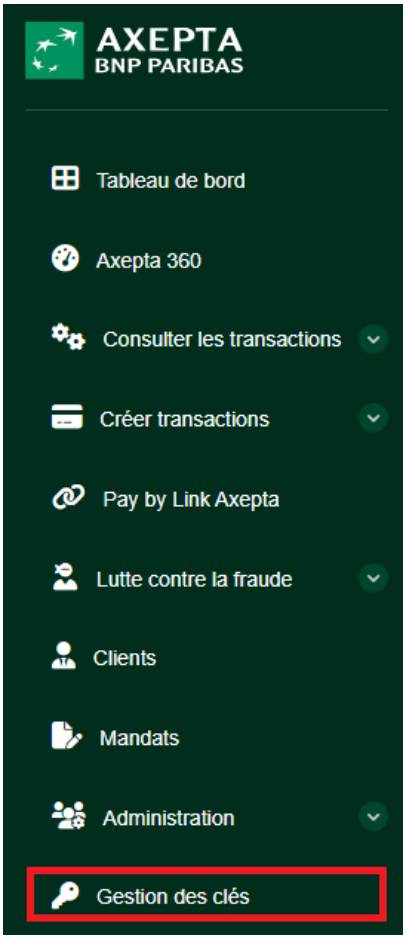
Gestion des clés

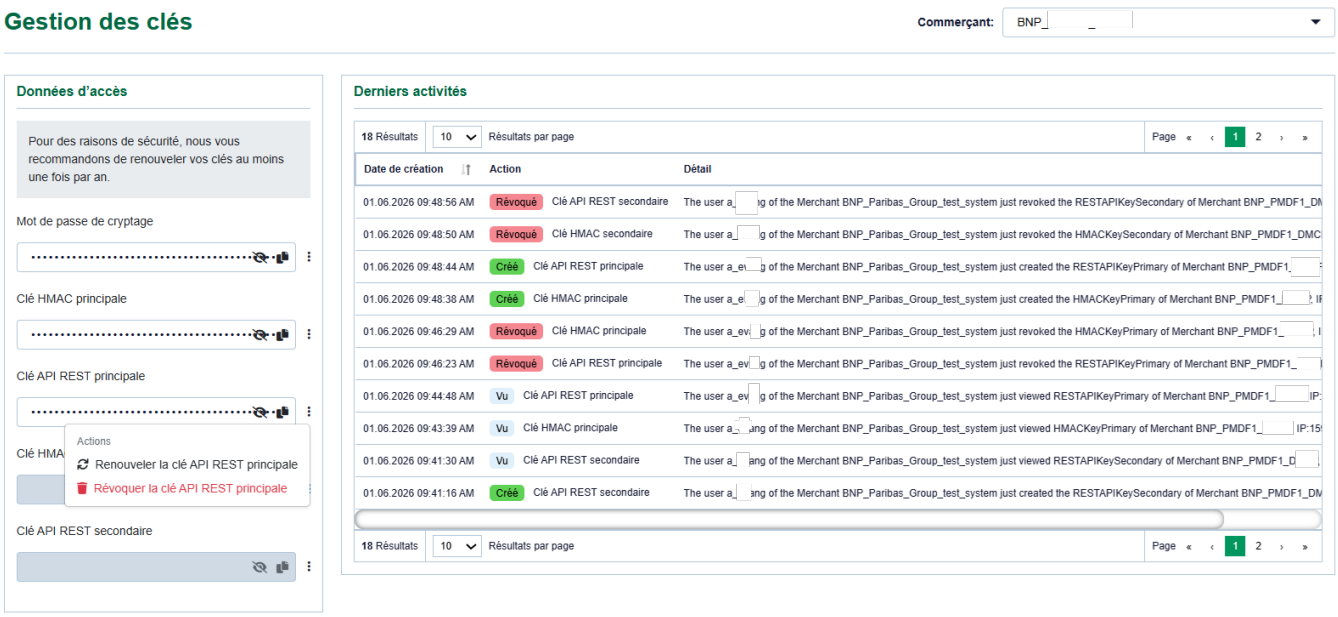
Cette page explique comment consulter, renouveler et révoquer les clés utilisées pour l'intégration technique de la solution Axepta Online BNP Paribas depuis le Portail Marchand.

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"



Accès à la page de gestion des clés

Depuis le Portail Marchand Axepta Online, accédez à la section **Gestion des clés**. La page affiche les informations suivantes :

- le commerçant sélectionné,
- les données d'accès disponibles,
- les clés principales et secondaires,
- les actions possibles sur chaque clé,
- l'historique des dernières activités.

Remarque : selon votre profil utilisateur, la section de gestion des clés peut ne pas être visible.

> **Sélection du commerçant**
>
> En haut à droite de l'écran, le champ **Commerçant** permet de sélectionner le compte marchand concerné (dans le cas d'une gestion multi-comptes (MIDs)).
>
> Avant toute opération, vérifiez que le bon commerçant est sélectionné.
> Les clés affichées et les actions réalisées s'appliquent uniquement au commerçant sélectionné.

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
Mot de passe de cryptage	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.

Historique des dernières activités

La section **Dernières activités** affiche les opérations réalisées sur les clés.

Elle permet notamment de consulter :

- la date de création ou d’action,
- le type d’action réalisée,
- la clé concernée,
- le détail de l’opération,
- l’utilisateur ayant réalisé l’action,
- le commerçant concerné.

Cette section est utile pour le suivi d’audit, la traçabilité et l’analyse en cas d’incident.

Exemples d’actions visibles :

- consultation d’une clé,
- renouvellement d’une clé,
- révocation d’une clé,
- consultation du mot de passe de cryptage.

Export et sécurité

- Les clés ne sont pas exportables en fichier,
- Pour des raisons de sécurité, elles sont affichées de manière masquée par défaut.