

API

## STRESZCZENIE DOKUMENTACJI TECHNICZNEJ








Strona 1 z 8

## SPIS TREŚCI

1	API – podstawowe informacje.....	3
2	Rejestracja TPP.....	4
3	Opis metod.....	6
4	Opis procesu uwierzytelniania PSU.....	7
5	Dodatkowe informacje na temat wersji testowej API.....	8

## 1 API – podstawowe informacje

### API – podstawowe informacje

	<p><b>CZYM JEST API?</b></p>	<p><b>API</b> to zdefiniowany interfejs programistyczny pozwalający na realizację założeń dyrektywy PSD2.</p>
	<p><b>W JAKI SPOSÓB API REALIZUJE ZAŁOŻENIA DYREKTYWY?</b></p>	<p>Pozwala na bezpieczną realizację nowych kategorii usług określonych w PSD2 (PIS, AIS, CAF) przez TPP.</p>
	<p><b>W JAKI SPOSÓB POWSTAŁO API?</b></p>	<p><b>API</b> jako samodzielne narzędzie realizujące założenia otwartej bankowości, powstało w oparciu o <i>Standard PolishAPI</i>.</p>
	<p><b>CZYM JEST STANDARD POLISHAPI?</b></p>	<p><i>Standard PolishAPI</i> został opracowany na potrzeby polskiego rynku finansowego w wyniku konsultacji prowadzonych przez podmioty polskiego sektora bankowego i płatniczego.</p>
	<p><b>W JAKIM STOPNIU API KORZYSTA Z OGÓLNODOSTĘPNEGO STANDARDU POLISHAPI?</b></p>	<p><b>API</b> to wciąż rozwijające się narzędzie. Zakres funkcjonalności i zakres danych odpowiada funkcjonalnościom udostępnianym w bankowości internetowej.</p>
	<p><b>JAKI TYP INTERFEJSU REALIZUJE API?</b></p>	<p><b>API</b> realizuje interfejs podstawowy. <b>API</b> nie realizuje interfejsu Callback.</p>
	<p><b>W JAKI SPOSÓB API ZAPEWNIĄ BEZPIECZEŃSTWO PRZESYŁANYCH DANYCH?</b></p>	<p>Bezpieczeństwo informacji zapewnia:</p> <ul style="list-style-type: none"> <li>▪ Uwierzytelnienie TPP</li> <li>▪ Autoryzacja TPP</li> <li>▪ Autoryzacja PSU dla operacji wykonywanych przez TPP</li> <li>▪ Bezpieczeństwo w przypadku aplikacji mobilnych</li> <li>▪ Walidacja i zapewnienie integralności danych</li> <li>▪ Kryptografia</li> <li>▪ Ochrona przed nadużyciami API</li> <li>▪ Logowanie informacji audytowych.</li> </ul>

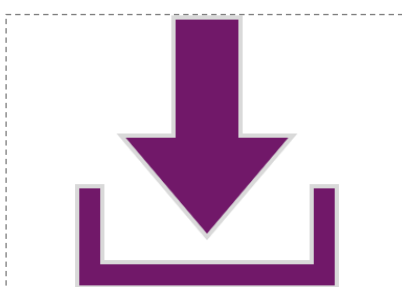
Nowelizacja dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego – **PSD2** – umożliwiła wprowadzenie na rynek nowych kategorii usług finansowych (**PIS, AIS, CAF**) oraz nowych typów dostawców tych usług (**TPP**). Pojawienie się nowych podmiotów oferujących usługi finansowe zrodziło potrzebę wykreowania narzędzia pozwalającego na bezpieczne zarządzanie przekazywanymi danymi o aktywności na rachunku klienta oraz środkach płatniczych, którymi dysponuje klient. Odpowiedzią na zapotrzebowanie rynku jest **API**.

Na poniższym schemacie zamieszczono odwołania do szczegółowej dokumentacji dotyczącej **API** oraz **PolishAPI**.

## Szczegółowe informacje na temat API oraz PolishAPI



**DOKUMENTACJA TECHNICZNA  
STANDARDU POLISH API**  
[PolishAPI-ver\\_1\\_2.yaml](#)



**POLISH API NA SWAGGERHUB**  
[Interfejs podstawowy](#)



**API SWAGGER**  
(dostęp możliwy po wypełnieniu formularza zamówienia)

## 2 Rejestracja TPP

Uzyskanie dostępu do **API** poprzedzone jest rejestracją **TPP**. Dostęp do strony (dostęp możliwy po wypełnieniu formularza zamówienia) umożliwiającej rejestrację mają wyłącznie użytkownicy posiadający aktualny certyfikat KIR zainstalowany w przeglądarce internetowej.

Rejestracja Klienta

Nazwa klienta:  
1

Adres aplikacji klienta:  
2

Redirect URL:  
3

Kwalifikowany certyfikat do zabezpieczeń witryn internetowych (QWAC):

Kwalifikowany certyfikat pieczęci elektronicznej (QSealC):  
  4

Parametr nagłówka Kid:  
 5

Podczas rejestracji dany podmiot powinien **obligatoryjnie uzupełnić** następujące informacje:

1. **Nazwa klienta** – należy podać nazwę podmiotu TPP.
2. **Adres aplikacji klienta** – należy podać adres aplikacji klienta.
3. **Redirect URL** – należy podać adres lub listę adresów po stronie TPP, na które może zostać przekierowany PSU, po zakończeniu procesu uwierzytelniania oraz autoryzacji dostępu do zasobów ASPSP.
4. W celu rejestracji, oprócz uzupełnienia wymaganych pól, **konieczne jest** również wczytanie następujących plików:
  - Kwalifikowanego certyfikatu do zabezpieczania witryn internetowych (*Qualified certificate for website authentication QWAC*)
  - Kwalifikowanego certyfikatu pieczęci elektronicznej (*Qualified certificate for electronic seal QSealC*).
5. **Kid** – należy podać unikalny ciąg znaków KID – parametr nagłówka podpisu JWS-SIGNATURE zgodnie z normą RFC 7515.

Po pozytywnej weryfikacji danych **TPP** otrzymuje identyfikator klienta (**Client Id**), który wymagany jest w ramach komunikacji z ASPSP. Nadany identyfikator Client Id jest stały i będzie wykorzystywany przez **TPP** zawsze podczas realizacji usług finansowych (**PIS, AIS, CAF**).

Rejestracja przebiegła pomyślnie. Klient **TPP** otrzymał identyfikator: **94f8332a-1713-4e46-81ad-1e91aba84987**.  
W przypadku utraty identyfikatora wymagana jest ponowna rejestracja klienta.

94f8332a-1713-4e46-81ad-1e91aba84987

Kopiuj



## UWAGA!

Aktualizacja certyfikatów i danych klienta realizowana jest poprzez ponowną rejestrację **TPP** i pozyskanie nowego identyfikatora klienta.

## 3 Opis metod

API, wzorując się na rozwiązaniach proponowanych w *Standardzie PolishAPI*, realizuje usługi za pomocą wymienionych w poniższej tabeli metod:

<b>Lista realizowanych metod</b>	<b>USŁUGI AUTORYZACJI</b>	<ul style="list-style-type: none"><li>• authorize</li><li>• token</li></ul>
	<b>USŁUGI ACCOUNT INFORMATION SERVICE (AIS)</b>	<ul style="list-style-type: none"><li>• deleteConsent</li><li>• getAccounts</li><li>• getAccount</li><li>• getTransactionsDone</li><li>• getTransactionsPending</li><li>• getTransactionsRejected</li><li>• getTransactionsCancelled</li><li>• getTransactionsScheduled</li><li>• getTransactionDetail</li></ul>
	<b>USŁUGI PAYMENT INITIATION SERVICE (PIS)</b>	<ul style="list-style-type: none"><li>• domestic</li><li>• tax</li><li>• recurring</li><li>• getPayment</li><li>• getRecurringPayment</li><li>• getMultiplePayments</li><li>• cancelPayments</li><li>• cancelRecurringPayment</li></ul>
	<b>USŁUGA CONFIRMATION OF THE AVAILABILITY OF FUNDS (CAF)</b>	<ul style="list-style-type: none"><li>• getConfirmaionOfFunds</li></ul>

W ramach **API** nie są realizowane wymienione w poniższej tabeli metody:

Metody nierealizowane	USŁUGI AUTORYZACJI	<ul style="list-style-type: none"><li>authorizeExt – uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym</li></ul>
	USŁUGI ACCOUNT INFORMATION SERVICE (AIS)	<ul style="list-style-type: none"><li>getHolds</li></ul>
	USŁUGI PAYMENT INITIATION SERVICE (PIS)	<ul style="list-style-type: none"><li>EEA</li><li>nonEEA</li><li>bundle</li><li>getBundle</li></ul>

#### 4 Opis procesu uwierzytelniania PSU

Proces uwierzytelnienia PSU przeprowadzany jest w interfejsie **usługi eSKOK**.

Uwierzytelnienie PSU obejmuje dwa etapy:

1. **Logowanie do usługi eSKOK** – w procesie logowania PSU powinien podać swój login i hasło.
2. **Potwierdzenie operacji** – PSU powinien potwierdzić operację.



#### UWAGA!

Podczas procesu uwierzytelniania PSU możliwy będzie wybór NRB.

## 5 Dodatkowe informacje na temat wersji testowej API

Możliwość uwierzytelnienia PSU w wersji testowej **API** jest dostępna za pomocą loginu i hasła przypisanego do testowych użytkowników:

DANE DO LOGOWANIA	LOGIN	HASŁO
	9991110000	PolishAPI111#
	9992220000	PolishAPI222#
	9993330000	PolishAPI333#
	9994440000	PolishAPI444#
	9995550000	PolishAPI555#