Lp	Komentarz / uwaga	Sugerowany zapis / uzasadnienie zmiany	Czy uwzględniono w specyfikacji?	Odpowiedź / komentarz zaspołu projektowego
1	Od 1 stycznia 2017 r. wprowadzono jeden przelew do ZUS oparty na standardowym poleceniu przelewu i komunikacie Elixir 11n. Każdy płatnik składek otrzymał własny Numer Rachunku Składkowego, w którym zaszyty jest m.in. jego numer NIP i numer rozliczeniowy ZUS. W specyfikacji Polish API uwzględniono stary standard przelewu dedykowany płatnościom do ZUS, który obowiązywał do końca grudnia 2017 r. i oparty był na komunikacie Elixir 12n (przelew zawierał m.in. pola zawierające informacje identyfikujące płatnika, fundusz, typ wpłaty, okres itp.).	Nie ma potrzeby uwzględniania w Polish API standardu przelewu, który przestał istnieć z końcem grudnia 2017 r.	nie	W ramach usługi inicjowania płatności przelew do ZUS nie został uwzględniony - ze względu na zmiany w regulacjach.
2	Standard Polish API uwzględnia mechanizm uwierzytelniający oparty na przekierowaniu użytkownika w domenę ASPSP (tzw. mechanizm „redirection"). Jest to bezpieczna metoda uwierzytelnienia od lat z powodzeniem praktykowana w polskim sektorze bankowym np. w usłudze pay-by-link. Jednak w RTSie on SCA and CSC w art. 32 wyraźnie wskazano: Dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, zapewniają, aby interfejs ten nie stwarzał przeszkód w świadczeniu usług inicjowania płatności i usług dostępu do informacji o rachunku. Przeszkody takie mogą obejmować m.in. uniemożliwianie dostawcom usług płatniczych, o których mowa w art. 30 ust. 1, wykorzystywania danych uwierzytelniających wydanych przez dostawców usług płatniczych prowadzących rachunek ich klientom, wymuszanie przekierowania do mechanizmu uwierzytelniania lub innych funkcji dostawcy usług płatniczych prowadzącego rachunek, wymóg uzyskania dodatkowych zezwoleń oraz dodatkowych rejestracji oprócz tych przewidzianych w art. 11, 14 i 15 dyrektywy 2015/2366 lub wymóg dodatkowej weryfikacji zgody udzielonej dostawcom usług inicjowania płatności i usług dostępu do	Warto ująć w standardzie Polish API inne metody uwierzytelnienia, które spełniają wymogi prawne (RTS on SCA and CSC). Dzięki temu Polish API zyska większą szansę na upowszechnienie.	tak	

	informacji o rachunku przez użytkowników usług płatniczych…			
3	Pola w specyfikacji biznesowej powinny wskazywać przykładowe wartości i określać, czy są one opcjonalne, aby format był bardziej czytelny	Dodać wartości przykładowe oraz opcjonalny wskaźnik do listy pól	nie	Zakres danych oraz ich wymagalność może różnić się w różnych implementacjach. 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

4	Pole identyfikacji rachunku powinno posiadać odpowiadające pole „typ identyfikacji". Kod IBAN jako domyślny typ identyfikacji przyjęty w standardzie nie jest szeroko stosowany w niektórych krajach, np. w Wielkiej Brytanii. Kod IBAN może nie mieć zastosowania w odniesieniu do portfeli niektórych banków powierniczych, które posiadają bardziej zdywersyfikowane papiery wartościowe. W konsekwencji, nie byłoby łatwo opisać przelewu do Wielkiej Brytanii, portfela cyfrowego lub na rachunek w banku powierniczym w Szwajcarii.	Dodać pole typu identyfikacji rachunku z domyślną wartością „kod IBAN"	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
5	Każda kwota powinna posiadać odpowiadające pole z walutą kwoty (np. w zapytaniu getTransactionsDoneRequest)	Dodać pole waluty do wszystkich odpowiednich pól kwot w specyfikacji	tak	
6	Parametry niestandardowe w zapytaniach API powinny być opcjonalne (np. scope_details) oraz powinny wskazywać wartości domyślne	Sprawić, aby parametry niestandardowe były opcjonalne w specyfikacji	nie	Ustalenie grupy projektowej Polish API. W parametrze scope_details zawarte są istotne informacje.
7	Czcionka wybrana w specyfikacji API powinna zawierać polskie znaki, widać, że stosowana jest czcionka zastępcza dla polskich znaków (np. w słowie „Płatności")		tak	
8	Regulacyjne standardy techniczne (RTS) wymagają lepszego wpisu w słowniku		tak	
9	Infrastruktura PKI powinna zostać opisana w dokumencie, lub co najmniej należałoby opisać model w którym ma operować.	Przyjęty model PKI może istotnie wpływać na implementację API, należy zatem zdecydować jak ma wyglądać a potem szczegółowo opisać go w dokumencie.	tak	

10	O ile ASPSP mają dowolność w przyjmowaniu rozwiązań technicznych (w tym nie korzystania z PolishAPI), sugeruję, aby standard musiał być zaimplementowany w całości.	Częściowa implementacja standardu mija się z celem - powstanie N implementacji, które w części będą działać identycznie, w części podobnie a w części - w ogóle. Jeśli celem wypracowania jednego rozwiązania jest redukcja kosztów związanych z implementacją po stronie konsumentów, to ten zapis nie ma sensu. Proponuję skoncentrować się na minimalnym podzbiorze, który może zostać zaimplementowany w całości a następnie rozwijać API w oparciu o ramy czasowe, które pozwolą na pełną implementację maksymalnej ilości podmiotów.	tak	
11	Uwaga ogólna - wszędzie w dokumencie należy stosować nomenklaturę branżową, preferowalnie w języku angielskim.	Wprowadzenie (pierwsza część dokumentu) opisuje relatywnie szczegółowe elementy posługując się sformułowaniem “kody autoryzacyjne” - nie jest jasne do końca dokładnie o który kod chodzi. Proponuję odwołanie do szczegółowego dokumentu opisującego dane sformułowanie, tak jak w dalszej części dokumentu.	tak	
12	Nie jest jasne co oznacza “odrębna sesja XS2A”.	Czy chodzi o sesję TLS, czyli każdy cykl zapytanie-odpowiedź wymaga odrębnego cyklu połączenia, czy może o inny rodzaj sesji? Należy to wyjaśnić poza wszelką wątpliwość.	tak	
13	Istnieją produkty finansowe z okresem ważności oprocentowania krótszym niż 1 rok (np 2 miesiące) Jak oznaczane jest zmienne oprocentowanie takiego rachunku?		tak	
14	Zahashowany numer karty płatniczej jest kiepskim rozwiązaniem z punktu widzenia użyteczności.	Zamiast tego, proponuję użyć pierwszych czterech + ostatnich czterech cyfr numeru karty, lub tylko czterech ostatnich.	tak	
15	Czym jest HUB PSD2 i jaki ma zakres odpowiedzialności?	Zakładam że to zagadnienie będzie całkowicie wyjaśnione po dodaniu opisu modelu PKI do dokumentu.	tak	

16	Uzasadnienie punktu 2 jest błędne.	Wykorzystanie wzajemnej autentykacji przez TLS nie ma absolutnie żadnego związku z tym, czy urządzenie klienckie (nie zdefiniowane pojęcie) może korzystać z API.	tak	
17	Ryzyko, że produkt PolishAPI będzie trudny w konsumpcji przez TPP.	Proponuję skupić się na podzbiorze funkcjonalności co do którego jest pewność, że może zostać zaimplementowany przez prawie wszystkich uczestników.	nie	Ustalenie grupy projektowej Polish API. Tam gdzie jest to możliwe, starano się wyjść poza minimalną część wspólną.
18	Błąd w rozumowaniu.	Nic nie stoi na przeszkodzie, aby zapewnić niezaprzeczalność indywidualnych wiadomości za pośrednictwem JWS (RFC7515), niezależnie od użytej metody HTTP.	nie	Ustalenie grupy projektowej Polish API.
19	Wymaganie, aby każda wymiana HTTP była podpisana w celu zapewnienia niezaprzeczalności wprowadza ryzyko związane z wydajnością.	Aby wygenerować JWS, lub jakikolwiek inny podpis cyfrowy, potrzebna jest cała treść do podpisania. Znaczy to, ze cała wiadomość do podpisania musi znaleźć się w pamięci, albowiem nagłówki HTTP wysyłane są zanim wysłana jest treść. Rezygnując z tego wymagania, zyskujemy możliwość inkrementalnego wysyłania danych do klienta, który to klient również może inkrementalnie te dane przetwarzać. To rozwiązanie może mieć znaczenie w przypadku dużych ilości danych przesyłanych jednocześnie.	nie	Ustalenie grupy projektowej Polish API. Uznajemy, że bezpieczeństwo ma w tym wypadku priorytet. Inkrementalne przekazywanie danych planujemy rozwiązać poprzez stronicowanie.
20	Użycie Accept-Language ma wątpliwy sens.	Trudno jest mi znaleźć taki scenariusz w którym zwracanie danych w różnych językach miałoby sens.	nie	Opis statusu transakcji wymaga decyzji o języku. Język jest wymagany w przypadku banków dysponujących wielojęzycznymi systemami.

21	Content-Type powinien być szczególny, nie ogólny, jak application/json.	Zamiast generycznego application/json, bardziej właściwe byłoby zastosowanie konkretnego typu (http://www.iana.org/form/media-types), na przykład: application/polishapi.v1+json	nie	Używamy application/json ze względu na powszechność wykorzystania tego standardu. Niektóre narzędzia mogą nie wspierać proponowanego podejścia.
22	Nie jest jasne dlaczego dane autoryzacyjne nie mogą być przesyłane w postaci parametrów URI.	Wyjaśnić powód tej decyzji.	nie	Przyjęliśmy założenie, że podpis nie obejmuje URI, w związku z tym przyjęliśmy użycie metody POST zamiast GET. URI jest częścią publiczną komukacji i może zostać skompromitowane.
23	Poświadczenia tożsamości są poufne (...) - pojęcie poświadczenia tożsamości nigdzie nie jest zdefiniowane, postać jawna nie jest zdefiniowana.	Tak naprawdę nie wiadomo co to znaczy i w jakim kontekście ta decyzja ma znaczenie - wyjaśnić.	tak	
24	To zdanie wydaje się być wyrwane z kontekstu - być może jest to pozostałość jakiś notatek?	Wyjaśnić jak miałaby działać autoryzacja po stronie klienta i dlaczego nie jest dozwolona.	tak	
25	Jak zarządzamy kluczami w kontekście podpisów JWS?	Wyjaśnić, jak klucze są dopuszczane do użycia, jak następuje rotacja, skąd można ustalić, że klucz użyty do podpisu nadal jest ważny, etc.	tak	
26	Mam wrażenie że ewentualna podatność na atak CSRF może odbywać się tylko przy interakcji przeglądarki z ASPSPs.	Wyjaśnić kontekst, do którego odnosi się ta uwaga, albowiem nie odnosi się ona do interakcji typu serwer-serwer.	nie	

27	Jeśli konieczne jest przechowywanie zawartości zapytań i odpowiedzi HTTP ze względu na niezaprzeczalność, to należy określić warunki przy których zapytanie będzie akceptowane.	W zależności od implementacji, czas od wygenerowania zapytania do odebrania go przez drugą stronę, może zająć nawet sekundę. Należy ustalić maksymalną rozbieżność zegarów między dwoma uczestnikami.	tak	
28	Trudno mi zrozumieć celowość wprowadzenia do API callbacków w tej postaci.	Ponad wszelką wątpliwość, zwrócenie listy kont, lib stronicowanej listy transakcji powinno zająć mniej czasu niż timeout odczytu w HTTP (30 sekund) więc nie istnieje powód, aby konkretnie te endpointy obsługiwały operacje w trybie asynchronicznym. Całkowicie sensowne natomiast byłoby dostarczanie informacji o zmieniającym się statusie płatności, ale w API tego nie ma.	nie	Jeżeli zapytanie TPP o historię transakcji przekracza zdefiniowany przez ASPSP w dokumentacji implementacyjnej rozmiar, wysyłany jest komunikat błędu, informujący o konieczności skorzystania z asynchronicznej metody.
29	Zasoby udostępniane przez API doskonale wpisują się w REST, ale autor z jakiegoś powodu wybrał coś co przypomina RPC. Według mnie, jest to decyzja której zmiana będzie miała największy pozytywny wpływ na to na ile API będzie użyteczne.	Przeważająca ilość publicznych API wykorzystywanych w ekosystemie webowym wykorzystuje REST jako styl architekturalny, oraz JSON jako reprezentację danych. Konwencje przyjęte przez REST są powszechnie znane w środowisku deweloperskim i proponuję, aby je tutaj zastosować. Zastosowanie REST radykalnie uprości konstrukcję całego API.	nie	Decyzje projektowe uzasadnione były zachowaniem maksymalnego poziomu bezpieczeństwa.
30	Brakuje informacji o tym jak ma być skonstruowany JWS.	Uzupełnić te informacje. W przypadku zastosowania REST, należy uzupełnić JWS o dane z nagłówków HTTP, które są istotne z punku widzenia niezaprzeczalności.	nie	Ustalenie grupy projektowej Polish API. Nagłówki HTTP są wykorzystaywane w ograniczonym zakresie.

31	Zamiast kilku endpointów do pobierania transakcji w różnych stadiach, wystarczy jeden endpoint z filtrem.		nie	Struktura danych w odpowiedzi jest różna.Struktura endpointów odzwierciedla strukturę obiektów biznesowych w systemach bankowych. W szczególności niektóre z tych obiektów nie są transakcjami finansowymi.
32	W jaki sposób klient korzystający z TPP będzie wiedział jakim opłatom podlega dany przelew? W bankowości internetowej pojawiają się ostrzeżenia o opłacie np. z rachunku oszczędnościowego, kiedy to zazwyczaj jeden przelew w miesiącu jest darmowy a pozostałe płatne. Opłaty lub prowizje pojawiają się tez przy przelewach ekspresowych, międzynarodowych, itp. Przeglądając specyfikację nie znalazłem takiego mechanizmu. Czy zakładamy, że TPP nie ma obowiązku informować klientów o opłatach czy o terminie realizacji przelewu (jeśli np. jest zlecony po cut-off time), a klient zgadza się na zlecanie przelewów „w ciemno” przez TPP?		nie	Decyzja o udostepnieniu tej informacji pozostaje w gestii ASPSP.

33	Opisany schemat jest nie do zaakceptowania z punktu widzenia RTS. De facto jest tu podwójna zgoda - najpierw na stronie TPP - potem na stronie ASPSP. Możliwość wyboru rachunków po zalogowaniu modyfikuje uprzednio przekazaną zgodę na pobranie danych ze wszystkich rachunków, co jest niezgodne z RTS. Informacyjnie: w praktyce AISP-y takie jak Kontomatik zawsze będą potrzebowały wszystkich rachunków. Ten flow należy traktować jako powszechny w praktyce rynkowej.		tak	Zaproponowano nowy proces.
34	Bieżący Swagger pozostawia niemal wszystkie pola technicznie opcjonalne. Mam tu na myśli wiersze "Required: ...". Przykładowo w rachunku nie jest wymagane nawet saldo, a w transakcji nie jest wymagany ani recipient and sender. Jako programista i CTO mogę zagwarantować, że programiści z firm zewnętrznych, którzy będą to implementowali na zlecenie ASPSP, nie przeczytają "biznesowej" specyfikacji (gdzie sytuacja wygląda trochę lepiej), tylko skupią się na technicznej (Swagger) i wyplują z systemów techniczne minimum. Potem jako AISP będziemy musieli z 26 bankami latami "użerać się" o brakujące pola. I nie mówię tu już nawet o "złej woli" ASPSP tylko o najbardziej prawdopodobnym scenariuszu implementacyjnym wynikającym ze Swaggera i realiów pracy programistów.		nie	Zakres danych oraz ich wymagalność może różnić się w różnych implementacjach. 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
35	Brakuje np daty otwarcia rachunku, choćby jako opcjonalne pole. Taka informacja jest bardzo często widoczna w bankowości internetowej.		nie	Standard obejmuje zakres pól w oparciu o regulacje (PSD2 oraz RTS).

36	opis procesu wyrażania zgody na AIS według nas jest niepoprawny - w szczególności przekierowanie na stronę TPP w naszej opinii następuje po wyborze rachunków przez PSU. Jeżeli bowiem to Bank miałby przesłać do TPP wszystkie dostępne rachunki, to powstaje problem czy jest do tego uprawniony. To bowiem TPP „przychodząc" do Banku powinien mieć już wskazane rachunki. Przekazanie przez Bank na tym etapie numerów rachunków, jeżeli klient ich nie wskazał konkretnie może być uznane za ujawnienie tajemnicy bankowej. Ze swojej strony prosimy, aby podczas analizy tego materiału, zweryfikować także, czy w ramach procesu wyrażania zgody na AIS, PSU może wyrazić zgodę na kilka 'wskazanych' przez niego rachunków płatniczych. Doprecyzowując, czy jeśli PSU wskaże np. dwa rachunki płatnicze, to może to potwierdzić jednym SCA (np. SMS)?		tak	Zaproponowano nowy proces.
37	dlaczego „Proces udzielania zgody przez PSU dla ASPSP na wykonanie usługi COF jest poza zakresem niniejszego dokumentu"?		tak	Proces udzielania zgody przez PSU dla ASPSP na wykonanie usługi COF zostanie opisany w kolejnych wersjach specyfikacji.
38	dlaczego „Sposób realizacji tej funkcjonalności jest poza zakresem standardu Polish API."?		nie	Poza zakresem dokumentu, ponieważ nie specyfikujemy interfejsów ani po stronie TPP, ani po stronie ASPSP.
39	brak definicji składników SCA (tj. „pierwszy" i „drugi") – szczególnie istotne w kontekście mechanizmu 'embeded'.		nie	Nie widzimy potrzeby uszczegóławiania tych zapisow.
40	nie rozumiem stwierdzenia „(…) w tym zakres dat".		tak	

41	uważamy, że z zakresu danych AIS powinno jeszcze zostać wyłączony „Oprocentowanie rachunku”. Co prawda wysokość oprocentowania danego rachunku jest jedną z informacji o rachunku, której dotyczy usługa AIS, to jednak wskazać należy, iż wysokość oprocentowania, często ustalana indywidulanie z klientem powinna być uznana za tajemnicę handlową i nie udostępniana podmiotom trzecim.		tak	
42	występuje niespójność pomiędzy częścią biznesową, a techniczną, które funkcjonalności mają być uwzględnione w sekcji Compliance, a które w Premium. W szczególności mamy tutaj na myśli funkcje: Dla AIS Compliance powinno być: 6.1. /accounts/{wersja}/getAccount - Pobiera pojedynczy rachunek płatniczy 6.2. /accounts/{wersja}/getTransactionsDone - Pobiera transakcje zrealizowane na rachunku 6.3. /accounts/{wersja}/getTransactionsRejected - Pobiera transakcje odrzucone na rachunku 6.4. /accounts/{wersja}/getHolds - Pobiera blokady na rachunku 6.5. /accounts/{wersja}/getTransationDetail - Pobiera szczegóły pojedynczej transakcji/blokady Dla AIS Premium: 6.6. /accounts/{wersja}/getAccounts - Pobiera wszystkie rachunki PSU 6.7. /accounts/{wersja}/getTransactionsPending - Pobiera transakcje oczekujące na rachunku		nie	Zaproponowano nowy proces.
43	czy została rozstrzygnięta kwestia tajemnicy bankowej? W nowelizacji Ustawy o Usługach Płatniczych brak informacji i brak informacji o ewentualnych zmianach również do Prawa bankowego.		nie	W procedowanym projekcie UUP uwzględniono zmiany do Prawa bankowego, zwalniające bank z tajemnicy bankowej w ramach świadczenia usług AIS i PIS)

44	W zależności od decyzji dot. definiowania przelewów zagranicznych EEA i nonEEA, należy zmienić pole „Typ przelewu". Jeśli wprowadzone zostanie podział na przelewy standardowe (realizowane w trybie D+1) i ekspresowe (w trybie D), to wówczas należy zaktualizować pole komentarza. Natomiast jeśli pozostanie tylko tryb standard, to w ogóle trzeba usunąć „Wartość stała – SEPA" z pola komentarza. Per analogia, w przypadku przelewów zagranicznych nonEEA, komentarz do pola „Typ przelewu" albo należy uzupełnić o tryb standardowy (D+2), ekspresowy (D) i pilny (D+1), lyb całkowicie usunąć „- Wartość stała – nieEEA".		tak	
45	Występuje niespójność pomiędzy częścią biznesową i techniczna. Dlatego proponujemy zmianę zapisu z: Jest: „Ponadto, ASPSP udostępni mechanizmy filtrowania danych, zgodnie z kryteriami dostępnymi on-line w systemie ASPSP (czyli przez bankowość elektroniczną), np.: a) Data księgowania transakcji, w tym zakres dat; b) Kwota transakcji; c) Dane drugiej strony transakcji; d) Opis transakcji; e) Inne cechy przypisane do transakcji widoczne w historii transakcji rachunku płatniczych. Powinno być:" Ponadto, ASPSP udostępni mechanizmy filtrowania danych, zgodnie z kryteriami dostępnymi on-line w systemie ASPSP (czyli przez bankowość elektroniczną), tj.: a) Zakres data księgowania transakcji; b) Zakres kwot transakcji; c) obciążenia i uznania na rachunku płatniczym.		tak	

46	uwaga dot. /v1.0/payments/v1.0/standardDomestic-Request, /v1.0/payments/v1.0/expressDomestic- Request, /v1.0/payments/v1.0/standardNonEEA- Request: Wskazane pola są zbędne: "transferType": { "code": "string", "description": "string" }, Proponujemy, aby dla expressDomestic inne pole transferType o typie enumeratywnym: ExpressElixir, BlueCash, Sorbnet, Proponujemy również dla addTax pole transferType o typie enumeratywnym Standard, ExpressElixir, jeśli biznesowo zostanie podjęta decyzja o udostępnieniu przelewów podatkowych również ExpressElixirem. Jeśli nie, to pole transferType zbędne.		tak	
47	W nawiązaniu do pkt. dot. przelewów EEA i nonEEA. Wówczas proponujemy rozważyć zmianę nazwy endpointów: payments/standardEEA na payments/EEA, payments/standardNonEEA na payments/nonEEA i wówczas można dodać pole transferType na wejściu z enumeratorami. Dla EEA: Standard, Express, dla NonEEA: Standard, Urgent, Express.		tak	

48	Potrzebujemy udostępniać informację o więcej niż jednym kursie w szczegółach transakcji. Przykładowo wysyłając USD z rachunku EUR następuje najpierw przewalutowanie EUR->PLN (kupno EUR), a następnie PLN->USD (sprzedaż USD) i pokazujemy oba. Prośba, aby w klasie TransactionDetailResponse- zastąpić pole transactionRate poprzez tablicę: transactionRate: tablica z następującymi polami (od 0 do 2 wystąpień) rate: number($double) format 4,7 fromCurrency: string toCurrency: string Ponadto potrzebujemy 7 miejsc po przecinku w polu na kurs. Obecnie: Kurs transakcji, Format 4,6 / Currency exchange rate		tak	
49	Obecna propozycja metod asynchronicznych zakłada call-back z danymi. Nie jest obsłużone stronnicowanie danych ani integralność ich dostarczenia, co przy znacznej ilości danych może rodzić problemy. Może lepiej, aby ASPSP sygnalizowało poprzez callback do TPP, że wygenerowany został plik (o zdefiniowanym formacie) do pobrania i wówczas TPP pobierało ten plik. Problem do dyskusji.		nie	Ustalenie grupy projektowej Polish API.
50	Prośba o dodanie do getTransactionsRejected pola rejectionDate.		tak	
51	Jak wygląda przypadek użycia getMultiplePayments w ramach PIS? Jaki token byłby tu walidowany? Nie widzę zastosowania w kontekście PISu jednokrotnego, który jest przedmiotem Compliance- proponuję usunąć ze swaggera.		tak	
52	Jeśli oczekujące transakcje nie mają być przedmiotem Compliance, to należy usunąć ze swaggera getTransactionsPending i -Async.		nie	W specyfikacji wprowadzono definicję transakcji oczekujących.

53	Jeśli transactionSegment został usunięty z wymagań biznesowych, to należy usunąć go ze swaggera klasyTransactionDetailResponse		tak	
54	Dużo literówek w opisach Klasa zawierająca infromacje o PSU / PSU Information Class Get list of user"s holded operations Opis pozycji słownika / Descriptiontion Klasa zapytania o pojedyńczy rachunek / Account Information Request Class Status - Czy medoda wykonała się prawidłowo / Status Klasa zawierająca dane banku używanana w żądaniach AIS / AIS Bank Data Class Klasa zawierająca dane nazwy i adresu w postaci czterech lini danych / Simple name and Klasa zawierająca dane nadawcy/odbiorcy używanana w żądaniach AIS / AIS Sender Klasa zawierająca dane pozwalajace nakorzystanie z mechanizmu stronicowania / Paging Information Class Klasa reprezentująca inforacje o karcie w ramach transakcji / Transaction Card Information		tak	

55	„Realizacja usług w zakresie Zgodności Każde ASPSP jest zobowiązane do udostępniania usług w zakresie usług Zgodności na mocy PSD2 oraz powiązanych aktów prawnych. ASPSP samodzielnie definiuje, które rachunki bankowe są rachunkami płatniczymi i niezależnie podejmuje decyzje o zakresie udostępnianych danych rachunków płatniczych dostępnych w ramach tej usługi. Realizacja usług w zakresie Zgodności nie będzie wymagała relacji umownej pomiędzy ASPSP a TPP.” Chodzi o podkreślony fragment. O ile drugą część zdania da się wywieść z faktu, że to faktycznie ASPSP decyduje, jaki zakres danych do danego rachunku płatniczego udostępnia online (a przez to jest zobligowany do udostępniania go w ramach AIS), o tyle stwierdzenie, że ASPSP samodzielnie definiuje, które rachunki bankowe są rachunkami płatniczymi jest wg nas nieakceptowalne. Po pierwsze, nie każdy ASPSP to bank, więc słowo „bankowe” należy wykreślić. Przede wszystkim jednak uważamy, że ASPSP nie mogą arbitralnie i dowolnie ustalać, które z prowadzonych przez nich rachunków są płatnicze, a które nie. To dotyczy sedna dyskusji odnośnie definicji rachunku płatniczego… Gdyby można było to sobie ustalać samodzielnie, to w bardzo łatwy sposób ASPSP mogłyby obejść przepisy PSD2 dotyczące obowiązku udostępniania informacji o rachunku płatniczym w ramach usługi AIS, a idąc dalej również obowiązek budowy interfejsu, raportowania itd. Konkludując: uważamy, że zapis ten może pozostać ewentualnie w takiej formie, jak poniżej: „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.”		tak	

56	Zastanawiam się, jaki będzie ten standard, jeśli jego przyjęcie nie będzie obowiązkowe. Gdzie możemy sprawdzić, kto przyjął które elementy? Na innych rynkach, choć API nie jest obowiązkowe, banki dobrowolnie zobowiązały się przestrzegać standardów API na tym rynku w pełni	Opublikować banki, które dobrowolnie zobowiązały się przyjąć API w całości. Lista banków, które zobowiązały się przyjąć jedynie część (jaką część). Słownik banków, które zapewniają alternatywę, z linkiem do opublikowanej dokumentacji.	tak	
57	Jeśli chodzi o kategorie usług, sądzę, że należy przewidzieć więcej opcji. Jest bardzo możliwe (i prawdopodobne), że TPP będą miały podwójne role AISP i PISP. Uwzględnienie tego zmieni przypadek użycia dotyczący sposobu, w jaki TPP będzie interagować z ASPSP poprzez pojedyncze wezwanie oraz uzyskiwać dostęp zarówno do danych, jak i inicjowania płatności. Traktowanie ich jako niezależnych funkcji może prowadzić do gorszego doświadczenia użytkownika poprzez budowanie samodzielnych API, które obsługują tylko jedną rolę – patrz Open Banking w Wielkiej Brytanii	Uznać połączoną rolę AISP i PISP oraz udokumentować sposób, w jaki połączone PISP i AISP mogą wchodzić w interakcję, a ASPSP działać poprzez jednorazowe zapytanie API.	nie	Według interpretacji prawnej ta usługa leży poza zakresem zgodności.
58	W dyskusji na temat metod uwierzytelniania nie wydaje się, aby umożliwiały one TPP wykonywanie uwierzytelnienia bezpośrednio przez klienta. Uważamy, że rozporządzenie (oraz oświadczenia organów regulacyjnych i branżowych UE) zachęcają do nieprzekazywania do ASPSP oraz do przyjmowania przez TPP odpowiedzialności za uwierzytelnienie	Usunąć postanowienie, że metoda uwierzytelnienia pozostaje w gestii ASPSP. Powinna ona pozostawać w gestii TPP. Wymaga się, aby ASPSP zapewniał metodę, dzięki której TPP może zastosować swoje własne uwierzytelnienie. Najgorszy przypadek - to klient dzieli swoje dane z TPP, aby uzyskać bezpośredni dostęp (uznany za ważną ścieżkę dostępu tam, gdzie API nie działają)	nie	Według naszej opinii nie jest to dopuszczalne z regulacyjnego punktu widzenia.
59	Definicja Uwierzytelnienia to proces, w wyniku którego ASPSP weryfikuje tożsamość użytkowników. Jest to również możliwe dla TPP.	Zmienić Uwierzytelnianie – „proces, w wyniku którego ASPSP lub TPP weryfikuje tożsamość PSU.”	nie	Według naszej opinii nie jest to dopuszczalne z regulacyjnego punktu widzenia.

60	1.4.5.2 4) podaje,, że ASPSP prezentuje PSU do wyboru listę rachunków płatniczych. Uważamy, że to TPP powinno kontrolować to doświadczenie użytkownika. Gdy tylko zgoda oraz uwierzytelnienie zostały zaakceptowane, TPP powinno posiadać pełną kontrolę nad doświadczeniem użytkownika, jakie chcą przedstawić klientowi.	Zmienić na 'ASPSP lub TPP prezentuje PSU do wyboru listę rachunków płatniczych, z których...."	nie	Inne procesy zostaną dodane po ustaleniu metod uwierzytelniania.
61	1.4.5.2 Nie wspomina, że saldo oraz dane transakcji (w minimalnym zakresie) będą również dzielone w ramach licencji PISP	Ująć konkretne odniesienie do salda oraz danych transakcji dzielonych z PISP, aby mogli oni zdecydować, czy pragną zainicjować transakcję (Uwaga - PISP powinien mieć dostęp do takich informacji bez żądania dostępu do licencji AISP. Te dane są wymagane w inicjowaniu płatności, ponieważ bez nich PISP ryzykuje inicjowanie płatności, których realizacja jest nieprawdopodobna, co sprawia, że jest to bezużyteczne)	nie	W ramach usługi PIS udostepniane są te dane, które zgodnie z regulacjami, umozliwiają inicjacje płatnosci.
62	Zastosowanie silnego uwierzytelniania klienta (SCA). Istnieją uznane wyłączenia co do czasu stosowania SCA, np. płatności o niskiej wartości, zaufani odbiorcy itp.	Zmienić sformułowanie na „ASPSP lub TPP korzystają z dowolnego wybranego przez siebie systemu silnego uwierzytelnienia (Strong Customer Authentication – SCA), a standard Polish API nie definiuje ani nie rekomenduje żadnego ze sposobów przeprowadzania tej procedury. Jednakże, transakcje będą wyłączone (szczegóły poniżej) zgodnie z tą regulacją. ASPSP może jedynie wyjątkowo oraz przy szczegółowym	nie	W regulacjach opisane są wyjątki, jednak to ASPSP podejmuje decyzję o zastosowaniu procedury SCA.

		uzasadnieniu zdecydować się na zastosowanie SCA w tych przypadkach”		
63	Zakres informacji w zakresie Zgodności powinien zasadniczo obejmować wszystko co, co klient może przejrzeć na swoim rachunku bankowym online.	Dodać początkowe zdanie, że „ W zakresie Zgodności mieszczą się wszelkie dane, jakie mogą być przeglądane online przez klientów w banku. W minimalnym zakresie, będzie to obejmowało mechanizmy filtrowania danych....”	nie	Zakres danych oraz ich wymagalność może różnić się w różnych implementacjach. 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
64	Proszę zapewnią, aby saldo oraz dane transakcji za 3 miesiące były ujęte w zakresie Zgodności usługi PIS	Zgodnie z powyższym dane te są wymagane jako minimum, aby PISP mógł zainicjować transakcję	nie	Uwaga dotyczy usług AIS.
65	Nie ma odniesienia do HUBU PSD2	Proszę udokumentować, co oznacza HUB PSD2 – kto to jest i co robi?	tak	

66	Niejasne jest dla mnie umiejscowienie punktu 2 w diagramie, przedstawiającym schemat przebiegu procesu nawiązywania sesji XS2A (strona 10). Dlaczego punkt 2 - nawiązanie komunikacji pomiędzy TPP a ASPSP znajduje się po lewej i prawej stronie diagramu, a nie na dole, pomiędzy TPP a ASPSP? Co obejmuje ta komunikacja? Jeżeli mowa o komunikacji miedzy TPP a ASPSP, to punkt 2 powinien być na dole diagramu, czynności PSU zawierają się bowiem w punkcie 3. Jeżeli natomiast punkt 2 obejmuje także komunikację między PSU a ASPSP, to powinien być właściwie opisany, a nie jako komunikacja TPP-ASPSP.		tak	
67	Niejasna jest również dla mnie kwestia udostępniania przez ASPSP mechanizmów filtrowania danych w usłudze AIS, zgodnie z punktami 3.1 i 3.1.3. Komu są udostępniane te mechanizmy - PSU, czy TPP? Jeżeli PSU, to w jakim celu? Przecież przy usłudze AIS, PSU ma tylko zaznaczyć rachunki, których dotyczy AIS. Czy chodzi o to, że PSU ma dokładnie, poprzez wyfiltrowanie, wskazać szczegółowy zakres informacji, które ASPSP ma udostępnić TPP? Jeżeli TPP, to właściwie o co chodzi - czy TPP nie może samodzielnie filtrować paczki przekazanych mu danych przez ASPSP?		tak	

68	W lekturze dokumentu pomogłoby odniesienie do pojęć, którymi posługuje się dyrektywa oraz RTS	Proponuję powiązać pojęcia pojawiające się w dokumencie z pojęciami pojawiającymi się w: PSD2: • Kody dynamiczne (motyw 95) • Zainicjowana płatność (motyw 29) • Dowód uwierzytelnienia transakcji (artykuł 72) • Unikatowy identyfikator (art. 4 pkt 33) RTS SCA: • Authentication code (artykuł 4) • Sposób zaadresowania wymagań dynamicznego powiązania (artykuł 5) • Trusted beneficiaries • Identyfikator sesji (art. 29, pkt 2.(a),	tak	
69	Należy doprecyzować, że ASPSP ma obowiązek zaprezentowania PSU informacji przesłanych w scope oraz scope_details	Art. 97 dyrektywy PSD2, w szczególności: „dostawcy usług płatniczych stosowali silne uwierzytelnianie klienta obejmujące elementy, które dynamicznie łączą transakcję z określoną kwotą i określonym odbiorcą.” Oraz art. 64 pkt 3 „udzielenie zgody na wykonanie jednej transakcji płatniczej lub kilku transakcji płatniczych odbywa się w sposób uzgodniony pomiędzy płatnikiem a dostawcą usług płatniczych.	nie	

70	Oprócz scope należy przekazać też do TPP parametr scope_details, ponieważ to w scope_details można przekazać informację o numerze rachunku, który zgodził się obciążyć PSU	Propozycja zapisu: „Wraz z tokenem dostępowym przekazywany jest do TPP również parametr scope (taki sam, jak w żądaniu, lub ograniczony przez użytkownika w toku autoryzacji) oraz parametr scope_details uzupełniony informacjami, które podał użytkownik.	nie	Zaproponowano nowy proces.
71	W jaki sposób TPP ma przekazać formularz z pkt 2? Jako część żądania w ramach OAuth, czy w ramach wywołania usługi /payments/v1.0/* ?	Przekazywanie tych informacji powinno odbywać się w ramach żądania OAuth o pozyskanie tokenu. Obowiązkiem ASPSP jest wyświetlenie tych informacji w ramach wyrażania zgody przez PSU.	tak	
72	Zgoda na wykonanie usługi AIS powinna być wyświetlana przez APSPS a nie TPP	Patrz uwaga 69	nie	Zaproponowano nowy proces.
73	Jeżeli odwołanie zgody ma być dostępne przez interfejs TPP, to należy zdefiniować w PolishAPI metody na odwołanie zgody	Dodanie opisu unieważniającej token – revoke – zgonie ze standardem OAuth 2.0.	nie	Zaproponowano nowy proces.
74	Definicja „udzielanie zgody” jest niezgodna z art. 64 PSD2 oraz z założeniami technicznymi Polish API (rozdział 5.1, l.p. 3)	Patrz uwaga 69. Propozycja: „Udzielenie zgody – proces, w wyniku którego PSU udziela ASPSP zezwolenia na dostęp do jego rachunku, prowadzonego przez ASPSP w celu realizacji usługi, w tym usług AIS, PIS i COF.”	nie	Zaproponowano nowy proces.
75	Dla usług płatności brakuje możliwości podania callback’u z aktualizacją o stanie płatności – odpowiedź w ramach /payments/* może być submitted albo pending, w tej chwili o późniejsze statusu TPP musi dopytywać aktywnie. Zamiast tego proponujemy, by to ASPSP, o ile tego zażądał TPP, informował o zmianach statusu transakcji	Propozycja zapisu: „ASPSP powiadomi TPP, o ile ten tego zażądał, niezwłocznie po zmianie statusu transakcji za pomocą”	tak	

76	Należy dodać diagram stanów dla transakcji	Bez informacji o tym, jakie statusy może mieć transakcja oraz które stany są terminalne, TPP nie ma możliwości wywnioskowania, kiedy ma uznać transakcję za przyjętą do realizacji i może np. zacząć świadczyć usługę, czy wysłać towar.	tak	
77	„ASPSP zapewnia możliwość autoryzacji transakcji zleconej przez PSU za pomocą usług PIS, dostarczonej przez TPP," Usługa PIS nie jest dostarczana przez TPP	Propozycja zapisu: „ASPSP zapewnia możliwość autoryzacji transakcji zleconej przez PSU dostarczonej przez TPP za pomocą usług PIS"	tak	
78	Czy usługa PIS służy do autoryzacji transakcji, czy do jej realizacji? Pozyskanie zgody i authentication token odbywa się przecież przez flow Oauth	ASPSP używa protokołu OAuth 2.0 zgodnie rozdziałem 7 do autoryzacji transakcji zleconej przez PSU za pośrednictwem TPP z wykorzystaniem usług PIS, bez względu na metodę autoryzacji oraz jej złożoność. Wybór metody autoryzacji jest po stronie ASPSP.	nie	Usługa PIS służy do zainicjowania płatności.
79	Zastosowanie diagramów sekwencji oraz wskazanie konkretnych metod API, które zostaną użyte znacząco by ułatwiły TPP zrozumienie standardu, najlepiej z przykładami komunikatów które są wymieniane pomiędzy TPP a ASPSP		tak	
80	Brakuje rozdziału opisującego uwierzytelnienie ASPSP		nie	Wzajemna identyfikacja TPP i ASPSP następuje na podstawie certyfikatów eIDAS, zgodnie z draftem ETSI TS 119 495
81	Należy udokumentować schema'ę dla scope_details, np. w formacie json schema		tak	
82	Niezgodność przykładów z opisami typów w rozdziale 5.13 - brak typu dla duration - niespójność podawania duration (raz minuty, raz dni) -np. maxAllowedHistoryLong vs scopeTimeDuration - kwota podana niezgodnie z definicją typu (PIS, amount.value) - niektórze przykłady nie są prawidłowymi JSON-ami		tak	

83	Należy rozdzielić definicję scope_details dla żądania od TPP do ASPSP – które pola są przekazywane (np. informacje o kwotach w przypadku PIS), oraz na to, co TPP powinien oczekiwać w odpowiedzi (np. wybrany numer rachunku, itp.)		nie	Zaproponowano nowy proces. Dodano definicję scope_details
84	Brak obsługi wielokrotnego obciążenia PIS	Dodać podrozdział w rozdziale 1 wymieniający wszystkie ograniczenia PolishAPI w stosunku do PSD2 / RTS SCA. Rozdział 1.3 sugeruje, że PolishAPI opisuje wszystkie usługi wymagane przez PSD2. Art. 64 w pkt 2 mówi o wielokrotnych płatnościach	nie	Według naszej opinii to nie jest obszar zgodności.
85	Pobranie access tokena na podstawie refresh tokena może mieć miejsce w przypadku wielkrotnego PIS	Taka sytuacja będzie miała miejsce w przypadku usługi AIS wielokrotny, PIS wielokrotny oraz COF	nie	PIS wielokrotny jest poza zakresem usług zgodności.
86	Ponieważ komunikacja jest synchroniczna, to chyba w tym przypadku należy powiedzieć o sytuacji typu TIMEOUT. ASPSP nie ma możliwości ponowienia komunikatu – nie ma zdefiniowanego adresu na który taki komunikat miałoby wysłać	Zamiast „Brak możliwości nawiązania komunikacji z TPP” – „Wysłano żądanie do ASPSP natomiast ASPSP nie udzielił odpowiedzi” Zamiast „TPP ponawia komunikat x3” W 3.2.3.1 należy zdefiniować pole identyfikujące transakcję i nałożyć na ASPSP obowiązek, że wielokrotnie zlecone transakcje przez TPP o tym samym identyfikatorze zostaną zrealizowane raz	tak	

87	Brak zdefiniowanego ponawiania komunikatów i odpowiedzialności ASPSP i TPP oraz minimalnej wartości TIMEOUT, jaką powinien ustawić TPP ASPSP powinien weryfikować, czy nie otrzymuje transakcji o takim samym tppTransactionId dla danego TPP. W przypadku gdy tppTransactionId powtarza się, powinien wygenerować nową odpowiedź i zwrócić informację o transakcji, która została już zarejestrowana – pod warunkiem że token OAuth pozwala na dostęp do tej transakcji. W takim przypadku powinien być ustawiony dedykowany status http (np. 208 Already reported?). W przypadku, gdy tppTransactionId się powtarza, ale token OAuth nie pozwala na dostęp do oryginalnej transakcji, powinien zostać zwrócony dedykowany status http (może 409 Conflict?)		tak	
88	Brak zdefiniowanego interfejsu do przekazywania informacji o zmianach realizacji dyspozycji	Patrz uwaga 74. – należy uzupełnić	tak	
89	Załącznik „Model dziedziny KMD – ModelKMD.xlsx" nie został udostępniony do konsultacji		n/a	Treść załącznika została włączona do głównego dokumentu.
90	Obsługa zgód udzielanych przez więcej niż jednego użytkownika (np. konta firmowe) mogłaby być realizowana poprzez wydanie tokena OAuth, który nie upoważnia jeszcze do dokonania transakcji. Po stronie ASPSP lubPSU byłoby przekazanie informacji do innego użytkownika, który może potwierdzić transakcję i robiłby to w systemie ASPSP. Dopiero po tej operacji token wydany TPP upoważniałby do realizacji właściwej operację (PIS, AIS, COF). Należałoby wystawić dodatkowy endpoint na którym TPP może podać adres callback, który zostanie wywołany, gdy zmieni się stan tokenu (drugi użytkownik potwierdzi dostęp albo odrzuci)		nie	Do uwzględnienia w kolejnych wersjach standardu

91	Brakuje informacji o tym, w jaki sposób następuje uwierzytelnienie TPP w przypadku komunikacji inicjowanej przez ASPSP w stronę TPP. Czy ma następować w tej sytuacji weryfikacja certyfikatu TPP (np. czy należy do TPP) oraz czy ASPSP powinien przedstawić się certyfikatem klienckim X.509. A jeśli tak, (jako że w przypadku AIS przekazywane są w ten sposób informacje objęte tajemnicą bankową), to którego certyfikatu/klucza użyć, oraz jak TPP pozyska te informacje 6.1 Uwierzytelnienie TPP Dla usług w których podaje się adres callback oprócz adresu TPP podaje odcisk palca certyfikatu, którym powinien się legitymować podany adres podczas nawiązywania połączenia przez ASPSP. W PolishAPI należy dodać usługę, która potwierdza, czy certyfikat jest certyfikatem który wykorzystuje ASPSP w trakcie nawiązywania połączeń callback		tak	
92	Klasa UserInfo nie została zdefiniowana w plikach yaml	Chodziło o klasę RequestHeader?	tak	
93	ASPSP oprócz sprawdzenia certyfikatu powinien zweryfikować, że RequestHeader.tppID jest zgodny z tym, co zostało ustalone na podstawie certyfikatu	Jeżeli weryfikacje odnośnie nadużyć są realizowane w oparciu o dane w RequestHeader, a nie dane ustalone na podstawie certyfikatu – to należy zapewnić, że jest zgodność pomiędzy tym co zostało ustalone na podstawie certyfikatu z podanym tppID	tak	
94	Brakuje opisu znaczenia dla account/auxData		tak	

95	Zapisywanie adresów jako listy stringów daje sporą elastyczność TPP. Należałoby opisać w jaki sposób należy wypełniać to pole, tj. które informacje powinny się znaleźć w której linijce		nie	Standard nie powinien określać sposobu opisu przelewu stosowanego przez banki. ASPSP mają obowiązek zwrócić dane, które prezentują w serwisie WWW.Taki jest format systemu Elixir. W tym polu jest podawane to co klient wypełnił przy zlecaniu przelewu. ASPSP nie ma możliwości podania tych danych w jakiejkolwiek strukturze.
96	requestHeader/tppID – w jaki sposób TPP ma ustalić wartość tego pola?	Usunięcie pola, posługiwanie się wyłącznie informacją o TPP wynikającą z certyfikatu X.509. Jednocześnie ustalenie wymagań odnośnie certyfikatu, by zawierał informację o identyfikatorze TPP (np. EUNIP)	tak	
97	Zmiana opisu statusu „Not found authorization header”	Proponowany zapis: „Authorization header not found”	tak	
98	Klaryfikacja zapisu co robi metoda	Proponowany zapis opisu operacji: „ Get information about all user's payment accounts”	tak	
99	Zmiana opisu statusu: „Request limit for the requested service has exceeded”	Proponowany zapis: “Request limit for the requested service exceeded”	tak	

100	Pole transactionIdFrom zakłada, że identyfikatory transakcji są ściśle rosnąco monotoniczne. Brakuje tego założenia w części biznesowej, że ASPSP udostępnia identyfikator spełniający ten warunek		nie	Pole transactionIdFrom nie zakłada, że identyfikatory są monotoniczne - identyfiukatory nie są bowiem liczbami i nie mogę być tak traktowane. Pole umożliwia zawężenie zakresu transakcji wskazując punkt w rozumieniu chronologii jako alternatywa dla timestampów .
101	Niepotrzebny przedrostek add w nazwach operacji	Powinno być: • expressDomestic • standardDomestic • standardEEA • standardNonEEA • Tax Zgodnie z adresami operacji	tak	
102	Skąd TPP ma znać status rezydencji? Czyj jest to status rezydencji? Odbiorcy? Nadawcy (tą chyba zna ASPSP)? Jaki są dopuszczalne wartości?		nie	To jest zakres pól wypełnianych przez PSU.
103	PayerInfo zamiast PayorInfo		tak	
104	Brak możliwości podania daty obciążenia	W rozdziale 7.1.1, scope_details pozwalają na podanie daty transakcji, tak samo jak wspomina o tym Art. 80, pkt 3 PSD2. Należy tą informację też dodać do interfejsu	nie	W zakresie zgodności znajdują się porzelewy z datą bieżącą.

105	Możliwość zlecenia przez TPP wielokrotnie transakcji PIS pomimo udzielenia jednokrotnej zgody na obciążenie. W tej chwili ASPSP musi implementować weryfikację, czy transakcja została zrealizowana na podstawie wydanego AuthenticationToken (który zresztą, może zostać wymieniony na inny – za pomocą refreshToken'a).	Proponujemy dodanie do scope_details pola tppTransactionId. Dzięki temu, token OAuth będzie pozwalał na dokonanie transakcji tylko z określonym tppTransactionId. Po stronie ASPSP weryfikacja, czy nadane uprawnienia zostały już zrealizowane, będzie odbywała się na podstawie tppTransactionId. Takie podejście spowoduje, że tppTransactionId będzie użyte wielokrotnie w przypadku PIS wielokrotnego. W zależności od podejścia do obsługi timeout'ow (uwagi 19, 20) – może być konieczność zdefiniowania kolejnego pola (np. accessGrantId), które powinno być przesyłane przez TPP przy każdym zapytaniu)	nie	Według naszej opinii to nie jest obszar zgodności.
106	Nasza wątpliwość dotyczy wykonania płatności, czyli wykonanie PISP przez PTT. Czy w odpowiedzi do PTT na wykonanie PISP otrzymamy informację o poprawnej inicjalizacji przelewu czy również o jego faktycznym wykonaniu, czyli że środki wyszły z konta i trafiły do odbiorcy. Nie jest to w tej chwili jasno przedstawione w dokumentacji API. W 3.2.2 jest stwierdzenie, że PIS powiadomi PTT o przyjęciu bądź odrzuceniu zlecenia - co może oznaczać, że jest to osobna komunikacja niż tylko zlecenie przelewu. W 3.2.4 jest informacja, że diagram w 4.2 przedstawia komunikat PIS. Następnie w 4.2 jest opis komunikacji (diagram) z którego wynika, że jest to zapytanie o historię rachunku. Co jest już przypadkiem AISP a nie PISP. Z tego wynika, że PTT potrzebuje zarówno PISP jak i AISP aby to w pełni obsłużyć.	Wyraźne wskazanie które metody w API odpowiadają za przekazanie tych informacji i którym aktorom będą one przydzielone.	tak	

107	Dot. mechanizmów Uwierzytelnienia – jako procesu w wyniku którego ASPSP weryfikuje tożsamość PSU zgodnie z 1.4.5.1. (str. 11)	W pierwszej kolejności należy zwrócić uwagę na poniższe zapisy USTAWY PSD2: • art. 1 pkt. 36) lit. a) „Zgody na wykonanie transakcji płatniczej można również udzielić za pośrednictwem odbiorcy, dostawcy odbiorcy albo dostawcy świadczącego usługę inicjowania transakcji płatniczej.” przy czym zgodnie z art. 40 ust. 1 ustawy o usługach płatniczych „Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda może dotyczyć także kolejnych transakcji płatniczych.” - zatem Ustawodawca utożsamia pojęcie autoryzacji transakcji z wyrażeniem zgody na jej wykonanie, a wyrażenie zgody może nastąpić za pośrednictwem TPP (PISP). • art. 1 pkt. 41) lit. b) 1a. „Jeżeli transakcja płatnicza jest inicjowana za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej, na dostawcy tym spoczywa ciężar udowodnienia, że w zakresie jego właściwości transakcja płatnicza została autoryzowana i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą, za którą ten dostawca odpowiada.” • art. 1 pkt. 42) lit b) „1b. Jeżeli dostawca świadczący usługę inicjowania transakcji płatniczej odpowiada za dokonanie nieautoryzowanej transakcji płatniczej, na wniosek dostawcy prowadzącego rachunek,	nie	Uwaga niezrozumiała.

		niezwłocznie, nie później jednak niż do końca następnego dnia roboczego po stwierdzeniu danej transakcji lub doręczenia wniosku, rekompensuje mu poniesione straty lub zwraca kwoty zapłacone w wyniku dokonania przez niego zwrotu na rzecz płatnika, w tym kwotę nieautoryzowanej transakcji płatniczej. Przepis art. 45 ust. 1a stosuje się. • art. 1 pkt. 47) lit a) „2. W przypadku gdy transakcja płatnicza jest inicjowana przez dostawcę świadczącego usługę inicjowania transakcji płatniczej lub przez odbiorcę lub za jego pośrednictwem, płatnik nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji płatniczej zgody na zainicjowanie transakcji płatniczej albo po udzieleniu zgody odbiorcy na wykonanie transakcji płatniczej.”- zatem Ustawodawca nie przewiduje możliwości niewykonania transakcji w przypadku udzielenia zgody (autoryzacji w rozumieniu art. 40) na rzecz TPP (PISP). • art. 1 pkt. 52) „3. Dostawca świadczący usługę inicjowania transakcji płatniczej: 2) zapewnia, aby indywidualne dane uwierzytelniające użytkownika nie były dostępne dla innych podmiotów niż użytkownik i dostawca prowadzący rachunek oraz aby były one przekazywane za pośrednictwem bezpiecznych i wydajnych kanałów.” art. 1 pkt. 52) „4. Dostawca prowadzący rachunek: 2) niezwłocznie po otrzymaniu zlecenia płatniczego od dostawcy świadczącego usługę inicjowania transakcji		

		płatniczej przekazuje lub udostępnia temu dostawcy informacje o zainicjowaniu transakcji płatniczej oraz dostępne mu informacje dotyczące wykonania transakcji płatniczej; W związku z powyższym powstają wątpliwości czy pojęcia autoryzacja, uwierzytelnienie i udzielenie zgody to trzy osobne procesy w ramach specyfiki Polish API? Czy na autoryzację składają się łącznie udzielenie zgody i uwierzytelnienie? Jak pojęcia te mają się do ustawowych pojęć autoryzacji (art. 40 stawy o usługach płatniczych) i zasadach odpowiedzialności? Jaki jest moment złożenia oświadczenia woli w rozumieniu art. 60 KC o wyrażeniu zgody na wykonanie transakcji płatniczej w świetle zapisu 1.4.5.2. 1) i 5) oraz 3.2.5 specyfiki Polish API. Zgodnie z 1.4.5.2.5) specyfiki PSU autoryzuje transakcję w interfejsie ASPSP, co w świetle przywołanych przepisów wydaje się sprzeczne z art. 40 ustawy o usługach płatniczych w brzmieniu po nowelizacji zgodnie z projektem USTAWY PSD2 w związku z art. 1 pkt. 47) lit a) USTAWY PSD2. Autoryzacja jest pojęciem ustawowym z art. 40 (definicja ta ma m.in. znaczenie z powodu uzależnienia odpowiedzialność stron od dokonania autoryzacji transakcji – w szczególności art. 46 w kontekście nowelizacji USTAWA PSD2 i odpowiedzialności PISP) i 3stanowić ma ostateczne potwierdzenie obowiązku realizacji zainicjowanej transakcji płatniczej, a to ze względu na brak możliwości jej odwołania przez PSU po wyrażeniu zgody (autoryzacji) wobec dostawcy świadczącego		

		usługę inicjowania transakcji płatniczej (PISP). Co więcej, w ramach obowiązków ASPSP zobowiązane jest niezwłocznie po otrzymaniu autoryzacji w postaci zlecenia płatniczego od dostawcy świadczącego usługę inicjowania transakcji płatniczej do przekazania lub udostępnienia temu dostawcy informacji o zainicjowaniu transakcji płatniczej – co nie zostało uzależnione przez Ustawodawcę od dalszych warunków. Tym samym proces uwierzytelnienia w rozumieniu 1.4.5.1. specyfiki Polish API powinien odbywać się przed umożliwieniem PSU wyrażenia zgody wobec TPP (PISP) na inicjowanie transakcji płatniczej w ramach interfejsu TPP (PISP). Za takim stanowiskiem przemawia również zakres ustawowej odpowiedzialności TPP (PISP) w formie ciężaru dowodowego prawidłowej autoryzacji, a także obowiązkach naprawienia szkody lub zwrotu środków w przypadku odpowiedzialności za nieautoryzowaną transakcję. Przeciwne rozumowanie wyrażone w specyfice Polish API wydaje się stanowić zatem błąd logiczny (błędne koło) w którym najpierw wyrażana jest zgoda wobec TPP (PISP) w rozumieniu art. 40 ustawy, a dopiero potem dokonuje się uwierzytelnienie i dalsza autoryzacja w rozumieniu specyfiki Polish API tyle że wobec ASPSP, przy czym już na pierwszym etapie odwołanie tego zlecenia przez PSU jest niemożliwe, niezależnie od skuteczności autoryzacji wobec ASPSP zgodnie z 1.4.5.2.5). Co więcej, przyjęty w 1.4.5.2. specyfiki Polish API proces wydaje się		

		powodować, że zapis art. 1 pkt. 42) lit b) USTAWY PSD2 będzie zapisem martwym, bowiem wyłączona zostaje w pkt 1.4.5.2.5) odpowiedzialność TPP (PISP) skoro autoryzacja ma następować wobec ASPSP i w jego intefejsie. Tym samym proces w pkt 1.4.5.2.5) powinien zostać wykreślony w świetle wyrażonej zgody (autoryzacji) w pkt 1.4.5.2.1) i uwierzytelnienia 1.4.5.2.3). Dodatkowo należy rozważyć czy proces uwierzytelniania z punktu widzenia użyteczności usług PIS jak i AIS powinien zostać wyłącznie tożsamy z procesem logowania do interfejsu TPP (PISP, AISP), zgodnie z zapisem 1.4.4.2.1 b) specyfiki Polish API i nie powinien odbywać się w interfejsie ASPSP, skoro prawnie wiążąca zgoda (autoryzacja w rozumieniu art. 40) wyrażana będzie w interfejsie TPP. Ostatecznie sama Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, w preambule w akapicie 32 przewiduje, że „Usługi inicjowania płatności opierają się na bezpośrednim lub pośrednim dostępie dostawcy świadczącego usługę inicjowania płatności do rachunku płatnika. Dostawca usług płatniczych prowadzący rachunek, który zapewnia mechanizm pośredniego dostępu, powinien również umożliwiać bezpośredni dostęp dostawcom		

		świadczącym usługę inicjowania płatności.” Proponuje się usunięcie zmianę 3.2.5 poprzez zmianę słowa autoryzacja na słowo uwierzytelnianie. Proponuje się usunięcie 1.4.4.1 oraz 1.4.4.2.1 a), pozostawiając narzędzie uwierzytelniające w ramach interfejsu TPP (PISP), co wydaje się spójne z brzmieniem projektu USTAWY PSD2, przepisami Kodeksu Cywilnego (moment złożenia oświadczenia woli) oraz intencją Ustawodawcy w zakresie eliminacji „niepotrzebnych barier w rozwoju rynku fintech.”		

108	Dot. listy rachunków płatniczych	Proponuje się zapis: 1.4.5.2.4) w przypadku braku wskazania w formularzu inicjacji przelewu numeru rachunku nadawcy przelewu ASPSP prezentuje PSU do wyboru listę rachunków płatniczych, z których możliwe jest zainicjowanie transakcji płatniczej. PSU wybiera jeden rachunek z listy. Powyższy zapis pozostaje spójny z założeniami specyfiki Polish API 3.2.3. Komentarze dla pól Numer rachunku	nie	Zaproponoawano nowy proces.
109	Dot. zakresu informacji (Zgodność)	Czy zakres historii obejmuje blokady/zajęcia na rachunku płatniczym wynikające z prawa (blokady/zajęcia rachunku płatniczego przez ZUS, US, organy podatkowe, komornika, itp.), a nie z transakcji instrumentami płatniczymi? W przypadku gdyby powyższe informacje nie były objęte zakresem wskazanym w pkt 3.1.3. proponuje się dodanie przedmiotowych informacji do zakresu w pkt 3.1.3 zgodnie z argumentacją wskazaną w pkt. powyżej bowiem dotyczy ona szeroko rozumianej sytuacji finansowej PSU i jako taka winna w ocenie Ustawodawcy stanowić element usługi dostępu do informacji o rachunku (AIS) i powinna być dostępna do uzyskania za pośrednictwem TPP (AISP).	tak	W specyfikacji zostaną zaprezentowane wszystkie blokady, nie tylko te, wynikające z transakcji instrumentami płatniczymi

110	Dot. warunków płatności możliwej do zainicjowania przez TPP – przelew pojedynczy	Proponuje się wykreślenie tego warunku, w celu umożliwienia wprowadzanie paczek przelewów, które w dalszym ciągu będą autoryzowane przez PSU, ewentualnie Proponuje się zapis: 3.2.1.b) przelew pojedynczy chyba że co innego wynika z umowy ramowej; ewentualnie Proponuje się zapis: 3.2.1.b) przelew pojedynczy w przypadku przelewów zewnętrznych dla rachunków płatniczych jednego PSU - brak tego wymogu/ograniczenia dla rachunków płatniczych jednego PSU, co umożliwiłoby wprowadzenie paczek przelewów w ramach rachunków płatniczych będących w dyspozycji jednego PSU. Zgodnie z art. 40 ust. 1 ustawy o usługach płatniczych „Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda może dotyczyć także kolejnych transakcji płatniczych.” Uszczegółowienie tego przepisu zgodnie z USTAWĄ PSD2 pozwala na udzielenie zgody na rzecz TPP (PISP) i powinno obejmować kolejne transakcje płatnicze, co należy utożsamiać z poleceniami zapłaty, jak również innymi długotrwałymi stosunkami umownymi, w których na podstawie jednej zgody płatnika wykonywanych jest większa liczba transakcji płatniczych. Należy uznać, iż zgoda może dotyczyć zarówno określonej liczby transakcji,	nie	Według naszej opinii to nie jest obszar zgodności.

		ich (też łącznej) wysokości, jak i określonego czasu, w którym dane transakcje mogą być wykonywane w przyszłości. W konsekwencji cofnięcie zgody może dotyczyć pojedynczych z serii transakcji płatniczych objętych zgodą lub też wszystkich przyszłych (dot. uwagi w pkt 6) transakcji płatniczych objętych uprzednio wyrażoną zgodą. Zgoda taka może także podlegać modyfikacji w zakresie tylko pewnych elementów takich jak czas wykonania transakcji czy też ich maksymalna wysokość. Cofnięcie zgody dotyczy tylko transakcji niewykonanych i nie powoduje, że już wykonane transakcje stają się nieautoryzowane. W świetle powyższego należy pamiętać, że intencją Ustawodawcy jest eliminacja „niepotrzebnych barier w rozwoju rynku fintech”, a ograniczenie inicjowania płatności przez PSU za pośrednictwem TPP (PISP) do płatności pojedynczych i bieżących z pominięciem kolejnych transakcji płatniczych wydaje się niecelowe. Usunięcie tego zapisu będzie również zgodne z ogólnym celem Ustawodawcy jakim jest eliminacja „niepotrzebnych barier w rozwoju rynku fintech.”		

111	Dot. warunków płatności możliwej do zainicjowania przez TPP – przelew z datą bieżącą	Proponuje się wykreślenie tego warunku lub zapis 3.2.1.c) przelew opatrzony datą, w celu umożliwienia wprowadzanie przelewów z datą przyszłą, które w dalszym ciągu będą autoryzowane przez PSU, ewentualnie Proponuje się zapis: 3.2.1.c) przelew z datą bieżącą chyba że co innego wynika z umowy ramowej; ewentualnie Proponuje się zapis: 3.2.1.c) przelew z datą bieżącą w przypadku przelewów zewnętrznych dla rachunków płatniczych jednego PSU - Uzasadnienie jak w pkt. powyżej.	nie	Według naszej opinii to nie jest obszar zgodności.
112	Dot. możliwości ustawienia flagi blokady środków na rachunku w przypadku transakcji z datą przyszłą	W przypadku możliwości zlecania transakcji z datą przyszłą należ rozważyć wprowadzenia opcjonalnego pola „Flaga blokady środków”.	nie	Według naszej opinii to nie jest obszar zgodności.
113	Komentarz dla parametru response_type jest niezrozumiały: Wartone “code”	Zgodnie z RFC 6749 4.1.1. Jest: Wartone “code” Powinno być: Wartość “code”	tak	
114	Literówka w zdaniu „Parametr scopes definuje…”. Nie ma parametru scopes.	Jest: scopes Powinno być: scope	tak	

115	Dotyczy przykładowej struktury scope_details dla AIS wielokrotnego, który umożliwi dostęp przez 90 dni do historii transakcji oraz szczegółów transakcji na ostatnie 4 miesiące (liczone od momentu wydania zgody przesz klienta) Pytania: a) Czy 4 miesiące liczone od momentu wydania zgody oznaczają, że 90-tego dnia od uzyskania zgody TPP będzie mógł pobrać historię wskazanych rachunków za okres ostatnich ~7 miesięcy? Dodawane przez ASPSP wartości notBefore i notAfter opisane na str. 40 wskazują, że nie TPP nie będzie miał raczej dostępu do operacji, które pojawiły się w historii rachunku PSU już po wydaniu zgody na dostęp do historii operacji, ale prosimy jeszcze o potwierdzenie, że 4 miesiące zakresu historii rachunku obowiązują przez cały okres trwania zgody i nie rozszerzają dostępu TPP do historii bieżącej rachunku PSU. b) Czy pusta tablica creditCardAccount nie ma tu żadnego znaczenia i zgoda dotyczyć będzie tylko rachunku płatniczego PL45363346345234234243332, czy też wskazuje na konieczność prezentacji na formatce zgody w systemie ASPSP możliwości wyboru rachunków kart kredytowych, których ta zgoda będzie dotyczyć? Wątpliwości budzi tu zapis „jeśli TPP nie zna numeru konta może określić tylko typ konta”.		nie	Historia będzie udostepniania za okres, na jaki została zdefiniowana zgoda.
116	Brak na liście zakresów dostępowych ze stron 36-37 pozycji ais:transactionDoneDetails widocznej w przykładowej strukturze scopeDetails dla AIS wielokrotnego. Podobnie jest w kolejnym przykładzie dla AIS jednokrotnego oraz w przykładzie na str. 40.	Jest: ais:transactionDoneDetails Powinno być: ais:transationDetail	tak	

117	Brak na liście zakresów dostępowych ze stron 36-37 pozycji ais:transactionDone widocznej w przykładowej strukturze scopeDetails dla AIS wielokrotnego. Podobnie jest w kolejnym przykładzie dla AIS jednokrotnego oraz w przykładzie na str. 40.	Jest: ais:transactionDone Powinno być: ais:transactionsDone	nie	scope_details został opisany na nowo w oddzielnym pliku swaggera
118	Dotyczy przykładowej struktury scope_details dla AIS jednokrotnego. Pytanie: Czy uprawnienie ais:accounts dotyczy możliwości pobrania przez TPP listy wszystkich rachunków PSU niezależnie od tego, że parametr resource w tym żądaniu definiuje tylko jeden konkretny rachunkek płatniczy PL45363346345234234243 32?		nie	scope_details został opisany na nowo w oddzielnym pliku swaggera

119	Dotyczy przykładowej struktury scope_details dla PIS jednokrotnego – zgody na przelew krajowy. Pytania: a) Czy wysłanie przez TPP żądania określającego zgodę PSU na jednokrotną realizację przelewu na kwotę 454,34 PLN na zdefiniowany w elemencie scopeGroup rachunek odbiorcy bez równoczesnego podania rachunku lub listy rachunków PSU, z których taki przelew może być wykonany oznacza, że PSU musi jawnie w systemie ASPSP wskazać co najmniej jeden rachunek, którego ta zgoda będzie dotyczyła? Przykład ze str. 41 opisuje konto wybrane przez klienta (PSU), co wskazywałoby na taki wymóg, ale prosimy o dodatkowe potwierdzenie. b) Czy token zwrócony TPP przez ASPSP wygenerowany na podstawie dyspozycji takiej zgody PSU zawsze musi się odnosić do konkretnego rachunku/listy rachunków? c) Czy istnieje taki rodzaj zgody, który upoważnia TPP do złożenia płatności z wykorzystaniem usługi np. addStandardDomestic bez konieczności autoryzacji tej płatności przez PSU? Czy autoryzacja zgody na taką płatność jednocześnie autoryzuje samą płatność realizowaną przez TPP bez interakcji z PSU po wywołaniu jednej z usług PIS?		nie	scope_details został opisany na nowo w oddzielnym pliku swaggera
120	W przykładowej strukturze scope_details dla PIS jednokrotnego – zgoda na przelew krajowy wartością pola scopeGroupType jest pisInformationService. Jeśli ma to oznaczać usługę PIS, to wartością powinno być raczej paymentInitiationService. Podobny błąd na str. 41. W tej samej strukturze nie podano wartości pola paymentAccount, jak również niepoprawnie sformatowano wartość pola privilegeList w związku z czym JSON jest niepoprawny.	Jest: pisInformationService Powinno być: paymentInitiationService	nie	scope_details został opisany na nowo w oddzielnym pliku swaggera

121	Dla spójności w tabelach dotyczących parametrów żądań nazwy parametrów Code i Scope powinny być pisane małymi literami. Ponadto wymagalność parametrów scope i scope_details odnosi się do punktu 8.1.1, a powinno do 7.1.1.	Jest: Code, Scope, 8.1.1 Powinno być: code, scope, 7.1.1	nie	scope_details został opisany na nowo w oddzielnym pliku swaggera
122	Dlaczego parametry is_user_session, user_ip i user_agent zdefiniowane są tylko dla żądania odświeżenia ważności access tokena? Czy wszystkie żądania zrealizowane przez TPP z wykorzystaniem nowo otrzymanego tokena, dla którego podano is_user_session = true, przez cały czas ważności tego tokena mają być traktowane jako żądania związane z interakcją z PSU (w celu zapewnienia kontroli limitów dostępności funkcji API)?		nie	scope_details został opisany na nowo w oddzielnym pliku swaggera
123	Jak się ma informacja zawarta w tym punkcie do procedury pobierania nowego access tokena na podstawie refresh tokena opisanej w punkcie 7.1.5. Pobranie access tokena na podstawie refresh tokena? Naszym zdaniem w myśl RFC 6749 (6. Refreshing an Access Token) refresh token powinien być wykorzystywany przez TPP do odnowienia ważności access tokena tylko po jego wygaśnięciu, a nie przekazywany z każdym wywołaniem funkcji API wykorzystującej access token umożliwiający akcję dostęp wielokrotny.		nie	scope_details został opisany na nowo w oddzielnym pliku swaggera
124	Punkt 6 diagramu aktywności w usłudze PIS mówi o każdorazowym przekazywaniu TPP przez ASPSP informacji o zmianach stanu realizacji dyspozycji. W jaki sposób ASPSP ma informować o zmianach statusu dyspozycji płatności zleconej przez TPP, skoro nie zastosowano w tym procesie mechanizmu callback, jak również nie opisano żadnej usługi po stronie TPP umożliwiającej taką interakcję zwrotną?		tak	Dodano metodę callback do przekazania informacji na temat statusu płatności (PIS).
125	Nadmiarowe słowo działania w pierwszym wierszu.	Jest: działania Powinno być: <<do usunięcia>>	tak	

126	Na stronie https://polishapi.org nie został udostępniony załącznik nr 5 Model dziedziny KMD (ModelKMD.xlsx)		n/a	Treść załącznika została włączona do głównego dokumentu.
127	Nie udostępniono kompletnej specyfikacji obiektu typu scopeGroup (JSON Schema). Prosimy o informację, czy taka specyfikacja będzie dostępna po ukończeniu prac nad podstawową wersją standardu PolishAPI.		tak	scope_details został opisany na nowo w oddzielnym pliku swaggera
128	Niezbyt zrozumiała jest idea mechanizmu stronicowania z wykorzystaniem pól pageId i perPage parametru getAccountsRequest. W jaki sposób pageId opisane jako „numer rachunku rozpoczynającego stronę" miałoby być wykorzystane jako identyfikator kolejnej strony z wynikami. Pobierając pierwszą stronę zawierającą n rachunków nie wiemy, jaki jest numer rachunku rozpoczynającego stronę drugą i ile w ogóle stron określonej wielkości zawiera niepodlegająca żadnemu filtrowaniu lista rachunków klienta. Takich informacji nie zwraca obiekt response zdefiniowany dla tej metody. Dla metod AIS służących do pobrania listy blokad lub transakcji w obiekcie response występuje pole pageInfo, które takich informacji dostarcza.		tak	
129	Szczegóły transakcji pobierane są z wykorzystaniem m.in. pola transactionID. Zakładamy, że jest to unikalny identyfikator transakcji w systemie ASPSP. Pytania: a) W obiekcie zwrotnym mamy zdefiniowane pole zusInfo. Czy w świetle zmian, które weszły w życie 01.01.2018 w zakresie likwidacji typu przelewu ZUS, to pole ma nadal rację bytu? b) W obiekcie zwrotnym mamy zdefiniowane pola tppTransactionIdID oraz tppName. Sugerowana jest zmiana nazwy pola tppTransactionIdID na tppTransactionID. Czy pole to ma być wypełniane dla wszystkich transakcji zleconych za pośrednictwem TPP, gdzie w wywołaniach metod PIS TPP		nie	W historii rachunku mogą być obecne transakcje przelewów do ZUS wg starych zasad. Pola związane z informacja na temat TPP mają być zwracane dla wszystkich transakcji zlecanych za pośrednictwem TPP, o ile ASPSP takimi danymi dysponuje.

	przekazuje do ASPSPS taką wartość. Co w takiej sytuacji z polem tppName? Co ASPSPS powinno zwrócić w tym polu?			
130	Wszystkie metody usługi PIS zwracają wymagane pole detailedStatus. Jaką wartość powinno mieć to pole? Czy jest to po prostu opis znaczenie statusu przekazanego w polu generalStatus spośród dostępnych wartości ze słownika?		nie	Tak
131	Odwołanie zgody przez PSU. W dokumencie jest zapis, że sposób realizacji tej funkcjonalności jest poza zakresem standardu Polish API. Zgodnie z nowym zakresem za proces zgód odpowiedzialny jest TPP - Czy to oznacza, że TPP musi z ASPSP uzgodnić/potwierdzić jak taki proces ma wyglądać? Wg naszej oceny w/w proces powinien być ustandaryzowany.		nie	W specyfikacji opisano nowe procesy związane z udzieleniem, edycją i cofnięciem zgody na AIS.

132	Podstawowe formaty danych: Kwoty	Jest: Zapisane jako liczby z 0 lub 2 miejsca po przecinku (znak kropki) […]. Powinno być: Zapisane jako liczby z 0 lub ze znakiem oddzielającym część całkowitą od części ułamkowej 2 miejsca (znak kropki) […]	tak	
133	W/w punkcie jest zapis: W ramach usługi PIS w zakresie Zgodności ASPSP będzie umożliwiało PSU, za pośrednictwem TPP (PISP) inicjację płatności spełniających łącznie poniższe warunki: […] c) Jest to przelew z datą bieżącą, […] Jeśli składane przez PSU zlecenie przelewu będzie po tzw. COT (Cut Off Time) dla danego typu przelewu, to w systemie transakcyjnym takie zlecenie nie będzie zrealizowane w dacie bieżącej – system powinien zrealizować taki przelew w najbliższym dniu roboczym. Dla w/w przypadku takie zlecenie będzie oczekiwało na realizację.		nie	Dodano pole (opcjonalne) umożliwiające przekazanie informacji o chęci założenia blokady w związku z inocjacją przelewu np. w dniu wolnym.
134	Koniecznym jest opublikowanie szczegółowego procesu udzielenia zgody PSU dla TPP na wykonanie usługi COF.		nie	Proces ten zostanie uwzględniony w kolejnej wersji standardu.

135	w modelu danych brakuje informacji dot. opcji kosztowej przy zlecaniu przelewu zagranicznego (usługa addStandardNonEEA, pole transferCharges)	W polu do opłat przy zlecaniu przelewu zagranicznego (usługa addStandardNonEEA, pole transferCharges), powinna się znaleźć jedna z następujących wartości: • podział kosztów, • obciążenie beneficjenta, • obciążenie nadawcy Uzasadnienie: Klient powinien wybrać tę opcję przy zlecaniu przelewu zagranicznego, aby bank wiedział z jaką instrukcją kosztów należy zrealizować przelew. Opcja kosztowa przy przelewach zagranicznych ma duży wpływ na łączne koszty przelewu i w przypadku państw i walut nie należących do EEA, nie jest ona odgórnie uregulowana.	tak	
136	W pierwszej kolejności mam czysto techniczną uwagę i proszę o dokonanie korekty w liście podmiotów uczestniczących w grupie roboczej na Spółdzielczą Kasę Oszczędnościowo – Kredytową im. F. Stefczyka oraz Krajową Kasę Oszczędnościowo – Kredytową – jesteśmy dwom całkowicie osobnymi bytami prawnymi i organizacyjnymi, wobec czego będę wdzięczna za uwzględnienie tej drobnej zmiany.		tak	
137	Chciałam również zwrócić uwagę na pewien fakt, iż specyfika wszystkich SKOKów w zakresie uczestnictwa w systemie Elixir jest znaczenie odmienna od sytuacji banków, gdyż SKOKi nie są bezpośrednimi uczestnikami systemu rozliczeniowego Elixir, a odbywa się on za pośrednictwem Kasy Krajowej, która w tym zakresie ma bezpośrednio zawartą umowę z KIRem. Stąd zastanawiam się, czy ta zgoła odmienna sytuacja nie będzie miała jakiś konsekwencji dla platformy Polish API zwłaszcza w kontekście usługi PIS?		nie	Nie dotyczy specyfikacji Polish API.

138	prośba o uwzględnienie w specyfikacji zmiany w punkcie 3.2.1. polegającej na doprecyzowaniu i zapisaniu wprost w specyfikacji, że ASPSP w ramach usługi PIS udostępniają tylko takie rodzaje przelewów, jakie oferowane są PSU, ta sama sytuacja dotyczy rachunków płatniczych udostępnianych przez ASPSP TPP w ramach usługi AIS.		tak	
139	Niezaprzeczalność każdego zapytania może wprowadzać poważne problemy ze skalowalnością. Aby zapewnić niezaprzeczalność, konieczne jest nie tylko rejestrowanie niedającego się podrobić podpisu zapytania, ale również sprawienie, że zapytanie jest możliwe do zidentyfikowania w unikalny sposób. Unikalność identyfikacji zapytań musi być wymuszona, a jedynym sposobem zapewnienia tego jest śledzenie wykorzystanych identyfikatorów przy świadomości bariery wszystkich wykorzystanych identyfikatorów.	Rozważyć, czy niezaprzeczalność zapytań jest rzeczywiście wymagana (oraz czy może być zastąpiona logowaniem kontrolnym, bez udowadniania wydania). Jeśli nie, wprowadzić specyfikację generowania unikalnych identyfikatorów, które można sprawdzać pod kątem unikalności bez kontroli w bazie danych na wysokim poziomie izolacji transakcji (wymagana byłaby SERIALIZACJA ISO). Potencjalne rozwiązanie może opierać się na monotoniczności (zamawianie identyfikatorów) oraz weryfikacji, czy użyte identyfikatory są „większe niż widziano ostatnio”. Koordynacja kontroli unikalności w przypadkach API oraz/lub przypadkach na bramkach API (potencjalnie w setkach....) pozostaje nadal kwestią i może stanowić ograniczenie skalowalności.	nie	Zagadnienie implementacyjne, w naszej opinii nie do rozstrzygnięcia na poziomie standardu.

140	Wybrany sposób wymuszania niezaprzeczalności uniemożliwia RESTful Maturity Level 1 (lub wyższy) API	Rezygnacja z adresowalności zasobów, jak również wartości semantycznej metody HTTP może mieć negatywny wpływ na zdolność do generowania standardowych klientów API, scaffolding, testowanie, a w konsekwencji na przyjecie. Standardy de-facto, w tym HATEOAS oparty na dicoverability oraz self-descriptivity są trudne we wdrożeniu (nie w standardowy sposób). Jest prawdopodobne, że PolishAPI będzie jedynym non-RESTful API (w znaczeniu modelu dojrzałości Richardsona) w UE, i może to negatywnie wpływać ja jego przyjmowanie, a z pewnością nie będzie wysoko oceniane w środowisku programistycznym.	nie	Zagadnienie implementacyjne, w naszej opinii nie do rozstrzygnięcia na poziomie standardu.

141	The standard, pomimo rezygnacji z pomysłów Maturity level 1+ RESTful API nie korzysta z tego jako możliwości do stworzenia API niezależnego od transportu (transport agnostic).	Odkładając na bok decyzję w sprawie rezygnacji z RESTfulness w odniesieniu do API, jeśli standard będzie zależeć od treści zapytania oraz treści odpowiedzi, nie ma bariery co do dodawania WSZYSTKICH koniecznych elementów do komunikatu przekazywanego w treści, w tym semantyki operacji, podpisów oraz wszelkiego rodzaju metainformacji. Standard powinien umożliwiać tworzenie komunikatów zamkniętych w sobie (self-contained). Pozwoli to na wyabstrahowanie mechanizmu transportowego, a API niezależne od transportu jest znaczącą wartością. W szczególności przyjecie API np. dla transportu opartego o email byłoby relatywnie prostym zadaniem. Znacząco łatwiejsze byłoby zarządzanie komunikatami protokołu, np. brokerach komunikatów, ponieważ pełny kontekst to sam komunikat. IFX (ifxforum.org) może być podany jako przykład standardu podobnego co do celu, wdrażającego ideę protokołu niezależnego od transportu.	nie	Ustalenie grupy projektowej Polish API. Przyjęto założenie o przekazywaniu większego zakresu danych w body ze względów bezpieczeństwa.

142	Niepotrzebne asymetrie w operacjach sprawiają, że interfejs jest zaśmiecony (np. AccountsRequest i AccountInfoRequest, getPayment i getMultiplePayments)	Usunąć duplikaty, redundantne warianty. Zmienność zakresu informacji powinna być rozwiązana pojedynczą schema'ą z informacjami opcjonalnymi potencjalnie pominiętymi. Wybór zasobów do ujęcia w odpowiedzi powinien być dokonany na podstawie kryteriów zapytania, a nie schema'y specjalnego przypadku dla zapytania „pojedynczego podmiotu". Np. kryteria mogą obejmować konkretny identyfikator zasobu, oddając w ten sposób pojedynczy podmiot w odpowiedzi. Nie powinno być różnicy pomiędzy odpowiedzią zawierająca pojedynczy podmiot, ponieważ został on nazwany przez identyfikator, a odpowiedzią zawierającą pojedynczy podmiot, ponieważ jest to jedyny podmiot spełniający podane kryteria - efektywnym kryterium powinien być złożony identyfikator. Również Pozwala to na to, aby wspólny kod dotyczył wszystkich przypadków, redukując liczbę wariantów, a w konsekwencji klas równoważności do testowania itp.	nie	Ustalenie grupy projektowej Polish API.

143	Selektywny (w konsekwencji potencjalnie wprowadzający w błąd) opis parametrów rachunku	Brak uzasadnienia co do arbitralnego wyboru niektórych parametrów rachunku / produktu (np. InterestRate) jako obowiązkowych, przy pominięciu innych. Na przykładzie oprocentowania, informacje przedstawione nie są wystarczające do opisania danej cechy rachunku. Na przykład schemat stawek oprocentowania z przedziałami nie może być opisany pojedynczą wartością. W konsekwencji, należy albo wprowadzić bardziej kompletny opis, albo sprawić, że dany element jest opcjonalny i wprowadzić sposób wskazania, że opis nie jest kompletny (oraz potencjalnie niesformalizowaną metodę podawania brakujących informacji). Patrz specyfikacja brytyjskiego Open Data API, gdzie podano przykład specyfikacji podobnych parametrów rachunku w sposób zaprojektowany do automatycznego porównywania (choć nadal niekompletny, idzie znacznie dalej i będzie obejmować znaczącą większość potrzeb): https://www.openbanking.org.uk/open-data-apis/ https://openbanking.atlassian.net/wiki/spaces/DZ/pages/13369388/PCA+API+Specification+-+v2.1.1	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.

144	Słownik typów przelewów jest ograniczony i nie jest otwarty na rozszerzenia. Schema obsługująca przelewy jest inna w zależności od przelewu i nie jest generyczna.	Proponowany API uznaje zamkniętą listę rodzajów przelewów: krajowy, SEPA, zagraniczny, nieSEPA. Nie można wykorzystać takiego podejścia do modelu w przypadku krajowych przelewów w innym kraju (np. przelewy UK BACS lub Faster Payment w Wielkiej Brytanii adresowane do / z kodu sortowania oraz numer rachunku). Rodzaj przelewu powinien być wartością słownika, determinującą interpretację innych pól (ewentualnie pomocniczy lub w inny sposób otwarty na rozszerzenia). Jeśli zostanie zwiększone za pomocą generycznej (otwartej) specyfikacji rachunku źródłowego (docelowego (schemat identyfikacji generycznej zdolny do zakodowania arbitralnych rodzajów identyfikatorów), większość przypadków może zostać ujednolicona w ramach jednego schema, przy identyfikatorach zdolnych do wyabstrahowania różnic (np. użycie BIC jako elementu identyfikatora rachunku docelowego, użycie kodu kraju jako części IBAN, w przeciwieństwie do BBAN, rozróżniania na przelewy krajowe/zagraniczne itp.)	nie	Ustalenie grupy projektowej Polish API. W tej wersji API opisuje funkcjonalności obsługiwane przez polskie, albo działające na polskim rynku banki.

145	Identyfikacja rachunków jest prowadzona wyłącznie za pomocą IBAN Choć numery IBAN są popularne w Polsce i ustandaryzowane w SEPA, nie są jedynym sposobem. Założenie stosowania IBAN do określania rachunków źródłowych jest potencjalnie szczególnie problematyczne dla niektórych banków, które stosują wewnętrzną identyfikację rachunków podczas ich zwracania (podczas gdy Polish API wymusza, aby stosowały IBAN-y). W wielu krajach IBAN-y są prawie nieznane z punktu widzenia klienta końcowego (PSU), i nie są stosowane przez klientów końcowych, co mogłoby skutkować potrzebą, aby TPP stosował jakąś formę (nieustandaryzowaną w PolishAPI, a zatem niedostępną z samego banku) konwertowania z IBAN na identyfikatory znane klientowi. Adresowanie z / na rachunki instrumentów płatniczych (np. kart kredytowych identyfikowanych przez PAN lub numery kart plastikowych, e-portfeli, posiadających własne schematy identyfikacji, lub kryptoportfeli) jest logicznym przyszłym przypadkiem użycia – i powinno być obsługiwane. Wskazanie rachunku docelowego powinno dopuszczać istnienie innego sposobu przekazywania rzeczywistego identyfikatora rachunku, np. numeru telefonu lub adresu email odbiorcy lub numer pojedynczego czeku BLIK – co zostanie przekształcone na późniejszym etapie. Przyszłe scenariusze, np. przelewy na rachunki w mediach społecznościowych, adresy pocztowe, pokoje hotelowe itp. powinny być obsługiwane w sposób ujednolicony	Identyfikacja rachunków powinna być abstrakcyjna i samoopisująca się (self-descriptive). Każdy dający zidentyfikować się podmiot, w tym rachunki, lecz również transakcje, blokady itp.. powinny uwzględniać wiele alternatywnych sposobów identyfikacji (np. przez podmiot zewnętrzny, przez bank, przez bank w innych systemach itp.). Takie identyfikatory mogą współistnieć. UK Read/Write APIs, oraz STET, bardziej lub mniej luźnie oparte na ISO 20022, uznają „inne” sposoby identyfikacji rachunków, z metapolem będącym nazwą / identyfikatorem schematu identyfikacji w celu interpretacji identyfikatora podanego wewnątrz). Aby uprościć typowe przypadki użycia, należy zdefiniować wartości domyślne metapól, aby można je było pomijać (tak więc korzystanie tylko z wartości pola identyfikacji rachunku byłoby interpretowane jako najbardziej typowy rodzaj identyfikatora – potencjalnie jako IBAN). Intive, projektując dla potrzeb identyfikacji (wszelkich dających się zidentyfikować podmiotów) korzystał z koncepcji identyfikacji rekursywnej z 3 metapolami, które same są identyfikatorami oraz rodzajem obiektu identyfikowanego w sposób domyślny (pseudokod poniżej): class Identifier { identificationAuthority : Identifier // który wydaje identyfikatory identificationScheme : Identifier // co to jest za schemat – czy ewentualnie mógłby zostać	nie	Ustalenie grupy projektowej Polish API. Do rozważenia podczas prac nad kolejnymi wersjami.

		spłaszczony z identificationAuthority używając oddzielnych nazw schematów dla różnych uprawnień format : Identyfikator // oznaczenie opcji struktury kodowania identyfikatora, jeśli istnieją liczne sposoby, np. kod sortowania oraz numer rachunku mogą być dwoma oddzielnymi podpolami identyfikatora, lub pojedynczy string rozdzielony pewnymi znakami, np. myślnikiem lub spacją, kod sortowania może być zapisywany z myślnikami lub bez nich itp. id : string[1..N] } Zapraszamy do skorzystania z pomysłu.		

146	getAccount / getAccounts return accountNumber jako nieokreślony identyfikator, podczas gdy inne API wymagają IBAN-ów jako identyfikacji rachunków źródłowych (patrz addStandardDomestic, addExpressDomestic, addStandardEEA, ...)	Opisać powiązanie pomiędzy identyfikatorami zwracanymi a tymi stosowanymi podczas inicjowania płatności. Najlepiej wprowadzić mechanizm metadanych, aby zapisać typ zwróconego identyfikatora i zezwolić na stosowanie arbitralnego typu jako wykorzystywany schemat identyfikacji. Pozwolić na zwracanie alternatywnych identyfikatorów, w szczególności: wewnętrzny bankowy identyfikator rachunku, być może GUID, dla niektórych rachunków. Uwzględnić definicję nowych typów (np. customer ID oraz aliasy rachunku?). Dodać wsparcie innych identyfikatorów, które mogą być logicznie używane w scenariuszu, np. numerów PAN – ponownie, najlepiej poprzez wprowadzenie metainformacji, kodując schemat identyfikacji w celu umożliwienia interpretacji identyfikatora podanego wewnątrz.	tak	
147	Wprowadzenie corner cases (np. przekazy do urzędów skarbowych), konkretnych dla danego kraju (PL) i stosowanie ich w głównej części standardu	Corner cases powinny być obsługiwane przez mechanizm rozszerzenia (np. mapa pól pomocniczych). Dla wyjątkowo ważnych (np. przelewy podatkowe) uzupełniająca specyfikacja zamrażająca semantykę oraz kodującą wartości specjalnego znaczenia - słowniki (np. długości terminu itp.) powinny być wydawane poza głównym standardem, np. w suplemencie specyficznym dla PL. Naruszenie symetrii sposobu, w jaki traktowane są specjalne przypadki lokalne, nie jest pożądane i może uniemożliwiać przyjecie poza PL.	nie	Ustalenie grupy projektowej Polish API. W tej wersji API opisuje funkcjonalności obsługiwane przez polskie, albo działające na polskim rynku banki.

148	Użycie niestrukturyzowanego adresu jako jedynego sposobu oznaczania adresu klienta.	Adresy w systemach bankowych bardzo często są opisywane semantycznie przez indywidualne komponenty. Ujednolicenie wszystkich potencjalnych kombinacji pól używanych w różnych miejscach pozostaje problemem, więc abstrakcyjny sposób opisywania adresu jako kilki wolnych wierszy formularza pozostaje ważne, lecz przydatne byłoby również utrzymanie możliwości opisywania go również w ustrukturyzowanej formie, z podaniem miejscowości, kodu pocztowego, numeru mieszkania itp. jako oddzielnych, semantycznie oznaczonym pól.	nie	Ustalenie grupy projektowej Polish API.
149	Długość identyfikatorów transakcji, szczególnie przypisanych zewnętrznie może być ograniczająca.	TppTransactionId i podobne identyfikatory mają 32 znaki, co może być ograniczeniem. Choć powinien istnieć limit (aby zapobiegać przeciążeniu buforów itp.) długość powinna być znacznie większa, prawdopodobnie bliżej 500 znaków, a nie 30. Trudno jest robić założenia o zewnętrznych schematach identyfikacji, lecz transaction id mają tendencję do kodowania wielu informacji, plus przypadkowość pożądanej entropii – mogą być naprawdę długie. 32 znaki to naprawdę niewiele.	tak	

150	Zamknięta liczba ról w transakcjach	API opisuje nadawcę i odbiorcę w oddzielnych zestawach pól ściśle powiązanych z rachunkiem. Pożądana byłaby możliwość opisywania dowolnej liczby stron i ich ról (poprzez identyfikator roli, przy pewnych predefiniowanych wartościach, np. „nadawca” i „odbiorca”). Na przykład akceptant jest stroną związaną z transakcją (rola „akceptanta"), podobnie jak przetwarzający, agent rozliczeniowy, a potencjalnie nawet urzędnik bankowy obsługujący pieniądze lub czek. API powinno zezwalać, nawet jeśli nie standaryzować, na tworzenie otwartej listy relacji. Ustandaryzować tylko niektóre – poprzez zdefiniowanie role id oraz jego znaczenia w standardzie.	nie	Ustalenie grupy projektowej Polish API.
151	Brak informacji o relacji osób do rachunku	Możliwość pobrania listy właścicieli, współwłaścicieli, pełnomocników, odbiorców / niepełnoletnich, przedstawicieli ... jak również zaufanych odbiorców, wydaje się pożądana w niektórych scenariuszach.	nie	Ustalenie grupy projektowej Polish API. Do rozważenia podczas prac nad kolejnymi wersjami.
152	Wymóg zdolności definiowania zaufanych odbiorców (zgodnie z wymogami PSD2 i RTS) nie jest uwzględniony w API	Wprowadzić w API obsługę i pobieranie listy zaufanych odbiorców. Można połączyć z API pobieranie relacji między rachunkiem a osobami, przy czyn zaufany odbiorca będzie specjalnym podtypem typu relacji.	nie	Według naszej opinii to nie jest obszar zgodności.

153	Ograniczony i zamknięty sposób kategoryzacji dla rachunków, transakcji i innych podmiotów	Uwzględnić otwartą liczbę kategorii, opisaną przez identyfikator kategorii oraz identyfikator wartości kategorii, w szeregu. Ujednolicić koncepcje takie jak rodzaje rachunku – np. rachunek depozytowy, karty kredytowej itp, aby były tylko jedną z kategorii. Typ produktu potencjalnie może być ujednolicony w ten sam sposób („rachunek super saver" w kategorii „ProductType"). Ewentualnie umożliwić klientom zdefiniowane kategorie, które będą podsuwane w ten sposób– np. znaczniki przypisane przez klienta do rachunku lub transakcji.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
154	Dodanie spersonalizowanego pola do specyfikacji Oauth2 jako obowiązkowego może wpływać na niektóre biblioteki klientów	Proszę upewnić się, że istnieje sposób tworzenia żadnego podstawowego zapytania o uwierzytelnienie z użyciem tylko podstawowych pól opisywanych przez standard. W przeciwnym razie trudno będzie korzystać z niektórych bibliotek klientów Ewentualnie zdefiniować standardową wartość spersonalizowanych pól: no. scope_details powinno mieć domyślna wartość oznaczającą brak dodatkowych ograniczeń zakresu.	nie	Ustalenie grupy projektowej Polish API.
155	Spersonalizowany sposób kodowania dodatkowego zawężenia zakresu (pole scope_details) może być ewentualnie zastąpione innym mechanizmem standardu	Wartość parametru scope może sama w sobie kodować ograniczenia	nie	Ustalenie grupy projektowej Polish API.
156	Rozważyć zastosowanie OpenID Connect w celu wdrożenia ważności access tokena, jak również sprawdzenia, czy tokeny i kody są oryginalne, zwłaszcza przy użyciu at_hash oraz c_hash	Dodatkowy środek zabezpieczenia	nie	Ustalenie grupy projektowej Polish API. Do rozważenia podczas prac nad kolejnymi wersjami.
157	Rozważyć użycie Proof Key of Token Exchange jako części standardu	Dodatkowy środek zabezpieczenia	nie	Ustalenie grupy projektowej Polish API.

158	Rozważyć użycie OpenID Connect jako standardowego sposobu zwracania informacji o kliencie	Przyszłe wdrożenie wzajemnej zaufanej wymiany, np. KYC, otwarcie rachunku itp.	nie	Ustalenie grupy projektowej Polish API. Do rozważenia podczas prac nad kolejnymi wersjami.
159	Częściowa zgoda klienta nie jest właściwie sygnalizowana	Standard oraz charakter bankowości otwartej oznaczają, że klient może otrzymać więcej niż tylko binarną zdolność decydowania, np. może wybrać rachunki, do których udzielić dostępu, podczas gdy zapytanie może stosować tylko terminy ogólne, np. „dostęp do rachunków karty kredytowej". Dla wielu scenariuszy, np. przy agregacji rachunków, fakt częściowej zgody nie jest ważny dla TPP, lecz w innych scenariuszach – np. ocena kredytowa, częściowa zgoda może być problemem. TPP powinien uzyskać wskazanie, że jego zapytanie jest objęte jedynie częściową zgodą, aby mógł odpowiednio działać (np. poinformować klienta, że mogą przetwarzać dalej jedynie posiadając całość wymaganych informacji) Skontaktować się z Intive, aby omówić opcje zwracania informacji zwrotnych dotyczących decyzji klienta do pytającego w ramach standardu Oauth2 oraz bez ujawniania informacji, do których TPP nie ma uprawnień (zastrzeżona wiedza jest częścią IP Intive).	nie	Ustalenie grupy projektowej Polish API. Do rozważenia podczas prac nad kolejnymi wersjami.
160	uwaga ogólna do specyfikacji: prosimy uzupełnić dokument o szczegółowe diagramy sekwencji oraz diagramy aktywności dla poszczególnych procesów	Wysokopoziomowe diagramy dają tylko ogólny pogląd na proces, nie pozwalają dokładnie przeanalizować całej komunikacji pomiędzy aktorami	tak	

161	prosimy o wyjaśnienie / doprecyzowanie czy zaprezentowany schemat dotyczy nawiązywania pierwszej sesji XS2A czy każdej, odrębnej sesji. W legendzie schematu, w pkt. 3 opisana jest czynność „uwierzytelnienia PSU w mechanizmie wskazanym przez TPP spośród udostępnionych przez ASPSP" co w przypadku AIS wielokrotnego nie będzie wymagane każdorazowo.		tak	
162	zdanie: „Realizacja każdej transakcji, w ramach usługi AIS, PIS oraz COF, powinna odbywać się w ramach dedykowanej, odrębnej sesji XS2A" jest niezrozumiałe w kontekście usługi AIS. Prosimy o wyjaśnienie / doprecyzowanie.		tak	
163	prosimy o uspójnienie opisu dla kroku 3) uwierzytelnienie PSU z zapisami dot. schematu nawiązywania sesji XS2A, zgodnie z intencją grupy roboczej		nie	Zapisy rozdziału zostały zmienione w całości.
164	proponujemy zmianę dla metody re-direction, do której na ten moment referuje Polish API, polegającą na zamianie kolejności pkt 4) i 5), co skutkuje wyborem rachunków na stronie ASPSP, a nie TPP. Dla innych metod będzie wymagane wypracowanie nowego procesu udzielania zgody.		nie	Zapisy rozdziału zostały zmienione w całości.
165	jeżeli ww. uwaga nie zostanie uwzględniona i nadal pozostanie wskazana w procesie kolejność pkt. 4) i 5) - prosimy o doprecyzowanie jaki minimalny zakres informacji będzie możliwy / konieczny do przekazania w ramach „listy rachunków"? Czy będą to wyłącznie numery rachunków czy również informacje pozwalające zidentyfikować je klientowi, np. nazwa rachunku, rodzaj (karta kredytowa, ROR, rachunek oszczędnościowy) czy segment (rachunki konsumentów, rachunki SME)? Czy przekazana lista rachunków ma być w jakiś sposób posortowana / pogrupowana?		nie	Zapisy rozdziału zostały zmienione w całości.

166	proces udzielenia zgody PSU na wykonywanie usługi AIS kończy się na kroku 6) „PSU wskazuje rachunki". • Czy ASPSP dostaje zwrotnie informację jakie rachunki wybrał Klient w ramach zgody? • Kiedy w tym procesie następuje przekazanie Access Token dla TPP (opcj. również Refresh Token)? – po uwierzytelnieniu PSU czy po wyborze konkretnych rachunków? Prosimy o uzupełnienie procesu o te kroki.		nie	Zapisy rozdziału zostały zmienione w całości.
167	prosimy o zmianę opisu definicji rachunku płatniczego, dla którego może być realizowana usługa AIS. Zgodnie z Dyrektywą i RTS warunki są dwa: to musi być rachunek płatniczy (w rozumieniu dyrektywy) oraz musi być dostępny dla PSU on-line. Niezrozumiałe są wskazane dodatkowe warunki konieczne, tj. możliwość zarówno jego obciążania jak i uznawania.		tak	
168	prosimy o uzupełnienie zdania pierwszego o frazę „oraz informacji o rachunku płatniczym"		tak	
169	prosimy o wyjaśnienie dlaczego zakres informacji obejmuje tylko blokady wynikające z transakcji instrumentami płatniczymi? Czy będą mogły być przekazane inne blokady prezentowane na historii w kanale on-line?		tak	

170	prosimy o przeredagowanie tabeli z polami, tak aby pola były posegregowane wg ich rodzaju, np. dodanie w tabeli 3 sekcji: 1. informacje o PSU 2. informacje o rachunku płatniczym 3. informacje o historii transakcji i przyporządkowanie tam poszczególnych pól; dodatkowo prosimy o włączenie do tabeli dodatkowych pól auxData, o których mowa na str.19 • Prosimy również o wprowadzenie jednorodnych komentarzy, najlepiej oddających ogólny opis co pole zawiera, kogo / jakiego zlecenia dotyczy. Prosimy o zwrócenie uwagi, że nie wszystkie pola dotyczą „każdej transakcji w historii rachunku", np. pole Kurs. • Prosimy o uzupełnienie w tabeli pól o wszystkie pola, które zostały dodane do Swaggera, np. Data transakcji, waluta, itp. – specyfikacja powinna być zgodna z załącznikami • Prosimy o połączenie w tabeli pól Nazwa i adres płatnika / odbiorcy – Nazwa i adres będą przekazywane w jednym polu • Pole Imiona i nazwisko / Nazwa PSU – do weryfikacji czy faktycznie dla osoby prawnej będzie tu podawana nazwa. Wydaje się, że również w przypadku firmy jako PSU będzie występować osoba fizyczna (faktyczny użytkownik). Nazwa firmy jest w tym przypadku wtórna. Kluczowe jest uprawnienie PSU do rachunków tej firmy. • Numer instrumentu płatniczego – prosimy o doprecyzowanie, że chodzi o zaciemnienie (np. zaiksowanie) numeru instrumentu płatniczego		tak	
171	Prośba o dodanie nowego pola w kategorii "informacja o rachunku płatniczym" o nazwie: "Ograniczenia dla rachunku płatniczego".	Powinna istnieć informacja czy dany rachunek ma jakieś ograniczenia, np. brak możliwości uznania, brak możliwości obciążenia itp.	nie	Każdy ASPSP może dodać do udostępnianego zakresu danych na temat rachunku i transakcji dodatkowe pola
172	Prosimy o dodanie pola "MCC" dla transakcji kartowych".	Pole to umożliwi przekazanie tej danej tym ASPSP, którzy prezentują ją klientowi on-line.	tak	

173	Proponujemy dodanie pola „client type” ze słownikiem, np.: • konsument • firma (forma prawna)	Jest to pole niezbędne dla rozróżnienia rodzaju konta w celu jego prawidłowej prezentacji.	nie	Każdy ASPSP może dodać do udostępnianego zakresu danych na temat rachunku i transakcji dodatkowe pola
174	Proponujemy dodanie nowych pól w kategorii Informacja o rachunku, tj.: • status karty (ze słownikiem) • numer rachunku karty • informacja o użytkowniku (Imię i nazwisko) • numer karty głównej (n pól) • numer karty dodatkowej (n pól) • termin ważności karty • bieżący cykl rozliczeniowy (data od-do) • całkowita kwota i waluta spłaty • minimalna kwota i waluta spłaty • oprocentowanie • termin spłaty karty (data) • wykorzystany limit (kwota i waluta) • przyznany limit (kwota i waluta) • zaległa kwota spłaty z poprzedniego cyklu rozliczeniowego (kwota i waluta)	Pole te umożliwią nam (jako ASPSP) przekazanie danych o wszystkich rachunkach płatniczych, w szczególności informacji o karcie kredytowej zgodnie z art. 36 p. 1 (a) RTS.	nie	Zakres danych oraz ich wymagalność może różnić się w różnych implementacjach. 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
175	Proponujemy dodanie nowych pól w kategorii Informacja o rachunku, tj.: • saldo nowych środków • stan twoich środków na dzień DD-MM-RRRR/Saldo początkowe;	Pola te umożliwią nam (jako ASPSP) przekazanie danych, które wydają się być istotne z punktu widzenia klienta dla produktów na nowe środki.	nie	Każdy ASPSP może dodać do udostępnianego zakresu danych na temat rachunku i transakcji dodatkowe pola
176	Pole, które w specyfikacji nazywa się „**nazwa rodzaju rachunku (definiowana przez Bank)**”, w swaggerze nosi nazwę „**nazwa typu rachunku (definiowana przez Bank)**”.		tak	
177	pole, które w specyfikacji nazywa się **„dostępne środki”,** w swaggerze nosi nazwę **„dostępne środki - po wykonaniu transakcji”.**		tak	
178	pole, które w specyfikacji nazywa się „**saldo księgowe rachunku**”, w swaggerze nosi nazwę „**saldo księgowe rachunku - po wykonaniu transakcji**”.		tak	

179	pole, które w specyfikacji nazywa się „**data waluty**", w swaggerze nosi nazwę „**data kursu waluty"**		tak	
180	pole, które w specyfikacji nazywa się **„id transakcji",** w swaggerze nosi nazwę **„identyfikator transakcji".**		tak	
181	pole, które w specyfikacji nazywa się „**typ przelewu**", w swaggerze nosi nazwę „**typ transferu".**		tak	
182	prośba o wyjaśnienie / doprecyzowanie zapisu w wierszu 3 w kontekście usługi AIS. Na ten moment interpretujemy go tak: po pozytywnej procedurze udzielenia wyraźnej zgody i po przekazaniu przez ASPSP Acess Token nie może być od razu przekazana informacja o wybranych rachunkach i historii. Czy taka była intencja tego zapisu?		nie	Zapisy tego rozdziału uległy zmianom.
183	prosimy o doprecyzowanie co oznacza oczekująca transakcja płatnicza? Czy chodzi o transakcje, które zostały zlecone (mają datę transakcji) i oczekują na księgowanie? E - brak informacji o takiej transakcji w rozdziale 3.1.3. str. 17 – w naszej ocenie wymaga uzupełnienia)		tak	
184	prosimy o doprecyzowanie wg jakiej daty będą sortowane zwracane rekordy (daty transakcji czy daty księgowania)? i czy będzie możliwość dodania tej informacji w ramach Polish API?		tak	
185	Prosimy o wpisanie w pierwszym wierszu tabeli w wierszu Data formatu daty w formie zgodnej z ISO, tj.: YYYY-MM-DD na YYYY-MM-DDThh:mm:ss.ccczzzzzz Ten format daty jest uwzględniony w swaggerze.	Jest to niezbędne w celu prezentacji transakcji w historii z zachowaniem osi czasu (chronologicznie) w kolejności takiej jaka jest prezentowana klientowi w jego bankowości elektronicznej.	tak	
186	Proponujemy aby w ramach usługi PIS dla jako domyślnie przyjąć tryb realizacji SHA dla przelewów SEPA oraz dla przelewów innych niż SEPA po wybraniu IBAN który jest z krajów EOG		tak	

187	Prosimy o uwzględnienie w specyfikacji zasad obsługi rachunków płatniczych służących do obsługi podzielonej płatności tzw. Split Payments w kontekście zarówno ich agregacji (usługa AIS) jak również inicjowania płatności (PIS)	Brak informacji w specyfikacji w tym zakresie.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
188	Prosimy o uwzględnienie w specyfikacji zasad obsługi procesu wieloosobowej autoryzacji płatności w ramach usługi inicjowania płatności (PIS)	Brak informacji w specyfikacji w tym zakresie, podczas gdy wieloosobowa autoryzacja płatności dotyczy dużej części rachunków płatniczych firm.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
189	Rozszerzenie zapisu “TPP posiada ważny certyfikat”	“TPP posiada ważny certyfikat kliencki, którym identyfikuje się przed ASPSP.”	tak	
190	Korekta do zapisu “ Wymaganym sposobem przyznawania autoryzacji dostępu do zasobu jest zastosowanie przez serwer w odpowiedzi na żądanie użytkownika jednorazowych kodów autoryzacyjnych OAuth 2.0 zanim zostanie przyznany właściwy token dostępu.”	"Wymaganym sposobem autoryzacji dostępu do zasobu jest zwrócenie przez serwer w odpowiedzi na żądanie użytkownika jednorazowego kodu autoryzacyjnego, który zostanie w kolejnym kroku zamieniony na właściwy token dostępu zgodnie z protokołem OAuth 2.0.”	tak	
191	Niejasne jest sformuowanie “stanie żądania” w zdaniu: “Token dostępowy przekazywany jest do TPP wraz z informacją o stanie żądania”. Authorization Response w protokole oAuth 2.0 nie zawiera informacji o stanie żądania, chyba że autor ma na myśli parametr “state”.	Doprecyzowanie co oznacza “stan żądania” lub usunięcie tego fragmentu.	tak	

192	Korekta sugerowanego podejścia: “Kod autoryzacyjny może być zaimplementowany po stronie serwera w postaci odniesienia do bazy danych utrzymywanej przez serwer (tj. jako identyfikator obiektu przechowywanego na serwerze) lub zawierać w sobie wszystkie informacje.“ Sugerujemy, aby zawrzeć zapis, że kod / token powinien być wskazaniem obiektu w bazie danych, gdzie dane wskazanego obiektu służą do identyfikacji klienta na rzecz którego realizowane są operacje. Zalecamy stosowanie tzw. stateless token (np. JWT Token - RFC 7519) tylko w przypadku, gdy ujawnienie danych o kliencie (w tym identyfikatora) ASPSP jest zgodne z polityką bezpieczeństwa.	“Sugeruje się aby Po stronie serwera ASPSP kod autoryzacyjny 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.”	tak	
193	Wprowadzenie obowiązkowego mechanizmu uwierzytelnienia 1.4.4.1 lub następcy 1.4.4.2.1, a kolejne uznać jako dodatkowe.	Wprowadzenie oAuth 2.0 jako mechanizmu uwierzytelnienia to bardzo dobra praktyka i dlatego sugeruje się aby w ramach PolishAPI wprowadzony został obowiązek co do implementacji mechanizmu z pkt. 1.4.4.1 lub przekierowania do mechanizmu zgodnego z 1.4.4.1 w ramach 1.4.4.2.1. Pozostawienie dowolności w tej kwestii może skutkować faktem, że każdy ASPSP będzie wymagał innego mechanizmu, co będzie utrudnieniem w implementacji standardu.	nie	Metoda, uwzględniająca uwierzytelnienie PSU po stronie ASPSP nie jest jedyną metodą dopuszczaną przez standard, zgodnie z regulacjami.
194	Korekta do zapisu “w interfejsie udostępnionym przez ASPSP”. Warto jasno określić, że proces uwierzytelnienia musi być realizowany w interfejsie udostępnionym.	“Uwierzytelnienie PSU przeprowadzane jest w interfejsie udostępnionym przez ASPSP lub wskazanym przez ASPSP. Niedopuszczalne jest podawanie danych uwierzytelniających klienta w interfejsie niepowiązanym z ASPSP.”	nie	Ustalenie grupy projektowej Polish API.

195	Doprecyzowanie faktu, czy licznik liczby zapytań w ciągu 24 godzin resetuje się wraz z żądaniem inicjowanym przez PSU.	W ramach aktualnego zapisu nie jest jasne czy licznik dopuszczalnej liczby zapytań w ciągu 24h będzie zresetowany wraz z nowym zapytaniem inicjowanym przez PSU.	nie	Nie, licznik zapytań inicjowanych przez TPP w ciągu 24-godzinnego okresu nie resetuje się po zapytaniu inicjowanym przez PSU.
196	Lista pól w zakresie Zgodności zawiera nazwę TPP oraz inicjator transakcji. Czy aby na pewno te dane powinny być udostępniane innym TPP?	Cel udostępnienie danych o TPP oraz inicjatora transakcji jest niejasny i może być powodem łamania tajemnicy handlowej między bankiem a TPP.	nie	Uwaga niezrozumiała.
197	Sugerowana zmiana do "PSU wypełni wszystkie dane wymagane do …" Odpowiedzialnym za dostarczenie danych w celu złożenia zlecenia wykonania przelewu jest TPP. Natomiast TPP musi zadbać o to, że te dane pochodzą po części z jego wiedzy ale również od PSU.	"TPP we współpracy z PSU dostarczy wszystkie dane wymagane do …"	nie	
198	Sugerowane rozszerzenie opisu złożenia zlecenia przelewu o fakt niemodyfikowalności danych przekazanych w ramach złożenia zlecenia przelewu.	Dane, które przekazuje TPP w zleceniu przelewu nie powinny być modyfikowane przez PSU w domenie ASPSP. Jedyna możliwość modyfikacji mogłaby dotyczyć wyboru rachunku, z którego ma być dokonany przelew. Zalecamy dodanie stosownego zapisu w tym zakresie.	tak	
199	Wprowadzenie jednolitej definicji, które pola są wymagane. W tym momencie wymagane pola są określone tylko dla List pól wymaganych przez APSP w zakresie Zgodności (pkt. 3.3.1), natomiast brak tej informacji dla tabel w 3.2.3.	W tym momencie brakuje jasnej informacji, które pola są wymagane, a wprowadzenie takiej kolumny w jednej z tabel sugeruje, że nie wszystkie pola są wymagane w poprzednich tabelach	tak	
200	Korekta do opisu w Ilustracji 7: "ASPSP może odrzucić transakcję…"	"ASPSP może odrzucić zapytanie…"	tak	
201	Korekta do opisu w Ilustracji 8: "ASPSP może odrzucić transakcję…"	"ASPSP może odrzucić zapytanie…"	tak	
202	Korekta do opisu w Ilustracji 9: "Przekierowanie użytkownika w domenę ASPSP."	"Przekierowanie użytkownika do domeny ASPSP."	tak	

203	W opisie pojawia się pojęcie Hub PSD2, które wcześniej jest niewprowadzone.	Pojawiające pojęcie Hub PSD2 powinno być wyjaśnione z uwagi na fakt, że jest istotnym elementem PKI. Czy w ramach ZBB lub zespołu PolishAPI powstanie Certificate Authority, które będzie zajmowało się utrzymaniem PKI?	tak	
204	W opisie pojawia się stwierdzenie, które mówi, że wykorzystanie mutual authentication zabezpieczy ASPSP przed sytuacją, w którzym urządzenie klienckie korzystałoby bezpośrednio z serwerów ASPSP.	Mutual authentication nie zabezpieczy ASPSP przed tego typu sytuacją. Nic nie stoi na przeszkodzie, żeby TPP stworzył aplikację mobilną np. na platformę Android w którym tak skonfiguruje KeyStore, że wykorzysta certyfikat klienci w celu komunikacji z serwerem.	tak	
205	Istnienie instytucji pełniącej Hub tożsamości jest niejasne i ewentualne związane z tym koszty TPP mogą być niezgodne z dyrektywą PSD2.	W związku z wprowadzeniem mutual authentication i potrzebą istnienia PKI, nie jest jasne czy zyskanie certyfikatu będzie wiązało się z poniesieniem kosztów?Co więcej, koszty z tym związane mogą być niezgodne z PSD2, z uwagi na fakt, że dostęp do API nie powinien nieść za sobą żadnych kosztów.	nie	Zapisy dotyczące Huba PSD2 zostały ograniczone, kwestie związane z certyfikatami oraz ich uzyskiwaniem są poza zakresem dokumentu.

206	Proponujemy rezygnację z mutual authentication na rzecz klucza API.	Wprowadzenie mutual authentication w stosunku do rozwiązania z kluczem API wprowadza wymaganie utrzymywania bezpiecznej infrastruktury klucza publicznego co może nieść za sobą niepotrzebne koszty i odpowiedzialność. Proponujemy aby ASPSP umożliwiał wygenerowanie TPP klucza dostępu do API z ograniczonym czasem ważności. Zastosowanie PKI w żaden sposób nie wprowadza większego poziomu bezpieczeństwa w zakresie przechowywania danych dostępowych przez TPP. Ujawnienie klucza prywatnego (nawet zabezpieczonego, ponieważ hasło musi być w tym samym miejscu co klucz) czy też klucza API jest równoważne.	nie	Ustalenie grupy projektowej Polish API.
207	Korekta do “Domena DNS/adres - URL, pod którym…” Słowo URL w tym kontekście jest niepoprawne, URL oznacza pełny adres zasobu.	“Domena DNS - adres, pod którym…”	tak	

208	W tym momencie w ramach udokumentowanych statusów brak rozróżnienia pomiędzy niepoprawnym syntaktycznie zapytaniem a błędem walidacji danych.	Proponujemy aby serwer zwracał 400 Bad Request, jeżeli zapytanie jest niepoprawne syntaktycznie - np. podano dane w niepoprawnym formacie JSON. Natomiast w przypadku wystąpienia błędu walidacji dla zapytania poprawnego synktaktycznie serwer powinien zwrócić status 422 Unprocessable Entity (https://httpstatuses.com/422). Takie podejście pozwoli ASPSP łatwiej implementować mechanizm walidacji, ponieważ w większości przypadków frameworki automatycznie zwracają status 400 kiedy zapytanie było niepoprawne z opisem słownym. Natomiast wprowadzenie statusu 422 pozwoli zawsze zwracać błędy walidacji w formacie JSON. Co więcej TPP, będzie pewien, że status 422 zawsze może być przetwarzany jako JSON, natomiast status 400 będzie zawierał opis w postacji napisu.	tak	
209	Zaleca się wprowadzenie prefix “Bearer” w nagłówku Authorization.	Wartość nagłówka Authorization powinien składać się z “type” + “credentials”, gdzie w przypadku podejścia z wykorzystaniem tokenu “type” powinien mieć wartość “Bearer”.	tak	
210	Kwota transakcji powinna być prezentowana w groszach w JSON.	Proponujemy aby kwota była reprezentowana jako typ number w JSON, gdzie część dziesiętna i setna jest usuwana poprzez przemnożenie kwoty x 100.	nie	Ustalenie grupy projektowej Polish API.
211	Reprezentacja liczby rzeczywistej w JSON powinna być typem number.	JSON pozwala reprezentować liczby rzeczywiste jako typ number.	nie	Ustalenie grupy projektowej Polish API.

212	Wymaganie mówiące o tym, że implementacja API musi być zabezpieczona przed CSRF jest niepoprawne.	Zalecamy doprecyzowanie zabezpieczenia przed CSRF. ASPSP udostępnia tak na prawdę 2 rodzaje: - API oAuth 2.0 (TPP - PSU - ASPSP) - API do komunikacji TPP-ASPSP Dla API oAuth 2.0 zabezpieczenie przed CSRF powinno być zrealizowane w oparciu o parametr state. Natomiast wymaganie wprowadzenia zabezpieczeń przed CSRF dla API TPP-ASPSP powinno być usunięte, ponieważ tego typu komunikacja nie jest podatna na ten typ ataku.	nie	
213	Wykonanie Authorization Request nie może być zapytaniem POST, tylko GET	Zgodnie z wymaganiami RFC (4.1.1) dla oAuth 2.0 zapytanie Authorization Request powinno być zapytaniem typu GET, natomiast parametry query powinny być zakodowane zgodnie z application/x-www-form-urlencoded.	tak	
214	Czym jest client_id w Authorization Request.	W protokole oAuth 2.0 client_id jest identyfikatorem klienta - domniema się zatem, że w PolishAPI client_id to identyfikator TPP? Jak zatem ASPSP będzie w stanie powiązać dane ze scope_details (np. paymentAccount) z klientem ASPSP?	nie	Uwaga niezrozumiała.

215	Rezygnacja z wprowadzenia parametru scope_details z uwagi na fakt, że rozszerza to niepotrzebnie oAuth 2.0 i bez enkodowania nie zadziała poprawnie z zapytaniem GET.	Proponujemy zrezygnować z wprowadzenia scope_details, na rzecz udostępnienia metody w API dla TPP - ASPSP, gdzie TPP będzie w stanie zarejestrować definicje tzw. scopeGroup w wyniku czego otrzyma $ID. Otrzymane $ID mogłoby być przekazane w ramach parametru scope np. Jako “pis:payment:$ID”. Rezygnacja ze scope_details sprawi, że PolishAPI będzie w pełni zgodnie z oAuth 2.0 oraz wszystkie istniejące implementacji oAuth 2.0 będą mogły zostać wykorzystane zarówno po stronie TPP jaki i ASPSP.	nie	Ustalenie grupy projektowej Polish API.
216	Usunięcie wymagania podania JWS dla protokołu oAuth 2.0	Nie ma potrzeby aby ASPSP na poziomie oAuth wymagał i weryfikował JWS z uwagi na istnienie parametru client_id, state oraz redirect_uri. Nawet w przypadku próby podrobienia zapytania, implementacja TPP poradzi sobie z niewłaściwym redirectem wykorzystując parametr state.	nie	Ustalenie grupy projektowej Polish API.
217	Wprowadzenie wymagania weryfikacji przez ASPSP redirect_uri.	Zaleca się aby ASPSP posiadał w swojej konfiguracji dla danego client_id listę redirect_uri, które mogą być wykorzystane. Dzięki czemu ASPSP nie przeniesie klienta na adres URI, który może być adresem podłożonym przez niezaufaną stronę.	nie	Ustalenie grupy projektowej Polish API.
218	Wprowadzenie API do weryfikacji access_token i przydzielonych scopeDetails.	Proponujemy, aby wprowadzone zostało wymaganie udostępnienia API dla TPP, dzięki któremu TPP podając access_token oraz client_id będzie w stanie otrzymać informacje o tokenie oraz przydzielone ostatecznie scopeDetails.	nie	Ustalenie grupy projektowej Polish API.

219	Brak wyjaśnienia dlaczego wprowadza się wymaganie przekazania is_user_session, user_ip, user_agent w procedurze generowania access_token na podstawie refresh_token.	Ciężko znaleźć zastosowanie w którym TPP w momencie generowania access_token na podstawie refresh_token będzie to robił w ramach sesji PSU. Zwracamy się z prośbą o wyjaśnienie tego wymagania.	tak	
222	Naszym zdaniem API nie jest zgodne z PSD2, tj nie oddaje obowiązków ASPSP/banków wynikających z PSD2. Zgodnie z obecną propozycją TPP nie byliby i nie mogliby być zobowiązani do opierania się na tym interfejsie. Istnieje kilka braków, którymi należy się zająć, jeśli API ma być zgodne z obowiązkami nałożonymi przez PSD2 i RTS.		tak	W naszej opinii standard spełnia wymogi regulacyjne.
223	Po pierwsze i najważniejsze standard musi zapewniać, że PISP otrzymują wszelkie informacje o tej inicjatywie i wykonaniu, jakich potrzebują, aby realizować swoje usługi i jakie są wymagane zgodnie z Art. 66 ust. 4b PSD2. Obecnie nie ma to miejsca, ponieważ przypadek użycia PIS nie obejmuje tej informacji i nie może być to usługa premium ani dodatkowa, która jest świadczona za dodatkową opłatą.		tak	PISP ma pełną możliwość uzyskania informacji statusowej, dotyczącej zainicjowanej płatności, istnieją 3 drogi jej uzyskania: w odpowiedzi na request inicjujący płatność oraz asynchronicznie w sposób inicjowany przez PISP oraz asynchronicznie w sposób inicjowany przez ASPSP.
224	Po drugie mechanizm przekierowania (uwierzytelnienie po stronie ASPSP') może być oferowane jako jedna opcja, lecz nie może być narzucone. Obowiązkowe przekierowanie do strony ASPSP jest niezgodne z PSD2/RTS (patrz np. Art. 32 ust. 3 RTS). To samo dotyczy Oauth, gdzie należy zapewnić, że można z tego korzystać bez przekierowania.		nie	Wersja 1.0. uwzględnia dodatkową metodę autentykacji (decoupled).
225	Po trzecie należy zapewnić, że PISP i AISP mogą polegać na istniejących procedurach uwierzytelniania podczas korzystania z API. Nie może istnieć żaden „dodatkowy zestaw" procedur dla API lub dla TPP, ani w odniesieniu do SCA ani wyłączeń z SCA. Równorzędne traktowanie oraz zakaz dyskryminacji wymagają, aby procedury uwierzytelniania były takie same w przypadku bezpośredniego i pośredniego dostępu przez API. API powinien umożliwiać poleganie na		tak	Wersja 1.0. uwzględnia dodatkową metodę autentykacji (decoupled). Trwają prace nad kolejnymi metodami autentykacji. Metoda wykorzystująca redirection jest na polskim rynku powszechnie akceptowana i używana przez klientów, banki i strony trzecie.

	istniejących procedurach (bez mechanizmu przekierowania, patrz powyżej).			
226	Po czwarte API powinno pozwalać na połączenie PIS i AIS, przynajmniej w jednej połączonej sesji. W oparciu o PSD2 ustalił się konsensus w Grupie Roboczej Euro Retail Payments Board (ERPB) dot. PIS, że dedykowane API musi obsługiwać przekazywanie tylko PIS, tylko AIS lub obu tych usług podczas jednej łączonej sesji komunikacyjnej.		nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
227	Ponadto pragniemy podkreślić, że poniższe komentarze niekoniecznie stanowią wyczerpującą listę wątpliwości i zastrzeżeń. Konsultacje w pierwszym kroku nie zapraszały do testowania praktycznego, lecz były prowadzone wyłącznie w oparciu o papiery. W wielu przypadkach nie możemy jeszcze ocenić sposobu, w jaki teoria zostanie przełożona na praktykę. Wiele terminów, np. „wbudowany” (embedded) mechanizm uwierzytelniania to nowe rzeczy, w odniesieniu do których rzeczywiste wdrożenie w praktyce będzie decydujące. W drugim kroku tej konsultacji, gdzie przedstawiana jest rzeczywista infrastruktura do praktycznego testowania, możemy mieć znacznie więcej komentarzy i pytań.		nie	Tak, zgadzamy się.

228	Zapewnienie koniecznych informacji na temat roli PISP Jedyny przypadek użycia przypisany do roli PISP to „inicjacja pojedynczej płatności przez PISP". Jednakże ten przypadek użycia nie jest wystarczający, aby objąć całą rolę usługi inicjacji płatności. Zgodnie z dogłębną dyskusją w ramach Grupy Roboczej ERPB dot. PIS, usługa PIS nie powinna potrzebować drugiej licencji / rejestracji jako AIS w celu uzyskania danych, jakie potrzebuje do realizacji PIS. API powinien zatem udostępniać dodatkowe dane, aby obsługiwać oceny oparte na ryzyku dotyczące prawdopodobieństwa niewykonania transakcji (w przypadku, gdy brak jest wykonania w czasie rzeczywistym).	Przypadku użycia, jakie są obecnie przewidziane dla roli AISP, powinny również być dostępne dla TPP działającego tylko jako PIS.	nie	W oparciu o regulacje, do uzyskania informacji w ramach AIS niebędna jest licencja AISP.
229	Zapewnienie informacji o realizacji transakcji PSD2 przewiduje, że ASPSP „niezwłocznie po otrzymaniu zlecenia płatniczego od dostawcy świadczącego usługę inicjowania transakcji płatniczej przekaże lub udostępni […] wszystkie informacje dostępne dostawcy usług płatniczych prowadzącemu rachunek dotyczących wykonania transakcji dostawcy usługi inicjowania transakcji płatniczej" Jednakże, nie możemy znaleźć takiej odpowiedzi o wykonaniu transakcji płatności w dokumentacji. W ramach ERPB strony omówiły informacje, jakie muszą być udostępnione PISP zgodnie z PSD2 („Co"). Omówiono w ramach ERPB i potwierdzono z EBC oraz Komisją Europejską, że muszą one obejmować co najmniej albo potwierdzenie płatności w środowisku w czasie rzeczywistym (natychmiastowe księgowanie) albo w środowisku wsadowym (i) saldo rachunku, (ii) limit kredytowy w rachunku bieżącym oraz (iii) transakcje oczekujące/zaplanowane.	Dla roli PISP, dodać odpowiedź na wykonanie transakcji płatniczej (tj przedstawić pełne informacje wymagane przez PSD2).	nie	PISP ma pełną możliwość uzyskania informacji statusowej, dotyczącej zainicjowanej płatności, istnieją 3 drogi jej uzyskania: w odpowiedzi na request inicjujący płatność oraz asynchronicznie w sposób inicjowany przez PISP oraz asynchronicznie w sposób inicjowany przez ASPSP.

230	Sesja w API Kluczowe jest, aby koncepcja sesji była obowiązkową częścią ram Polish API. Jeśli klient zdecyduje się korzystać z TPP do, np. agregowania danych swojego rachunku, a następnie inicjacji transakcji, możliwe musi być połączenie takich przypadków użycia w jednej sesji. W przeciwnym razie klient będzie musiał się logować dla każdego przypadku użycia, co poważnie pogorszy doświadczenie klienta, uniemożliwiając dostawcy PIS i AIS realizację bezproblemowej usługi.	Obsługa sesji w API musi być obowiązkowa dla ASPSP. Jeśli klient zleci TPP wykonanie kilku przypadków użycia, możliwe musi być wykonanie tych transakcji/przypadków użycia bez realizacji SCA dla każdego pojedynczego przypadku użycia.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
231	Zgoda Należy zauważyć, że zgoda na inicjację i wykonanie transakcji płatniczej jest zawsze udzielana za pośrednictwem PISP pod warunkiem, że jest on zaangażowany. PISP następnie przekazuje informacje o zgodzie na inicjację i wykonanie transakcji płatniczej do ASPSP (patrz również szkic ostatecznego raportu Grupy Roboczej ERPB dot. PIS). Nie ma żadnych dodatkowych zgód, lub też rozdzielenie jest wymagane pomiędzy (a) wyrażeniem zgody na skorzystanie z usługi PIS oraz (b) autoryzacją transakcji płatniczej. Patrz również Art. 32 ust. 3 RTS: „Dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, zapewniają, aby interfejs ten nie stwarzał przeszkód w świadczeniu usług inicjowania płatności i usług dostępu do informacji o rachunku. Przeszkody takie mogą obejmować m.in. (...) wymóg uzyskania dodatkowych zezwoleń oraz dodatkowych rejestracji oprócz tych przewidzianych w art. 11, 14 i 15 dyrektywy 2015/2366 lub wymóg dodatkowej weryfikacji zgody udzielonej dostawcom usług inicjowania płatności i usług dostępu do informacji o rachunku przez użytkowników usług płatniczych.”	Zgoda na inicjację i wykonanie transakcji płatniczej jest zawsze udzielana za pośrednictwem PISP pod warunkiem, że jest on zaangażowany. API zgodne z PSD2/RTS nie może wymagać dodatkowych zezwoleń lub sprawdzeń zgody udzielonej PISP i AISP przez PSU.	tak	Dodatkowa autoryzacja zgody nie jest wymagana.

232	Przekierowanie / „Mechanizm uwierzytelniania po stronie ASPSP” „Podejście przekierowania” lub „Mechanizm uwierzytelniania po stronie ASPSP” jest niedopuszczalny dla TPP z wielu względów, np. nie jest zgodny z prawem TPP do swobodnego projektowania interfejsu klienta. Wszystkie te argumenty zostały omówione szczegółowo w ramach Grupy Roboczej ERPB dot. PIS. Patrz (szkic) ostatecznego raportu tej Grupy. W związku z tym nie można żądać od dostawców PIS i AIS wymuszonego przekierowania do strony ASPSP. API, które polega na przekierowaniu narusza PSD2 oraz RTS, tj ASPSP będzie naruszać swoje obowiązku wg PSD2 poprzez oferowanie tego, a TPPs nie będzie zobowiązany do stosowania tego API. Patrz również Art. 32 ust. 3 RTS: „Dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, zapewniają, aby interfejs ten nie stwarzał przeszkód w świadczeniu usług inicjowania płatności i usług dostępu do informacji o rachunku. Przeszkody takie mogą obejmować m.in. uniemożliwianie dostawcom usług płatniczych, o których mowa w art. 30 ust. 1, wykorzystywania danych uwierzytelniających wydanych przez dostawców usług płatniczych prowadzących rachunek ich klientom, wymuszanie przekierowania do mechanizmu uwierzytelniania lub innych funkcji dostawcy usług płatniczych prowadzącego rachunek (…)’.	Usunąć cały paragraf 1.4.4.1 Mechamizm uwierzytelniania po stronie ASPSP	nie	Nie zgadzamy się z tą opinią. Metoda redirection, jako taka, nie jest zakazana przez regulatora. Było to wielokrotnie wskazywane przez przedstawicieli Komisji Europejskiej, którzy zwracali uwagę, że jeżeli użycie tej metody nie powoduje przeszkod - wówczas moze być stosowana. Metoda wykorzystująca redirection jest na polskim rynku powszechnie akceptowana i używana przez klientów, banki i strony trzecie (transakcje uwzględniające autentykację PSU w ten sposób stanowią np. połowę wszystkich transakcji e-commerce). Jej masowa adopcja gwarantuje brak przeszkód w jej użyciu, jest to także metoda wspierana przez KNF (polskiego nadzorcę rynku finansowego).

233	„Mechanizm wbudowanego uwierzytelniania” PSD2 zakłada podejście wbudowane zgodnie z dyskusją w ramach Grupy Roboczej ERPB dot. PIS, oto dlaczego, m.in. Art. 66 ust. 3b stanowi, że PISP jest zobowiązany do zapewnienia, aby dane uwierzytelniające były przesyłane przez bezpieczne i wydajne kanały. Tak więc, kiedy ASPSP zapewnia procedurę uwierzytelniania opartą o przesyłane / przenośne dane uwierzytelniające, PISP lub AISP przesyła spersonalizowane dane uwierzytelniające bezpieczeństwa do ASPSP. Jednakże „mechanizm wbudowanego uwierzytelniania” przedstawiony tutaj jest nieakceptowalny z punktu widzenia TPP, szczególnie w odniesieniu do wymogu „uprzedniego uzgodnienia pomiędzy ASPSP oraz TPP w oparciu o dokumentację wdrożeniową dostarczoną przez ASPSP”. PSU udzieli zgody i uwierzytelni transakcję płatniczą za pomocą SCA za pośrednictwem TPP. Art. 97 ust. 5 PSD2 precyzuje, że TPP będą mogły polegać na wszystkich istniejących procedurach uwierzytelniania. Art. 66 ust. 3b PSD2 oraz punt 30 w preambule wskazują, że obejmuje to zdolność przesyłania dalej danych uwierzytelniających w imieniu PSU.	Podczas gdy przekierowanie musi być wyłączone, opieranie się na istniejących procedurach uwierzytelniania w „podejściu wbudowanym” zgodnie z dyskusją w ramach Grupy Roboczej ERPB dot. PIS musi być ujęte w każdym API. Jednakże „mechanizm wbudowanego uwierzytelniania” przedstawiony tutaj, wymagający „uprzedniego uzgodnienia pomiędzy ASPSP oraz TPP „ jest nieakceptowalny.	tak	Problem zostanie zaadresowany w następnej wersji specyfikacji.

233	„Mechanizm wbudowanego uwierzytelniania” PSD2 zakłada podejście wbudowane zgodnie z dyskusją w ramach Grupy Roboczej ERPB dot. PIS, oto dlaczego, m.in. Art. 66 ust. 3b stanowi, że PISP jest zobowiązany do zapewnienia, aby dane uwierzytelniające były przesyłane przez bezpieczne i wydajne kanały. Tak więc, kiedy ASPSP zapewnia procedurę uwierzytelniania opartą o przesyłane / przenośne dane uwierzytelniające, PISP lub AISP przesyła spersonalizowane dane uwierzytelniające bezpieczeństwa do ASPSP. Jednakże „mechanizm wbudowanego uwierzytelniania” przedstawiony tutaj jest nieakceptowalny z punktu widzenia TPP, szczególnie w odniesieniu do wymogu „uprzedniego uzgodnienia pomiędzy ASPSP oraz TPP w oparciu o dokumentację wdrożeniową dostarczoną przez ASPSP”. PSU udzieli zgody i uwierzytelni transakcję płatniczą za pomocą SCA za pośrednictwem TPP. Art. 97 ust. 5 PSD2 precyzuje, że TPP będą mogły polegać na wszystkich istniejących procedurach uwierzytelniania. Art. 66 ust. 3b PSD2 oraz punt 30 w preambule wskazują, że obejmuje to zdolność przesyłania dalej danych uwierzytelniających w imieniu PSU.	Podczas gdy przekierowanie musi być wyłączone, opieranie się na istniejących procedurach uwierzytelniania w „podejściu wbudowanym” zgodnie z dyskusją w ramach Grupy Roboczej ERPB dot. PIS musi być ujęte w każdym API. Jednakże „mechanizm wbudowanego uwierzytelniania” przedstawiony tutaj, wymagający „uprzedniego uzgodnienia pomiędzy ASPSP oraz TPP „ jest nieakceptowalny.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
234	Protokół Oauth2 Jeśli ASPSP zdecyduje się skorzystać z protokołu OAuth2, musi zapewnić, że zwracany token może być przesyłany za pośrednictwem podejścia wbudowanego zgodnie z dyskusją w ramach Grupy Roboczej ERPB WG dot. PIS – oraz że przekierowanie jest w związku z tym wykluczone, tj. API nie może wymagać opuszczenia strony TPP w żadnym momencie procesu.		nie	Ustalenie grupy projektowej Polish API.
235	Pod rozwagę sugerujemy zmianę w całym dokumencie nazwy COF na CAF	Zmiana podyktowana wytycznymi i nazewnictwem KNF	tak	
236	Czy nie powinno być doprecyzowane o jaki certyfikat chodzi?	Prośba o doprecyzowanie	tak	
237	Czy token dostępu również jest przyznawany danej instytucji TPP jednorazowo?	Prośba o doprecyzowanie	n/a	

238	Wydaje się, że nie jest wskazanym twarde określanie ilości („trzy") mechanizmów uwierzytelniania przed finalnym określeniem wybranych metod.	Zmiana redakcyjna	tak	
239	Z zapisu „Zgodnie z PSD2, TPP… definiuje ramy udzielania oraz odwoływania zgód przez PSU." wynika, że z poziomu TPP, PSU powinien mieć możliwość zmiany uprawnień.	Może się okazać niemożliwym realizacja takiego wymagania ponieważ użytkownik końcowy nie musi mieć umocowań do zarządzania uprawnieniami po stronie firmy.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
240	„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 COF" - dla Klientów instytucjonalnych PSU (rozumiany jako osoba reprezentująca firmę) może nie mieć umocowań do udzielania takiej zgody	Prośba o doprecyzowanie w zakresie obszaru firm/korporacyjnego	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
241	Co rozumiemy przez pojęcie „wyraźnej zgody"?	Prośba o doprecyzowanie	nie	Zapisy dotyczące zgód zostały zmienione i doprecyzowane.
242	Z zapisu można rozumieć, że TPP przekazuje tylko zgodę, a ASPSP nic z nią nie robi. Prosimy o doprecyzowanie czym jest „zgoda PSU" w tym kontekście?	Prośba o doprecyzowanie	nie	Zapisy rozdziału zostały zmienione w całości.
243	Czy standard będzie przewidywał możliwość dwustronnej kilkukrotnej komunikacji innej niż odebranie zgody (czy też przekazanie informacji o statusie transakcji)? Np. gdy w Banku zabraknie jakiejś informacji	Przykładowo: gdyby w ASPSP zabrakło jakiejś danej do prawidłowego wykonania usługi (a takiej danej nie uwzględnia specyfikacja Polish API), ASPSP mogłoby poprosić TPP o tą informację	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
245	„PSU wskazuje ASPSP" - Czy nie powinno zostać doprecyzowane jak ma wyglądać proces wskazania ASPSP przez PSU po stronie TPP? (np. wybór Banku z listy, i/lub wpisanie nazwy/nr rachunku w formularzu lub ewentualnie inny proces)	Prośba o doprecyzowanie	nie	

246	1. Czy i ewentualnie jak ASPSP ma weryfikować te parametry? 2. Czy treść tej zgody jest przekazywana do ASPSP? 3. W nawiązaniu do dyskusji na ostatnim spotkaniu prawno-biznesowym – czy na tym etapie PSU ma wskazać rachunek płatniczy z którego mają zostać pobrane informacje, czy też ten filtr ma się znaleźć na poziomie ASPSP? 4. Czy takie menu na początku dla PSU do wskazania u TPP nie jest w żadnym punkcie „przeszkodą”?	Prośba o analizę prawną i doprecyzowanie	nie	Zapisy rozdziału zostały zmienione w całości.
247	„zakres danych” – W jaki sposób będzie określony zakres tych danych?	Prośba o doprecyzowanie	nie	Zapisy rozdziału zostały zmienione w całości.
248	„cel oraz sposób wykorzystania danych” – Czy informacje przekazywane w tym zakresie nie powinny być wystandaryzowane – zamknięta lista celów i sposobów wykorzystania?	Zdefiniowana lista ułatwi obsługę i wystandaryzuje podejście na rynku	nie	Zapisy rozdziału zostały zmienione w całości.
249	Czy przy takim rozpisaniu kroków nie powstaje ryzyko podwójnego autoryzowania PSU w ASPSP?	Prośba o analizę prawną	nie	Zapisy rozdziału zostały zmienione w całości.
250	1. Zakładamy, że ten fragment zostanie poprawiony zgodnie z dyskusją na spotkaniu grupy roboczej PolishAPI w dniu 30 stycznia w ZBP – zbieranie zgód na COF powinno odbywać się po stronie ASPSP 2. Czy może być stosowane SCA przy każdym zapytaniu COF?	Prośba o analizę prawną i uzupełnienie	tak	
251	Czy przewiduje się odwolywanie zgód udzielonych wobec TPP w interfejsie użytkownika ASPSP?	Prośba o doprecyzowanie	nie	W naszej opinii nie jest to dopuszczone przez regulacje.
252	Czy 4 razy liczy się od pierwszego zapytania (i następne od kolejnego pierwszego zapytania?), czy w cyklach 0:00-24:00, codziennie?	Prośba o doprecyzowanie	nie	Od pierwszego zapytania.
253	Jak w tym kontekście ma zadziałać SCA dla przykładowej funkcjonalności pokazywania stanu konta w bankowości internetowej? Czy może być tak, że jest to zależne od strategii danego ASPSP i będzie się różnić na rynku?	Prośba o doprecyzowanie	nie	W naszej opinii zagadnienie jest poza zakresem dokumentu specyfikacji standardu.

254	Czy jeżeli interfejs ASPSP pokazuje blokady i transakcje odrzucone w oddzielnym miejscu niż historia transakcji na rachunku płatniczym, to czy takie informacje (tzn. blokady i odrzucenia) mają być przekazywane do TPP? Inaczej mówiąc również, czy takie informacje jak blokady i odrzucone transakcje są definicyjnie informacjami o rachunku płatniczym i związanymi z nimi transakcjami?	Prośba o doprecyzowanie	nie	Ostateczna decyzja o udostepnieniu informacji pozostaje w gestii ASPSP.
255	„Oprocentowanie rachunku” - 1. A co w przypadku gdy oprocentowanie na jednym rachunku płatniczym ma trzy różne wartości (np. środki do 100 tys. od 100 tys. do 1 mln, od 1 mln w górę)? 2. Czy w ramach rachunku płatniczego mówimy tylko o oprocentowaniu środków na rachunku, czy też środków kredytowych (w przypadku rachunku z limitem kredytowym lub rachunku karty kredytowej)?	Prośba o doprecyzowanie	tak	
256	„Imiona i nazwisko / Nazwa PSU” - Co pokazujemy w przypadku współwłaścicieli? Czy pokazujemy tu tylko imiona i nazwisko osoby zalogowanej?	Prośba o doprecyzowanie - przedstawiciel czy też pełnomocnik współwłaścicieli może widzieć wszystkich właścicieli mających uprawnienia do rachunku.	nie	Problem zostanie zaadresowany w następnej wersji specyfikacji.
257	„Dostępne środki” – rozumiemy, że chodzi o środki wyrażone w walucie rachunku?	Prośba o doprecyzowanie	tak	
258	„ID transakcji” - To pole powinno być raczej opcjonalne, ponieważ nie jest prezentowane przy każdej transakcji. ASPSP nie zawsze udostępnia tą informację w bankowości elektronicznej (np. przy transakcji kartowej jest, ale przy przelewie zwykłym już nie).	Prośba o doprecyzowanie	tak	
259	„Numer rachunku nadawcy” oraz „Numer rachunku odbiorcy” – Czy nie powinno być „dla każdej transakcji przelewu”?	Zmiana redakcyjna	tak	
260	„Opis/tytuł” – Jak rozumiemy, w przypadku sytuacji w których mamy transakcje zarówno z opisem jak i tytułem to zwracamy obie wartości.	Prośba o doprecyzowanie lub rozdzielenie pól na dwa odrębne	tak	
261	„Typ przelewu” - Czy nie powinno być „Typ transakcji”?	W dokumencie Swagger jest „transactionType”	tak	

262	„Kurs transakcji – Dla każdej transakcji w historii rachunku” - Czy nie powinno być „dla transakcji w walucie innej niż waluta rachunku”?	Zmiana redakcyjna	tak	
263	„Unikalny Unikalny identyfikator instrumentu płatniczego, za którego pomocą wykonano transakcję - Np. numer karty płatniczej (zahashowany)” - Czy tu nie powinno być „częściowo-zahashowany”?	Jeśli mielibyśmy w całości hashować numer karty to klient nie mógłby odróżnić którą kartą zrealizował płatność (w przypadku gdy ma ich kilka).	tak	
264	„Rodzaj operacji” - Sugerujemy przygotowanie słownika z definicjami w celu wystandaryzowanego uzupełniania pola konkretnymi danymi	Prośba o uzupełnienie w celu wystandaryzowania rodzajów operacji	nie	Każdy ASPSP może samodzielnie zdefiniować pozycje słownika.
265	„Nazwa odbiorcy przelewu przychodzącego – Dla każdej transakcji w historii rachunku” - Powinno zdaje się być „dla każdego przelewu przychodzącego”. Generalną zasadą powinno być to, że dane pozycje dotyczą tylko przelewów, a nie wszystkich transakcji, na przykład „prowizji za prowadzenie rachunku”	Zmiana redakcyjna	tak	
266	„Nazwa odbiorcy przelewu przychodzącego – Dla każdej transakcji w historii rachunku. Pole określa odbiorcę płatności kartą dla transakcji kartowej” - Czy to pole nie powinno dotyczyć tylko przelewu przychodzącego, a nie też transakcji kartowej?	Zmiana redakcyjna	tak	
267	„Nazwa odbiorcy przelewu wychodzącego – Dla każdej transakcji w historii rachunku” - Powinno zdaje się być „dla każdego przelewu wychodzącego”.	Zmiana redakcyjna	tak	
268	„Kod Banku odbiorcy” oraz „Numer BIC/SWIFT Banku odbiorcy” - Czym się różni wartość pola kod banku odbiorcy od numeru BIC-jak należy je interpretować? O jaki kod chodzi?	Prośba o doprecyzowanie	tak	Dokonano zmian w zakresie przelewów zagranicznych
269	„Nazwa nadawcy przelewu przychodzącego - Dla każdej transakcji w historii rachunku” - Powinno być „tylko dla przelewów przychodzących”	Zmiana redakcyjna	tak	
270	„Nazwa nadawcy przelewu wychodzącego - Dla każdej transakcji w historii rachunku” - Powinno być „tylko dla przelewów wychodzących”	Zmiana redakcyjna	tak	

271	„Inicjator transakcji" – czy chodzi o imię i nazwisko inicjatora?	Prośba o doprecyzowanie	tak	
272	„Nazwa TPP" – prosimy o zdefiniowanie długości pola	Ma to znaczenie dla systemów domenowych	tak	
273	Brakuje podanego tppID na wejściu zlecenia przelewu, a przecież ma być później zwracane na szczegółach operacji	Prośba o uzupełnienie	tak	
274	„Nazwa nadawcy przelewu" - Co jeśli nadawcą nie jest właściciel tylko jego przedstawiciel? Podajemy nazwę przedstawiciela?	Prośba o doprecyzowanie	nie	Nadawcą jest właściciel rachunku. Wprowadzone zostało dodatkowe pole, zawierające informację o osobie zlecającej daną płatność
275	„Waluta - W przypadku, gdy pole jest puste, ASPSP wykona przelew w walucie rachunku." – czyli de facto przewalutuje wskazaną kwotę w domniemanej walucie rachunku na walutę PLN i przekaże do systemu rozliczeniowego? Może należy doprecyzować rzeczywiste działanie ASPSP.	Prośba o doprecyzowanie	nie	ASPSP może zdecydować o wymagalności tego pola.
276	1. Dlaczego została zmieniona nazwa na EEA? 2. Co będzie wyznacznikiem kwalifikacji do tej kategorii – waluta EUR i co jeszcze? 3. Z jakiego powodu nie ma tu pola „Klauzula kosztowa"	Prośba o doprecyzowanie i ewentualne przywrócenie nazwy SEPA – od sierpnia br. wszystkie banki musza się posługiwać pojęciem polecenie przelewu SEPA.	tak	Dokonano zmian w zakresie przelewów zagranicznych
277	„Nazwa Banku odbiorcy" - Jakie inne płatności mają być pod nową nazwą? Czy to pole ma być też dla innych płatności niż SEPA?	Zgodnie z Rozporządzeniem 260/2012 bank odbiorcy ma być zidentyfikowany poprzez wywnioskowane z rachunku IBAN – ta reguła dotyczy SEPA.	tak	Dokonano zmian w zakresie przelewów zagranicznych
278	„Wartość stała – SEPA" - Jaka jest relacja tego pola do nowej nazwy rodzaju przelewu?	Prośba o doprecyzowanie	tak	Dokonano zmian w zakresie przelewów zagranicznych
279	„Data wykonania przelewu" - W komentarzu należałoby doprecyzować co oznacza data wykonania przelewu – czy datę wysłania komunikatu, czy datę uznania banku beneficjenta czy jeszcze inna datę(?)	Prośba o doprecyzowanie	tak	Dokonano zmian w zakresie przelewów zagranicznych

280	„Numer BIC/SWIFT Banku odbiorcy” – 1. Jeżeli ma zostać utrzymane wspólne istnienie 4 pól dotyczących danych banku odbiorcy, to w komentarzu powinna być informacja co dla klienta oznacza wypełnienie wszystkich z nich np. jeżeli dane banku odbiorcy wynikające z kodu BIC będą sprzeczne z danymi wypełnionymi przez klienta w poniższych trzech polach, to płatność zostanie odrzucona – czy taki jest zamysł autorów? 2. Należy dodać „Numer ABA”. Jest to numer rozliczeniowy do Stanów Zjednoczonych zamiast SWIFT	Prośba o uzupełnienie	tak	Dokonano zmian w zakresie przelewów zagranicznych
281	Co do opisu w pkt 1 na diagramie, czy faktycznie PSU „inicjuje transakcje płatniczą”?	Prośba o doprecyzowanie	nie	Diagramy i ich opisy uległy zmianom w obecnej wersji.
282	"Kurs transakcji, Format 4,6 / Currency exchange rate" – niezrozumiały format pola numerycznego “4,6” (10 cyfr z czego 6 po przecinku?)	Zmiana redakcyjna	tak	