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

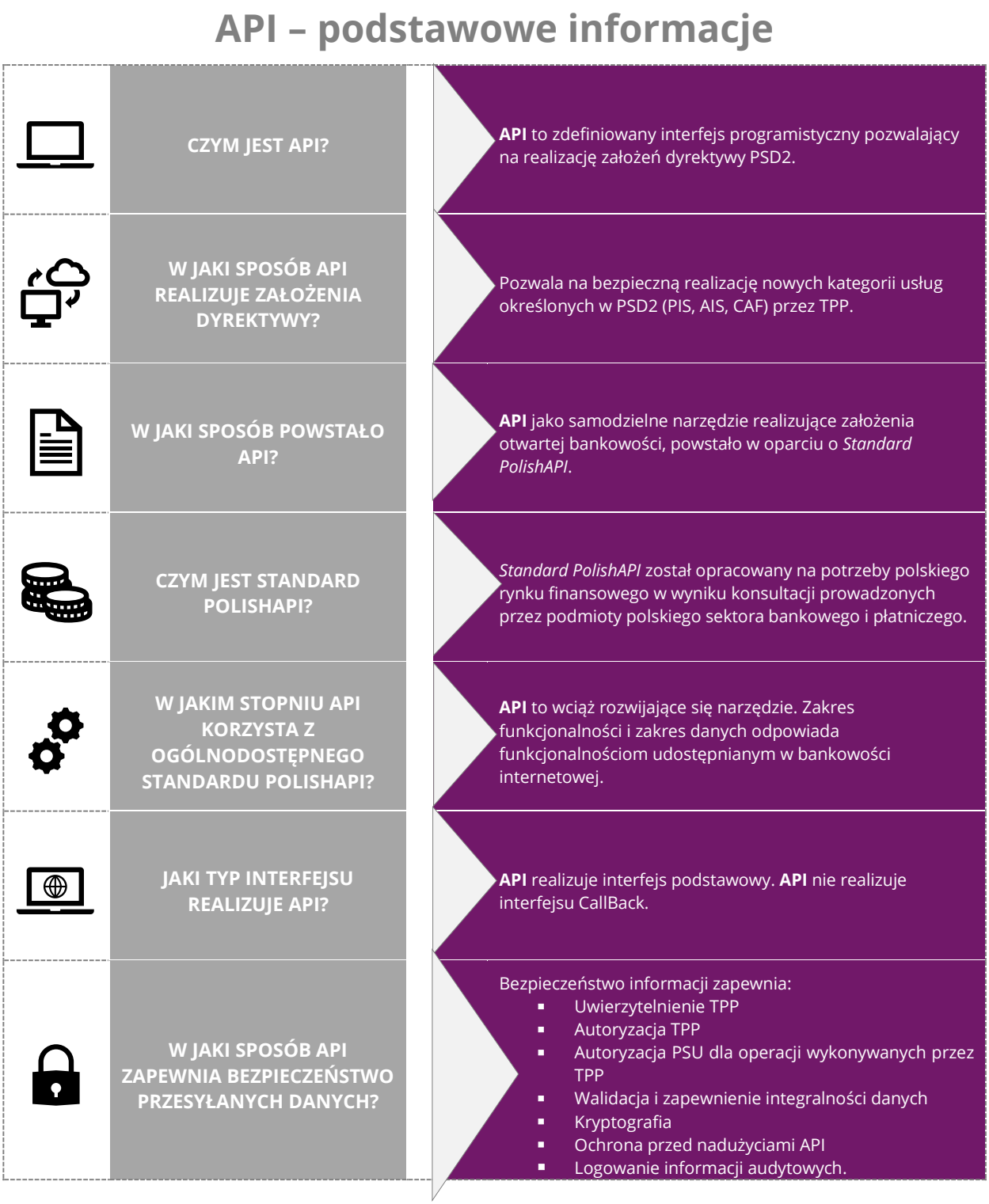
APL!TT

API

SPIS TREŚCI

APLITT

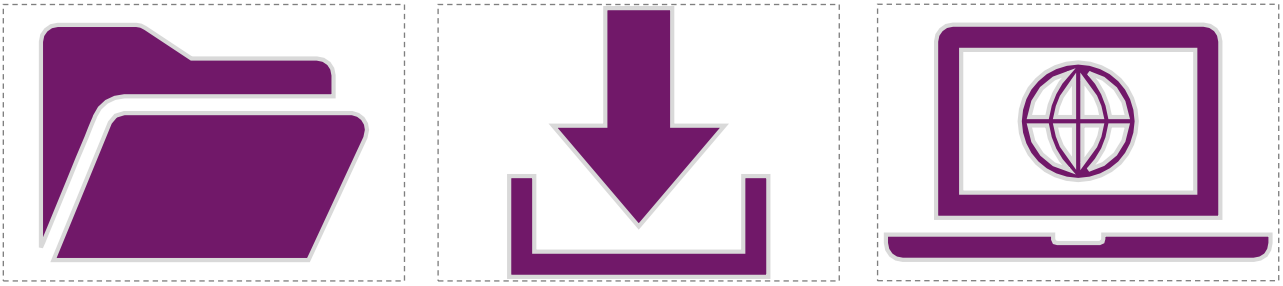
1 API – podstawowe informacje



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 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



DOKUMANTACJA 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 inferfejsu 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**.

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.

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

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

Pola żądania rejestracji zawarte w **tokenie software_statement**.

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
Iat	Moment wystawienia software_statement.	Nie	
aud	Zakładany odbiorca danego żądania.	Nie	
iss	Identyfikator wystawcy software_statement.	Tak	
iss_name	Nazwa wystawcy software_statement.	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_namelub 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 asymetrycznej), które mogą zostać użyte przez TPP dla podpisu żądań (i opcjonalnie nawiązania	Warunkowo TAK (o ile nie podano jwks_uri)	
jwks_uri		Warunkowo TAK (o ile nie podano jwks)	

IDENTYFIKATOR FAKTU	ZNACZENIE	WYMAGANY	UWAGI
	szyfrowanej komunikacji TLS) 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.		
scope	Lista (separowana spacjami) nazw zakresów uprawnień. Jedna lub więcej wartości z listy: - ais-accounts - ais - pis W przypadku nie podania przyjmowane jest na podstawie uprawnień na podstawie ról opisanych w certyfikacie TPP. Zgodnie z RFC 7591 I RFC 6749.	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:

Lista realizowanych metod	
USŁUGI AUTORYZACJI	• **register** • **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 • 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 • getMultiplePayments

5 Opis procesu uwierzytelniania PSU

Proces uwierzytelnienia 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:

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