CREDIT AGRICOLE BANK POLSKA S.A.

Streszczenie dokumentacji interfejsu XS2A

Wdrożonego w Credit Agricole Bank Polska SA

Wersja 3.0

2023-11-20

Spis treści

1 PSD2 informacje ogólne

1.1 Definicje

Pojęcia pisane w niniejszym dokumencie z wielkiej litery mają znaczenie nadane im poniżej.

AIS (Account Information Service) - usługa online, polegająca na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych.

API (Application Programming Interface) - interfejs programistyczny aplikacji to zestaw reguł, który opisuje w jaki sposób aplikacje i systemy mogą komunikować się ze sobą.

API XS2A - interfejs programistyczny udostępniony przez Bank, który umożliwia upoważnionym podmiotom prowadzenie zautomatyzowanej komunikacji z Bankiem w zakresie realizacji usług PIS, AIS i CAF.

ASPSP (Account Servicing Payment Service Provider) - dostawca usług płatniczych zapewniający i utrzymujący rachunek płatniczy dla płatnika.

AST (Agreed Service Time) - dostępność miesięczna tj. całkowity czas działania do całkowitego czasu, w jakim usługa powinna działać, liczony w okresach miesięcznych w godzinach świadczenia usługi.

Bank - Credit Agricole Bank Polska S.A.

CAF (Confirming of the Availability of Funds) - usługa potwierdzenia dostępności kwoty na rachunku płatniczym niezbędnej do przeprowadzenia transakcji w oparciu o kartę.

Dzień roboczy - dzień od poniedziałku do piątku, z wyłączeniem sobót oraz dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.

Piaskownica PSD2 - jest wydzielone środowisko informatyczne w ramach systemu IT Banku, w ramach którego Użytkownik ma możliwość samodzielnego testowania udostępnionych przez Bank API XS2A.

PIS (Payment Initiation Service) - usługa polegająca na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych.

Polish API - Standard interfejsu wypracowany w ramach grupy roboczej Polish API przy Związku Banków Polskich.

PSD2 (Payment Service Directive) - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

PSU (Payment Services User) - osoba fizyczna lub prawna korzystającą z usługi płatniczej w charakterze płatnika, odbiorcy lub płatnika i odbiorcy.

Serwis – serwis informacyjny API Portal dostępny pod adresem: https://www.credit-agricole.pl/apiportal.

TPP (Third Party Providers) – podmiot świadczący usługi płatnicze typu PIS, AIS, CAF na podstawie Ustawy z dnia 19 sierpnia 2019 r. o usługach płatniczych.

Użytkownik - Osoba fizyczna reprezentująca TPP lub podmiot ubiegający się o status TPP kontaktująca się z Bankiem w tematach związanych z API XS2A.

1.2 Kontekst biznesowy

API (ang. *Application Programming Interface*) to pojęcie określające zestaw technologii pozwalających na wymianę danych pomiędzy rozwiązaniami informatycznymi.

Współczesne banki przy pomocy złożonych i bezpiecznych systemów informatycznych realizują usługi polegające min. na udostępnianiu informacji o rachunkach płatniczych oraz możliwości realizowania płatności z tych rachunków. W celu umożliwienia budowania zaawansowanych rozwiązań dostosowanych do potrzeb biznesu (klientów korporacyjnych) banki już od lat oferują różnego rodzaju API umożliwiające dostęp do ich usług.

Dotychczasowo usługi udostępniane przez banki w postaci API nie były regulowane i zależały głównie od strategii banku. Wejście w życie dyrektywy PSD2 (ang. *Payment Services Directive*) normalizuje rynek w tym zakresie, nakładając na banki obowiązek udostępniania danych o rachunkach płatniczych i inicjalizowania płatności z tych rachunków upoważnionym podmiotom w sposób określony w dyrektywie. Równocześnie PSD2 nie ogranicza banków w zakresie tego, ile usług udostępnią ponad te wymienione w dyrektywie jako obowiązkowe.

1.3 Możliwe sposoby integracji

Do podstawowych sposobów integracji należy zaliczyć :

- indywidualne integracje poprzez dedykowane interfejsy z wybranymi partnerami biznesowymi,
- powszechna integracja poprzez zunifikowany interfejs z pośrednikami (TPP) oferującym usługi wykorzystujące bankowość elektroniczną lub z nią współpracujące.

Dotychczas podstawowym sposobem integracji było udostępnienie przez bank autorskiego zestawu API. Z wykorzystaniem tego typu interfejsu możliwe jest tworzenie rozwiązań biznesowych, które wspierają bezpośrednią komunikację z bankiem. Dedykowane API stanowią również trzon komunikacji z istniejącymi już na rynku systemami płatności.

Wejście w życie regulacji PSD2 wprowadza drugi sposób integracji oparty o zunifikowane API. W przypadku rynku polskiego jest to standard PolishApi będący implementacją (operacjonalizacją) dyrektywy PSD2.

1.4 Bezpieczeństwo

Bezpieczeństwo usług dostępnych dzięki PSD2 realizowane jest na kilku płaszczyznach.

W płaszczyźnie formalnej, by zostać TPP nie wystarczy stworzyć usługi zgodnej z interfejsami XS2A. TPP co do zasady podlega zgłoszeniu i weryfikacji, która po pozytywnym przebiegu skutkuje wydaniem odpowiedniego certyfikatu, który determinuje również w jakich rolach dany TPP może występować.

Na płaszczyźnie technicznej, by umożliwić komunikację z bankami, podmioty TPP muszą zostać poprawnie uwierzytelnione przed udzieleniem im dostępu do interfejsu XS2A tak, aby zapewnić wysoki poziom ochrony zarówno przed podszyciem się nieuprawnionych podmiotów pod właściwych TPP, jak i przed nieuprawnioną eskalacją poziomu autoryzacji przez TPP mających legalny dostęp do interfejsu

XS2A. Uwierzytelnienie następuje w oparciu o certyfikaty klucza publicznego w procesie wzajemnego uwierzytelnienia (Mutual authentication) za pomocą protokołu TLS 1.2+

Autoryzacja TPP w stosowanym przez Bank modelu musi być oparta na modelu RBAC (Role Based Access Control), w którym poziom i zakres dostępu do poszczególnych zasobów API zależy od roli użytkownika PolishAPI.

Niezależnie od zastosowanego mechanizmu uwierzytelniania PSU (klient, użytkownik końcowy) w ramach usług AIS i PIS zakłada się, iż proces ten kończy się wydaniem przez ASPSP access tokenu. Zlecanie operacji przez TPP odbywa się zawsze z wykorzystaniem ważnego access tokenu.

2 Realizacja wymagań PSD2 w zakresie API w Credit Agricole Bank Polska SA

2.1 Informacje ogólne

API XS2A udostępniane przez Bank to produkt umożliwiający TPP zainicjowanie płatności, pobieranie danych dotyczących rachunków płatniczych prowadzonych przez Bank oraz potwierdzenie dostępności kwoty na rachunku w zakresie wymaganym przez znowelizowaną ustawę o usługach płatniczych i określonym przez standard PolishAPI.

https://polishapi.org/dokumentacja-standardu/

Dokumentacja techniczna usług z instrukcją ich świadczenia zamieszczona jest w Serwisie informacyjnym API Portal dostępnym pod adresem https://www.credit-agricole.pl/apiportal.

Uwaga

Każdy podmiot chcący rozpocząć korzystanie z API w zakresie świadczenia usług wprowadzonych zgodnie z Dyrektywą PSD2 do ustawy o usługach płatniczych, musi być uprzednio zarejestrowana w przynajmniej jednym rejestrze w kraju członkowskim Unii Europejskiej w roli, w jakiej chce występować w tym procesie. Musi również posiadać ważny certyfikat służący do identyfikacji przez banki w procesie komunikacji. Certyfikat wydają kwalifikowani dostawcy usług zaufania.

2.2 Bezpieczeństwo

Udostępnione przez Bank rozwiązanie zapewnia:

- Najwyższy poziom bezpieczeństwa w procesie uwierzytelnienia i autoryzacji żądania TPP poprzez wykorzystanie tokenów oraz certyfikatów kwalifikowanych,
- Poufność przesyłanych danych, gwarantowaną przez zastosowanie bezpiecznego protokołu SSL/TLS do zabezpieczenia kanału transmisji,
- Autoryzację zgód na wywołania usług PolishAPI, zrealizowaną w oparciu o przepływy autoryzacyjne zdefiniowane w PolishAPI.
- Przechowywane zgód klienta w odpowiednio zabezpieczonej bazie autoryzacyjnej.
- Weryfikację każdego żądania przesyłanego od TPP w zakresie usług AIS/PIS/CAF zdefiniowanych w PolishAPI, pod kątem zgód udzielonych przez klienta oraz względem podpisów komunikatów w celu zapewnienia ich niezaprzeczalności.

2.3 Zakres usług

Udostępnione przez Bank API XS2A jest zgodne ze specyfikacją standardu PolishAPI w wersji 3.0.

Rozwiązanie umożliwia:

- Autoryzację klienta dla operacji wykonywanych przez TPP w zakresie:
    - Uprawnień do pobierania listy rachunków
    - Uprawnień do pobierania informacji o jednym lub wielu wskazanych przez klienta rachunkach
    - Uprawnień do zainicjowania pojedynczej płatności lub wielu płatności w postaci paczki oraz do pobierania informacji o statusie zainicjowanych płatności oraz paczki płatności

- Pobranie informacji o rachunkach płatniczych w zakresie:
    - Listy wszystkich rachunków klienta
    - Szczegółowych informacji o konkretnym rachunku
    - Informacji o transakcjach w podziale na ich typy
    - Szczegółowych informacji o konkretnej transakcji

- Obsługę zleceń płatniczych w zakresie:
    - Zlecania płatności krajowych
    - Zlecania płatności zagranicznych
    - Zlecania płatności do urzędu podatkowego
    - Zlecania paczek płatności danego typu
    - Pobierania informacji o statusach pojedynczych płatności, wielu płatności w jednym zapytaniu oraz o paczkach płatności
    - Usuwania zleceń płatności z datą przyszłą

- Obsługę zapytań o dostępność środków na rachunku płatniczym

2.4 Warianty API XS2A

Bank udostępnia dwa warianty API zorientowane na dostęp do dwóch różnych segmentów działalności :

- obsługi klientów indywidualnych oraz małych i średnich przedsiębiorstw - API XS2A Retail https://xs2a.credit-agricole.pl/CaPolishAPI/prod/individual/,
- obsługi klientów korporacyjnych – API XS2A Corpo https://xs2a.credit-agricole.pl/CaPolishAPI/prod/corporate/.

3 Środowisko testowe

Bank udostępnia TPP oraz dostawcom usług płatniczych, którzy ubiegają się o status TPP (złożyli do właściwych organów wniosek o stosowne zezwolenie/wpis do rejestru) środowisko pozwalające na funkcjonalne testy udostępnianych API XS2A (Piaskownica PSD2).

3.1 Informacje ogólne

Piaskownica PSD2 jest wydzielonym środowiskiem informatycznym w ramach systemu IT Banku, w ramach którego Użytkownik ma możliwość samodzielnego testowania udostępnionych przez Bank API XS2A.

Dane dostępne w Piaskownicy PSD2 są to dane statyczne, przygotowane specjalnie na potrzeby testów. Dane umożliwiają przetestowanie wszystkich udostępnionych usług zgodnie z przygotowanymi przez Bank scenariuszami.

Piaskownica PSD2 nie implementuje wszystkich funkcji bezpieczeństwa zapewnianych na środowisku rzeczywistym, m.in. weryfikacji kwalifikowanego certyfikatu TPP (ze specjalnymi atrybutami roli PSD2), limitów transakcji, uprawnień klienta, mechanizmów anti-fraud itp.

3.2 Dostęp do środowiska

Uwierzytelnienie w Piaskownicy PSD2 następuje w oparciu o certyfikaty klucza publicznego w procesie wzajemnego uwierzytelnienia (Mutual authentication) za pomocą protokołu TLS 1.2+. W przypadku Piaskownicy, TPP stosuje certyfikat niekwalifikowany, zgodny co do formatu ze specyfikacją techniczną „ETSI TS 119 495".

Nadanie dostępu do Piaskownicy PSD2 polega na wydaniu zestawu certyfikatów oraz instrukcji połączenia ze środowiskiem testowym.

3.2.1 Certyfikaty

- Certyfikaty służące do uwierzytelniania się klientów usług Piaskownicy PSD2 są wydawane przez Bank.
- Certyfikaty na potrzeby testów wydawane są na okres 6 miesięcy (w przypadku podmiotów, które udokumentują ubieganie się o status TPP) oraz na okres 12 miesięcy w przypadku podmiotów o statusie TPP.
- Certyfikaty pozwalają na testy wszystkich usług, niezależnie od faktycznej roli TPP.

3.2.2 Wydanie certyfikatu

W celu otrzymania dostępu do Piaskownicy PSD2 należy:

- Wypełnić formularz dostępny na stronie Serwisu,
- Wysłać wypełniony i podpisany kwalifikowanym podpisem elektronicznym dokument pocztą elektroniczną na adres, apiportal@credit-agricole.pl

W przypadku spełnienia przez Użytkownika wymogów formalnych, Bank dostarczy instrukcję połączenia oraz certyfikat testowy w terminie 5 dni roboczych od momentu złożenia przez Użytkownika kompletnego wniosku.

3.2.3 Anulowanie certyfikatu

Certyfikat wydany przez Bank na potrzeby testów może być anulowany ze względu na:

- zabranie Użytkownikowi dostępu do dokumentacji PSD2 wynikające np. z utraty przez organizację, którą reprezentuje statusu TPP,
- wykrycie naruszenia przez użytkownika Piaskownicy PSD2 reguł bezpieczeństwa (np. próby przełamywania mechanizmów zabezpieczeń),
- wykrycie kompromitacji certyfikatu,
- z innych względów - na żądanie Użytkownika Piaskownicy PSD2.

3.3 Reguły bezpieczeństwa

Zabronione jest korzystanie z Piaskownicy PSD2 w sposób inny, niż opisany w dokumentacji. W szczególności zabronione jest testowanie mechanizmów bezpieczeństwa zaimplementowanych przez Bank w sposób niedozwolony i próby ich przełamywania.

Bank jest uprawniony do stosowania środków technicznych i organizacyjnych w celu przeciwdziałania manipulacjom w zakresie korzystania z Piaskownicy.

Bank może zablokować Użytkownikowi dostęp do Piaskownicy w przypadku uzasadnionego podejrzenia wystąpienia oszustwa lub wystąpienia zagrożeń dla bezpieczeństwa funkcjonowania Piaskownicy, związanych z korzystaniem przez Użytkownika z Piaskownicy w niedozwolony sposób.

Odpowiedzialność za ewentualne naruszenia powszechnie obowiązującego prawa oraz praw osób trzecich, wynikłe z korzystania z Serwisu, w szczególności niezgodnie z jego testowym przeznaczeniem, spoczywa w pełni na korzystającym z Serwisu Użytkowniku.

3.4 Warunki techniczne i dostępność

Bank zakłada dostępność Piaskownicy (AST) na poziomie 90% w skali miesiąca kalendarzowego.

Liczba zapytań pochodzących od konkretnego użytkownika może być limitowana w jednostce czasu (Bank gwarantuje realizację nie mniej niż 10 zapytań na sekundę).

Ze względu na testowy charakter środowiska, jego wydajność nie odpowiada wydajności środowiska rzeczywistego i nie może być podstawą do roszczeń oraz nie może służyć do prowadzenia na nim testów wydajnościowych.

4 Wsparcie

Bank świadczy wsparcie techniczne i biznesowe w dni robocze w godzinach od 9:00 do 17:00.

Zgłoszenia należy kierować w języku polskim lub angielskim na adresy:

- API_PSD2@credit-agricole.pl – w przypadku błędów oraz problemów technicznych związanych z API oraz Piaskownicą PSD2 w tym problemów z dostępnością interfejsów;
- apiportal@credit-agricole.pl - w przypadku pozostałych pytań związanych z wdrożonym przez Credit Agricole rozwiązaniem w tym pytań dotyczących dokumentacji oraz certyfikatów wydanych przez Bank na potrzeby testów w Piaskownicy;

Bank dołoży należytej staranności, aby użytkownik otrzymał odpowiedź na zapytanie w terminie nie dłuższym niż 10 dni roboczych.

5 Logotypy

Credit Agricole Bank Polska S.A. („Bank") w ramach świadczenia usług inicjacji płatności oraz dostępu do informacji o rachunku, celem umożliwienia odniesienia się do usług Banku jako właściciela znaku towarowego, udostępnia swoje znaki towarowe w formie znajdującej się w Serwisie informacyjnym API Portal (https://www.credit-agricole.pl/apiportal).

Bank wyraża zgodę na informacyjne użycie znaku towarowego na potrzeby świadczenia usług PIS i AIS, bez konieczności uzyskiwania licencji na korzystanie ze znaków towarowych Banku, o ile jest to niezbędne do świadczenia usług przez podmiot trzeci (o statusie dostawcy usług płatniczych, o którym mowa w art. 2 pkt 4b-4f ustawy o usługach płatniczych). Bank nie wyraża zgody na użytkowanie zmodyfikowanej w jakikolwiek sposób wersji znaku, w tym w szczególności zmiany koloru, proporcji, kształtu czy połączenia znaku towarowego Banku z innym znakiem towarowym. Jedyną dopuszczalną formą korzystania ze znaku jest forma określona w dokumentacji interfejsu dostępowego Banku.

Jednocześnie Bank zastrzega, że zakazuje korzystania ze swojego znaku towarowego w sposób, który sugerowałby istnienie powiązań pomiędzy Bankiem a danym TPP czy też promowanie usług TPP z wykorzystaniem znaku towarowego Banku.