APLITT

API
STRESZCZENIE DOKUMENTACJI TECHNICZNEJ

Aplitt Sp. z o.o.
ul. Arkońska 6/A1, 80-387 Gdańsk
tel.: +48 58 782 82 82
e-mail: kontakt@aplitt.pl
www.aplitt.pl

Spółka zarejestrowana w Sądzie Rejonowym w Gdańsku
VII Wydział Gospodarczy KRS 0000692419
Kapitał zakładowy: 14 047 350,00 zł
NIP 584-27-63-014

APL!TT

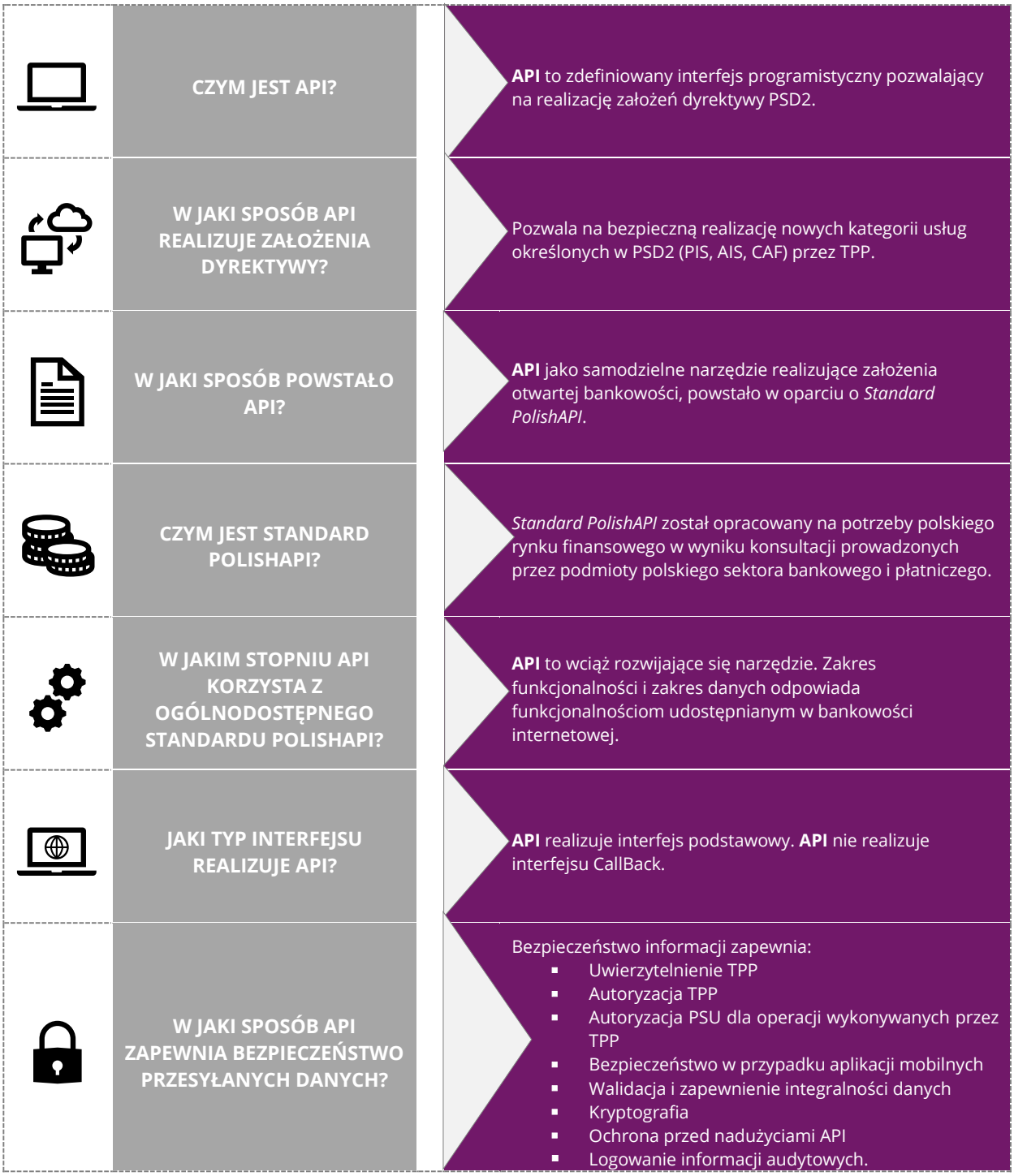
API

SPIS TREŚCI

APL!TT

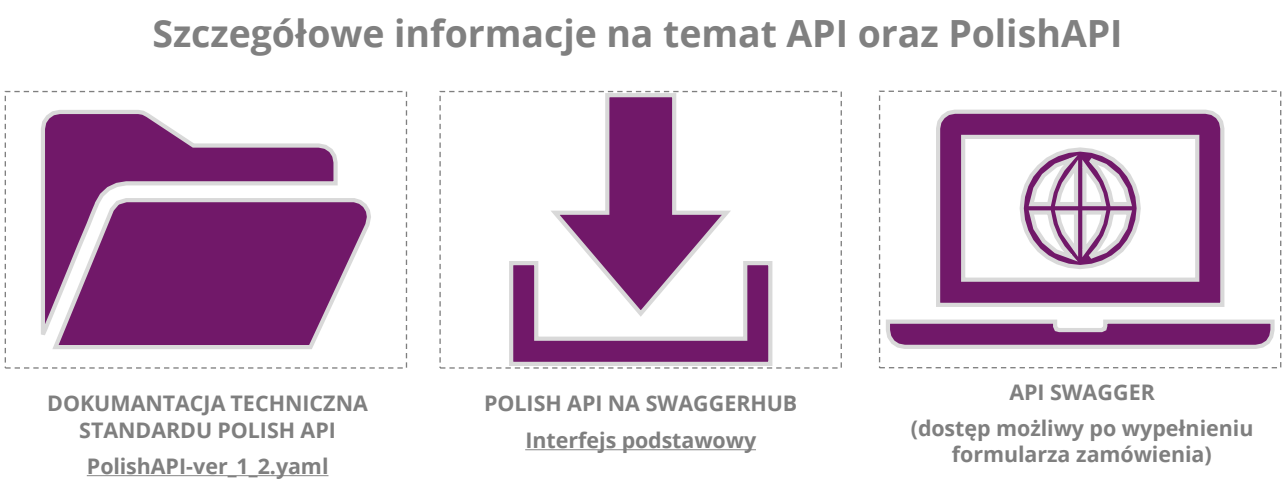
1 API – podstawowe informacje

API – podstawowe informacje



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**.



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.

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

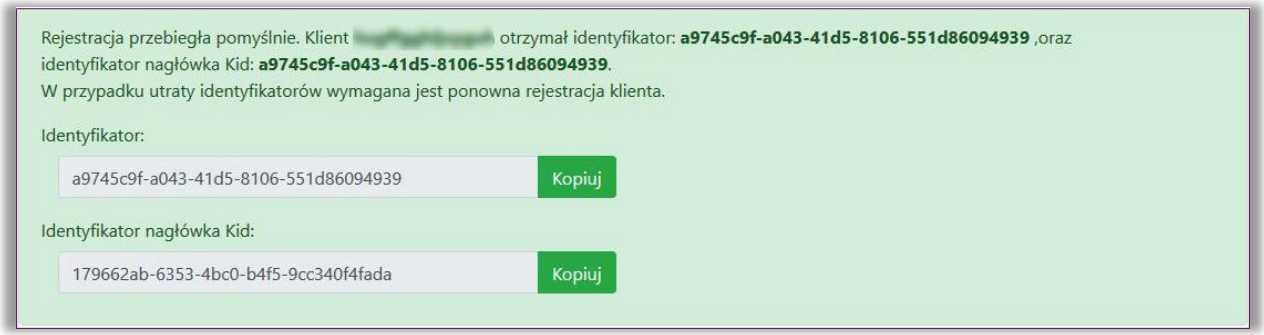
1. **Podmiot** – należy wybrać z list rozwijanej typ podmiotu TPP.
2. **Nazwa klienta** – należy podać nazwę podmiotu TPP.
3. **Adres aplikacji klienta** – należy podać adres aplikacji klienta.
4. **Redirect URL** – należy podać adres lub listę adresów (oddzielone średnikiem ;) po stronie TPP, na które 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.



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:

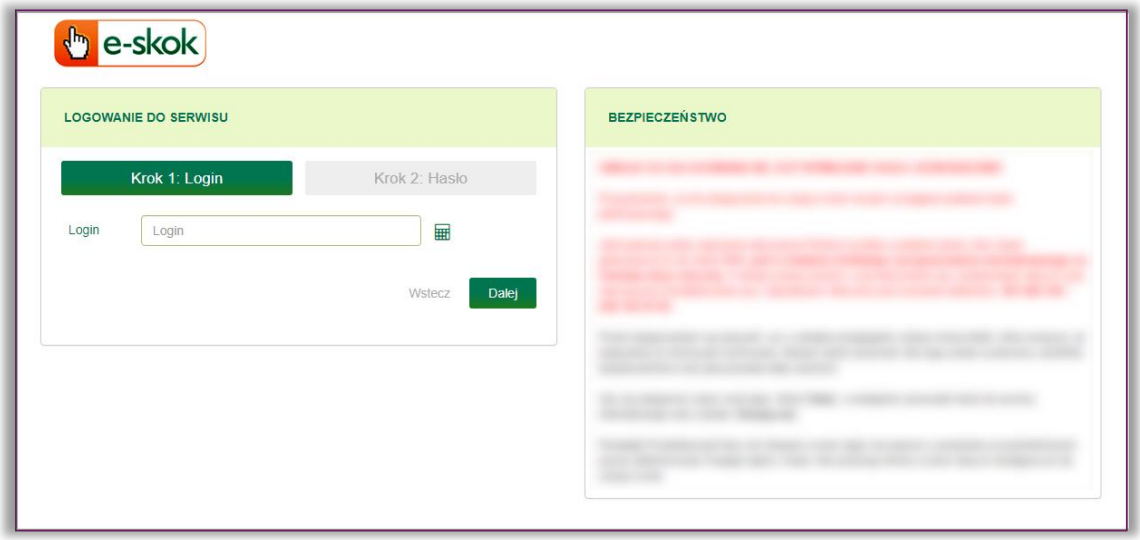
Lista realizowanych metod	
USŁUGI AUTORYZACJI	• authorize • token
USŁUGI ACCOUNT INFORMATION SERVICE (AIS)	• deleteConsent • getAccounts • getAccount • getTransactionsDone • getTransactionsPending • getTransactionsRejected • getTransactionsCancelled • getTransactionsScheduled • getTransactionDetail
USŁUGI PAYMENT INITIATION SERVICE (PIS)	• domestic • tax • recurring • getPayment • getRecurringPayment • getMultiplePayments • cancelPayments • cancelRecurringPayment
USŁUGA CONFIRMATION OF THE AVAILABILITY OF FUNDS (CAF)	• getConfirmaionOfFunds

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

Metody nierealizowane	**USŁUGI AUTORYZACJI**	• authorizeExt – uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym
	USŁUGI ACCOUNT INFORMATION SERVICE (AIS)	• getHolds
	USŁUGI PAYMENT INITIATION SERVICE (PIS)	• EEA • nonEEA • bundle • getBundle

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#