

API

## STRESZCZENIE DOKUMENTACJI TECHNICZNEJ








Strona 1 z 9

## SPIS TREŚCI

1	API – podstawowe informacje.....	3
2	Interfejs awaryjny (Fallback).....	4
3	Rejestracja aplikacji klienckiej TPP.....	4
4	Opis metod.....	8
5	Opis procesu uwierzytelniania PSU.....	9
6	Dodatkowe informacje na temat wersji testowej API.....	9

## 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>▪ Walidacja i zapewnienie integralności danych</li> <li>▪ Kryptografia</li> <li>▪ Ochrona przed nadużyciami API</li> <li>▪ Logowanie informacji audytowych.</li> </ul>

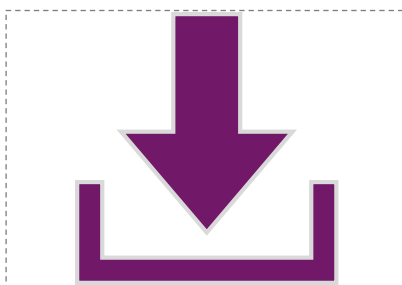
Nowelizacja dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego – **PSD2** – umożliwiła wprowadzenie na rynek nowych kategorii usług finansowych (**PIS, AIS, CAF**) oraz nowych typów dostawców tych usług (**TPP**). Pojawienie się nowych podmiotów oferujących usługi finansowe zrodziło potrzebę 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 linki do szczegółowej dokumentacji *Standardu PolishAPI* – API realizuje założenia bankowości elektronicznej w oparciu o *Standard PolishAPI*. Pełna dokumentacja techniczna API udostępniana 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 umożliwia 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 aplikacji klienckiej TPP

W związku z utworzeniem dedykowanej metody **register** w wersji **3.0 Polish API**, usunięta została możliwość rejestracji TPP poprzez formularz dostępny na stronie. Korzystanie z interfejsu XS2A musi zostać poprzedzone rejestracją aplikacji klienckiej TPP za pomocą metody **register**. Wymagane jest przekazanie danych rejestracyjnych w **tokenie software\_statement** zgodnie ze *Standardem PolishAPI*.

Żądanie TPP inicjowało będzie rejestrację nowej aplikacji klienckiej. W przypadku pozytywnej rejestracji TPP otrzyma odpowiedź zgodną ze *Standardem PolishAPI*. W odpowiedzi TPP otrzyma **unikalny identyfikator aplikacji klienckiej nadany przez ASPSP** oraz **miejsce pobrania certyfikatu pieczęci**.

# APL!TT

Na potrzeby interfejsu zawartość żądania, określona w dokumentacji *Polish API w wersji 3.0*, została rozszerzona o parametr **client\_id**, który pozwala na aktualizację danych aplikacji klienckiej TPP oraz certyfikatów. Podanie identyfikatora klienta w tokenie `software_statement` zainicjuje aktualizację:

- wszystkich danych aplikacji klienckiej,
- danych TPP oraz
- certyfikatów.

Przy każdorazowej aktualizacji danych wymagane jest przekazanie kompletnego zestawu parametrów.



## UWAGA!

W przypadku aktualizacji danych globalnych (np. nazwy organizacji), należy zainicjować aktualizację wszystkich aplikacji klienckich lub wykonać ponowną rejestrację.

Potwierzeniem poprawnej aktualizacji danych będzie przesłanie odpowiedzi zgodnej z dokumentacją standardu. Odpowiedź będzie zawierała **identyfikator aplikacji klienckiej**, nadany podczas rejestracji aplikacji klienckiej.

Poniżej przedstawiono szczegółowy opis pól obsługiwanych w ramach metody **register**.

Pola żądania rejestracji zawarte w **tokenie software\_statement**.

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
iat	Moment wystawienia <code>software_statement</code> .	Nie	
aud	Zakładany odbiorca danego żądania.	Nie	
iss	Identyfikator wystawcy <code>software_statement</code> .	Tak	
iss_name	Nazwa wystawcy <code>software_statement</code> .	Nie	
sub	Identyfikator organizacji żądającej dostępu dla swojej aplikacji.	Nie	O ile podany, musi być tożsamy z identyfikacją organizacji, której dotyczy certyfikat.
sub_name	Nazwa (pełna) organizacji żądającej dostępu dla swojej aplikacji – pełna nazwa TPP.	Nie	O ile podany, nie może pozostawać w sprzeczności (być różny) od nazwy podanej w certyfikacie przedstawionym przez organizację.
sub_descr	Opis organizacji żądającej dostępu dla swojej aplikacji.	Nie	

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
sub_logo	URL logo organizacji żądającej dostępu dla swojej aplikacji.	Nie	
sub_contact_name	Imię i nazwisko osoby kontaktowej.	Nie	
sub_contact_email	Email do osoby kontaktowej.	Nie	
sub_org_number	NIP w formacie europejskim organizacji rejestrującej.	Nie	
sub_country	Kraj rejestracji organizacji.	Nie	
client_name	Nazwa aplikacji klienckiej. W razie nie podania, przyjmuje się nazwę TPP (z pola sub_name lub z certyfikatu).	Nie	W razie nie podania, przyjmuje się nazwę TPP (z pola sub_name lub z certyfikatu).
response_types	Zgodnie z RFC 7591.	Tak	Wartość stała: „code”.
grant_types		Tak	Wartość stała: „authorization_code”.
redirect_uris	Adresy URL, na które dopuszczalne jest przekierowanie klienta po zakończeniu wywołania metody /authorize.	Tak	Niedopuszczalne jest przekierowanie na inny URL niż wskazany w tym parametrze. Domena z adresów URL musi być zgodna z domeną podaną w certyfikacie.
jwks	Kolekcja kluczy (certyfikatów – dla kryptografii	Warunkowo TAK (o ile nie podano jwks_uri)	
jwks_uri	asymetrycznej), które mogą zostać użyte przez TPP dla podpisu żądań (i opcjonalnie nawiązania	Warunkowo TAK (o ile nie podano jwks)	

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
	<p>szyfrowanej komunikacji TLS)</p> <p>Musi zawierać certyfikat (lub miejsce pobrania certyfikatu) pieczęci zgodny z ETSI TS 119 495, który może zostać wykorzystany do podpisu żądań wysyłanych do interfejsu XS2A. Bank może opcjonalnie wspierać obsługę wielu certyfikatów per TPP/ aplikacja w takiej sytuacji może zawierać więcej niż jeden certyfikat pieczęci. Użycie parametru „kid” oraz jednoznacznego identyfikatora klucza x5t#256 (fingerprint) w żądaniach jest wymagane.</p>		
scope	<p>Lista (separowana spacjami) nazw zakresów uprawnień. Jedna lub więcej wartości z listy:</p> <ul style="list-style-type: none"> <li>- ais-accounts</li> <li>- ais</li> <li>- pis</li> </ul> <p>W przypadku nie podania przyjmowane jest na podstawie uprawnień na podstawie ról opisanych w certyfikacie TPP.</p> <p>Zgodnie z RFC 7591 I RFC 6749.</p>	Nie	

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
client_id	Unikalny identyfikator aplikacji TPP nadany przez ASPSP. Podawany tylko w przypadku aktualizacji danych aplikacji klienckiej lub certyfikatu.	Nie	

#### 4 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>• <b>register</b></li> <li>• <b>authorize</b></li> <li>• <b>token</b></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>• 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:

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

## 5 Opis procesu uwierzytelniania PSU

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

Uwierzytelnienie PSU obejmuje trzy etapy:

1. **Logowanie do usługi eSKOK** – w procesie logowania PSU powinien podać swój login, hasło i potwierdzić logowanie za pomocą kodu przesłanego SMS-em.
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:

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