

APLITT

API STRESZCZENIE DOKUMENTACJI TECHNICZNEJ

APL!TT

API








SPIS TREŚCI

1	API – podstawowe informacje
2	Interfejs awaryjny (Fallback).....
3	Rejestracja TPP.....
4	Opis metod
5	Opis procesu uwierzytelniania PSU
6	Dodatkowe informacje na temat wersji testowej API

API – podstawowe informacje

Nowelizacja dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego – **PSD2** – umożliwiła

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.

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

APLITT

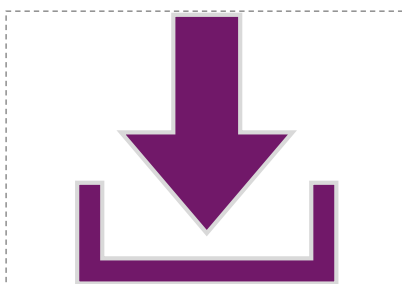
narzędzie pozwalającego na bezpieczne zarządzanie przekazywanymi danymi o aktywności na rachunku klienta oraz środkach płatniczych, którymi dysponuje klient. Odpowiedzią na zapotrzebowanie rynku jest **API**.

Na poniższym schemacie zamieszczono linki do szczegółowej dokumentacji *Standardu PolishAPI* – API realizuje założenia bankowości elektronicznej w oparciu o *Standard PolishAPI*. Pełna dokumentacja techniczna API udostępniania jest TPP po wypełnieniu formularza zamówienia.

Szczegółowe informacje na temat API oraz PolishAPI



DOKUMENTACJA TECHNICZNA
STANDARDU POLISH API



POLISH API NA SWAGGERHUB
Interfejs podstawowy



API SWAGGER
(dostęp możliwy po wypełnieniu formularza zamówienia)

2 Interfejs awaryjny (Fallback)

W celu zapewnienia płynności w realizacji usług PIS oraz AIS, oprócz interfejsu podstawowego **API**, przygotowany został specjalny interfejs awaryjny – **Fallback**.

Interfejs awaryjny został opracowany zgodnie z rekomendacją Związku Banków Polskich (*Rekomendacje oraz podstawowe założenia do przygotowania interfejsu awaryjnego*).

Interfejs awaryjny umożliwi TPP realizację usług w przypadku braku dostępu lub awarii interfejsu podstawowego.



UWAGA!

Dostęp oraz szczegółowe informacje dotyczące działania interfejsu awaryjnego **Fallback** zostaną udostępnione TPP po wcześniejszej rejestracji.

3 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.

API ITT

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.

API ITT

Rejestracja przebiegła pomyślnie. Klient [imię] 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:

a9745c9f-a043-41d5-8106-551d86094939

Kopiuuj

Identyfikator nagłówka Kid:

179662ab-6353-4bc0-b4f5-9cc340f4fada

Kopiuuj

4 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 cancelPayments cancelRecurringPayment
	USŁUGA CONFIRMATION OF THE AVAILABILITY OF FUNDS (CAF)	<ul style="list-style-type: none"> getConfirmaionOfFunds

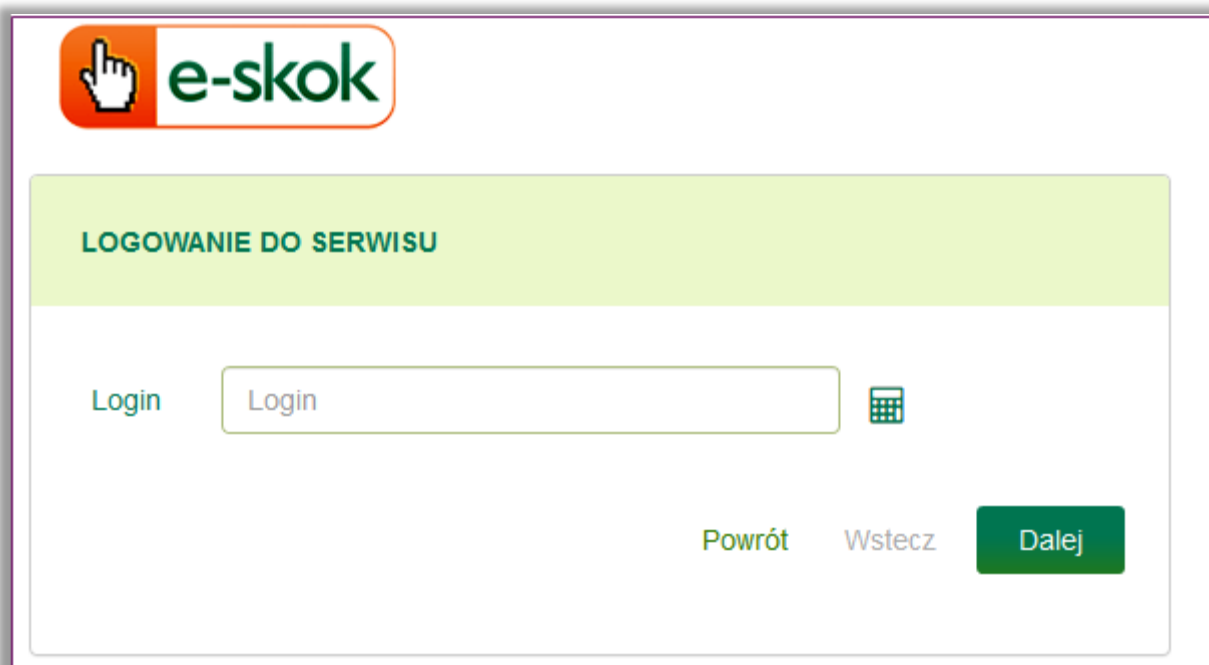
APLITT

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

Metody nierrealizowane	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"> EEA nonEEA bundle getBundle getMultiplePayments

5 Opis procesu uwierzytelniania PSU

Proces uwierzytelniania PSU przeprowadzany jest w interfejsie **usługi bankowości elektronicznej Kasy Stefczyka** (online.kasastefczyka.pl).



The screenshot shows the 'e-skok' login page. At the top left is the 'e-skok' logo with a hand icon. Below it is a green header with the text 'LOGOWANIE DO SERWISU'. The main area contains a 'Login' label, a text input field with 'Login' inside, and a calculator icon to the right. At the bottom right, there are three buttons: 'Powrót', 'Wstecz', and a green 'Dalej' button.

Uwierzytelnienie PSU obejmuje trzy etapy:

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

3 Weryfikacja SMS – PSU powinien potwierdzić operację za pomocą kodu przesłanego SMS-em.



UWAGA!

Jeśli NRB nie zostanie przekazane przez TPP, PSU będzie mógł wybrać numer NRB podczas procesu uwierzytelniania.

6 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#

Celem otrzymania dostępu do API oraz pełnej wersji dokumentacji technicznej należy zgłosić swoją prośbę o dostęp na adres mailowy api@kasastefczyka.pl.