

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

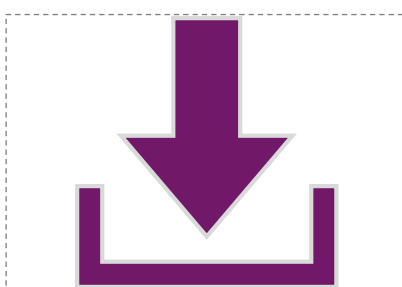
Nowelizacja dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego – **PSD2** – umożliwiła wprowadzenie na rynek nowych kategorii usług finansowych (**PIS, AIS, CAF**) oraz nowych typów dostawców tych usług (**TPP**). Pojawienie się nowych podmiotów oferujących usługi finansowe zrodziło potrzebę 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

Podmiot: 1
-- Wybierz podmiot --

Nazwa klienta: 2
Nazwa klienta

Adres aplikacji klienta: 3
Adres aplikacji klienta

Redirect URL: 4
Redirect URL

Kwalifikowany certyfikat do zabezpieczeń witryn internetowych (QWAC): 5
Plik QWAC... Wybierz plik...

Kwalifikowany certyfikat pieczęci elektronicznej (QSealC): 6
Plik QSealC... Wybierz plik...

Zarejestruj

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

1. **Podmiot** – należy wybrać z list rozwijanej typ podmiotu TPP.
2. **Nazwa klienta** – należy podać nazwę podmiotu TPP.
3. **Adres aplikacji klienta** – należy podać adres aplikacji klienta.
4. **Redirect URL** – należy podać adres lub listę adresów (oddzielone średnikiem ;) po stronie TPP, na które może zostać przekierowany PSU, po zakończeniu procesu uwierzytelniania oraz autoryzacji dostępu do zasobów ASPSP.

W celu rejestracji, oprócz uzupełnienia wymaganych pól, **konieczne jest** również wczytanie następujących plików:

5. Kwalifikowanego certyfikatu do zabezpieczania witryn internetowych (*Qualified certificate for website authentication QWAC*)
6. Kwalifikowanego certyfikatu pieczęci elektronicznej (*Qualified certificate for electronic seal QSealC*).

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**).
- identyfikator nagłówka Kid (parametr nagłówka podpisu JWS-SIGNATURE zgodnie z normą RFC 7515) – unikalny ciąg znaków Kid, który jest generowany przez ASPSP.

Rejestracja przebiegła pomyślnie. Klient [redacted] otrzymał identyfikator: **a9745c9f-a043-41d5-8106-551d86094939**, oraz identyfikator nagłówka Kid: **a9745c9f-a043-41d5-8106-551d86094939**.
W przypadku utraty identyfikatorów wymagana jest ponowna rejestracja klienta.

Identyfikator:

Identyfikator nagłówka Kid:



UWAGA!

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

3 Opis metod

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

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

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

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

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#