API PKO BANKU POLSKIEGO
INSTRUKCJA DO PROCESU REJESTRACJI

Bank Polski

Przedmiot dokumentu:	Dokument zawiera podstawowe informacje potrzebne do rejestracji dostawcy usług płatniczych w API PKO Banku Polskiego	Nr wersji dokumentu:	2.0
		Data wersji dokumentu:	01.03.2024

Historia wersji (zmian) dokumentu

Wersja	Data	Opis zmian
2.0	01.03.2024	Utworzenie dokumentu

Dokumenty powiązane

Dokument	Wersja dokumentu	Opis
API PKO Banku Polskiego Dokumentacja techniczna	2.0	Szczegółowy opis techniczny API PKO Banku Polskiego
Dokumentacja JSON	1.5.2	Dokumentacja techniczna JSON dostępna na stronie https://developers.pkobp.pl/documentation

SPIS TREŚCI

WSTĘP

Celem tej dokumentacji jest opisanie sposobu w jaki uprawnieni zewnętrzni dostawcy usług (Third Party Provider- TPP) mogą połączyć się z produkcyjnym API PKO Banku Polskiego lub środowiskiem testowym Sandbox. Zawartość dokumentacji będzie aktualizowana wraz z powstawaniem nowych wersji środowiska, odzwierciedlających m.in. postępy procesu testowania i uwzględniających uwagi TPP.

Zanim rozpoczniesz proces developmentu/testowania zapoznaj się z *Regulaminem świadczenia usług drogą elektroniczną przez PKO Bank Polski* w zakresie Otwartej Bankowości PKO Banku Polskiego, dostępnym pod adresem https://developers.pkobp.pl/terms.

Nasze API jest oparte na standardzie PolishAPI, jeżeli chciałbyś zobaczyć pełną dokumentację standardu PolishAPI to przejdź na stronę: https://polishapi.org/#docs.

Dostęp do API PSD2 PKO Banku Polskiego udzielany jest jedynie podmiotom ze statusem TPP lub dla Technical Service Providera (TSP) działającego w imieniu TPP. Dostęp do API Sandbox udzielany jest jedynie podmiotom ze statusem TPP, TSP ewentualnie podmiotom starającym się o ten status.

Status TPP jest nadawany przez Komisję Nadzoru Finansowego (KNF) w Polsce lub jego odpowiednik w pozostałych krajach Uni Europejskiej.

1. PROCES REJESTRACJI DO ŚRODOWISKA TESTOWEGO (SANDBOX)

1.1 Aby rozpocząć proces korzystania z API Sandbox należy w pierwszej kolejności zawnioskować o dostęp. Wniosek złożyć można po rejestracji Konta Użytkownika na Portalu Developera https://developers.pkobp.pl w sekcji ustawienia -> produkty

1.2 Weryfikacja wniosku

Po prawidłowym wypełnieniu wniosku, przedstawiciel Banku dokonuje weryfikacji zgłoszenia, a następnie wysyła do TPP dalszą procedurę.
TPP zostanie poproszony o przesłanie części publicznej certyfikatu eIDAS zgodnego z normą ETSI TS 119 495 oraz udowodnienia posiadania klucza prywatnego korespondującego z tym certyfikatem (PKO Bank Polski pomoże w procesie przeprowadzenia tego dowodu, jeśli TPP będzie miał wątpliwości). Jest to warunek niezbędny do korzystania z API Sandbox.

Podmioty będące w trakcie ubiegania się o licencję TPP mogą wystąpić o dostęp do Sandbox używając certyfikatów testowych pod warunkiem wcześniejszego udostępnienia złożonego skanu wniosku o status TPP.

1.3 Weryfikacja certyfikatu

Po przesłaniu przez klienta certyfikatu następuje proces weryfikacji. Potwierdzenie własności następuje certyfikatu poprzez podpisanie kluczem prywatnym (związanym z tym certyfikatem) zawartości otrzymanego we wcześniejszej wiadomości pliku.

W przypadku jakichkolwiek wątpliwości, Bank zastrzega sobie prawo do wstrzymania dalszego procesu weryfikacji do czasu wyjaśnienia wątpliwości.

1.4 Nadanie dostępu

W następnym kroku firma zostanie dodana do wewnętrznej bankowej bazy TPP i zostaną dla niej utworzone dostępy, które pozwolą na testowani usług API Banku na środowisku testowym. Po zakończeniu procesu otrzyma od nas wiadomość na Portalu powiadamiającą o pozytywnej weryfikacji.

2. PROCES AUTOMATYCZNEJ REJESTRACJI DO ŚRODOWISKA API PSD2 PKOBP

2.1 Podstawowe informacje niezbędne do rejestracji

Aby skorzystać z połączenia API, należy wywołać usługę /register na endpoint:
https://api.pkobp.pl/v2_1_1.1/register/v2_1_1.1/register
Proces przeprowadzany jest w oparciu o protokół „OAuth 2.0 Dynamic Client Registration" (RFC 7591).

Proces automatycznej rejestracji przebiega dwuetapowo:
1. Generowanie Software Statement.
2. Żądanie automatycznej rejestracji /register z wykorzystaniem Software Statement.

Do połączenia z API potrzebne są:
- Certyfikat eIDAS, zgodny ze standardem ETSI TS 119 495, wskazujący na umocowanie regulacyjne.
- Podpisany kluczem prywatnym z certyfikatu QSeal Software Statement.
- Wywołanie usługi /register.

Do środowiska Inteligo nie jest wymagana osobna rejestracja.

Komunikacja ze środowiskami:
- W przypadku braku dostępności interfejsu API możliwe jest skorzystanie z rozwiązania awaryjnego. Informacje na temat tego rozwiązania zawarte zostały w pełnej wersji dokumentacji API PKO Banku Polskiego.
- TLS (ang. Transport Layer Security) – przyjęte jako standard w Internecie rozwinięcie protokołu SSL (ang. Secure Socket Layer). TLS zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509.
- Certyfikaty SSL są narzędziem zapewniającym ochronę witryn internetowych, a także gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania komunikacji pomiędzy komputerami. Certyfikaty SSL rejestrowane są na określoną nazwę domeny, zawierają informacje o właścicielu domeny, jego adresie itp. Dane te są zabezpieczone kryptograficznie i nie można ich samodzielnie zmienić.

- Certyfikaty pieczęci - pieczęć elektroniczna to usługa zaufania służąca do potwierdzania autentyczności i tożsamości wystawcy dokumentów elektronicznych. Rozwiązanie wykorzystuje kwalifikowany certyfikat pieczęci elektronicznej, który w odróżnieniu od podpisu elektronicznego, nie zawiera danych osoby fizycznej, a jedynie dane podmiotu posiadającego osobowość prawną (tj. firmy, organizacji, podmiotu administracji publicznej). Pieczęć elektroniczna to efektywne narzędzie zapewniające:
- Integralność – zabezpieczenie danych oraz dokumentów elektronicznych przed zmianą
- Wiarygodność – identyfikacja tożsamości przedsiębiorstwa /organizacji w świecie elektronicznym
- Niezaprzeczalność – brak możliwości wyparcia się procesu pieczętowania.
- Certyfikaty pieczęci są zgodne z europejskim rozporządzeniem eIDAS.
- Usługa jest zgoda z europejskim rozporządzeniem eIDAS, dzięki czemu dokumenty opieczętowane pieczęcią elektroniczną zachowują pełną moc prawną oraz dowodową.

2.2 Generowanie Software Statement

Niezbędne jest posiadanie następujących elementów:
- Klucz prywatny x509,
- Certyfikat x509, który powinien być umieszczony na zaufanym endpoint'cie,
- Lista adresów URL, na które mają być wysyłane odpowiedzi (redirect_uris).

Software Statement ma postać SignedJWT w formacie:
- Base64(Header).Base64(Claims).Base64(Signature)

Header może dodatkowo zawierać:
- jwks lub jwks_uri
- redirect_uris
- Parametry te mogą zostać umieszczone bezpośrednio w żądaniu zamiast w software_statement.

Claims musi zawierać:
- iat - moment wystawienia software_statement w formie NumericDate w sekundach
- iss - nazwa organizacji wystawiającej software_statement
- sub - nazwa organizacji, dla której wystawiony jest software_statement

W przypadku, gdy organizacja samodzielnie wystawia software_statement, parametry iss oraz sub będą tożsame.
JWKS musi zawierać dokładnie jeden element "keys".
Przykładowa struktura JWKS:

```
"jwks": {
  "keys": [
    {
      "alg":
      "SHA256withRSA",
      "kid": "TestowyKid",
      "kty": "RSA",
      "x5u": "https://test.com/certyfikat.pem"
    }
  ]
}
```

Przykładowa struktura JWT:

Header	{
	"alg" : "SHA256withRSA",
	"typ" : "JWT"
	}

Payload	{
	"iat" : 1422779638,
	"sub" : "TEST S.A.",
	"iss" : "TEST S.A."
	}

Signature	RSASHA256(base64urlEncoding(header) + '.' + base64urlEncoding(payload), certificate)

2.3 Żądanie automatycznej rejestracji /register
Żądanie automatycznej rejestracji składa się z:
1. Danych teleadresowych (limit znaków dla każdego z pól wynosi 70)
    a. Address
    b. delivery_address
    c. phone (włącznie z numerem kierunkowym kraju np. +48)
    d. email
2. Jeżeli nie zawarte w Software Statement:
    a. jwks lub jwks_uri
    b. redirect_uris
3. Software Statement

Wygenerowane w ten sposób Software Statement wysyłane jest żądanie automatycznej rejestracji /register. Adresy podane są w rozdziale „3. Podstawowe informacje dotyczące Sandboxa i API PKO Banku Polskiego".

Przykład 1.

JWKS (lub JWKS_uri) oraz Redirect uris zawarty w Software Statement:

```
POST
https://api.pkobp.pl/v2_1_1.1/register/v2_1_1.1/register
Content-Type: application/json
Accept: application/json
{
  "address": "string",
  "delivery_address":
  "string", "phone":
  "string",
  "email": "string",
  "software_statement": "/*wygenerowana wartość Software Statement*/"
}
```

Przykład 2.

JWKS (lub JWKS_uri) oraz Redirect uris niezawarty w Software Statement:

```
POST https://api.pkobp.pl/v2_1_1.1/register/v2_1_1.1/register
Content-Type: application/json
Accept: application/json
{
 "address": "string",
  "delivery_address":
  "string", "phone":
  "string",
  "email":
  "string",
  "jwks": {
    "keys": [
      {
        "alg":
        "SHA256withRSA",
        "kid": "TestowyKid",
        "kty": "RSA",
        "x5u": "https://test.com/certyfikat.pem"
      }
    ]
  }
  "redirect_uris": ["string"],
  "software_statement": "/*wygenerowana wartość Software Statement*/"
}
```

Jeśli żądanie zostanie obsłużone poprawnie, zwrócona zostanie odpowiedź z kodem 201, która zwierać będzie client_id.

2.4 Dalsze kroki po rejestracji

Po pozytywnej weryfikacji TPP otrzyma od nas dane (indywidualny identyfikator, dalej: clientId) oraz możliwość pobrania pełnej dokumentacji technicznej, która pozwoli na korzystanie z API. Dokumentację można pobrać po zalogowaniu na Portalu w sekcji PRODUKTY -> PSD2 -> Pliki do pobrania.

W pełnej dokumentacji znajdują się:

- Spis dostępnych endpoint'ów
- Opis kroków procesu autoryzacji zgody na rzecz TPP, który jest pierwszą czynnością pozwalającą na otrzymanie przez TPP tokenu wymaganego do wywoływania usług
- Różnice między PolishAPI a API PKO Banku Polskiego S.A
- Opis zaimplementowanych usług wraz z kodami odpowiedzi i słownikami wybranych pól
-

PODSUMOWANIE

Cieszymy się, że jesteście zainteresowani naszymi usługami. Dołożymy wszelkich starań, by integracja Waszej aplikacji z naszym API przebiegła bez żadnych problemów. Jeśli chcecie uzyskać dalsze informacje – zapraszamy do kontaktu poprzez stronę https://developers.pkobp.pl -> po rejestracji i aktywacji Konta Użytkownika w sekcji Zgłoszenia.