

# Mise à disposition du fichier de réconciliation via sFTP

Axepta Online propose un [reporting quotidien de réconciliation \(Settlement File\)](#).

Le fichier de réconciliation ( Settlement File ) regroupe l'ensemble des données des différents moyens de paiement utilisés par le commerçant afin de répondre à ses besoins en matière de rapprochement et de reporting. Les informations de compensation (clearing) et de règlement (settlement) sont récupérées auprès des différents prestataires de services de paiement et acquéreurs.

Le fichier se présente dans un format CSV (Comma Separated Values – valeurs séparées par des virgules).

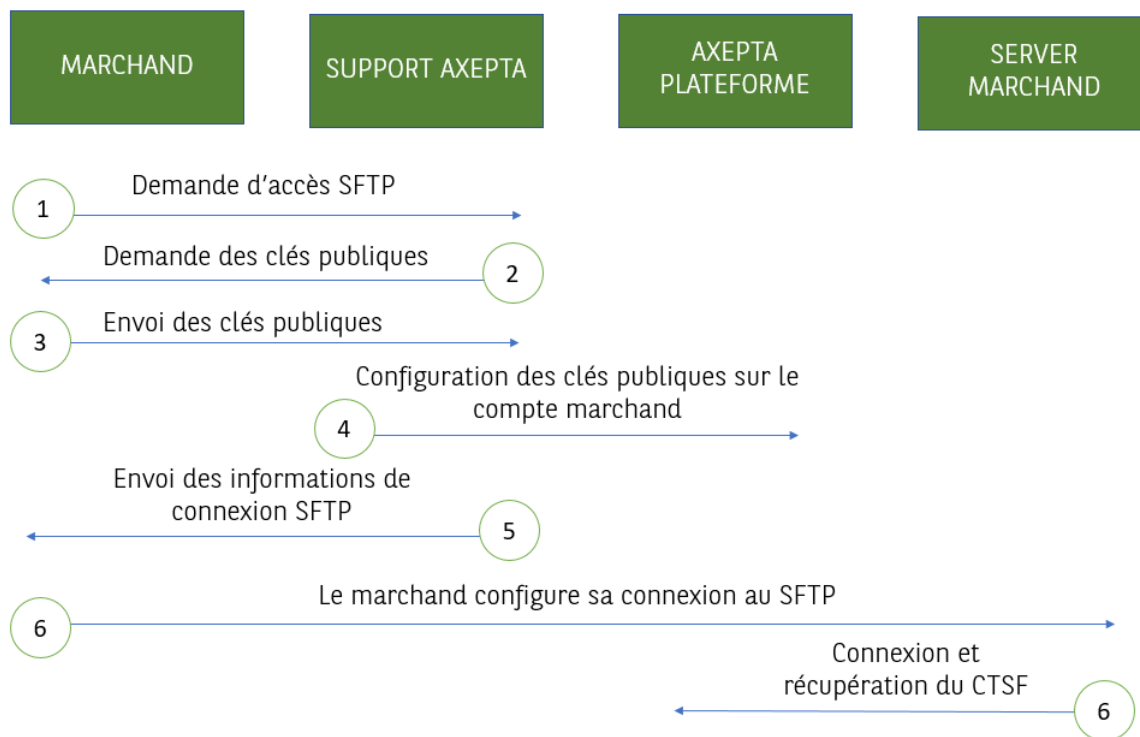
Cette documentation explique pas à pas les étapes permettant de récupérer le fichier de réconciliation ( Settlement File ) lorsque celui-ci est mis à disposition sur un sFTP Axepta.



Cette méthode de récupération de fichier nécessite la génération de paires de clés SSH et PGP qui seront utilisées pour :

- La mise en place d'une connexion sécurisée entre le système d'information du marchand et le serveur de sFTP Axepta
- Le décryptage du fichier de réconciliation généré par Axepta

## Étapes de mise en place



1. Le Marchand contacte le Support Axepta afin de demander la mise à disposition du fichier de réconciliation via sFTP
2. Le Support Axepta contacte le Marchand et lui demande d'envoyer ses clés publiques SSH et PGP
3. Le Marchand crée ses paires de clés SSH et PGP. Il transmet uniquement ses clés publiques au Support Axepta
4. Le Support Axepta effectue la configuration appropriée
5. Le Support Axepta envoie au Marchand les données de connexion au sFTP Axepta
6. Le Marchand établit la connexion entre son système d'information et le sFTP Axepta, procède à la récupération du fichier crypté et le décrypte

# Description détaillée de chaque étape

## Étape 1: Demande de mise à disposition du fichier de réconciliation via sFTP

La demande de mise à disposition du fichier de réconciliation via sFTP est transmise par mail au Support Axepta.



Pour plus de détails : [Contacter l'Assistance Axepta BNP Paribas](#)

## Étape 2 : Demande d'envoi des clés publiques SSH et PGP

En réponse le Support Axepta contacte le marchand par mail afin que celui-ci lui transmette ses clés publiques SSH et PGP.

Ce mail contient également la clé publique Axepta Online qui sera utilisée uniquement dans le cas où le marchand souhaite effectuer des opérations via Batch.



### Exemple de template de demande de clé publique emise par le Support Axepta

*Veillez noter les informations suivantes afin de mettre en place la mise à disposition des fichiers de réconciliation par sFTP :*

- *Veillez trouver notre clé publique en pièce jointe.*
- *Merci de bien vouloir nous fournir votre clé publique PGP en format .asc (avec une longueur RSA d'au moins 4096 Bit).*
- *Veillez nous envoyer une clé SSH publique en format .ssh (la commande pour la création d'une clé SSH se présente comme suit : `ssh-keygen -b 4096 -t rsa`).*

*Il est nécessaire d'attribuer une adresse e-mail à votre clé PGP publique car elle fera office d'identifiant.*

*Nous vous recommandons de ne pas utiliser une adresse e-mail privée mais bien une adresse e-mail du domaine de l'entreprise.*

*Nous compléterons la configuration de votre compte et vous enverrons vos données d'accès par e-mail après réception de vos données.*

## Étape 3 : Génération des paires de clés SSH et PGP et envoi au support

### Étape 3.1 : Génération des paires de clés

Le Marchand (son intégrateur ou son service informatique) génère des paires de clés SSH et PGP.

Les systèmes SSH et PGP utilisent des modes de cryptage dit asymétrique se caractérisant par l'utilisation d'une paire de clés.

Cette paire est composée :

- d'une clé de chiffrement appelée clé publique
- d'une clé de déchiffrement appelée clé privée

#### Utilisation des clés

- Les clés SSH sont utilisées pour sécuriser les échanges (inc. authentification) entre le système d'information du marchand et le serveur sFTP Axepta
- Les clés PGP sont utilisées pour crypter et décrypter le fichier de réconciliation

#### Prérequis:

- La commande pour la création d'une clé SSH se présente comme suit : `ssh-keygen -b 4096 -t rsa`.
- La clé PGP doit avoir une longueur RSA d'au moins 4096 Bit.
- La clé PGP doit être en format .asc

### Étape 3.2 : Envoi au support

Le marchand envoie ses clés publiques SSH et PGP au Support Axepta, en précisant son MID.

 Pour plus de détails : [Contacter l'Assistance Axepta BNP Paribas](#)

## Étape 4 et 5 : Configuration par le Support Axepta

Le Support Axepta configure les clés publiques SSH et PGP fournies par le marchand sur la plateforme Axepta.

Une fois cette opération terminée, un mail de confirmation contenant les identifiants de connexion au server Axepta est envoyé au marchand.

#### Exemple de retour mail :

*La clé publique SSH a été configurée*

*La configuration de votre compte SFTP est finalisée. Dorénavant, vous pouvez télécharger vos fichiers de réconciliation à l'aide des informations suivantes.*

- Nom d'utilisateur : `bnp_"nom du MID"_batch`
- Répertoire : `/paygate/"nom du MID"`
- URL : `"nom du MID"@xxxxxx.axepta.bnpparibas`

## Étape 6 : Connexion au sFTP et récupération du fichier de réconciliation

Le Marchand (son intégrateur ou son service informatique) met en place la connexion entre son système d'information et le serveur Axepta.

Une fois la connexion établie, le fichier de réconciliation peut quotidiennement être récupéré à partir de 15h.

Le fichier peut être décrypté (grâce à la clé privée PGP) et intégré dans les outils du Marchand.



Les fichiers seront automatiquement supprimés du serveur sFTP Axepta après 14 jours.

Le fichier de réconciliation est généré uniquement lorsque des transactions sont effectuées.