



## IHRE DIENSTE FÜR DEN ALLTAG

### PSD2 – API-Dokumentation

#### Einleitung

Die überarbeitete Richtlinie über Zahlungsdienste (Payment Services Directive - PSD2) erfordert, dass Finanzinstitute, die Zahlungskonten von Zahlungsdienstnutzern führen, verschiedenen dritten Zahlungsdienstleistern (Third-Party Payment Service Provider - TPP) Zugriff auf Konten gewähren, sofern diese über die ausdrückliche Genehmigung des betreffenden Kunden verfügen.

Diese Zahlungsdienstleister können die nachstehenden Dienste erbringen:

- **Kontozugriffsdienst:** Ein Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten des Zahlungsdienstnutzers bei einem oder mehreren anderen Zahlungsdienstleistern.
- **Zahlungsauslösedienst:** Ein Dienst, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst.
- **Informationsdienste über die Verfügbarkeit von Geldbeträgen:** Ein Dienst, der unverzüglich bestätigt, ob ein für die Ausführung eines kartengebundenen Zahlungsvorgangs erforderlicher Betrag auf dem Zahlungskonto des Zahlers verfügbar ist.

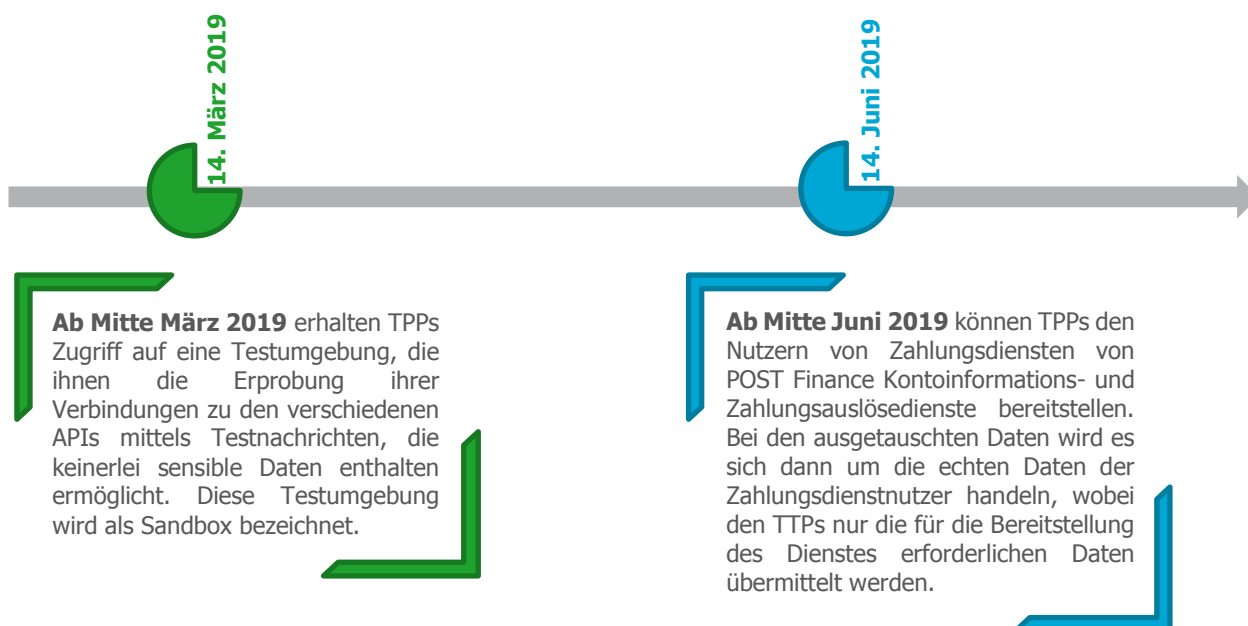
Um diesen Zahlungsdienstleistern die Bereitstellung dieser drei Arten von Diensten zu ermöglichen, richten deren kontenführende Finanzinstitute Kommunikationsschnittstellen ein, die üblicherweise als Application Programming Interface (API) bezeichnet werden.

POST Finance nutzt die Dienste von LUXHUB, um TPPs den Zugriff auf die für die Bereitstellung des Kontoinformations- und des Zahlungsauslösedienstes erforderlichen Informationen ihrer Kunden zu ermöglichen. LUXHUB ist eine gemeinsame Initiative von POST Finance, BCEE, BGL BNP Paribas und Banque Raiffeisen, die auf die Betreuung der verschiedenen Akteure beim Umgang mit den Herausforderungen und Chancen der PSD2 abzielt.

Das vorliegende Dokument beschreibt die technischen Merkmale der von POST Finance verwendeten APIs, um TPPs die Bereitstellung der Kontoinformations- und Zahlungsauslösedienste an ihre Kunden zu ermöglichen.

## Fristen

Der Zugriff auf die APIs erfolgt in zwei Etappen:



## Wer kann für welche Dienste auf die Konten zugreifen?

Die APIs von POST Finance können ausschließlich von TPPs genutzt werden, die über eine seitens einer zuständigen Behörde eines Mitgliedstaats der Europäischen Union ausgestellte Lizenz verfügen. Zur Identifizierung bei POST Finance müssen die TPPs im Besitz eines als eIDAS bezeichneten elektronischen Zertifikats sein, aus dem hervorgeht, auf welche Arten von Informationen sie zugreifen können. PRETA, eine Tochtergesellschaft von EBA Clearing, führt mit dem *Open Banking Europe Directory* ein Verzeichnis der Zertifikate. LUXHUB hat mit PRETA ein Abkommen im Hinblick auf den Zugriff auf dieses Verzeichnis und die Verwaltung einer für Luxemburg geltenden Kopie dieses Verzeichnisses getroffen.

Die nachstehende Tabelle fasst zusammen, auf welche Informationen die autorisierten Finanzinstitute zugreifen können:

	AISP-Lizenz	PISP-Lizenz	Banklizenz	Karten- ausgabelizenz (CBPII)
Zahlungs- auslösedienst		✓	✓	
Zugriff auf die Kontostände	✓		✓	
Zugriff auf die Transaktions- historie	✓		✓	
Bescheinigung über die Verfügbarkeit von Geldbeträgen				✓

## Funktionsweise der API

- **Onboarding**

TPPs, die Zugriff auf die Zahlungsinformationen der Kunden von POST Finance haben möchten, müssen über LUXHUB verbunden und autorisiert sein.

TPPs, die den Kunden von POST Finance über die API von LUXHUB Dienste bereitstellen möchten, können über [dieses Portal](#) ein Konto erstellen und sich authentifizieren. Die gesamte Verwaltung der TPPs erfolgt über LUXHUB und nicht über POST Finance.

- **Autorisierung**

Die Konten der Kunden von POST Finance sind vor unbefugtem Zugriff geschützt. TPPs müssen sich über OAuth2.0 authentifizieren und über die Genehmigung des Kunden verfügen, um Zugriff auf dessen bei POST Finance gespeicherten Informationen zu erhalten.

- **Eingesetzte Technik**

Die von LUXHUB bereitgestellten APIs von POST Finance gründen auf dem Modell und dem Standard der Version 1.3 des NextGenPSD2 Framework der Berlin Group.

Bei den APIs handelt es sich um REST APIs, die über Nachrichten im JSON-Standard kommunizieren. Das von LUXHUB-APIs für den Zugriff auf POST Finance verwendete Authentifizierungsmodell ist wie folgt:

- Redirect SCA Approach

Die nachstehenden drei Arten von HTTP-Nachrichten können über die APIs eingesetzt werden:

- POST** Diese Nachrichtenart wird übermittelt, um die Hinzufügung einer neuen Ressource bei der Verarbeitungseinheit zu beantragen.
- GET** Diese Nachrichtenart wird übermittelt, um Zugriff auf eine Ressource zu erhalten (ohne jedwede Änderung).
- DELETE** Diese Nachrichtenart wird zum Löschen der Ressourcen übermittelt.

## Welche verschiedenen APIs stehen zur Verfügung?

- **Payment Initiation Services (PIS)**

Diese API ermöglicht den PISP die Auslösung und Änderung einer Zahlungsanfrage sowie den Erhalt von Informationen über den Status der ausgelösten Zahlung. Dies kann unter anderem über die nachstehenden Anfragen erfolgen:

- Zahlungsauslöseanfrage [POST]
- Erhalt von Zahlungsinformationen [GET]
- Erhalt des SCA-Status (starke Authentifizierung) der Autorisierung einer Zahlung [GET]
- Erhalt des SCA-Status der Autorisierung der Stornierung einer Zahlung [GET]
- Erhalt des Status der Zahlungsauslöseanfrage [GET]

- **Confirmation of Funds Services**

Diese API ermöglicht den Emittenten von Zahlungskarten (CBPII) im Rahmen der Auslösung einer Zahlung seitens eines Kunden bei Account Servicing Payment Service Providern (ASPSP) einen Status in Bezug auf die Verfügbarkeit eines Geldbetrags auf dem mit der Bankkarte verbundenen Konto zu erfragen. Der ASPSP teilt die Verfügbarkeit des

Geldbetrags über eine sehr vereinfachte Nachricht in Form von „Ja“ oder „Nein“ mit. Die einzige mögliche Anfrage lautet wie folgt:

- Bestätigung der Anfrage in Bezug auf den Geldbetrag [POST]

- **Account Information Services**

Diese API ermöglicht den AISP den Erhalt von Informationen über das oder die Konten des Kunden. Vorbehaltlich des Erhalts der ausdrücklichen Zustimmung des Kunden stehen die nachstehenden Informationen zur Verfügung:

- Transaktionsbericht für ein bestimmtes Konto
- Kontostand eines bestimmten Kontos
- Verzeichnis der verfügbaren Konten
- Einzelheiten über ein bestimmtes Konto

Dieser Dienst kann unter anderem über die nachstehenden Anfragen bereitgestellt werden:

- Erhalt der Liste der Konten mit oder ohne Kontostand nach Einholung der Zustimmung des Kunden seitens des TPP [GET]
- Erhalt von Einzelheiten (darunter des Kontostands) über ein bestimmtes Konto [GET]
- Erhalt der Transaktionsliste oder des Transaktionsberichts für ein bestimmtes Konto [GET]
- Erstellung der Zustimmung für Zugriffsrechte auf ein bestimmtes Konto [POST]
- Löschung der Zustimmung zu bestimmten Zugriffen [DELETE]
- Erhalt des Status der Zustimmung zum Zugriff auf Kontoinformationen [GET]

## Glossar

<b>AISP</b>	Account Information Service Provider / Kontoinformationsdienstleister
<b>API</b>	Application Programming Interface / Programmierschnittstelle
<b>ASPSP</b>	Account Servicing Payment Service Provider / Kontoführender Zahlungsdienstleister
<b>Berlin Group</b>	Die Berlin Group ist eine Institution, die technische Standards entwickelt, die den Schwerpunkt auf technische Details und betriebliche Anforderungen legen
<b>CBPII</b>	Card-based payment instrument issuer / Emittent von Zahlungskarten
<b>eIDAS-Zertifikat</b>	Bei den eIDAS-Zertifikaten handelt es sich um Zertifikate, die die elektronische Identifizierung und die Vertraulichkeit des Austauschs ermöglichen - Electronic IDentification Authentication and trust Services (eIDAS) bezieht sich auf die gleichnamige Verordnung (Verordnung (EU) Nr. 910/2014)
<b>PISP</b>	Payment Initiation Service Provider / Zahlungsauslösedienstleister
<b>PSD2</b>	Revised Payment Service Directive / Die überarbeitete Richtlinie über Zahlungsdienste ist eine am 13. Januar 2018 in Kraft getretene europäische Richtlinie zur Regelung der Zahlungsdienste
<b>SCA</b>	Strong Customer Authentication / Starke Kundenauthentifizierung ist eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist
<b>TPP</b>	Third-Party Payment Service Provider / Dritter Zahlungsdienstleister