PolishAPI

Specyfikacja interfejsu na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych

Dokument opracowany przez Grupę Projektową ds. PolishAPI

17 kwietnia 2018
Wersja 1.0.0

Licencja

Spis treści

Spis ilustracji

1 Wstęp

1.1 Kontekst

Wdrożenie przez Unię Europejską nowej dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD2) wprowadza możliwość oferowania nowych produktów i usług związanych nie tylko z rynkiem usług płatniczych, ale także szerzej rozumianym rynkiem usług finansowych. Zarówno podmioty będące obecne na tym rynku, takie jak banki, Spółdzielcze Kasy Oszczędnościowo-Kredytowe czy oddziały zagranicznych instytucji kredytowych, ale także nowe rodzaje podmiotów (dostawcy będący stroną trzecią, Third Party Providers, TPP) będą mogły wykorzystać możliwość oferowania nowych usług budowanych w oparciu o PSD2, akty wykonawcze (w tym Regulacyjne Standardy Techniczne – RTS) i akty prawa krajowego. Nowymi kategoriami usług są:

a) **Account Information Service (AIS)** – usługa dostępu do informacji o rachunku, zdefiniowana w art. 67 PSD2
b) **Payment Initiation Service (PIS)** – usługa inicjowania transakcji płatniczej, zdefiniowana w art. 66 PSD2
c) **Confirmation of the Availability of Funds (CAF)** – usługa potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej, zdefiniowana w art. 65 PSD2

Umożliwienie realizacji powyższych usług przez podmioty do tego uprawnione wymaga przygotowania przez dostawców prowadzących rachunek (ASPSP) dedykowanych interfejsów umożliwiających dostęp do rachunków płatniczych (interfejs XS2A) przez uprawione do tego strony trzecie (TPP), opartych o otwarte API.

Banki oraz inne podmioty współpracujące w ramach Związku Banków Polskich podjęły decyzję o stworzeniu wspólnego, uniwersalnego standardu API, wykorzystującego dotychczasowe osiągnięcia polskiego sektora bankowego i płatniczego, najlepsze praktyki i doświadczenia, w tym z zagranicznych standardów API, oraz istniejące już interfejsy w ramach infrastruktury międzybankowej. Standard ten będzie mógł być wdrożony przez banki oraz inne ASPSP, zgodne z niezależnie podjętymi decyzjami biznesowymi. W ramach prac grup biznesowej, IT i bezpieczeństwa oraz prawnej, powstały założenia, a następnie opis standardu, przedstawiony w niniejszym dokumencie.

Jako podstawę do niniejszej wersji standardu przyjęto Rozporządzenie Delegowane w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (RTS), opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 13 marca 2018 roku (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.POL&toc=OJ:L:2018:069:TOC).

W tworzeniu niniejszego standardu brały udział następujące podmioty (wymienione w kolejności alfabetycznej):

1) Allegro Group
2) Biuro Informacji Kredytowej S.A.
3) Billbird S.A.
4) Blue Media S.A.
5) Diners Club Polska
6) Krajowa Izba Rozliczeniowa S.A.
7) Kontomierz.pl Sp. z o.o.
8) Krajowa Kasa Oszczędnościowo – Kredytowa
9) Krajowy Związek Banków Spółdzielczych
10) PayU S.A.
11) Polska Izba Informatyki i Telekomunikacji

12) Polska Izba Ubezpieczeń
13) Polski Standard Płatności Sp. z o.o.
14) Polska Organizacja Niebankowych Instytucji Płatności
15) Skycash Poland S.A.
16) Spółdzielcza Kasa Oszczędnościowo – Kredytowa im. F. Stefczyka
17) Związek Banków Polskich wraz ze stowarzyszonymi bankami[1]

Projekt specyfikacji był poddany konsultacjom publicznym (w dn. 17-31 stycznia 2018), w wyniku których 21 podmiotów polskich i zagranicznych przekazało ok. 300 uwag i komentarzy, częściowo uwzględnionych w niniejszym dokumencie.

1.2 Struktura dokumentu

Dokument składa się z dwóch zasadniczych części oraz załączników:

a) Części dotyczącej charakterystyki biznesowej Standardu PolishAPI (rozdziały 1 – 4)
b) Części dotyczącej rozwiązań technologicznych przyjętych w standardzie PolishAPI (rozdziały 5 – 13)
c) Załączników, których spis znajduje się w rozdziale 14

1.3 Misja Standardu PolishAPI

Głównym celem dokumentu jest zdefiniowanie interfejsów dla usług opisanych w PSD2 oraz powiązanych aktach prawnych, w zakresie interakcji pomiędzy ASPSP a TPP podczas realizacji usług AIS, PIS oraz CAF. Wymóg pojawienia się otwartych API daje również szansę, aby w ramach jednego standardu ASPSP oraz TPP miały możliwość zaoferowania nie tylko usług wymaganych przepisami prawa, ale także dodatkowych usług, które swoim zakresem wykraczają poza ramy wyznaczone przez prawodawcę. Możemy zatem wyróżnić następujące zakresy usług w ramach standardu PolishAPI:

a) **Zakres Zgodności** w ramach usług AIS, PIS i CAF - usługi wymagane przez PSD2
b) **Zakres Premium** w ramach usług AIS, PIS i CAF - usługi wykraczające poza wymogi PSD2, poza zakresem niniejszego dokumentu

Każdy ASPSP i TPP może skorzystać ze standardu PolishAPI jak z otwartego standardu. Korzystanie ze standardu nie jest obowiązkowe. Każdy z podmiotów działających na rynku w oparciu o dyrektywę PSD2, może stosować dowolne rozwiązanie, zgodne z PSD2 oraz powiązanymi aktami prawnymi.

Interakcje występujące pomiędzy TPP a PSU oraz ASPSP oraz PSU, a także zagadnienia związane z procesami wpisów do rejestru krajowego TPP, udzielania zezwolenia na działalność TPP w zakresie usług związanych z PSD2 przez organy administracji publicznej nie mieszczą się w zakresie niniejszego dokumentu.

Część zagadnień, pozostających w zakresie specyfikacji standardu, będzie do niego systematycznie dodawana w miarę prowadzenia prac projektowych i uzgodnieniowych (w tym konsultacji publicznych). Powyższe zastrzeżenie odnosi się m.in. do zagadnień związanych ze specyficznymi funkcjonalnościami dla rachunków korporacyjnych oraz szczegółami technicznymi dotyczącymi metod uwierzytelniania, opisanych w rozdziale 1.4.3.

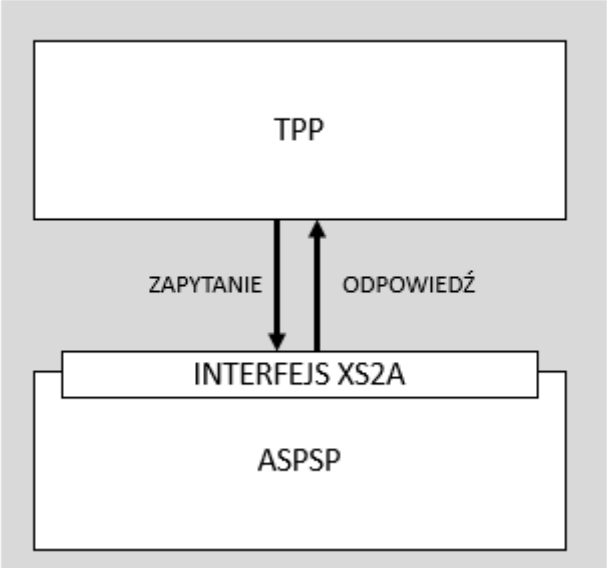
[1] Alior Bank S.A., Bank BGŻ BNP Paribas S.A., Bank Handlowy w Warszawie S.A., Bank Millennium S.A., Bank Pekao S.A., Bank Pocztowy S.A., Bank Polskiej Spółdzielczości S.A., Bank Zachodni WBK S.A., Credit Agricole Bank Polska S.A., Deutsche Bank Polska S.A., DNB Bank Polska S.A., Eurobank S.A., Getin Noble Bank S.A., Idea Bank S.A., ING Bank Śląski S.A., mBank S.A., Nest Bank S.A., PKO Bank Polski S.A., Raiffeisen Bank Polska S.A., SGB-Bank S.A.

1.4 Główne założenia

1.4.1 Aktorzy w procesach definiowanych w standardzie PolishAPI

Standard definiuje wyłącznie trzy kategorie aktorów, którzy mogą wziąć udział w procesach definiowanych w standardzie PolishAPI:

a) **Payment Service User (PSU)** – Użytkownik rachunku płatniczego, którego dotyczy dana transakcja płatnicza
b) **Account Servicing Payment Service Provider (ASPSP)** – Dostawca prowadzący rachunek płatniczy i udostępniający interfejs XS2A dla TPP
c) **Third Party Provider (TPP)** – Podmiot korzystający z interfejsu XS2A na podstawie i w ramach zgód wyrażonych przez PSU. ASPSP może występować również jako TPP i korzystać z interfejsów wystawionych przez inne ASPSP



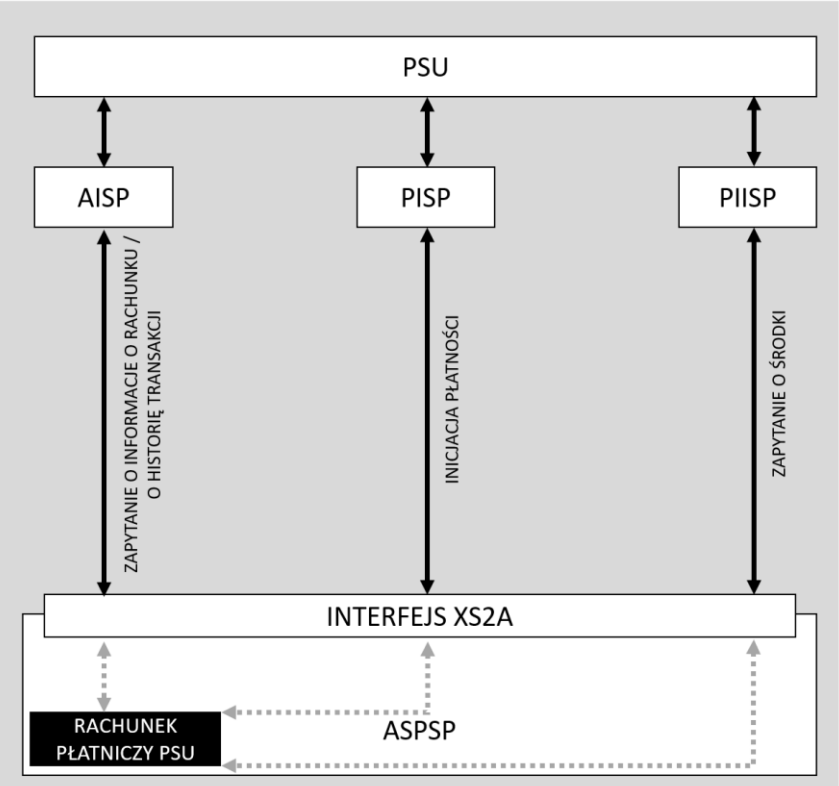
Ilustracja 1: Ogólny schemat komunikacji w Standardzie PolishAPI

Standard definiuje trzy role, w których mogą występować aktorzy biorący udział w procesach zdefiniowanych w ramach standardu PolishAPI. Poniższa kategoryzacja nie ogranicza podmiotów występujących w roli TPP do ubiegania się o wpis do rejestru krajowego w więcej niż jednej roli, a ma na celu jedynie zdefiniowanie ról poszczególnych aktorów w opisie komunikacji w ramach standardu PolishAPI.

a) **Account Information Service Provider (AISP)** - Dostawca Świadczący Usługę Dostępu do Informacji o Rachunku – TPP używające interfejsu XS2A w celu dostępu do informacji o rachunku płatniczym PSU.
b) **Payment Initiation Service Provider (PISP)** – Dostawca Świadczący Usługę Inicjowania Transakcji Płatniczej – TPP używające interfejsu XS2A w celu inicjacji transakcji płatniczej w ciężar rachunku PSU.
c) **Payment Instrument Issuer Service Provider (PIISP**) – Dostawca Wydający Instrumenty Płatnicze Oparte na Karcie – TPP używające interfejsu XS2A w celu potwierdzania dostępności na rachunku płatniczym PSU kwoty niezbędnej do wykonania transakcji płatniczej realizowanej w oparciu o instrument wydany przez PIISP.

Aktorzy mogą występować w następujących rolach:

Aktor / Rola	PSU	ASPSP	TPP
AISP	NIE	TAK	TAK
PISP	NIE	TAK	TAK
PIISP	NIE	TAK	TAK



Ilustracja 2: Ogólny schemat zależności pomiędzy aktorami w Standardzie PolishAPI

1.4.2 Wymagania dot. aktorów w procesach definiowanych w standardzie PolishAPI

a) ASPSP musi wdrożyć interfejs XS2A zgodny ze standardem PolishAPI. ASPSP może wdrożyć również inne standardy interfejsów XS2A, nie są one jednak objęte zakresem niniejszego dokumentu
b) Interfejsy wdrożone przez ASPSP muszą być zgodne z PSD2, Ustawą o Usługach Płatniczych oraz aktami powiązanymi, w szczególności z RTS-ami
c) TPP musi być zarejestrowane w przynajmniej jednym rejestrze w kraju członkowskim Unii Europejskiej w roli, w której chce występować podczas realizacji komunikacji opartej na standardzie PolishAPI
d) TPP musi posiadać ważny certyfikat, służący do identyfikacji w interfejsie XS2A, otrzymany od kwalifikowanego dostawcy usług zaufania, spełniającego wymogi ustawy o usługach zaufania oraz identyfikacji elektronicznej. Certyfikat ten dodatkowo powinien spełniać wymagania zdefiniowane w RTS oraz specyfikacji technicznej ETSI (TS 119 495)

1.4.3 Mechanizmy uwierzytelniania PSU

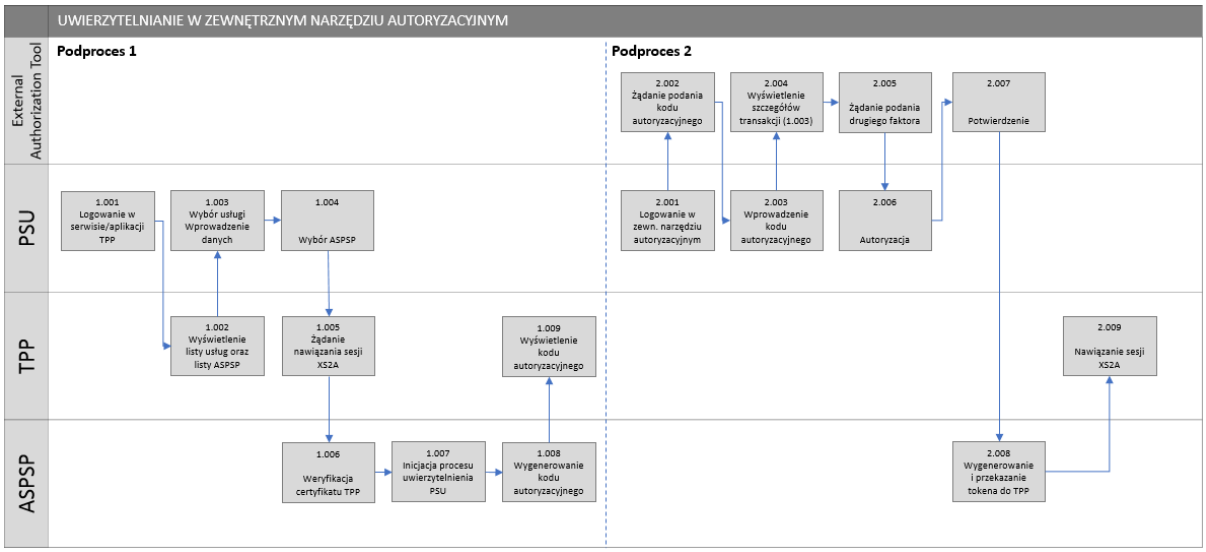
Standard PolishAPI dopuszcza poniższe mechanizmy uwierzytelnienia PSU. Wybór mechanizmów pozostaje wyłącznie w gestii ASPSP. Wybór ten powinien być zgodny z obowiązującymi regulacjami.

1.4.3.1 Mechanizm uwierzytelniania po stronie ASPSP

Standard PolishAPI dopuszcza wykorzystanie mechanizmu uwierzytelniania po stronie ASPSP, zakładającego przekierowanie na stronę internetową ASPSP podczas realizowania usług AIS, PIS i CAF, co oznacza, że dane uwierzytelniające i autoryzacyjne PSU podawane są wyłącznie na stronie internetowej ASPSP. Uwierzytelnienie PSU przeprowadzane jest w interfejsie ASPSP.

1.4.3.2 Mechanizm uwierzytelniania w zewnętrznym narzędziu autoryzacyjnym (decoupled)

Standard PolishAPI dopuszcza wykorzystanie mechanizmu uwierzytelniania w zewnętrznym narzędziu autoryzacyjnym podczas realizowania usług AIS, PIS i CAF. Mechanizm uwierzytelniania w zewnętrznym narzędziu autoryzacyjnym został wysokopoziomowo przedstawiony na poniższym diagramie. Szczegóły dotyczące jego wykorzystania zostaną uzupełnione w kolejnej wersji niniejszego dokumentu.



Ilustracja 3: Uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym

1.4.3.3 Inne mechanizmy uwierzytelniające

W standardzie mogą zostać opisane inne, spełniające wymogi regulacyjne oraz uzgodnione w ramach prac grupy projektowej mechanizmy uwierzytelniania. Publikowane będą w kolejnych wersjach niniejszego dokumentu.

1.4.4 Zarządzanie zgodami PSU na wykonywanie usług przez TPP

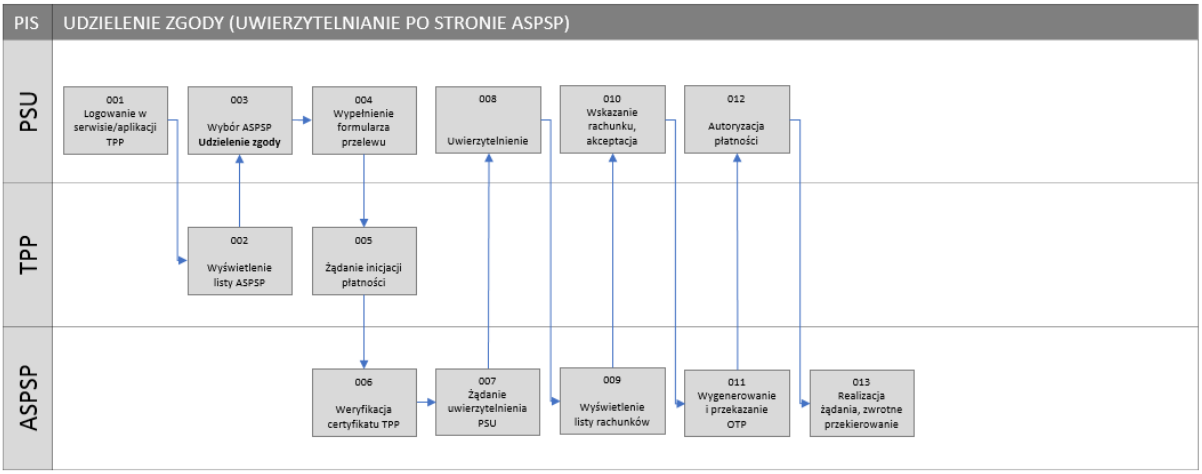
Zgodnie z PSD2, TPP może wykonywać usługi na rzecz PSU jedynie za jego zgodą i w zakresie objętym tą zgodą. Standard PolishAPI definiuje ramy udzielania oraz odwoływania zgód przez PSU.

1.4.4.1 Proces udzielenia zgody PSU na wykonanie usługi PIS

Zakłada się, że realizacja procesu inicjacji płatności za każdym razem jest związana z udzieleniem na to zgody przez PSU w ramach interfejsu TPP.

1.4.4.1.1 Opcja w przypadku użycia mechanizmu uwierzytelniania po stronie ASPSP

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz udziela TPP zgody na świadczenie usługi PIS
- 004 / PSU wypełnia formularz przelewu, który powinien zawierać przynajmniej informacje, wskazane w rozdziale 3.1.3 niniejszej specyfikacji: „Lista pól wymaganych przez ASPSP w zakresie Zgodności”
- 005 / TPP przekazuje do ASPSP żądanie inicjacji płatności i następuje przekierowanie do domeny ASPSP w celu dokonania uwierzytelnienia PSU
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP przesyła żądanie uwierzytelnia PSU
- 008 / Uwierzytelnienie
- 009 / ASPSP prezentuje PSU do wyboru listę rachunków płatniczych, z których możliwe jest zainicjowanie transakcji płatniczej
- 010 / PSU wybiera jeden rachunek z listy i akceptuje transakcję
- 011 / ASPSP generuje i przekazuje PSU dodatkowy element autoryzacyjny (np. OTP) – o ile jest to wymagane zgodnie z obowiązującymi regulacjami
- 012 / PSU autoryzuje transakcję wg metody stosowanej w relacjach z ASPSP (PSU ma możliwość niedokonania autoryzacji, co skutkuje niezrealizowaniem transakcji płatniczej)
- 013 / ASPSP realizuje żądanie, następuje przekierowanie do domeny TPP



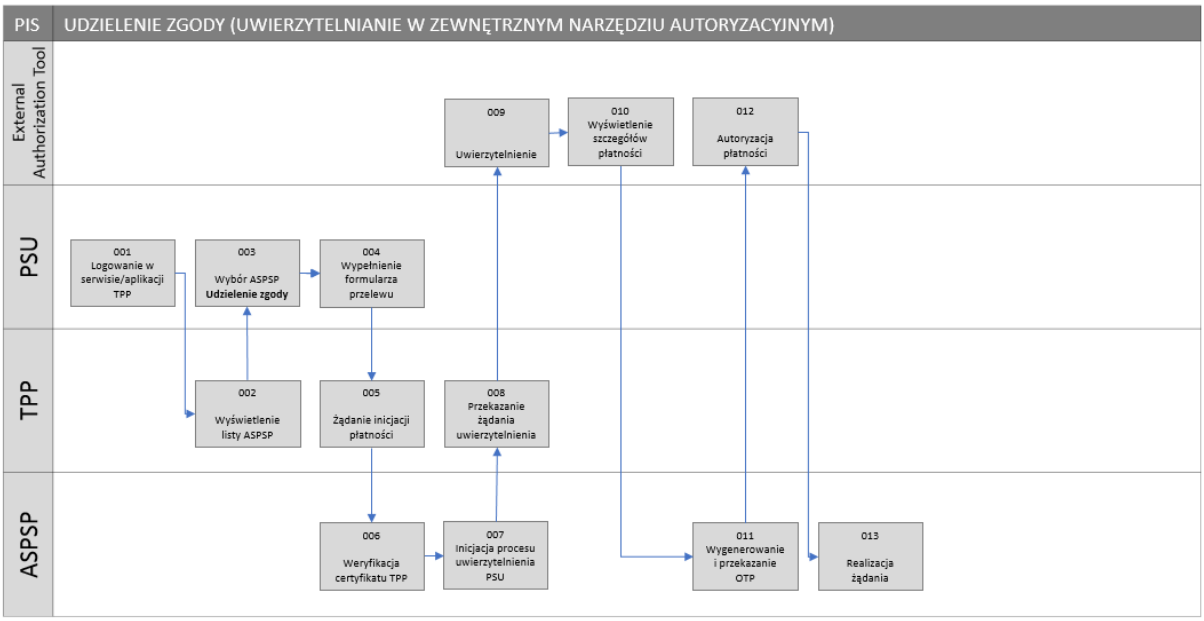
Ilustracja 4: PIS. Udzielenie zgody (uwierzytelnianie po stronie ASPSP)

1.4.4.1.2 Opcja w przypadku użycia mechanizmu uwierzytelniania w zewnętrznym mechanizmie autoryzacyjnym

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz udziela TPP zgody na świadczenie usługi PIS
- 004 / PSU wypełnia formularz przelewu, który powinien zawierać przynajmniej informacje, wskazane w rozdziale 3.1.3 niniejszej specyfikacji: „Lista pól wymaganych przez ASPSP

w zakresie Zgodności" (w tym podaje numer rachunku, z którego płatność ma być zainicjowana)

- 005 / TPP przekazuje do ASPSP żądanie inicjacji płatności
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP inicjuje proces uwierzytelnienia PSU
- 008 / TPP przekazuje PSU żądanie uwierzytelnienia
- 009 / Uwierzytelnienie w zewnętrznym narzędziu autoryzacyjnym (por. pkt. 1.4.3.2)
- 010 / W zewnętrznym narzędziu autoryzacyjnym wyświetlane są szczegóły płatności, PSU akceptuje transakcję
- 011 / ASPSP generuje i przekazuje PSU dodatkowy element autoryzacyjny (np. OTP) – o ile jest to wymagane zgodnie z obowiązującymi regulacjami
- 012 / PSU autoryzuje płatność (PSU ma możliwość niedokonania autoryzacji, co skutkuje niezrealizowaniem transakcji płatniczej)
- 013 / ASPSP realizuje żądanie



Ilustracja 5: PIS. Udzielenie zgody (uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym)

1.4.4.2 Proces udzielenia zgody PSU na wykonanie usługi AIS

W poniższym rozdziale termin zgoda odnosi się wyłącznie do świadczenia usług AIS i oznacza wyrażenie zgody na usługę, bez wskazywania konkretnych rachunków (w przypadku opcji z pobraniem listy rachunków) lub z ich wskazaniem (w przypadku opcji z ręcznym wprowadzeniem numeru rachunku). Proces ten zawsze łączy się z silnym uwierzytelnianiem klienta (SCA).
Określenie parametrów dostępu (w przypadku opcji z pobraniem listy rachunków) oznacza każdą operację na konkretnych rachunkach w ramach zgody na świadczenie usług AIS, w tym:

- wskazanie konkretnego rachunku
- zmianę parametrów dla konkretnego rachunku (np. daty dostępu)
- cofnięcie wskazania konkretnego rachunku lub
- cofnięcie zgody

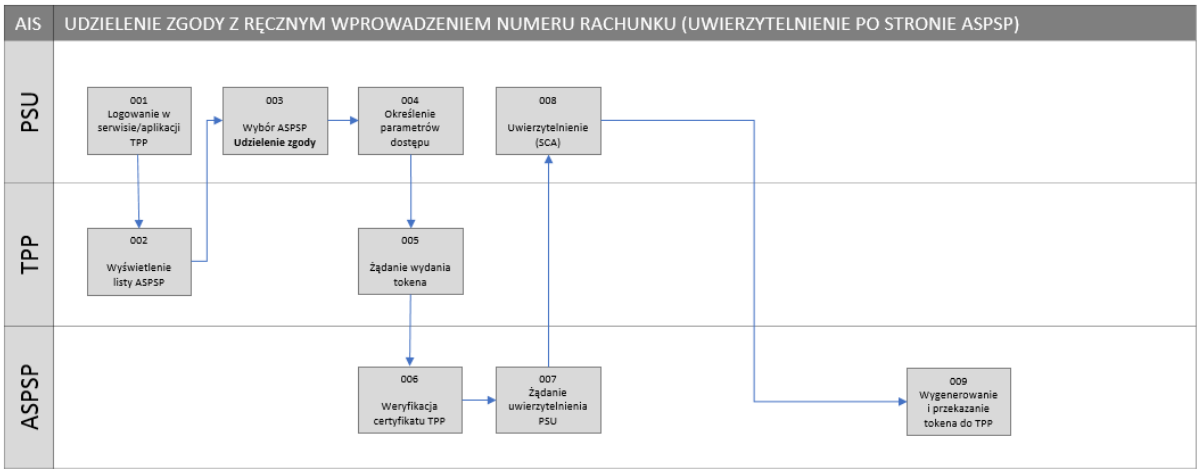
Operacje te nie wymagają silnego uwierzytelnienia klienta (SCA).

Standard dopuszcza dwa procesy udzielania zgody na usługę AIS (w opcjach uwzględniających uwierzytelnianie po stronie ASPSP oraz w zewnętrznym narzędziu autoryzacyjnym) opisane w pkt. od 1.4.4.2.1 do 1.4.4.2.4. ASPSP może zaimplementować jeden lub oba procesy.

1.4.4.2.1 Udzielenie zgody z ręcznym wprowadzeniem numeru rachunku w przypadku uwierzytelnienia po stronie ASPSP

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz wyraża dla danego TPP zgodę na świadczenie usługi dostępu do informacji o rachunku prowadzonym przez danego ASPSP
- 004 / PSU wprowadza numer rachunku (-ów) oraz określa zakres dostępu
- 005 / TPP wysyła do ASPSP żądanie wydania tokena
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP przesyła żądanie uwierzytelnia PSU
- 008 / Uwierzytelnienie SCA
- 009 / ASPSP przekazuje do TPP token dostępowy (zawierający informacje o zakresie dostępu), w przypadku AIS wielokrotnej wraz z refresh tokenem

W przypadku, gdy wprowadzony numer rachunku lub jeden lub więcej z wielu wprowadzonych numerów rachunku jest błędny lub dostęp do niego nie może być udzielony, zwrócony zostanie komunikat błędu 400.



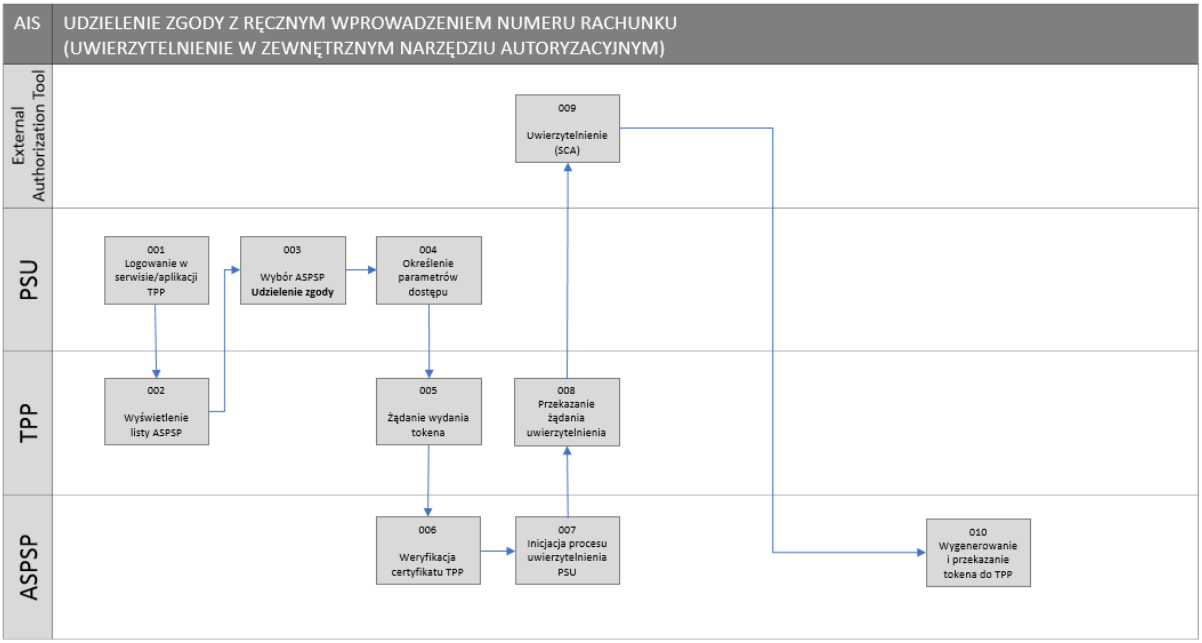
Ilustracja 6: AIS. Udzielenie zgody z ręcznym wprowadzeniem numeru rachunku (uwierzytelnienie po stronie ASPSP)

1.4.4.2.2 Udzielenie zgody z ręcznym wprowadzeniem numeru rachunku w przypadku uwierzytelnienia w zewnętrznym narzędziu autoryzacyjnym

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz wyraża dla danego TPP zgodę na świadczenie usługi dostępu do informacji o rachunku prowadzonym przez danego ASPSP
- 004 / PSU wprowadza numer rachunku (-ów) oraz określa zakres dostępu
- 005 / TPP wysyła do ASPSP żądanie wydania tokena
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP inicjuje proces uwierzytelniania PSU
- 008 / TPP przekazuje żądanie uwierzytelnienia do PSU
- 009 / Uwierzytelnienie SCA w zewnętrznym narzędziu autoryzacyjnym (por. pkt. 1.4.3.2)

- 010 / ASPSP przekazuje do TPP token dostępowy (zawierający informacje o zakresie dostępu), w przypadku AIS wielokrotnej wraz z refresh tokenem

W przypadku, gdy wprowadzony numer rachunku lub jeden lub więcej z wielu wprowadzonych numerów rachunku jest błędny lub dostęp do niego nie może być udzielony, zwrócony zostanie komunikat błędu 400.

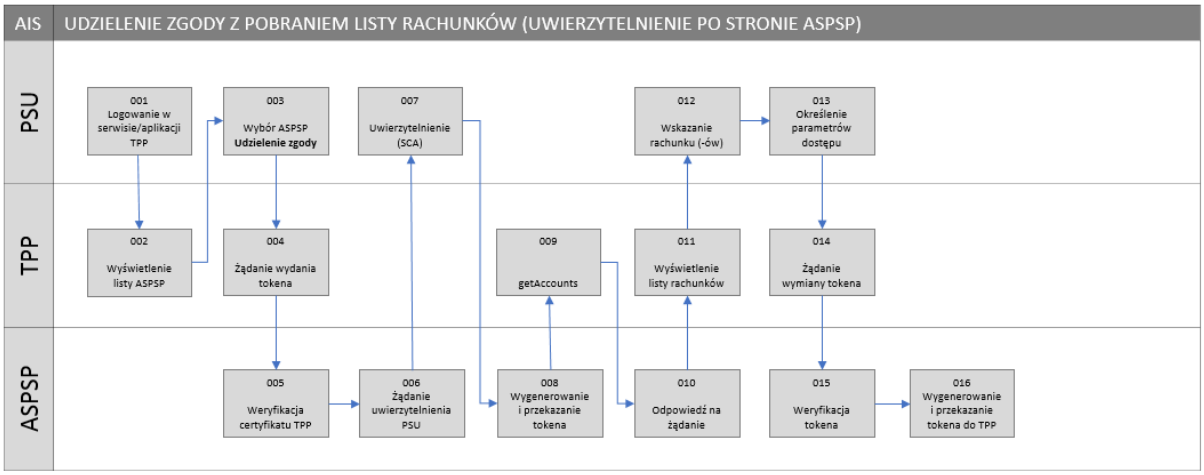


Ilustracja 7: AIS. Udzielenie zgody z ręcznym wprowadzeniem numeru rachunku (uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym)

1.4.4.2.3 Udzielenie zgody z pobraniem listy rachunków w przypadku uwierzytelnienia po stronie ASPSP

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz wyraża dla danego TPP zgodę na świadczenie usługi dostępu do informacji o rachunku prowadzonym przez danego ASPSP
- 004 / TPP wysyła do ASPSP żądanie wydania tokena
- 005 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 006 / ASPSP przesyła żądanie uwierzytelnia PSU
- 007 / Uwierzytelnienie SCA
- 008 / ASPSP przekazuje do TPP token dostępowy
- 009 / TPP wysyła do ASPSP żądanie przekazania listy rachunków PSU (wraz z tokenem dostępowym)
- 010 / ASPSP przekazuje TPP listę rachunków PSU (pełny albo częściowo maskowany numer rachunku + nazwa produktu + typ rachunku)
- 011 / TPP wyświetla listę rachunków
- 012 / PSU wskazuje rachunek (lub rachunki) w celu określenia zakresu dostępu
- 013 / PSU określa parametry dostępu
- 014 / TPP wysyła do ASPSP żądanie wymiany tokena (na token zawierający szczegóły dostępu)
- 015 / ASPSP weryfikuje tożsamość TPP oraz PSU (na podstawie pierwszego tokena dostępowego)

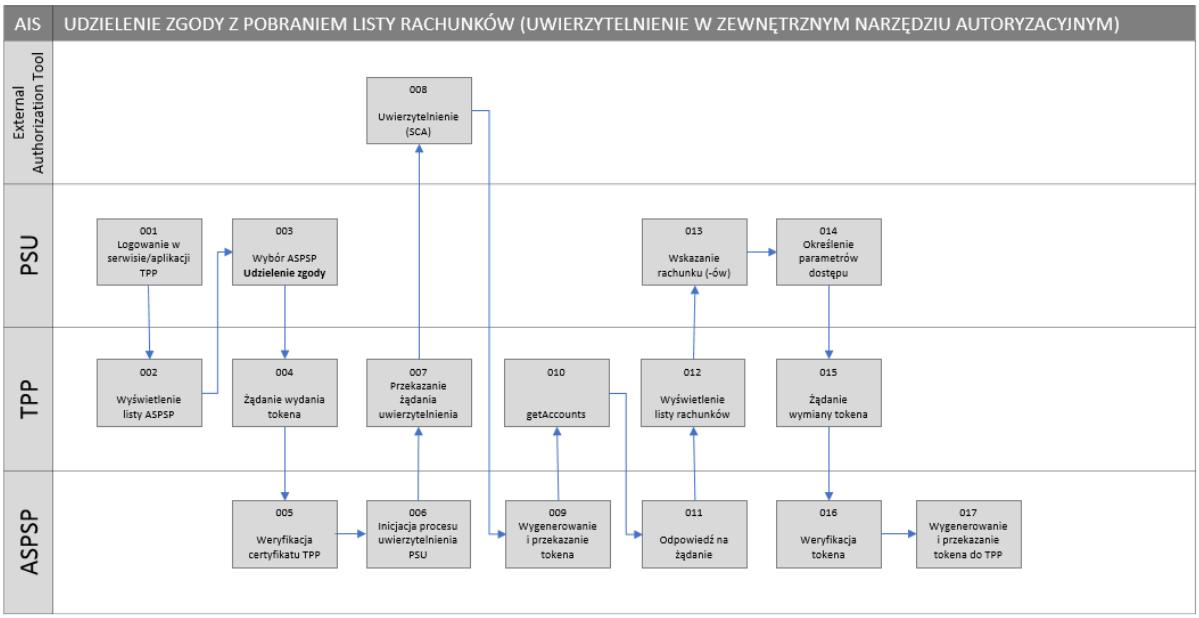
- 016 / ASPSP przekazuje do TPP nowy token dostępowy (zawierający informacje o zakresie dostępu), w przypadku AIS wielokrotnej wraz z refresh tokenem



Ilustracja 8: AIS. Udzielenie zgody z pobraniem listy rachunków (uwierzytelnianie po stronie ASPSP)

1.4.4.2.4 Udzielenie zgody z pobraniem listy rachunków w przypadku uwierzytelnienia w zewnętrznym narzędziu autoryzacyjnym

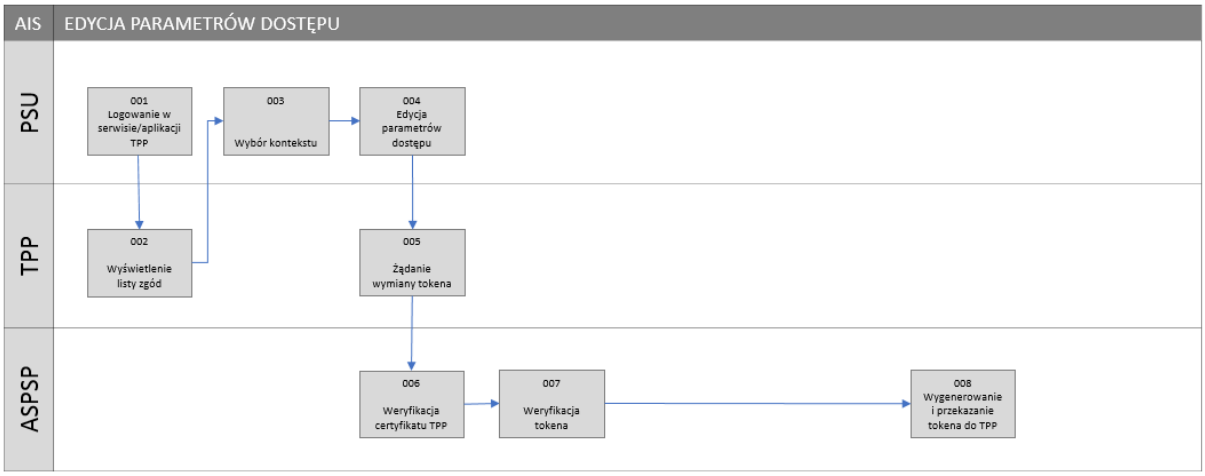
- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę ASPSP
- 003 / PSU wybiera z listy ASPSP oraz wyraża dla danego TPP zgodę na świadczenie usługi dostępu do informacji o rachunku prowadzonym przez danego ASPSP
- 004 / TPP wysyła do ASPSP żądanie wydania tokena
- 005 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 006 / ASPSP inicjuje proces uwierzytelnia PSU
- 007 / TPP przekazuje żądanie uwierzytelnienia do PSU
- 008 / Uwierzytelnienie SCA w zewnętrznym narzędziu autoryzacyjnym (por. pkt. 1.4.3.2)
- 009 / ASPSP przekazuje do TPP token dostępowy
- 010 / TPP wysyła do ASPSP żądanie przekazania listy rachunków PSU (wraz z tokenem dostępowym)
- 011 / ASPSP przekazuje TPP listę rachunków PSU (pełny albo częściowo maskowany numer rachunku + nazwa produktu + typ rachunku)
- 012 / TPP wyświetla listę rachunków
- 013 / PSU wskazuje rachunek (lub rachunki) w celu określenia zakresu dostępu
- 014 / PSU określa parametry dostępu
- 015 / TPP wysyła do ASPSP żądanie wymiany tokena (na token zawierający szczegóły dostępu)
- 016 / ASPSP weryfikuje tożsamość TPP oraz PSU (na podstawie pierwszego tokena dostępowego)
- 017 / ASPSP przekazuje do TPP nowy token dostępowy (zawierający informacje o zakresie dostępu), w przypadku AIS wielokrotnej wraz z refresh tokenem



Ilustracja 9: AIS. Udzielenie zgody z pobraniem listy rachunków (uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym)

1.4.4.2.5 Edycja parametrów dostępu

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę zgód
- 003 / PSU wybiera konkretną zgodę z listy zgód, w ramach której dokonane zostaną zmiany
- 004 / PSU wprowadza zmiany w ramach zgody (edytuje parametry dostępu)
- 005 / TPP wysyła do ASPSP żądanie wymiany tokena
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP weryfikuje token powiązany ze zgodą
- 008 / ASPSP generuje nowy token dostępowy i przekazuje go do TPP

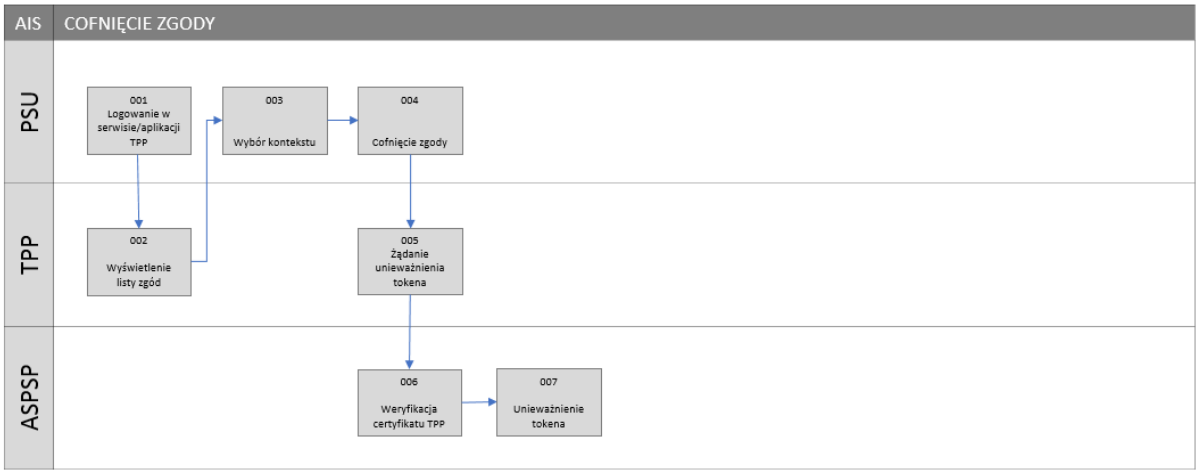


Ilustracja 10: AIS. Edycja parametrów dostępu

1.4.4.2.6 Cofnięcie zgody

- 001 / PSU inicjuje proces w interfejsie TPP
- 002 / TPP wyświetla listę zgód

- 003 / PSU wybiera konkretną zgodę z listy zgód, w ramach której dokonane zostaną zmiany
- 004 / PSU cofa zgodę na usługę AIS
- 005 / TPP wysyła do ASPSP żądanie unieważnienia tokena
- 006 / ASPSP weryfikuje tożsamość TPP na podstawie certyfikatu (lub także na podstawie rejestru TPP)
- 007 / ASPSP unieważnia token powiązany ze zgodą



Ilustracja 11: AIS. Cofnięcie zgody

1.4.4.3 Proces udzielenia zgody PSU na wykonanie usługi CAF

Proces udzielania zgody przez PSU dla ASPSP na wykonanie usługi CAF zostanie opracowany w kolejnej wersji dokumentu. Na potrzeby aktualnej wersji przyjmuje się, że zapytanie w ramach usługi CAF jest wykonywane wyłącznie w sytuacji uprzednio udzielonej zgody.

1.4.5 Zastosowanie mechanizmu silnego uwierzytelnienia (SCA)

ASPSP korzystają z dowolnego wybranego przez siebie systemu silnego uwierzytelnienia PSU (Strong Customer Authentication – SCA), a standard PolishAPI nie definiuje ani nie rekomenduje żadnego ze sposobów przeprowadzania tej procedury. Ponadto, decyzja o zwolnieniu danej transakcji z obowiązku realizacji procedury SCA pozostaje w wyłącznej gestii ASPSP.

1.4.6 Realizacja usług w zakresie Zgodności

Każde ASPSP jest zobowiązane do udostępniania usług w zakresie usług Zgodności na mocy PSD2 oraz powiązanych aktów prawnych. ASPSP niezależnie podejmuje decyzje o zakresie udostępnianych online danych dot. rachunków płatniczych dostępnych w ramach tej usługi. Realizacja usług w zakresie Zgodności nie będzie wymagała relacji umownej pomiędzy ASPSP a TPP.

1.4.7 Realizacja usług w zakresie Premium

Każde ASPSP podejmuje decyzje o udostępnianiu usług w zakresie Premium oraz, w przypadku decyzji o rozpoczęciu ich oferowania, kształtuje ich zakres niezależnie. Realizacja usług w zakresie Premium będzie wymagała relacji umownej pomiędzy ASPSP a TPP.

1.5 Rozwój standardu PolishAPI

W chwili obecnej standard PolishAPI definiuje zakres Zgodności dla usług AIS, PIS i CAF. Zakłada się stały rozwój standardu w odpowiedzi na zmiany regulacyjne, technologiczne i biznesowe na rynku polskim oraz europejskim. Zmiany będą publikowane jako kolejne wersje specyfikacji standardu PolishAPI.

2 Słownik pojęć użytych w dokumencie

Account Information Service (AIS) – usługa dostępu do informacji o rachunku, zdefiniowana w art. 66 PSD2.

Account Information Service Provider (AISP) – Dostawca Świadczący Usługę Dostępu do Informacji o Rachunku – TPP używające interfejsu XS2A w celu dostępu do informacji o rachunku płatniczym PSU.

Confirmation of the Availability of Funds (CAF) – usługa potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej, zdefiniowana w art. 65 PSD2.

European Banking Authority (EBA) – Europejski Urząd Nadzoru Bankowego.

ETSI – Europejski Instytut Norm Telekomunikacyjnych.

OAuth2 – Oauth2 jest otwartym standardem autoryzującym. Pozwala użytkownikom dzielić swoje prywatne zasoby (np. zdjęcia, filmy, kontakty) przechowywane na jednej stronie z inną stroną bez konieczności zagłębiania się w obsługę ich poświadczeń, dostarczając zazwyczaj nazwę użytkownika oraz token (hasło jednorazowe).

Payment Initiation Service Provider (PISP) – Dostawca Świadczący Usługę Inicjowania Transakcji Płatniczej – TPP używające interfejsu XS2A w celu inicjacji transakcji płatniczej w ciężar rachunku PSU.

Payment Initiation Services (PIS) – usługa inicjowania transakcji płatniczej, zdefiniowana w art. 67 PSD2.

Payment Instrument Issuer Service Provider (PIISP) – Dostawca Wydający Instrumenty Płatnicze Oparte na Karcie – TPP używające interfejsu XS2A w celu potwierdzania dostępności na rachunku płatniczym PSU kwoty niezbędnej do wykonania transakcji płatniczej realizowanej w oparciu o instrument wydany przez PIISP.

Payment Services Directive (PSD) – Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego.

Payment Services Directive 2 (PSD2) – Dyrektywa 2015/2366 Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego, uchylająca Dyrektywę 2007/64/WE.

Payment Services User (PSU) – użytkownik usług płatniczych, osoba fizyczna lub prawna korzystająca z usługi płatniczej w charakterze płatnika, odbiorcy lub płatnika i odbiorcy.

Rachunek płatniczy – rachunek prowadzony w imieniu co najmniej jednego użytkownika usług płatniczych, wykorzystywany do wykonywania transakcji płatniczych.

Regulatory Technical Standard (RTS) – Rozporządzenie Delegowane Komisji (UE) nr 2018/389 z dnia 27.11.2017, uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji.

Revised Payment Services Directive (PSD2) – Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (znowelizowana dyrektywa w sprawie usług płatniczych).

Strong Customer Authentication (SCA) – silne uwierzytelnianie klienta, oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów (składników) należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia

wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Swagger – to oprogramowanie open source które pomaga projektować, budować, dokumentować i konsumować usługi RESTful Web.

TS 119 495 – draft (v. 0.0.3) specyfikacji technicznej normy odnoszącej się do profilu certyfikatów kwalifikowanych na potrzeby dyrektywy w sprawie usług płatniczych (Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU), opublikowany w styczniu 2018 r.

Udzielenie zgody – proces, w wyniku którego PSU udziela TPP zezwolenia na dostęp do jego rachunku, prowadzonego przez ASPSP w celu realizacji usługi, w tym usług AIS, PIS i CAF.

Uwierzytelnianie – proces, w wyniku którego ASPSP weryfikuje tożsamość PSU.

Ustawa o usługach płatniczych (UUP) – Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych.

XS2A (Access to Account) – dostęp do rachunków płatniczych, wykorzystywany do wykonywania usług AIS, PIS, CAF oraz innych realizowanych w ramach PolishAPI.

Zakres Premium w ramach usług AIS, PIS i CAF **–** usługi wykraczające poza wymogi PSD2.

Zakres Zgodności w ramach usług AIS, PIS i CAF **–** usługi wymagane przez PSD2.

3 Definicja biznesowa usług z zakresu Zgodności

3.1 Definicja biznesowa zakresu Zgodności dla usługi PIS

Usługa inicjowania transakcji płatniczej w zakresie Zgodności polega na udostępnieniu przez ASPSP możliwości zainicjowania płatności z rachunku płatniczego przez PSU za pośrednictwem TPP, występującego w roli PISP, po uprzednim pozyskaniu odpowiednich zgód od PSU.

3.1.1 Rodzaje transakcji w zakresie Zgodności

W ramach usługi PIS w zakresie Zgodności ASPSP będzie umożliwiało PSU, za pośrednictwem TPP (PISP) inicjację płatności spełniających łącznie poniższe warunki:

a) Jest to przelew bankowy
b) Jest to przelew pojedynczy
c) Jest to przelew z datą bieżącą
d) Jest to przelew na IBAN (NRB w przypadku ASPSP działających w Polsce), w tym przelew do polskiego Urzędu Skarbowego
e) Jeżeli jest to przelew krajowy, to rozliczany jest w jednym z poniższych systemów (w zależności, który z systemów jest wspierany przez ASPSP):
    a. Elixir,
    b. Express Elixir,
    c. SORBNET2,
    d. Blue Cash.
f) Jeżeli jest to przelew zagraniczny, to rozliczany jest w jednym z poniższych systemów:
    a. SWIFT
    b. SEPA
    c. TARGET
g) Jest dostępny w ramach interfejsu online danego ASPSP
h) PSU wypełni wszystkie dane wymagane do złożenia zlecenia wykonania przelewu (ASPSP nie zapewnia wsparcia w postaci słowników, list rozwijalnych ani innych kreatorów), lub w przypadku procesu opisanego w pkt. 1.4.4.1.1 wszystkie dane z wyjątkiem numeru rachunku, z którego płatność zostanie zainicjowana.

Dane, które przekazuje TPP w zleceniu przelewu nie powinny być modyfikowane przez PSU w domenie ASPSP. Każde ASPSP jest zobowiązane do udostępniania usług w zakresie usług Zgodności na mocy PSD2 oraz powiązanych aktów prawnych. ASPSP niezależnie podejmuje decyzje o zakresie udostępnianych online danych dotyczących rachunków płatniczych dostępnych w ramach tej usługi. Realizacja usług w zakresie Zgodności nie będzie wymagała relacji umownej pomiędzy ASPSP a TPP.

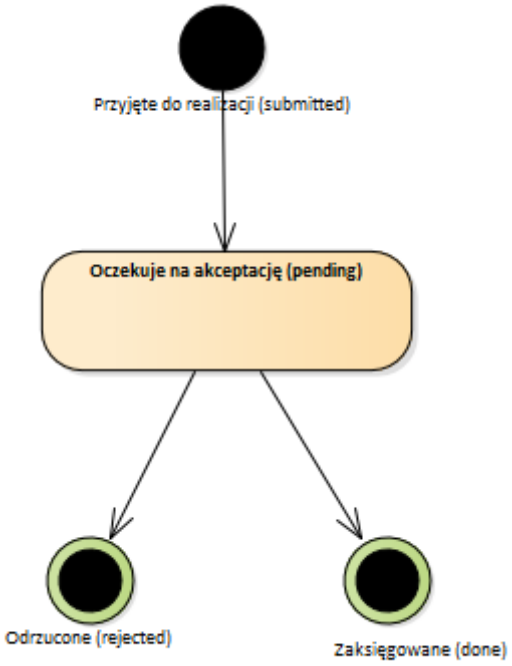
3.1.2 Informacja o statusie transakcji

W ramach wymiany komunikatów w usłudze PIS w zakresie Zgodności ASPSP powiadomi TPP niezwłocznie o przyjęciu bądź odrzuceniu zlecenia. Dodatkowo TPP będzie miał możliwość pobrania informacji na temat statusu płatności przy użyciu metody getPayment z opcjonalną możliwością zapytania o status wielu płatności (getMultiplePayments), o ile ASPSP będzie oferował taką funkcjonalność. ASPSP będzie miał opcjonalną możliwość przekazania do TPP (asynchronicznie) informacji o statusie płatności przy wykorzystaniu metody /v1.0/accounts/v1.0/paymentCallBack.

Zdefiniowane są następujące statusy:

a) Przyjęte do realizacji (submitted)
b) Oczekujące (pending)
c) Odrzucone (rejected)

d) Zaksięgowane (done)



Ilustracja 12: Diagram statusów płatności

3.1.3 Lista pól wymaganych przez ASPSP w zakresie Zgodności

Do poprawnego zainicjowania transakcji płatniczej w ramach usługi PIS w zakresie Zgodności, ASPSP może zażądać od PSU, za pośrednictwem TPP (PISP), aby poniższe pola zostały wypełnione danymi dotyczącymi zlecenia transakcji. Każde ASPSP może oczekiwać od PSU przekazania za pośrednictwem TPP innego zestawu danych.

W odniesieniu do przelewów zagranicznych użycie poszczególnych pól będzie opcjonalne, uzależnione od funkcjonalności obsługiwanej przez dane ASPSP. ASPSP będzie realizował płatności pod warunkiem odpowiedniej inicjacji tej płatności przez TPP tzn. przekazaniu odpowiednich pól z właściwą zawartością.

Pola obowiązkowe, definiujące TPP:

a) Nazwa TPP

3.1.3.1 Przelew krajowy

NAZWA POLA	KOMENTARZE
Adres odbiorcy przelewu	
Data zlecenia	
Data wykonania przelewu	
Kwota przelewu	

Nazwa nadawcy przelewu	Nazwa nadawcy uzupełniana przez ASPSP, aby uniknąć sytuacji, gdzie w zleceniu przelewu wychodzącym z ASPSP podane są dane nadawcy inne niż właściciela obciążanego rachunku.
Nazwa odbiorcy przelewu	
Numer rachunku nadawcy przelewu	Może zostać podane przez TPP, jednak PSU powinien mieć możliwość wyboru rachunku obciążanego po przekierowaniu do ASPSP.
Numer rachunku odbiorcy przelewu	
Pole opisujące przelew	
Tryb pilności	ExpressD0, StandardD1
Typ przelewu (system)	W przypadku przelewu krajowego Elixir, ExpressElixir, Sorbnet, BlueCash, Internal
Waluta	W przypadku, gdy pole jest puste, ASPSP wykona przelew w walucie rachunku.
Blokada	Pole typu bool (domyśla wartość false), dzięki któremu klient będzie mógł explicite wyrazić życzenie, że chce założyć blokadę (w przypadku np. zlecenia przelewu w dniu wolnym)

3.1.3.2 Przelew krajowy do Organu Podatkowego/Izby Celnej w Polsce

NAZWA POLA	KOMENTARZE
Adres odbiorcy przelewu	
Dane urzędu	
Data zlecenia	
Data wykonania przelewu	
Identyfikator płatnika	
Identyfikator zobowiązania	
Kwota przelewu	
Nazwa płatnika	Nazwa nadawcy uzupełniana przez ASPSP, aby uniknąć sytuacji, gdzie w zleceniu przelewu wychodzącym z ASPSP podane są dane nadawcy inne niż właściciela obciążanego rachunku.
Numer okresu	
Numer rachunku nadawcy przelewu	Może zostać podane przez TPP, jednak PSU powinien mieć możliwość wyboru rachunku obciążanego po przekierowaniu do ASPSP.
Numer rachunku odbiorcy przelewu	
Symbol formularza	
Typ okresu	
Typ przelewu	Wartość stała – przelew do urzędu skarbowego
Tryb pilności	ExpressD0, StandardD1
Tryb realizacji przelewu (system)	Standard (Elixir), ekspres (ExpressElixir)
Waluta	
Blokada	Pole typu bool (domyśla wartość false), dzięki któremu klient

	będzie mógł explicite wyrazić życzenie, że chce założyć blokadę (w przypadku np. zlecenia przelewu w dniu wolnym)

3.1.3.3 Przelew zagraniczny EEA

NAZWA POLA	KOMENTARZE
Adres odbiorcy przelewu	
Kwota przelewu	
Nazwa Banku odbiorcy	
Nazwa nadawcy przelewu	Nazwa nadawcy uzupełniana przez ASPSP, aby uniknąć sytuacji, gdzie w zleceniu przelewu wychodzącym z ASPSP podane są dane nadawcy inne niż właściciela obciążanego rachunku.
Nazwa odbiorcy przelewu	
Numer rachunku nadawcy przelewu	Może zostać podane przez TPP, jednak PSU powinien mieć możliwość wyboru rachunku obciążanego po przekierowaniu do ASPSP.
Numer rachunku odbiorcy przelewu	
Pole opisujące przelew	
Status rezydencji	
Tryb realizacji przelewu	Standard, express
Typ przelewu (system)	SEPA, Instant SEPA, Target
Waluta	Wartość stała - EUR
Blokada	Pole typu bool (domyśla wartość false), dzięki któremu klient będzie mógł explicite wyrazić życzenie, że chce założyć blokadę (w przypadku np. zlecenia przelewu w dniu wolnym)

3.1.3.4 Przelew zagraniczny inny niż EEA

NAZWA POLA	KOMENTARZE
Numer rachunku nadawcy przelewu	Nazwa nadawcy uzupełniana przez ASPSP, aby uniknąć sytuacji, gdzie w zleceniu przelewy wychodzącym z ASPSP podane są dane nadawcy inne niż właściciela obciążanego rachunku.
Numer rachunku odbiorcy przelewu	
Nazwa nadawcy przelewu	Nazwa nadawcy uzupełniana przez ASPSP, aby uniknąć sytuacji, gdzie w zleceniu przelewu wychodzącym z ASPSP podane są dane nadawcy inne niż właściciela obciążanego rachunku.
Nazwa odbiorcy przelewu	
Adres odbiorcy przelewu	
Pole opisujące przelew	
Kwota przelewu	
Waluta	
Numer BIC/SWIFT Banku odbiorcy	
Kraj Banku odbiorcy	

Nazwa Banku odbiorcy	
Adres Banku odbiorcy	
Status rezydencji	
Klauzula kosztowa	
Tryb realizacji przelewu	Standard, urgent, express
Typ przelewu (system)	SWIFT
Blokada	Pole typu bool (domyśla wartość false), dzięki któremu klient będzie mógł explicite wyrazić życzenie, że chce założyć blokadę (w przypadku np. zlecenia przelewu w dniu wolnym)

3.1.4 Diagram zapytania w ramach usługi PIS w zakresie Zgodności

Diagram został przedstawiony w Przypadku Użycia #1 w rozdziale 4.

3.1.5 Autoryzacja transakcji płatniczej zainicjowanej za pomocą usługi PIS

ASPSP zapewnia możliwość autoryzacji transakcji płatniczej zleconej przez PSU za pomocą usługi inicjowania transakcji płatniczej w rozumieniu ustawy o usługach płatniczych (UUP), bez względu na metodę autoryzacji oraz jej złożoność. Wybór metody autoryzacji jest po stronie ASPSP.

3.2 Definicja biznesowa zakresu Zgodności dla usługi AIS

Usługa dostępu do informacji o rachunku w zakresie Zgodności polega na udostępnieniu przez ASPSP danych dotyczących historii transakcji oraz wybranych informacji dotyczących rachunku płatniczego, do którego PSU posiada aktywny dostęp on-line. Dostęp udzielany jest dla TPP występującego jako AISP, po uprzednim pozyskaniu odpowiednich zgód od PSU. Ponadto, ASPSP udostępni mechanizmy filtrowania danych, zgodnie z kryteriami dostępnymi on-line w systemie ASPSP (czyli przez bankowość elektroniczną), np.:

a) Data księgowania transakcji (wg wskazanej konkretnej daty księgowania oraz w podanym zakresie dat)
b) Kwota transakcji
c) Obciążenia i uznania na rachunku płatniczym

3.2.1 Definicja rachunku płatniczego

Usługa ta realizowana jest wyłącznie dla rachunków płatniczych, do których dany PSU posiada dostęp on-line. Rachunek taki musi spełniać łącznie poniższe warunki:

a) Jest to rachunek prowadzony dla jednego lub większej liczby użytkowników służący do wykonywania transakcji płatniczych (zgodnie z definicją UUP)
b) PSU posiada dostęp do rachunku on-line

3.2.2 Częstotliwość zapytań w zakresie Zgodności

W ramach usługi AIS w zakresie Zgodności, TPP (AISP) może zażądać od ASPSP przesłania historii rachunku płatniczego oraz wybranych informacji o rachunku płatniczym:

a) Do 4 razy w ciągu 24 godzin od momentu przesłania pierwszego zapytania, w przypadku, gdy pobranie danych nie jest inicjowane na żądanie PSU za pośrednictwem TPP (AISP), ale przez TPP (AISP) na mocy zgód wyrażonych uprzednio przez PSU;
b) Każdorazowo, w przypadku, gdy żądanie jest bezpośrednio inicjowane przez PSU za pośrednictwem TPP (AISP).

Większa częstotliwość zapytań w przypadku, gdy pobranie danych nie jest inicjowane na żądanie PSU za pośrednictwem TPP (AISP), ale przez TPP (AISP) na mocy zgód wyrażonych uprzednio przez PSU, może być realizowana w usłudze AIS wyłącznie w zakresie Premium i jest przedmiotem odrębnych ustaleń bilateralnych pomiędzy ASPSP i TPP (AISP).

3.2.3 Zakres informacji dot. historii rachunku płatniczego w zakresie Zgodności

W zakresie Zgodności usługi AIS jest udostępnienie pełnej dostępnej on-line historii rachunku w zakresie transakcji zaksięgowanych, oczekujących i odrzuconych na danym rachunku płatniczym, wraz z mechanizmami filtrowania danych (w tym zakres dat dla historii transakcji) dla PSU, oraz blokad, które są widoczne dla PSU w kanale on-line ASPSP. Przy czym transakcja oczekująca (pending) oznacza transakcję niezaksięgowaną, niemodyfikowalną, wpływającą na dostępne środki (saldo dostępne).

3.2.4 Lista pól udostępnianych przez ASPSP w zakresie Zgodności

W ramach odpowiedzi na przesłane przez TPP (AISP) żądanie, ASPSP przesyła odpowiedź w zakresie poniższych pól.

NAZWA POLA	KOMENTARZ
Numer rachunku	Numer rachunku
Waluta rachunku	Dla każdego rachunku płatniczego
Imiona i nazwisko / Nazwa i adres PSU	Dla osoby fizycznej imiona i nazwisko, dla osoby prawnej nazwa
Dostępne środki	Dostępne środki w walucie rachunku - po wykonaniu transakcji
Identyfikator transakcji	Unikalny identyfikator danej transakcji nadany przez ASPSP
Kwota w oryginalnej walucie	Dla każdej transakcji w historii rachunku
Saldo księgowe rachunku	Saldo księgowe rachunku - po wykonaniu transakcji
Typ rachunku	Np. rachunek dla konsumenta / firmowy + odniesienie do produktu, np. konto, karta kredytowa, rachunek oszczędnościowy, itd.
Data transakcji	Dla każdej transakcji w historii rachunku
Kwota	Dla każdej transakcji w historii rachunku
Numer rachunku nadawcy	Dla każdej transakcji w historii rachunku
Numer rachunku odbiorcy	Dla każdej transakcji w historii rachunku
Opis	Dla każdej transakcji w historii rachunku
Tytuł	Dla każdej transakcji w historii rachunku
Status transakcji	Dla każdej transakcji w historii rachunku
Typ transakcji	Transakcja uznaniowa/obciążeniowa. Dla każdej transakcji w historii rachunku
Waluta oryginalna transakcji	Dla każdej transakcji w historii rachunku
Nazwa typu rachunku (definiowana przez ASPSP)	Nazwa handlowa produktu
Dane Urzędu Skarbowego	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Data księgowania	Dla każdej transakcji w historii rachunku
Data kursu waluty	Dla każdej transakcji w historii rachunku
ID transakcji TPP	Unikalny identyfikator danej transakcji nadany przez TPP
Identyfikator płatnika	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Identyfikator zobowiązania	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Kurs transakcji	Dla każdej transakcji w historii rachunku
Numer okresu	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Numer wirtualny rachunku odbiorcy	Dla każdej transakcji w historii rachunku
Rok	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Symbol formularza	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Typ okresu	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Typ wpłaty	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce

Unikalny identyfikator instrumentu płatniczego, za którego pomocą wykonano transakcję	Np. numer karty płatniczej (maskowany, zgodnie z prezentacją danych w interfejsie on-line ASPSP)
Rodzaj operacji	Dla każdej transakcji w historii rachunku
Saldo rachunku po transakcji	Dla każdej transakcji w historii rachunku
Typ identyfikatora płatności	Tylko dla przelewu do Organu Podatkowego / Izby Celnej w Polsce
Nazwa i adres odbiorcy przelewu przychodzącego	Dla każdej transakcji przelewu przychodzącego w historii rachunku
Nazwa i adres odbiorcy przelewu wychodzącego	Dla każdej transakcji przelewu wychodzącego w historii rachunku
Adres Banku odbiorcy	Tylko dla przelewów zagranicznych
Kod Banku odbiorcy	Tylko dla przelewów zagranicznych
Nazwa Banku odbiorcy	Tylko dla przelewów zagranicznych
Numer BIC/SWIFT Banku odbiorcy	Tylko dla przelewów zagranicznych
Nazwa i adres nadawcy przelewu przychodzącego	Dla każdej transakcji przelewu przychodzącego w historii rachunku
Nazwa i adres nadawcy przelewu wychodzącego	Dla każdej transakcji przelewu wychodzącego w historii rachunku
Nazwa konta ustawiona przez klienta	O ile ASPSP udostępnia taką usługę.
Inicjator transakcji	W przypadku transakcji zlecanych przez osobę inną niż właściciel rachunku (imię i nazwisko)
Nazwa TPP	W przypadku transakcji inicjowanych w ramach usługi PIS
MCC	Kod dla każdej transakcji / operacji wykonanej przy użyciu karty

Opisane w powyższej tabeli pola stają się obligatoryjne dla ASPSP w relacji do zakresu informacji o rachunkach i transakcjach płatniczych, jakie dany ASPSP udostępnia w swoim interfejsie online, z zastrzeżeniem wyjątków wynikających z przepisów prawa (np. w zakresie szczególnie chronionych danych dotyczących płatności lub danych osobowych). Każdy ASPSP może dodać do udostępnianego zakresu danych na temat rachunku i transakcji dodatkowe pola, wykorzystując w tym celu pole auxData typu Mapa w strukturach AccountInfo, TransactionInfo, TransactionHoldInfo, TransactionPendingInfo oraz TransactionRejectedInfo.

Lista pól udostępnianych w przypadku, gdy ASPSP umożliwia skorzystanie z opcji pobrania listy rachunków w ramach procesu udzielania zgody na usługi AIS lub PIS.

NAZWA POLA	**KOMENTARZ**
Numer rachunku	Numer rachunku w formie maskowanej, widoczne 2 pierwsze i 4 ostatnie cyfry rachunku lub bez maskowania, zgodnie z decyzją ASPSP
Nazwa typu rachunku (definiowana przez Bank)	Nazwa handlowa produktu
Typ rachunku	Np. rachunek dla konsumenta / firmowy + odniesienie do produktu, np. konto, karta kredytowa, rachunek oszczędnościowy, itd.

3.2.5 Diagramy zapytań w ramach usługi AIS w zakresie Zgodności

Diagram został przedstawiony w Przypadku Użycia#2, w rozdziale 4.

3.3 Definicja biznesowa zakresu Zgodności dla usługi CAF

Usługa potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej w zakresie Zgodności polega na przesłaniu zapytania przez TPP, występującego w roli PIISP do ASPSP, o potwierdzenie czy na danym rachunku płatniczym PSU znajdują się środki w

określonej w zapytaniu kwocie, na podstawie zgód uprzednio udzielonych przez PSU. W odpowiedzi ASPSP zwraca odpowiedź będącą komunikatem „TAK" albo „NIE".

3.3.1 Lista pól wymaganych przez ASPSP w zakresie Zgodności

Do poprawnego obsłużenia zapytania o potwierdzenie dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej w ramach usługi CAF w zakresie Zgodności, ASPSP może zażądać od PSU, za pośrednictwem TPP (PIISP), aby poniższe pola zostały wypełnione danymi dot. zlecenia transakcji. Szczegóły dot. pól zdefiniowane są w rozdziale 5.7 Kanoniczny model danych.

NAZWA POLA	WYMAGANE	KOMENTARZE
Identyfikator rachunku, którego dotyczy zapytanie	X	Rachunek uprzednio powiązany z instrumentem płatniczym na bazie zgody wyrażonej przez PSU.
Kwota	X	
Waluta	X	Waluta transakcji

3.3.2 Diagram zapytania w ramach usługi CAF w zakresie Zgodności

Diagram został przedstawiony w Przypadku Użycia #3, w rozdziale 4.

4 Przykładowe przypadki użycia

Bieżąca wersja Standardu PolishAPI opisuje sposób realizacji transakcji opartych o interfejs XS2A w zakresie Zgodności, zdefiniowanym w rozdziale 3 niniejszego dokumentu, a TPP może uczestniczyć w tych transakcjach w jednej ze zdefiniowanych ról.

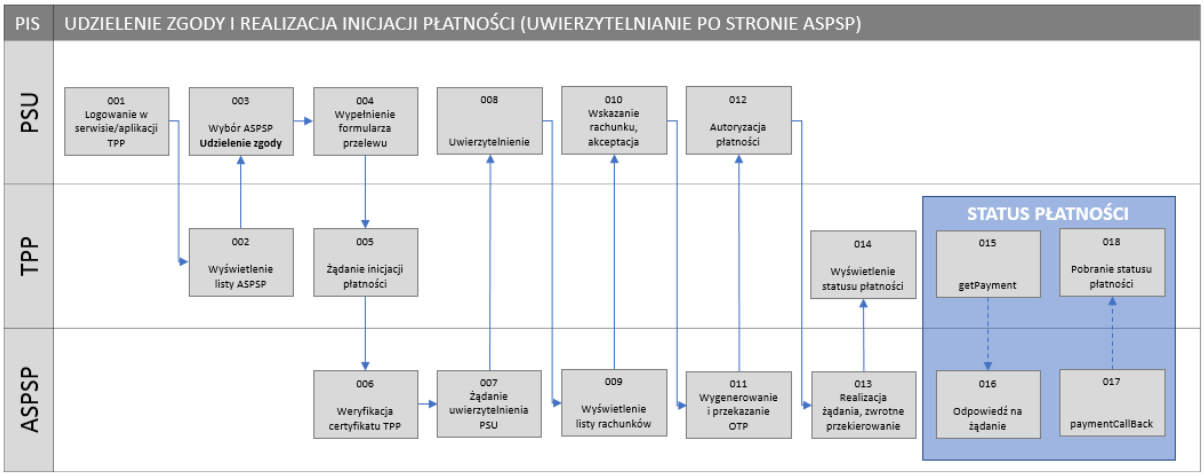
Przykłady obrazujące wykorzystanie poszczególnych usług zostały przedstawione w niniejszym rozdziale. Mają one na celu wyłącznie zilustrowanie kroków dla poszczególnych usług i nie powinny być traktowane jako wyczerpująca lista dopuszczalnych przypadków użycia.

4.1 Przypadek Użycia #1: inicjacja pojedynczej płatności przez PISP (PIS)

Wykorzystanie usługi PIS w zakresie Zgodności zaprezentowane w tym Przypadku Użycia polega na zainicjowaniu przez TPP występującego w roli PISP transakcji płatniczej w ciężar rachunku płatniczego PSU prowadzonego przez ASPSP, w oparciu o stosowne zapisy UUP. ASPSP może odrzucić transakcję, jeżeli TPP (PISP) nie zostanie zidentyfikowany jako podmiot uprawniony do realizacji usługi PIS.

4.1.1 Inicjacja pojedynczej płatności przez PISP z wykorzystaniem mechanizmu uwierzytelniania po stronie ASPSP

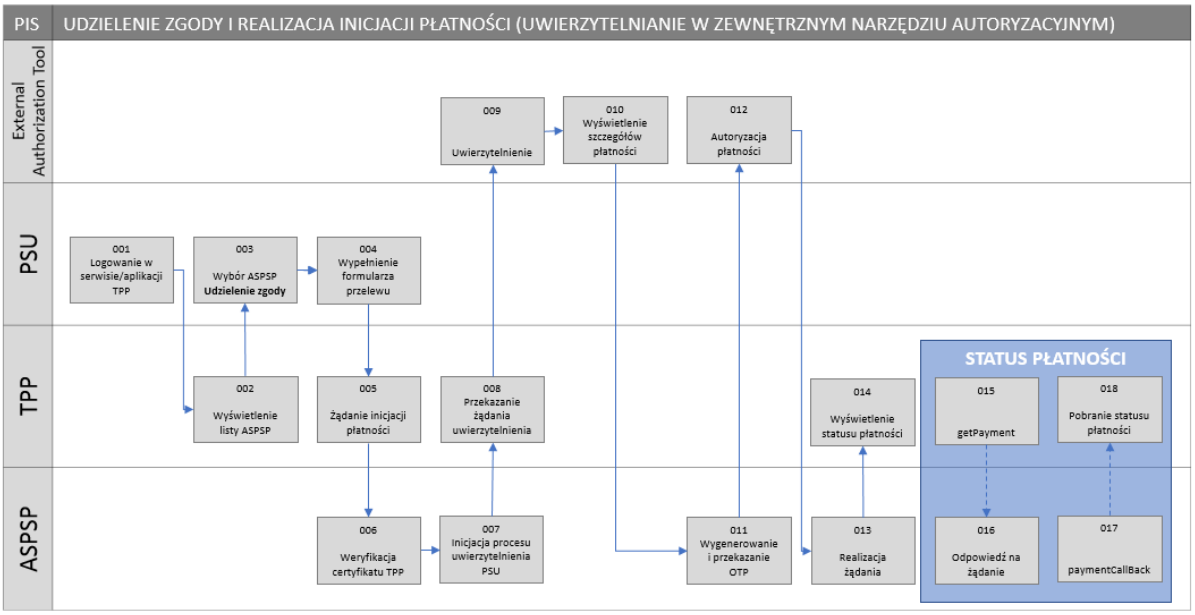
Poniższy diagram odnosi się do procesów opisanych w rozdziale 1.4.4.1.1 (Proces udzielenia zgody PSU na wykonanie usługi PIS – uwierzytelnianie po stronie ASPSP) oraz 3.1.2 (Informacja o statusie transakcji).



Ilustracja 13: PIS / Udzielenie zgody i realizacja inicjacji płatności oraz pobranie statusu płatności

4.1.2 Inicjacja pojedynczej płatności przez PISP z wykorzystaniem mechanizmu uwierzytelniania w zewnętrznym narzędziu autoryzacyjnym

Poniższy diagram odnosi się do procesów opisanych w rozdziale 1.4.4.1.2 (Proces udzielenia zgody PSU na wykonanie usługi PIS – uwierzytelnianie w zewnętrznym narzędziu autoryzacyjnym) oraz 3.1.2 (Informacja o statusie transakcji).



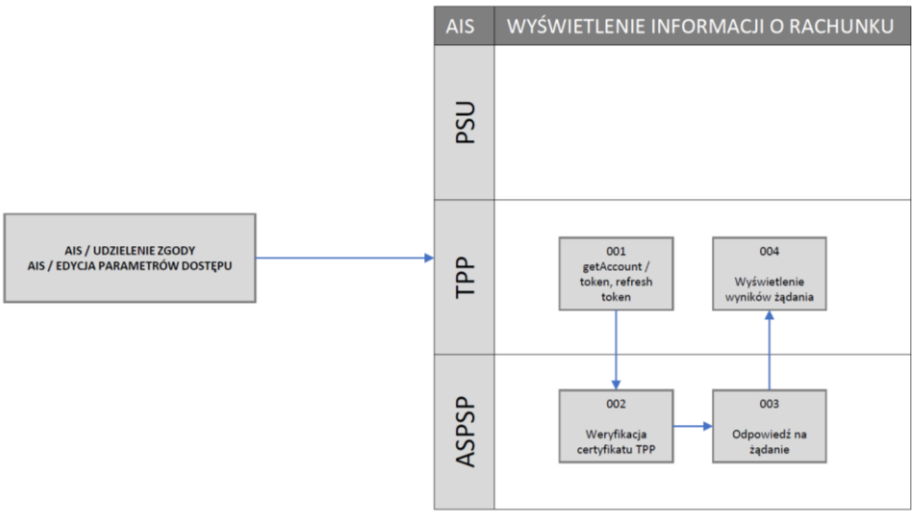
Ilustracja 14: PIS / Udzielenie zgody i realizacja inicjacji płatności (uwierzytelnienie w zewnętrznym narzędziu autoryzacyjnym) oraz pobranie statusu płatności

4.2 Przypadek Użycia #2: wyświetlenie informacji o rachunku płatniczym przez AISP (AIS)

Wykorzystanie usługi AIS w zakresie Zgodności zaprezentowane w tym Przypadku Użycia polega na pozyskaniu przez TPP występującego w roli AISP informacji na temat rachunku płatniczego PSU, prowadzonego przez ASPSP, w oparciu o stosowne zapisy UUP.

Proces udzielenia zgody na skorzystanie z usługi AIS został opisany w rozdziale 1.4.4.2. W opisanym poniżej Przypadku przyjęto założenie, że PSU udzielił AISP zgody na pobranie danych w określonym zakresie. Zapytanie jest inicjowane przez AISP w imieniu PSU.

Proces ten został wysokopoziomowo pokazany na poniższym diagramie.



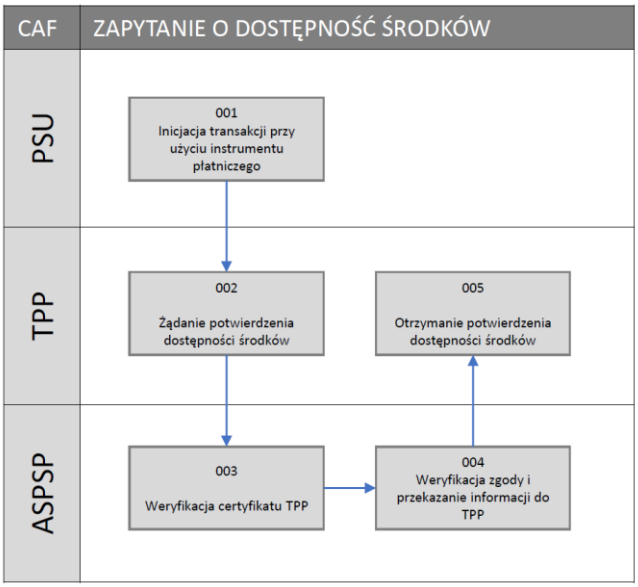
Ilustracja 15: AIS / Wyświetlenie informacji o rachunku płatniczym przez AISP

4.3 Przypadek użycia #3: zapytanie o dostępność środków przez PIISP (CAF)

Wykorzystanie usługi CAF w zakresie Zgodności zaprezentowane w tym Przypadku Użycia polega na zainicjowaniu przez TPP występującego w roli PIISP zapytania o dostępność środków w kwocie transakcji na rachunku płatniczym PSU, w oparciu o stosowne zapisy UUP.

PSU musi uprzednio wskazać PIISP rachunek płatniczy, który będzie każdorazowo odpytywany o dostępność środków oraz udziela uprzednich zgód na udzielanie odpowiedzi przez ASPSP prowadzącego dany rachunek płatniczy. PSU inicjuje proces biznesowy wymagający weryfikacji, czy na wskazanym uprzednio przez PSU rachunku płatniczym znajdują się dostępne środki w kwocie co najmniej równiej kwocie zapytania. W celu realizacji usługi, PIISP nawiązuje sesję XS2A z ASPSP, dokonuje zapytania i uzyskuje odpowiedź „TAK" lub „NIE".

Proces ten został wysokopoziomowo pokazany na poniższym diagramie.



Ilustracja 16: Ilustracja 16: CAF / Zapytanie o dostępność środków

Proces ten może być wykorzystany np. do dokonywania autoryzacji transakcji instrumentami płatniczymi niepowiązanymi z rachunkiem płatniczym prowadzonym przez wydawcę instrumentu.

5 Specyfikacja techniczna PolishAPI

5.1 Założenia techniczne

Poniższa tabela prezentuje założenia techniczne przyjęte dla PolishAPI:

Lp	Założenie	Opis	Uzasadnienie
1	Bezpośrednia komunikacja TPP-ASPSP	TPP i ASPSP w ramach podstawowego wariantu PolishAPI komunikują się bezpośrednio.	Stosowana architektura peer-to-peer zwiększa bezpieczeństwo, wydajność i pozwala na uniknięcie pojedynczego punktu awarii.
2	Rola HUB PSD2	W przypadku korzystania przez ASPSP z usług HUB PSD2 jest to neutralne dla TPP. HUB PSD2 przedstawia się certyfikatem ASPSP, z perspektywy TPP nie ma różnicy czy łączy się z HUB PSD2 czy z ASPSP bezpośrednio.	Ułatwienie wdrożenia API i standardu PolishAPI w sposób wydajny i bezpieczny.
3	Komunikacja TPP-ASPSP to serwer-serwer	Nie jest dopuszczalna bezpośrednia komunikacja urządzenia klienta (np. aplikacji mobilnej) z serwerami PolishAPI ASPSP. Należy prawnie zobligować TPP do zabezpieczenia kluczy dostępowych (tzw certyfikat dostępowy). W szczególności certyfikaty dostępowe nie mogą być instalowane w aplikacjach mobilnych udostępnianych dla PSU)	
4	Rozdzielenie kroku wyrażenia zgody klienta od realizacji operacji	Krok wyrażenia zgody klienta na realizację usługi będzie realizowany przy pomocy standardu OAuth2 i będzie oddzielony od samej realizacji operacji. Jednym ze skutków jest to, iż samo wyrażenie zgody nie rodzi skutków finansowych.	Elastyczność we wdrażaniu nowych usług, w tym Usług Premium.
5	Zakres PolishAPI	Zakres PolishAPI specyfikuje: - sposób wyrażenia zgody na wykonywanie przez TPP operacji w imieniu klienta - zakres operacji i uprawnień - URL, pod jakim dana usługa jest dostępna - standardowy zakres parametrów per usługa - mechanizmy zabezpieczeń - zasady komunikacji - obsługę błędów PolishAPI nie specyfikuje - pełnego zakresu funkcjonalności, które mają być udostępnione przez ASPSP, oraz które z nich	RTS uzależnia zakres funkcjonalności i zakres danych od zakresu funkcjonalności udostępnianych w bankowości internetowej, która jest różna u każdego ASPSP

		będą w Usługach Zgodności - pełnej specyfikacji pól per usługa dla każdego ASPSP	

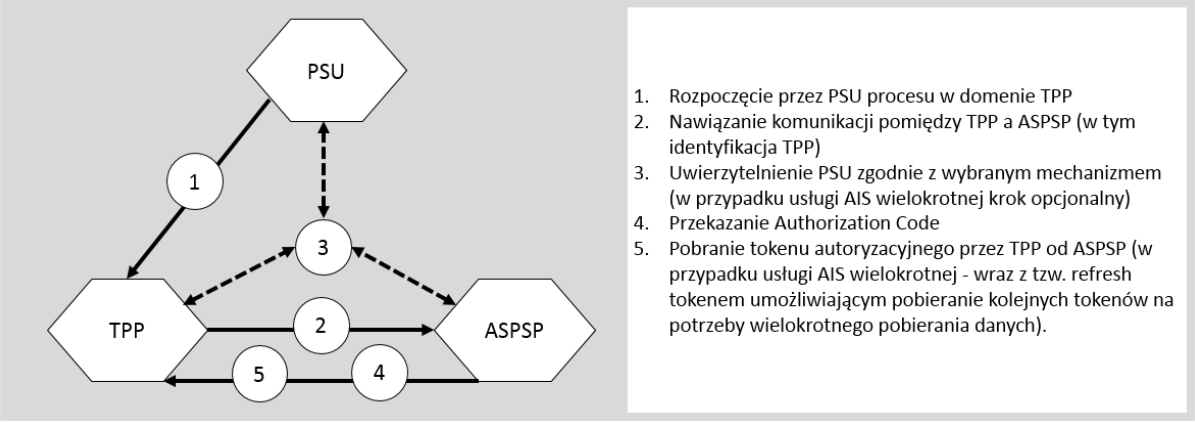
5.2 Nawiązanie sesji XS2A

Sesja komunikacyjna XS2A obejmuje zapytania i odpowiedzi w komunikacji pomiędzy TPP a ASPSP w ramach operacji w usługach dostępu do informacji o rachunku, inicjacji płatności oraz zapytania o dostępne środki, realizowane po dokonaniu identyfikacji TPP. W szczególności może obejmować uwierzytelnienie przez PSU w ramach tej sesji.

Nawiązanie sesji XS2A pomiędzy TPP a ASPSP musi spełniać między innymi poniższe warunki:

a) Wymaganym sposobem autoryzacji dostępu do zasobu jest zwrócenie przez serwer w odpowiedzi na żądanie użytkownika jednorazowego kodu uwierzytelniającego (Authorisation code) – w rozumieniu Art. 4 RTS, który zostanie w kolejnym kroku zamieniony na właściwy token dostępu zgodnie z protokołem OAuth 2.0
b) Parametr state musi być unikalny dla każdego procesu autoryzacji realizowanego przez danego TPP
c) Sugeruje się aby po stronie serwera ASPSP kod uwierzytelniający (Authorisation code) oraz token dostępu były identyfikatorem obiektu w bazie danych, gdzie wskazane dane obiektu posłużą do identyfikacji klienta na rzecz którego generowany jest token dostępu lub realizowana operacja.
   Zastosowanie tzw. stateless token (np. JWT Token - RFC 7519) powinno być stosowane tylko w przypadku, gdy ujawnienie danych o kliencie (w tym identyfikatora) ASPSP jest zgodne z polityką bezpieczeństwa
d) Wraz z tokenem dostępowym przekazywany jest do TPP również parametr scope (taki sam, jak w żądaniu, lub ograniczony przez użytkownika w toku autoryzacji)
e) Uwierzytelnianie PSU może odbywać się według metod wymienionych w rozdziale 1.4.3. niniejszego dokumentu

Schemat przebiegu procesu nawiązywania sesji XS2A przedstawia poniższy diagram.



Ilustracja 17: Wysokopoziomowy diagram nawiązywania sesji XS2A

Realizacja każdej transakcji, w ramach usług AIS, PIS oraz CAF, powinna odbywać się w ramach dedykowanej, odrębnej sesji komunikacyjnej XS2A, przy czym dla AIS dopuszczalne jest wykorzystanie tej samej sesji dla większej liczby operacji AIS przy zachowaniu czasu bezczynności, po którym PSU zostanie automatycznie wylogowany, a sesja zakończona.

5.3 Definicje tokena

Dla usługi AIS:

Token – pozwala na wywołanie wielokrotne usług AIS maksymalnie przez okres 90 dni, zgodnie z Art. 10 RTS,

Refresh token – umożliwia pobranie nowego tokena (zgodnie z The OAuth 2.0 Authorization Framework, 1.5 Refresh token: https://tools.ietf.org/html/rfc6749#page-10).

Dla usługi PIS:

Token – [w mechanizmie uwierzytelniania po stronie ASPSP] pozwala na jednokrotne wywołanie usługi inicjacji oraz wywołanie wielokrotne usługi z zapytaniem o status płatności przez określony przez ASPSP czas (np. 3 dni). Token zostaje unieważniony w momencie zwrócenia nieodwracalnego statusu płatności „zaksięgowane" lub „odrzucone". Powyższe założenie jest niezależne od modelu autoryzacji i autentykacji użytkownika (PSU), zgoda jednokrotna oznacza jednokrotne wykonanie przelewu, token będzie pozwalał na odpytywanie o status płatności przez określony czas. Uwzględnienie w definicji tokenu możliwości inicjacji płatności poprzez wywołanie dedykowanych usług nastąpi po uzupełnieniu w kolejnych wersjach specyfikacji innych mechanizmów uwierzytelniania PSU niż po stronie ASPSP.

5.4 Wzajemne uwierzytelnienie TPP i ASPSP

Uwierzytelnienie wzajemne TPP i ASPSP następuje na podstawie certyfikatów X.509v3 wystawionych przez zaufaną stronę trzecią. Zaufaną trzecią stroną, w szczególności może być instytucja pełniąca funkcję Hub tożsamości. Mogą nim być także inne podmioty powiązane relacjami zaufania opartymi o mechanizmy infrastruktury klucza publicznego.

Wszystkie operacje składające się na wyszczególnione i opisane w standardzie przepływy są możliwe jedynie w sytuacji poprawnego uwierzytelnienia w procesie, na który składa się wzajemne uwierzytelnienie serwera jak i klienta (Mutual authentication).

Opis infrastruktury klucza publicznego wykorzystywanej na potrzeby uwierzytelnień stron (TPP, ASPSP, PISP) nie stanowi części standardu PolishAPI. Powinien być opisany w oddzielnych dokumentach (standardach roboczych) z uwzględnieniem struktury relacji zaufania pomiędzy urzędami certyfikacji oraz interoperacyjności PolishAPI z innymi tego rodzaju rozwiązaniami działającymi w innych krajach.

5.5 Protokół komunikacyjny

Jako protokół komunikacyjny zastosowany zostanie HTTP /2 lub HTTP 1.1, zabezpieczony za pomocą SSL/TLS (wersja) z uwierzytelnianiem klienta za pomocą certyfikatu (Mutual authentication). Ze względu na wymóg zapewnienia niezaprzeczalności (podpisywanie żądań i odpowiedzi) w komunikacji http stosowana będzie jedynie metoda POST.

5.6 Schemat nazewnictwa zasobów

Usługi PolishAPI będą udostępniane pod adresami zgodnymi z następującym wzorcem:

```
https://{domenaDNS}/{v{numerWersjiZasobu 1}/{nazwaZasobu 1}}/.../v{numerWersjiZasobu n}/{nazwaZasobu n}
```

Opis pól:

a) Domena DNS/adres – pod którym ASPSP udostępnia usługi PolishAPI (informacja udostępniana w rejestrze PSD2)

b) Numer wersji zasobu – numer wersji zgodnie ze specyfikacją PolishAPI (liczba przed kropką) i kolejnej wersji interfejsu w ramach danego ASPSP (liczba po kropce)
c) Nazwa zasobu – nazwa zasobu, którego dotyczy zapytanie; dopuszczalne są ścieżki zagnieżdżające zasoby, np. /v{numer wersji zasobu accounts}/accounts/v{numer wersji zasobu transactionsDone}/transactionsDone

5.7 Kanoniczny model danych

W celu unifikacji typów danych został zaproponowany kanoniczny model danych przedstawiony w tabeli. Szczegółową definicje modelu zawiera Załącznik nr 1, Dokumentację modelu zawiera Załącznik nr 2.

Nazwa klasy	**Przeznaczenie**
AccountIban	Numer konta
AccountInfo	Klasa informacji o koncie
AccountInfoRequest	Klasa zapytania o pojedynczy rachunek
AccountResponse	Klasa odpowiedzi na zapytania o konto PSU
AccountsRequest	Klasa zapytania o rachunki
AccountsResponse	Klasa odpowiedzi na zapytania o wiele kont PSU
Address	Klasa zawierająca dane adresu pocztowego
Bank	Klasa zawierająca dane banku
BankAIS	Klasa zawierająca dane banku wykorzystywana w żądaniach AIS
ConfirmationOfFundsRequest	Klasa zapytania o dostępne środki płatnicze na rachunku
ConfirmationOfFundsResponse	Klasa odpowiedzi na zapytanie o dostępne środki płatnicze na rachunku
Error	Klasa informacji zawierająca dane o zwracanym błędzie
Map	Klasa mapy <string, string>
NameAddress	Klasa zawierająca dane nazwy i adresu w postaci czterech lini danych
PageInfo	Klasa zawierająca dane pozwalające na korzystanie z mechanizmu stronicowania
PaymentAddResponse	Klasa odpowiedzi zlecenia płatności
PaymentDomestic	Klasa pomocnicza standardowego przelewu krajowego
PaymentExpressDomesticAddRequest	Klasa zlecenia ekspresowego przelewu krajowego
PaymentInfo	Klasa informacji o płatność
PaymentRequest	Klasa zapytania o status płatności
PaymentResponse	Klasa odpowiedzi na pytanie o płatność
PaymentStandardDomesticAddRequest	Klasa zlecenia standardowego przelewu krajowego
PaymentStandardEEAAddRequest	Klasa zlecenia przelewu zagranicznego SEPA
PaymentStandardNonEEAAddRequest	Klasa zlecenia przelewu zagranicznego innego niż SEPA
PaymentStatus	Słownik statusów płatności
PaymentTaxAddRequest	Klasa zlecenia przelewu podatkowego
PaymentsRequest	Klasa zapytania o statusy wielu płatności
PaymentsResponse	Klasa odpowiedzi na pytanie o wiele płatności
Payor	Klasa informacji o płatniku do ZUS i US
RecipientAIS	Klasa zawierająca dane odbiorcy używana w żądaniach AIS
RecipientPIS	Klasa zawierająca dane odbiorcy używana w żądaniach PIS

RecipientPISTax	Klasa zawierająca dane odbiorcy używana w żądaniach PIS dla operacji podatkowych
RequestHeader	Klasa zawierająca informacje o PSU
ResponseAsync	Klasa odpowiedzi na zapytania asynchroniczne
ResponseHeader	Klasa zawierająca zwrotne metadane
SenderAIS	Klasa zawierająca dane nadawcy używana w żądaniach AIS
SenderPIS	Klasa zawierająca dane nadawcy używana w żądaniach PIS
TransactionDetailRequest	Klasa zapytania o pojedynczą transakcję
TransactionDetailResponse	Klasa odpowiedzi na zapytanie o transakcję
TransactionDoneInfoResponse	Klasa odpowiedzi zawierająca listę transakcji done
TransactionHoldInfoResponse	Klasa odpowiedzi zawierająca listę transakcji
TransactionInfo	Klasa opisująca zaksięgowaną transakcję płatniczą
TransactionInfoBase	Klasa bazowa opisująca transakcję płatniczą
TransactionInfoCard	Klasa reprezentująca informacje o karcie w ramach transakcji
TransactionInfoRequest	Klasa zapytania o transakcje
TransactionInfoRequestBase	Bazowa klasa dla zapytań o transakcje
TransactionInfoTax	Klasa informacji danych dla przelewu do Organu Podatkowego/Izby Celnej
TransactionInfoZUS	Klasa informacji danych dla przelewu do ZUS
TransactionPendingInfo	Klasa opisująca oczekującą transakcję płatniczą
TransactionPendingInfoResponse	Klasa odpowiedzi zawierająca listę transakcji pending
TransactionRejectedInfo	Klasa opisująca odrzuconą transakcję płatniczą
TransactionRejectedInfoResponse	Klasa odpowiedzi zawierająca listę transakcji rejected
TransferData	Klasa zawierająca dane przelewu

Transakcja oczekująca (pending) – transakcja niezaksięgowana, niemodyfikowalna, wpływająca na dostępne środki (saldo dostępne).

5.8 Operacje

Ze względu na wymóg zapewnienia niezaprzeczalności w komunikacji http stosowana będzie jedynie metoda POST pozwalającą na złożenie podpisu w formacie JWS Signature. W ramach operacji kontekst konkretnego użytkownika określany jest na podstawie tokena dostępowego.

5.9 Sortowanie

Zwracane rekordy sortowane są chronologicznie (odwrotnie).

5.10 Filtrowanie

Filtrowanie w usłudze AIS odbywa się przez ustawienie odpowiednich właściwości w obiekcie klasy TransactionInfoRequest:

a) transactionIdFrom -Transakcje od podanego identyfikatora transakcji „chronologicznie”
b) transactionDateFrom – początkowa data transakcji żądanego zakresu danych
c) transactionDateTo – końcowa data transakcji żądanego zakresu danych
d) bookingDateFrom – początkowa data księgowania żądanego zakresu danych
e) bookingDateTo – końcowa data księgowania żądanego zakresu danych
f) type – CREDIT lub DEBIT

g) minAmount – minimalna kwota operacji w żądanym zakresie danych
h) maxAmount – maksymalna kwota operacji w żądanym zakresie danych

5.11 Stronicowanie

Wyniki zapytań zawierające wiele rekordów (gdzie wiele > 100) powinny być stronicowane. Kolejne strony będą pobierane poprzez ustawianie atrybutu pageId w klasie TransactionInfoRequest. Atrybut pageId należy ustawić na wartość zwróconą w klasie PageInfo poprzedniego żądania. Dla nawigacji w przód nextPage, dla nawigacji w tył previousPage. Liczba rekordów na stronie definiowana jest za pomocą atrybutu perPage w klasie TransactionInfoRequest. Sugeruje się maksymalna wartość, jaką można ustawić w parametrze perPage to 100. Numerowanie stron rozpoczyna się od 1. Pominięcie parametru pageId zwróci pierwszą stronę.

5.12 Statusy odpowiedzi

Statusy techniczne będą zwracane poprzez następujące kody http:

Status	**Opis**
200 OK	Operacja się powiodła
304 Not Modified	Używane, jeżeli użyto nagłówków cache'owania
400 Bad Request	Zapytanie jest niepoprawne syntaktycznie
401 Unauthorized	Niepoprawnie uwierzytelniony użytkownik
403 Forbidden	Błąd autoryzacji (brak uprawnień dostępu do zasobu)
404 Not Found	Odwołanie do nieistniejącego zasobu
405 Method Not Allowed	Użycie niewłaściwej metody – metoda zawarta w żądaniu nie jest dozwolona dla wskazanego zasobu (Używany jest tylko POST)
406 Not Acceptable	Nieprawidłowy nagłówek accept w zapytaniu (serwer nie jest w stanie obsłużyć)
415 Unsupported Media Type	Jeżeli nieprawidłowy content type został ustawiony w zapytaniu
422 Unprocessable Entity	Błąd walidacji
429 Too Many Requests	Zapytanie odrzucone ze względu na przekroczenie maksymalnej liczby żądań dostępu do zasobu

5.13 Nagłówki HTTP

W zapytaniach zostaną użyte następujące nagłówki http:

Nagłówek	**Typ**	**Opis**
Authorization	String	Nagłówek uwierzytelnienia (używany przy przesyłaniu tokenu). Wartość nagłówka Authorization powinien składać się z „type" + „credentials", gdzie w przypadku podejścia z wykorzystaniem tokenu „type" powinien mieć wartość „Bearer".
Date	Date	Timestamp żądania w formacie RFC 5322 date and time format.
Accept	Content type	Należy ustawić na application/json W przeciwnym razie aplikacja powinna zwrócić 406 Not Acceptable HTTP.
Accept-Encoding	Gzip, deflate	Operacja powinna wspierać GZIP oraz kodowanie DEFLATE, może również zwrócić dane nieskompresowane.
Accept-Language	„pl", „en", etc.	Określa, preferowany język w jakim ma być zwrócona odpowiedź. Operacja nie musi wspierać tego nagłówka
Accept-Charset	Charset type like „UTF-8"	UTF-8

Content-Type	application/json	Należy ustawić na application/json. W przeciwnym razie operacja zwraca 415 Unsupported Media Type HTTP status code
X-JWS-SIGNATURE	String	Podpis JWS Signature (Detached)

Nagłówki odpowiedzi:

Nagłówek	Obligatoryjny?	Opis
Date	Tak	Timestamp na bazie czasu serwera GMT zgodnie z RFC 5322
Content-Type	Tak	application/json
Content-Encoding	Tak	GZIP lub DEFLATE
Expires	Nie	Określa politykę cacheowania dla wolnozmiennych obiektów np. Expires: Mon, 25 Jun 2012 21:31:12 GMT
Size	Tak	Wielkość odpowiedzi w bajtach
ETag	Nie	Identyfikator wersji zasobu
Last-Modified	Nie	Data ostatniej modyfikacji zasobu
X-JWS-SIGNATURE	Tak	Podpis JWS Signature (Detached)

5.14 Format wiadomości

Formatem wymiany danych będzie JSON z kodowaniem UTF-8. Wszystkie komunikaty mają zdefiniowaną JSON schema draft #4. Nazwy parametrów będą zapisane camelCase.

5.15 Podstawowe formaty danych

Format	Format JSON	Opis
Tekst	String	Tekst kodowany w UTF-8
Daty	String	Zgodnie z ISO8601. Data i czas będą reprezentowane w postaci YYYY-MM-DD na YYYY-MM-DDThh:mm:ss.ccczzzzzz z obowiązkowym podaniem strefy czasowej Oznaczenia: YYYY – rok, MM – miesiąc, DD – dzień, hh – godzina, mm – minuta, ss – sekunda, ccc – milisekundy (opcjonalne) zzzzzz – np. +02:00 lub Z dla oznaczenia czas uniwersalnego Przykładowo 2016-10-10T12:00:05.342+01:00
Kwoty	String	Zapisane jako liczby ze znakiem oddzielającym część całkowitą od części ułamkowej 2 miejsca (znak kropki). Przy kwotach dodatnich nie dodajemy żadnych dodatkowych znaków. Przy liczbach ujemnych dodajemy przed liczbą „-„
Liczba całkowita	Number	Liczby całkowite reprezentowane są bez separatorów grupowych
Liczba rzeczywista	String	Liczby rzeczywiste reprezentowane są bez separatorów grupowych i ze znakiem ‘.’ jako separatorem dziesiętnym
Oznaczenia krajów	String	Zgodnie z ISO 3166
Waluty	String	Oznaczenia walut zgodnie z ISO 4217
Numery rachunków	String	Numery IBAN zgodnie z ISO 13616
Identyfikatory banków	String	Bank Identifier Codes (BIC) zgodnie z ISO 9362

6 Bezpieczeństwo informacji

Niniejszy rozdział obejmuje ogólne wymagania bezpieczeństwa, istotne z punktu widzenia kreowania standardu oraz projektowania na jego podstawie ekosystemu rozwiązań informatycznych zgodnych z PolishAPI. Szczegółowe wymagania bezpieczeństwa, obejmujące dodatkowo kwestie bezpieczeństwa implementacji, operacji i utrzymania systemów opartych na PolishAPI zostaną opisane w oddzielnym dokumencie, a jego opracowanie zostanie poprzedzone przygotowaniem szczegółowego modelu zagrożeń. Będą zatem odpowiedzią na zidentyfikowane konkretne zagrożenia, miejsca potencjalnej materializacji tych zagrożeń, a także ocenę poziomu istotności oraz prawdopodobieństwa i wpływu przypadków materializacji zagrożeń na bezpieczeństwo i ciągłość działania ekosystemu PolishAPI.

Poszczególne komponenty systemów informatycznych opartych na PolishAPI powinny mieć jasno zdefiniowany rozdział pomiędzy warstwą danych, warstwą kontrolera i warstwą prezentacyjną. Komponenty powinny być odseparowane od siebie poprzez zdefiniowane zabezpieczenia takie jak segmentacja sieci lub reguły zapory sieciowej.

6.1 Uwierzytelnienie TPP

Użytkownicy muszą zostać poprawnie uwierzytelnieni przed udzieleniem im dostępu do funkcji API tak, aby zapewnić wysoki poziom ochrony zarówno przed podszyciem się nieuprawnionych podmiotów pod właściwych użytkowników, jak i przed nieuprawnioną eskalacją poziomu autoryzacji przez użytkowników mających legalny dostęp do API. Uwierzytelnienie następuje w oparciu o certyfikaty klucza publicznego w procesie dwustronnego uwierzytelnienia TLS (*server side* & *client side authentication*) za pomocą protokołu https.

Błędy uwierzytelnienia muszą skutkować odmową dostępu do funkcji API.

Dane uwierzytelniające użytkownika oraz sesję, a także tokeny do autoryzowania operacji nie mogą być przekazywane w postaci parametrów URI.

6.2 Autoryzacja TPP

Autoryzacja TPP 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.

Użycie poszczególnych metod musi być autoryzowane w taki sposób, aby uprawnienia były zależne od roli użytkownika. W szczególności, poziom i zakres autoryzacji powinien być różny dla TPP w zależności od zakresu ich uprawnień.

6.3 Autoryzacja PSU dla operacji wykonywanych przez TPP

Niezależnie od zastosowanego mechanizmu uwierzytelniania PSU w ramach usług AIS/PIS/CAF zakłada się, iż proces ten kończy się wydaniem przez ASPSP Access Tokenu (RFC 6749 – 1.4. Access Token) i opcjonalnie refresh tokenu (RFC 6749 – 1.5. Refresh Token). Zlecanie operacji przez TPP odbywa się zawsze z wykorzystaniem ważnego Access Tokenu

6.4 Bezpieczeństwo w przypadku aplikacji mobilnych

Ze względu na bezpieczeństwo w modelu wykorzystującym mechanizm uwierzytelniania po stronie ASPSP, przekierowanie na stronę ASPSP i z powrotem na stronę TPP będzie odbywało się w przeglądarce systemowej (nie będą dopuszczone przeglądarki inne niż systemowa, nie będzie

dopuszczone stosowanie WebView) a nie w samej aplikacji mobilnej. TPP może zarejestrować odpowiedni URL w systemie operacyjnym urządzenia, aby po przekierowaniu do TPP automatycznie wznowić aplikację mobilną.

6.5 Walidacja i zapewnienie integralności danych

Dane muszą być poddane procedurom walidacji w kontekście typu zmiennych, zakresu i wzorca dopuszczalnych wartości. W szczególności ustrukturyzowane dane JSON muszą być parsowane zgodnie z formalnymi procedurami walidacyjnymi z zastosowaniem podejścia opartego na listach dopuszczalnych wartości (white list). Walidacji muszą być także poddane nagłówki Content-type i Accept (application/json) na Zgodność wartości nagłówka z rzeczywistą treścią komunikatu HTTP.

Podczas walidacji musi być zwalidowany podpis cyfrowy w nagłówku (X-JWS-SIGNATURE) w kontekście odebranych w żądaniu danych.

W razie błędów walidacji treści Content-type i Accept powinien zostać zwrócony komunikat http numer 406 (Not Acceptable).

Błędy walidacji danych wejściowych muszą być rejestrowane w logach.

Błędy walidacji muszą być sygnalizowane komunikatem HTTP 400 (Bad Request) i dane muszą być odrzucane.

Dane niezwalidowane bądź niepoprawnie zwalidowane muszą być odrzucane.

6.6 Kryptografia

Komunikacja przez PolishAPI musi być zabezpieczona kryptograficznie na dwóch poziomach:

a) Na poziomie transportu za pomocą(https/TLS). Renegocjacja parametrów połączenia TLS musi być wykonywana bezpiecznie, zgodnie z RFC 5746
b) Na poziomie komunikatu do zapewniania niezaprzeczalności należy zastosować podpis JSON Web Signature (JWS https://tools.ietf.org/html/rfc7515) sygnatura podpisu musi znajdować się w nagłówku X-JWS-SIGNATURE

Każdy TPP musi posiadać własne unikatowe dwie pary kluczy (do transmisji i podpisu).

Do zabezpieczania transmisji na poziomie https oraz podpisu JWS-SIGNATURE muszą być zastosowane odrębne certyfikaty. Dla https certyfikat musi posiadać rozszerzone użycie klucza (Client Authentication) dla podpisu (Digital signature).

Certyfikaty użyte do zestawienia transmisji oraz podpisu muszą zostać walidowane pod względem:

a) Ważności (daty ważności certyfikatu od i do)
b) Braku odwołania (crl/ocsp)
c) Weryfikacji ścieżki (https://tools.ietf.org/html/rfc4158)

Informacje szczególnie wrażliwe, w tym poświadczenia tożsamości oraz klucze autoryzacyjne nie mogą podlegać buforowaniu oraz zapisywania w logach.

Certyfikaty powinny być wydawane z uwzględnieniem specyfikacji ETSI TS 119 495.

6.7 Ochrona przed nadużyciami API

Implementacja API powinno uwzględniać mechanizmy ochrony przez nadmiarem żądań ze strony użytkowników (uprawnionych i nieuprawnionych), w szczególności celowo wygenerowanych z

zamiarem spowodowania niedostępności zasobu (DoS/DDoS), przez zastosowanie mechanizmów limitujących liczbę obsługiwanych żądań w jednostce czasu. Wartości limitów winny być ustalane na podstawie rozpoznania konkretnych warunków operacyjnych. Limity tego rodzaju powinny podlegać parametryzacji. Mierzenie liczby żądań dostępu do zasobów powinno bazować na zastosowaniu jednoznacznie identyfikującego danego TPP klucza (Klasa RequestHeader.tppID) oraz liczników zaimplementowanych per TPP po stronie serwera. Przekroczenie limitów musi być sygnalizowane komunikatem HTTP numer 429 (Too Many Requests).

Zabezpieczenia powinny być zrealizowane w oparciu o zalecenia OWASP – REST Security Cheat Sheet (https://www.owasp.org/index.php/REST_Security_Cheat_Sheet).

Kontrola limitów powinna być przeprowadzana 4 razy na dobę. Należy zaznaczyć, wysłanie zapytanie przez PSU resetuje licznik zapytań wysyłanych przez TPP w kontekście PSU.

6.8 Logowanie informacji audytowych

Zaleca się, aby źródła czasu wszystkich podmiotów korzystających z PolishAPI powinny być synchronizowane, aby zapewnić, że wpisy w logach mają poprawny czas.

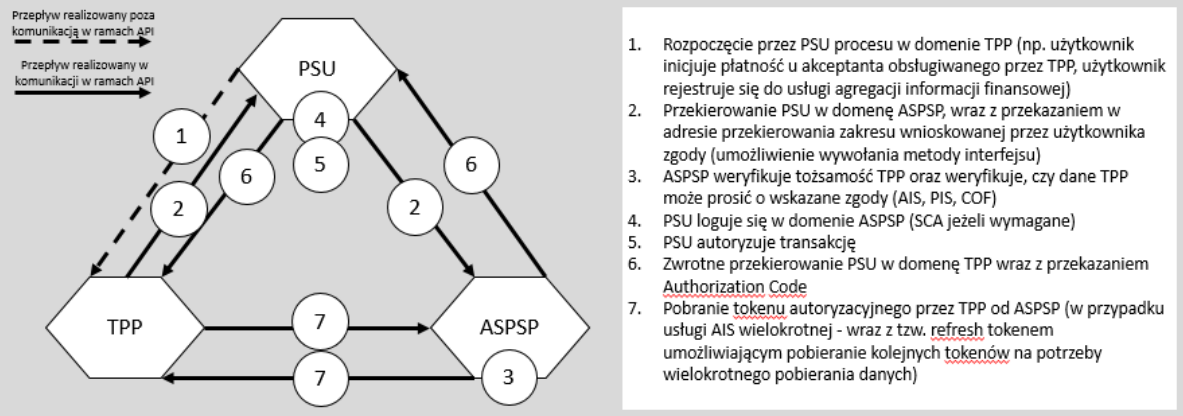
Logowanie kluczowych operacji biznesowych powinno zapewniać niezaprzeczalność i integralność wpisów przez wykorzystanie danych z podpisu JWS Signature.

Log powinien zawierać niezbędne informacje, które pozwolą na precyzyjną analizę czasową w przypadku wystąpienia zdarzenia pozwalającą na złączenie poszczególnych wpisów w jedną transakcje. Elementem łączącym poszczególne wpisy może być np. skrót z tokenu autoryzacyjnego.

7 Opis techniczny procesu uwierzytelniania i autoryzacji

7.1 Mechanizm uwierzytelniania po stronie ASPSP

W modelu wykorzystującym mechanizm uwierzytelniania po stronie ASPSP proces oparty jest o protokół OAuth 2.0 Authorization Code.



Ilustracja 18: Mechanizm uwierzytelniania po stronie ASPSP

Proces został opisany RFC 6749 w rozdziale 4.1. Authorization Code Grant

Poniżej opisano kroki wraz ze zmianami wprowadzonymi przez PolishAPI wynikającymi z wymogów prawnych oraz bezpieczeństwa

7.1.1 Przekierowanie z TPP do ASPSP

Zgodnie z RFC 4.1.1. Authorization Request przekierowanie obejmuje następujące parametry

Parametr	**Wymagalność w PolishAPI**	**Komentarz**
response_type	Wymagane	Wartość „code”
client_id	Wymagane	Zgodnie z tym co proponuje berliner group używamy następującej konwencji clientId=TPP.[CountryCode].[LicenseNumber]
redirect_uri	wymagane	
scope	Wymagane	
scope_details	Wymagane	
state	Wymagane	Losowa, unikalna w ramach TPP wartość – zabezpieczenie przed atakiem Cross-Site Request Forgery

Parametr scope_details określa zakresy czasowe, ograniczenia, szczegóły danego uprawnienia:

a) co do zakresu zasobów jakie są udostępniane (np. lista kont)
b) czasu na jaki są udostępniane
c) limitu liczby użycia
d) listy operacji jakich dotyczy
e) wybranych parametrów operacji np. długości historii wstecz, parametrów przelewu itp.

Specyfikacja struktury parametru scope_details znajduje się w załączniku nr 5 i nr 6.

Powyższe parametry są przesyłane poprzez przeglądarkę PSU jako POST (ze względu na możliwą wielkość scope_details) w formacie JSON zakodowane i podpisane przy użyciu JSON Web Signature zgodnie z RFC 7515

Parametr *scope* definuje następujące zakresy dostępowe (odpowiadające poszczególnym zasobom (paths) specyfikacji:

- ais:accounts: Uprawnienie do wykonania AIS-Accounts
- ais:holds: Uprawnienie do wykonania AIS-Holds
- ais:transactionsDone: Uprawnienie do wykonania AIS-TransactionsDone
- ais:transactionsPending: Uprawnienie do wykonania AIS-TransactionsPending
- ais:transactionsRejected: Uprawnienie do wykonania AIS-TransactionsRejected
- ais:transationDetail: Uprawnienie do wykonania AIS-TransationDetail
- pis:multiplePayments: Uprawnienie do wykonania PIS-MultiplePayments
- pis:payment: Uprawnienie do wykonania PIS-Payment
- pis:domestic: Uprawnienie do wykonania PIS-Domestic
- pis:EEA: Uprawnienie do wykonania PIS-EEA
- pis:nonEEA: Uprawnienie do wykonania PIS-NonEEA
- pis:tax: Uprawnienie do wykonania PIS-Tax
- CAF:confirmationOfFunds: Uprawnienie do wykonania CAF-ConfirmationOfFunds

7.1.2 Uwierzytelnienie PSU i autoryzacja

Realizacja po stronie ASPSP

7.1.3 Zwrotne przekierowanie przeglądarki PSU do TPP

Zgodnie z RFC 6749 4.1.2. Authorization Response

7.1.4 Pobranie tokenu na podstawie Auhtorization Code

Zgodnie z RFC 6749 4.1.3. Access Token Request pobranie tokenu

Parametr	**Wymagalność w PolishAPI**	**Komentarz**
grant_type	wymagane	Wartość „authorization_code”
Code	wymagane	Zgodna z wartością przekazaną w kroku 7.1.3
redirect_uri	wymagane	Wartość zgodna z wartością z kroku7.1.1
client_id	wymagane	Zgodnie z tym co proponuje berliner group używamy następującej konwencji clientId=TPP.[CountryCode].[LicenseNumber]

Uwierzytelnienie TPP odbywa się na podstawie certyfikatu użytego do połączenia TLS

Zwracane dane oprócz zestawu danych przewidzianego w OAuth2 (RFC 5.1. Successful Response) powinny zawierać także pole scope_details zawierające szczegóły zgód, na jakie zgodził się PSU

Parametr	**Wymagalność w PolishAPI**	**Komentarz**
access_token	wymagane	
token_type	wymagane	
expires_in	wymagane	

refresh_token	opcjonalne	
scope	wymagane	
scope_details	wymagane	

7.1.5 Wycofanie zgody

Wycofanie zgody jest realizowane za pomocą metody /v1.0/accounts/v1.0/deleteConsent

7.1.6 Stosowanie struktury scope_details

- Zgodę jednorazową obsługujemy za pomocą parametru scopeUsageLimit.

7.1.7 Pobranie access tokena na podstawie refresh tokena

Zgodnie z RFC 6749 6. „Refreshing an Access Token", po wygaśnięciu ważności access tokenu, TPP może pobrać nowy Access Token korzystając z refresh tokenu (o ile został wydany). Taka sytuacja będzie miała miejsce w przypadku usługi AIS wielokrotny oraz CAF.

Poniżej przedstawiono żądanie TPP i odpowiedź serwera ASPSP

Parametr	**Wymagalność w PolishAPI**	**Komentarz**
grant_type	wymagane	Wartość „refresh_token"
refresh_token	wymagane	Zgodna z wartością przekazaną przez ASPSP w kroku 7.1.4
scope	opcjonalny	Żądany zakres nie może być większy niż ten, który przekazano w kroku 7.1.4
scope_details	opcjonalny	Żądany zakres nie może być większy niż ten, który przekazano w kroku 7.1.4
is_user_session	opcjonalne	Określa czy dana sesja jest związana z interakcją z PSU – wartości true/false. Rozszerzenie standardu OAuth2
user_ip	Wymagane, jeśli is_user_session=true	IP przeglądarki użytkownika (informacja na potrzeby fraud detection) Rozszerzenie standardu OAuth2
user_agent	Wymagane, jeśli is_user_session=true	Informacja dotycząca wersji przeglądarki użytkownika (informacja na potrzeby fraud detection) Rozszerzenie standardu OAuth2

Odpowiedź odsyłana przez ASPSP jest taka sama jak w pkt. 7.1.4

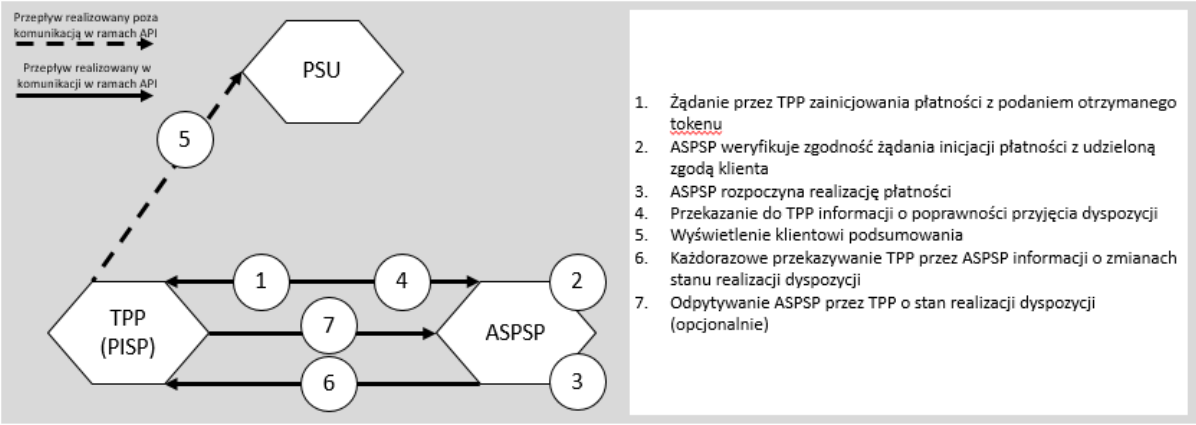
7.2 Inne mechanizmy uwierzytelniania

Niniejszy rozdział zostanie uzupełniony w dalszym etapie prac grupy projektowej.

8 Opis techniczny usługi PIS

Rozdział stanowi streszczenie specyfikacji API w formacie swagger zdefiniowanej w Załączniku nr 1 oraz dokumentacji w formacie swagger-html2 w Załączniku nr 2.

8.1 Diagram aktywności w usłudze PIS



Ilustracja 19: Wysokopoziomowy diagram aktywności w usłudze PIS

8.2 Struktura zapytania

Poniższa tabela zawiera zapytania do usługi PIS wraz z wyspecyfikowaniem klas obiektów przekazywanych w żądaniu i odpowiedzi.

Zasób (endpoint)	**Opis**	**Klasa obiektu KMD przekazywana w żądaniu i odbierana w odpowiedzi**
/payments/{wersja}/domestic	Inicjuje przelew krajowy	PaymentDomesticAddRequest/ PaymentAddResponse
/payments/{wersja}/ EEA	Inicjuje przelew zagraniczny SEPA	PaymentStandardEEAAddRequest/ PaymentAddResponse
/payments/{wersja}/ nonEEA	Inicjuje przelew zagraniczny poza SEPA	PaymentStandardNonEEAAddRequest/ PaymentAddResponse
/payments/{wersja}/ tax	Inicjuje przelew do US	PaymentTaxAddRequest/ PaymentAddResponse
/payments/{wersja}/ getPayment	Pobiera status realizacji przelewu	PaymentRequest/ PaymentResponse
/payments/{wersja}/ getMultiplePayments	Pobiera statusy realizacji wielu płatności. Wywołanie nie wymaga podania tokenu.	PaymentsRequest/ PaymentResponse

8.3 Asynchroniczna usługa PIS

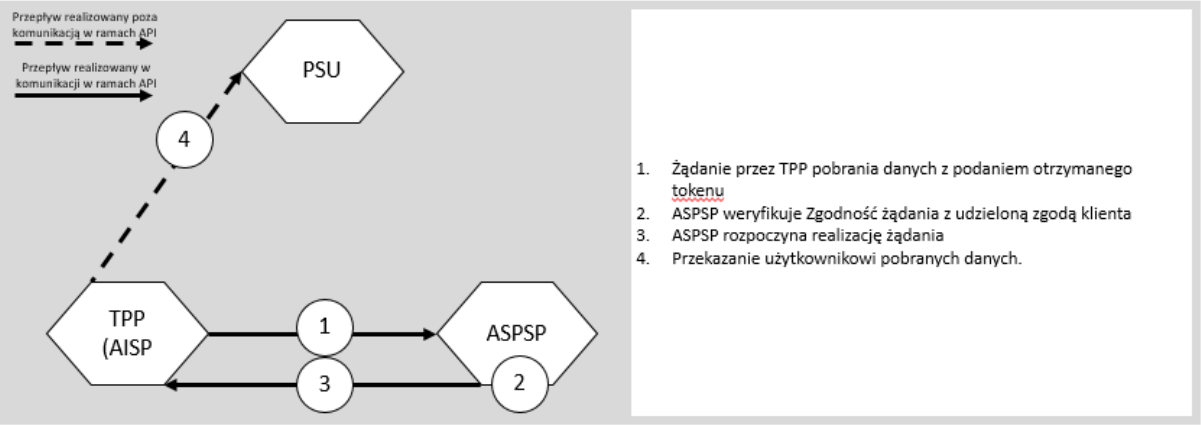
Specyfikacja definiuje interfejs wywołań zwrotnych (CallBack), gdzie ASPSP informuje TPP za pomocą metody paymentCallBack o zmianie statusu przelewu. Interfejs wywołań zwrotnych zdefiniowano w załączniku nr 3.

Jako metodę zabezpieczającą API zastosowano typ „apiKey” (https://swagger.io/docs/specification/2-0/authentication/) oraz dodatkowo weryfikowany jest odcisk palca certyfikatu serwerowego TPP, który używany jest do zestawiania połączenia TLS wywołania zwrotnego - przekazywany w parametrze keyID. W wywołanych PIS TPP przekazuje do ASPSP wartość apiKey oraz callbackURL, które są użyte w wywołaniach zwrotnych.

9 Opis techniczny usługi AIS

Rozdział stanowi streszczenie specyfikacji API w formacie swagger zdefiniowanej w Załączniku nr 1 oraz dokumentacji w formacie swagger-html2 w Załączniku nr 2.

9.1 Diagram aktywności w usłudze AI



Ilustracja 20: Wysokopoziomowy diagram aktywności w usłudze AIS

9.2 Struktura zapytań AIS

Poniższa tabela zawiera zapytania do usługi AIS wraz z wyspecyfikowaniem klas obiektów przekazywanych w żądaniu i odpowiedzi.

Zasób (endpoint)	**Opis**	**Klasa obiektu KMD przekazywana w żądaniu i odbierana w odpowiedzi**
/accounts/{wersja}/deleteConsent	Usuwa/unieważnia zgodę	DeleteConsentRequest/ string
/accounts/{wersja}/getAccounts	Pobiera wszystkie rachunki PSU	AccountsRequest/ AccountsResponse
/accounts/{wersja}/getAccount	Pobiera pojedynczy rachunek płatniczy	AccountInfoRequest/ AccountInfo
/accounts/{wersja}/getTransactionsDone	Pobiera transakcje zrealizowane na rachunku	TransactionInfoRequest/ TransactionDoneInfoResponse
/accounts/{wersja}/getTransactionsPending	Pobiera transakcje oczekujące na rachunku	TransactionInfoRequest/ TransactionPendingInfoResponse
/accounts/{wersja}/getTransactionsRejected	Pobiera transakcje odrzucone na rachunku	TransactionInfoRequest/ TransactionRejectedInfoResponse
/accounts/{wersja}/getHolds	Pobiera blokady na rachunku	TransactionInfoRequest/ TransactionHoldInfoResponse
/accounts/{wersja}/getTransationDetail	Pobiera szczegóły pojedynczej transakcji/blokady	TransactionDetailRequest/ TransactionDetailResponse

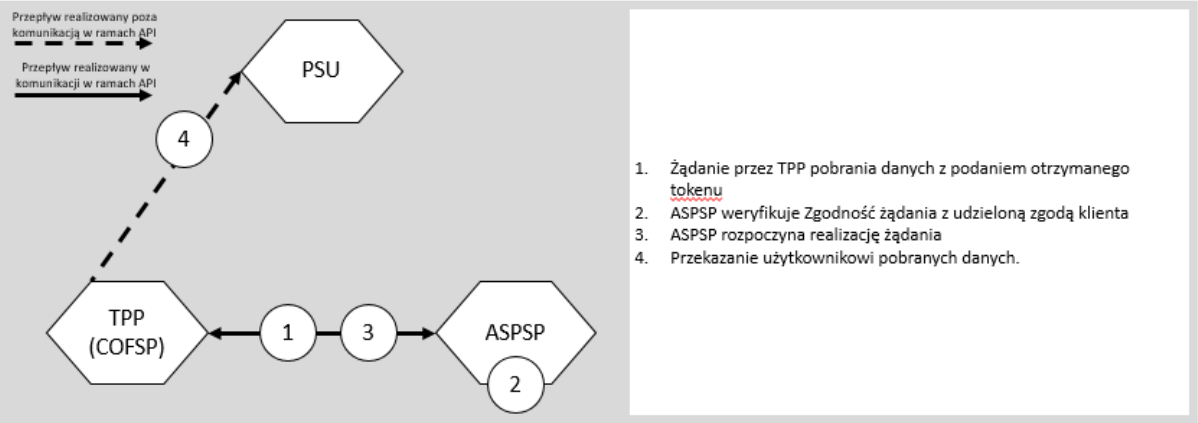
9.3 Asynchroniczna usługa AIS

Asynchroniczne wywołania metod jako wywołania zwrotne (CallBack), gdzie TPP przekazuje zlecenie wykonania operacji do ASPSP wraz z przekazaniem zwrotnego adresu, zostaną zdefiniowane w kolejnej wersji standardu PolishAPI.

10 Opis techniczny usług CAF

Rozdział stanowi streszczenie specyfikacji API w formacie swagger zdefiniowanej w Załączniku nr 1 oraz dokumentacji w formacie swagger-html2 w Załączniku nr 2.

10.1 Diagram aktywności w usłudze CAF



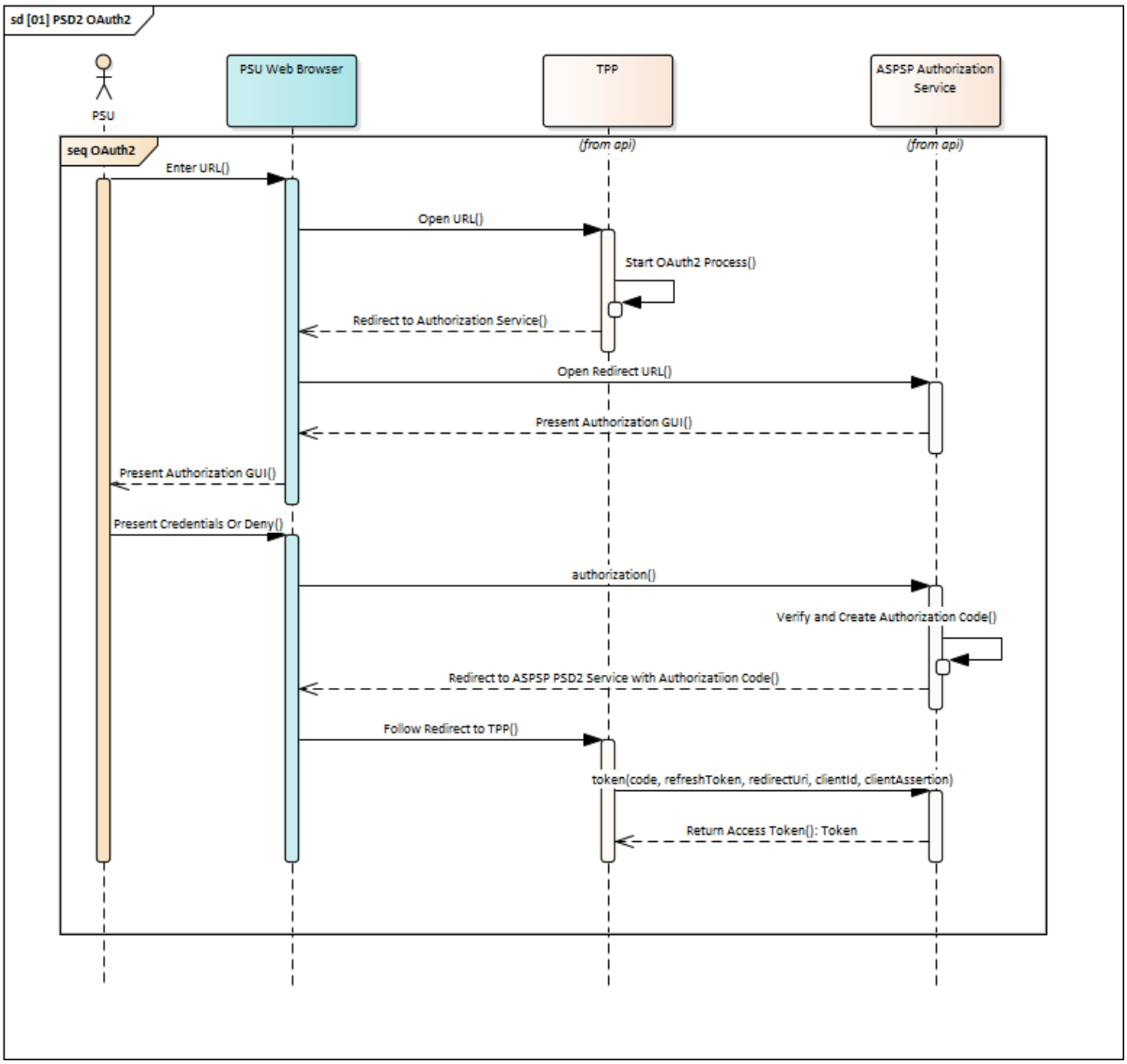
Ilustracja 21: Wysokopoziomowy diagram aktywności w usłudze CAF

10.2 Struktura zapytania (w tym opis pól i wymagalność)

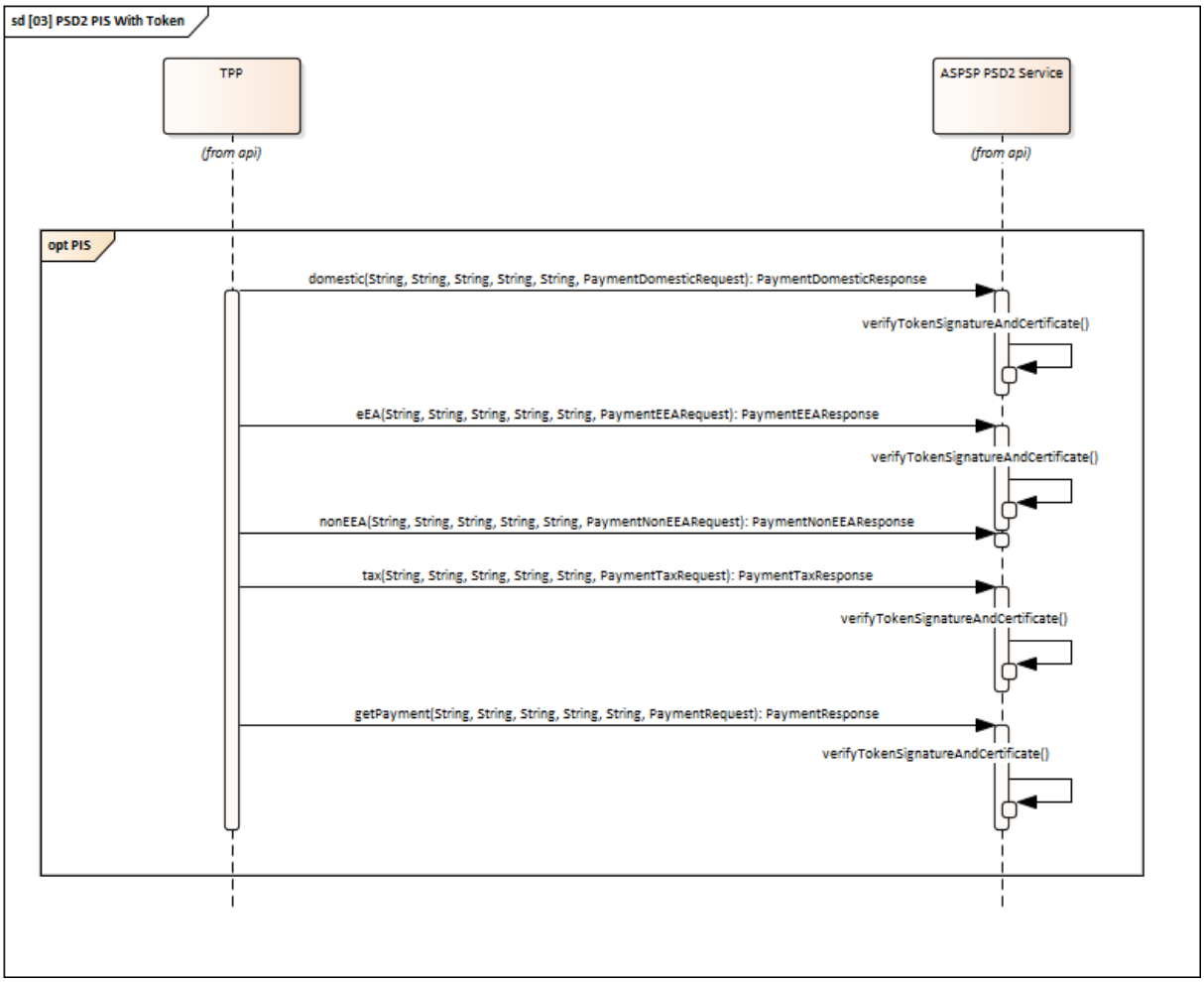
Zasób (endpoint)	Opis	Klasa obiektu KMD przekazywana w żądaniu i odbierana w odpowiedzi
/confirmation/{wersja}/getConfirmationOfFunds	Potwierdzenia dostępności środków	confirmationOfFundsRequest/ confirmationOfFundsResponse

11 Diagramy sekwencji dla wywołań metod interfejsu PSD2 (PL)

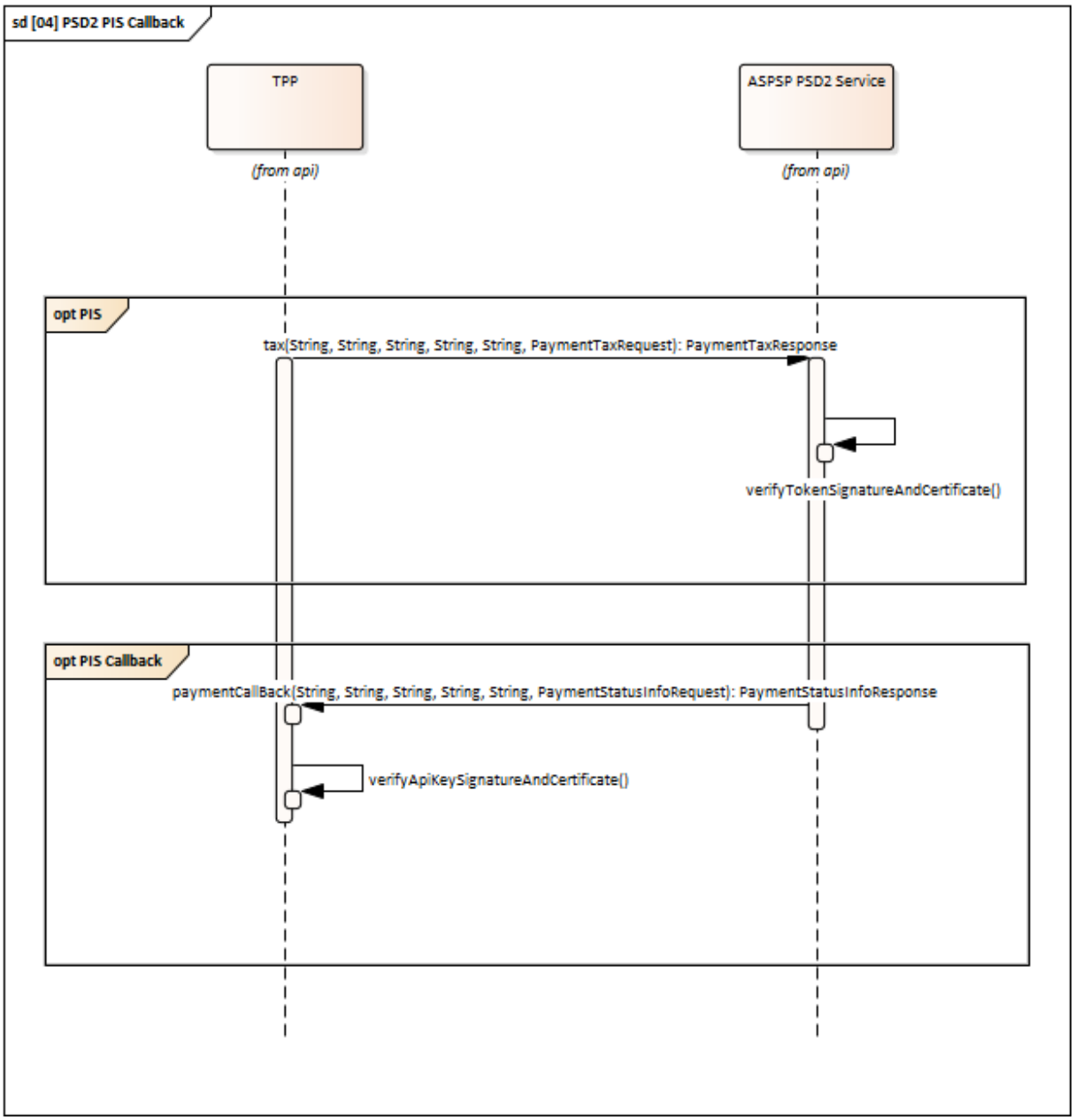
11.1 Diagram sekwencji dla autoryzacji OAuth2



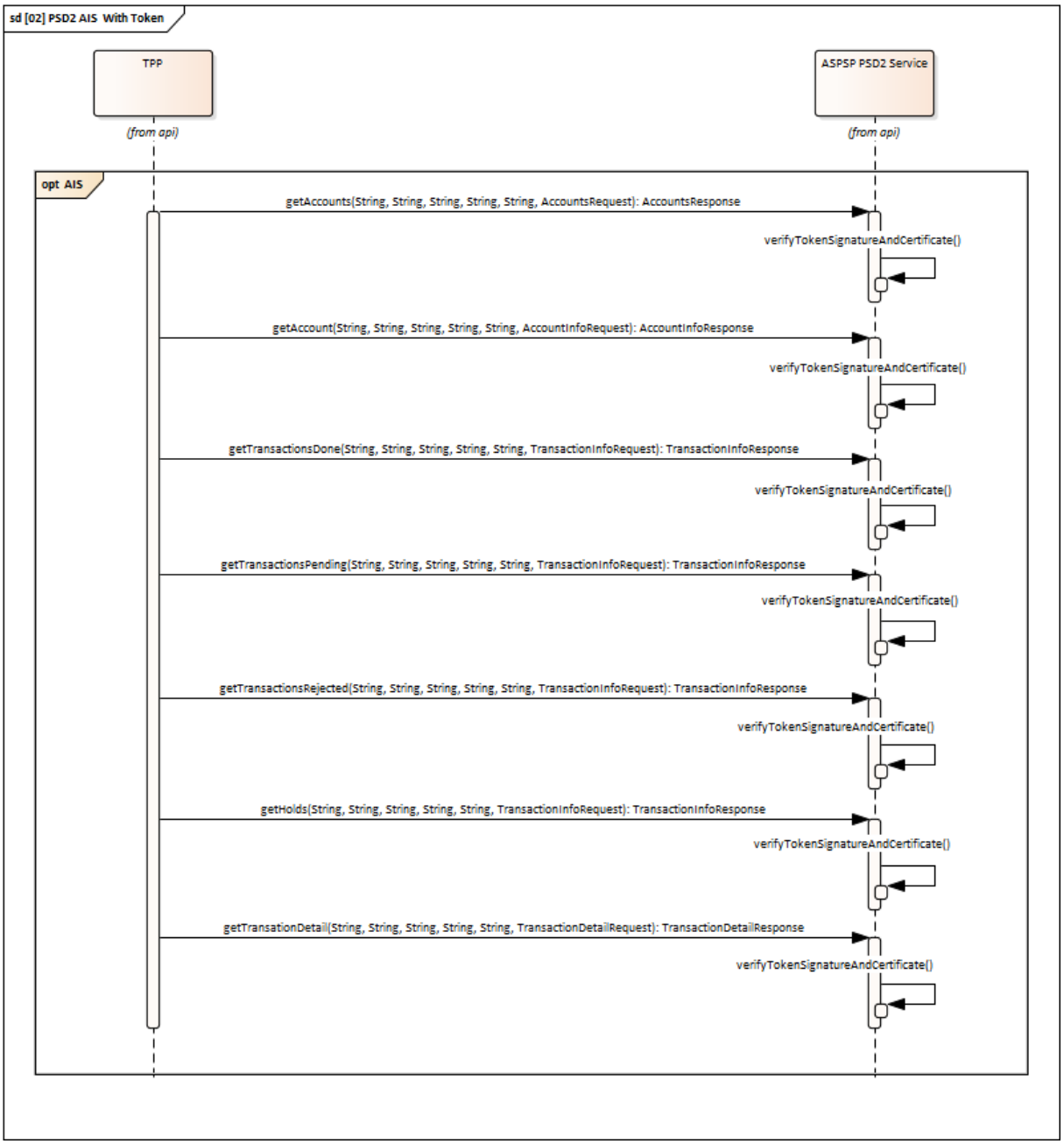
11.2 Diagram sekwencji dla wywołań PIS z autoryzacją OAuth2



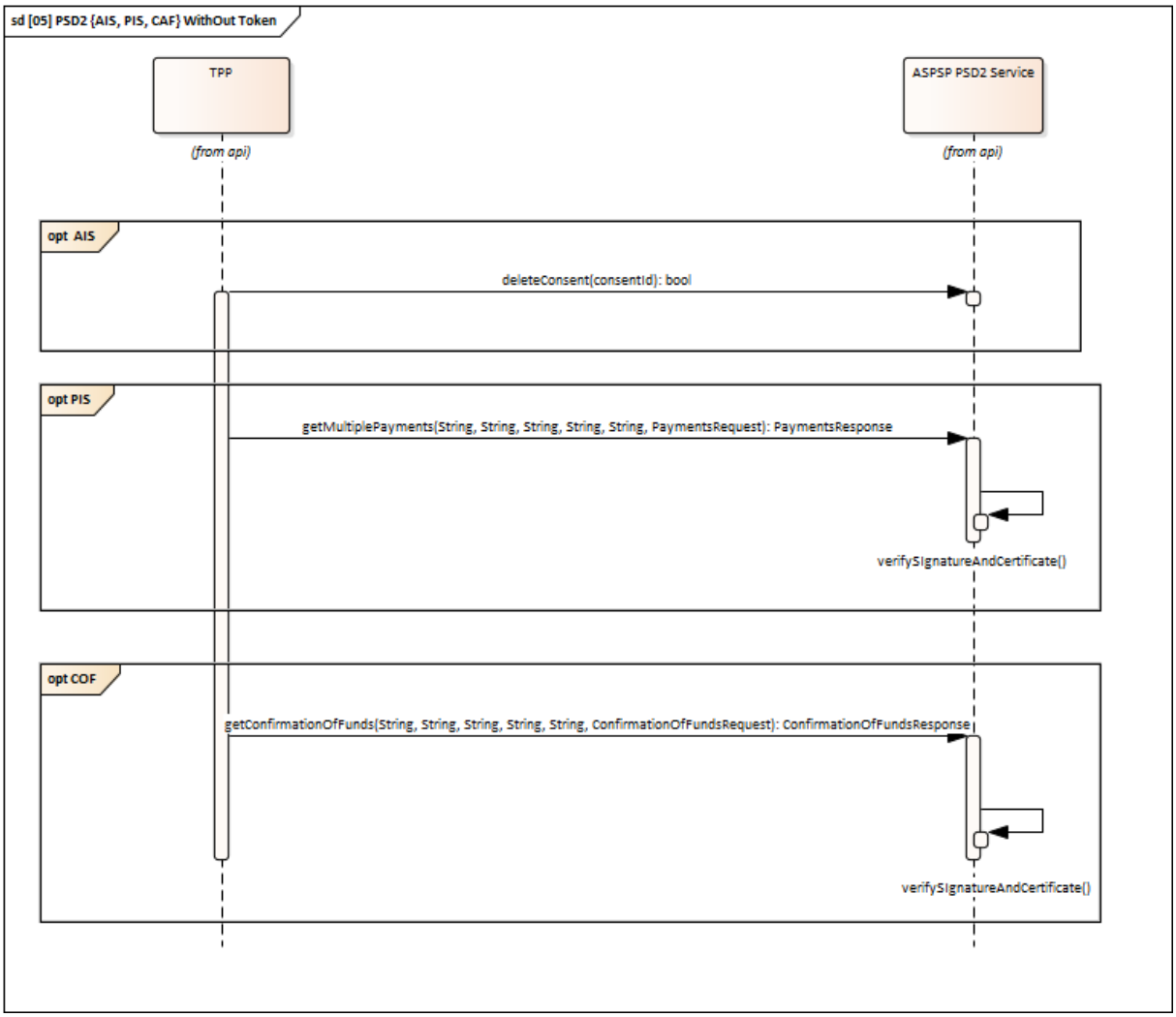
11.3 Diagram sekwencji dla wywołań Callback PIS



11.4 Diagram sekwencji dla wywołań AIS z autoryzacją OAuth2



11.5 Diagram sekwencji dla wywołań AIS, PIS, CAF bez autoryzacji OAuth2



12 Kody błędów

Etap	Błąd	Kod HTTP	Sposób obsługi
Przekierowanie klienta w domenę ASPSP, wraz z przekazaniem w adresie przekierowania parametrów inicjowanej płatności	Przekazanie niepoprawnych parametrów	400	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (zgodnie z RFC6749 4.1.2.1)
ASPSP weryfikuje tożsamość TPP w Hub Tożsamości oraz weryfikuje, czy dane TPP może prosić o wskazane zgody (AIS czy PIS)	Niepoprawna weryfikacja tożsamości TPP	401	Wyświetlenie komunikatu użytkownikowi
	Niepoprawna weryfikacja licencji TPP (np. tylko AIS)	403	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (zgodnie z RFC6749 4.1.2.1)
Klient loguje się w domenie ASPSP	Niepoprawne logowanie 1 raz	401	Oczekiwanie na poprawne zalogowanie klienta
	Niepoprawne logowanie kilkukrotnie	401	Oczekiwanie na poprawne zalogowanie klienta
	Brak aktywacji usług TPP (opt-out)	403	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (zgodnie z RFC6749 4.1.2.1)
	Brak środków	422	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (odpowiedni kod błędu zwracany przy wywołaniu usługi płatności)
Klient wyraża zgodę w żądanym lub ograniczonym zakresie, ewentualnie odrzuca prośbę	Odrzucenie żądania przez klienta	403	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (zgodnie z RFC6749 4.1.2.1)
	Niepoprawna autoryzacja przez klienta	403	Zwrotne przekierowanie klienta w domenę TPP i zakończenie procesu (zgodnie z RFC6749 4.1.2.1)
Zwrotne przekierowanie klienta w domenę TPP	Wyłączenie urządzenia końcowego klienta bezpośrednio przed przekierowaniem	-	TPP ma możliwość dokończenia operacji poprzez pobranie tokenu przy pomocy contextId
Pobranie tokenu autoryzacyjnego przez TPP od ASPSP	Nieznany TPP	401	Zakończenie procesu bez przyjęcia dyspozycji
	Niepoprawne parametry żądania tokenu	400	Zakończenie procesu bez przyjęcia dyspozycji
	Brak możliwości nawiązania komunikacji z ASPSP	-	Zakończenie procesu bez przyjęcia dyspozycji
ASPSP weryfikuje zgodność żądania inicjacji płatności z udzieloną zgodą klienta	Niezgodność z udzieloną zgodą	401	Zakończenie procesu bez przyjęcia dyspozycji

	Przekroczono limit żądania dla żądanej usługi	429	Zakończenie procesu bez przyjęcia dyspozycji
ASPSP rozpoczyna realizację płatności	Brak środków	422	Zakończenie procesu (zwracany kod błędu)
Przekazanie do TPP informacji o poprawności przyjęcia dyspozycji	Brak możliwości nawiązania komunikacji z TPP	-	Ponowienie komunikatu x3 Informacja o awarii Możliwość ponowienia wszystkich komunikatów
Przekazywanie TPP przez ASPSP informacji o zmianach stanu realizacji dyspozycji	Brak możliwości nawiązania komunikacji z TPP	-	Ponowienie komunikatu x3 Informacja o awarii Możliwość ponowienia wszystkich komunikatów
ASPSP weryfikuje zgodność żądania danych o rachunku płatniczym z udzieloną zgodą klienta	Niezgodność z udzieloną zgodą	403	Zakończenie procesu
ASPSP otrzymuje dowolne żądanie	Dostęp do serwisu zablokowany przez ASPSP	403	Zakończenie procesu
ASPSP otrzymuje dowolne żądanie	Dostęp do serwisu zablokowany przez PSU	403	Zakończenie procesu

12.1 Kody błędów dla kodu odpowiedzi HTTP 403

Code	Message
1	Niepoprawna weryfikacja licencji TPP / Incorrect verification of TPP licenses
2	Brak aktywacji usług TPP / No activation of TPP services
3	Odrzucenie żądania przez klienta / Rejection of the request by the client
4	Niepoprawna autoryzacja przez klienta / Incorrect authorization by the client
5	Niezgodność z udzieloną zgodą / Non-compliance with the consent given
6	Dostęp do serwisu zablokowany przez ASPSP / Access to the service blocked by ASPSP
7	Dostęp do serwisu zablokowany przez PSU / Access to the website blocked by the PSU
8	Zablokowany dostęp TPP do usług bankowych przez bank / Blocked TPP's access to bank services by the bank
9	Zablokowany dostęp TPP do usług bankowych przez klienta / Blocked TPP's access to bank services by the client

13 Rekomendacje implementacji standardu

13.1 Obsługa przekroczenia maksymalnego dozwolonego czasu (timeout)

Ze względu na mogące wystąpić w trakcie przetwarzania żądania http zdarzenia typu timeout, ASPSP musi zapewnić weryfikację unikalności na w warstwie serwerowej na poziomie id wywołania (requestId). Po stwierdzeniu nie-unikalności wywołania ASPSP zwraca błąd 400.1 (Powtórzone wywołanie).

Rekomendowana wartość timeout (czasu przetwarzania żądania) to 30 sekund.

13.2 Weryfikacja TPP

Autentykację TPP należy przeprowadzać w oparciu o certyfikaty komunikacyjny (SSL) oraz podpisujący (jws) sprawdzając jednocześnie czy certyfikaty odpowiadają identyfikatorowi TPP (tppId) w bazie danych ASPSP. Wartość tppId jest ustalana przez ASPSP podczas rejestracji TPP, sugerowaną wartością jest EUNIP TPP.

13.3 Oauth2

Zaleca się aby ASPSP posiadał w swojej konfiguracji dla danego client_id listę redirect_uri, które mogą być wykorzystane. Dzięki czemu ASPSP nie przekieruje klienta na niewłaściwy adres URI, który może być podłożony przez niezaufaną stronę.

13.4 Antyfraud

W celach przeciwdziałania potencjalnym oszustwom wprowadzona została dedykowana Klasa RequestHeader, przekazywana w każdym żądaniu, zawierająca informacje o PSU takie jak: adres IP oraz userAgent. Struktura będzie pomocna ASPSP w zaimplementowaniu mechanizmów zabezpieczających.

Dodatkowo rekomenduje się, aby podmioty uczestniczące w projekcie dokonywały wymiany informacji w zakresie podejrzeń nieautoryzowanych transakcji/skompromitowanych IP, itp.

14 Spis Załączników

Załącznik nr 1: Plik definicji interfejsu RESTfull api w formacie swagger: „2.0” - PolishAPI-ver1.0.0.yaml

Załącznik nr 2: Dokumentacja SDK RESTfull api w formacie swagger-html2 - PolishAPI-ver1.0.0.html

Załącznik nr 3: Plik definicji interfejsu wywołań zwrotnych RESTfull api w formacie swagger: "2.0" - PolishAPI-CallBack-ver1.0.0.yaml

Załącznik nr 4: Dokumentacja SDK interfejsu wywołań zwrotnych RESTfull api w formacie swagger-html2 - PolishAPI-CallBack-ver1.0.0.html

Załącznik nr 5: Plik definicji scope_details - rozszerzenia interfejsu OAuth2 w postaci json/schema - PolishAPI-scope_details-ver1.0.0.json

Załącznik nr 6: Dokumentacja SDK scope_details - rozszerzenia interfejsu OAuth2 w formacie swagger-html2 - PolishAPI- scope_details -ver1.0.0.html