Privatbanka

Privatbanka, a.s.
PSD2 API dokumentácia

11.9.2019

Vykonané zmeny

P.č.	Zmena	Dátum	Meno
1.	Vytvorenie prvej verzie dokumentu	21.2.2019	
2.	Úprava dokumentácie (riešenie podľa SBAS)	3.5.2019	
3.	Úprava kapitoly 2.4.2 (presunutí úvodného bodu do kapitoly 2.4.2.1)	23.7.2019	
4.	Úprava kapitoly 2.4.2.1 (Postup vytvorenia súhlasu)	24.7.2019	
5.	Kapitola 2.6 a subkapitoly 2.6.1, 2.6.2 – úprava endpointov	24.7.2019	
6.	Kapitola 2.7.1, 2.7.2, 2.7.3., 2.7.4., 2.8.1.3, 2.8.1.4, 2.8.1.5, 2.9.2.4, 2.9.2.5, 2.9.2.6, 2.9.3.3., 2.9.3.4, 2.9.3.4.2., 2.9.3.4.3, 2.9.3.5., 2.9.3.6. 2.9.4.4. – úprava endpointov	24.7.2019	
7.	Kapitola 2.8.1.1, 2.8.1.2, 2.9.4.3. – úpravy textu	24.7.2019	
8.	Kapitola 2.9.4.4. – Doplnenie položky dateTime v tabulke Response	24.7.2019	
9.	Služba pre zrušenie platby pridaná do kapitol: 2.5.3, 2.6.2.3, 2.9.3.2	29.7.2019	
10.	Kapitola 2.9.3.5 - nový status ACCR (zrušenie platby klientom)	29.7.2019	
11.	Nová kapitola 2.9.3.6 (Cancel payment)	29.7.2019	
12.	Kapitole 2.3 – upresnenie textu	30.7.2019	
13.	Kapitola 2.4.2.1 – úprava textu - zrušen popis možnosti vytvorenia súhlasu pre TPP z prostredia IB	16.8.2019	
14.	Zrušenie kapitoly 2.4.3 – správa súhlasu v IB	16.8.2019	
15.	Presunutie kapitoly „Detail ‚Súhlas s prístupom pre tretiu stranu' pod kapitolu 2.4.2"	16.8.2019	
16.	Zrušenie funkcionality „Obnova ukončeného súhlasu" z IB – odstranená kapitola, popisujúci túto funkcionalitu v IB	16.8.2019	
17.	Kapitola 2.9.2.4 – Account Information - pridaná nová položka openDate	16.8.2019	
18.	Kapitola 2.9.2.5.1 – pridaná položka PaymentDate	16.8.2019	
19.	Kapitola 2.5.2, 2.6.2.2, 2.9.2.2 metóda Account List – nepodporovaná služba	2.9.2019	
20.	Kapitola 2.3, 2.4.1 – úprava textu, prístup TPP k účtom disponenta je umožnený iba na základe dokončenia aktivačného workflow – vznikne aktivačný záznam, na základe ktorého môže tretia strana požiadať o vygenerovanie prístupových tokenov.	2.9.2019	
21.	Kapitola 2 – zrušená podmienka kontroly existencie súhlasu	2.9.2019	
22.	Nová kapitola 2.4.3 – správa aktivačného záznamu disponentom	2.9.2019	
23.	Zrušená kapitola 2.9.2.6 – metóda Account List	2.9.2019	
24.	Do metódy /token pridaná voliteľná položka IBAN, pomocou ktorej je TPP pri žiadosti o token umožnené, aby vygenerované tokeny boli použiteľné len so špecifikovanými účtami	11.9.2019	

Dátum: 11.9.2019
Verzia: 2.4

Obsah

1. Úvod

Riešenie API PSD2 je implementované podľa slovenského národného štandardu (ďalej SBAS).

Pre autorizáciu požiadaviek je použitý autentizačný protokol OAuth 2.0 (popis resource používaných v rámci tohto protokolu pozrite kapitolu 2.8).

Pre komunikačné rozhranie API sa používa transportný protokol REST (Representational State Transfer). Pre formát zápisu dát dotazu aj odpovede cez API je použitý JSON (JavaScript Object Notation) (výnimkou je formát dát pre požiadavku typu inicializácia platby, kedy je použitý formát XML).

Komunikácia medzi aplikáciou tretej strany a bankou je zabezpečená pomocou TLS 1.2 protokolu s minimálne 256-bitovým šifrovaním.

Tretia strana bude svoje požiadavky zasielať na vystavené endpointy. Popis jednotlivých metód, ktoré budú pre tretiu stranu k dispozícii, je súčasťou kapitoly 2.9.

1.1 Terminológia

ASPSP - Account Servicing Payment Service Provider – poskytovateľ platobných služieb, v tomto prípade banka.

SBAS – Skratka pre Slovak Banking API Standard.

TPP - Third Party Provider – tretia strana, subjekt, ktorý sprostredkováva služby banky. Tretia strana môže používať maximálne tri nasledujúce typy služieb (AISP, PISP, PIISP).

Consent - Súhlas klienta s poskytovaním služieb cez sprostredkovateľa – TPP.

AISP - Account Information Service Provider – poskytovateľ služby informovania o platobnom účte - na základe dokončenia aktivačného workflow (volanie metódy /Authorize zo strany TPP) klientom poskytuje TPP informácie o platobnom účte a transakciách, ktoré sú vykonané na účte klienta v banke. Napríklad, ak má klient vedené účty vo viacerých bankách, prostredníctvom tretej strany môže vidieť históriu transakcií, prípadne aj zostatky na všetkých týchto účtoch súčasne na jednom mieste (cez aplikáciu alebo portál TPP).

PISP - Payment Initiation Service Provider – poskytovateľ služby nepriameho zadania platobného príkazu - ak má TPP povolenú túto službu, môže:

- iniciovať z účtu klienta platbu,
- potvrdiť (autorizovať) odoslanie platby iniciované treťou stranou do banky na spracovanie (ak predtým klient túto platbu autorizoval)
- pýtať sa na stav platby

PIISP - Payment Instrument Issuer Service Provider – poskytovateľ platobných služieb vydávajúci platobný nástroj (platobnú kartu). TPP si bude môcť overiť, či má klient na bankovom účte, ku ktorému TPP vydala kartu, dostatok prostriedkov na zrealizovanie transakcie kartou. Banka odpovie na otázku TPP odpoveďou ÁNO / NIE.

API Gateway – aplikácia v DMZ banky, ktorá poskytuje prístup k PSD2 službám vystavených bankou pre tretie strany.

Internetbanking - Platforma elektronického bankovníctva, prevádzkovaného v Privatbanke.

PSD2 - Podpora PSD2 funkcionalít (autorizácia TPP pre AISP/PISP/PIISP).

2. Bezpečnostný model

Základný bezpečnostný model pre prístup k API je založený na kombinácii nižšie uvedených bezpečnostných prvkov (aby TPP mohla posielať požiadavky cez API, musia byť splnené všetky tieto bezpečnostné prvky):

- Šifrovaná komunikácia medzi TPP a bankou (Použitie platného certifikátu na strane TPP i banky)
- Registrovaný platný záznam TPP v banke (Internetbankingu)
- Registrovaná aplikácia TPP v banke (s jedinečným client_id a client_secret)
- Platný access token (naviazaný na špecifický aktivačný záznam, vytvorený disponentom na základe dokončenia aktivačného workflow (spusteného zavoláním metódy /authorize zo strany TPP) uvádzaný v hlavičke zaslanej požiadavky cez API

2.1 Šifrovaná komunikácia TPP-Banka

Komunikácia medzi klientskym systémom a bankou predpokladá zabezpečenie pomocou TLS 1.2 protokolu s minimálne 256-bitovým šifrovaním. TPP musí pre vytvorenie zabezpečeného kanála použiť kvalifikovaný certifikát pre autentizáciu webových serverov podľa eIDAS pre PSD2.

2.2 Registrácia TPP v banke

Ak existuje v databáze Internetbankingu platný záznam TPP, musí TPP cez špecifický endpoint vystaveného PSD2 API vykonať registračný proces v banke.

Pri registračnom procese si TPP v banke zaregistruje svoju aplikáciu / Multibank portál (TPP môže prevádzkovať viac aplikácií). Ak TPP ponúka klientom viac svojich aplikácií, musia každú svoju PSD2 aplikáciu zaregistrovať v banke. TPP dostane ku každej zaregistrovanej aplikácii od banky technické identifikátory (client_id, client_secret). Technické identifikátory sa používajú pri autentizačnom procese s použitím OAuth 2.0.

2.3 Aktivácia prístupu TPP k účtom disponenta

Ďalšou podmienkou, ktorá musí byť splnená, aby TPP mohla zasielať požiadavky cez API, je vygenerovanie dvojice prístupových tokenov (access_token a refresh_token). O vygenerovanie tejto dvojice môže tretia strana požiadať až v okamihu, keď klient banky, s ktorým má tretia strana spísanú zmluvu, dokončí aktivačný workflow (aktivačný workflow pre vydanie prístupových tokenov sa vykoná volaním metódy / Authorize, pri ktorom je užívateľ aplikácie / portálu TPP presmerovaný na autorizačnú stránku banky, kde vykoná silnú autorizáciu svojim autentizačným zariadením (pozri kapitolu 2.4.2.1).

Súčasťou vzniknutého záznamu o aktivácii sú položky:

- Aplikácia TPP, z ktorej disponent banky inicioval aktiváciu prístupu na API banky
- Oprávnenie k používaniu metód pre služby AISP, PISP, PIISP. Služba pre PIISP nie je pri aktivácii implicitne povolená. Túto službu musí disponent dodatočne povoliť z prostredia Internetbankingu.

Po dokončení aktivácie (vygenerovaní prístupového tokenu) vznikne v databáze Internetbankingu aktivačný záznam, nad ktorým môže užívateľ, ktorý aktivoval prístup, po svojom prihlásení do Internetbankingu dodatočne povoliť službu PIISP alebo túto povolenú službu môže deaktivovať.

Aktiváciu / deaktiváciu PIISPu musí disponent autorizovať svojím autorizačným zariadením.

2.4 Popis riešenia

2.4.1 Hlavné vlastnosti API

- API rozhranie podporuje všetky mandatórne služby v rámci SBAS a nemandatórnu službu „Account list“
- API rozhranie: bankové API je riešené ako webová služba (WS).
- API rozhranie:

- Pre komunikačné rozhranie API je použitý transportný protokol REST (Representational State Transfer).
- Pre formát zápisu dát dotazu aj odpovede cez API je použitý JSON (JavaScript Object notácie) (výnimkou je formát dát pre požiadavku typu inicializácia platby, kedy sa používa formát XML).

- Evidencia aplikácií TPP: TPP si registruje v banke pri registračnom procese 1 až n aplikácií.
- Požiadavka zaslaná z TPP cez API do banky dostane požadovanú odpoveď iba pri splnení všetkých nasledujúcich podmienok:
  - na základe čísla licencie uvedeného v certifikáte (číslo licencie vrátane prefixu), ktorý TPP používa pri komunikácii, je záznam TPP dohľadaný v banke v zozname TPP - identické číslo licencie musí byť uvedené v certifikáte aj v zázname TPP v banke
  - dohľadaný záznam TPP je platný,
  - typ použitej metódy zodpovedá službe (AISP, PISP, PIISP), ktorá je povolená v dohľadanom zázname TPP
  - access_token použitý v požiadavky je platný
  - na základe použitého access_tokenu (OAuth protokol), uvedeného v požiadavke, je dohľadaný záznam aktivácie, ktorý vznikol na základě dokončenia aktivačného workflow disponentom (aktivačné workflow sa spustí zo strany TPP použitím metódy /authorize)
  - ak je v tele požiadavky uvedený účet, musí na tento účet mať disponent povolený aktívny prístup.
  - aplikácia TPP má v dohľadanom aktivačnom zázname povolenú službu (AISP, PISP, PIISP), ktorá zodpovedá metóde použitej v prijatej požiadavke.

2.4.2 Popis workflow – nastavenie prístupu TPP k účtom disponenta

- TPP zaregistruje svoju aplikáciu v banke (cez API vystavené bankou pre TPP) s použitím špecifických metód (viď. kapitola 2.7).
- V okamihu prijatia požiadavky na registráciu aplikácie TPP cez PSD2 API vystavené bankou, prebehne na strane banky v systéme elektronického bankovníctva overenie TPP. Overenie je vykonávané na základe ID licencie vydanej národným regulátorom a certifikátu daného subjektu (ID licencie uvedenej v certifikáte, ktorý TPP používa pri komunikácii cez PSD2 API vystavenej bankou, musí byť obsiahnuté v zázname TPP v banke).
- V prípade, že ID licencie obsiahnuté v certifikáte použitého pri komunikácii TPP cez API, nie je obsiahnuté v žiadnom zázname TPP v databáze IB, je postup nasledujúci:

- TPP kontaktuje pracovníka banky, ktorý vykoná manuálne overenie (TPP banke odovzdá svoj certifikát (bez tajne časti) s potrebnými dokladmi, na základe ktorých pracovník banky overí a dohľadá danú TPP v databáze IB.
- Po manuálnom overení pracovník banky doplní do databázy IB do záznamu TPP chýbajúce ID licencie (použité v certifikáte TPP).
- Po doplnení ID licencie bankou, TPP vykoná ďalší pokus registrácie svojej aplikácie cez API.

- Pri registrácii aplikácie TPP pre komunikáciu cez API banky sú po overení TPP v elektronickom bankovníctve vygenerované nasledujúce technické bezpečnostné prvky potrebné pri autentizačnom procese s použitím OAuth 2.0:
  - Identifikátor (client_id), ktorý bude TPP pri komunikácii cez API používať
  - secret kód (client_secret), ktorý TPP bude použitý v OAuth protokole pri výmene jednorázového autorizačného kódu za refresh a access token.
- Vygenerované technické bezpečnostné prvky sú odovzdané TPP (TPP tieto technické bezpečnostné prvky dostane pri registrácii cez API ako odpoveď na požiadavku registrácie)

2.4.2.1 Postup ativácie prístupu pre aplikáciu TPP disponentom

Nasledujú kroky, ktoré musí vykonať disponent.

- Disponent klienta banky podpíše zmluvu s TPP.
- Klient banky (užívateľ aplikácie) si nainštaluje aplikáciu TPP alebo pristupuje k portálu TPP.
- Klient banky (užívateľ aplikácie) si v aplikácii / portáli vyberie svoju banku a spustí aktivačný proces.
- Klient je po spustení aktivačného procesu v aplikácii TPP presmerovaný na autentizačný frontend banky (centrálnu autorizačnú stránku) s využitím protokolu OAuth 2.0.
- Klient sa na centrálnej stránke štandardným spôsobom autentizuje (ako v IB).
- **Po autentizácii disponenta sa disponentovi zobrazí stránka s následujúcim obsahom:**
  - Názov spoločnosti TPP,
  - Názov aplikácie TPP, z ktorej disponent vykonáva aktiváciu prístupu
  - Zoznam služieb, ku ktorým môže tretia strana žiadať o vydanie prístupových tokenov (množina služieb vzniknutých prienikom:
    - služieb, ktoré má tretia strana registrované vo svojej licenciu v NBS
    - služieb, ktoré si TPP zaregistrovala v banke pre aplikáciu, cez ktorú disponent vykonáva aktivačný proces)
  - Ak bude mať TPP zaregistrovanú aj službu PIISP, zobrazí se na tejto stránke disponentovi aj text „Službu PIISP (služba pre poskytovateľa platobných služieb vydávajúci platobný prostriedok viazaný na

platobnú kartu) si môžete povoliť priamo v Internet bankingu našej banky v sekcii Nastavenia - Prehľad PSD2 aktivácií.“

- Text: **„Pre dokončenie aktivácie používania služieb cez aplikáciu / portál vyššie uvedenej spoločnosti stlačte tlačidlo "Pokračovať".“**
- Tlačidlo „Pokračovať“.
  - **Pokiaľ užívateľ stlačí tlačidlo "Pokračovať":**
    - je presmerovaný späť do aplikácie TPP a pri presmerovaní v odpovedi v rámci protokolu OAuth TPP získa jednorazový autorizačný kód.
    - TPP následne kontaktuje endpoint token vystavený na frontende banky, aby tento jednorazový autorizačný kód vymenil za dvojicu tokenov access a refresh token.
    - Aplikácia TPP následne Access token používa pri komunikácii s PSD2 API vystavený bankou. Vnútrobankové systémy následne budú žiadať o overenie platnosti tokenu a príslušnej služby (AIS / PIS / PIIS), pre ktorú bol token vystavený a príslušnej užívateľskej identity, ku ktorej token patrí.

2.4.3 Internet Banking

2.4.3.1 Prehľad „Prehľad aktivácií“

Ak používateľ vyberie v sekci „Nastavenia“ ponuku "Prehľad PSD2 aktivácií", zobrazí sa prehľad všetkých aktivačných záznamov, ktoré vznikli na základe dokončenia workflow aktivácie, ktorá bola vyvolaná metodou /Authorize zo strany TPP.

Štruktúra prehľadu - prehľad obsahuje nasledujúce stĺpce:

Názov stĺpca	Popis
Tretia strana	Názov tretej strany, pre ktorú disponent dokončil aktiváciu
Aplikácia tretej strany	Názov aplikácie tretej strany, pre ktorú disponent aktivoval prístup

Na konci každého zobrazeného riadku je grafický prvok, pomocou ktorého si užívateľ IB otvorí detail aktivácie.

2.4.3.2 Detail „Aktivácia prístupu pre tretiu stranu“

Názov položky	Popis
PIISP aktivované	Informácie, či k danej aktivácii existuje dodatočný súhlas vytvorený disponentom s používaním služby PIISP pre aplikáciu, cez ktorú bola vykonávaná aktivácia prístupu TPP cez PSD2 API. Implicitne tu bude zobrazená hodnota "Nie". Po autorizácii súhlasu so službou PIISP tu bude uvedená hodnota "Áno".
Ovládacie prvky	viď kapitolu 2.4.3.2.1

2.4.3.2.1 Ovládacie prvky v detaile záznamu o aktivácii

V detaile **záznamu o aktivácii** sa užívateľovi ponúkajú tlačidlá:

Tlačidlo	Popis
Aktivovať PIISP	Tlačidlo sa zobrazí iba v prípade, ak tretia strana má registrovanú službu PIISP a disponent túto službu zatiaľ v aktivačnom zázname nepovolil. Po stlačení tlačidla sa vytvorí nová žiadosť o aktiváciu služby PIISP pre danú aplikáciu TPP Disponent žiadosť o aktiváciu súhlasu používať PIISP autorizuje svojim autorizačným zariadením.
Deaktivovať PIISP	Tlačidlo sa zobrazí iba v prípade, ak tretia strana má registrovanú službu PIISP a disponent túto službu v aktivačnom zázname povolil. Po stlačení tlačidla sa vytvorí nová žiadosť o deaktiváciu služby PIISP pre danú aplikáciu TPP Disponent žiadosť o deaktiváciu súhlasu používať službu PIISP autorizuje svojim autorizačným zariadením.
Zneplatnenie tokenov	Toto tlačidlo sa bude užívateľovi ponúkať iba v prípade, ak bude v aktivačnom zázname existovať platný access_token alebo refresh_token. Použitie tohto tlačidla užívateľom plne nahradzuje metódu pre revokáciu (zneplatnenie) platného tokenu, ktorá je súčasťou autorizačného protokolu OAuth2. Po zneplatnení tokenov (access_token a refresh_token) môže klient prostredníctvom aplikácie / portálu TPP zažiadať o novú autorizačnú požiadavku (/authorize), na základe ktorej je z aplikácie / portálu TPP presmerovaný na centrálnu autentizačnú stránku banky pre vykonanie svojej identifikácie a autentizácie užívateľa (klienta banky). Po úspešnej autentizácii banka vygeneruje nový autorizačný kód (code), ktorý TPP získa z odpovede požiadavky autorizácie. Na základe tohto autorizačného kódu TPP môže požiadať o vygenerovanie novej dvojice prístupových tokenov.

2.5 Služby podporované v API PSD2

- riešenie PSD2 umožňuje tretej strane používať cez WS služby PSD2 popísané v nasledujúcich podkapitolách.

2.5.1 Metódy pre automatickú registráciu aplikácie TPP cez API

Metóda služby	Popis
Registrácia aplikácie TPP (JSON)	prostredníctvom tejto služby TPP s platným certifikátom a licenčným číslom vykoná automatickú registráciu svojej aplikácie v banke a v odpovedi dostane k registrovanej aplikácii technické bezpečnostné prvky (client_id a client_secret)

Zmena registrácie aplikácie (JSON)	prostredníctvom tejto služby bude TPP môcť vykonať zmenu registračných údajov
Zrušenie registrácie aplikácie (JSON)	prostredníctvom tejto služby bude TPP môcť zrušiť registráciu aplikácie
Žiadosť o vygenerovanie nového client_secret	Prostredníctvom tejto služby bude TPP moci požiadať o vygenerovanie nového client_secret

2.5.2 Metódy oblasti AISP

Metóda služby	Popis
Account information (JSON)	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad zostatkov bankového účtu disponenta vedeného v banke
Account transactions (JSON)	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad transakcií
Accounts List (JSON)	služba na požiadavku vráti zoznam účtov bez zostatkov Nepodporovaná metóda

2.5.3 Metódy oblasti PISP

Metóda služby	Popis
Standard payment initialization (XML)	prostredníctvom tejto služby disponentom autorizovaná tretia strana iniciuje (vytvorí) jeden SEPA príkaz z bankového účtu disponenta vo formáte XML (PAIN.001). TPP následne použije na iniciovaný príkaz službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu daný príkaz autorizuje svojim autentizačným zariadením.
Payment status (JSON)	zisťovanie stavu platobného príkazu
Standard payment submission (JSON)	autorizácia platby treťou stranou, (daná platba musí byť iniciovaná touto treťou stranou)
Balance check (JSON)	overenie dostatočného zostatku na účte
Cancel payment (JSON)	zrušenie platby, ktorá ešte nebola autorizovaná treťou stranou (tretia strana nepoužila metódu "Standard payment submission") a ktorá bola vytvorená prostredníctvom služby PISP Standard payment initialization (XML)

2.5.4 Metódy oblasti PIISP

Metóda služby	Popis
Balance check (JSON)	overenie dostatočného zostatku na účte

2.6 Endpointy použité pre API PSD2

2.6.1 Endpointy pre OAuth (autorizácia klienta, autorizácia platby klientom, vydávanie tokenov)

Endpoint	Typ metódy	Popis
https://api.privatbanka.sk/auth/oauth/authorize	GET	Endpoint používaný v rámci Oauth **Authorization code grant pre:** - **autorizáciu klienta,** - **autorizáciu platby klientom**.
https://api.privatbanka.sk/auth/oauth/token	POST	Endpoint používaný v rámci Oauth **Authorization code grant pre:** - **vygenerovanie novej dvojice access_token a refresh_token** - **obnovenie access tokenu** - **vygenerovanie jednorazového access tokenu pre použitie v metóde /api/v1/payment/submission**

2.6.2 Endpointy pre PSD2 API (registračné resource (Enrollment), volanie metód AISP, PISP, PIISP)

2.6.2.1 Enrollment (registrácia aplikácie v banke)

Endpoint	Typ metody	Popis
https://api.privatbanka.sk/**api/enroll**	POST	Endpoint pre metódu, prostredníctvom ktorej TPP s platným certifikátom a licenčným číslom vykoná automatickú registráciu svojej aplikácie v banke a v odpovedi dostane k registrované aplikácii technické bezpečnostné prvky (client_id a client_secret).
https://api.privatbanka.sk/**api/enroll/{client_id}**	PUT	Zavolaním tohto resource môže TPP požiadať o zmenu registračných údajov pre konkrétnu aplikáciu.
https://api.privatbanka.sk/**api/enroll/{client_id}**	DELETE	Zavolaním tohto resource môže TPP požiadať o zmazanie registrácie konkrétnej aplikácie.
https://api.privatbanka.sk/**api/enroll/{client_id}/renewSecret**	POST	Zavolaním tohto resource môže TPP požiadať o vydanie nového client_secret k danej aplikáci.

2.6.2.2 AISP

Endpoint	Typ metódy	Popis
https://api.privatbanka.sk/**api/v1/accounts/information**	POST	Endpoint pre metódu, prostredníctvom ktorej dostane disponentom autorizovaná tretia strana prehľad zostatkov bankového účtu disponenta vedeného v danej banke
https://api.privatbanka.sk/**api/v1/accounts/transactions**	POST	Endpoint pre metódu, prostredníctvom ktorej dostane disponentom autorizovaná tretia strana prehľad transakcií
https://api.privatbanka.sk/**api/v2/accounts**	GET	Nepodporovaná metóda

2.6.2.3 PISP

Endpoint	Typ metódy	Popis
https://api.privatbanka.sk/**api/v1/payments/standard/iso**	POST	Endpoint pre metódu **Standard payment initialization (XML)** - disponentom autorizovaná tretia strana iniciuje (vytvorí) jeden SEPA príkaz z bankového účtu disponenta.
https://api.privatbanka.sk/**api/v1/payments/submission**	POST	Endpoint pre metódu **Standard payment submission –** autorizácia platby tretou stranou (platbu predtým musí povoliť svojou autorizáciou disponent).
https://api.privatbanka.sk/**api/v1/payments/{orderId}/status**	GET	Endpoint pre metódu **Payment order status –** zisťovanie stavu platobného príkazu
https://api.privatbanka.sk/**api/v1/payments/{orderId}/rcp**	DELETE	Endpoint pre metódu **Cancel payment –** zrušenie platby, ktorá ešte nebola autorizovaná treťou stranou (tretia strana nepoužila metódu "Standard payment submission") a ktorá bola vytvorená prostredníctvom služby PISP Standard payment initialization (XML)
https://api.privatbanka.sk/**api/v1/accounts/balanceCheck**	POST	Endpoint pre metódu **Balance check** - overenie, či má klient na bankovom účte dostatok prostriedkov na zrealizovanie transakcie

2.6.2.4 PIISP

Endpoint	Typ metódy	Popis
https://api.privatbanka.sk/**api/v1/accounts/balanceCheck**	POST	Endpoint pre metódu **Balance check** - overenie, či má klient na bankovom účte, ku ktorému TPP vydala kartu, dostatok prostriedkov k zrealizovaniu transakcie kartou

2.7 Registračné resource vystavenej bankou (Enrollment)

Nasledujúce kapitoly popisujú metódy, pomocou ktorých TPP žiada o registráciu svojej aplikácie v banke, prípadne môže vykonať zmeny alebo zrušenia registrácie svojej aplikácie.

2.7.1 Automatické generovanie technických identifikátorov

Pre zavolanie resource je potreba:

- **Použiť platný certifikát**

Výstupom sú parametre client_id a client_secret, ktoré TPP potrebuje pre následné získanie dvojice tokenov access_token a refresh_token.

Endpoint: POST https://api.privatbanka.sk/api**/enroll**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
redirect_uris	Áno	Array of strings e.g. URL [Max 3x 2047 B]	Zoznam URL kam môže byť proces autentizácie na konci presmerovaný. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
logo_uri	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. Miesto odkiaľ je možné ho pri registrácii stiahnuť)
contacts	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
scopes	Nie	Array of strings [Max 10x 255 B]	Pole požadovaných Scopes pre aplikáciu. Pri registrácii sú Scopes validované proti obsahu použitého certifikátu a proti Scopes uvedených v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.
licence_number	Áno	String [Max 1024 B]	Licenčné číslo, ktoré má TPP pridelené od národného regulátora. Licenčné číslo je validované proti licenčnému číslu uvedenému v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Response			
Atribut	**Povinný**	**Typ**	**Popis**
client_id	Áno	String	client_id priradené aplikácii. Toto ID je používané pri spustení autentizačného procesu a pri komunikačnom procese (výmene jednorazového code za dvojicu tokenov access_token a refresh_token a pri obnovení tokenu).
client_secret	Áno	String	Client_secret - password / token vydaný bankou (ASPSP) pre TPP aplikáciu (client_id)
client_secret_expires_at	Nie	DateTime	Defaultná hodnota je 0 (client_secret nikdy neexspiruje). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z
api_key	Nie	String	API kľúč, ktorý aplikácia používa pri komunikácii s API banky. **API kľúč nie je v tomto riešení bankou podporovaný** (v odpovedi v položke uvedené "NOT_PROVIDED")
redirect_uris	Áno	Array of strings e.g. URL [Max 3x 2047 B]	Zoznam URL kam môže byť proces autentizácie na konci presmerovaný. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
logo_uri	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. miesto, odkiaľ je možné ho pri registrácii stiahnuť)
contacts	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
scopes	Nie	Array of strings [Max 10x 255 B]	Pole požadovaných služieb (Scopes pre aplikáciu. Pri registrácii sú služby validované proti obsahu použitého certifikátu a proti službám uvedených v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.
licence_number	Áno	String [Max 1024 B]	Licenčné číslo, ktoré má TPP pridelené od národného regulátora. Licenčné číslo je validované proti licenčnému číslu uvedenému v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**invalid_request**	Nevalidný request. V požiadavke chýba povinné pole alebo je v nevhodnom / nevalidnom formáte.
400	**invalid_scope**	Nevalidný scope v požiadavke.
400	**invalid_redirect_uri**	Hodnota jedného alebo viacerých redirect uri nie je validná
401	**invalid_client**	Nevalidný client_id.
401	**unauthorized_client**	TPP nie je oprávnený vykonávať túto požiadavku.
401	**access_denied**	Autorizačný server odmietol prístup.
403	**insufficient_scope**	Napr. nedostatočné oprávnenia pre použitie požadovanej služby
500, 503	**server_error**	Chyba autorizačného servera.

Príklad použitia viac zdroj [8] kapitola 4.5.1.

2.7.2 Zmena registračných údajov

Zavolaním tohto resource môže TPP požiadať o zmenu registračných údajov pre konkrétnu aplikáciu.

Pre zavolanie resource je potreba:

- Použiť platný certifikát

- Použiť client_id, vydané k tomuto TPP.

Výstupom je prehľad zmenených údajov.

Endpoint: PUT https://api.privatbanka.sk/api**/enroll/{client_id}**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
redirect_uris	Áno	Array of strings e.g. URL [Max 3x 2047 B]	Zoznam URL kam môže byť proces autentizácie na konci presmerovaný. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
logo_uri	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. miesto, odkiaľ je možné ho pri registrácii stiahnuť)
contacts	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
scopes	Nie	Array of strings [Max 10x 255 B]	Pole požadovaných Scopes pre aplikáciu. Pri registrácii sú Scopes validované proti obsahu použitého certifikátu a proti Scopes uvedených v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Response			
Atribut	**Povinný**	**Typ**	**Popis**
client_id	Áno	String	client_id priradené aplikácii bankou.
client_secret_expires_at	Nie	DateTime	Defaultná hodnota je 0 (client_id nikdy neexspirujú). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z
redirect_uris	Áno	Array of strings e.g. URL [Max 3x 2047 B]	Zoznam URL kam môže byť flow autentizácie na konci presmerované. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidental.
logo_uri	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. Miesto odkiaľ je možné ho pri registrácii stiahnuť)
contacts	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
scopes	Nie	Array of strings [Max 10x 255 B]	Pole požadovaných služieb (Scopes pre aplikáciu. Pri registrácii sú služby validované proti obsahu použitého certifikátu a proti službám uvedených v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**invalid_request**	Nevalidný request. V požiadavke chýba povinné pole alebo je v nevhodnom / nevalidnom formáte.
400	**invalid_scope**	Nevalidný scope v požiadavke.
400	**invalid_redirect_uri**	Hodnota jedného alebo viacerých redirect uri nie je validná
401	**invalid_client**	Nevalidný client_id.
401	**unauthorized_client**	TPP nie je oprávnený vykonávať túto požiadavku.
401	**access_denied**	Autorizačný server odmietol prístup.
403	**insufficient_scope**	Napr. nedostatočné oprávnenia pre použitie požadovanej služby.
500, 503	**server_error**	Chyba autorizačného servera.

Príklad použitia viac zdroj [8] kapitola 4.5.2.

2.7.3 Zmazanie aplikácie

Zavolaním tohto resource môže TPP požiadať o zmazanie údajov a prístupu konkrétnu aplikáciu.

Pre zavolanie resource je potreba:

- Použiť platný certifikát

- Použiť platné client_id, ktoré je vydané tomuto TPP.

Výstupom je potvrdenie o zmazanie.

Endpoint: DELETE https://api.privatbanka.sk/api**/enroll/{client_id}**

Ak sa zmazanie aplikácia vykoná, je vrátená odpoveď HTTP 204 ako úspešná odozva na zmazanie záznamu aplikácie s konkrétnym client_id).

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**invalid_request**	Nevalidný request. V požiadavke chýba povinné pole alebo je v nevhodnom / nevalidnom formáte.
401	**invalid_client**	Nevalidný client_id.
401	**unauthorized_client**	TPP nie je oprávnený vykonávať túto požiadavku.
401	**access_denied**	Autorizačný server odmietol prístup.
500, 503	**server_error**	Chyba autorizačného servera.

Príklad použitia viac zdroj [8] kapitola 4.5.3.

2.7.4 Žiadosť o nový client_secret

Zavolaním tohto resource môže TPP požiadať o vydanie nového client_secret.

Pre zavolanie resource je potreba použiť:

- Platný certifikát

- Platný client_id, ktoré je vydané tomuto TPP.

Pôvodný client_secret bude touto požiadavkou zrušený.

Endpoint: POST https://api.privatbanka.sk/api**/enroll/{client_id}/renewSecret**

Response			
Atribut	**Povinný**	**Typ**	**Popis**
client_id	Áno	String	client_id priradené aplikácii.
client_secret	Áno	String	Client_secret - password / token vydaný bankou (ASPSP) pre TPP aplikáciu (client_id)
client_secret_expires_at	Nie	DateTime	Defaultná hodnota je 0 (client_id nikdy neexspirujú). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**invalid_request**	Nevalidný request. V požiadavke chýba povinné pole alebo je v nevhodnom / nevalidnom formáte.
401	**invalid_client**	Nevalidný client_id.
401	**unauthorized_client**	TPP nie je oprávnený vykonávať túto požiadavku.
401	**access_denied**	Autorizačný server odmietol prístup.
500, 503	**server_error**	Chyba autorizačného servera.

Príklad použitia viac zdroj [8] kapitola 4.5.4.

2.8 Autentizácia a Autorizácia requestu (OAuth2)

Autorizácia requestu je založená na autorizačnom procese konceptu OAuth2 zabezpečeného tokenom - aplikácia len skontroluje platnosť tokenu použitého v hlavičke požiadavky, ktorý TPP poskytuje pre každé volanie ako dôkaz, že môže pristupovať k požadovaným údajom.
V rámci API je autorizačný token považovaný za krátkodobý a bezstavový prvok, ktorý musí byť použitý v každom volaní API, ktoré požaduje autorizáciu requestu.

Základom riešenia je použitie OAuth2 otvoreného protokolu pre vystavovanie autorizačných tokenov – **je podporovaný iba autorizačný framework Authorization code grant**.

2.8.1 OAuth2 Authorization Code Grant

V rámci protokolu OAuth2 sa v prípade autorizačného frameworku Authorization code grant jedná o spôsob, ako partnerskej aplikácii vydať refresh token aj access token ako výsledok identifikácie a autentizácie užívateľa. Krátkodobý access token partnerská aplikácia používa pre komunikáciu s API banky a po jeho expirácii môže použiť refresh token pre vyžiadanie nového access tokenu.

2.8.1.1 Základné vlastnosti

- Access token je vydávaný ako krátkodobý (3600 s)
- Access token je vydávaný pre konkrétnu aplikáciu a konkrétneho užívateľa, pre inú aplikáciu a užívateľa ho nie je možné úspešne použiť
- Refresh token nie je možné priamo použiť pre komunikáciu s API, má dlhú platnosť (v prípade PSD2 90 dní)
- v metóde /token (žiadosť o token / obnova tokenu) je tretej strane umožnené na základe voliteľnej položky IBAN používať vygenerované tokeny iba k špecifickému účtu (množine účtov) daného disponenta
- Banka a TPP aplikácia spolu zdieľa spoločné "tajomstvo" (client secret)
- Výsledkom identifikácie a autentizácie užívateľa je jednorazový kód, ktorý aplikácia tretej strany môže s použitím **client_id** a **client secret** vymeniť za refresh token a access token

- Samotný jednorázový kód bez znalosti client secret nie je možné použiť

2.8.1.2 Popis Code grand flow

Podmienky použitia flow:

- Aplikácia TPP má od banky pridelené vlastné jedinečné client_id a TPP backend server pozná pre dané client_id aj client secret
- Pri vydaní client_id a client_secret banka získa informáciu o redirect uri - teda o URL, kam má presmerovať užívateľa po úspešnej autentifikácii

Jednotlivé kroky code grant flow:

1. TPP zavolá resource banky /Authorize a následne je užívateľ (klient banky) presmerovaný na centrálnu autentizačnú stránku pre vykonanie identifikácie a autentizácie užívateľa (klienta banky).
2. Prebieha identifikácia a autentizácia klienta - tieto kroky sú plne v réžii banky
3. Po úspešnej autentizácii banka vygeneruje code a presmeruje s ním používateľa na URI, ktoré bolo súčasťou požiadavky /Authorize (redirect_uri)
4. TPP použije resource /token na získanie refresh_tokenu a access_tokenu. Pri volaní tohto zdroja TPP použije:
   - v hlavičke v položke Authorization dvojicu client_id a client_secret, ktorá však musí byť zašifrovaná pomocou Base64 (formát použitého reťazca: Basic <hodnota vygenerovaná pomocou Base64 (client_id:client_secret)>)
   - a v tele požiadavky hodnotu code, ktorý dostala v odpovedi predchádzajúcej požiadavky / Authorize.
5. Aplikácia TPP používa pri komunikácii na API banky v prípadoch, keď je to potrebné, v hlavičke požiadavky, získaný access_token
6. Banka interne vykonáva overovanie access_tokenu. Pri tomto overení získava identitu používateľa, na základe ktorého autentizácie bol access token vydaný.

2.8.1.3 Autorizačný resource

Ak neexistuje platná dvojica tokenov (access_token a refresh_token), musí TPP vytvoriť Autorizačnú požiadavku, na základe ktorej je klient banky z aplikácie presmerovaný na centrálnu autentizačnú stránku banky, kde danú požiadavku následne autorizuje. Požiadavka je typu **OAuth 2.0 Authorization Code Grant s PKCE rozšírením**.

Endpoint: GET https://api.privatbanka.sk/auth/oauth**/authorize**

Request			
Atribut	**Povinný**	**Typ / hodnota**	**Popis**
response_type	Áno	**code**	Povinný parameter. Hodnotou parametra je určené, aký typ autentizačného flow je požadovaný. V tomto prípade sa jedná o code grant. Pre autentizačný proces to znamená, že výsledkom tejto požiadavky bude jednorazový auth_code, ktorý TPP následne pomocou ďalšej požiadavky (metódou token) zamení za dvojicu tokenov access_token a refresh_token
client_id	Áno	String	Jedinečný identifikátor, ktorý banka vygenerovala pre aplikáciu TPP
redirect_uri	Áno	URL	URL kam je na konci presmerované flow autentizácie. Toto URL je stanovené už pri vydaní client_id a v rámci autentizácia je tento parameter validovaný proti URL zavedenému k client_id v zázname aplikácie registrovanej v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrovanej aplikácie.
Scope	Áno	String	Jedná sa o pole aplikácií požadovaných scope (oprávnenie). V prípade PSD2 to môžu byť role AISP, PISP, PIISP. Napr. ak je TPP držiteľom viac oprávnenia, môže tu pre svoju aplikáciu požiadať len o jedno z nich alebo viac. Ak je použitých viac typov scope, sú oddelené medzerou.
state	Áno	Libovolný string [min 128 bits]	Parametrom sa zvyšuje bezpečnosť komunikácie pri presmerovaní. Chráni pred útokmi CSRF a odovzdáva informácie z aplikácie prostredníctvom toku autentizácie.
code_challenge	Áno	String	code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier))) viz. zdroj [3] RFC 7636 (OAuth PKCE)
code_challenge_method	Áno	String	S256

Response			
Atribut	**Povinný**	**Typ**	**Popis**
Code	Áno	String	Jednorazový autorizačný kód
State	Áno	String	Hodnota atribútu odovzdaného z TPP požiadavky

Chybové kódy

- Chybové kódy sú definovány podľa [1] RFC 6749, kapitola 4.1.2.1

Príklad použitia viac zdroj [8] kapitola 5.2.2.

2.8.1.4 Získanie tokenov

Ak TPP na základe odpovede požiadavky /Authorize dostane autorizačný kód (code) a string uvedený v položke state je validný (hodnota state je v odpovedi zhodná s hodnotou state, ktorá bola uvedená v požiadavke), môže TPP požiadať o prístupové tokeny z ASPSP pomocou autorizačného kódu. TPP zašle spoločne s týmto autorizačným kódom (ktorý musí byť uvedený v tele požiadavky) aj client_id a client_secret (ktoré však musí byť uvedené v hlavičke požiadavky zakódované pomocou Base64).

Ak je pri volaní požiadavke /token vyplnená aj dobrovoľná položka IBAN, je používanie tokenov obmedzené iba na tieto vyšpecifikované účty.

Endpoint: POST https://api.privatbanka.sk/auth/oauth/**token**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
code	Áno	string	Autorizačný code navrátený z autentizačného flow (code grant)
redirect_uri	Áno	URL	URL redirect zhodné s URL doručenom v autentizačnom requestu
grant_type	Áno	**authorization_code**	Existujúca definícia / zvyklosti OAuth2 bude táto hodnota authorization_code, ak dochádza k výmene code za dvojicu tokenov access_token a refresh_token.
code_verifier	Áno	String	code_verifier slúži na generovanie code_challenge z predchádzajúcej žiadosti o minimálnej dĺžke 43 znakov a maximálnou dĺžkou 128 znakov
Iban	Nie	String	IBAN účtu, pre ktorý môže byť vygenerovaný token používaný. V prípade zadania viacerých IBAN je nutné ako oddeľovač použiť čiarku.

Response			
Atribut	**Povinný**	**Typ**	**Popis**
access_token	Áno	string	Krátkodobý (v niektorých prípadoch jednorazový) token (platnosť tokenu je 3600s), ktorý je možné znovu vygenerovať použitím refresh_tokenu. Tento token slúži na autorizáciu requestu na API.
expires_in	Áno	number	Zostávajúci čas do expirácie access_tokenu - v sekundách.
refresh_token	Áno	String	Dlhodobý token (platnosť 90 dní) vydaný na základe výmeny za jednorazový **code**.
token_type	Áno	String	Typ tokenu “Bearer”
scope	Nie	String	Zoznam Scope oddelených medzerou, pre ktorých je token vydaný.

Chybové kódy

- Chybové kódy sú definované podľa [1] RFC 6749, kapitola 5.2

Príklad použitia viac zdroj [8] kapitola 5.2.3.

2.8.1.5 Obnovenie Access tokenu

TPP môže po expirácii access_tokenu prostredníctvom refresh tokenu požiadať o nový. Preto je možné použiť resource "Získanie tokenov" s nižšie uvedenými parametrami. TPP zašle spoločne s refresh_token (ktorý musí byť

uvedený v tele požiadavky) aj client_id a client_secret (ktoré však musí byť uvedené v hlavičke požiadavke zakódované pomocou Base64).

Voliteľná položka IBAN je pri obnovení Access tokenu ignorovaná.

V odpovedi sa TPP vráti nový access_token, ktorý bude mať platnosť 3600 sekúnd. Súčasťou odpovede je aj refresh_token, ktorý bol použitý pre obnovenie access_tokenu (vygenerovanie nového access_tokenu). Platnosť refresh_tokenu sa obnovením acces_tokenu nijako nemení - od okamihu, kedy je refresh_token vytvorený (okamih, kedy vznikne prvá platná dvojica access_token a refresh token) je platnosť refresh_tokenu 90 dní. Po uplynutí 90 dní prestane refresh_token platiť a TPP nemôže žiadať o obnovenie prístupového tokenu (access_tokenu).

Endpoint: POST https://api.privatbanka.sk/auth/oauth/**token**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
grant_type	Ano	**refresh_token**	Existujúca definícia / zvyklosti OAuth2 bude táto hodnota refresh_token, ak dochádza k obnoveniu access_tokenu na základe refresh_token.
refresh_token	Ano	String	Validný **refresh_token**
scope	Ano	String	Rozsah scope o prístup. Ak sa používa rozsah, je skontrolovaný proti scope uvádzaným v zázname TPP, aplikácie TPP a zázname aktivácie, ktorý vznikol na základe dokončenia workflow aktivácie (/Authorize) užívateľom aplikácie.
Iban	Nie	String	IBAN účtu, pre ktorý môže byť vygenerovaný token používaný. V prípade zadania viacerých IBAN je nutné ako oddeľovač použiť čiarku. V tejto metóde je parameter IBAN ignorovaný.

Response			
Atribut	**Povinný**	**Typ**	**Popis**
access_token	Ano	string	Krátkodobý (v niektorých prípadoch jednorázový token) token (platnosť tokenu je 3600s), ktorý je možné znovu vygenerovať použitím refresh_tokenu. Tento token slúži na autorizáciu requestu na API.
token_type	Ano	String	Typ tokenu “Bearer”
expires_in	Ano	number	Zostávajúci čas do expirácie access_tokenu - v sekundách.
refresh_token	Ano	String	Refresh_token, na základe ktorého prebehlo obnovenie access_tokenu (jedná se o identický refresh_token, ktorý bol použitý v tomto requeste).

Chybové kódy

- Chybové kódy sú definované podľa [1] RFC 6749, kapitola 5.2

Príklad použitia viac zdroj [8] kapitola 5.2.4.

2.9 Popis metód používaných pre poskytovateľov služieb (TPP)

2.9.1 Všeobecná definícia hlavičiek

Štruktúra hlavičiek uvedených v tejto kapitole sa používa u všetkých nižšie uvedených metód služieb pre AISP, PISP, PIISP.

Hlavička pre Request

Attribute	Mandatory	Typ	Popis
Host	Ano	String	Doménové meno servera a číslo portu
Content-Type	Ano	String	application/json alebo application/xml
Authorization	Ano	String	Typ autorizácie definovaný podľa RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage
Request-ID	Ano	String	Jedinečný identifikátor konkrétnej požiadavky. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).
Correlation-ID	Ne	String	Jedinečný korelačný identifikátor, možno ho použiť ako kontrolu prepojenie požiadavky a odpovede. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).
Process-ID	Ne	String	Identifikátor obchodného alebo technického procesu, na základe ktorého možno párovať sadu dvojíc požiadaviek a odpovedí. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).
PSU–IP-Address	Ano	String	IP adresa zákazníka (disponenta banky), z ktorej je pripojený k infraštruktúre TPP.
PSU-Device-OS	Ano	String	Identifikácia zariadenia zákazníka (disponenta banky), alebo operačného systému, z ktorého je pripojený k infraštruktúre TPP
PSU-User-Agent	Ano	String	Identifikácia webového prehliadača zákazníka alebo identifikácia klientskeho zariadenia, z ktorého je pripojený k infraštruktúre TPP
PSU-Geo-Location	Ne	String	Súradnice GPS aktuálnej polohy zákazníka v okamihu pripojenia k infraštruktúre TPP. (Požadovaný formát GPS: zemepisná šírka, zemepisná dĺžka)
PSU-Last-Logged-Time	Ne	DateTime	Dátum a čas, kedy bol používateľ prihlásený k aplikácii TPP (formát RFC3339)
PSU-Presence	Ne	Enum	Stav prítomnosti používateľa (PSU) počas volania na API. Hodnota parametra môže byť "true" (PSU je prítomný) alebo "false" (PSU nie je prítomný).

Hlavička pre Response

Attribute	Mandatory	Typ	Popis
Content-Type	Ano	String	application/json nebo application/xml
Response-ID	Ano	String	Jedinečný identifikátor konkrétnej odpovede. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).
Correlation-ID	Ne	String	Jedinečný korelačný identifikátor, možno ho použiť ako kontrolu prepojenia požiadavky a odpovede. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).
Process-ID	Ne	String	Identifikátor obchodného alebo technického procesu, na základe ktorého možno párovať sadu dvojíc požiadaviek a odpovedí. Odporúča sa použiť formulár UUID (Universally Unique Ifentifier) verzie 4 (RFC4122).

2.9.2 Služby AISP (Dotazy k účtom, prehľad transakcií)

Kapitola definuje zoznam metód poskytovaných pre AISP.

2.9.2.1 Predpoklady pre používanie metód API pre AISP

a/ záznam TPP je na základe licenčného čísla (vrátane použitého prefixu) uvedeného v certifikáte, ktorý TPP používa pri komunikácii, nájdený v databáze IB

b/ nájdený záznam TPP je platný,

c/ TPP má vo svojom zázname povolenú službu AISP (táto informácia je súčasťou záznamu TPP v databáze IB, ktorý sa automaticky aktualizuje z NBS)

d/ registrovaná aplikácia TPP má povolenú službu AISP

e/ v certifikáte, ktorý používa TPP pri komunikácii je uvedená služba AISP

f/ TPP použil v hlavičke požiadavky access_token, na základe ktorého je na strane banky dohľadaný záznam aktivácie, ktorý vznikol na základe aktivačného workflow dokončeného disponentom.

g/ aplikácia TPP má v nájdenom aktivačnom zázname, ktorý vznikol na základe aktivačného workflow dokončeného disponentom, uloženú službu AISP

2.9.2.2 Zoznam metód používaných pre AISP

Endpoint	Metoda	Popis
/api/v1/**accounts/information**	POST	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad zostatkov bankového účtu disponenta vedeného v danej banke
/api/v1/**accounts/transactions**	POST	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad transakcií
/api/v2/accounts	GET	nepodporovaná metóda

2.9.2.3 Token pre AISP operácie

Pre AISP operácie bude používaný access_token získaný na základe autorizačného resource Authorization Code Grant s PKCE rozšírením popísaného v kapitole 2.8.1 alebo prípadne pozri [1], kapitola 4.1.

2.9.2.4 AISP operácia: Account Information

Endpoint: POST https://api.privatbanka.sk/api**/v1/accounts/information**

Request

Metoda: accounts/information			
Názov atribútu	Formát	Povinný	Poznámka
iban	String (34)	Áno	IBAN účtu disponenta.

Response

Metoda: accounts/information				
Názov atribútu		Formát	Povinný	Poznámka
account	BaseCurrency	String (3)	Áno	Mena účtu (kód meny podľa ISO 4217 - 3 veľké písmená)
	Name	string	Áno	Názov účtu (meno klienta)
	ProductName	string	Nie	Názov produktu
	Type	enum	Nie	Skratka typu účtu podľa normy ISO 20022 - Cash Account Type Code – napr . • CACC - bežný účet
	openDate	dateTime	Nie	Dátum otvorenia účtu (nová položka, ktorá nie je súčasťou SBAS)
Balances		typ:ArrayOfAccountsInformationResponseBalance	Áno	Pole zostatkov

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

Príklad použitia viac zdroj [8] kapitola 5.2.5.

2.9.2.4.1 Definícia typu ArrayOfAccountsInformationResponseBalance

Metóda: accounts/information - typ: ArrayOfAccountsInformationResponseBalance				
Názov atribútu		Formát	Povinný	Poznámka
amount	value	decimal (2 desatinné miesta)	Áno	Hodnota zostatku
	currency	String (3)	Áno	Kód meny zostatku podľa ISO 4217 - 3 veľké písmená

creditDebitIndicator		enum	Áno	Skratka Indikátoru Kredit / Debet • CRDT (Kredit) • DBIT (Debet)
dateTime		dateTime	Áno	Dátum aktualizácie zostatku
typeCodeOrProprietary		enum	Áno	Typ zostatku • CLBD (aktuálny zostatok) • ITAV (disponibilný zostatok) • ITBD (vlastné prostriedky)

2.9.2.5 AISP operácia: Account Transactions

Prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad transakcií uskutočnených na bankovom účte zákazníka v rámci zadaného termínu. História transakcií zahŕňa iba transakcie, ktoré ovplyvňujú zostatok (rezervácie, zaúčtované transakcie). Transakcie sú zoradené od najnovšej po najstaršiu.

Endpoint: POST https://api.privatbanka.sk/api/**v1/accounts/transactions**

Request

Metóda: accounts/transactions			
Názov atribútu	Formát	Povinný	Poznámka
iban	String (34)	Áno	IBAN účtu.
dateFrom	dateTime	Nie	Dátum začiatku obdobia pre históriu transakcií. Predvolená hodnota je aktuálny deň
dateTo	dateTime	Nie	Dátum konca obdobia pre históriu transakcií. Predvolená hodnota je aktuálny deň
page	integer	Nie	Poradové číslo stránky vzhľadom na veľkosť stránky pre záznamovú sadu. Predvolená hodnota je 0 (prvá stránka).
pageSize	integer	Nie	Počet záznamov zahrnutých na jednej stránke pre zobrazenie. Predvolená hodnota je 50 záznamov. Maximálna povolená hodnota je 200 záznamov na stránku.
Status	Enum	Nie	Typ transakcie. Povolené typy: • BOOK (rezervácia) • INFO (zaúčtované transakcie) • ALL (všetky transakcie) Predvolená hodnota je ALL.

Response

Metóda: accounts/transactions

Názov atribútu	Formát	Povinný	Poznámka
pageCount	integer	Nie	Celkový počet stránok
transactions	typ: ArrayOfAccountsTransactionsResponseTransaction	Áno	Pole transakcií

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

Príklad použitia viac zdroj [8] kapitola 5.2.6.

2.9.2.5.1 Definícia typu ArrayOfAccountsTransactionResponseTransaction

Metóda: accounts/transactions - typ: ArrayOfAccountsTransactionsResponseTransaction				
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)		Formát	Povinný	Poznámka
amount	value	decimal (2 desatinné miesta)	Áno	Hodnota čiastky transakcie
	currency	String (3)	Áno	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená
creditDebitIndicator		enum	Áno	Skratka Indikátoru Kredit / Debet • CRDT (Kredit) • DBIT (Debet)
reversalIdentificator		boolean	Nie	Príznak určuje, či sa jedná o reverznú transakciu
status		enum	Áno	Typ transakcie. • BOOK (rezervácia) • INFO (zaúčtované transakcie)
bookingDate		dateTime	Povinné pre transakciu typu BOOK	Dátum rezervácie transakcie
valueDate		dateTime	Áno	Dátum valuty transakcie
paymentDate		dateTime	Áno	Dátum dokladu (nová položka, ktorá nie je súčasťou SBAS)
bankTransactionCode		String	Nie	Kód kategórie typu transakcie zo zoznamu kódov SBA
transactionDetails		typ:AccountsTransactionsResponseTransactionDetail	Áno	Položky detailu transakcie

2.9.2.5.2 Definícia typu AccountsTransactionsResponseTransactionDetail

Metóda: AccountTransaction - typ: ArrayOfAccountsTransactionsResponseTransaction					
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)			Formát	Povinný	Poznámka
additionalTransactionInformation			String	Nie	Popis bankovej transakcie
counterValueAmount	amount	value	Decimal (2 desatinné miesta)	Nie	Hodnota čiastky transakcie
		currency	String (3)	Nie	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená
	currencyExchange	exchangeRate	Decimal (2 desatinné miesta)	Nie	Použitý výmenný kurz pre konverziu z inštruovanej meny na menu cieľového účtu
references	additionalTransactionInformation		String (35)	Nie	Jedinečné ID transakcie generované bankou
	chequeNumber		String (35)	Nie	Používané pri kartových transakciách Číslo karty vo formáte **** **** **** 1111
	endToEndIdentification		String (35)	Nie	Jedinečná identifikácia definovaná žiadateľom
	instructionIdentification		String (35)	Nie	Identifikácia platby generovaná klientom
	mandateIdentification		String (35)	Nie	Odkaz na mandát (referenčné číslo)
	transactionIdentification		String (35)	Nie	ID platby
relatedAgents	creditorAgent	financialInstitutionIdentification	String (11)	Nie	Identifikácia banky príjemcu, obvykle bankový identifikačný kód (BIC)
	deptorAgent	financialInstitutionIdentification	String (11)	Nie	Identifikácia banky platiteľa, obvykle bankový identifikačný kód (BIC)
relatedDates	acceptanceDateTime		Date	Nie	Dátum zadania transakcie (dátum prijatia transakcie v banke)
relatedParties	creditor	identification	String (35)	Nie	Identifikátor príjemcu (CID) v transakcii inkasa
		name	String	Nie	Meno príjemcu

	creditorAccount	identification	String (34)	Nie	Jedinečná identifikácia účtu príjemcu (IBAN)
	debtor	Name	String	Nie	Meno platiteľa
	debtorAccount	Identification	String (34)	Nie	Jedinečná identifikácia účtu platiteľa (IBAN)
	tradingParty	Identification	String (35)	Nie	Jedinečná identifikácia tretej strany. Pre kartové transakcie je tu uvádzané ID obchodníka
		merchantCode	String (4)	Nie	Kód kódu obchodníka (MCC) koordinovaný spoločnosťou MasterCard a Visa
		name	String	Nie	Meno tretej strany. Pre kartové transakcie je tu uvádzané obchodníka
remittanceInformation			String	Nie	Text pre príjemcu transakcie

2.9.3 Služby PISP (Vytvorenie platby, zisťovanie stavu platby, autorizácia platby, zrušenie platby)

Kapitola definuje zoznam metód poskytovaných pre PISP.

2.9.3.1 Predpoklady pre používanie metód API pre PISP

a/ záznam TPP je na základe licenčného čísla (vrátane použitého prefixu) uvedeného v certifikáte, ktorý TPP používa pri komunikácii, nájdený v databáze IB

b/ nájdený záznam TPP je platný,

c/ TPP má vo svojom zázname povolenú službu PISP (táto informácia je súčasťou záznamu TPP v databáze IB, ktorý sa automaticky aktualizuje z NBS)

d/ registrovaná aplikácia TPP má povolenú službu PISP

e/ v certifikáte, ktorý používa TPP pri komunikácii je uvedená služba PISP

f/ TPP použil v hlavičke požiadavky access_token, na základe ktorého je na strane banky dohľadaný záznam aktivácie, ktorý vznikol na základe aktivačného workflow dokončeného disponentom.

g/ aplikácia TPP má v nájdenom aktivačnom zázname, ktorý vznikol na základe aktivačného workflow dokončeného disponentom, uloženú službu PISP

2.9.3.2 Zoznam metód používaných pre PISP

Endpoint	Metoda	Popis
/api/v1/**payments/standard/iso**	POST	**Standard payment initialization (XML)** - Prostredníctvom tejto metódy disponentom autorizovaná tretia strana iniciuje (vytvorí) SEPA príkaz z bankového účtu disponenta. Iniciovanie platby bude vykonané zaslaním súboru vo formáte XML (PAIN.001) v tele požiadavky.
/api/v1/**payments/submission**	POST	**Standard payment submission –** prostredníctvom tejto služby je umožnené TPP autorizovať platbu iniciovanú pomocou služby "Standard payment initialization"
/api/v1/**payments/{orderId}/status**	GET	**Payment order status –** Prostredníctvom tejto služby je TPP umožnené zisťovanie stavu platobného príkazu
/api/v1/**payments/{orderId}/rcp**	DELETE	**Cancel payment -** prostredníctvom tejto služby je umožnené zrušenie platby, ktorá ešte nebola autorizovaná treťou stranou (tretia strana nepoužila metódu "Standard payment submission") a ktorá bola vytvorená prostredníctvom služby PISP Standard payment initialization (XML)
/api/v1/**accounts/balanceCheck**	POST	**Balance check** - prostredníctvom tejto metódy si TPP môže overiť, či má klient na bankovom účte, dostatok prostriedkov na zrealizovanie transakcie

2.9.3.3 PISP operácia: Standard payment initialization (XML)

Operácia umožňuje inicializáciu jednej platby vo formáte XML (PAIN.001.001.03).

PISP odošle cez API požiadavku obsahujúcu jednu platbu založenú na štruktúre definovanej normou ISO20022 pain.001.001.03. Odoslaním tejto požiadavky sa na strane banky vytvorí platobný príkaz, ktorý sa vzťahuje k obchodnej transakcii medzi PSU a obchodníkom (TPP typu PISP).

Endpoint: POST https://api.privatbanka.sk/api**/v1/payments/standard/iso**

Request

Telo požiadavky obsahuje jednu platbu vo formáte xml: pain.001.001.03
Viz https://www.iso20022.org/documents/general/Payments_Maintenance_2009.zip

Response (pokiaľ nedôjde pri spracovaní požiadavky k chybe)

Telo odpovede obsahuje opis zadanej platby vo formáte xml: pain.002.001.03

Metoda: payments/standard/iso				
Názov atribútu	Výskyt v XML struktuře odpovědi	Formát	Povinný	Poznámka
orderId	TxInfAndSts/AcctSvcrRef	String	Áno	Číslo príkazu vytvoreného v databáze Internetbankingu
reasonCode	TxInfAndSts/StsRsnInf/Rsn	String	Nie	Status Reason Code podle ISO 20022 Viz: https://www.iso20022.org/sites/default/files/documents/External_code_lists/ExternalCodeSets_4Q2017_05Mar2018_v1.xls, (listy: 16-StatusReason, 60-ReceivedReason, 61-AcceptedReason, 62-PendingProcessingReason, 63-RejectedReason
status	TxInfAndSts/TxSts	Enum	Áno	Status spracovania príkazu Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
statusDateTime	GrpHdr/CreDtTm	dateTime	Nie	Dátum prijatia príkazu do banky

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

Príklad použitia viac zdroj [8] kapitola 6.2.2.

2.9.3.4 PISP operácia: Standard payment submission

Operácia umožňuje tretej strane autorizáciu platby, ktorú táto TPP inicializovala.

Endpoint: POST https://api.privatbanka.sk/api**/v1/payments/submission**

Request

Telo požiadavky neobsahuje žiadne atribúty.

Hlavička požiadavky bude obsahovať token "bearer token" (access_token), ktorý bude prepojený s práve autorizovaným príkazom s daným "orderId". Aby TPP získala tento access_token, musí predtým prebehnúť autorizácia danej platby disponentom (pozri kapitolu 2.9.3.4.2). Výsledkom tejto autorizácie je autorizačný kód (code), ktorý

dostane TPP v odpovedi. Tento code následne TPP vymení pomocou Authorization code flow za daný access_token, previazaný s daným príkazom (pozri kapitolu 2.9.3.4.3).

Response (pokiaľ nedôjde pri spracovaní požiadavky k chybe)

Metoda: payments/submission			
Názov atributu	Formát	Povinné	Poznámka
orderId	String	Áno	Číslo príkazu vytvoreného v databáze Internetbankingu
reasonCode	String	Nie	Status Reason Code podle ISO 20022 Viz: https://www.iso20022.org/sites/default/files/documents/External_code_lists/ExternalCodeSets_4Q2017_05Mar2018_v1.xls, (listy: 16-StatusReason, 60-ReceivedReason, 61-AcceptedReason, 62-PendingProcessingReason, 63-RejectedReason
status	Enum	Áno	Status príkazu Status môže nadobúdať nasledujúce hodnoty: › RJCT (Odmietnuté - Rejected) › PDNG (Autorizované - Authorized) › ACTC (K podpisu - WaitingForSignatures) › ACSP (Zpracováva sa - InProgress, Exportované - Exported) › ACSC (Akceptované bankovým systémom)
statusDateTime	dateTime	Nie	Datum přijetí příkazu do banky.

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

Príklad použitia viac zdroj [8] kapitola 6.2.4.3.

2.9.3.4.1 Token pre PISP operáciu Autorizácia platby (Standard Payment submission)

Pre autorizáciu platby bude používaný access_token získaný na základe autorizačného resource Authorization Code Grant s PKCE rozšírením popísaného v kapitole 2.8.1 alebo prípadne pozri [1], kapitola 4.1.

Generovanie access_tokenu na základe Client Credentials Grant flow nie je v riešení podporované.

2.9.3.4.2 Autorizácia platby (disponentom - užívateľom aplikácie TPP)

Proces autorizácie platby disponentom musí PISP iniciovať po tom, čo sa po vytvorení (inicializácii) platby vráti v odpovedi z ASPSP (banky) číslo, pod akým sa daná platba na strane banky vytvorila (OrderId).

Endpoint: GET https://api.privatbanka.sk/auth/oauth**/authorize**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
response_type	Áno	**code**	Povinný parameter. Hodnotou parametra je určené, aký typ autentizačného procesu je požadovaný. V tomto prípade sa jedná o code grant. Pre autentizačný proces to znamená, že výsledkom tejto požiadavky bude jednorazový auth_code, ktorý TPP následne pomocou ďalšej požiadavky (metódou token) zamení za token access_token
client_id	Áno	String	Jedinečný identifikátor, ktorý banka vygenerovala pre aplikáciu TPP
redirect_uri	Áno	URL	URL kam je na konci presmerované proces autentizácie. Toto URL je stanovené už pri vydaní client_id a v rámci autentizácia je tento parameter validovaný proti URL zavedenému k client_id v zázname aplikácie registrovanej v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrovanej aplikácie.
Scope	Áno	String	Jedná sa o pole požadovaných scope (oprávnenia). V prípade PSD2 to môžu byť role AISP, PISP, PIISP. Napr. ak je TPP držiteľom viac oprávnenia, môže tu pre svoju aplikáciu požiadať len o jedno z nich alebo viac. Ak je použitých viac typov scope, sú oddelené medzerou.
state	Áno	Libovolný string [min 128 bits]	Parametrom sa zvyšuje bezpečnosť komunikácie pri presmerovaní. Chráni pred útokmi CSRF a odovzdáva informácie z aplikácie prostredníctvom toku autentizácie.
code_challenge	Áno	String	code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier))) viz. zdroj [3] RFC 7636 (OAuth PKCE)
code_challenge_method	Áno	String	S256
request	Áno	JWT	Príklad použitia viz [8] kapitola 6.2.9

Súčasťou požiadavky o autorizáciu platby disponentom je podpísaný JWT Request, ktorý obsahuje OrderId. Pri požiadavke o autorizáciu platby disponentom bude disponent presmerovaný z aplikácie TPP na centrálnu autorizačnú stránku.

Potom, čo disponent vykoná dvojfaktorovú autorizáciu, zobrazí sa mu detail platby, ktorú musí autorizovať svojím autorizačným zariadením. Po autorizácii platby disponentom je v odpovedi vrátený autorizačný code, ktorý je previazaný s daným OrderId a platba čaká na autorizáciu treťou stranou.

Response			
Atribut	**Povinný**	**Typ**	**Popis**
Code	Áno	String	Jednorazový autorizačný kód
Id_token	Nie	JWT	**Nie je podporované**
State	Áno	String	Hodnota atribútu odovzdaného z TPP požiadavky

Chybové kódy

- Chybové kódy sú definovány podľa [1] RFC 6749, kapitola 4.1.2.1

Príklad použitia viac zdroj [8] kapitola 6.2.4.1.

2.9.3.4.3 Získanie tokenu

Aby PISP mohol vykonať podpísanie vytvorené platby (/payments/submission), musí získať od banky access_token. Toto vykoná výmenou autorizačného Code, ktorý dostal v odpovedi požiadavky /Authorize, za daný access_token.

PISP zašle spoločne s týmto autorizačným kódom (ktorý musí byť uvedený v tele požiadavke) aj client_id a client_secret (ktoré však musí byť uvedené v hlavičke požiadavke zakódovanej pomocou Base64).

Endpoint: POST https://api.privatbanka.sk/auth/oauth/**token**

Request			
Atribut	**Povinný**	**Typ**	**Popis**
code	Áno	string	Autorizačný code navrátený z autentizačného procesu (code grant)
redirect_uri	Áno	URL	URL redirect zhodné s URL doručenom v autentizačnom requeste
grant_type	Áno	**authorization_code**	Podľa existujúcej definície / zvyklosti OAuth2 bude táto hodnota authorization_code, ak dochádza k výmene code za access_token.
code_verifier	Áno	String	code_verifier slúži na generovanie code_challenge z predchádzajúcej žiadosti o minimálnej dĺžke 43 znakov a maximálnou dĺžkou 128 znakov

Response			
Atribut	**Povinný**	**Typ**	**Popis**
access_token	Áno	string	Krátkodobý token (platnosť tokenu je 3600s), ktorý slúži na autorizáciu requestu na API.
expires_in	Áno	number	Zostávajúci čas do expirácie access_tokenu - v sekundách.
token_type	Áno	String	Typ tokenu “Bearer”

Chybové kódy

- Chybové kódy sú definované podľa [1] RFC 6749, kapitola 5.2

Príklad použitia viac zdroj [8] kapitola 6.2.4.2.

2.9.3.4.4 Autorizácia platby treťou stranou (TPP)

Potom, čo TPP získa access_token previazaný s daným príkazom, prevedie posledný krok - vytvorí požiadavku na autorizáciu danej platby (pozri kapitolu 2.9.3.4)

2.9.3.5 PISP operácia: Payment Order Status

Operácia poskytuje informácie o stave spracovania prijatej platobnej transakcie na základe parametra {orderId}.

Endpoint: GET https://api.privatbanka.sk/api**/v1/payments/{orderId}/status**

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: payments/{orderId}/status			
Názov atribútu	Formát	Povinný	Poznámka
orderId	String	Áno	Číslo príkazu vytvoreného v databáze Internetbankingu
reasonCode	String	Nie	V položke sa uvádza informácia o skutočnom statuse, ktorý ma príkaz v Internetbankingu. Jedná sa o dodatočnú informáciu k poľu „status“. Hodnota z tejto položky má význam predovšetkým v prípade, keď bude v položke „status“ uvedená hodnota „Others“ – (tzn. že pri spracovaní príkazu v Internetbankingu je príkaz v stave, ktorý nie je pri spracovaní bežný (nie je obsiahnutý v množine statusov uvedených v poli „status“).
status	Enum	Áno	Status príkazu Status môže dosahovať nasledujúce hodnoty: • RJCT (Odmietnuté / Zrušené klientom - Rejected) • PDNG (Autorizované - Authorized) • ACTC (K podpisu - WaitingForSignatures) • ACSP (Zpracováva sa - InProgress, Exportované - Exported) • ACSC (Akceptované bankovným systémom) • OTHR (rezerva)
statusDateTime	dateTime	Nie	Dátum prijatia príkazu do banky.

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

2.9.3.6 PISP operácia: Cancel payment

Operácia umožňuje zrušiť platbu, ktorá bola iniciovaná prostredníctvom identického providera (tretej strany) typu PISP pomocou služby "Standard payment Initialization (XML)". Platbu je možné zrušiť, kým TPP túto platbu neautorizuje službou "Payment Order Submission".

Endpoint: GET https://api.privatbanka.sk/api**/v1/payments/{orderId}/rcp**

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: payments/{orderId}/status			
Názov atribútu	Formát	Povinný	Poznámka
orderId	String	Áno	Číslo príkazu zrušeného v databáze Internet Bankingu

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

2.9.3.7 PISP operácia: Balance Check

Prostredníctvom tejto metódy si TPP môže overiť, či má klient na bankovom účte, dostatok prostriedkov na vykonanie platby.

Endpoint: POST https://api.privatbanka.sk/api**/v1/accounts/balanceCheck**

Request

Metóda: accounts/balanceCheck					
Názov atribútu			Formát	Povinný	Poznámka
iban			String (34)	Áno	IBAN účtu.
creationDate			dateTime	Nie	Dátum a čas vytvorenia požiadavky podľa RFC 3339
amount	value		Decimal (2 desatinné miesta)	Nie	Hodnota čiastky transakcie
	currency		String (3)	Nie	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená
instructionIdentification			string	Áno	Technická identifikácia platby generovaná na strane PISP
relatedParties	tradingParty	address	string	Nie	Adresa obchodníka (obvykle obsahuje zreťazenie názvu ulice, čísla ulice atď.).)
		countryCode	string	Nie	Dvojznakový kód zeme obchodníka podľa normy ISO3166
		identification	string	Nie	Jedinečná identifikácia tretej strany. Pre transakciu s kartou je tu uvedené číslo obchodníka.
		merchantCode	string	Nie	Kód kódu obchodníka (MCC) koordinovaný spoločnosťou MasterCard a Visa
		name	string	Nie	Meno tretej strany V prípade kartových transakcií sa tu uvádza meno obchodníka
references	chequeNumbe		string	Nie	V prípade kartových transakcií sa tu uvádza číslo karty vo formáte **** **** **** 1111
	holderName		string	Nie	Meno držiteľa karty

Response

Metóda: accounts/balanceCheck			
Názov atribútu	Formát	Povinný	Poznámka
response	Enum	Áno	Výsledok volania. Môže nadobúdať nasledujúce hodnoty: APPR (dostatočné finančné prostriedky na účte) DECL (nedostatočné prostriedky na účte)
dateTime	dateTime	Áno	Dátum a čas formátovaný podľa RFC3339, v ktorom bola akcia vyžiadaná

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

2.9.4 Služba PIISP (Overenie dostatočných prostriedkov na účte)

Kapitola definuje zoznam metód poskytovaných pre PIISP.

2.9.4.1 Predpoklady pre používanie metód API pre PIISP

a/ záznam TPP je na základe licenčného čísla (vrátane použitého prefixu) uvedeného v certifikáte, ktorý TPP používa pri komunikácii, nájdený v databáze IB

b/ nájdený záznam TPP je platný,

c/ TPP má vo svojom zázname povolenú službu PIISP (táto informácia je súčasťou záznamu TPP v databáze IB, ktorý sa automaticky aktualizuje z NBS)

d/ registrovaná aplikácia TPP má povolenú službu PIISP

e/ v certifikáte, ktorý používa TPP pri komunikácii je uvedená služba PIISP

f/ TPP použil v hlavičke požiadavky access_token, na základe ktorého je na strane banky dohľadaný záznam aktivácie, ktorý vznikol na základe aktivačného workflow dokončeného disponentom.

g/ aplikácia TPP má v nájdenom aktivačnom zázname, ktorý vznikol na základe aktivačného workflow dokončeného disponentom, dodatočne disponentom aktivovanú službu PIISP

2.9.4.2 Zoznam metód používaných pre službu PIISP

Endpoint	Metoda	Popis
/api/v1/**accounts/balanceCheck**	POST	Balance check - prostredníctvom tejto metódy si TPP môže overiť, či má klient na bankovom účte, ku ktorému TPP vydala kartu, dostatok prostriedkov k zrealizovaniu transakcie kartou

2.9.4.3 Token pre PIISP operáciu

Pre PIISP operáciu bude používaný access_token získaný na základe autorizačného resource Authorization Code Grant s PKCE rozšírením popísaného v kapitole 2.8.1 alebo prípadne pozri [1], kapitola 4.1.

Generovanie access_tokenu na základe Client Credentials Grant flow, ktoré je v SBAS uvedené ako alternatívne rešenie (teda je nepovinné), nie je v riešení podporované.

2.9.4.4 PIISP operácia: Balance Check

Prostredníctvom tejto metódy si TPP môže overiť, či má klient na bankovom účte, ku ktorému TPP vydala kartu, dostatok prostriedkov na zrealizovanie transakcie kartou.

Endpoint: POST https://api.privatbanka.sk/api**/v1/accounts/balanceCheck**

Request

Metóda: AccounBalanceCheck					
Názov atribútu			Formát	Povinný	Poznámka
iban			String (34)	Áno	IBAN účtu.
creationDate			dateTime	Nie	Dátum a čas vytvorenia požiadavky podľa RFC 3339
amount	value		Decimal (2 desatinné miesta)	Nie	Hodnota čiastky transakcie
	currency		String (3)	Nie	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená
instructionIdentification			string	Áno	Technická identifikácia platby generovaná na strane PIISP
relatedParties	tradingParty	address	string	Nie	Adresa obchodníka (obvykle obsahuje zreťazenie názvu ulice, čísla ulice atď.).)

		countryCode	string	Nie	Dvojznakový kód krajiny obchodníka podľa normy ISO3166
		identification	string	Nie	Jedinečná identifikácia tretej strany. Pre transakciu s kartou je tu uvedené číslo obchodníka.
		merchantCode	string	Nie	Kód kódu obchodníka (MCC) koordinovaný spoločnosťou MasterCard a Visa
		name	string	Nie	Meno tretej strany V prípade kartových transakcií sa tu uvádza meno obchodníka
references	chequeNumbe		string	Nie	V prípade kartových transakcií sa tu uvádza číslo karty vo formáte **** **** **** 1111
	holderName		string	Nie	Meno držiteľa karty

Response

Metóda: AccounBalanceCheck			
Názov atribútu	Formát	Povinný	Poznámka
response	Enum	Áno	Výsledok volania. Môže nadobúdať nasledujúce hodnoty: APPR (dostatočné finančné prostriedky na účte) DECL (nedostatočné prostriedky na účte)
dateTime	dateTime	Áno	Dátum a čas formátovaný podľa RFC3339, v ktorom bola akcia vyžiadaná

Chybové kódy		
HTTP Status	**Error kód**	**Popis**
400	**parameter_missing**	Chýba povinný parameter.
400	**parameter_invalid**	Nevalidná hodnota vstupného parametra.
500, 503	**server_error**	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [1] RFC 6749, kapitola 5.2		

Príklad použitia viac zdroj [8] kapitola 7.2.2 (upozornenie: grant_type “client_credentials” uvedený v príklade nie je v tomto riešení podporovaný – pozri kapitolu 2.9.4.3).

3. Zdroje

1. *RFC 6749 - The OAuth 2.0 Authorization Framework*, [online]. The Internet Engineering Task Force, October 2012. WWW: https://tools.ietf.org/html/rfc6749
2. *RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage,* [online]. The Internet Engineering Task Force, October 2012. WWW: https://tools.ietf.org/html/rfc6750
3. *RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients,* [online]. The Internet Engineering Task Force, September 2015. WWW: https://tools.ietf.org/html/rfc7636
4. *RFC 7519 - JSON Web Token (JWT)*, [online]. The Internet Engineering Task Force, May 2015. WWW: https://tools.ietf.org/html/rfc7519
5. *RFC 7515 - JSON Web Signature (JWS)*, [online]. The Internet Engineering Task Force, May 2015. WWW: https://tools.ietf.org/html/rfc7515
6. *Slovak Banking API Standard, SBA et al.,* [online]. WWW: http://docs.sbaonline.apiary.io/#
7. *ISO 20022 Financial Services - Universal financial industry message scheme,* [online]. International Organization for Standardization. WWW: https://www.iso20022.org/
8. *Slovak Banking API Standard*, dokument. WWW: https://www.sbaonline.sk/Content/files/projects/slovak-banking-api-standard-2_0.pdf