

Privatbanka, a.s.
PSD2 API dokumentácia

11.10.2021

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 funkcionality 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	
25.	Upravené kapitoly 2.5.3, 2.6.2.3 - pridané nové metódy pre: <ul style="list-style-type: none"> - import dávky príkazov (hromadný príkaz) - prácu s trvalými príkazmi 	2.10.2019	

26.	<p>Nové kapitoly: 2.9.3.8, 2.9.3.9, 2.9.3.10, 2.9.3.11, 2.9.3.12, 2.9.3.13, 2.9.3.14, 2.9.3.15, 2.9.3.16</p> <p>Kapitoly s popisom nových metód pre:</p> <ul style="list-style-type: none"> - import dávky príkazov (hromadný príkaz) - prácu s trvalými príkazmi 	2.10.2019	
27.	Kapitola 2.8.1.4 – oprava podľa dokumentácie „Slovak Banking API standard“ - atribút refresh_token je v odpovedi požiadavky „Nepovinný“ – doplnený popis plnenia tohto atribútu	11.10.2021	
28.	Kapitola 2.8.1.5 – oprava podľa dokumentácie „Slovak Banking API standard“ - atribút refresh_token je v odpovedi požiadavky „Nepovinný“	11.10.2021	
29.	Kapitola 2.5.2 – upravený popis pre službu Account list	11.10.2021	
30.	Kapitola 2.6.2.2 – upravený popis pre endpoint /api/v2/accounts	11.10.2021	
31.	Pridané kapitoly 2.9.2.6, 2.9.2.6.1 – AISP operácia Account List	11.10.2021	

Dátum: 11.10.2021

Verzia: 2.6

Obsah

1. ÚVOD	6
1.1 TERMINOLÓGIA.....	6
2. BEZPEČNOSTNÝ MODEL	7
2.1 ŠIFROVANÁ KOMUNIKÁCIA TPP-BANKA.....	7
2.2 REGISTRÁCIA TPP V BANKE	8
2.3 AKTIVÁCIA PRÍSTUPU TPP K ÚČTOM DISPONENTA	8
2.4 POPIS RIEŠENIA	8
2.4.1 Hlavné vlastnosti API.....	8
2.4.2 Popis workflow – nastavenie prístupu TPP k účtom disponenta	9
2.4.3 Internet Banking.....	11
2.5 SLUŽBY PODPOROVANÉ V API PSD2.....	12
2.5.1 Metódy pre automatickú registráciu aplikácie TPP cez API	12
2.5.2 Metódy oblasti AISP	13
2.5.3 Metódy oblasti PISP.....	13
2.5.4 Metódy oblasti PIISP.....	15
2.6 ENDPOINTY POUŽITÉ PRE API PSD2	15
2.6.1 Endpointy pre OAuth (autorizácia klienta, autorizácia platby klientom, vydávanie tokenov)	15
2.6.2 Endpointy pre PSD2 API (registračné resource (Enrollment), volanie metód AISP, PISP, PIISP)	15
2.7 REGISTRACNÉ RESOURCE VYSTAVENEJ BANKOU (ENROLLMENT)	18
2.7.1 Automatické generovanie technických identifikátorov	18
2.7.2 Zmena registračných údajov	21
2.7.3 Zmazanie aplikácie	22
2.7.4 Žiadosť o nový client_secret	23
2.8 AUTENTIZÁCIA A AUTORIZÁCIA REQUESTU (OAUTH2)	24
2.8.1 OAuth2 Authorization Code Grant	24
2.9 POPIS METÓD POUŽÍVANÝCH PRE POSKYTOVATEĽOV SLUŽIEB (TPP).....	29
2.9.1 Všeobecná definícia hlavičiek.....	29
2.9.2 Služby AISP (Dotazy k účtom, prehľad transakcií)	30
2.9.3 Služby PISP (Vytvorenie platby / žiadosti, zisťovanie stavu platby / žiadosti, autorizácia platby / žiadosti, zrušenie platby)	41
2.9.4 Služba PIISP (Overenie dostatočných prostriedkov na účte).....	69
3. ZDROJE	73

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

ASPS - 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 posilať 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 zavolaním 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 dohľadovaný v banke v zozname TPP - identické číslo licencie musí byť uvedené v certifikáte aj v zázname TPP v banke
 - dohľadovaný záznam TPP je platný,
 - typ použitej metódy zodpovedá službe (AISP, PISP, PIISP), ktorá je povolená v dohľadanom zázname TPP
 - access_token použitý v požiadavke je platný
 - na základe použitého access_tokenu (OAuth protokol), uvedeného v požiadavke, je dohľadovaný záznam aktivácie, ktorý vznikol na základe 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 aktivácie 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 nasledujúcim 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 licencii 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 sa 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 sekcii „Nastavenia“ ponuku "Prehľad PSD2 aktivácií", zobrazí sa prehľad všetkých aktivačných záznamov, ktoré vznikli na základe dokončenia workflow aktivácie, ktorá bola vyvolaná metódou /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	<p>Tlačidlo sa zobrazí iba v prípade, ak tretia strana má registrovanú službu PIISP a disponent túto službu zatiaľ v aktivačnom zázname nepovolil.</p> <p>Po stlačení tlačidla sa vytvorí nová žiadosť o aktiváciu služby PIISP pre danú aplikáciu TPP</p> <p>Disponent žiadosť o aktiváciu súhlasu používať PIISP autorizuje svojim autorizačným zariadením.</p>
Deaktivovať PIISP	<p>Tlačidlo sa zobrazí iba v prípade, ak tretia strana má registrovanú službu PIISP a disponent túto službu v aktivačnom zázname povolil.</p> <p>Po stlačení tlačidla sa vytvorí nová žiadosť o deaktiváciu služby PIISP pre danú aplikáciu TPP</p> <p>Disponent žiadosť o deaktiváciu súhlasu používať službu PIISP autorizuje svojim autorizačným zariadením.</p>
Zneplatnenie tokenov	<p>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.</p> <p>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).</p> <p>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.</p>

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)	<p>služba na požiadavku vráti zoznam účtov (bez zostatkov). V odpovedi sa vrátia len účty, ktoré spĺňajú všetky nasledujúce kritériá:</p> <ul style="list-style-type: none"> ➤ disponent, ktorý aktivoval prístup k svojim účtom pre aplikáciu TPP, má v internetbankingu k účtu aktívny prístup ➤ disponent má vo väzbe na klienta - majiteľa daného účtu - povolenú službu PSD2

2.5.3 Metódy oblasti PISP

Metóda služby	Popis
Standard payment initialization (XML)	<p>prostredníctvom tejto služby disponentom autorizovaná tretia strana iniciuje (vytvorí) jeden SEPA príkaz z bankového účtu disponenta vo formáte XML (PAIN.001).</p> <p>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.</p>
Payment status (JSON)	získovanie 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)
Batch Payment initialization (XML)	prostredníctvom tejto služby disponentom autorizovaná tretia strana iniciuje (vytvorí) dávku SEPA príkazov 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.
Trvalý príkaz – periodicity	Na základe tejto požiadavky sa vráti zoznam kódov periodicít, ktoré je povolené používať pri vytváraní nového a zmene trvalého príkazu
Trvalý príkaz - opisy	Na základe tejto požiadavky sa vrátia opisy trvalých príkazov
Trvalý príkaz – vytvorenie	Na základe tejto požiadavky sa vytvorí žiadosť na vytvorenie nového trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.
Trvalý príkaz - zmena	Na základe tejto požiadavky sa vytvorí žiadosť na zmenu existujúceho trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.
Trvalý príkaz – vyradenie	Na základe tejto požiadavky sa vytvorí žiadosť na vyradenie existujúceho trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.
Trvalý príkaz – blokácia	Na základe tejto požiadavky sa vytvorí žiadosť na novú blokáciu existujúceho trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.
Trvalý príkaz – deblokácia	Na základe tejto požiadavky sa vytvorí žiadosť na zrušenie existujúcej blokácie trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.
Trvalý príkaz – obnova	Na základe tejto požiadavky sa vytvorí žiadosť na obnovenie vyradeného trvalého príkazu TPP následne použije na žiadosť službu "/Authorize" - klient banky je presmerovaný na centrálnu autentizačnú stránku banky a tu danú žiadosť autorizuje svojim autentizačným zariadením.

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: <ul style="list-style-type: none"> - autorizáciu klienta, - autorizáciu platby klientom.
https://api.privatbanka.sk/auth/oauth/token	POST	Endpoint používaný v rámci OAuth Authorization code grant pre: <ul style="list-style-type: none"> - 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 metódy	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 registrovanej 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 aplikácii.

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	Endpoint pre metódu, ktorá na požiadanie vráti zoznam účtov (bez zostatkov).

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
https://api.privatbanka.sk/api/v1/payments/batch/iso	POST	Endpoint pre metódu Batch Payment initialization (XML) - disponentom autorizovaná tretia strana iniciuje (vytvorí) dávku SEPA príkazov z bankového účtu disponenta
https://api.privatbanka.sk/api/v1/standingOrders/Periodicity	GET	Endpoint pre metódu Trvalý príkaz – periodicity – žiadosť o zoznam kódov periodicit, ktoré sú povolené v trvalých príkazoch
https://api.privatbanka.sk/api/v1/standingOrders	GET	Endpoint pre metódu Trvalý príkaz – opisy – žiadosť o opisy trvalých príkazov
https://api.privatbanka.sk/api/v1/standingOrders	POST	Endpoint pre metódu Trvalý príkaz – vytvorenie – žiadosť o vytvorenie nového trvalého príkazu
https://api.privatbanka.sk/api/v1/standingOrders/{id}	PUT	Endpoint pre metódu Trvalý príkaz – zmena – žiadosť o zmenu existujúceho trvalého príkazu
https://api.privatbanka.sk/api/v1/standingOrders/{id}	DELETE	Endpoint pre metódu Trvalý príkaz – vyradenie – žiadosť o vyradenie existujúceho trvalého príkazu
https://api.privatbanka.sk/api/v1/standingOrders/{id}/block	POST	Endpoint pre metódu Trvalý príkaz – blokácia – žiadosť o vytvorenie blokácie existujúceho trvalého príkazu
https://api.privatbanka.sk/api/v1/standingOrders/{id}/unblock	POST	Endpoint pre metódu Trvalý príkaz – deblokácia – žiadosť o zrušenie blokácie trvalého príkazu
https://api.privatbanka.sk/api/v1/standingOrders/{id}/renew	POST	Endpoint pre metódu Trvalý príkaz – obnova – žiadosť o obnovenie vyradeného trvalého príkazu

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
<i>redirect_uris</i>	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.
<i>client_name</i>	Áno	String [Max 255 B]	Meno TPP aplikácie
<i>client_name##en-US</i>	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
<i>client_type</i>	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
<i>logo_uri</i>	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. Miesto odkiaľ je možné ho pri registrácii stiahnuť)
<i>contacts</i>	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
<i>scopes</i>	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.
<i>licence_number</i>	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
<i>client_id</i>	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).
<i>client_secret</i>	Áno	String	Client_secret - password / token vydaný bankou (ASPSP) pre TPP aplikáciu (client_id)
<i>client_secret_expires_at</i>	Nie	DateTime	Defaultná hodnota je 0 (client_secret nikdy neexpiruje). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z
<i>api_key</i>	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")
<i>redirect_uris</i>	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.
<i>client_name</i>	Áno	String [Max 255 B]	Meno TPP aplikácie
<i>client_name#en-US</i>	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
<i>client_type</i>	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
<i>logo_uri</i>	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. miesto, odkiaľ je možné ho pri registrácii stiahnuť)
<i>contacts</i>	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
<i>scopes</i>	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.
<i>licence_number</i>	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
<i>client_id</i>	Áno	String	client_id priradené aplikácii bankou.
<i>client_secret_expires_at</i>	Nie	DateTime	Defaultná hodnota je 0 (client_id nikdy neexpirujú). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z
<i>redirect_uris</i>	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.
<i>client_name</i>	Áno	String [Max 255 B]	Meno TPP aplikácie
<i>client_name#en-US</i>	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
<i>client_type</i>	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
<i>logo_uri</i>	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. Miesto odkiaľ je možné ho pri registrácii stiahnuť)
<i>contacts</i>	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
<i>scopes</i>	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 konkrétnej aplikácie.

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	<code>invalid_request</code>	Nevalidný request. V požiadavke chýba povinné pole alebo je v nevhodnom / nevalidnom formáte.
401	<code>invalid_client</code>	Nevalidný <code>client_id</code> .
401	<code>unauthorized_client</code>	TPP nie je oprávnený vykonávať túto požiadavku.
401	<code>access_denied</code>	Autorizačný server odmietol prístup.
500, 503	<code>server_error</code>	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
<code>client_id</code>	Áno	String	<code>client_id</code> priradené aplikácii.
<code>client_secret</code>	Áno	String	<code>Client_secret</code> - password / token vydaný bankou (ASPSP) pre TPP aplikáciu (<code>client_id</code>)
<code>client_secret_expires_at</code>	Nie	DateTime	Defaultná hodnota je 0 (<code>client_id</code> nikdy neexpirujú). 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 (žiadost' 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 grant 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
<i>response_type</i>	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
<i>client_id</i>	Áno	String	Jedinečný identifikátor, ktorý banka vygenerovala pre aplikáciu TPP
<i>redirect_uri</i>	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.
<i>Scope</i>	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.
<i>state</i>	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.
<i>code_challenge</i>	Áno	String	code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier))) viz. zdroj [3] RFC 7636 (OAuth PKCE)
<i>code_challenge_method</i>	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 definované 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
<i>code</i>	Áno	string	Autorizačný code navrátený z autentizačného flow (code grant)
<i>redirect_uri</i>	Áno	URL	URL redirect zhodné s URL doručenom v autentizačnom requestu
<i>grant_type</i>	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.
<i>code_verifier</i>	Áno	String	code_verifier slúži na generovanie code_challenge z predchádzajúcej žiadosti o minimálnej dĺžke 43 znakov a maximálnou dĺžkou 128 znakov
<i>iban</i>	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
<i>access_token</i>	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.
<i>expires_in</i>	Áno	number	Zostávajúci čas do expirácie access_tokenu - v sekundách.
<i>refresh_token</i>	Nie	String	Dlhodobý token (platnosť 90 dní) vydaný na základe výmeny za jednorazový code . Hodnota „refresh_token“ sa v odpovedi vráti iba v prípade požiadavky o výmenu jednorazového code , za novú dvojicu tokenov: access_token a refresh_token. refresh_token nie je súčasťou odpovede, v prípade požiadavky o výmenu jednorazového code za access_token, ktorý je následne použitý pre požiadavku typu PISP Standard payment submission (viď kapitolu 2.9.3.4). Jedná sa o code , ktorý TPP dostane v odpovedi po autorizácii platobného príkazu klientom.
<i>token_type</i>	Áno	String	Typ tokenu "Bearer"
<i>scope</i>	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 access_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	Áno	refresh_token	Existujúca definícia / zvyklosti OAuth2 bude táto hodnota refresh_token, ak dochádza k obnoveniu access_tokenu na základe refresh_token.
refresh_token	Áno	String	Validný refresh_token
scope	Áno	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
<i>access_token</i>	Áno	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.
<i>token_type</i>	Áno	String	Typ tokenu "Bearer"
<i>expires_in</i>	Áno	number	Zostávajúci čas do expirácie access_tokenu - v sekundách.
<i>refresh_token</i>	Nie	String	Refresh_token, na základe ktorého prebehlo obnovenie access_tokenu (jedná sa 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	Mandator y	Typ	Popis
<i>Host</i>	Ano	String	Doménové meno servera a číslo portu
<i>Content-Type</i>	Ano	String	application/json alebo application/xml
<i>Authorization</i>	Ano	String	Typ autorizácie definovaný podľa RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage
<i>Request-ID</i>	Ano	String	Jedinečný identifikátor konkrétnej požiadavky. Odporúča sa použiť formulár UUID (Universally Unique Identifier) verzie 4 (RFC4122).
<i>Correlation-ID</i>	Ne	String	Jedinečný korelačný identifikátor, možno ho použiť ako kontrolu prepojenie požiadavky a odpovede. Odporúča sa použiť formulár UUID (Universally Unique Identifier) verzie 4 (RFC4122).
<i>Process-ID</i>	Ne	String	Identifikátor obchodného alebo technického procesu, na základe ktorého možno párovať sadu dvojíc požiadaviek a odpovedí. Odporúča sa použiť formulár UUID (Universally Unique Identifier) verzie 4 (RFC4122).
<i>PSU-IP-Address</i>	Ano	String	IP adresa zákazníka (disponenta banky), z ktorej je pripojený k infraštruktúre TPP.
<i>PSU-Device-OS</i>	Ano	String	Identifikácia zariadenia zákazníka (disponenta banky), alebo operačného systému, z ktorého je pripojený k infraštruktúre TPP
<i>PSU-User-Agent</i>	Ano	String	Identifikácia webového prehliadača zákazníka alebo identifikácia klientskeho zariadenia, z ktorého je pripojený k infraštruktúre TPP
<i>PSU-Geo-Location</i>	Ne	String	Súradnice GPS aktuálnej polohy zákazníka v okamihu pripojenia k infraštruktúre TPP. (Požadovaný formát GPS: zemepisná šírka, zemepisná dĺžka)
<i>PSU-Last-Logged-Time</i>	Ne	DateTime	Dátum a čas, kedy bol používateľ prihlásený k aplikácii TPP (formát RFC3339)
<i>PSU-Presence</i>	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	Mandator y	Typ	Popis
<i>Content-Type</i>	Ano	String	application/json nebo application/xml
<i>Response-ID</i>	Ano	String	Jedinečný identifikátor konkrétnej odpovede. Odporúča sa použiť formulár UUID (Universally Unique Identifier) verzie 4 (RFC4122).
<i>Correlation-ID</i>	Ne	String	Jedinečný korelačný identifikátor, možno ho použiť ako kontrolu prepojenia požiadavky a odpovede. Odporúča sa použiť formulár UUID (Universally Unique Identifier) verzie 4 (RFC4122).
<i>Process-ID</i>	Ne	String	Identifikátor obchodného alebo technického procesu, na základe ktorého možno párovať sadu dvojíc požiadaviek a odpovedí. Odporúča sa použiť formulár UUID (Universally Unique Identifier) 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	služba na požiadanie vráti zoznam účtov disponenta (bez zostatkov). V odpovedi sa vráti len účty, ktoré spĺňajú všetky nasledujúce kritériá: <ul style="list-style-type: none"> > disponent, ktorý aktivoval prístup k svojim účtom pre aplikáciu TPP, má v internetbankingu k účtu aktívny prístup > disponent má vo väzbe na klienta - majiteľa daného účtu - povolenú službu PSD2

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 . <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> • CRDT (Kredit) • DBIT (Debet)
dateTime		dateTime	Áno	Dátum aktualizácie zostatku
typeCodeOrProprietary		enum	Áno	Typ zostatku <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • CRDT (Kredit) • DBIT (Debet)
reversalIndicator		boolean	Nie	Príznak určuje, či sa jedná o reverznú transakciu
status		enum	Áno	Typ transakcie. <ul style="list-style-type: none"> • 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)
	debtorAgent	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

2.9.2.6 AISP operácia: Account List

Prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana možnosť požiadať o zoznam účtov, ktoré je možné používať v požiadavkách zaslaných cez rozhranie PSD2.

V odpovedi sa vrátia len účty, ktoré spĺňajú všetky nasledujúce kritériá:

- disponent, ktorý aktivoval v internetbankingu prístup k svojim účtom pre aplikáciu TPP, má k účtu aktívny prístup
- disponent má vo väzbe na klienta - majiteľa daného účtu - povolenú službu PSD2

Endpoint: GET <https://api.privatbanka.sk/api/v2/accounts>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: accounts			
Názov atribútu	Formát	Povinný	Poznámka
creationDateTime	DateTime	Áno	Dátum a čas formátovaný podľa RFC3339, v ktorom bola konkrétna akcia vyžiadaná
accounts	typ: ArrayOfAccountInfo	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 5.2.7.

2.9.2.6.1 Definícia typu ArrayOfAccountInfo

Metóda: accounts - typ: ArrayOfAccountInfo				
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)		Formát	Povinný	Poznámka
identification	iban	String (34)	Áno	IBAN účtu disponenta
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 . <ul style="list-style-type: none"> • CACC - bežný účet • LOAD – úverový účet • SVGS – sporiaci účet
baseCurrency		String (3)	Áno	Mena účtu (kód meny podľa ISO 4217 - 3 veľké písmená)
servicer	financialInstitutionIdentification	String (11)	Áno	BIC kód Privatbanky
consent		Array of string	Áno	Zoznam služieb, ktoré má TPP povolené disponantom v súhlase. Pole môže obsahovať nasledujúce reťazce: AISP, PISP, PIISP

2.9.3 Služby PISP (Vytvorenie platby / žiadosti, zisťovanie stavu platby / žiadosti, autorizácia platby / žiadosti, 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 dohľadovaný 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. Inicializácia platby bude vykonaná 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
/api/v1/payments/batch/iso	POST	Batchpayment initialization (XML) - Prostredníctvom tejto metódy disponentom autorizovaná tretia strana iniciuje (vytvorí) dávku SEPA príkazov z bankového účtu disponenta. Inicializácia dávky príkazov bude vykonaná zaslaním súboru vo formáte XML (PAIN.001) v tele požiadavky.
/api/v1/standingOrders/Periodicity	GET	Trvalý príkaz – periodicity – prostredníctvom tejto služby je umožnené poslať žiadosť o zoznam kódov periodicít, ktoré sú povolené v trvalých príkazoch
/api/v1/standingOrders	GET	Trvalý príkaz – opisy – prostredníctvom tejto služby je umožnené poslať žiadosť o opisy trvalých príkazov k špecifickému účtu disponenta
/api/v1/standingOrders	POST	Trvalý príkaz – vytvorenie – prostredníctvom tejto služby je umožnené poslať žiadosť o vytvorenie nového trvalého príkazu
/api/v1/standingOrders/{id}	PUT	Trvalý príkaz – zmena – prostredníctvom tejto služby je umožnené poslať žiadosť o zmenu trvalého príkazu
/api/v1/standingOrders/{id}	DELETE	Trvalý príkaz – vyradenie – prostredníctvom tejto služby je umožnené poslať žiadosť o vyradenie trvalého príkazu
/api/v1/standingOrders/{id}/block	POST	Trvalý príkaz – blokácia – prostredníctvom tejto služby je umožnené poslať žiadosť o vytvorenie blokácie trvalého príkazu
/api/v1/standingOrders/{id}/unblock	POST	Trvalý príkaz – deblokácia – prostredníctvom tejto služby je umožnené poslať žiadosť o zrušenie blokácie trvalého príkazu
/api/v1/standingOrders/{id}/renew	POST	Trvalý príkaz – obnova – prostredníctvom tejto služby je umožnené poslať žiadosť o obnovenie vyradeného trvalého príkazu

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 štruktúre odpovedi	Formát	Povinný	Poznámka
orderId	GrpHdr/MsgId Alebo OrgnPmtInfAndSts/ TxInfAndSts/StsId	String	Áno	Číslo príkazu vytvoreného v databáze Internetbankingu
status	OrgnlGrpInfAndSts/ NbOfTxPerSts/ DtldSts	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 podľa 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: <ul style="list-style-type: none"> > RJCT (Odmietnuté - Rejected) > PDNG (Autorizované - Authorized) > ACTC (K podpisu - WaitingForSignatures) > ACSP (Zpracováva sa - InProgress, Exportované - Exported) > ACSC (Akceptované bankovým systémom)
statusDateTime	dateTime	Nie	Datum prijetí 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 6.2.4.3.

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
<code>response_type</code>	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 <code>auth_code</code> , ktorý TPP následne pomocou ďalšej požiadavky (metódou token) zamení za token <code>access_token</code>
<code>client_id</code>	Áno	String	Jedinečný identifikátor, ktorý banka vygenerovala pre aplikáciu TPP
<code>redirect_uri</code>	Áno	URL	URL kam je na konci presmerované proces autentizácie. Toto URL je stanovené už pri vydaní <code>client_id</code> a v rámci autentizácie je tento parameter validovaný proti URL zavedenému k <code>client_id</code> v zázname aplikácie registrovanej v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrovanej aplikácie.
<code>Scope</code>	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.
<code>state</code>	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>code_challenge</code>	Áno	String	<code>code_challenge = BASE64URL- ENCODE(SHA256(ASCII(code_verifier)))</code> viz. zdroj [3] RFC 7636 (OAuth PKCE)
<code>code_challenge_method</code>	Áno	String	S256
<code>request</code>	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 svojim 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 definované 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
<code>access_token</code>	Áno	string	Krátkodobý token (platnosť tokenu je 3600s), ktorý slúži na autorizáciu requestu na API.
<code>expires_in</code>	Áno	number	Zostávajúci čas do expirácie <code>access_tokenu</code> - v sekundách.
<code>token_type</code>	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: <code>payments/{orderId}/status</code>			
Názov atribútu	Formát	Povinný	Poznámka
<code>orderId</code>	String	Áno	Číslo príkazu vytvoreného v databáze Internetbankingu
<code>reasonCode</code>	String	Nie	V položke sa uvádza informácia o skutočnom statuse, ktorý má 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: <ul style="list-style-type: none"> • RCT (Odmietnuté / Zrušené klientom - Rejected) • PDNG (Autorizované - Authorized) • ACTC (K podpisu - WaitingForSignatures) • ACSP (Zpracováva sa - InProgress, Exportované - Exported) • ACSC (Akceptované bankovním 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 Banking

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 zrežazenie názvu ulice, čísla ulice atď..)
		countryCode	string	Nie	Dvojnakový 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		

2.9.3.8 PISP operácia: Batch payment initialization (XML)

Operácia umožňuje inicializáciu dávky príkazov vo formáte XML (PAIN.001.001.03).

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

Endpoint: POST <https://api.privatbanka.sk/api/v1/payments/batch/iso>

Request

Telo požiadavky obsahuje jednu alebo viacej platieb 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 zadaných príkazov vo formáte xml: pain.002.001.03

Metoda: payments/batch/iso				
Názov atribútu	Výskyt v XML struktuře odpovedi	Formát	Povinný	Poznámka
orderId	GrpHdr/MsgId	String	Áno	Číslo dávky príkazov vytvorené v databáze Internetbankingu.
	OrgnPmtInfAndSts/ TxInfAndSts/StsId	String	Áno	Číslo platby v dávke (toto číslo sa nepoužíva pri autorizácii platby klientom). Pri autorizácii dávky sa používa iba číslo z GrpHdr/MsgId
status	OrgnlGrpInfAndSts/ NbOfTxPerSts/ DtldSts	Enum	Áno	Status spracovania príkazov Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
statusDateTime	GrpHdr/CreDtTm	dateTime	Nie	Dátum prijatia dávky 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		

2.9.3.9 PISP operácia: Trvalý príkaz - periodicity

Operácia poskytuje zoznam kódov periodicít používaných v trvalých príkazov Privatbanky.

Endpoint: GET <https://api.privatbanka.sk/api/v1/standingOrders/Periodicity>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Odpoveď obsahuje dvojicu „code“, „name“. Ak je kódov viac, zobrazí sa viac dvojíc, pričom každá dvojica bude v zložených zátvorkách a oddelená podľa zvyklosti JSON čiarkou.

Metóda: standingOrders/Periodicity			
Názov atribútu	Formát	Povinný	Poznámka
code	String	Áno	Kód periodicity
name	String	Áno	Slovný význam kódu (iba v anglickom jazyku)

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		

2.9.3.9.1 Príklad

Príklad response

```
[
  {
    "code": "0",
    "name": "no periodicity = never"
  },
  {
    "code": "1",
    "name": "monthly maturity"
  }
]
```

2.9.3.10 PISP operácia: Trvalý príkaz - opisy

Prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana opis trvalých príkazov existujúcich k danému bankovému účtu zákazníka.

Endpoint: GET <https://api.privatbanka.sk/api/v1/standingOrders>

Request

Metóda: standingOrders			
Názov atribútu	Formát	Povinný	Poznámka
iban	String (34)	Áno	IBAN účtu, ku ktorému sa majú vrátiť opisy trvalých príkazov

Response

Metóda: standingOrders			
Názov atribútu	Formát	Povinný	Poznámka
	typ: ArrayOfStandingOrder	Áno	Pole opisov trvalých príkazov

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		

2.9.3.10.1 Definícia typu ArrayOfStandingOrder

Metóda: StandingOrders - typ: ArrayOfStandingOrder				
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)	Formát	Povinný	Poznámka	
Id	Numeric	Áno	Identifikátor trvalého príkazu	
Sequence	Integer	Áno	Sekvenčné číslo trvalého príkazu	
standingOrder	typ:StandingOrderDetail	Áno	Parametre trvalého príkazu	
standingOrderState	String	Áno	Status trvalého príkazu Množina stavov trvalého príkazu, ktoré sa môžu vracat' v opise: <ul style="list-style-type: none"> - ACTIVE (aktívny trvalý príkaz) - CANCELLED (zrušený trvalý príkaz) - DISABLED (vyradený trvalý príkaz) - FORMAL_ERROR (trvalý príkaz s formálnou chybou) 	
createDate	dateTime	Áno	Dátum vytvorenia trvalého príkazu	
changeDate	dateTime	Áno	Dátum poslednej zmeny trvalého príkazu	
blockIntervals	typ:StandingOrderBlockInterval	Áno	Pole, v ktorom sa uvádzajú blokácie evidované k danému príkazu	

2.9.3.10.2 Definícia typu StandingOrderDetail

Metóda: StandingOrder - typ: StandingOrderDetail					
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)	Formát	Povinný	Poznámka		
Iban			String	Nie	Iban účtu klienta
partner	name		String	Nie	Meno partnera

	address	street	String	Nie	Adresa - ulica
		city	String	Nie	Adresa - mesto
		country	String	Nie	Adresa - štát
	iban		String	Áno	IBAN príjemcu
	bic		String	Nie	BIC banky príjemcu
	bankName		String	Nie	Meno banky príjemcu
	bankAdress	street	String	Nie	Adresa banky príjemcu - ulica
		city	String	Nie	Adresa banky príjemcu – mesto
		country	String	Nie	Adresa banky príjemcu – štát
currency		String	Áno	Mena	
amount		Numeric	Áno	Čiastka	
periodicity		String	Áno	Kód periodicity – význam tu uvedeného kódu sa zistí z odpovede volania metódy standingOrders/Periodicity	
dayOfPayment		Integer	Áno	Deň vykonávania trvalého príkazu	
failureRetries		Integer	Nie	Počet opakovaní pri neúspešnom pokuse o odoslanie platby	
dateFrom		dateTime	Áno	Platnosť trvalého príkazu OD	
dateTo		dateTime	Áno	Platnosť trvalého príkazu DO	
variableSymbol		String	Nie	Variabilný symbol	
specificSymbol		String	Nie	Špecifický symbol	
constantSymbol		String	Niew	Konštantný symbol	
paymentPurpose		String	Áno	Účel operácie	
noteForBeneficiary		String	Áno	Text pre príjemcu (avízo)	

2.9.3.10.3 Definícia typu StandingOrderBlockInterval

Metóda: StandingOrder - typ: StandingOrderBlock Interval			
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)	Formát	Povinný	Poznámka
Number	Numeric	Áno	Číslo blokácie
dateFrom	DateTime	Áno	Dátum blokácie OD
dateTo	DateTime	Áno	Dátum blokácie Do

2.9.3.10.4 Príklad

Príklad request (body)

```
{
  "iban": "SK6481200000000000123123"
}
```

Príklad response

```
[
  {
    "id": 2216269,
    "sequence": 3,
    "standingOrder": {
      "iban": "SK6481200000000000123123",
      "partner": {
        "name": "Meno partnera",
        "address": {
          "street": null,
          "city": null,
          "country": null
        }
      },
      "iban": "SK30812000000000000272727",
      "bic": "BSLOSK22XXX",
      "bankName": "",
      "bankAddress": {
        "street": null,
        "city": null,
        "country": null
      }
    },
    "currency": "EUR",
    "amount": 250.0000000000,
    "periodicity": "23",
    "dayOfPayment": 15,
    "failureRetries": 4,
  }
]
```

```

    "dateFrom": "0001-01-01T00:00:00",
    "dateTo": "2017-06-20T00:00:00",
    "variableSymbol": "846131161",
    "specificSymbol": "1234567890",
    "constantSymbol": "0008",
    "paymentPurpose": "Účel operácie",
    "noteForBeneficiary": "text avizo "
  },
  "standingOrderState": "CANCELLED",
  "createdDate": "2014-07-01T00:00:00",
  "changedDate": "0001-01-01T00:00:00",
  "blockIntervals": []
}
]

```

2.9.3.11 PISP operácia: Trvalý príkaz – vytvorenie nového

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na vytvorenie nového trvalého príkazu.

Pre autorizáciu žiadosti sa používa resource vid kapitolu 2.8.1.3 a 2.8.1.4.

Endpoint: POST <https://api.privatbanka.sk/api/v1/standingOrders>

Request

Metóda: POST standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
standingOrderData	typ: StandingOrderData	Áno	Parametre trvalého príkazu

Response

Metóda: POST standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	Invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.11.1 Definícia typu StandingOrderData

Metóda: POST StandingOrder - typ: StandingOrderData					
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)			Formát	Povinný	Poznámka
Iban			String	Áno	Iban účtu klienta
partner	name		String	Nie	Meno partnera
	address	street	String	Nie	Adresa - ulica
		city	String	Nie	Adresa - mesto
		country	String	Nie	Adresa - štát
	iban		String	Áno	IBAN príjemcu
	bic		String	Nie	BIC banky príjemcu
	bankName		String	Nie	Meno banky príjemcu
	bankAddress	street	String	Nie	Adresa banky príjemcu - ulica
city		String	Nie	Adresa banky príjemcu – mesto	
country		String	Nie	Adresa banky príjemcu – štát	
currency			String	Áno	Mena
amount			Numeric	Áno	Čiastka
periodicity			String	Áno	Kód periodicity – zoznam povolených kódov je k dispozícii z odpovede volania metódy standingOrders/Periodicity
dayOfPayment			Integer	Áno	Deň vykonávania trvalého príkazu (povolený rozsah 1-31)
failureRetries			Integer	Nie	Počet opakovaní pri neúspešnom pokuse o odoslanie platby (povolený rozsah 0-9)
dateFrom			Date (YYYY-MM-DD)	Áno	Platnosť trvalého príkazu OD (minimálna hodnota – aktuálny deň)
dateTo			Date (YYYY-MM-DD)	Nie	Platnosť trvalého príkazu DO (dátum Platnosť DO nesmie byť menší ako dátum Platnosť OD a musí to byť pracovný deň)
variableSymbol			String	Nie	Variabilný symbol
specificSymbol			String	Nie	Špecifický symbol
constantSymbol			String	Nie	Konštantný symbol

paymentPurpose			String	Nie	Účel operácie
noteForBeneficiary			String	Áno	Text pre príjemcu (avízo)

2.9.3.11.2 Príklad

Príklad request (body)

```
{
  "standingOrderData":
  {
    "iban": "SK6481200000000000123123",
    "partner":
    {
      "name": "Meno partnera",
      "address":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      },
      "iban": "SK30812000000000000272727",
      "bic": "BSLOSK22XXX",
      "bankname": "Meno banky partnera",
      "bankaddress":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      }
    },
    "currency": "EUR",
    "amount": 2.60,
    "periodicity": "51",
    "dayOfPayment": 15,
    "failureRetries": 1,
    "dateFrom": "2019-10-09",
    "dateTo": "2019-10-30",
    "variableSymbol": "1111111111",
    "specificSymbol": "2222222222",
    "constantSymbol": "0968",
    "paymentPurpose": "Poznamka",
    "noteForBeneficiary": "Správa pre príjemcu"
  }
}
```

2.9.3.12 PISP operácia: Trvalý príkaz – zmena

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na zmenu existujúceho trvalého príkazu, ktorý je dohľadaný na základe parametra {Id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitolu 2.9.3.10.

Pre autorizáciu žiadosti sa používa resource viz kapitolu 2.8.1.3 a 2.8.1.4.

Podmienka: Použitie tejto metódy je možné iba za nasledujúcich podmienok:

- atribút {Id} použitý v požiadavke, zodpovedá trvalému príkazu so statusom "ACTIVE"
- k danému trvalému príkazu neexistuje v Internetbankingu nespracovaná žiadosť.

Endpoint: PUT <https://api.privatbanka.sk/api/v1/standingOrders/{Id}>

Request

Metóda: PUT standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
sequence	Integer	Áno	Sekvenčné číslo trvalého príkazu (z opisu trvalého príkazu)
standingOrderData	typ: StandingOrderData	Áno	Parametre zmeny trvalého príkazu

Response

Metóda: PUT standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	Invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.12.1 Definícia typu StandingOrderData

Metóda: PUT StandingOrder / {id} - typ: StandingOrderData					
Názov atribútu (každý stĺpec predstavuje jednu úroveň v JSON štruktúre)			Formát	Povinný	Poznámka
Iban			String	Áno	Iban účtu klienta
partner	name		String	Nie	Meno partnera
	address	street	String	Nie	Adresa - ulica
		city	String	Nie	Adresa - mesto
		country	String	Nie	Adresa - štát
	iban		String	Áno	IBAN príjemcu
	bic		String	Nie	BIC banky príjemcu
	bankName		String	Nie	Meno banky príjemcu
	bankAddress	street	String	Nie	Adresa banky príjemcu - ulica
city		String	Nie	Adresa banky príjemcu – mesto	
country		String	Nie	Adresa banky príjemcu – štát	
currency			String	Áno	Mena
amount			Numeric	Áno	Čiastka
periodicity			String	Áno	Kód periodicity – zoznam povolených kódov je k dispozícii z odpovede volania metódy standingOrders/Periodicity
dayOfPayment			Integer	Áno	Deň vykonávania trvalého príkazu (povolený rozsah 1-31)
failureRetries			Integer	Nie	Počet opakovaní pri neúspešnom pokuse o odoslanie platby (povolený rozsah 0-9)
dateFrom			Date (YYYY-MM-DD)	Áno	Platnosť trvalého príkazu OD (minimálna hodnota – aktuálny deň)
dateTo			Date (YYYY-MM-DD)	Nie	Platnosť trvalého príkazu DO (dátum Platnosť DO nesmie byť menší ako dátum Platnosť OD a musí to byť pracovný deň)
variableSymbol			String	Nie	Variabilný symbol
specificSymbol			String	Nie	Špecifický symbol
constantSymbol			String	Nie	Konštantný symbol

paymentPurpose			String	Nie	Účel operácie
noteForBeneficiary			String	Áno	Text pre príjemcu (avízo)

2.9.3.12.2 Príklad

Príklad request (body)

```
{
  "sequence": 1,
  "standingOrderData": {
    "iban": "SK6481200000000000123123",
    "partner": {
      "name": "Meno partnera",
      "address": {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      },
      "iban": "SK30812000000000000272727",
      "bic": "BSLOS22XXX",
      "bankname": "jméno",
      "bankaddress": {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      }
    },
    "currency": "EUR",
    "amount": 2.60,
    "periodicity": "51",
    "dayOfPayment": 15,
    "failureRetries": 1,
    "dateFrom": "2019-10-09",
    "dateTo": "2019-10-30",
    "variableSymbol": "1111111111",
    "specificSymbol": "2222222222",
    "constantSymbol": "0968",
    "paymentPurpose": "Poznamka",
    "noteForBeneficiary": "Správa pre príjemcu"
  }
}
```

2.9.3.13 PISP operácia: Trvalý príkaz – vyradenie

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na zmenu existujúceho trvalého príkazu, ktorý je dohľadaný na základe parametra {Id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitolu 2.9.3.10.

Pre autorizáciu žiadosti sa používa resource viz kapitolu 2.8.1.3 a 2.8.1.4.

Podmienka: Použitie tejto metódy je možné iba za nasledujúcich podmienok:

- atribút {Id}, použitý v požiadavke, zodpovedá trvalému príkazu so statusom "ACTIVE"
- k danému trvalému príkazu neexistuje v Internetbankingu nespracovaná žiadosť.

Endpoint: DELETE <https://api.privatbanka.sk/api/v1/standingOrders/{id}>

Request

Metóda: DELETE standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
executeDate	Date (YYYY-MM-DD)	Áno	Dátum vykonania zadaný dátum musí spĺňať nasledujúce podmienky: - min dátum: nasledujúci pracovný deň, - zadaná hodnota musí byť pracovný deň

Response

Metóda: DELETE standingOrders/{id}			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	Invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.13.1 Príklad

Príklad request (body)

```
{
  "executeDate": "2019-10-10"
}
```

2.9.3.14 PISP operácia: Trvalý príkaz – blokácia

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na vytvorenie novej blokácie k existujúcemu trvalému príkazu, ktorý je dohľadaný na základe parametra {Id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitulu 2.9.3.10.

Pre autorizáciu žiadosti sa používa resource viz kapitolu 2.8.1.3 a 2.8.1.4.

Podmienka: Použitie tejto metódy je možné iba za nasledujúcich podmienok:

- atribút {Id}, použitý v požiadavke, zodpovedá trvalému príkazu so statusom "ACTIVE"
- k danému trvalému príkazu neexistuje v Internetbankingu nespracovaná žiadosť.

Endpoint: POST <https://api.privatbanka.sk/api/v1/standingOrders/{id}/block>

Request

Metóda:POST standingOrders/{id}/block			
Názov atribútu	Formát	Povinný	Poznámka
suspendedFrom	Date (YYYY-MM-DD)	Áno	Dátum blokácie OD zadaný dátum musí spĺňať nasledujúce podmienky: - min dátum: nasledujúci pracovný deň, - max. dátum: aktuálny deň + 365 - zadaná hodnota musí byť pracovný deň

suspendedTo	Date (YYYY-MM-DD)	Áno	Dátum blokácie DO zadaný dátum musí spĺňať nasledujúce podmienky: - dátum nesmie byť menší ako „Dátum blokácie OD“ - max. dátum: aktuálny deň + 365 - zadaná hodnota musí byť pracovný deň
--------------------	-------------------	-----	--

Response

Metóda: POST standingOrders/{id}/block			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.14.1 Príklad

Príklad request (body)

```
{
  "suspendedFrom": "2019-10-10",
  "suspendedTo": "2019-11-29"
}
```

2.9.3.15 PISP operácia: Trvalý príkaz – deblokácia

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na zrušenie blokácie, ktorá je evidovaná k trvalému príkazu, dohľadaného na základe parametra {id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitulu 2.9.3.10.

Pre autorizáciu žiadosti sa používa resource viz kapitolu 2.8.1.3 a 2.8.1.4.

Podmienka: Použitie tejto metódy je možné iba za nasledujúcich podmienok:

- atribút {id}, použitý v požiadavke, zodpovedá trvalému príkazu so statusom "ACTIVE"
- číslo blokácie, uvedené v žiadosti, je evidované k danému trvalému príkazu (sekvenčné číslo blokácie sa uvádza v opise trvalého príkazu v sekcii "blockIntervals")
- k danému trvalému príkazu neexistuje v Internetbankingu nespracovaná žiadosť.

Endpoint: POST <https://api.privatbanka.sk/api/v1/standingOrders/{id}/unblock>

Request

Metóda: POST standingOrders/{id}/unblock			
Názov atribútu	Formát	Povinný	Poznámka
blockIntervalNumber	Integer	Áno	Číslo blokácie, uvedené v opise trvalého príkazu v sekcii „blockIntervals“ v položke „number“
executeIn	Date (YYYY-MM-DD)	Áno	Požadovaný dátum vykonania zadaný dátum musí spĺňať nasledujúce podmienky: - min dátum: nasledujúci pracovný deň, - zadaná hodnota musí byť pracovný deň
suspendedFrom	Date (YYYY-MM-DD)	Áno	Dátum blokácie OD (dátum uvedené v opise trvalého príkazu v sekcii „blockIntervals“ v položke „dateFrom“)
suspendedTo	Date (YYYY-MM-DD)	Áno	Dátum blokácie DO (dátum uvedené v opise trvalého príkazu v sekcii „blockIntervals“ v položke „dateTo“)

Response

Metóda: POST standingOrders/{id}/unblock			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	Invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.15.1 Príklad

Príklad request (body)

```
{
  "blockIntervalNumber": 1,
  "executeIn": "2019-10-09",
  "suspendedFrom": "2019-10-05",
  "suspendedTo": "2019-10-04"
}
```

2.9.3.16 PISP operácia: Trvalý príkaz – obnova

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky uloží žiadosť pod špecifickým orderId na obnovenie vyradeného trvalého príkazu, dohľadaného na základe parametra {id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitolu 2.9.3.10.

Pre autorizáciu žiadosti sa používa resource viz kapitolu 2.8.1.3 a 2.8.1.4.

Podmienka: Použitie tejto metódy je možné iba za nasledujúcich podmienok:

- atribút {id}, použitý v požiadavke, zodpovedá trvalému príkazu so statusom "DISABLED"
- k danému trvalému príkazu neexistuje v Internetbankingu nespracovaná žiadosť.

Endpoint: POST <https://api.privatbanka.sk/api/v1/standingOrders/{id}/renew>

Request

Metóda:POST standingOrders/{id}/renew			
Názov atribútu	Formát	Povinný	Poznámka
executeIn	Date (YYYY-MM-DD)	Áno	Požadovaný dátum vykonania žiadosti zadaný dátum musí spĺňať nasledujúce podmienky: - min dátum: nasledujúci pracovný deň, - zadaná hodnota musí byť pracovný deň

Response

Metóda: POST standingOrders/{id}/renew			
Názov atribútu	Formát	Povinný	Poznámka
id	Numeric	Áno	Číslo, pod ktorým sa žiadosť uložila do databázy Internetbankingu
status	Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate	dateTime	Áno	Dátum prijatia žiadosti do banky

Chybové kódy		
HTTP Status	Error kód	Popis
400	parameter_missing	Chýba povinný parameter.
400	Invalid_request	Nevalidná požiadavka (popis chyby uvedený v položke error_description)
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		

2.9.3.16.1 Príklad

Príklad request (Body)

```
{
  "executeIn": "2019-10-10"
}
```

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 dohľadovaný 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
<code>/api/v1/accounts/balanceCheck</code>	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 riešenie (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	Nie	Adresa obchodníka (obvykle obsahuje zreženie názvu ulice, čísla ulice atď..)	
		countryCode	Nie	Dvojnakový 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