YOUR DAY-TO-DAY SERVICES

PSD2 – API Documentation

Introduction

The Payment Services Directive, or PSD2, requires Account Servicing Payment Service Providers (ASPSP) holding payment service accounts of payment service users (PSUs) to provide access to accounts to different third-party payment providers (TPPs), provided they have the explicit consent of a given client.

Payment services providers may provide the following services:

- **Account Access Services**: An online service that provides consolidated information about one or more payment accounts held by a PSU, either from another payment services provider or from more than one payment services provider;

- **Payment initiation services**: consist in initiating a payment order at the request of a PSU regarding a payment account held with another payment services provider;

- **Funds availability information services**: consists in providing immediate confirmation that the amount required to complete a card-related payment transaction is available in a payer's payment account.

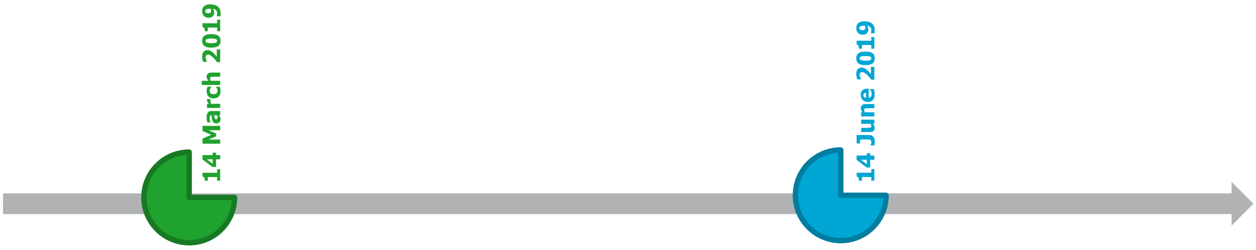
To provide these three types of services, the institutions holding payment service accounts set up communication interfaces that are more commonly known as APIs, or Application Programming Interfaces.

POST Finance uses the services of LUXHUB to enable TPPs to access necessary customer information in providing account information and payment initiation services. LUXHUB is a joint initiative of POST Finance, BCEE, BGL BNP Paribas and Banque Raiffeisen intended to support the various stakeholders in facing the challenges and opportunities of the PSD2 directive.

The purpose of this document is to describe the API technical specifications used by POST Finance to enable TPPs to provide account initiation and access services to its clients.

Timeline

API access will be rolled out in two phases:



From mid-March, TPPs can access a test environment that will allow them to test their connections to different APIs by means of test messages that contain no sensitive data. This test environment is known as Sandbox.

From mid-June, TPPs will be able to provide account access and payment initiation services to POST Finance. Whilst actual data of PSUs will be exchanged, it will only be data that is essential to providing services that will be submitted to the TPPs.

Who can access the accounts and for which services?

Only TPPs with a license from a competent authority of a member state of the European Union can use POST Finance APIs. In order to register with POST Finance, TPPs must have an eIDAS electronic certificate that specifies the types of information they can access. A certificate register, the Open Banking Europe directory, is maintained by PRETA, a subsidiary of EBA Clearing. LUXHUB has signed an agreement with PRETA so that it can access and manage a Luxembourg copy of this register.

The table below summarizes what information authorised financial institutions can access:

	AISP License	PISP License	Banking license	CBPII Card Issuer license
Payment Initiation Services		✓	✓	
Access to account balances	✓		✓	
Access to transaction histories	✓		✓	
Certificate of funds availability				✓

How APIs work

- **Onboarding**

TPPs who want access to POST Finance customer payment information must be logged in and authorised via LUXHUB.

TPPs wishing to use the LUXHUB API to serve POST Finance customers can create an account and authenticate via this portal. All management processes concerning TPPs will be accomplished via LUXHUB and not via POST Finance.

- **Authorisation**

POST Finance customer accounts are protected against unauthorised access. All TPPs must authenticate via Oauth2.0 and have obtained customer authorisation to access the information in these accounts through POST Finance.

- **Technical**

POST Finance APIs that are made available by LUXHUB are based on the model and standards of Version 1.3 of NextGenPSD2 Framework of the Berlin Group.

APIs are of the REST type and communicate via standard JSON messages. The model used for authentication by LUXHUB APIs to access POST Finance is the following:

– Redirect SCA Approach

There are three types of HTTP messages that can be used via APIs:

POST	This type of message is sent to ask an entity to add a new resource
GET	This type of message is sent to access a resource (without modification)
DELETE	This type of message is sent to delete resources

What types of API are available?

- **Payment Initiation Services (PIS)**

This API enables PIS providers to initiate and modify a payment request and to obtain information on the status of the payment initiated. They can achieve this via the following queries:

- Payment initiation request [POST]
- Get Payment Information [GET]
- Obtain SCA (strong authentication) status of a payment authorisation [GET]
- Obtain SCA status for an authorisation to cancel a payment [GET]
- Obtain the status of a payment initiation request [GET]

- **Confirmation of Funds Services**

This API allows Card Issuers (CBPII) to request ASPSP status for the availability of funds on account-lined bank cards when a given customer’s payment initiation process begins. The ASPSP will communicate the availability of funds via a very simplified message as either a "yes" or a "no". The only available query is:

- Confirmation of a funds enquiry [POST]

- **Account Information Services**

This API allows account information service providers (AISPs) to obtain information regarding customer accounts. The following information may be obtained, contingent upon obtaining explicit consent:

- Transaction reports for a given account;
- Balance of a given account;
- A list of available accounts;
- Details of a given account.

This and other services can be rendered via the following queries:

- Obtain the list of accounts with or without balances, once consent has been obtained by a TPP [GET]
- Obtain details relating to a given account, including the balance [GET]
- Obtain a list or report of transactions for a given account [GET]
- Create consent for access rights to a given account [POST]
- Delete consent for specific access [DELETE]
- Obtain the status of consent for access to account information [GET]

Glossary

AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
Berlin Group	The Berlin group is an institution that develops standards focusing on technical details and operational requirements
CBPII	Card-based Payment Instrument Issuer
eIDAS certificate	eIDAS certificates are certificates for electronic identification and confidentiality of exchanges. eIDAS refers to EU Regulation 910/2014 of the same name.
PISP	Payment Initiation Service Provider
PSD2	Revised Payment Service Directive is a European Directive that came into force in January 2018 and regulates payment services.
SCA	Strong Customer Authentication is an authentication that relies on the use of two or more items belonging to independent "knowledge" (something that only a user knows), "possession" (something that only a user has), and "inheritance" (something that a user is) categories, in as much as the compromise of one does not call into question the reliability any of the others. This process is meant to protect the confidentiality of authentication data
TPP	Third Party Provider