VOS SERVICES AU QUOTIDIEN
PSD2 – API Documentation

Introduction

La Directive sur les services de paiement, ou PSD2, requiert que les institutions financières détenant les comptes de paiement des utilisateurs de services de paiement donnent accès aux comptes à différents prestataires de services de paiement tiers (TPPs) sous condition qu'ils aient l'accord explicite du client en question.

Ces prestataires de services de paiement peuvent fournir les services suivants :

- **Service d'accès aux comptes** : un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement ;

- **Service d'initiation de paiement** : un service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement;

- **Services d'information sur la disponibilité des fonds** : un service consistant en la confirmation immédiate que le montant nécessaire à l'exécution d'une opération de paiement liée à une carte est disponible sur le compte de paiement du payeur.

Afin de permettre à ces prestataires de services de paiement de fournir ces trois types de services, les institutions détenant les comptes de ces derniers mettent en place des interfaces de communication que l'on appelle plus couramment API pour Application Programming Interface.

POST Finance utilise les services de LUXHUB pour permettre aux TPPs d'accéder aux informations de ses clients qui sont nécessaires à la prestation de service d'information des comptes et d'initiation de paiement. LUXHUB est une initiative commune de POST Finance, BCEE, BGL BNP Paribas et Banque Raiffeisen qui a pour but d'accompagner les différentes parties prenantes pour faire face aux défis et opportunités de la PSD2.

Ce document a pour but de décrire les spécifications techniques des API utilisées par POST Finance afin de permettre aux TPPs de fournir des services d'initiation et d'accès aux comptes à ses clients.

Délais

L'accès aux API se fera en deux temps :

À partir de mi-mars, les TPPs auront accès à un environnement de test qui leur permettra de tester leurs connections avec les différents API au moyen de messages test qui ne contiennent aucune données sensibles. Cet environnement de test est ce que l'on appelle la Sandbox.

À partir de mi-juin, les TPPs pourront fournir des services d'accès aux comptes et d'initiation de paiement aux utilisateurs de services de paiement de POST Finance. Les données échangées seront les données réelles des utilisateurs de services de paiement mais seules les données qui sont essentielles à la prestation du service seront communiquées aux TPPs.

Qui peut avoir accès aux comptes et pour quels services ?

Seuls les TPPs ayant une licence d'une autorité compétente d'un état membre de l'Union Européenne peuvent utiliser les APIs de POST Finance. Afin de s'identifier auprès de POST Finance, les TPPs doivent détenir un certificat électronique qualifié eIDAS qui spécifie à quels types d'information ils peuvent avoir accès. Un registre des certificats, *l'Open Banking Europe directory*, est tenu par PRETA, une filiale d'EBA Clearing. LUXHUB a signé un accord avec PRETA pour qu'il puisse accéder à ce registre et gérer une copie Luxembourgeoise de celui-ci.

Le tableau ci-dessous résume à quelles informations les institutions financières autorisées peuvent avoir accès :

	Licence d'AISP	Licence de PISP	Licence bancaire	Licence d'émission de carte (CBPII)
Service d'initiation de paiement		✓	✓	
Accès aux balances des comptes	✓		✓	
Accès à l'historique des transactions	✓		✓	
Certificat de disponibilité des fonds				✓

Comment fonctionne l'API

- **Onboarding**

Les TPPs qui veulent avoir accès aux informations de paiement des clients de POST Finance doivent être connectés et autorisés via LUXHUB.

Les TPPs souhaitant utiliser l'API LUXHUB pour servir les clients de POST Finance peuvent créer un compte et s'authentifier via ce portail. L'ensemble de la gestion des TPPs se fera via LUXHUB et non via POST Finance.

- **Autorisation**

Les comptes des clients de POST Finance sont protégés contre les accès non-autorisés. Les TPPs doivent s'authentifier via l'Oauth2.0 et avoir l'autorisation du client afin d'accéder aux informations de ceux-ci auprès de POST Finance.

- **Aspect technique**

Les APIs POST Finance qui sont mis à disposition par LUXHUB sont basées sur le modèle et standard de la version 1.3 du NextGenPSD2 Framework du Berlin Group.

Les APIs sont du type REST et communiquent via des messages au standard JSON. Le modèle utilisé pour l'authentification par les API de LUXHUB pour accéder à POST Finance est le suivant :

– Redirect SCA Approach

Il y a trois types de messages HTTP qui peuvent être utilisés via les API :

POST Ce type de message est envoyé pour demander à une entité d'ajouter une nouvelle ressource

GET Ce type de message est envoyé pour accéder à une ressource (sans aucune modification)

DELETE Ce type de message est envoyé pour supprimer des ressources

Quelles sont les différentes APIs disponible ?

- **Payment Initiation Services (PIS)**

Cette API permet aux PISP d'initier et de modifier une requête de paiement ainsi que d'obtenir des informations sur le statut du paiement initié. Ils peuvent entre autres le faire via les requêtes suivantes :

- Requête d'initiation de paiement [POST]
- Obtenir des informations de paiement [GET]
- Obtenir le statut du SCA (authentification forte) de l'autorisation de paiement [GET]
- Obtenir le statut du SCA de l'autorisation de l'annulation d'un paiement [GET]
- Obtenir le statut de la requête d'initiation de paiement [GET]

- **Confirmation of Funds Services**

Cette API permet aux émetteurs de cartes (CBPII) de demander un statut aux ASPSP quant à la disponibilité des fonds sur le compte lié à la carte bancaire dans le cadre de l'initiation d'un paiement par le client en question. L'ASPSP communiquera la disponibilité des fonds via un message très simplifié qui prendra la forme d'un « oui » ou d'un « non ». La seule requête disponible est la suivante :

- Confirmation de la requête sur les fonds [POST]

- **Account Information Services**

Cette API permet aux AISP d'obtenir des informations sur le(s) compte(s) du client. Les informations disponibles, sous condition de la réception du consentement explicite, sont les suivantes :

- Rapport de transactions pour un compte donné ;
- Solde d'un compte donné ;
- Une liste des comptes disponibles ;
- Détails d'un compte donné.

Ce service peut être rendu, entre autres, via les requêtes suivantes :

- Obtenir la liste des comptes avec ou sans solde suivant le consentement obtenu par le TPP [GET]
- Obtenir les détails, dont le solde, d'un compte donné [GET]
- Obtenir la liste ou rapport des transactions pour un compte donné [GET]
- Créer le consentement pour les droits d'accès à un compte donné [POST]
- Supprimer le consentement pour des accès spécifiques [DELETE]
- Obtenir le statut du consentement pour l'accès aux informations de compte [GET]

Glossaire

AISP	Account Information Service Provider / Prestataire de service d'accès aux comptes
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider / Prestataire de services de paiement gestionnaire du compte
Berlin Group	Le Berlin group est une institution qui développe des standards techniques qui se concentrent sur les détails techniques et les exigences opérationnelles
CBPII	Card-based payment instrument issuer / Émetteur de carte de paiement
Certificat eIDAS	Les certificats eIDAS sont des certificats permettant l'identification électronique et la confidentialité des échanges. eIDAS se réfère au règlement (Règlement (UE) n°910/2014) du même nom.
PISP	Payment Initiation Service Provider / Prestataire de service d'initiation de paiement
PSD2	Revised Payment Service Directive / Seconde Directive sur les Services de Paiement est une Directive européenne qui est entrée en vigueur en janvier 2018 et qui régule les services de paiements.
SCA	Strong Customer Authentication / Authentification forte est une authentification qui repose sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification
TPP	Third Party Provider / Prestataire de service de paiement tiers