masterMID ne peut pas être utilisé pour réaliser des transactions.
- MID de test: Permet d'accéder aux transactions réalisées dans un environnement de test (sans remise en banque).
- MID de production: Permet d'accéder aux transactions réalisées dans un environnement de production (environnement LIVE).

Presentation du backoffice

Le back-office Axepta est une application web qui offre une vue d'ensemble et un contrôle sur toutes les transactions d'un commerçant. Le back-office est compatible avec la majorité des navigateurs web, il est recommandé d'utiliser les navigateurs Chrome et Firefox (Safari non disponible actuellement).

Il comporte 4 rubriques principales présentées ci-dessous et expliquées par la suite.

Le backoffice Axepta Online est multilingue (allemand, anglais, français, espagnol, italien, polonaise, danois, suédois et chinois).

L'URL pour accéder à cette application web est le suivant :

https://backoffice.axepta.bnpparibas/

Pour accéder au Backoffice, le commerçant recevra, lors de sa souscription à la solution, ses **données d'accès** personnelles via un mail dédié et chiffré pour des raisons de sécurité :

- Commerçant (Merchant ID)
- Nom d'utilisateur
- Mot de passe

Pour déchiffrer l'email, le commerçant devra utiliser le mot de passe reçu sur son téléphone portable (envoyé par le support client Axepta BNP Paribas).

Il pourra ensuite accéder à la page d'authentification suivante pour ouvrir une session :

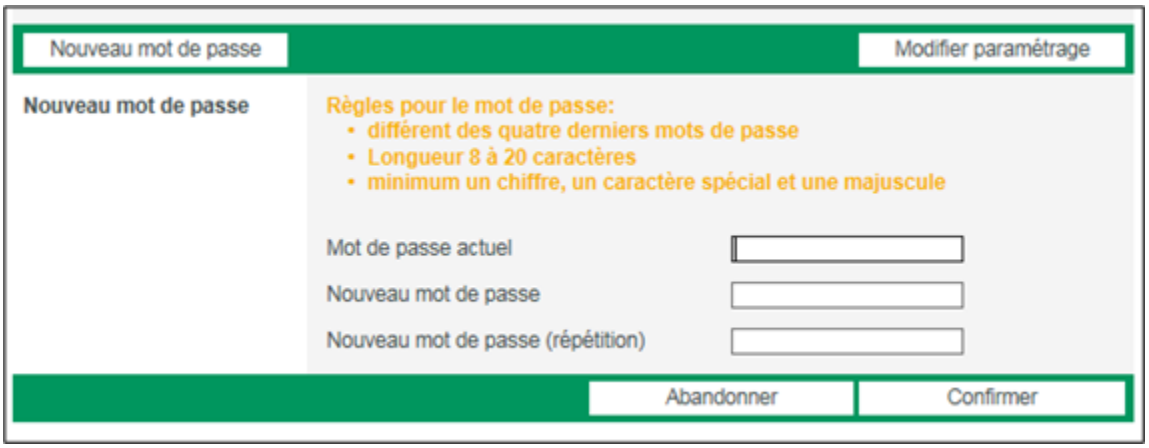
Il est obligatoire de changer le mot de passe attribué par BNP Paribas dès la première connexion, ensuite le mot de passe devra être changé toutes les **6 semaines** pour des raisons de sécurité.

Si le mot de passe expire au bout de 6 semaines, vous pouvez contacter le support de BNP Paribas.

Si l'utilisateur saisit un mot de passe incorrect plusieurs fois (7 fois), l'accès est automatiquement bloqué, il devra alors contacter le support de BNP Paribas.

Pour des raisons de sécurité, le mot de passe :

- Ne doit pas être utilisé plusieurs fois
- Doit comporter entre 8 et 20 caractères
- Contient au minimum un chiffre, un caractère spécial et une majuscule.



Gestion des transactions

La rubrique « Transactions » permet à l'utilisateur de visualiser et gérer toutes ses transactions.

Transactions

Lorsque le commerçant souhaite consulter ses transactions, il est possible de les filtrer selon différents critères :

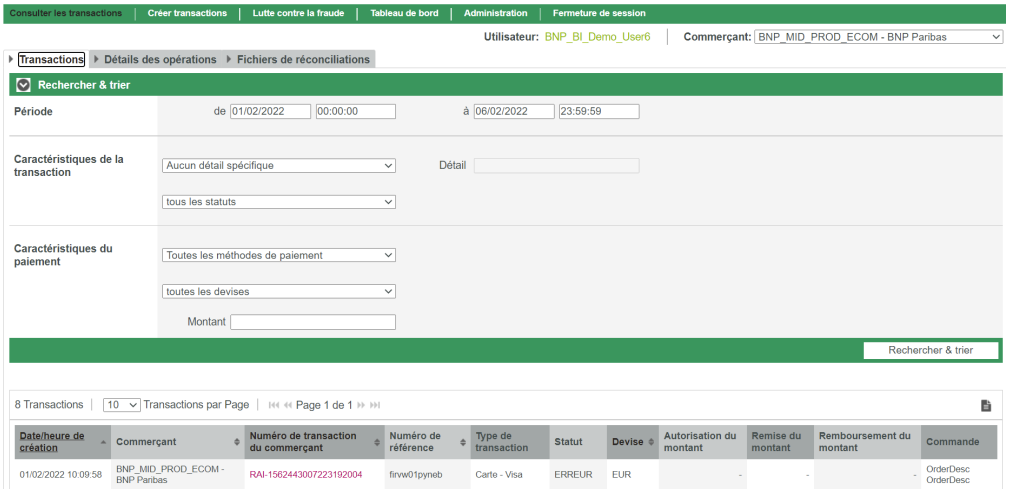
- Période qui correspond à la date de la transaction.
- Caractéristique d'une transaction (numéro de transaction défini par la solution de paiement, numéro de carte, token, numéro de contrat, IBAN, BIC, numéro de transaction défini par le commerçant, référence définie par le commerçant, code erreur...)
- Statut d'une transaction: Transaction confirmée, échouée, en attente.
- Moyen de paiement
- Devise utilisée
- Montant de la transaction acceptée (à saisir directement).

Le commerçant peut choisir de ne mettre aucun filtre, il verra alors uniquement les transactions du jour.

Résultats de la recherche :

La liste de toutes les transactions (filtrées ou non) s'affiche et les informations obtenues sont les suivantes :

- Date et heure de création de la transaction.
- Commerçant (MID)
- Numéro de transaction (défini par le commerçant)
- Numéro de référence (Référence d'archivage générée par le commerçant)
- Type de transaction (représente le moyen de paiement utilisé)
- Statut actuel de la transaction: Confirmé, en attente (de capture), Erreur.
- Devise de la transaction.
- Montant autorisé
- Montant remis en banque
- Montant remboursé le cas échéant
- Commande : représente la description de la commande.



<u>Vue détaillée d'une transaction :</u>

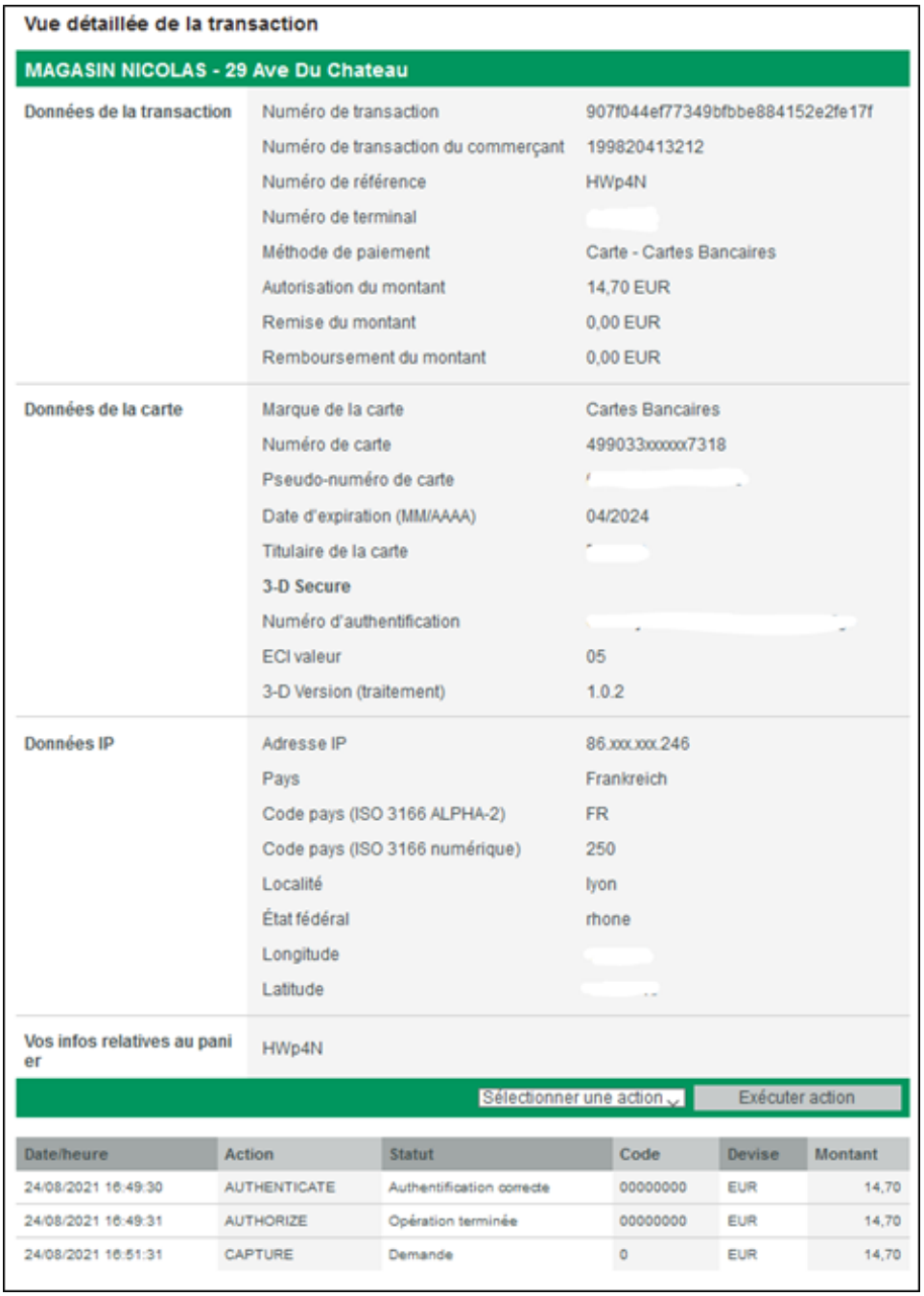
Pour voir les détails d'une transaction, il suffit de cliquer sur le numéro de transaction. Une fenêtre superposée apparaîtra avec le détail de celle-ci :

- Données de la transaction:
  - Numéro de la transaction (Identifiant généré par la solution Axepta)
  - Numéro de la transaction du commerçant (identifiant généré par le commerçant)
  - Numéro de référence (Référence d'archivage générée par le commerçant)
  - Numéro de terminal (représente le numéro de contrat monétique BNP Paribas)
  - Méthode de paiement
  - Montant autorisé
  - Montant remis à la banque
  - Montant remboursé le cas échéant.

- Données de la carte:
  - Marque de la carte
  - Numéro de la carte (tronqué)
  - Token (Pseudo Card Number)
  - Date d'expiration de la carte
  - Pays d'origine de la carte.
  - Données supplémentaires 3DS (numéro d'authentification, ECI valeur, Version du 3DS)

- Données IP:
  - Adresse IP (tronquée)
  - Pays
  - Code Pays (en lettres et en chiffres)
  - Localité
  - Etat fédéral
  - Longitude
  - Latitude

- Informations relatives au panier (description de la commande)
- Opérations effectuées sur cette transaction (autorisation, capture, remboursement…)



Vue détaillée de la transaction

MAGASIN NICOLAS - 29 Ave Du Chateau

Données de la transaction	Numéro de transaction	907f044ef77349bfbbe884152e2fe17f
	Numéro de transaction du commerçant	199820413212
	Numéro de référence	HWp4N
	Numéro de terminal	
	Méthode de paiement	Carte - Cartes Bancaires
	Autorisation du montant	14,70 EUR
	Remise du montant	0,00 EUR
	Remboursement du montant	0,00 EUR
Données de la carte	Marque de la carte	Cartes Bancaires
	Numéro de carte	499033xxxxxx7318
	Pseudo-numéro de carte	
	Date d'expiration (MM/AAAA)	04/2024
	Titulaire de la carte	
	3-D Secure	
	Numéro d'authentification	
	ECI valeur	05
	3-D Version (traitement)	1.0.2
Données IP	Adresse IP	86.xxx.xxx.246
	Pays	Frankreich
	Code pays (ISO 3166 ALPHA-2)	FR
	Code pays (ISO 3166 numérique)	250
	Localité	lyon
	État fédéral	rhone
	Longitude	
	Latitude	
Vos infos relatives au panier	HWp4N	

Sélectionner une action | Exécuter action

Date/heure	Action	Statut	Code	Devise	Montant
24/08/2021 16:49:30	AUTHENTICATE	Authentification correcte	00000000	EUR	14,70
24/08/2021 16:49:31	AUTHORIZE	Opération terminée	00000000	EUR	14,70
24/08/2021 16:51:31	CAPTURE	Demande	0	EUR	14,70

<u>Comment intérpréter le code retour d'une transaction :</u>

Un code retour est composé de 8 caractères et est construit de la manière suivante :

Format: **N8**, (**N NNNNNNN)**

- **N (status)**
- **NNN (categorie)**
- **NNNN (détails)**

Exemple :

2 206 0203

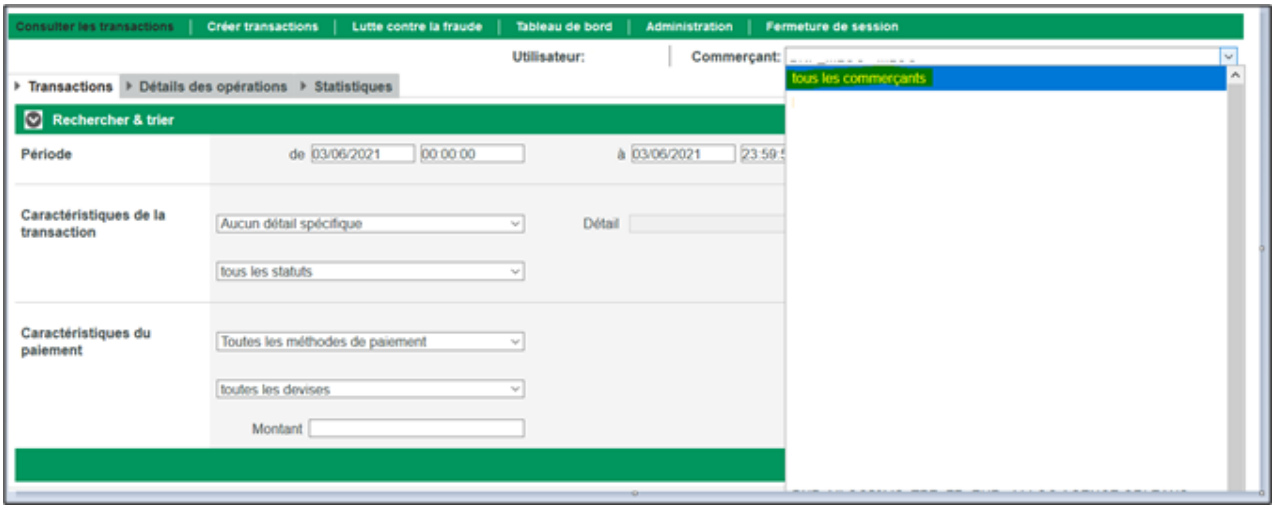
- **2** Error
- **206** 3DS credit card adapater for authorization protocol GICC
- **0203** Card brand does not support 3DS

La liste complète des codes retour est disponible via ce lien.

Vue globale des transactions de tous mes MIDs :

Pour afficher la liste complète des transactions lorsque le commerçant possède plusieurs boutiques, il suffit de s'authentifier avec les données d'accès du MasterMID (données reçues par le support AXEPTA lors de la souscription) et de sélectionner « tous les commerçants » dans la liste des MIDs.

A noter que le MasterMID ne peut pas être utilisé pour réaliser des transactions mais uniquement pour la visualisation de l'activité globale du commerçant.



Détails des opérations (remboursement, annulation, capture..)

Dans « détails des opérations », le commerçant aura une visibilité plus complète et plus détaillée sur ses transactions avec des colonnes en plus telles que :

- Action sur une transaction (authentification, autorisation, capture, remboursement…)
- Date de la dernière action sur la transaction
- Code retour
- Description du code retour

Action sur une transaction :

Le commerçant peut effectuer des opérations manuellement sur une transaction donnée, comme l'annulation, la capture, et le remboursement.

Selon le statut de la transaction et les droits de l'utilisateur connecté au back office, une liste d'opérations (actions) sera proposée telles que :

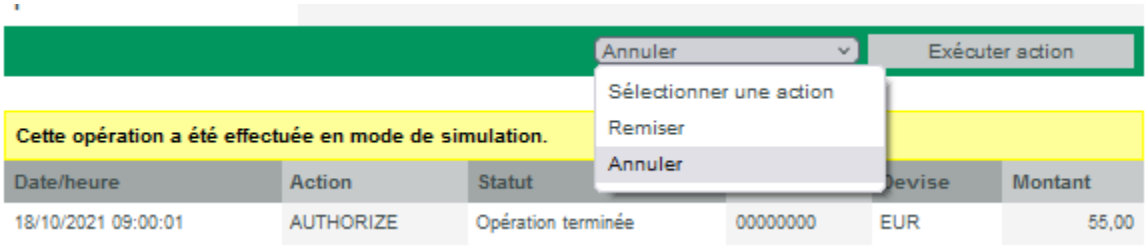
- **Le remboursement**

Pour rembourser un paiement, il suffit de sélectionner une transaction et de choisir l'action « Rembourser » et une fenêtre de saisie s'affiche pour saisir le montant du remboursement . Ce montant ne doit évidemment pas dépasser le montant du paiement. C'est le montant total qui est affiché par défaut, mais le commerçant peut décider de rembourser partiellement une transaction. Dans ce cas, il devra saisir le nouveau montant (inférieur au montant initial).

Pour tous les montants qui comportent des décimales, veuillez utiliser une virgule et non un point. Sinon le paiement sera automatiquement rejeté.

- **L'annulation**

Une transaction qui n'a pas encore été capture (remise en banque) peut-être annulée via le backoffice AXEPTA. Pour ce faire, il suffit de sélectionner une transaction et de choisir l'action « Annuler »



- **La capture manuelle : totale ou partielle**

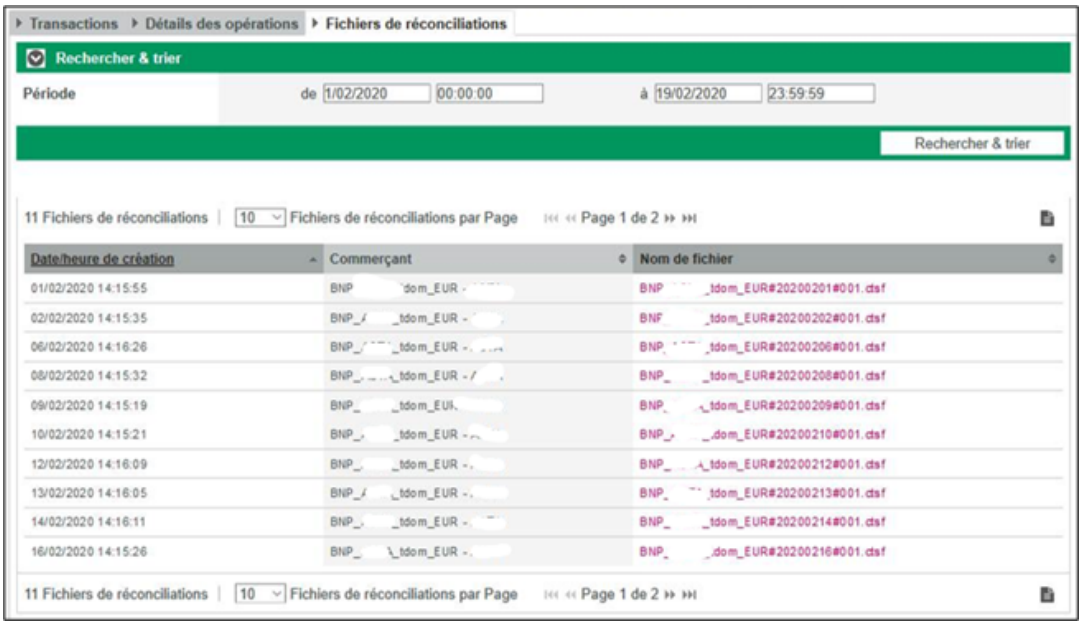
Pour capturer manuellement un montant, l'utilisateur devra saisir le montant à capturer (inférieur au montant total de la transaction) dans le champ « montant » et cliquer sur « Remiser » pour remettre la transaction en banque.

L'utilisateur peut également saisir un montant à capturer (inférieur au montant total de la transaction) dans le champ « montant » et cliquer sur « Remiser » pour remettre partiellement la transaction en banque.

Fichier de réconciliation (Settlement file)

Le fichier de réconciliation permet de répondre aux besoins des commerçants en matière de rapprochement bancaire. Il regroupe les données des différents prestataires de services de paiement ou organismes acquéreurs. Le fichier est disponible sur le backoffice sur demande et peut être téléchargé en format CSV (toutes les valeurs sont séparées par des virgules). Le fichier est généré quotidiennement (à 15h environs) tant qu'il n'est pas vide.

Le commerçant peut sélectionner une période spécifique (Jusqu'à 60 jours) dans la section « Fichier de réconciliations » pour filtrer les résultats.



Le contenu et la structure de ce fichier sont expliqués dans une documentation dédiée.

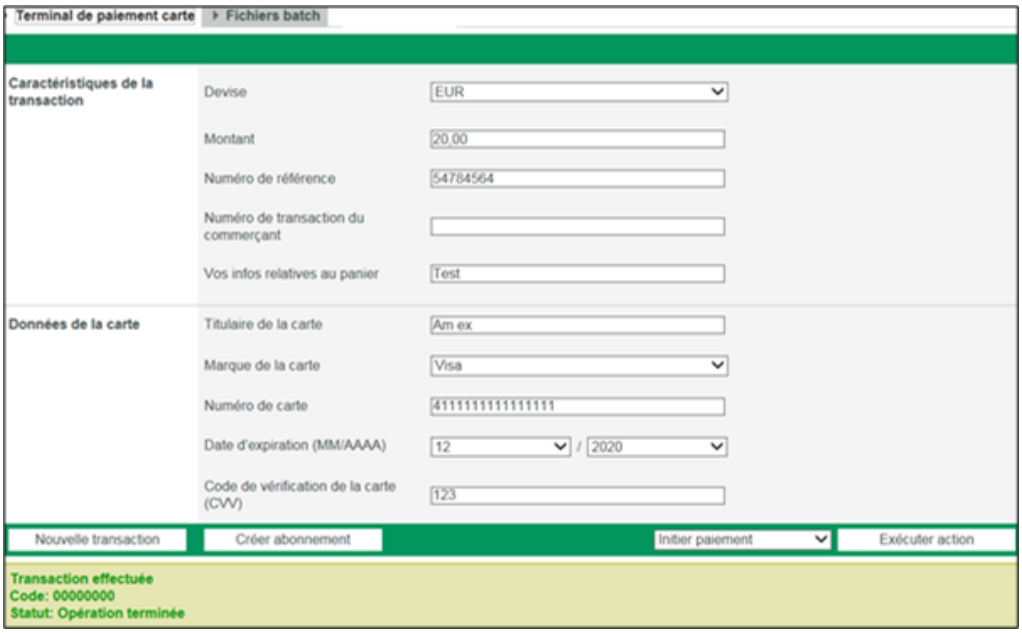
Création de transaction

Le commerçant a la possibilité de créer un paiement manuellement depuis son Back-Office (Mail Order Telephone Order = MoTo), il doit saisir les caractéristiques de la transaction :

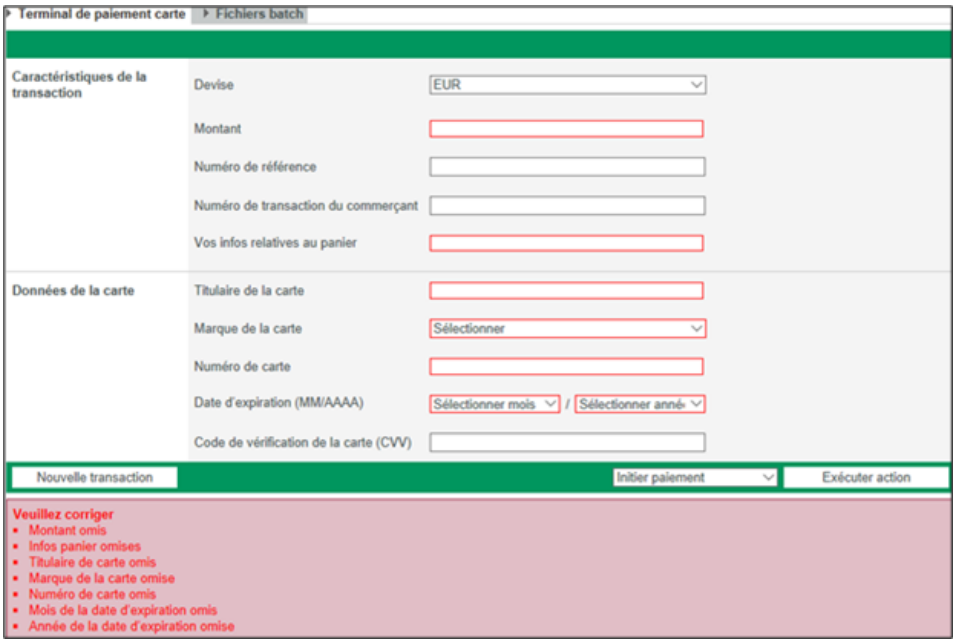
- Devise,
- Montant,
- Numéro de référence (permet d'identifier le paiement): 12 caractères alphanumériques max.
- Numéro de transaction (permet d'identifier la transaction): 64 caractères alphanumériques max.
- Informations sur le panier (description de la commande)
- Données de la carte : nom et prénom du titulaire de la carte, le numéro ou le PCNr (Pseudo card number), la marque et la date d'expiration de la carte, le CVV.

La création de paiement est possible avec les cartes uniquement (CB, Visa, MasterCard)

Pour concrétiser l'action, le commerçant clique sur « Initier paiement ».



Veuillez noter que certains champs sont obligatoires (champs en rouge ci-dessous).



Fichiers Batch

Il est possible de transmettre, manuellement, des transactions de paiement sous forme de fichiers.

Au cours de ce processus, Il faut :

- Saisir les données de transaction, telles que le numéro de carte, le montant et la devise, dans un **fichier de traitement en format CSV**
- Transmettre le fichier (via la fonction d'upload) dans la section dédiée du Back-Office
- La solution Axepta BNP Paribas exécute le paiement et enregistre le statut de la transaction dans le fichier de retour (qui sera transmis au commerçant).
- Après le traitement, le commerçant peut récupérer le fichier avec les détails sur le statut de la transaction et le télécharger.

La structure du fichier CSV à transférer est la même que pour un transfert automatique via FTP (se référer à la documentation technique).

Au niveau du backoffice, il suffit de se rendre sur la section « Créer transactions » puis « Fichiers Batch »

Tableau de bord

La rubrique « tableau de bord » permet au commerçant d'analyser ses transactions et d'évaluer ses performances afin d'améliorer son taux de conversion.

Le tableau de bord est composé de 5 sections :

- Chiffres clés
- Analyse des opérations
- Statut des transactions
- Analyse des tendances
- Analyse par pays

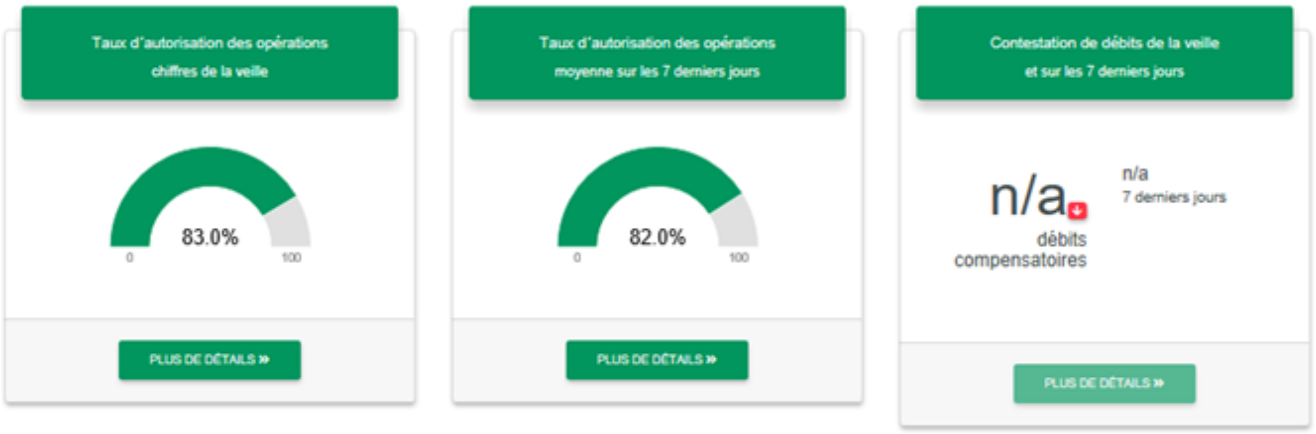
Chiffres clés

Les graphiques proposés dans cette section permettent de visualiser les indices de performance du commerçant (Key Performance Indicator = KPI).

Le commerçant peut suivre instantanément l'évolution du nombre de transactions et de son chiffre d'affaires en fonction des différents moyens de paiement qu'il propose.

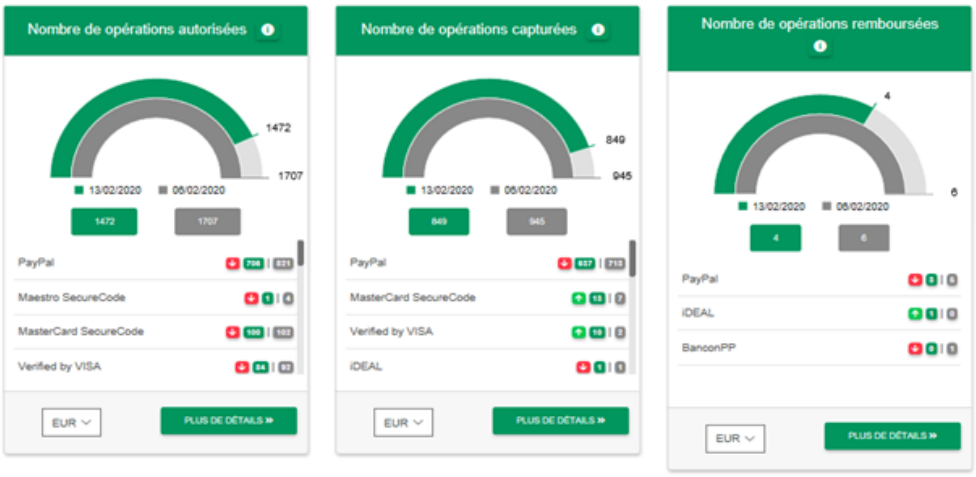
Le taux d'acceptation de la veille permet au commerçant de visualiser le taux de succès et le taux d'échec après chaque redirection de l'acheteur sur la page du moyen de paiement choisi. Ce taux se base sur l'ensemble des codes retour reçus par les différents moyens de paiement. Le taux d'acceptation est brut, c'est-à-dire que si un acheteur tente 2 fois successivement de faire un paiement et que ceux-ci sont en échecs, mais que la 3^{e} tentative est un succès, alors le taux d'acceptation du commerçant sera de 33% (un taux d'acceptation net aurait donné 100% de succès puisqu'il s'agit du même acheteur).

Le commerçant peut également visualiser le taux d'acceptation moyen sur les 7 derniers jours dans cette section ainsi que le nombre d'impayés (chargebacks) sur les 7 derniers jours.

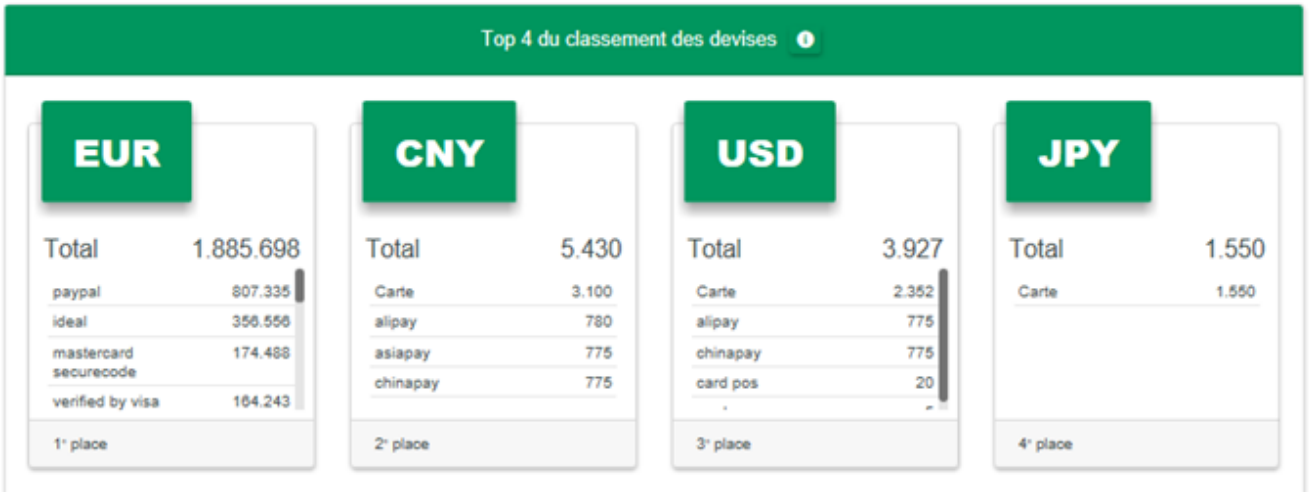


Les 3 graphiques suivants montrent la **performance de la veille** avec la répartition entre les différentes opérations (autorisées, capturées, remboursées) selon les moyens de paiement.

Par ailleurs, cette section établit un comparatif entre les opérations de la veille et celles réalisées le même jour de la semaine dernière. Cela permet de **visualiser la tendance** sur un même jour à une semaine d'intervalle (tendance à la hausse ou à la baisse) en ce qui concerne le nombre de transaction par moyen de paiement.



Le commerçant visualise le classement du **nombre de transactions par devise** et par **méthode de paiement.**



Le commerçant peut également consulter une vue d'ensemble de **l'origine géographique** de ses transactions dans une carte dynamique (possibilité de définir les critères de provenance : adresse IP et pays d'émission de la carte).

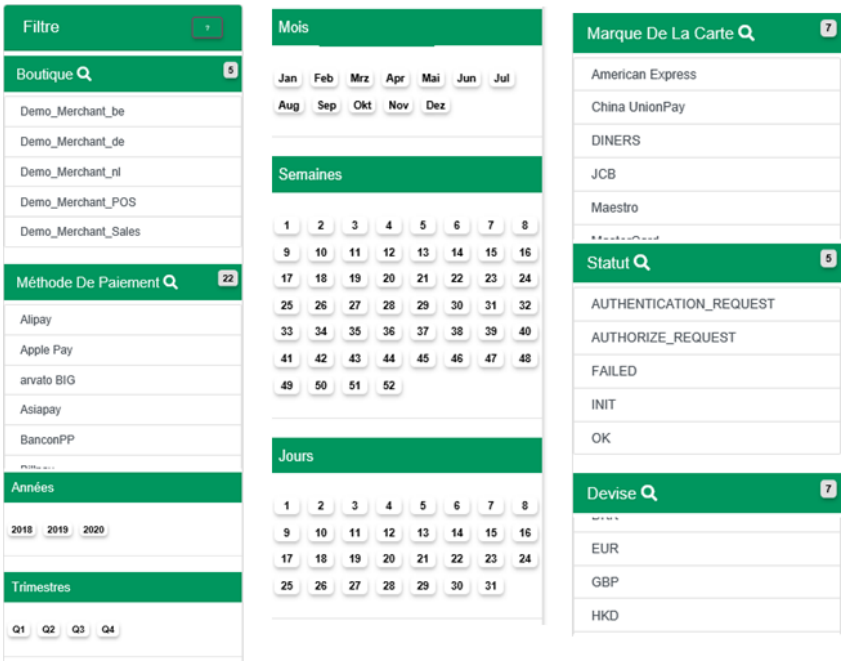
Analyse des operations

Cette section détaille la répartition des opérations du commerçant par méthode de paiement pour une devise donnée.

Le commerçant peut également appliquer un filtre ou exporter les données dans un fichier Excel.

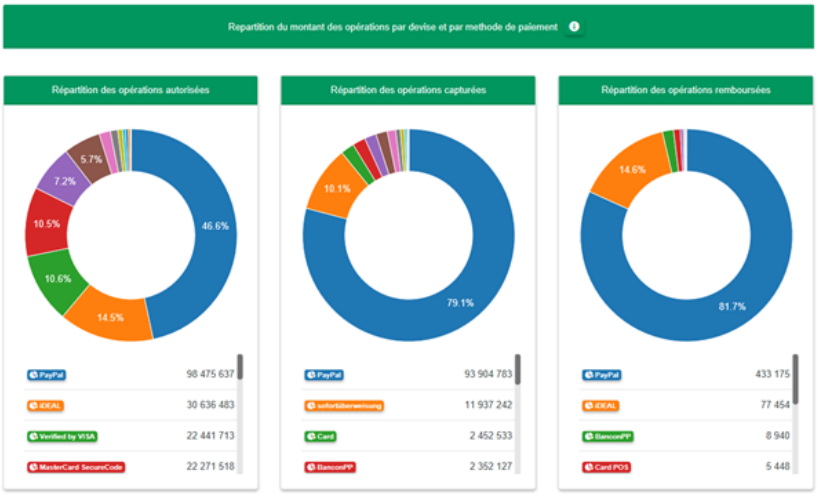
Filtres (applicables également pour les prochaines sections)

Des filtres sont mis à la disposition du commerçant pour affiner ses recherches et obtenir des résultats personnalisés.

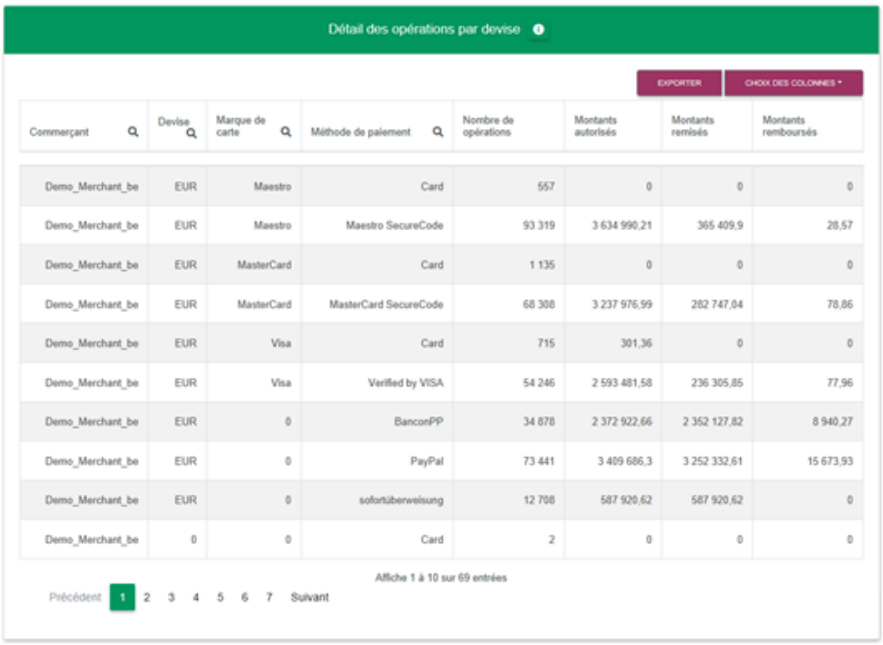


Répartition du nombre de transaction

La répartition du montant des opérations par devise et par méthode de paiement se présente comme suit :

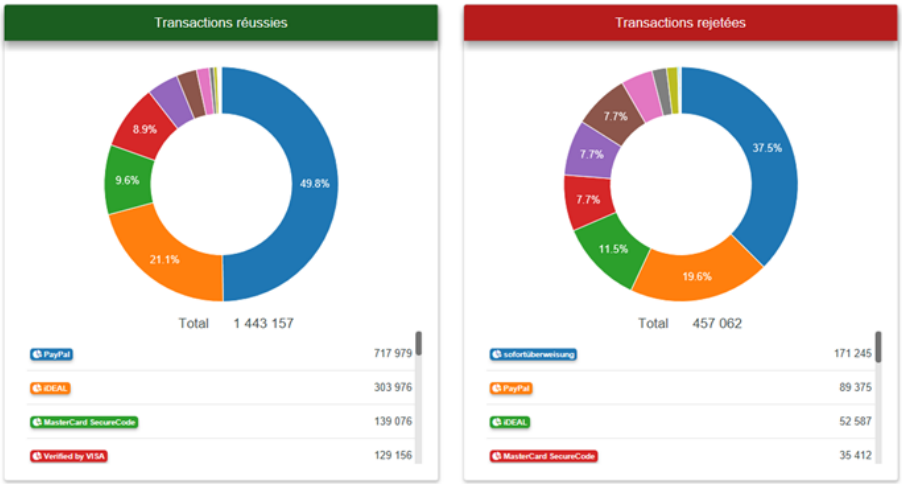


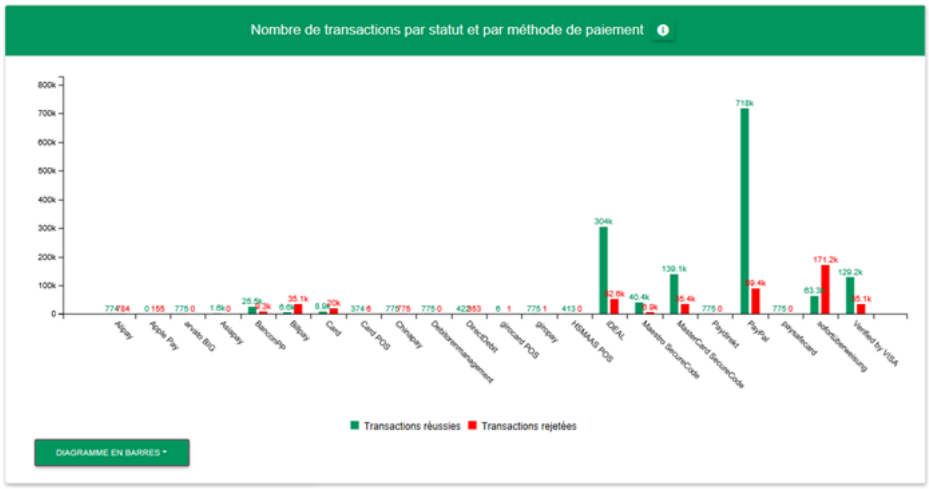
Pour consulter plus de détails sur les opérations, le commerçant peut choisir les colonnes des données qu'il souhaite visualiser et exporter le résultat obtenu.



Statut des transactions

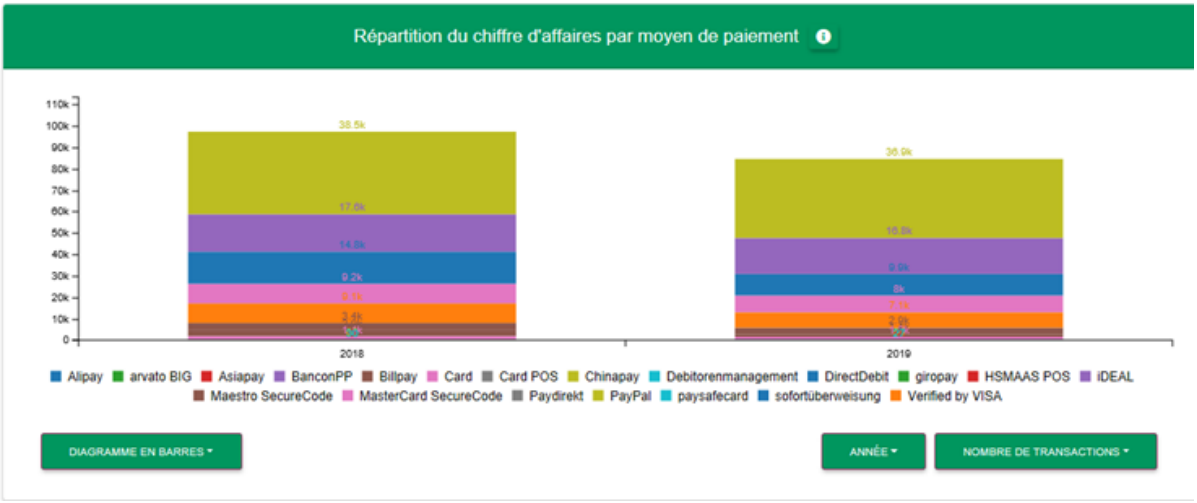
Cette section montre le nombre de transactions selon les statuts (succès / échec) et selon le moyen de paiement. Le commerçant peut également **ana lyser les rejets avec les codes retour associés** (time out/ invalid value/ invalid card/ amount mistmatch/ etc) et cela par transaction et par moyen de paiement.





Analyse des tendances

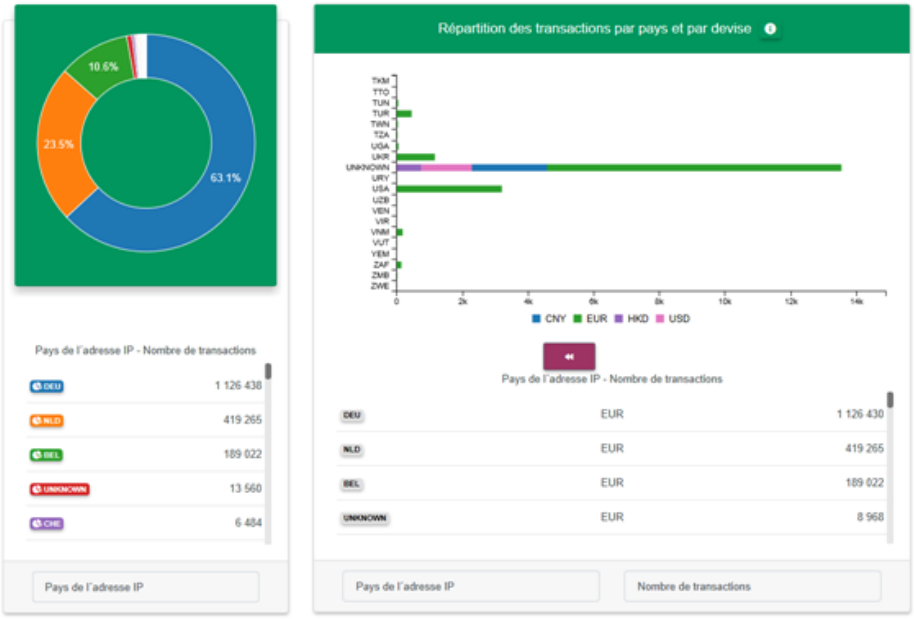
Cette vue d'ensemble montre une tendance dans le temps du **chiffre d'affaires par moyen de paiement** ou par **devise** sur une période donnée. Le commerçant peut utiliser les filtres placés sur la gauche pour affiner cette analyse.



Analyse par pays

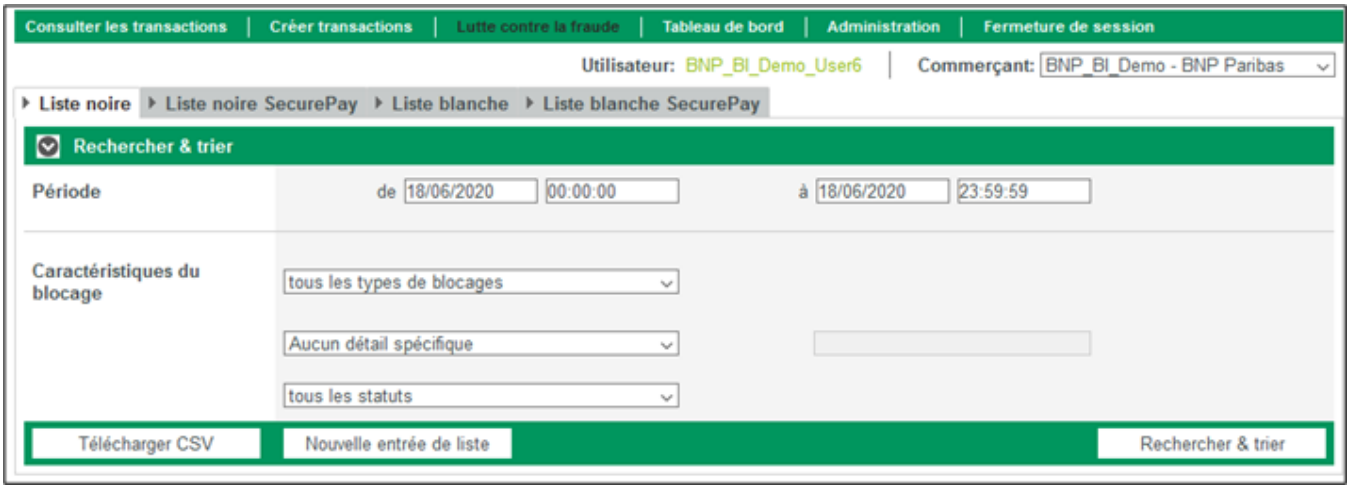
Cette section détaille la répartition des transactions du commerçant par pays et devise.

Le commerçant peut sélectionner un pays et une devise dans les filtres sous les diagrammes.



Lutte contre la Fraude

Le commerçant peut se rendre dans la rubrique « Lutte contre la fraude » dans le back-office pour gérer manuellement les listes noires et les listes blanches C'est-à-dire que la solution permet de bloquer les clients suspicieux (dans une liste noire) et de répertorier les clients de confiance (liste blanche).



Nous distinguons les listes dont les données sont alimentées manuellement par le commerçant et les listes générées automatiquement par la solution de paiement (appelées securePay dans le backoffice) selon les critères définis par le commerçant (règles anti-fraude).

Rappel des règles anti-fraude : (ces règles sont à définir lors de la phase de souscription) :

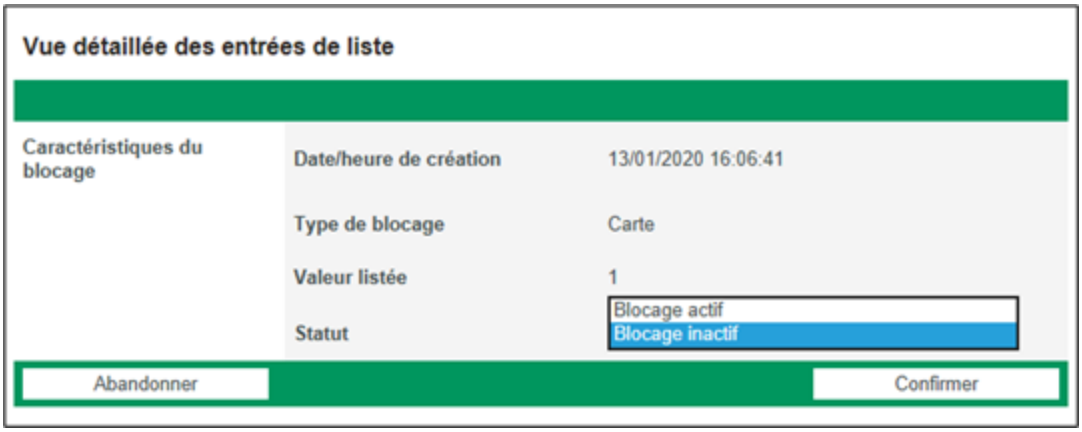
- Contrôle de l'origine de la carte utilisée par l'acheteur
- Contrôle de l'origine de l'adresse IP de l'acheteur
- Contrôle du nombre de transactions par carte sur une durée donnée
- Contrôle du nombre de cartes pour une même adresse IP sur une durée donnée
- Contrôle du montant d'opérations par adresse IP sur une durée donnée
- Contrôle du nombre d'adresses email par compte utilisateur sur une durée donnée
- Contrôle du nombre de transactions par adresse IP sur une durée donnée
- Contrôle de cohérence origine IP - origine Carte

	Liste noire/blanche	Liste noire/blanche SecurePay
Alimentation de la liste	· **Manuelle** par le commerçant.	· **Automatique** par la solution Axepta selon les critères prédéfinis par le commerçant (règles anti-fraude).
Action par le commerçant	· Ajout de numéro de carte, token (pseudo numéro de carte), IBAN, ID appareil… · Ajout d'un fichier CSV · Suppression d'une entrée de la liste · Consultation	· Consultation · Désactivation/Activation d'un blocage

Listes noires

Pour se protéger contre les paiements avec des cartes frauduleuses, le commerçant peut ajouter une nouvelle carte (token), un IBAN ou l'identifiant d'un appareil (device ID) à la liste noire pour empêcher le porteur d'effectuer une transaction.

Il peut également gérer manuellement cette liste en modifiant le statut d'un blocage d'une carte spécifique.

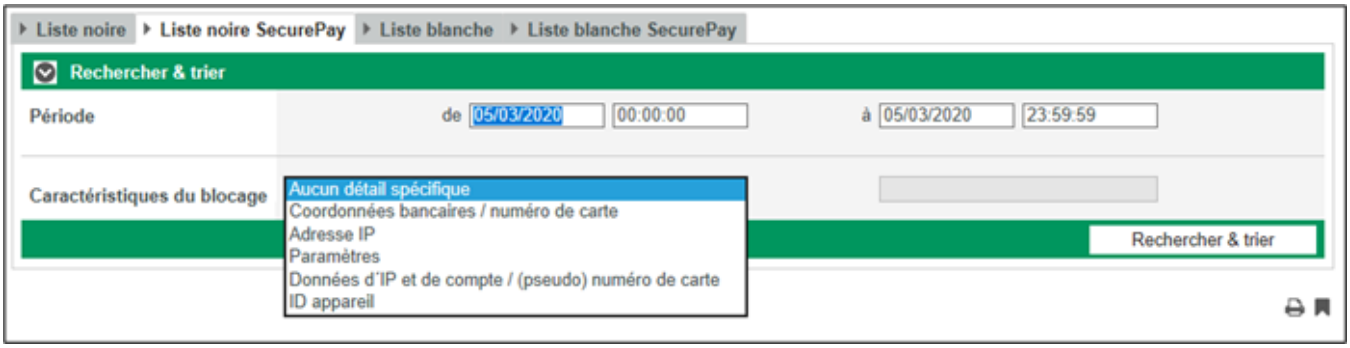


Il est également possible d'ajouter un fichier en CSV (fonction « upload ») contenant les données cartes à ajouter à la liste noire.

Listes noires SecurePay

La liste noire SecurePay est une liste noire temporaire générée par la solution de paiement selon des critères définis par le commerçant telle que la spécification d'un nombre maximal de transactions par jour avec la même carte de paiement ou bien depuis la même adresse IP. Lorsque ce nombre maximal est atteint, le numéro de carte ou l'adresse IP est automatiquement placée dans la liste noire securePay.

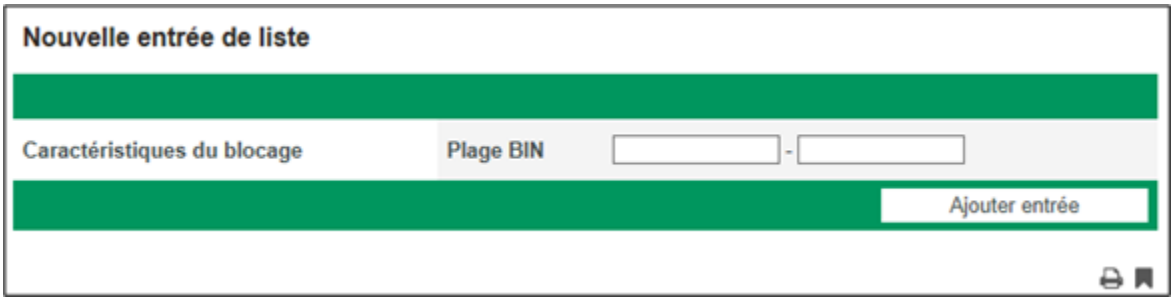
Le commerçant peut uniquement visualiser la liste complète et retirer une entrée s'il le souhaite. Il ne pourra donc pas y insérer des entrées.



Listes blanches

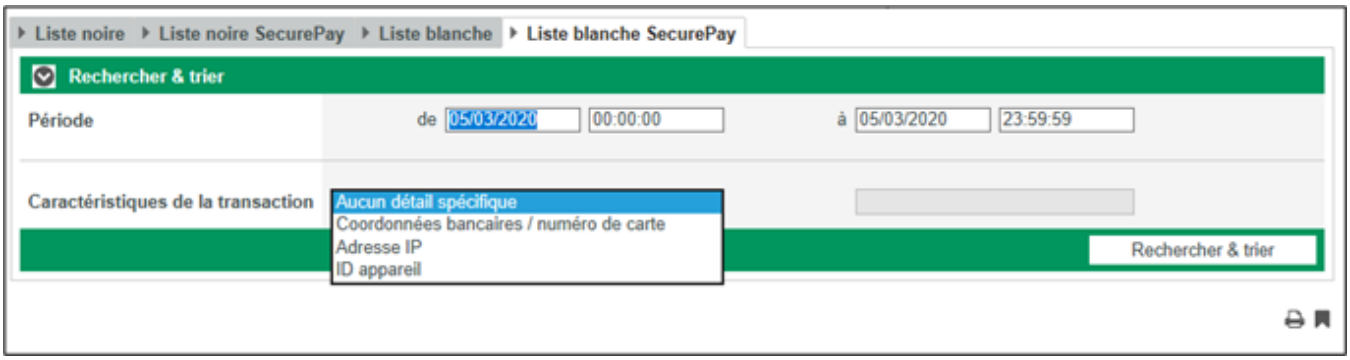
Le commerçant a la possibilité d'ajouter des BINs (Bank Identification Number) manuellement dans la liste. Le BIN permet de reconnaître la carte du client, son pays d'origine et sa banque émettrice. Les contrôles de fraude ne s'appliquent donc pas à des transactions dont les cartes figurent sur une liste blanche.

L'ajout d'une entrée se fait donc manuellement en saisissant uniquement une plage de BIN ou bien en remplissant un fichier CSV.



Listes blanches SecurePay

Le commerçant peut définir des critères (règles anti-fraude) permettant à des clients de ne pas être limités lors de leurs paiements. Les données de paiement liés à ces clients seront automatiquement ajoutées à la liste blanche SecurePay.



Gestion des utilisateurs

L’utilisateur qui recevra ses données d’accès au backoffice en premier lieu (super-administrateur) aura la charge de gérer les profils de ses collaborateurs en leur attribuant différents droits d’accès et des mots de passe.

L’administrateur principal peut ajouter autant d’utilisateurs qu’il le souhaite, modifier leurs informations, consulter la liste complète des utilisateurs et activer/désactiver le statut d’un utilisateur.

Il peut également tracer les activités des utilisateurs (sous forme de logs).

Les utilisateurs peuvent réaliser des opérations selon les droits qui leur sont attribués.

Les droits d’accès (divisés en groupes) :

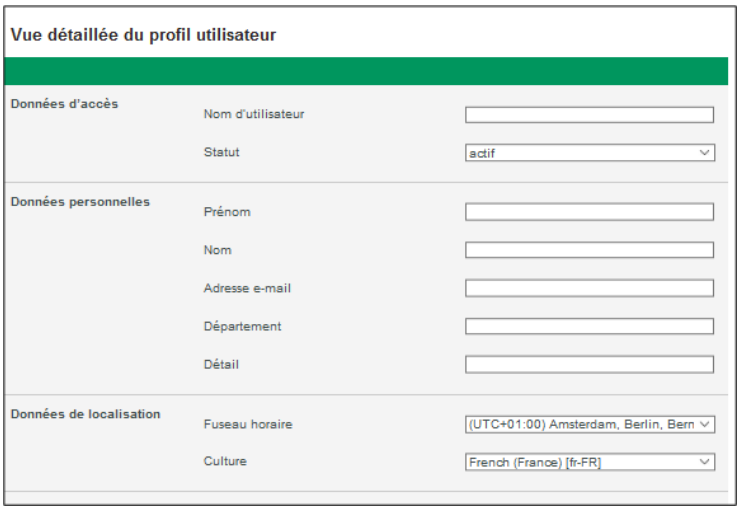
- **Visualisation**: Droit de visualiser certaines sections
- **Modification**: Droit d’exécuter des opérations (captures, annulations, remboursements)
- **Création** : Créer manuellement une transaction
- **Transfert de fichiers**: Droit de transférer des fichiers BATCH vers la solution de paiement ou de recevoir des fichiers de réconciliation
- **Prévention de la fraude**: Droit de gérer les listes blanches et les listes noires (ajouter/supprimer des entrées)
- **Administration**: Cette section doit être réservée à un seul utilisateur qui aura la charge de gérer les droits d’accès des utilisateurs et de tracer leurs activités.

Créer un nouvel utilisateur :

La création d’un nouvel utilisateur se fait au niveau de chaque MID. C’est-à-dire que pour que l’utilisateur puisse avoir un accès à l’ensemble des MIDs du commerçant, il faut effectuer la création au niveau du masterMID. Si l’utilisateur ne doit avoir accès qu’à un MID d’une entité en particulier, il faut se connecter au MID de l’entité en question et de suivre les étapes suivantes pour la création d’un utilisateur.

Pour ajouter un utilisateur, il suffit de se rendre à l’onglet « administration » du menu principal et de cliquer sur « Création nouveau profil utilisateur »

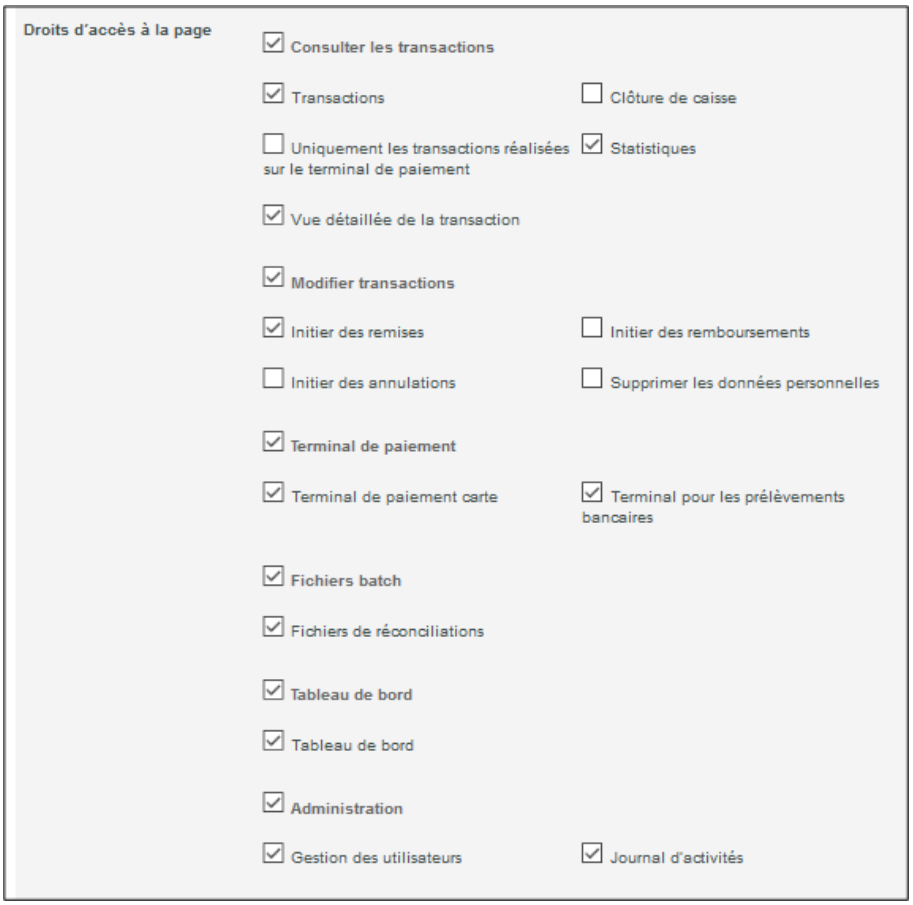
Une interface apparaitra et vous permettra de renseigner les informations liées à cet utilisateur :



Certaines informations comme le nom d'utilisateur, le nom, prénom, adresse e-mail sont obligatoires.

Ensuite il faudra renseigner les droits qui seront attribués à cet utilisateur :

- Consulter les transactions :
  - Transactions : Tableau contenant la liste complète des transactions
  - Clôture de caisse
  - Uniquement les transactions réalisées sur le terminal de paiement (transactions en MoTo : Mobile Order Telephone Order)
  - Statistiques : Nombre total de transactions par jour et par moyen de paiement.
  - Vue détaillée de la transaction : Plus d'informations sur les transactions en cliquant sur le numéro de transaction (telles que les données cartes).
- Modifier les transactions
  - Initier des remises : capturer des transactions (remise en banque)
  - Initier des remboursements
  - Initier des annulations
  - Supprimer les données personnelles
- Terminal de paiement
  - Terminal de paiement carte : créer une transaction par carte via l'outil
  - Terminal pour les prélèvements bancaires : créer une transaction par prélèvement via l'outil
- Fichiers batch : utiliser les fichiers batch pour les créations de transactions
- Fichiers de réconciliations : accèder aux données de réconciliations
- Tableau de bord : accéder aux KPI et aux chiffres et statistiques du commerçant
- Administration
  - Gestion des utilisateurs : ajouter, désactiver, modifier un utilisateur et lui attribuer des droits
  - Journal d'activités : accéder aux logs de l'activité des utilisateurs connectés au backoffice.

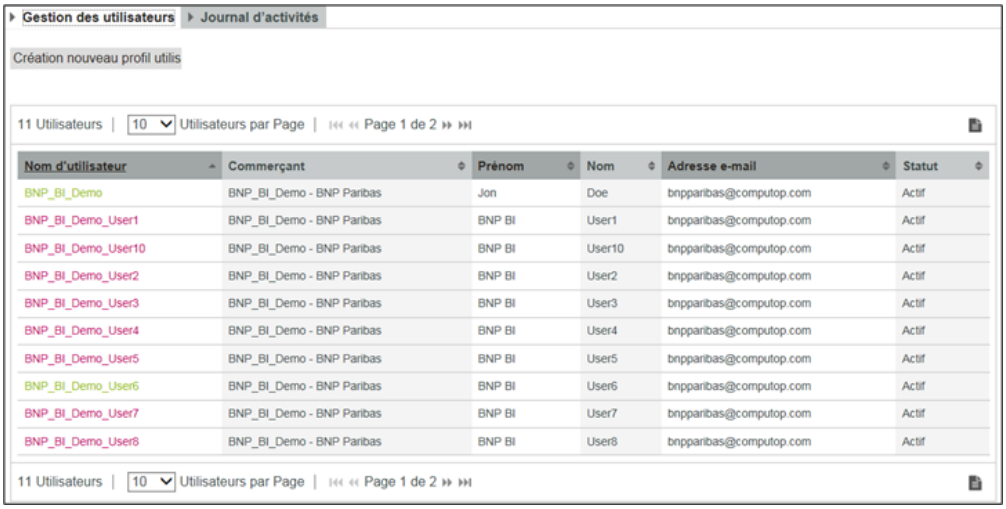


Et enfin, il faudra attribuer également un mot de passe à l'utilisateur qu'il vous faudra communiquer vous-même à la personne concernée.

Un mot de passe doit contenir une lettre majuscule, un caractère spécial, un chiffre et au moins 6 caractères au total.

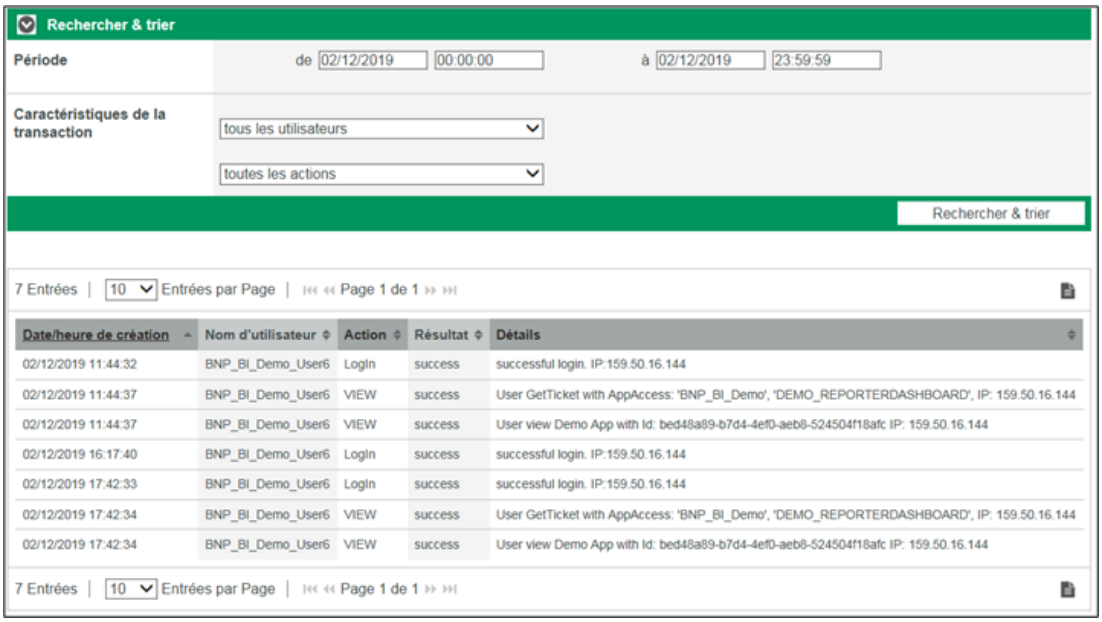
Consulter la liste des utilisateurs :

Il suffit de se rendre sur l'onglet « gestion des utilisateurs » pour visualiser la liste complète des utilisateurs. En cliquant sur le nom d'utilisateur d'un utilisateur, vous retrouverez les détails sur cet utilisateur et ses droits d'accès. Vous pouvez également télécharger ces informations sous forme d'un document CSV.



Consulter le Journal d’activités

Pour des raisons de sécurité, Visa et MasterCard demandent de tracer l’activité de chaque utilisateur qui accède aux données. Les informations archivées concernent tous les détails de l’activité de chaque utilisateur dans le back office.



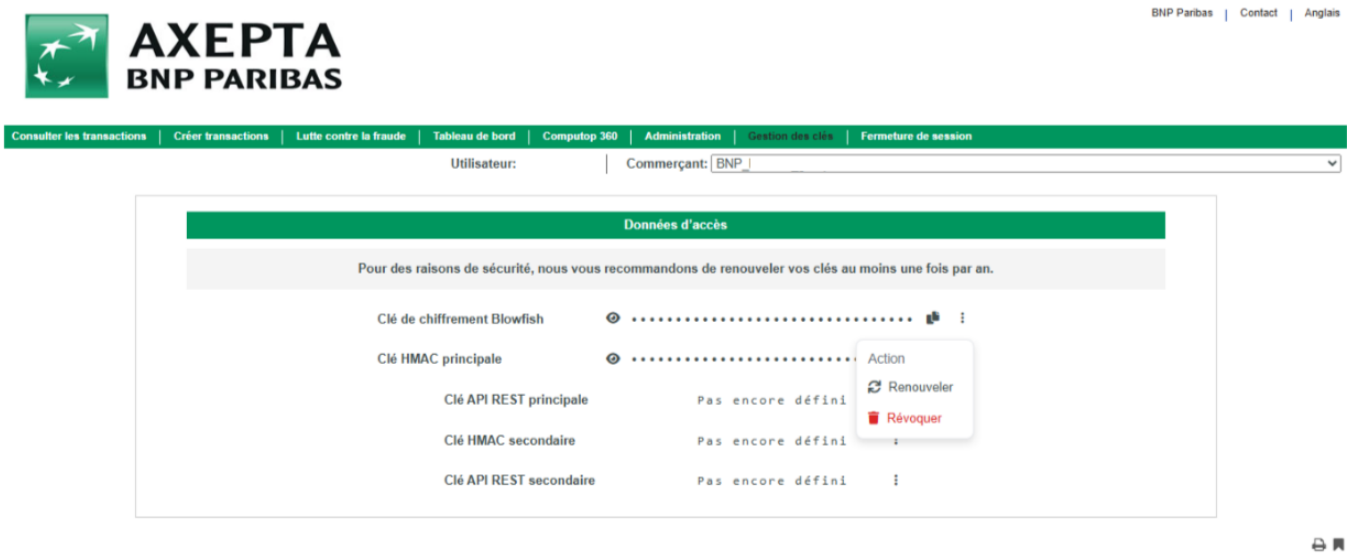
Gestion des clés

Cette section explique comment consulter, renouveler et révoquer les clés utilisées pour l’intégration technique de la solution Axepta Online BNP Paribas depuis le Backoffice.

La gestion des clés permet au commerçant ou à son intégrateur technique de sécuriser les échanges entre son système et la plateforme Axepta Online, notamment pour les appels API REST, les notifications serveur à serveur et, selon le mode d’intégration, les échanges utilisant les clés HMAC ou le mot de passe de cryptage.

Le renouvellement régulier des clés est recommandé pour des raisons de sécurité. Une rotation maîtrisée permet de remplacer les anciennes clés sans interruption de service.

Vue d’ensemble de l'onglet "Gestion des clés"



Données d'accès disponibles

La section **Données d'accès** contient les éléments techniques nécessaires à l'intégration.

Selon la configuration du compte, les éléments suivants peuvent être affichés :

Élément	Description	Usage principal
Clé de chiffrement Blowfish	Mot de passe utilisé dans certains modes d'intégration historiques ou spécifiques	Chiffrement ou sécurisation de certains échanges
Clé HMAC principale	Clé HMAC active principale	Signature ou vérification de messages
Clé API REST principale	Clé principale utilisée pour les appels API REST	Appels API REST en production ou en test
Clé HMAC secondaire	Clé HMAC secondaire	Rotation de clé ou double run
Clé API REST secondaire	Clé secondaire utilisée pour les appels API REST	Rotation de clé ou double run

Les valeurs des clés sont masquées par défaut. Une icône d'affichage permet de visualiser temporairement une clé si votre profil y est autorisé. Une icône de copie est également disponible pour copier la valeur dans le presse-papiers.

- **Icône d'affichage** : permet de révéler temporairement la valeur masquée de la clé.
- **Icône de copie** : permet de copier la clé dans le presse-papier pour une utilisation rapide.
- **Bouton de rafraîchissement** : Menu des actions sur les Clés.

Actions disponibles sur les clés

Chaque ligne de clé dispose d'un menu d'actions accessible via l'icône située à droite du champ concerné.

Les actions disponibles peuvent sont les suivantes :

Action	Description	Effet
Créer	Génère une clé lorsque le champ est vide	La nouvelle clé devient utilisable immédiatement
Renouveler	Génère une nouvelle valeur pour une clé existante	L'ancienne valeur est remplacée
Révoquer	Désactive et supprime la clé	La clé ne peut plus être utilisée

> **Attention**
>
> la révocation d'une clé est immédiate. Une fois révoquée, la clé ne doit plus être considérée comme utilisable.

Renouveler une clé API REST principale

Utilisez cette procédure lorsque vous souhaitez remplacer la clé API REST principale.

Étapes

1. Connectez-vous au Portail Marchand Axepta Online,
2. Accédez à la section **Gestion des clés**,
3. Vérifiez que le bon **Commerçant** est sélectionné (dans le cas d'une gestion multi-comptes (MIDs)),
4. Dans la section **Données d'accès**, identifiez la ligne **Clé API REST principale**,
5. Cliquez sur le menu d'actions situé à droite de la clé,
6. Sélectionnez **Renouveler la clé API REST principale**,
7. Confirmez l'action sur la page de confirmation qui s'affiche,
8. Affichez ou copiez la nouvelle clé,
9. Mettez à jour votre configuration avec la nouvelle clé,
10. Testez les appels API REST avec la nouvelle clé,
11. Vérifiez que les transactions ou opérations techniques attendues fonctionnent correctement.

Rotation sans interruption avec les clés secondaires

La solution Axepta Online BNP Paribas permet l'utilisation de deux jeux de clés en parallèle : une clé principale et une clé secondaire.

Ce fonctionnement est particulièrement utile pour effectuer une rotation de clés sans interruption de service.

Principe

La clé principale reste utilisée par le système existant pendant que la clé secondaire est créée ou renouvelée.
Le commerçant met ensuite à jour sa configuration pour utiliser la nouvelle clé secondaire.
Une fois la nouvelle clé validée, l'ancienne clé peut être révoquée ou renouvelée selon la stratégie définie.

Procédure recommandée

1. Vérifiez la clé actuellement utilisée dans votre configuration,
2. Créez ou renouvelez la clé secondaire,
3. Copiez la nouvelle clé secondaire dans un espace sécurisé,
4. Configurez votre application pour utiliser cette nouvelle clé,
5. Déployez la configuration,
6. Effectuez des tests techniques :
    - appel API REST simple,
    - création ou consultation d'une transaction,
    - vérification des notifications ou webhooks si applicables.
7. Lorsque la nouvelle clé est confirmée comme opérationnelle, révoquez l'ancienne clé devenue inutile.

Cette approche limite le risque d'interruption, car l'ancienne clé reste disponible pendant la phase de bascule.

Révoquer une clé API REST

La révocation désactive une clé existante. Elle doit être utilisée uniquement lorsque vous êtes certain que la clé n'est plus utilisée, ou lorsqu'une compromission est suspectée.

Étapes

1. Connectez-vous au Portail Marchand Axepta Online,
2. Accédez à **Gestion des clés**,
3. Sélectionnez le bon **Commerçant**,
4. Identifiez la clé à révoquer,
5. Cliquez sur le menu d'actions de la clé,
6. Sélectionnez **Révoquer**,
7. Confirmez l'opération sur la page de confirmation qui s'affiche,
8. Vérifiez dans l'historique que l'action a bien été enregistrée,
9. Contrôlez que vos applications n'utilisent plus cette clé.

Important : une clé révoquée ne doit plus être utilisée dans vos applications. Si l'application continue d'utiliser une clé révoquée, les appels API se concluront par des échecs.

Renouveler une clé HMAC

La clé HMAC est utilisée pour signer ou vérifier certains échanges techniques, notamment lorsque l'intégration repose sur des mécanismes de signature.

Étapes

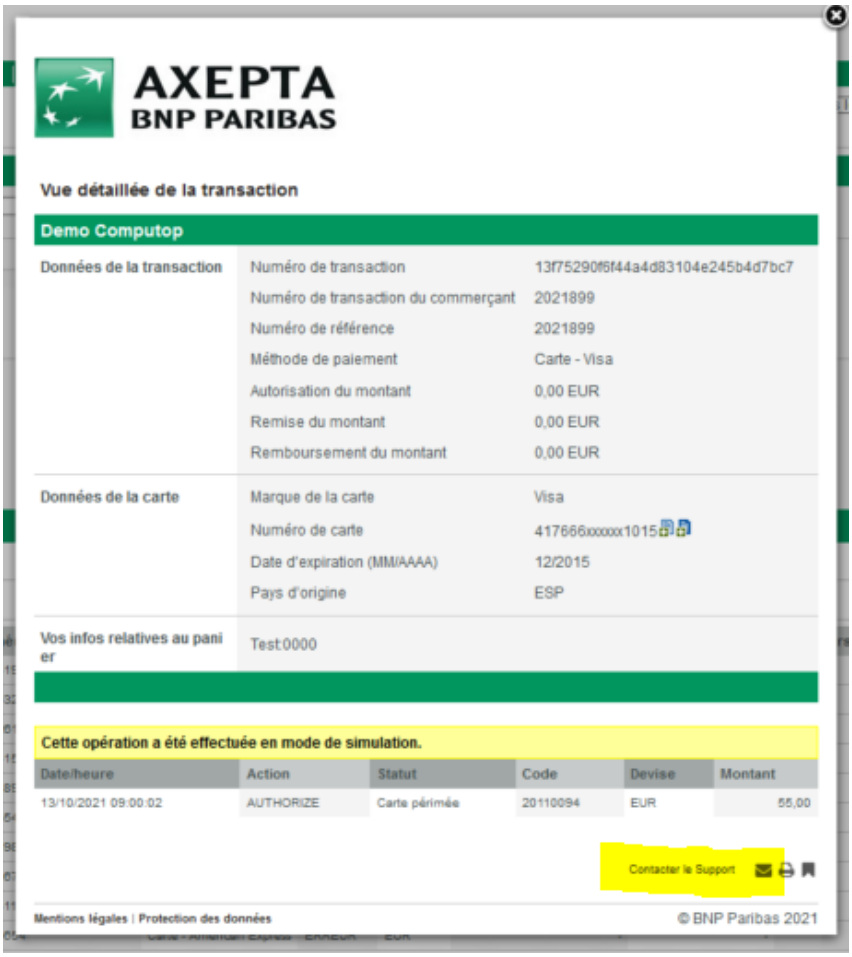
1. Accédez à la section **Gestion des clés**,
2. Identifiez la clé **HMAC principale** ou **HMAC secondaire**,
3. Ouvrez le menu d'actions,
4. Sélectionnez l'action de renouvellement,
5. Copiez la nouvelle valeur dans un espace sécurisé,
6. Mettez à jour la configuration de votre application,
7. Vérifiez que les signatures générées ou vérifiées par votre système restent valides.

Contacter le Support technique

Si vous rencontrez un problème en utilisant le backoffice AXEPTA, vous pouvez contacter le Support technique soit directement par mail (bnpparibas @computop.com) soit en cliquant sur le bouton "Contact" en haut à droite de la page.

Un formulaire de contact apparaîtra et vous pourrez expliquer le problème. N'oubliez pas de mentionner votre "MID" (Merchant ID).

Si vous rencontrez un problème relatif à une transaction spécifique (transaction échouée pour une raison quelconque..), vous pouvez cliquer sur l'icône de contact dans le popup du détail d'une transaction, en bas à droite, vous serez alors redirigé directement vers votre messagerie électronique en incluant le numéro de la transaction dans l'objet du message. Le numéro de transaction est une donnée primordiale pour le Support technique pour effectuer une analyse sur l'échec d'une transaction.



AXEPTA
BNP PARIBAS

Vue détaillée de la transaction

Demo Computop

Données de la transaction	Numéro de transaction	13f75290f6f44a4d83104e245b4d7bc7
	Numéro de transaction du commerçant	2021899
	Numéro de référence	2021899
	Méthode de paiement	Carte - Visa
	Autorisation du montant	0,00 EUR
	Remise du montant	0,00 EUR
	Remboursement du montant	0,00 EUR
Données de la carte	Marque de la carte	Visa
	Numéro de carte	417666xxxxxx1015
	Date d'expiration (MM/AAAA)	12/2015
	Pays d'origine	ESP
Vos infos relatives au panier	Test:0000	

Cette opération a été effectuée en mode de simulation.

Date/heure	Action	Statut	Code	Devise	Montant
13/10/2021 09:00:02	AUTHORIZE	Carte périmée	20110094	EUR	55,00

Contacter le Support

Mentions légales | Protection des données

© BNP Paribas 2021

À	bnpparibas@computop.com;
Cc	
Objet	BNP Paribas - Back Office - operationdetails.aspx - Numéro de transaction: 13f75290f6f44a4d83104e245b4d7bc7