

Slovenská záručná a rozvojová banka, a. s.
PSD2 – INFORMÁCIA
PRE TRETIE STRANY_v4

História zmien

Verzia dokumentu	Dátum platnosti	Popis zmien v dokumente
API PSD2 v SZRB_v2	Júl 2022	núdzové zmeny: doplnená kapitola 3: JWT token, Príklady http (request / response), zmena portu 98
API PSD2 v SZRB_v3	Október 2022	Dátum „Platnosť DO“ vydaného súhlasu – zrušenie poľa na zadanie.
API PSD2 v SZRB_v4	1.2.2023	<ul style="list-style-type: none">- PISP: nové kapitoly týkajúce sa správy trvalých príkazov,- PISP: Nová kapitola 2.9.3.8 - Payment initialization (JSON) – vytvorenie platby- správanie autorizačnej stránky na strane banky pri autorizácii platby disponentom, ak platba inciovaná treťou stranou neobsahuje účet platiteľa- súhlasy: nové kapitoly týkajúce sa súhlasov

Obsah

1. Úvod	5
1.1 Terminológia	5
2. Bezpečnostný model	6
2.1 Šifrovaná komunikácia TPP-Banka.....	6
2.2 Registrácia TPP v banke.....	7
2.3 Súhlas s prístupom TPP k účtom disponenta	7
2.3.1 Súhlasy – podporované typy.....	7
2.3.2 Súhlas použitý pri aktivačnom workflow	8
2.3.3 Súhlas - obsah.....	8
2.4 Popis riešenia.....	9
2.4.1 Hlavné vlastnosti API.....	9
2.4.2 Popis workflow – nastavenie prístupu TPP k účtom disponenta.....	10
2.4.3 E-Banking.....	12
2.5 Služby podporované v API PSD2	14
2.5.1 Metódy pre automatickú registráciu aplikácie TPP cez API	15
2.5.2 Metódy oblasti AISP	15
2.5.3 Metódy oblasti PISP	15
2.5.4 Metódy oblasti PIISP	17
2.5.5 Metódy pre správu súhlasu cez API	17
2.6 Endpointy použité pre API PSD2	17
2.6.1 Endpointy pre OAuth (autorizácia klienta, autorizácia platby klientom, vydávanie tokenov).....	18
2.6.2 Endpointy pre PSD2 API (registračné resource (Enrollment), volanie metód AISP, PISP, PIISP)	18
2.7 Registračné resource vystavené bankou (Enrollment).....	21
2.7.1 Automatické generovanie technických identifikátorov	22
2.7.2 Zmena registračných údajov	25
2.7.3 Zmazanie aplikácie	27
2.7.4 Žiadosť o nový client_secret.....	28
2.8 Autentizácia a Autorizácia requestu (OAuth2)	29

2.8.1 OAuth2 Authorization Code Grant	29
2.9 Popis metód používaných pre poskytovateľov služieb (TPP).....	35
2.9.1 Všeobecná definícia hlavičky požiadavky	35
2.9.2 Služba AISP (Dotazy k účtom, prehľad transakcií)	36
2.9.3 Služby PISP (Vytvorenie platby, zisťovanie stavu platby, autorizácia platby, zrušenie platby)	45
2.9.4 Služba PIISP (Overenie dostatočných prostriedkov na účte)	73
2.9.5 Súhlasy – správa cez PSD2 API.....	77
3. Prílohy	95
3.1 JWT token	95
3.1.1 Príklad obsahu JWT tokenu	95
3.1.2 Príklad vypočítaného tokenu JWT použitého do request	95
3.1.3 Popis parametrov použitých v JWT	95
3.2 Príklady http (request / response).....	97
3.2.1 (api/enroll) Registračné resource	97
3.2.2 (auth/oauth) Autentizácia a Autorizácia requestu	101
3.2.3 (api/) AISP	103
3.2.4 (api/) PISP	108
3.2.5 (api/) PIISP	124
3.2.6 (api/) Súhlasy	125
4. Zdroje.....	130

1. Úvod

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 SSL protokolu s minimálne 128 bitovým šifrovaním.

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

1.1 Terminológia

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

SBAS – Skratka pre Slovak Banking API Standard.

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

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

AISP - Account Information Service – poskytovateľ služby informovania o platobnom účte - na základe súhlasu klienta 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 – 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
- overiť či má klient na bankovom účte dostatok prostriedkov na zrealizovanie transakcie

PIISP - Payment Instrument Issuer Service Provider – poskytovateľ platobných služieb vydávajúci platobný nástroj (platobnú kartu). TPP si potom 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.

SZRB – Skratka pre banku Slovenská záručná a rozvojová banka, a. s.

Internet Banking - Platforma elektronického bankovníctva, prevádzkovaného v SZRB.

PSD2 - Podpora PSD2 funkcionalít.

2. Bezpečnostný model

Základný bezpečnostný model pre prístup k API je založený na kombinácii nižšie uvedených bezpečnostných prvkov (aby TPP mohla posielat požiadavky cez API týkajúce sa účtu / účtov klienta banky, 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 (Internet Banking)
- Registrovaná aplikácia TPP v banke (s jedinečným client_id a client_secret)
- Existencia platného súhlasu s definovaným prístupom aplikácie TPP k účtom disponenta
- Platný access token (naviazaný na špecifický súhlas, vytvorený disponentom) uvádzaný v hlavičke zaslanej požiadavky cez API

2.1 Šifrovaná komunikácia TPP-Banka

Komunikácia medzi klientskym systémom a bankou predpokladá zabezpečenie pomocou SSL protokolu s minimálne 128 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 registračné flow v banke.

Pri registračnom flow 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 flow s použitím OAuth 2.0.

2.3 Súhlas s prístupom TPP k účtom disponenta

Ďalšou podmienkou, ktorá musí byť splnená, aby TPP mohla zasielať požiadavky cez API, je existujúci platný súhlas prístupu aplikácie TPP k účtom disponenta.

2.3.1 Súhlasy – podporované typy

Banka podporuje vo svojom riešení nasledujúce typy súhlasov:

Typ súhlasu	Operácie povolené pri správe daného typu súhlasu v eBankingu	Popis
Bank offered consent (Parametrizovaný disponentom na strane banky)	<ul style="list-style-type: none"> › Zmena súhlasu › Ukončenie súhlasu 	Typ súhlasu, ktorý je vytvorený a parametrizovaný disponentom na strane banky. Tento typ súhlasu: <ul style="list-style-type: none"> - vzniká pri workflow aktivácie prístupu disponenta cez aplikáciu TPP - môže disponent vytvoriť priamo v Internet Bankingu (v sekcii Nastavenia – PSD2 – Zadanie nového súhlasu) - alebo môže vzniknúť na základe volania metódy /v1/consents/BankOffered (kapitola 2.9.5.5) prostredníctvom rozhraní API PSD2
Global consent (globálny)	Ukončenie súhlasu	Typ súhlasu, ktorý vzniká iba na základe požiadavky prijatej cez API PSD2 prostredníctvom volania metódy /v1/consents/global – tretej strane týmto typom súhlasu bude umožnené: <ul style="list-style-type: none"> - pracovať so všetkými bežnými účtami disponenta, ku ktorým má disponent v elektronickom bankovníctve nastavený aktívny prístup - používať služby ktoré odpovedajú prieniku <ul style="list-style-type: none"> o služieb, ktoré má TPP registrované vo svojej licencií v NBS o služieb, ktoré si TPP zaregistrovala v banke pre svoju aplikáciu
Detailed Consent (Parametrizovaný cez PSD2 API – cez aplikáciu TPP)	Ukončenie súhlasu	Typ súhlasu, ktorý vzniká iba na základe požiadavky prijatej cez API PSD2 prostredníctvom metódy /v1/consents/detailed . <ul style="list-style-type: none"> - Parametre súhlasu sú uvedené v tele prijatej požiadavky.

2.3.2 Súhlas použitý pri aktivačnom workflow

Ak neexistuje platný súhlas, riešenie PSD2 umožňuje disponentovi vytvoriť pri aktivačnom workflow žiadosť na vytvorenie súhlasu typu Bank Offered, ktorá sa disponentovi zobrazí po jeho presmerovaní na stranu banky z aplikácie TPP a jeho silnej autorizácii.

V žiadosti sú implicitne označené (povolené):

- všetky bežné účty, ku ktorým má daný disponent nastavený v banke aktívny prístup (účet sa v súhlase ponúka len vtedy, ak má disponent vo väzbe na klienta, ktorý je majiteľom účtu, povolenú v banke službu PSD2).
- všetky služby, ktoré sú evidované v zázname tretej strany registrované v databáze Internet Banking (okrem služby PIISP)

Disponent potom môže upraviť označenie položiek podľa svojich preferencií. Pre potvrdenie nastavených parametrov disponent iba stlačí tlačidlo „Uložiť“ (žiadosť už neautorizuje svojím autentizačným zariadením) a následne je presmerovaný späť do aplikácie TPP.

Na základe parametrov nastavených disponentom v tejto žiadosti vznikne súhlas typu Bank Offered s požadovanými parametrami.

Ak disponent žiadosť na súhlas typu Bank Offered vytvára priamo z prostredia Internet Banking, autorizuje ju svojím autentizačným zariadením.

2.3.3 Súhlas - obsah

Súčasťou uloženého súhlasu sú položky:

- Typ súhlasu
- Aplikácia TPP, pre ktorú tento súhlas vznikol
- Zoznam oprávnenia k službám (AISP, PISP, PIISP), ktoré sú povolené pre používanie aplikácie TPP vo väzbe na daného disponenta
 - ak sa jedná o súhlas typu Global Consent, sú implicitne povolené služby AISP a PISP.
 - ak sa jedná o súhlas typu Bank Offered Consent, sú v súhlase povolené iba služby, ktoré v žiadosti o súhlas povolil disponent (na strane banky)
 - ak sa jedná o súhlas typu Detailed Consent, sú v súhlase povolené iba služby, ktoré boli definované v požiadavke prijaté cez API PSD2 (cez metódu „Vytvorenie žiadosti o súhlas typu Detailed Consent“ – pozrite kapitolu 2.9.5.6)

- Zoznam účtov, ku ktorým je povolený prístup (táto informácia sa do súhlasu ukladá iba v prípade súhlasu typu Bank Offered Consent a Detailed Consent). Pre súhlas typu Global Consent sa účet použitý v AISP alebo PISP požiadavke validuje dynamicky proti účtom disponenta, ktoré má disponent k dispozícii v Internet Banking v okamihu prijatia požiadavky cez PSD2 API rozhranie.
- Dátum „Platnosť DO“ vydaného súhlasu (táto položka sa používa iba v prípade, ak disponent vykoná operáciu „Ukončenie súhlasu“ – do položky sa uloží dátum vykonania operácie). Súhlas je potom v databáze Internet Banking vedený ako neplatný.

2.4 Popis riešenia

2.4.1 Hlavné vlastnosti API

- API rozhranie podporuje všetky mandatórne služby v rámci SBAS a nemandatórnu službu „Account list“ a „Cancel payment“
- 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 flow 1 .. 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 dohľadný v banke v zoznamu TPP - identické číslo licencie musí byť uvedené v certifikátu aj v zázname TPP v banke,
 - dohľadný 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 dohľadaný platný súhlas,
 - ak je v tele požiadavky uvedený účet, musí byť tento účet obsiahnutý v súhlase, ktorý bol dohľadaný na základe access tokenu (uvedeného v hlavičke požiadavky),

- aplikácia TPP má v dohľadanom súhlasu povolenú od disponenta 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 kapitolu 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 vydanéj národným regulátorom a certifikátu daného subjektu (ID licencie, uvedené v certifikáte, ktorý TPP používa pri komunikácii cez PSD2 API vystavenej bankou, musí byť obsažené 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 tajnej časti) s potrebnými dokladmi, na základe ktorých pracovník banky overí a dohľadá danú TPP v databáze IB.
 - Po manuálnom overení pracovník banky doplnia do databázy IB do záznamu TPP chýbajúce ID licencie (použitie 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 flow 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 jednorazového 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)
- Od okamihu vygenerovanie technických bezpečnostných prvkov sa názov zaregistrované aplikácie TPP bude ponúkať klientom banky (disponentom) pri vytváraní súhlasov pre prístup TPP k účtom.

2.4.2.1 Postup vytvorenia súhlasu (udelenie prístupu pre TPP) disponentom

- Nasledujú kroky, ktoré musí vykonať disponent.

- Aby mohla TPP zasielať dotazy cez API na účty disponenta alebo vytvárať za disponenta platbu, musí k tomu dať disponent súhlas.
- Disponent klienta banky podpíše zmluvu s TPP.
- Disponent môže súhlas o prístup tretej strany k svojim bežným účtom vytvoriť dvoma spôsobmi:
 - z prostredia Internetbankingu
 - cez Centrálnu autorizačnú stránku, na ktorú je presmerovaný pri aktivácii PSD2 prístupu cez aplikáciu tretej strany.

- Ak je aplikácia tretej strany už zaregistrovaná v banke, disponent klienta banky **sa môže štandardným spôsobom prihlásiť do IB** a v sekcii PSD2 vytvoriť a autorizovať žiadosť o vytvorenie súhlasu typu Bank Offered Consent pre prístup špecifickej aplikácie TPP k svojim bežným účtom. **V žiadosti sú implicitne povolené:**

- **všetky bežné účty, ku ktorým má daný disponent v okamihu zobrazenia žiadosti o súhlas nastavený v banke aktívny prístup (účet sa v súhlase ponúka len vtedy, ak má disponent vo väzbe na klienta, ktorý je majiteľom účtu, povolenú v banke službu PSD2)**
- **všetky služby TPP (okrem služby pre PIISP), ktoré sú evidované v zázname TPP registrované v databáze Internet Banking.**

Služba pre PIISP nie je v žiadosti o súhlas implicitne povolená. Túto službu musí disponent v žiadosti manuálne povoliť. V prípade, že disponent službu pre PIISP nepovolí pri aktivácii súhlasu, môže ju dodatočne povoliť v internetbankingu editáciou súhlasu.

- Disponent žiadosť o súhlas autorizuje svojim autorizačným zariadením.
- 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 registračný workflow.
- Klient je po spustení registračného flow 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 IB skontroluje, či pre danú TPP aplikáciu a práve prihláseného disponenta existuje platný súhlas (súhlas vytvorený na základe žiadosti z Internet Banking alebo z Centrálnej autorizačnej stránky).**
- **Ak platný súhlas nie je dohľadný**
 - zobrazí sa stránka, ktorá obsahuje položky žiadosti o súhlas typu Bank Offered Consent., v ktorej sú implicitne povolené:
 - všetky **bežné** účty, ku ktorým má disponent v okamihu, keď sa zobrazí formulár žiadosti o súhlas, nastavený v banke aktívny prístup
 - všetky služby (okrem služby pre PIISP), ktoré sú evidované v zázname tretej strany registrované v

databáze Internet Banking.

Služba pre PIISP nie je v žiadosti o súhlas implicitne povolená. Túto službu musí disponent v žiadosti manuálne povoliť. V prípade, že disponent službu pre PIISP nepovolí pri aktivácii súhlasu, môže ju dodatočne povoliť v internetbankingu editáciou súhlasu. Disponent potom žiadosť o súhlas potvrdí (použije tlačidlo „Uložiť“).

- V odpovedi protokole OAuth získa TPP 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.
- **Ak v IB pre danú aplikáciu TPP existuje platný súhlas vytvorený disponentom**
 - v odpovedi protokole OAuth získa TPP 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. Vnútrobankovné systémy následne budú žiadať o overenie platnosti tokenu a získanie príslušného scope (AIS / PIS / PIIS) a príslušné užívateľské identity, ku ktorej token patrí.

2.4.3 E-Banking

2.4.3.1 Prehľad „Prehľad súhlasov“

Ak používateľ vyberie ponuku "Prehľad súhlasov", zobrazí sa prehľad všetkých aktívnych súhlasov, ktoré vznikli na základe žiadostí o udelenie prístupu pre TPP, ktorý prihlásený používateľ vytvoril.

Štruktúra prehľadu - prehľad obsahuje nasledujúce stĺpce:

Názov stĺpca	Popis
Tretia strana	Názov tretej strany, na ktorú je registrovaná aplikácia TPP, ktorú disponent uviedol v žiadosti
Aplikácia tretej strany	Názov aplikácie tretej strany, ktorú disponent uviedol v žiadosti
Typ súhlasu	Typ súhlasu (pozri kapitolu 2.3.1)
Povolené služby	Množina služieb (AISP, PISP, PIISP), ktoré disponent povolil na užívanie pre tretiu stranu

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

2.4.3.2 Detail súhlasu typu Bank Offered

Názov položky	Popis
Typ súhlasu	Typ súhlasu (pozri kapitolu 2.3.1)
Meno tretej strany	Meno TPP, na ktorú je registrovaná aplikácia TPP, pre ktorú disponent povolil prístup k svojim účtom.

Názov položky	Popis
Aplikácia tretej strany	Meno aplikácie TPP, pre ktorú disponent povolil prístup k svojim účtom.
Služby	Množina služieb, ktoré disponent nastavil do žiadosti o povolenie prístupu pre TPP. V súhlase sa zobrazujú služby: <ul style="list-style-type: none"> • AISP (Zoznam účtov povolených pre TPP, Otázka na zostatok účtu, Prehľad transakcií) • PISP (Vytvorenie platby, Stav spracovania príkazu v banke, Autorizácia platby, Overenie dostatočných prostriedkov na účte, Zrušenie platby) • PIISP (Overenie dostatočných prostriedkov na účte)
Účty	Zoznam účtov, ktoré disponent v žiadosti o povolenie prístupu pre TPP povolil.

Pod detailom sú zobrazené tlačidlá – pozri kapitolu (2.4.3.5)

2.4.3.3 Detail súhlasu typu Global Consent

Názov položky	Popis
Typ súhlasu	Typ súhlasu (pozri kapitolu 2.3.1)
Meno tretej strany	Meno TPP, na ktorú je registrovaná aplikácia TPP, pre ktorú disponent povolil prístup k svojim účtom.
Aplikácia tretej strany	Meno aplikácie TPP, pre ktorú disponent povolil prístup k svojim účtom.
Služby	V súhlase sa zobrazujú služby: <ul style="list-style-type: none"> • AISP (Zoznam účtov povolených pre TPP, Otázka na zostatok účtu, Prehľad transakcií) • PISP (Vytvorenie platby, Stav spracovania príkazu v banke, Autorizácia platby, Overenie dostatočných prostriedkov na účte, Zrušenie platby)
Účty	Je zobrazený nasledujúci text: „Všetky bežné účty, ku ktorým má disponent aktívny prístup“.

Pod detailom sú zobrazené tlačidlá – pozri kapitolu (**Chyba! Nenašiel sa žiaden zdroj odkazov.**)

2.4.3.4 Detail súhlasu typu Detailed

Názov položky	Popis
Typ súhlasu	Typ súhlasu (pozrite kapitolu 2.3.1)
Meno tretej strany	Meno TPP, na ktorú je registrovaná aplikácia TPP, pre ktorú disponent povolil prístup k svojim účtom.
Aplikácia tretej strany	Meno aplikácie TPP, pre ktorú disponent povolil prístup k svojim účtom.
Služby	<p>Množina služieb, ktoré boli uvedené v prijatej žiadosti o povolenie prístupu pre TPP v aplikácii TPP (žiadosť prijatá cez PSD2 API).</p> <p>V súhlase sa zobrazujú služby z nasledujúcej skupiny:</p> <ul style="list-style-type: none"> • AISP (Zoznam účtov povolených pre TPP, Otázka na zostatok účtu, Prehľad transakcií) • PISP (Vytvorenie platby, Stav spracovania príkazu v banke, Autorizácia platby, Overenie dostatočných prostriedkov na účte, Zrušenie platby) • PIISP (Overenie dostatočných prostriedkov na účte)
Účty	Zoznam účtov, ktoré boli uvedené v žiadosti o povolenie prístupu pre TPP.

Pod detailom sú zobrazené tlačidlá – pozri kapitolu (**Chyba! Nenašiel sa žiaden zdroj odkazov.**)

2.4.3.5 Ovládacie prvky v detaile AKTÍVNEHO SÚHLASU

V detaile každého **aktívneho** súhlasu sa užívateľovi ponúkajú tlačidlá:

Tlačidlo	Zobrazuje sa detail nasledujúceho typu súhlasu	Popis
Žiadosť o ukončenie	<ul style="list-style-type: none"> › Bank Offered › Global › Detailed 	po stlačení tlačidla sa vytvorí žiadosť o ukončenie platnosti súhlasu
Žiadosť o zmenu	Bank Offered	po stlačení tlačidla sa vytvorí nová žiadosť o udelenie prístupu, ktorá v sebe bude mať predvyplnené údaje súhlasu, z ktorého je zmena vykonávaná.

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

2.5.2 Metódy oblasti AISP

Metóda služby	Popis
AccountInformation (JSON)	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad zostatkov bankového účtu disponenta vedeného v banke
AccountTransaction (JSON)	prostredníctvom tejto služby dostane disponentom autorizovaná tretia strana prehľad transakcií
AccountList (JSON)	služba na požiadavku vráti zoznam účtov, ktoré disponent uviedol v súhlase na používanie s konkrétnym TPP (nie zoznam všetkých klientskych účtov) bez zostatkov

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 alebo zahraničný 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>

Metóda služby	Popis
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)
Payment initialization (JSON) – vytvorenie platby	Na základe tejto požiadavky disponentom autorizovaná tretia strana iniciuje (vytvorí) jeden príkaz typu SEPA alebo zahraničnú platbu. 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 – zrušenie	Na základe tejto požiadavky sa vytvorí žiadosť na zrušenie 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.

2.5.4 Metódy oblasti PIISP

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

2.5.5 Metódy pre správu súhlasu cez API

Metóda služby	Popis
Vytvorenie žiadosti o súhlas typu Global Consent (JSON)	prostredníctvom tejto služby TPP s platným certifikátom a licenčným číslom žiada o úplný prístup k všetkým bankovým účtom disponenta a službám dostupným prostredníctvom rozhrania PSD2. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
Vytvorenie žiadosti o súhlas typu Bank Offered Consent (JSON)	prostredníctvom tejto služby TPP s platným certifikátom a licenčným číslom žiada o vytvorenie súhlasu typu Bank Offered Consent – v tomto type súhlasu je rozsah prístupu k účtom a službám (AISP, PISP) pre TPP definovaný disponentom až po presmerovaní a silnej autentifikácii disponenta na strane banky. Disponent môže žiadosť po zobrazení upraviť a následne potvrdiť alebo zamietnuť.
Vytvorenie žiadosti o súhlas typu Detailed Consent (JSON)	prostredníctvom tejto služby TPP s platným certifikátom a licenčným číslom žiada o vytvorenie súhlasu typu Detailed Consent – v tomto type súhlasu je rozsah prístupu k účtom a službám definovaný priamo v tele požiadavky prijatej cez PSD2 API rozhranie. Žiadosť o súhlas s predvyplnenými parametrami (účty a služby, ktoré TPP poslala v požiadavke) sa disponentovi zobrazí po jeho presmerovaní z aplikácie TPP a vykonaní silnej autentifikácie na strane banky. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
Ukončenie súhlasu	Ukončenie platnosti aktívneho súhlasu
Potvrdenie žiadosti o súhlas (JSON)	autorizácia žiadosti o súhlas treťou stranou, (daná žiadosť musí byť iniciovaná touto treťou stranou)

2.6 Endpointy použité pre API PSD2

Banka v rámci riešenia PSD2 prevádzkuje dve prostredia:

- › Testovacie prostredie - určené pre vývojárov TPP; na tomto prostredí TPP môže vykonávať testy svojich vyvinutých aplikácií.
- › Produkčné prostredie - TPP sa môže pripojiť k tomuto prostrediu po otestovaní svojej aplikácie na testovacom prostredí.

Prístup do požadovaného prostredia (testovacie alebo produkčné) je TPP umožnený na základe workflow opísaného v kapitole 2.4.2.

Každé prostredie je prevádzkované na konkrétnej Root URL adrese vid' nasledujúca tabuľka.

Prostredie	Root URL	Popis
Produkčné prostredie	https://api.szrb.sk:98	V dokumente je táto root URL adresa primárne uvádzaná vo všetkých endpointoch.
Testovacie prostredie	https://apitest.szrb.sk:98	Ak chce TPP použiť testovacie PSD2 API dostupné na strane banky, použije sa v popisovaných Endpointoch namiesto koreňovej adresy https://api.szrb.sk:98 adresa pre testovacie prostredie (https://apitest.szrb.sk:98)

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

Endpoint	Typ metódy	Popis
https://api.szrb.sk:98/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.szrb.sk:98/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.szrb.sk:98/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.szrb.sk:98/api/enroll/{client_id}	PUT	Zavolaním tohto resource môže TPP požiadať o zmenu registračných údajov pre konkrétnu aplikáciu.
https://api.szrb.sk:98/api/enroll/{client_id}	DELETE	Zavolaním tohto resource môže TPP požiadať o zrušenie registrácie konkrétnej aplikácie.
https://api.szrb.sk:98/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.szrb.sk:98/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.szrb.sk:98/api/v1/accounts/transactions	POST	Endpoint pre metódu, prostredníctvom ktorej dostane disponentom autorizovaná tretia strana prehľad transakcií
https://api.szrb.sk:98/api/v2/accounts	GET	Endpoint pre metódu, ktorá na požiadanie vráti zoznam účtov, ktoré disponent uviedol v súhlase k používaniu s konkrétnym TPP (nie zoznam všetkých účtov disponenta) bez zostatkov

2.6.2.3 PISP

Endpoint	Typ metódy	Popis
https://api.szrb.sk:98/api/v1/payments/standard/iso	POST	Endpoint pre metódu Standard payment initialization (XML) - disponentom autorizovaná tretia strana iniciuje (vytvorí) jeden SEPA alebo zahraničný príkaz z bankového účtu disponenta.
https://api.szrb.sk:98/api/v1/payments/submission	POST	Endpoint pre metódu Standard payment submission - autorizácia platby tretou stranou (platbu predtým musí povoliť svojou autorizáciou disponent).
https://api.szrb.sk:98/api/v1/payments/{orderId}/status	GET	Endpoint pre metódu Payment order status - zisťovanie stavu platobného príkazu
https://api.szrb.sk:98/api/v1/payments/{orderId}/rpc	DELETE	Endpoint pre metódu Cancel payment - zrušenie platby, ktorá ešte nebola autorizovaná tretou stranou (tretia strana nepoužila metódu "Standard payment submission") a ktorá bola vytvorená prostredníctvom služby PISP Standard payment initialization (XML)
https://api.szrb.sk:98/api/v1/accounts/balanceCheck	POST	Endpoint pre metódu Balance check - overenie, či má klient na bankovom účte dostatok prostriedkov na zrealizovanie transakcie
https://api.szrb.sk:98/api/v1/payments	POST	Endpoint pre metódu Payment initialization (JSON) - vytvorenie platby
https://api.szrb.sk:98/api/v1/standingOrders/Periodicity	GET	Endpoint pre metódu Trvalý príkaz - periodicity - žiadosť o zoznam kódov periodicít, ktoré sú povolené v trvalých príkazoch
https://api.szrb.sk:98/api/v1/standingOrders	GET	Endpoint pre metódu Trvalý príkaz - opisy - žiadosť o opisy trvalých príkazov

Endpoint	Typ metódy	Popis
https://api.szrb.sk:98/api/v1/standingOrders	POST	Endpoint pre metódu Trvalý príkaz – vytvorenie – žiadosť o vytvorenie nového trvalého príkazu
https://api.szrb.sk:98/api/v1/standingOrders/{id}	PUT	Endpoint pre metódu Trvalý príkaz – zmena – žiadosť o zmenu existujúceho trvalého príkazu
https://api.szrb.sk:98/api/v1/standingOrders/{id}	DELETE	Endpoint pre metódu Trvalý príkaz – zrušenie – žiadosť o zrušenie existujúceho trvalého príkazu

2.6.2.4 PIISP

Endpoint	Typ metódy	Popis
https://api.szrb.sk:98/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

2.6.2.5 Consents (správa súhlasov cez PSD2 API)

Endpoint	Typ metódy	Popis
https://api.szrb.sk:98/api/v1/consents/global	POST	Endpoint pre metódu, prostredníctvom ktorej aplikácia TPP žiada o úplný prístup k všetkým bankovým účtom disponenta a službám dostupným prostredníctvom rozhrania PSD2. Žiadosť o súhlas sa disponentovi zobrazí po jeho presmerovaní z aplikácie TPP a vykonaní silnej autentifikácie na strane banky. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
https://api.szrb.sk:98/api/v1/consents/bankOffered	POST	Endpoint pre metódu, prostredníctvom ktorej aplikácia TPP žiada o vytvorenie súhlasu typu Bank Offered Consent – v tomto type súhlasu rozsah prístupu k účtom a službám (AISP, PISP) pre TPP je definovaný disponentom až po presmerovaní a silnej autentifikácii disponenta na strane banky . Disponent môže žiadosť po zobrazení upraviť a potvrdiť alebo zamietnuť.
https://api.szrb.sk:98/api/v1/consents/detailed	POST	Endpoint pre metódu, prostredníctvom ktorej aplikácia TPP žiada o vytvorenie súhlasu typu Detailed Consent – v tomto type súhlasu je rozsah prístupu k účtom a službám definovaný priamo v tele požiadavky prijatej cez PSD2 API rozhranie .. Žiadosť o súhlas s predvyplnenými parametrami (účty a služby, ktoré boli uvedené v požiadavke) sa disponentovi zobrazí po jeho presmerovaní z aplikácie TPP a vykonaní silnej autentifikácie na strane banky. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
https://api.szrb.sk:98/api/v1/consents/submission	POST	Endpoint pre metódu Potvrdenie žiadosti o súhlas (Request of consent submission) – autorizácia žiadosti o súhlas tretou stranou (žiadosť predtým musí povoliť disponent).
https://api.szrb.sk:98/api/v1/consents/terminate	POST	Endpoint pre metódu Ukončenie súhlasu (JSON) – ukončenie aktívneho súhlasu

2.7 Registračné resource vystavené 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.

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/enroll>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/enroll>

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

Response			
Atribut	Povinný	Typ	Popis
<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 vydený bankou (ASPSP) pre TPP aplikácii (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 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 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			
licence_number	Áno	String [Max 1024 B]	Licenčné číslo, ktoré má TPP pridelené od národného regulátora. Licenčné číslo je validované proti licenčnému číslu uvedenému v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Chybové kódy		
HTTP Status	Error kód	Popis
400	invalid_request	Nevalidný request. V dotazu 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 validný
401	invalid_client	Nevalidný client_id.
401	unauthorized_client	TPP nie je oprávnený vykonávať tento dotaz.
401	access_denied	Autorizačný server odmietol prístup.
403	insufficient_scope	Napr. nedostatočné oprávnenia pre použitie požadovaného scope
500, 503	server_error	Chyba autorizačného servera.

Príklad použitia vid' zdroj kapitola 3.2.1.1.

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.

Testovacie prostredie

Endpoint: PUT https://apitest.szrb.sk:98/api/enroll/{client_id}

Produkčné prostredie

Endpoint: PUT https://api.szrb.sk:98/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 flow autentizácie na konci presmerované. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.
logo_uri	Nie	URI [Max 2047 B]	URI loga aplikácie (resp. Miesto odkiaľ je možné ho pri registrácii stiahnuť)
contacts	Áno	Array of strings e-mail [Max 10x 255 B]	Zoznam E-mail adries, kontakty na zodpovednú osobu na strane TPP aplikácie.
scopes	Nie	Array of strings [Max 10x 255 B]	Pole požadovaných Scopes pre aplikáciu. Pri registrácii sú Scopes validované proti obsahu použitého certifikátu a proti Scopes uvedených v zázname TPP, ktorý v tom čase už musí existovať v databáze IB.

Response			
Atribut	Povinný	Typ	Popis
client_id	Áno	String	client_id priradené aplikácii bankou.
client_secret_expires_at	Nie	DateTime	Defaultná hodnota je 0 (client_id nikdy neexpirujú). V opačnom prípade je uvedená hodnota v sekundách od dátumu 1970-01-01T0:0:0Z
redirect_uris	Áno	Array of strings e.g. URL [Max 3x 2047 B]	Zoznam URL kam môže byť flow autentizácie na konci presmerované. Autorizačný request musí obsahovať práve jedno z týchto registrovaných URI v presnom formáte.
client_name	Áno	String [Max 255 B]	Meno TPP aplikácie
client_name#en-US	Nie	String [Max 1024 B]	Meno TPP aplikácie v príslušnom jazyku / kódovanie.
client_type	Áno	String	OAuth definuje dva typy klientov (Confidential / Public). ASPSP (banka) podporuje len typ Confidential.

Response			
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.

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

Príklad použitia vid' kapitola 3.2.1.2.

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 zmazení.

Testovacie prostredie

Endpoint: DELETE https://apitest.szrb.sk:98/api/enroll/{client_id}

Produkčné prostredie
Endpoint: DELETE https://api.szrb.sk:98/api/enroll/{client_id}

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

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

Príklad použitia vid' kapitola 3.2.1.3.

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 týmto požiadavkom zrušený.

Testovacie prostredie
Endpoint: POST https://apitest.szrb.sk:98/api/enroll/{client_id}/renewSecret
Produkčné prostredie
Endpoint: POST https://api.szrb.sk:98/api/enroll/{client_id}/renewSecret

Response			
Atribut	Povinný	Typ	Popis
client_id	Áno	String	client_id priradené aplikácii.
client_secret	Áno	String	Client_secret - password / token vydený bankou (ASPSP) pre TPP aplikácii (client_id)

Response			
client_secret_expires_at	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

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

Príklad použitia vid' kapitola 3.2.1.4.

2.8 Autentizácia a Autorizácia requestu (OAuth2)

Autorizácia requestu je založená na autorizačnom flow koncepte 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 partnerské 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)
- Banka a TPP aplikácia spolu zdieľa spoločné "tajomstvo" (client secret)
- Výsledkom identifikácie a autentizácie užívateľa je jednorazový code, ktorý aplikácia tretej strany môže s použitím **client_id** a **client secret** vymeniť za refresh token a access token
- Samotný jednorazový code bez znalosti client secret nie je možné použiť

2.8.1.2 Popis Code grand flow

Podmienky použitia flow:

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

Jednotlivé kroky code grant flow:

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

2.8.1.3 Autorizačný resource

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

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/auth/oauth/authorize>

Produkčné prostredie

 Endpoint: GET <https://api.szrb.sk:98/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 registrované v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrované 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))) vid'. 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] Chyba! Nenašiel sa žiaden zdroj odkazov. RFC 6749, kapitola 4.1.2.1

Príklad použitia vid' kapitolu 3.2.2.1.

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).

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/auth/oauth/token>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/auth/oauth/token>

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

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

Chybové kódy

- › Chybové kódy sú definované podľa [Chyba! Nenašiel sa žiaden zdroj odkazov.] Chyba! Nenašiel sa žiaden zdroj od kazov. RFC 6749, kapitola 5.2

Príklad použitia vid' kapitola 3.2.2.2.

2.8.1.5 Obnovenie Access tokenu

TPP môže po expirácii access_tokenu prostredníctvom refresh tokenu požiadať o nový. Pre to je možné použiť resouce "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).

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/auth/oauth/token>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/auth/oauth/token>

Request			
Atribut	Povinný	Typ	Popis
<i>grant_type</i>	Áno	refresh_token	Existujúca definícia / zvyklosti OAuth2 bude táto hodnota refresh_token, ak dochádza k obnoveniu access_tokenu na základe refresh_token.
<i>refresh_token</i>	Áno	String	Validný refresh_token
<i>scope</i>	Áno	String	Rozsah scope o prístup. Ak sa používa rozsah, je skontrolovaný proti scope uvádzaným v zázname TPP, aplikáciu TPP a súhlasu, ktorý nastavil užívateľ aplikácie.

Response			
Atribut	Povinný	Typ	Popis
<i>access_token</i>	Áno	string	Krátkodobý (v niektorých prípadoch jednorazový 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	Dlhodobý token (platnosť 90 dní). 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2

Príklad použitia vid' kapitola 3.2.2.3.

2.9 Popis metód používaných pre poskytovateľov služieb (TPP)

2.9.1 Všeobecná definícia hlavičky požiadavky

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

Hlavička pre Request

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

Hlavička pre Response

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

2.9.2 Služba AISP (Dotazy k účtom, prehľad transakcií)

Kapitola definuje zoznam metód poskytovaných pre AISP.

2.9.2.1 Predpoklady pre používanie metód API pre službu 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 dohľadáný platný súhlas vytvorený disponentom.
- g/ aplikácia TPP má v nájdenom súhlase povolenú od disponenta službu AISP

2.9.2.2 Zoznam metód používaných pre službu 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, ktoré disponent uviedol v súhlase k používaniu s konkrétnym TPP (nie zoznam všetkých účtov disponenta) bez zostatkov

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

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/v1/accounts/information>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/accounts/information>

Request

Metoda: accounts/information			
Názov atribútu	Formát	Povinný	Poznámka
<code>iban</code>	String (34)	Áno	IBAN účtu. Účet musí byť obsiahnutý v dohľadanom súhlase od disponenta

Response

Metoda: accounts/information				
Názov atribútu	Formát	Povinný	Poznámka	
<code>account</code>	<code>BaseCurrency</code>	String (3)	Áno	Mena účtu (kód meny podľa ISO 4217 - 3 veľké písmená)
	<code>Name</code>	string	Áno	Názov účtu (meno klienta)
	<code>ProductName</code>	string	Nie	Názov produktu
	<code>Type</code>	enum	Nie	Skratka typu účtu podľa normy ISO 20022 - Cash Account Type Code – napr . <ul style="list-style-type: none"> CACC - bežný účet
<code>Balances</code>	<code>typ:ArrayOfAccountsInformationResponseBalance</code>	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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.3.2.

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, ITBD (disponibilný zostatok)

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.

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/v1/accounts/transactions>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/accounts/transactions>

Request

Metóda: accounts/transactions			
Názov atribútu	Formát	Povinný	Poznámka
iban	String (34)	Áno	IBAN účtu. Účet musí byť obsiahnutý v dohľadanom súhlase od disponenta
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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.3.3.

2.9.2.5.1 Definícia typu ArrayOfAccountsTransactionResponseTransaction

Metóda: Account/Transaction - 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
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: Account/Transaction - 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	accountServicerReference		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

Metóda: Account/Transaction - typ: ArrayOfAccountsTransactionsResponseTransaction					
	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

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/api/v2/accounts>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2

Príklad použitia vid' kapitola 3.2.3.4.

2.9.2.6.1 Definícia typu ArrayOfAccountsInfo

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

Metóda: accounts - typ: ArrayOfAccountInfo				
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 SZRB
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, zisťovanie stavu platby, autorizácia platby, zrušenie platby)

Kapitola definuje zoznam metód poskytovaných pre PISP.

2.9.3.1 Predpoklady pre používanie metód API pre PISP

- a/ záznam TPP je na základe licenčného čísla (vrátane použitého prefixu) uvedeného v certifikáte, ktorý TPP používa pri komunikácii, nájdený v databáze IB
- b/ nájdený záznam TPP je platný,
- c/ TPP má vo svojom zázname povolenú službu PISP (táto informácia je súčasťou záznamu TPP v databáze IB, ktorý sa automaticky aktualizuje z NBS)
- d/ registrovaná aplikácia TPP má povolenú službu PISP
- e/ v certifikáte, ktorý používa TPP pri komunikácii je uvedená služba PISP
- f/ TPP použil v hlavičke požiadavky access_token, na základe ktorého je na strane banky dohľadovaný platný súhlas vytvorený disponentom.
- g/ aplikácia TPP má v nájdenom súhlase povolenú od disponenta 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 alebo zahraničný 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

Endpoint	Metoda	Popis
/api/v1/payments	POST	Payment initialization (JSON) - Prostredníctvom tejto metódy disponentom autorizovaná tretia strana iniciuje (vytvorí) príkaz typu SEPA alebo zahraničný z bankového účtu disponenta. Inicializácia platby bude vykonaná zaslaním príkazu vo formáte JSON 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 – zrušenie – prostredníctvom tejto služby je umožnené poslať žiadosť o zrušenie trvalého príkazu

2.9.3.3 PISP operácia: Standard payment initialization (XML)

Operácia umožňuje inicializáciu jednej SEPA platby alebo jednej zahraničnej 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 SEPA alebo zahraničný platobný príkaz, ktorý sa vzťahuje k obchodnej transakcii medzi PSU a obchodníkom (TPP typu PISP).

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/v1/payments/standard/iso>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/payments/standard/iso>

Request

Telo požiadavky obsahuje jednu SEPA alebo zahraničnú platbu vo formáte xml: pain.001.001.03
Vid' https://www.iso20022.org/documents/general/Payments_Maintenance_2009.zip

Response

Odpoveď, pokiaľ je príkaz uložený do databázy

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

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

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

Príklad použitia vid' kapitola 3.2.4.2.

2.9.3.4 PISP operácia: Standard payment submission

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

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/v1/payments/submission>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/payments/submission>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Hlavička požiadavky musí 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 Internet Banking
reasonCode	String	Nie	Status Reason Code podľa ISO 20022 Vid': 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	Dátum prijatia príkazu bankou.

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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.4.5.

2.9.3.4.1 Token pro 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.], 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).

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/auth/oauth/authorize>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/auth/oauth/authorize>

Request			
Atribut	Povinný	Typ	Popis
response_type	Áno	code	Povinný parameter. Hodnotou parametra je určené, aký typ autentizačného flow je požadovaný. V tomto prípade sa jedná o code grant. Pre autentizačný proces to znamená, že výsledkom tejto požiadavky bude jednorazový <code>auth_code</code> , ktorý TPP následne pomocou ďalšej požiadavky (metódou token) zamení za token <code>access_token</code>
client_id	Áno	String	Jedinečný identifikátor, ktorý banka vygenerovala pre aplikáciu TPP

Request			
redirect_uri	Áno	URL	URL kam je na konci presmerované flow autentizácie. Toto URL je stanovené už pri vydaní client_id a v rámci autentizácia je tento parameter validovaný proti URL zavedenému k client_id v zázname aplikácie registrované v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrované aplikácie.
Scope	Áno	String	Jedná sa o pole požadovaných scope (oprávnenia). V prípade PSD2 to môžu byť role AISP, PISP, PIISP. Napr. ak je TPP držiteľom viac oprávnenia, môže tu pre svoju aplikáciu požiadať len o jedno z nich alebo viac. Ak je použitých viac typov scope, sú oddelené medzerou.
state	Áno	Libovolný string [min 128 bits]	Parametrom sa zvyšuje bezpečnosť komunikácie pri presmerovaní. Chráni pred útokmi CSRF a odovzdáva informácie z aplikácie prostredníctvom toku autentizácie.
code_challenge	Áno	String	code_challenge = BASE64URL- ENCODE(SHA256(ASCII(code_verifier))) vid'. zdroj [3] RFC 7636 (OAuth PKCE)
code_challenge_method	Áno	String	S256
request	Áno	JWT	Príklad použitia vid' kapitola 3.1

Súčasťou požiadavky o autorizáciu platby disponentom je **podpísaný JWT Request, ktorý obsahuje OrderId** (pre podpis vygenerovaného JWT musí TPP použiť client_secret, aby banka dokázala obsah JWT dešifrovať – client_secret je tajná informácia, ktorá je známa iba TPP a na bankovej strane aplikácii IB, ktorá tento údaj pri registrácii TPP aplikácie vygenerovala).

Pri požiadavke o autorizácii platby disponentom bude disponent presmerovaný z aplikácie TPP na centrálnu autorizačnú stránku.

Potom, čo disponent vykoná dvojfázovú autorizáciu, aplikácia zistí, či platba iniciovaná prostredníctvom tretej strany (SEPA, zahraničná platba, žiadosť/zrušenie/zmena trvalý príkaz) obsahuje účet platiteľa (účet debet).

Varianta - platba **NEOBSAHUJE** účet debet:

- zobrazí sa obrazovka s opisom platby bez účtu platiteľa,
- disponent si vyberie účet zo zobrazeného zoznamu účtov, (ak má disponent len jeden účet, účet sa automaticky doplní), z ktorého sa platba uskutoční, a stlačí tlačidlo „Pokračovať“.
- Potom sa mu zobrazí detail platby s účtom, ktorý si disponent vybral v predchádzajúcom kroku a túto platbu musí autorizovať (rovnako ako v Internetbankingu) svojím autorizačným zariadením.

Varianta – platba OBSAHUJE účet debet:

- Disponentovi sa zobrazí detail platby, ktorú musí autorizovať (rovnako ako v Internetbankingu) svojim autorizačným zariadením.

Pre obe varianty platí, že po autorizácii platby disponentom je disponent presmerovaný späť do aplikácie tretej strany a v odpovedi je vrátený autorizačný code, ktorý je previazaný s daným OrderId a platba čaká na autorizáciu treťou stranou. zobrazí sa mu detail platby, ktorú musí autorizovať svojim autorizačným zariadením.

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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 4.1.2.1

Príklad použitia vid' kapitola 3.2.4.3.

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 zakódované pomocou Base64).

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/auth/oauth/token>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/auth/oauth/token>

Request			
Atribut	Povinný	Typ	Popis
code	Áno	string	Autorizačný code navrátený z autentizačného flow (code grant)

Request			
redirect_uri	Áno	URL	URL redirect zodné s URL doručenom v autentizačnom requestu
grant_type	Áno	authorization_code	Podľa existujúcej definície / zvyklosti OAuth2 bude táto hodnota authorization_code, ak dochádza k výmene code za access_token.
code_verifier	Áno	String	code_verifier slúži na generovanie code_challenge z predchádzajúcej žiadosti o minimálnej dĺžke 43 znakov a maximálnou dĺžkou 128 znakov

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

Chybové kódy

- › Chybové kódy sú definované podľa [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2

Príklad použitia vid' kapitola 3.2.4.4.

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 autorizácie 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}.

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/v1/payments/{orderId}/status>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/api/v1/payments/{orderId}/status>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: payments/{orderId}/status			
Názov atribútu	Formát	Povinný	Poznámka
orderId	String	Áno	Číslo príkazu vytvoreného v databáze Internet Banking
reasonCode	String	Nie	V položke sa uvádza informácia o skutočnom statuse, ktorý má príkaz v Internet Banking. 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 Internet Banking 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"> • RJCT (Zrušené klientom / Odmietnuté bankou- 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 bankou.

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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.4.6.

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“.

Testovacie prostredie

Endpoint: DELETE <https://apitest.szrb.sk:98/v1/payments/{orderId}/rcp>

Produkčné prostredie

Endpoint: DELETE <https://api.szrb.sk:98/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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.4.7.

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.

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/accounts/balanceCheck>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/accounts/balanceCheck>

Request

Metóda: accounts/balanceCheck					
Názov atribútu		Formát	Povinný	Poznámka	
iban		String (34)	Áno	IBAN účtu. Účet musí byť obsiahnutý v dohľadanom súhlase od disponenta	
creationDate		dateTime	Nie	Dátum a čas vytvorenia požiadavky podľa RFC 3339	
amount	value	Decimal (2 desatinné miesta)	Nie	Hodnota čiastky transakcie	
	currency	String (3)	Nie	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená	
instructionIdentification		string	Áno	Technická identifikácia platby generovaná na strane PISP	
relatedParties	tradingParty	address	string	Nie	Adresa obchodníka (obvykle obsahuje zreťazenie názvu ulice, čísla ulice atď..)
		countryCode	string	Nie	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	chequeNumber	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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.4.8.

2.9.3.8 PISP operácia: Payment initialization (JSON) – vytvorenie platby

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky vytvorí pod špecifickým orderId nová platba typu SEPA alebo zahraničná platba (typ platby sa deteguje automaticky podľa obsahu JSON zadaného príkazu).

Pre autorizáciu platby sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/payments>

Produkčné prostredie

 Endpoint: POST <https://api.szrb.sk:98/api/v1/payments>
Request

Metóda:POST payments						
Názov atribútu				Formát	Povinný	Poznámka
paymentIdentification	instructionIdentification			String (35)	Áno	Parametre trvalého príkazu
	endToEndIdentification			String (35)	Nie	Identifikácia usporiadaná medzi platiteľom a príjemcom Pre SEPA obsahuje reťazec hodnoty VS, SS alebo KS: Príklad: ("endToEndIdentification": "/vs123/ss456/ks0308")
paymentTypeInformation	instructionPriority			string	Nie	Povolené hodnoty: NORM = štandardná platba HIGH= prioritná platba (bankou nie je podporované) Ak prvok instructionPriority nie je vyplnený, použije sa hodnota NORM = štandardná platba
amount	instructedAmount	value		Numeric	Áno	Čiastka
		currency		String (3)	Áno	Mena

Metóda:POST payments							
requestedExecutionDate				ISODate	Áno	Požadovaný dátum vykonania príkazu	
chargeBearer				Enum	Nie	Platiteľ poplatkov Povolené hodnoty: DEBT (význam = OUR, poplatky platí platiteľ) SHAR alebo SLEV (význam = SHA, platiteľ vždy platí bankové poplatky platiteľa a príjemca platí poplatky príjemcu) Ak prvok nie je vyplnený, použije sa hodnota SHAR = SHA	
debtorAccount	identification	iban		String	Nie	Iban účtu platiteľa	
		other	identification	String (34)	Nie	Číslo účtu platiteľa vo formáte BBAN	
	Currency			String (3) CurrencyCode ISO 4217	Nie	Mena účtu platiteľa	
creditorAccount	identification	iban		String	Podmienečne povinná (Vyplňte, ak nie je zadaná hodnota identification - other)	IBAN účtu príjemcu	
		other	identification	String (34)	Podmienečne povinná (Vyplňte, ak nie je zadaná hodnota identification - iban)	Iný formát čísla účtu	
creditorAgent	financialInstitutionIdentification	bic		String (11)	Áno	BIC / SWIFT kód banky príjemcu	
		name		String (70)	Áno	Meno banky príjemcu	
		postalAddress	streetName		String (70)	Nie	Poštová adresa banky príjemcu (ulica)
			buildingNumber		String (16)	Nie	Poštová adresa banky príjemcu (číslo budovy)
			townName		String (35)	Nie	Poštová adresa banky príjemcu (mesto)
			postCode		String (16)	Nie	Poštová adresa banky príjemcu (PSČ)
			country		String (2)	Nie	Poštová adresa banky príjemcu (kód zeme podľa ISO3166)

Metóda: POST payments						
creditor	name			String (70)	Áno	Meno príjemcu
	postalAddress	streetName		String (70)	Nie	Poštová adresa (ulica)
		buildingNumber		String (16)	Nie	Poštová adresa (číslo budovy)
		townName		String (35)	Nie	Poštová adresa (mesto)
		postCode		String (16)	Nie	Poštová adresa (PSČ)
		country		String (2)	Nie	Poštová adresa (kód zeme podľa ISO3166)
remittanceInformation	unstructured			String (140)	Nie	Neštrukturovaná správa pre príjemcu
purpose	proprietary			String (140)	Nie	Účel platby

Response

Metóda: POST payments				
Názov atribútu		Formát	Povinný	Poznámka
id		Numeric	Áno	Číslo, pod ktorým sa príkaz uložil do databázy Internetbankingu
status		Enum	Áno	Status spracovania príkazu Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, príkaz čaká na autorizáciu klientom)
createDate		dateTime	Áno	Dátum prijatia príkazu bankou.
paymentTypeInformation	code	String	Áno	Typ zadaneho príkazu – ESCT = platba SEPA NXCT = zahraničná platba

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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] Chyba! Nenašiel sa žiaden zdroj odkazov. RFC 6749, kapitola 5.2		

Príklad použitia - viac kapitola 3.2.4.14

2.9.3.9 PISP operácia: Trvalý príkaz - periodicity

Operácia poskytuje zoznam kódov periodicít používaných v trvalých príkazoch SZRB banky.

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/v1/standingOrders/Periodicity>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/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)

Príklad použitia - viac kapitola 3.2.4.9

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.

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/v1/standingOrders>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/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: <code>ArrayOfStandingOrder</code>	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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia - viac kapitola 3.2.4.10

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: ACTIVE (aktívny trvalý príkaz) CANCELLED (zrušený trvalý príkaz) DISABLED (zrušený trvalý príkaz) FORMAL_ERROR (trvalý príkaz s formálnou chybou)
createDate		dateTime	Áno	Dátum vytvorenia trvalého príkazu
changeDate		dateTime	Áno	Dátum poslednej zmeny trvalého 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 (bankou nepodporované)
		city	String	Nie	Adresa - mesto (bankou nepodporované)
		country	String	Nie	Adresa - štát (bankou nepodporované)
	iban	String	Áno	IBAN príjemcu	
bic	String	Nie	BIC banky príjemcu		

Metóda: StandingOrder - typ: StandingOrderDetail					
	bankName		String	Nie	Meno banky príjemcu
	bankAdress	street	String	Nie	Adresa banky príjemcu - ulica (bankou nepodporované)
		city	String	Nie	Adresa banky príjemcu - mesto (bankou nepodporované)
		country	String	Nie	Adresa banky príjemcu - štát (bankou nepodporované)
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 (bankou nepodporované)
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	Nie	Konštantný symbol
paymentPurpose			String	Áno	Referencia platiteľa / Účel operácie
noteForBeneficiary			String	Áno	Text pre príjemcu (avízo)

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 **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov.**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/standingOrders>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/standingOrders>

Request

Metóda: POST standingOrders

Názov atribútu	Formát	Povinný	Poznámka
standingOrderData	typ: StandingOrderData	Áno	Parametre trvalého príkazu

Response

Metóda: POST standingOrders

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 bankou

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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2

Príklad použitia - viac kapitola 3.2.4.11.

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	Nie	Iban účtu klienta
partner	name	String	Nie	Meno partnera
	iban	String	Áno	IBAN príjemcu
	bic	String	Nie	BIC banky príjemcu
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	Podmienečne povinný	Deň vykonávania trvalého príkazu Nepovinný v prípade dennej periodicity – v tomto prípade je možné do tohto atribútu zadať iba hodnotu 0 (ak atribút nie je zadaný, implicitne je hodnota 0 doplnená). Povinný v prípade použitia ďalších typov periodicity. Ak je periodicita týždenná - sú v tomto atribúte povolené iba hodnoty v rozsahu 1 – 5 V ostatných prípadoch je povolený rozsah 1 – 31.
failureRetries		Integer	Áno	Počet opakovaní pri neúspešnom pokuse o odoslanie platby (bankou nepodporované – zadajte hodnotu 0)
dateFrom		Date (YYYY-MM-DD)	Áno	Platnosť trvalého príkazu OD (minimálna hodnota – aktuálny bankový deň + 1 pracovný 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	Referencia platiteľa
noteForBeneficiary		String	Áno	Text pre príjemcu (avízo)

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 dohľadovaný na základe parametra {id}. Zdrojom tohto parametra je opis trvalého príkazu vid kapitulu 3.2.4.10.

Pre autorizáciu žiadosti sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

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.

Testovacie prostredie

Endpoint: PUT <https://apitest.szrb.sk:98/v1/standingOrders/{id}>

Produkčné prostredie

Endpoint: PUT <https://api.szrb.sk:98/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	parameter_invalid	Nevalidná hodnota vstupného parametra.
500, 503	server_error	Chyba autorizačného servera.

Použitie ostatných http status kódov a chybových kódov podľa [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2

Príklad použitia - viac kapitola 3.2.4.12

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
	iban	String	Áno	IBAN príjemcu
	bic	String	Nie	BIC banky príjemcu

Metóda: PUT StandingOrder/{id} - typ: StandingOrderData				
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	Podmienečne povinný	Deň vykonávania trvalého príkazu Nepovinný v prípade dennej periodicity – v tomto prípade je možné do tohto atribútu zadať iba hodnotu 0 (ak atribút nie je zadaný, implicitne je hodnota 0 doplnená). Povinný v prípade použitia ďalších typov periodicity. Ak je periodicita týždenná - sú v tomto atribúte povolené iba hodnoty v rozsahu 1 – 5 V ostatných prípadoch je povolený rozsah 1 – 31.
failureRetries		Integer	Áno	Počet opakovaní pri neúspešnom pokuse o odoslanie platby (bankou nepodporované – zadajte hodnotu 0)
dateFrom		Date (YYYY-MM-DD)	Áno	Platnosť trvalého príkazu OD (minimálna hodnota – aktuálny bankový deň + 1 pracovný 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	Referencia platiteľa
noteForBeneficiary		String	Áno	Text pre príjemcu (avízo)

2.9.3.13 PISP operácia: Trvalý príkaz – zrušenie

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

Pre autorizáciu žiadosti sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

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.

Testovacie prostredie

Endpoint: DELETE <https://apitest.szrb.sk:98/v1/standingOrders/{id}>

Produkčné prostredie

Endpoint: PUT <https://api.szrb.sk:98/api/v1/standingOrders/{id}>

Request

Telo požiadavky neobsahuje žiadne atribúty.

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	parameter_invalid	Nevalidná hodnota vstupného parametra.
500, 503	server_error	Chyba autorizačného servera.
Použitie ostatných http status kódov a chybových kódov podľa [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia - viac kapitola 3.2.4.13

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 platný súhlas vytvorený disponentom.

g/ aplikácia TPP má v nájdenom súhlase povolenú od disponenta 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 **[Chyba! Nenašiel sa žiaden zdroj odkazov.]**, kapitola 4.1.

Generovanie `access_tokenu` na základe Client Credentials Grant flow, ktoré je v SBAS uvedené ako alternatívne riešenie (teda 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.

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/accounts/balanceCheck>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/accounts/balanceCheck>

Request

Metóda: Accounts/balanceCheck					
Názov atribútu			Formát	Povinný	Poznámka
iban			String (34)	Áno	IBAN účtu. Účet musí byť obsiahnutý v dohľadanom súhlase od disponenta
creationDate			dateTime	Nie	Dátum a čas vytvorenia požiadavky podľa RFC 3339
amount	value		Decimal (2 desatinné miesta)	Nie	Hodnota čiastky transakcie
	currency		String (3)	Nie	Mena čiastky transakcie podľa ISO 4217 - 3 veľké písmená
instructionIdentification			string	Áno	Technická identifikácia platby generovaná na strane PIISP
relatedParties	tradingParty	address	string	Nie	Adresa obchodníka (obvykle obsahuje zrežazenie názvu ulice, čísla ulice atď..)
		countryCode	string	Nie	Dvojnakový kód zeme obchodníka podľa normy ISO3166

Metóda: Accounts/balanceCheck					
		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	chequeNumber		string	Nie	V prípade kartových transakcií sa tu uvádza číslo karty vo formáte **** * 1111
	holderName		string	Nie	Meno držiteľa karty

Response

Metóda: Account/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 [Chyba! Nenašiel sa žiaden z droj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia viď kapitola 3.2.5.2.

Upozornenie: **grant_type "client_credentials"** uvedený v príklade v zdroji [Chyba! Nenašiel sa žiaden z droj odkazov.] kapitola 7.2.2 **nie je v tomto rešení podporovaný** – pozri kapitolu 2.9.4.3).

2.9.5 Súhlasy – správa cez PSD2 API

Kapitola definuje popis metód poskytovaných pre správu súhlasov cez PSD2 API.

2.9.5.1 Predpoklady pre používanie metód API pre správu súhlasov

a/ je použitý platný certifikát

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

c/ nájdený záznam TPP je platný,

d/ TPP použil v hlavičke požiadavky access_token, na základe ktorého je na strane banky dohľadaný platný súhlas vytvorený disponentom.

2.9.5.2 Workflow nad žiadosťou o súhlas alebo žiadosťou o ukončenie súhlasu

Krok	Strana	Popis
1	TPP Aplikácia TPP	Zadanie žiadosti a odoslanie požiadavky týkajúcej sa súhlasu na PSD2 API
2	Banka PSD2 API	Spracovanie prijatej požiadavky <ul style="list-style-type: none"> • Žiadosť o nový globálny súhlas - api/v1/consents/global • Žiadosť o nový súhlas definovaný PSU na strane banky - api/v1/consents/bankOffered • Žiadosť o nový súhlas definovaný parametrami zadanými priamo v aplikácii TPP - api/v1/consents/detailed • Žiadosť o ukončení aktuálneho súhlasu - api/v1/consents/terminate Podmienka: + prijatá požiadavka neobsahuje chyby <ul style="list-style-type: none"> • do databáze je uložená žiadosť požadovaného typu • v odpovedi požiadavky sa vráti orderId, pod ktorým bola žiadosť uložená v databáze IB + ak sa počas spracovania požiadavky zistí chyba <ul style="list-style-type: none"> • v odpovedi na požiadavku sa vráti príslušný kód chyby.
3	TPP	Podmienka: prijatá odpoveď obsahuje orderId <ul style="list-style-type: none"> • volá sa požiadavka typu /authorize, ktorá vo svojom tele obsahuje atribút request s použitým JWT (jeho súčasťou je orderId požiadavky, ktorú má potvrdiť PSU na strane banky) • PSU je presmerovaný na stranu banky

Krok	Strana	Popis
4	Banka WebPSD2	<ul style="list-style-type: none"> PSU vykoná silnú autentifikácia (rovnako ako v Internet bankingu). Zobrazí sa stránka s obsahom zodpovedajúca typu prijatej žiadosti PSU danú žiadosť: <ul style="list-style-type: none"> môže upravovať (ak to daný typ súhlasu umožňuje) môže potvrdiť (tlačidlo "Pokračovať") alebo prerušiť operáciu (tlačidlo "Späť") <p>Podmienka: PSU stlačil tlačidlo "Pokračovať"</p> <ul style="list-style-type: none"> Žiadosť sa uloží s informáciou, že bola potvrdená zo strany používateľa platobných služieb PSU, ale stav zostáva "Na podpísanie". PSU je presmerovaný späť na stránku TPP podľa redirect_url, ktorá bola súčasťou požiadavky /authorize Pri presmerovaní odpoveď vráti aj jednorazový kód code=<value>, ktorý je spojený s potvrdenou požiadavkou <p>Podmienka: PSU stlačil tlačidlo „Späť“</p> <ul style="list-style-type: none"> Do žiadosti sa uloží informácia o tom, že žiadosť nebola potvrdená (bola zamietnutá) zo strany PSU. PSU je presmerovaný späť na stránku TPP podľa redirect_url, ktorá bola súčasťou požiadavky /authorize Pri presmerovaní odpoveď vráti aj jednorazový kód code=<value>, ktorý je spojený s potvrdenou požiadavkou
5	TPP	<p>Ak TPP dostal v odpovedi hodnotu code:</p> <ul style="list-style-type: none"> TPP zavolá požiadavku /oauth/token, pričom v parametri kód použije hodnotu code prijatú v odpovedi na požiadavku /authorize v odpovedi požiadavky je vrátený access_token TPP zavolá požiadavku /v1/consents/submission, ktorá sa overuje pomocou prístupového_tokenu prijatého v odpovedi na požiadavku /oauth/token
6	Banka PSD2 API	<p>Ak overenie požiadavky prebehne bez chyby, stav žiadosti sa zmení podľa predchádzajúcej operácie vykonanej PSU:</p> <ul style="list-style-type: none"> Na "Autorizované", ak PSU použil v žiadosti tlačidlo "Pokračovať". Na "Zrušené", ak PSU použil v žiadosti tlačidlo "Späť" <p>Ak bol stav žiadosti nastavený na "Autorizované", následne sa na základe tejto žiadosti vykoná:</p> <ul style="list-style-type: none"> Aktualizuje sa existujúci súhlas (ak ide o žiadosť o vytvorenie súhlasu) alebo sa ukončí existujúci súhlas (ak ide o žiadosť o ukončenie súhlasu)

2.9.5.3 Súhlasy: zoznam metód

Názov metódy	Endpoint	Metoda	Popis
Vytvorenie žiadosti o súhlas typu Global Consent (JSON)	https://api.szrb.sk:98/api/v1/consents/global	POST	Metóda, prostredníctvom ktorej aplikácia TPP žiada o úplný prístup k všetkým bankovým účtom disponenta a službám dostupným prostredníctvom rozhrania PSD2. Žiadosť o súhlas sa disponentovi zobrazí po jeho presmerovaní z aplikácie TPP a vykonaní silnej autentifikácie na strane banky. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
Vytvorenie žiadosti o súhlas typu Bank Offered Consent (JSON)	https://api.szrb.sk:98/api/v1/consents/bankOffered	POST	Metóda, prostredníctvom ktorej aplikácia TPP žiada o vytvorenie súhlasu typu Bank Offered Consent – v tomto type súhlasu rozsah prístupu k účtom a službám (AISP, PISP) pre TPP je definovaný disponentom po jeho presmerovaní a silnej autentifikácii disponenta na strane banky. Disponent môže žiadosť po zobrazení upraviť a potvrdiť alebo zamietnuť.
Vytvorenie žiadosti o súhlas typu Detailed Consent (JSON)	https://api.szrb.sk:98/api/v1/consents/detailed	POST	Metóda, prostredníctvom ktorej aplikácia TPP žiada o vytvorenie súhlasu typu Detailed Consent – v tomto type súhlasu rozsah prístupu k účtom a službám je definovaný v aplikácii TPP. Žiadosť o súhlas s predvyplnenými parametrami (účty a služby, ktoré boli uvedené v tele prijatej požiadavky) sa disponentovi zobrazí po jeho presmerovaní z aplikácie TPP a vykonaní silnej autentifikácie na strane banky. Disponent môže žiadosť potvrdiť alebo zamietnuť - nemôže ju upraviť.
Potvrdenie žiadosti o súhlas (JSON)	https://api.szrb.sk:98/api/v1/consents/submission	POST	Metóda Potvrdenie žiadosti o súhlas (Request of consent submission) pre autorizáciu žiadosti tretou stranou (žiadosť predtým musí v požiadavke oauth/authorize potvrdiť disponent).
Ukončenie súhlasu	https://api.szrb.sk:98/api/v1/consents/terminate	POST	Metóda Ukončenie súhlasu (JSON) pre ukončenie aktívneho súhlasu

2.9.5.4 Súhlasy: Vytvorenie žiadosti o súhlas typu Global Consent (JSON)

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky vytvorí pod špecifickým orderId nová žiadosť o súhlas typu Global Consent

TPP týmto typom súhlasu bude umožnené:

- pracovať so všetkými bežnými účtami disponenta, ku ktorým má disponent v elektronickom bankovníctve nastavený aktívny prístup
- používať služby ktoré odpovedajú prieniku

- služieb, ktoré má TPP registrované vo svojej licencií v NBS
- služieb, ktoré si TPP zaregistrovala v banke pre aplikáciu, cez ktorú disponent pristupuje k API PSD2

Pre autorizáciu požiadavky sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/consents/global>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/consents/global>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: POST consents/global				
Názov atribútu		Formát	Povinný	Poznámka
id		Numeric	Áno	Číslo, pod ktorým sa žiadosť o súhlas uložila do databázy Internetbankingu
status		Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, žiadosť čaká na potvrdenie klientom)
createDate		dateTime	Áno	Dátum prijatia žiadosti 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia - kapitola 0

2.9.5.5 Súhlasy: Vytvorenie žiadosti o súhlas typu Bank Offered Consent (JSON)

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky vytvorí pod špecifickým orderId nová žiadosť o súhlas typu Bank Offered Consent.

Pre autorizáciu požiadavky sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/consents/bankOffered>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/consents/bankOffered>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: POST consents/bankOffered				
Názov atribútu		Formát	Povinný	Poznámka
id		Numeric	Áno	Číslo, pod ktorým sa žiadosť o súhlas uložila do databázy Internetbankingu
status		Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, žiadosť čaká na potvrdenie klientom)
createDate		dateTime	Áno	Dátum prijatia žiadosti 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia - kapitola 3.2.6.3

2.9.5.6 Súhlasy: Vytvorenie žiadosti o súhlas typu Detailed Consent (JSON)

Odoslaním tejto požiadavky vo formáte JSON sa na strane banky vytvorí pod špecifickým orderId nová žiadosť o súhlas typu Detailed Consent.

Obsah tejto žiadosti na súhlas je definovaný priamo v aplikácii TPP – odoslaná požiadavka v tele obsahuje zoznam účtov daného disponenta vo formáte IBAN a služby, ktoré majú byť v súhlase povolené.

Pre autorizáciu požiadavky sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj o odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov..**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/consents/detailed>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/consents/detailed>

Request

Metóda: POST consents/detailed			
Atribut	Povinný	Typ	Popis
accounts	Áno	Array of strings	<p>Pole IBAN bežných účtov, požadovaných pre používanie cez aplikáciu TPP.</p> <p>Pri prijatí požiadavky sú IBANy uvedené v požiadavke validované:</p> <ul style="list-style-type: none"> ➤ či formát všetkých zadaných účtov je validný ➤ či má k zadaným účtom disponent v elektronickom bankovníctve aktívny prístup. <p>Ak je pri validácii zistená chyba, je požiadavka zamietnutá.</p>
scopes	Áno	Array of strings	<p>Pole požadovaných Scopes (služieb AISP, PISP) pre súhlas. Služba PIISP nie je bankou podporovaná. Ak bude uvedená v poli Scopes, bude ignorovaná.</p> <p>Pri prijatí požiadavky sú Scopes validované proti obsahu použitého certifikátu a proti Scopes uvedených v zázname TPP, ktorý musí existovať v databáze IB.</p> <p>Ak je pri validácii zistená chyba, je požiadavka zamietnutá.</p>

Response

Metóda: POST consents/detailed				
Názov atribútu		Formát	Povinný	Poznámka
id		Numeric	Áno	Číslo, pod ktorým sa žiadosť o súhlas uložila do databázy Internetbankingu
status		Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, žiadosť čaká na potvrdenie klientom)
createDate		dateTime	Áno	Dátum prijatia žiadosti 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia - kapitola 3.2.6.4

2.9.5.7 Súhlasy: Ukončenie platného súhlasu

Operácia umožňuje ukončiť platnosť aktuálneho aktívneho súhlasu.

Pre autorizáciu požiadavky sa používa resource vid' kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.** a **Chyba! Nenašiel sa žiaden zdroj odkazov.**

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/v1/consents>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/consents>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Response

Metóda: POST consents/terminate				
Názov atribútu		Formát	Povinný	Poznámka
id		Numeric	Áno	Číslo, pod ktorým sa žiadosť o súhlas uložila do databázy Internetbankingu
status		Enum	Áno	Status spracovania žiadosti Status môže nadobúdať nasledujúce hodnoty: ACTC (vykonaná validácia položiek, žiadosť čaká na potvrdenie klientom)
createDate		dateTime	Áno	Dátum prijatia žiadosti 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 5.2		

Príklad použitia viď kapitola 3.2.6.5

Upozornenie: Ak sa zruší platný súhlas, sú požiadavky typu AISP, PISP, PIISP a Správa súhlasu odmietané – je nutné aby disponent vytvoril nový súhlas za použitia volania metódy Autorizačného resource, pri ktorom je presmerovaný z aplikácie TPP na stranu banky, kde sa autentizuje rovnako ako do Internetbankingu a následne vytvorí nový súhlas - kapitola **Chyba! Nenašiel sa žiaden zdroj odkazov..**

2.9.5.8 Potvrdenie žiadosti o súhlas (PSU - užívateľom aplikácie TPP)

Proces potvrdenia žiadosti na vytvorenie súhlasu alebo ukončenia platnosti súhlasu užívateľom aplikácie TPP (PSU) musí TPP iniciovať po tom, čo sa po vytvorení (inicializácii) novej žiadosti na vytvorenie súhlasu vráti v odpovedi z ASPSP (banky) číslo, pod akým sa daná žiadosť na strane banky vytvorila (OrderId).

Testovacie prostredie

Endpoint: GET <https://apitest.szrb.sk:98/auth/oauth/authorize>

Produkčné prostredie

Endpoint: GET <https://api.szrb.sk:98/auth/oauth/authorize>

Request			
Atribut	Povinný	Typ	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 token access_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 autentizácie je tento parameter validovaný proti URL zavedenému k client_id v zázname aplikácie registrované v banke. Hodnota by sa mala zhodovať s jednou z hodnôt uvedených v zázname registrované aplikácie.
<i>Scope</i>	Áno	String	Jedná sa o pole požadovaných scope (oprávnenia). V prípade PSD2 to môžu byť role AISP, PISP, PIISP. Napr. ak je TPP držiteľom viacerých oprávnení, 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	Ľubovoľný 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))) vid' zdroj [3] RFC 7636 (OAuth PKCE)
<i>code_challenge_method</i>	Áno	String	S256
<i>request</i>	Áno	JWT	Príklad použitia vid' kapitola 3.1

Súčasťou požiadavky o autorizáciu žiadosti disponentom je **podpísaný JWT Request, ktorý obsahuje OrderId** danej žiadosti (pre podpis vygenerovaného JWT musí TPP použiť client_secret, aby banka dokázala obsah JWT dešifrovať – client_secret je tajná informácia, ktorá je známa iba TPP a na bankovej strane aplikácie IB, ktorá tento údaj pri registrácii TPP aplikácie vygenerovala).

- Pri požiadavke o autorizáciu žiadosti bude PSU presmerovaný z aplikácie TPP na centrálnu autorizačnú stránku.
- Potom, čo PSU vykoná dvojfázovú autorizáciu, webová aplikácia zistí na základe prijatého OrderId obsah prijatej žiadosti a zobrazí príslušnú stránku - pozri kapitoly 2.9.5.8.1, 2.9.5.8.2, 2.9.5.8.3.
- Po tom, ako PSU stlačí tlačidlo "Pokračovať" alebo "Späť", je presmerovaný späť do aplikácie TPP a v odpovedi je vrátený autorizačný code, ktorý je previazaný s daným OrderId a žiadosť čaká na autorizáciu treťou stranou.

Obsah odpovede na žiadosť/autorizáciu je opísaný v nasledujúcej tabuľke:

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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, kapitola 4.1.2.1

Príklad použitia viď kapitola 3.2.6.6.

2.9.5.8.1 Obsah stránky - žiadosť na vytvorenie globálneho súhlasu (Global Consent)

Disponent môže žiadosť o tento typ súhlasu po presmerovaní z aplikácie TPP na stranu banky iba akceptovať alebo prerušiť operáciu akceptácie (odmietnuť) - nemôže ju upraviť.

Klientovi sa zobrazí obrazovka s nasledujúcim obsahom:

Typ	Hodnota	Popis
Label stránky	Žiadosť na vytvorenie globálneho súhlasu	
Text	Vážený klient (<id prihláseného disponenta>)	Za textom <i>Vážený klient</i> bude v zátvorke uvedený identifikátor prihláseného disponenta
Text	<p>Zaevidovali sme žiadosť o udelení prístupu pre:</p> <ul style="list-style-type: none"> ▪ Spoločnosť: <Názov TPP> ▪ Názov aplikácie / portálu: <Názov aplikácieTPP> 	<p>Za textom <i>Spoločnosť</i>: bude uvedený názov TPP na ktorú má väzbu aplikácia, cez ktorú vznikla požiadavka na vytvorenie súhlasu.</p> <p>Za textom <i>Názov aplikácie / portálu</i>: bude uvedený názov aplikácie, cez ktorú vznikla požiadavka na vytvorenie súhlasu.</p>
Text	<p>Na základe schválenia tejto žiadosti súhlasíte s nasledujúcim:</p> <ul style="list-style-type: none"> ▪ cez aplikáciu tretej strany povolujete prístup ku všetkým svojim účtom, ku ktorým máte v Internetbankingu povolený aktívny prístup 	
	<ul style="list-style-type: none"> ▪ cez aplikáciu tretej strany bude možné využívať nasledujúce služby: 	<p>Pod týmto textom sa zobrazí iba informatívny zoznam služieb, ktoré sú implicitne povolené v globálnom súhlase</p> <ul style="list-style-type: none"> ➤ Dotazy k účtom, prehľad transakcií (AISP) ➤ Vytvorenie platby (PISP)
Text	<p>Pre dokončenie udelenia súhlasu používania služieb cez aplikáciu / portál vyššie uvedenej spoločnosti stlačte tlačidlo "Pokračovať".</p> <p>Ak chcete prerušiť aktuálnu operáciu, stlačte tlačidlo "Späť".</p>	

Ovládacie prvky na stránke: V spodnej časti stránky sú ovládacie prvky (pozri kapitolu 2.9.5.8.5)

2.9.5.8.2 Obsah stránky – žiadosť na vytvorenie súhlasu, ktorý definuje disponent na strane banky (Bank Offered Consent)

Disponent môže žiadosť o tento typ súhlasu po presmerovaní z aplikácie TPP na stranu banky akceptovať (s možnosťou editácie položiek účtov a služieb) alebo prerušiť operáciu akceptácie (odmietnuť).

Klientovi sa zobrazí obrazovka s nasledujúcim obsahom:

Typ	Hodnota	Popis
Label stránky	Žiadosť na vytvorenie súhlasu definovaného klientom	
Text	Vážený klient (<id prihláseného disponenta>)	Za textom <i>Vážený klient</i> bude v zátvorke uvedený identifikátor prihláseného disponenta
Text	<p>Zaevidovali sme žiadosť o udelení prístupu:</p> <ul style="list-style-type: none"> Spoločnosť: <Názov TPP> Názov aplikácie / portálu: <Názov aplikácieTPP> 	<p>Za textom <i>Spoločnosť</i>: bude uvedený názov TPP na ktorú má väzbu aplikácia, cez ktorú vznikla požiadavka na vytvorenie súhlasu.</p> <p>Za textom <i>Názov aplikácie / portálu</i>: bude uvedený názov aplikácie, cez ktorú vznikla požiadavka na vytvorenie súhlasu.</p>
Text	Na základe schválenia tejto žiadosti súhlasíte s nasledujúcim:	
	<ul style="list-style-type: none"> cez aplikáciu tretej strany povolujete prístup k týmto účtom: 	<p>Pod textom sa zobrazia bežné účty disponenta, ku ktorým má daný disponent nastavený v banke aktívny prístup; pri každom účte je zobrazený checkbox.</p> <p>Editácia checkboxov je povolená. Disponent môže upraviť označenie položiek podľa svojich preferencií.</p> <ul style="list-style-type: none"> implicitne sú označené všetky zobrazené účty ak systém zistí, že súhlas typu Bank Offered Consent už v databáze IB existuje, sú označené iba údaje z existujúceho súhlasu typu Bank Offered Consent.
	<ul style="list-style-type: none"> cez aplikáciu tretej strany bude možné využívať nasledujúce služby: 	<p>Pod textom sa zobrazia služby, ku ktorým môže tretia strana žiadať o vydanie prístupových tokenov; pri každej službe je zobrazený checkbox.</p> <p>Editácia checkboxov je povolená. Disponent môže upraviť označenie položiek podľa svojich preferencií.</p> <ul style="list-style-type: none"> implicitne sú označené všetky služby, ktoré sú evidované v zázname tretej strany registrované v databáze Internet Banking (okrem služby PIISP) Ak systém zistí, že súhlas typu Bank Offered Consent už v databáze IB existuje, sú označené iba údaje z existujúceho súhlasu typu Bank Offered Consent.
Text	<p>Pre dokončenie udelenia súhlasu používania služieb cez aplikáciu / portál vyššie uvedenej spoločnosti stlačte tlačidlo "Pokračovať".</p> <p>Ak chcete prerušiť aktuálnu operáciu, stlačte tlačidlo "Späť".</p>	

Ovládacie prvky na stránke: V spodnej časti stránky sú ovládacie prvky (pozri kapitolu 2.9.5.8.5)

2.9.5.8.3 Obsah stránky – žiadosť na vytvorenie súhlasu, definovaná treťou stranou (Detailed Consent)

Obsah tejto žiadosti na súhlas je definovaný priamo v aplikácii TPP – TPP pošle požiadavku na žiadosť o súhlas, ktorá už v tele obsahuje zoznam účtov daného disponenta vo formáte IBAN a služby, ktoré majú byť v súhlase povolené.

Disponent môže žiadosť na tento typ súhlasu po presmerovaní z aplikácie TPP na stranu banky iba akceptovať alebo prerušiť operáciu akceptácie (odmietnuť) - nemôže ju upraviť.

Klientovi sa zobrazí obrazovka s nasledujúcim obsahom:

Typ	Hodnota	Popis
Label stránky	Žiadosť na vytvorenie súhlasu (parametrizovaná cez aplikácii tretej strany)	
Text	<i>Vážený klient (<id prihláseného disponenta>)</i>	Za textom <i>Vážený klient</i> bude v zátvorke uvedený identifikátor prihláseného disponenta
Text	<i>Zaevidovali sme žiadosť o udelení prístupu:</i> <ul style="list-style-type: none"> ▪ <i>Spoločnosť: <Názov TPP></i> ▪ <i>Názov aplikácie / portálu: <Názov aplikácieTPP></i> 	Za textom <i>Spoločnosť:</i> bude uvedený názov TPP na ktorú má väzbu aplikácia, cez ktorú vznikla požiadavka na vytvorenie súhlasu. Za textom <i>Názov aplikácie / portálu:</i> bude uvedený názov aplikácie, cez ktorú vznikla požiadavka na vytvorenie súhlasu.
Text	<i>Na základe schválenia tejto žiadosti súhlasíte s nasledujúcim:</i>	
	<ul style="list-style-type: none"> ▪ <i>cez aplikáciu tretej strany povolujete prístup k týmto účtom:</i> ▪ <i>cez aplikáciu tretej strany bude možné využívať nasledujúce služby:</i> 	Pod textom sa zobrazia bežné účty disponenta (iba readonly text), ktoré boli uvedené v prijatej požiadavke. Pod textom sa zobrazia služby (iba readonly text), ktoré boli uvedené v prijatej požiadavke.
Text	<i>Pre dokončenie udelenia súhlasu používania služieb cez aplikáciu / portál vyššie uvedenej spoločnosti stlačte tlačidlo "Pokračovať".</i> <i>Ak chcete prerušiť aktuálnu operáciu, stlačte tlačidlo "Späť".</i>	

Ovládacie prvky na stránke: V spodnej časti stránky sú ovládacie prvky (pozri kapitolu 2.9.5.8.5)

2.9.5.8.4 Obsah stránky – žiadosť o ukončenie súhlasu

Disponent môže žiadosť na ukončenie súhlasu po presmerovaní z aplikácie TPP na stranu banky iba akceptovať alebo prerušiť operáciu akceptácie (odmietnuť) - nemôže ju upraviť.

Klientovi sa zobrazí obrazovka s nasledujúcim obsahom:

Typ	Hodnota	Popis
Label stránky	Žiadosť o ukončenie súhlasu	
Text	<i>Vážený klient (<id prihláseného disponenta>)</i>	Za textom <i>Vážený klient</i> bude v zátvorke uvedený identifikátor prihláseného disponenta
Text	<i>Zaevidovali sme žiadosť na ukončenie súhlasu pre:</i> <ul style="list-style-type: none"> ▪ <i>Spoločnosť: <Názov TPP></i> ▪ <i>Názov aplikácie / portálu: <Názov aplikácieTPP></i> 	Za textom <i>Spoločnosť:</i> bude uvedený názov TPP na ktorú má väzbu aplikácia, cez ktorú vznikla požiadavka na vytvorenie súhlasu. Za textom <i>Názov aplikácie / portálu:</i> bude uvedený názov aplikácie, cez ktorú vznikla požiadavka na vytvorenie súhlasu.
Text	<i>Po potvrdení tejto žiadosti bude prístup k vašim účtom pre vyššie uvedenú aplikáciu tretej strany zrušený.</i> <i>Obnovenie prístupu tretích strán k vašim účtom môžete vykonať prostredníctvom aplikácie tretej strany aktiváciou prístupu.</i>	
Text	<i>Pre potvrdenie žiadosti o ukončenie súhlasu používania služieb cez aplikáciu / portál vyššie uvedenej spoločnosti stlačte tlačidlo "Pokračovať".</i> <i>Ak chcete prerušiť aktuálnu operáciu, stlačte tlačidlo "Späť".</i>	

Ovládacie prvky na stránke: V spodnej časti stránky sú ovládacie prvky (pozri kapitolu 2.9.5.8.5)

2.9.5.8.5 Ovládacie prvky na stránke žiadosti

Ovládací prvok	Label	Popis
Tlačidlo	Pokračovať	stlačením tlačidla „Pokračovať“ je disponent presmerovaný späť do aplikácie TPP a tretia strana v odpovedi obdrží kód, ktorý si vymení za autorizačný token a následne ho použije k autorizácii žiadosti o súhlas. Potom sa na základe tejto doautorizovanej žiadosti do väzby Disponent-Aplikácia TPP uloží záznam súhlasu daného typu (ak už záznam súhlasu existuje, tak bude aktualizovaný na požadovaný typ).
Tlačidlo	Späť	stlačením tlačidla „Späť“ je disponent presmerovaný späť do aplikácie TPP a tretia strana v odpovedi nedostane jednorázový kód pre vygenerovanie nových tokenov

2.9.5.9 Súhlasy: Potvrdenie žiadosti o súhlas treťou stranou

Operácia umožňuje tretej strane autorizáciu žiadosti o súhlas, ktorú táto TPP inicializovala.

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/api/v1/consents/submission>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/api/v1/consents/submission>

Request

Telo požiadavky neobsahuje žiadne atribúty.

Hlavička požiadavky musí obsahovať token "bearer token" (access_token), ktorý bude prepojený s práve autorizovanou žiadosťou s daným "orderId". Aby TPP získala tento access_token, musí predtým prebehnúť schválenie danej žiadosti o súhlas disponentom (pozri kapitolu 2.9.5.8). Výsledkom tejto operácie je autorizačný kód (code), ktorý dostane TPP v odpovedi. Tento code následne TPP vymení pomocou Authorization code flow za daný access_token, previazaný s danou žiadosťou (pozri kapitolu 2.9.5.9.1).

Response (pokiaľ nedôjde pri spracovaní požiadavky k chybe)

Metoda: consents/submission			
Názov atributu	Formát	Povinné	Poznámka
orderId	String	Áno	Číslo žiadosti o súhlas vytvorené v databáze Internet Bankingu
reasonCode	String	Nie	Status Reason Code podľa ISO 20022 Vid': https://www.iso20022.org/sites/default/files/ocuments/External_code_lists/ExternalCodeSets_4Q2017_05Mar2018_v1.xls , (listy: 16-StatusReason, 60-ReceivedReason, 61-AcceptedReason, 62-PendingProcessingReason, 63-RejectedReason)
status	Enum	Áno	Status žiadosti Status môže nadobúdať nasledujúce hodnoty: <ul style="list-style-type: none"> > RJCT (Odmietnuté - Rejected) > PDNG (Autorizované - Authorized) > ACTC (Na podpis - WaitingForSignatures) > ACSP (Spracováva sa - InProgress, Exportované - Exported) > ACSC (Akceptované)
statusDateTime	dateTime	Nie	Dátum prijatia žiadosti 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 [Chyba! Nenašiel sa žiaden zdroj odkazov.] 6749, kapitola 5.2		

Príklad použitia vid' kapitola 3.2.6.8.

2.9.5.9.1 Token pre operáciu Autorizácia žiadosti o súhlas (Consent submission)

Pre autorizáciu žiadosti o súhlas bude používaný access_token získaný na základe autorizačného resource Authorization Code Grant s PKCE rozšírením popísaného v kapitole 2.8.1 alebo prípadne pozri [Chyba! Nenašiel sa žiaden zdroj odkazov.] kapitola 4.1.

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

2.9.5.9.2 Získanie tokenu

Aby TPP mohol vykonať podpísanie vytvorenej žiadosti (/consents/submission), musí získať od banky access_token. Toto vykoná výmenou autorizačného Code, ktorý dostal v odpovedi požiadavky /Authorize, za daný access_token.

TPP zašle spoločne s týmto autorizačným kódom (ktorý musí byť uvedený v tele požiadavky) aj client_id a client_secret (ktoré však musia byť uvedené v hlavičke požiadavky zakódované pomocou Base64).

Testovacie prostredie

Endpoint: POST <https://apitest.szrb.sk:98/auth/oauth/token>

Produkčné prostredie

Endpoint: POST <https://api.szrb.sk:98/auth/oauth/token>

Request			
Atribut	Povinný	Typ	Popis
code	Áno	string	Autorizačný code navrátený z autentizačného flow (code grant)
redirect_uri	Áno	URL	URL redirect zhodné s URL doručenom v autentizačnom 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 s maximálnou dĺžkou 128 znakov

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

Chybové kódy

- › Chybové kódy sú definované podľa [Chyba! Nenašiel sa žiaden zdroj odkazov.] RFC 6749, k apitola 5.2

Príklad použitia viď kapitola 3.2.6.7

Header	"alg"	typ použitej šifrovacej metódy V rámci riešenia je podporovaný iba algoritmus "HS256"
	"typ"	typ tokenu V rámci riešenia je podporovaný iba typ "JWT"
Payload	"iss"	tu musí byť uvedená hodnota client_id z posielanej požiadavky na autorizáciu platby disponentom (identifikátor klientskej aplikácie TPP)
	"aud"	tu musí byť uvedené nasledujúce url: "https://api.szrb.sk:98"
	"response_type"	tu musí byť uvedený reťazec uvedený v špecifikácii štandardu: "code id_token"
	"client_id"	tu musí byť uvedená hodnota client_id z posielanej požiadavky na autorizáciu platby disponentom (identifikátor klientskej aplikácie TPP). Hodnota tejto položky je rovnaká ako v parametre "iss"
	"redirect_uri"	Tu musí byť uvedené redirect_url z posielanej požiadavky, na ktorú bude klient presmerovaný späť po autorizácii platby (táto URL adresa musí byť rovnaká s URL, ktorá je registrovaná pre aplikáciu TPP z procesu Enroll (pozri kapitolu 2.7))
	"scope"	Tu musí byť uvedená hodnota parametra „scope“ z posielanej požiadavky.
	"state"	Tu musí byť uvedená hodnota parametra „state“ z posielanej požiadavky.
	"claims"	Štruktúrovaný parameter, ktorý obsahuje OrderId. V parametri „claims“ je možné v parametri "value" použiť <i>Banka</i> : (rovnako ako v príklade uvedeného v SBA): Za parametrom order : musí byť uvedený identifikátor autorizovaného príkazu, ktorý je súčasťou odpovedi požiadavky na inicializáciu platby (pozri kapitolu 2.9.3.3) v atribúte: <GrpHdr><MsgId>???</MsgId> Ukážka štruktúrovaného parametru claims: <pre> "claims": { "id_token": { "orderId": { "value": "urn: Banka:order: 10004796", "essential": true } } } </pre>
Verify signature	V tejto časti sa používa podpis generovaný metódou HMACSHA256. Ako šifrovací kľúč sa používa client_secret, ktorý TPP prijala v odpovedi pri registrácii svojej aplikácie (pozri kapitolu 2.7.1). Príklad funkcie použitej pre výpočet Verify signature, ktorý je potom pripojený ako posledná časť do JWT (za oddeľovač - bodku). HMACSHA256(base64UrlEncoder(header) + "." + base64UrlEncode(payload), client_secret)	

3.2 Príklady http (request / response)

3.2.1 (api/enroll) Registračné resource

3.2.1.1 (POST api/enroll) Automatické generovanie technických identifikátorov

HTTP request:

Header

```
POST api/enroll HTTP/1.1
Host: api.szrb.sk:98
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "redirect_uris":
    ["http://www.tpp.sk/TPPTest/Home/LoginReturn",
     "http://www.tpp.sk/TPPTest/Home/AuthorizationReturn"],
  "client_name": "Moja_app",
  "client_type": "confidential",
  "logo_uri": "https://www.tpp.sk/logo.png",
  "contacts": ["info@tpp.sk"],
  "scopes": ["AISP", "PISP"],
  "licence_number": "11223344"
}
```

HTTP response:

Header

```
HTTP/1.1 201 Created
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
```

Body

```
{
  "client_id": "Moja_app_3263351",
  "client_secret":
    "Q6G0gsq6Kc7EXzyoxObzlgVxKOGGJifSWpUL6BOJNIni2qHHyrtgm9H6x1DAxYOCkdupBkbEqbFtKytwxGgGkg",
  "client_secret_expires_at": "0",
  "api key": "NOT PROVIDED",
  "redirect_uris": [
    "http://www.tpp.sk/TPPTest/Home/LoginReturn",
    "http://www.tpp.sk/TPPTest/Home/AuthorizationReturn"
  ],
  "client_name": "Moja_app",
  "client_name#en-US": null,
  "client_type": "confidential",
  "logo_uri": "https://www.tpp.sk/logo.png",
  "contacts": [
    "info@tpp.sk"
  ],
  "scopes": [
    "AISP",
    "PISP"
  ],
  "licence_number": "11223344"
}
```

3.2.1.2 (PUT `api/enroll/{client_id}`) Zmena registračných údajov

HTTP request:

Header

```
PUT api/enroll/Moja_app_3263351 HTTP/1.1
Host: api.szrb.sk:98
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "redirect_uris":
    ["http://www.tpp.sk/TPPTest/Home/LoginReturn",
     "http://www.tpp.sk/TPPTest/Home/AuthorizationReturn"],
  "client_name": "Moja_app",
  "client_type": "confidential",
  "contacts": ["info@tpp.sk", "contact@tpp.sk"],
  "scopes": ["AISP", "PISP"]
}
```

HTTP response:

Header

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Cache-Control: no-cache
Pragma: no-cache
```

Body

```
{
  "client_id": "Moja_app_3263351",
  "client_secret_expires_at": "0",
  "api_key": "NOT_PROVIDED",
  "redirect_uris": [
    "http://www.tpp.sk/TPPTest/Home/LoginReturn",
    "http://www.tpp.sk/TPPTest/Home/AuthorizationReturn"
  ],
  "client_name": "Moja_app",
  "client_name#en-US": null,
  "logo uri": null,
  "contacts": [
    "info@tpp.sk",
    "contact@tpp.sk"
  ],
  "scopes": [
    "AISP",
    "PISP"
  ],
  "client_type": "confidential"
}
```



3.2.1.3 (DELETE [api/enroll/{client_id}](#)) Zmazanie aplikácie

HTTP request:

Header

```
DELETE api/enroll/Moja_app_3263351 HTTP/1.1  
Host: api.srzb.sk  
Content-Type: application/json;charset=UTF-8
```

HTTP response:

```
HTTP/1.1 204 No content
```

3.2.1.4 (POST [api/enroll/{client_id}/renewSecret](#)) Žiadosť o nový client_secret

HTTP request:**Header**

```
POST api/enroll/Moja_app_3263351/renewSecret HTTP/1.1
Host: api.szrb.sk:98
Content-Type: application/json;charset=UTF-8
```

HTTP response:**Header**

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "client id": "Moja app 3263351",
  "client_secret": "29Jcq7LgvpgPB2Hqy6PvxE7hKxUbqy2EwhzAgLujG6faqo6mgPMmKji_vBwqQgOTUCfIUdtDQ",
  "client_secret_expires_at": "0"
}
```

3.2.2 (auth/oauth) Autentizácia a Autorizácia requestu

3.2.2.1 (GET auth/oauth/authorize) Autorizačný resource

HTTP request:

Header

```
GET auth/oauth/authorize HTTP/1.1
Host: api.szrb.sk:98
Content-Type: application/x-www-form-urlencoded
response_type=code&
scope=AISP&
client_id=Moja_app_3263351&
state=VsH0TiAB1d3t7yR6VvD31DpUZEVRBXAQ&
redirect_uri=http://www.tpp.sk/TPPTest/Home/LoginReturn&
login_hint=&
code_challenge=o077bZ2WVsphzUSIihF1VUB2H0AE5auo8uP_x8axjW0&
code_challenge_method=S256
```

HTTP response:

Header

```
HTTP/1.1 303 See Other
Content-Type: application/x-www-form-urlencoded
Location:
http://www.tpp.sk/TPPTest/Home/LoginReturn?code=gCyAymoimg0L1bEI&state=VsH0TiAB1d3t7yR6VvD31DpUZEVRBXAQ
```

Klient (PSU) je po autentifikácii presmerovaný späť na poskytovateľa (v našom prípade AISP). Súčasťou URL je parameter *state* a autorizačný kód, ktorý potom tretia strana používa na výmenu za dvojicu tokenov (*access_token* a *refresh_token*).

3.2.2.2 (POST [auth/oauth/token](#)) Získanie tokenov

HTTP request:**Header**

```
POST auth/oauth/token HTTP/1.1
Host: api.srzb.sk
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
TmV3X2N1cnRfMzIzMzNjOlVzVWTFFF5ajNGWGY5cVBUZHo3cTJ5UE4wZ1dVWkFmeDNmZnNpQXBGX3Z0MDE2MzNncEd4cU
9zTGdoUnRldUtiWXN6VW5Ea3FXQ1pFc0VocXpQm1JYQQ //Basic BASE64(CLIENT_ID + ":" + CLIENT_SECRET)
```

Body

```
grant_type=authorization_code&
code=gCyAymoimg0L1bEI&
redirect_uri=http://www.tpp.sk/TPPTest/Home/LoginReturn&
code_verifier=yDWNhLugLI3BqUvXDYWE3DPrggSEyXCR
```

HTTP response:**Header**

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "access_token":
  "RWZzdEJDDdEZXZx1EU0puOWlKWUswSEF4RWNvdUxGY1AycnRxeHdPRjhPa3dsbHFET11OeHdV",
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token":
  "v2FHUFkxYjhnSUhvaE5wcjZ1Qm1nQzFtZDdjSmxoYnlHRmpRb2xUQUhXVFZ1Q1VHcFg0YkM2",
  "scope": "AISP PISP"
}
```

3.2.2.3 (POST [auth/oauth/token](#)) Obnovenie Access tokenu

HTTP request:

Header

```
POST auth/oauth/token HTTP/1.1
Host: api.srzb.sk
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
TmV3X2N1cnRfMzIzMzNjoiVzVWTFFF5ajNGWGY5cVBuZHo3cTJ5UE4wZ1dVWkFmeDNmZnNpQXBGX3Z0MDE2MzNncEd4cU
9zTGdoUnRldUtiWXN6VW5Ea3FXQ1pFc0VocXpQMLJYQQ //Basic BASE64 (CLIENT_ID + ":" + CLIENT_SECRET)
```

Body

```
grant_type=refresh_token&
refresh_token=V2FHUFkxYjhnSUhvaE5wcjZlQmlnQzFtZDdjSmxoYn1HRmpRb2xUQUhXVFZlQ1VHcFg0YkM2&
scope=AISP PISP
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "access_token":
  "w1RjNVBaUDlHan15QVpncmJqYj1JcU1HTFBnallYdlcyZU5NMGZxZEhJa1RYeHAxdkh6Ymd0",
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token":
  "V2FHUFkxYjhnSUhvaE5wcjZlQmlnQzFtZDdjSmxoYn1HRmpRb2xUQUhXVFZlQ1VHcFg0YkM2",
  "scope": "AISP PISP"
}
```

3.2.3 (api/) AISP

3.2.3.1 Všeobecná definícia hlavičiek

HTTP request:

Header

```
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
```

```
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

3.2.3.2 (POST [api/v1/accounts/information](#)) Account Information

HTTP request:

Header

```
POST api/v1/accounts/information HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "iban": "SK8230000000000123123123"
}
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
{
  "account": {
    "name": "Acc 00002456",
    "productName": "Vkladový/Bežný účet",
    "type": "CACC",
    "baseCurrency": "EUR",
    "openDate": "2009-03-16T00:00:00"
  },
  "balances": [
    {
      "typeCodeOrProprietary": "ITAV",
      "amount": {
        "value": 10000000.00,
        "currency": "EUR"
      },
      "creditDebitIndicator": "CRDT",
      "dateTime": "2014-09-23T00:00:00"
    },
    {
      "typeCodeOrProprietary": "ITBD",
      "amount": {
        "value": 10000000.00,
        "currency": "EUR"
      },
      "creditDebitIndicator": "CRDT",
      "dateTime": "2014-09-23T00:00:00"
    }
  ]
}
```


3.2.3.3 (POST [api/v1/accounts/transactions](#)) Account transactions

HTTP request:

Header

```
POST api/v1/accounts/transactions HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "iban": "SK8230000000000123123123",
  "dateFrom": "2021-11-01",
  "dateTo": "2021-11-30",
  "pageSize": 50,
  "page": 0
}
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
{
  "pageCount": 1,
  "transactions": [
    {
      "amount": {
        "value": 75.74,
        "currency": "EUR"
      },
      "creditDebitIndicator": "CRDT",
      "reversalIndicator": false,
      "status": "INFO",
      "bookingDate": "2021-11-18T00:00:00",
      "valueDate": "2021-11-18T00:00:00",
      "paymentDate": "2021-11-18T00:00:00",
      "bankTransactionCode": null,
      "transactionDetails": {
        "references": {
          "additionalTransactionInformation": "",
          "instructionIdentification": null,
          "endToEndIdentification": "/VS/SS/KS",
          "transactionIdentification": null,
          "mandateIdentification": null,
          "chequeNumber": null
        },
        "counterValueAmount": null,
        "relatedParties": {
          "debtor": {
            "name": "Vnutrobankovy ucet"
          },
          "debtorAccount": {
            "identification": "SK208120000000002237060"
          },
          "creditor": {
            "name": "Account 00002456",
            "identification": null
          },
          "creditorAccount": {
            "identification": "SK8230000000000123123123"
          },
          "tradingParty": null
        },
        "relatedAgents": {
          "debtorAgent": {
            "financialInstitutionIdentification": "BSLOS22XXX"
          }
        }
      }
    }
  ]
}
```

```
    },
    "creditorAgent": {
      "financialInstitutionIdentification": "SLZBSKBAXXX"
    }
  },
  "remittanceInformation": "Informácia o platbe",
  "relatedDates": null,
  "additionalTransactionInformation": "Dalšie informácie o platbe"
}
]
}
```

3.2.3.4 (GET [api/v2/accounts](#)) List of accounts

HTTP request:

Header

```
GET api/v2/accounts HTTP/1.1
Host: api.srzrb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
{
  "creationDateTime": "2022-06-06T13:31:23.5937196+02:00",
  "accounts": [
    {
      "identification": {
        "iban": "SK823000000000123123123"
      },
      "name": "Acc 00002456",
      "productName": "Bežný účet",
      "type": "CACC",
      "baseCurrency": "EUR",
      "servicer": {
        "financialInstitutionIdentification": "SLZBSKBAXXX"
      },
      "consent": [
        "AISP",
        "PISP"
      ]
    }
  ]
}
```

3.2.4 (api/) PISP

3.2.4.1 Všeobecná definícia hlavičiek

HTTP request:**Header**

```
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:**Header**

```
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

3.2.4.2 (POST [api/v1/payments/standard/iso](#)) Standard payment initialization (XML)

HTTP request:

Header

```
POST api/v1/payments/standard/iso HTTP/1.1
Host: api.srzb.sk
Content-Type: application/xml;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
<?xml version="1.0" encoding="utf-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.03"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <CstmrCdtTrfInitn>
    <GrpHdr>
      <MsgId>1000027313</MsgId>
      <CreDtTm>2022-05-31T07:43:26</CreDtTm>
      <NbOfTxs>1</NbOfTxs>
      <CtrlSum>23.00</CtrlSum>
      <InitgPty>
        <Nm>Meno</Nm>
        <Id>
          <OrgId>
            <Othr>
              <Id>ABC83902001</Id>
            </Othr>
          </OrgId>
        </Id>
      </InitgPty>
    </GrpHdr>
    <PmtInf>
      <PmtInfId>1000027313</PmtInfId>
      <PmtMtd>TRF</PmtMtd>
      <PmtTpInf>
        <SvcLvl>
          <Cd>URNS</Cd>
        </SvcLvl>
      </PmtTpInf>
      <ReqdExctnDt>2022-06-06</ReqdExctnDt>
      <Dbtr>
        <Nm>meno</Nm>
        <PstlAdr>
          <Ctry>SK</Ctry>
          <AdrLine>Ulica 5</AdrLine>
        </PstlAdr>
      </Dbtr>
      <DbtrAcct>
        <Id>
          <IBAN>SK8230000000000123123123</IBAN>
        </Id>
        <Ccy>EUR</Ccy>
      </DbtrAcct>
      <DbtrAgt>
        <FinInstnId>
          <BIC>SLZBSKBAXXX</BIC>
          <PstlAdr>
            <Ctry>SK</Ctry>
          </PstlAdr>
        </FinInstnId>
      </DbtrAgt>
      <ChrgBr>SHAR</ChrgBr>
      <CdtTrfTxInf>
        <PmtId>
          <InstrId>02-5001F1100000012015</InstrId>
          <EndToEndId>/VS1111111111/KS0968/SS2222222222</EndToEndId>
        </PmtId>
        <PmtTpInf>
          <InstrPrty>NORM</InstrPrty>
        </PmtTpInf>
        <Amt>
```

```
<InstdAmt Ccy="EUR">23.00</InstdAmt>
</Amt>
<CdtrAgt>
  <FinInstnId>
    <BIC>BSLOS22</BIC>
    <PstlAdr>
      <Ctry>SK</Ctry>
    </PstlAdr>
  </FinInstnId>
</CdtrAgt>
<Cdtr>
  <Nm>Meno príjemcu</Nm>
  <PstlAdr>
    <Ctry>SK</Ctry>
    <AdrLine>Ulica 45</AdrLine>
    <AdrLine>Bratislava Slovenská republika</AdrLine>
  </PstlAdr>
</Cdtr>
<CdtrAcct>
  <Id>
    <IBAN>SK0281201020073084015915</IBAN>
  </Id>
</CdtrAcct>
<RmtInf>
  <Ustrd>/INV/1234567890</Ustrd>
</RmtInf>
</CdtTrfTxInf>
</PmtInf>
</CstmrCdtTrfInitn>
</Document>
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/xml;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
<Document xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:pain.002.001.03">
  <CstmrPmtStsRpt>
    <GrpHdr>
      <MsgId>10004851</MsgId>
      <CreDtTm>2022-06-06T13:58:25.3382882+02:00</CreDtTm>
      <DbtrAgt>
        <FinInstnId>
          <BIC>SLZBSKBA333</BIC>
        </FinInstnId>
      </DbtrAgt>
    </GrpHdr>
    <OrgnlGrpInfAndSts>
      <OrgnlMsgId>1000027313</OrgnlMsgId>
      <OrgnlCreDtTm>2022-05-31T07:43:26</OrgnlCreDtTm>
      <OrgnlNbOfTxs>1</OrgnlNbOfTxs>
      <OrgnlCtrlSum>23.00</OrgnlCtrlSum>
      <NbOfTxsPerSts>
        <DtldNbOfTxs>1</DtldNbOfTxs>
        <DtldSts>ACTC</DtldSts>
      </NbOfTxsPerSts>
    </OrgnlGrpInfAndSts>
    <OrgnlPmtInfAndSts>
      <OrgnlPmtInfId>1000027313</OrgnlPmtInfId>
      <OrgnlNbOfTxs>1</OrgnlNbOfTxs>
      <OrgnlCtrlSum>23.00</OrgnlCtrlSum>
      <TxInfAndSts>
        <StsId>10004851</StsId>
        <OrgnlInstrId>02-5001F1100000012015</OrgnlInstrId>
        <OrgnlEndToEndId>/VS1111111111/KS0968/SS2222222222</OrgnlEndToEndId>
        <StsRsnInf>
          <Orgtr>
            <Id>
              <OrgId>
```

```
        <BICorBEI>SLZBSKBAXXX</BICorBEI>
      </OrgId>
    </Orgtr>
  </StsRsnInf>
  <AcctSvcrRef>10004851</AcctSvcrRef>
  <OrgnlTxRef>
    <Amt>
      <InstdAmt Ccy="EUR">23.00</InstdAmt>
    </Amt>
    <ReqdExctnDt>2022-06-06</ReqdExctnDt>
    <RmtInf>
      <Ustrd>/INV/1234567890</Ustrd>
    </RmtInf>
    <Dbtr>
      <Nm>Meno</Nm>
    </Dbtr>
    <DbtrAcct>
      <Id>
        <IBAN>SK823000000000123123123</IBAN>
      </Id>
    </DbtrAcct>
    <DbtrAgt>
      <FinInstnId>
        <BIC>SLZBSKBAXXX</BIC>
      </FinInstnId>
    </DbtrAgt>
    <CdtrAgt>
      <FinInstnId>
        <BIC>BSLOS22</BIC>
      </FinInstnId>
    </CdtrAgt>
    <Cdtr>
      <Nm>Meno príjemcu</Nm>
    </Cdtr>
    <CdtrAcct>
      <Id>
        <IBAN>SK0281201020073084015915</IBAN>
      </Id>
    </CdtrAcct>
  </OrgnlTxRef>
</TxInfAndSts>
</OrgnlPmtInfAndSts>
</CstmrPmtStsRpt>
</Document>
```


3.2.4.4 (POST [auth/oauth/token](#)) Získanie tokenu pre požiadavku Standard payment submission

HTTP request:

Header

```
POST auth/oauth/token HTTP/1.1
Host: api.srzb.sk
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
TmV3X2NlcnRfMzIzMzNjoiVzVWTFFF5ajNGWGY5cVBUZHo3cTJ5UE4wZ1dVWkFmeDNmZnNpQXBGX3Z0MDE2MzNncEd4cU
9zTGdoUnRldUtiWXN6VW5Ea3FXQlpFc0VocXpQmlJYQQ //Basic BASE64 (CLIENT_ID + ":" + CLIENT_SECRET)
```

Body

```
grant_type=authorization_code&
code=IDPCyAymoimg0L1bEI&
redirect_uri=http://www.tpp.sk/TPPTest/Home/LoginReturn&
code_verifier=yDWNhLugLI3BqUvXDYWE3DPrggSEyXCR
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "access_token": "WmszcjFUOWJGRWpkRVlhSjhFZTRPekZHAGJGMU1GdcEFtWU5PdkI0aU91N315",
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token": null,
  "scope": "PISP"
}
```

3.2.4.5 (POST [api/v1/payments/paymentSubmission](#)) Standard payment submission

HTTP request:**Header**

```
POST api/v1/payments/paymentSubmission HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer WmszcjFUOWJGRWpkRVlhSjhFZTRPekZHaGJGMU1GdcEftWU5PdkI0aU91N315

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:**Header**

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "orderId": "10004851",
  "status": "PDNG",
  "reasonCode": "Authorized",
  "statusDateTime": "2022-06-06T14:40:08.2478907+02:00"
}
```

3.2.4.6 (GET [api/v1/payments/{orderId}/status](#)) Payment order status

HTTP request:

Header

```
GET api/v1/payments/10004851/status HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
{
  "orderId": "10004851",
  "status": "ACSP",
  "reasonCode": "Processing",
  "statusDateTime": "2022-06-06T13:58:25.3382882"
}
```

3.2.4.7 (DELETE [api/v1/payments/{orderId}/rcp](#)) Cancel payment

HTTP request:**Header**

```
DELETE api/v1/payments/10004851/rcp HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:**Header**

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

```
{
  "orderId": "10004851"
}
```

3.2.4.8 (POST [api/v1/accounts/balanceCheck](#)) Balance check

HTTP request:

Header

```
POST api/v1/accounts/balanceCheck HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "instructionIdentification": "9b76608457de48b2be531bd2804ae0b7",
  "creationDateTime": "2019-05-27T18:00:00+01:00",
  "iban": "SK8230000000000123123123",
  "amount": {
    "value": 123.56,
    "currency": "EUR"
  },
  "relatedParties": {
    "tradingParty": {
      "identification": "AAA-GG-SSSS",
      "name": "Merchant ID",
      "address": "Ulica 123123, Mesto",
      "countryCode": "SK",
      "merchantCode": "3370"
    }
  },
  "references": {
    "chequeNumber": "**** * 1111",
    "holderName": "Jan Dopek"
  }
}
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "response": "APPR",
  "dateTime": "2022-06-06T15:14:50.0564144+02:00"
}
```

3.2.4.9 (GET [api/v1/standingOrders/Periodicity](#)) Trvalý příkaz - periodicity

HTTP request:

Header

```
GET api/v1/standingOrders/Periodicity HTTP/1.1
Host: api.srzrb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

Body

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


3.2.4.11 (POST [api/v1/standingOrders](#)) Trvalý príkaz – vytvorenie nového

HTTP request:

Header

```
POST api/v1/standingOrders HTTP/1.1
Host: api.srzrb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "standingOrderData":
  {
    "iban": "SK8230000000000123123123",
    "partner":
    {
      "name": "Meno partnera",
      "address":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      },
      "iban": "SK308120000000000272727",
      "bic": "BSLOS22XXX",
      "bankname": "Meno banky partnera",
      "bankaddress":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      }
    },
    "currency": "EUR",
    "amount": 2.60,
    "periodicity": "21",
    "dayOfPayment": 31,
    "failureRetries": 0,
    "dateFrom": "2022-12-16",
    "dateTo": "2023-08-11",
    "variableSymbol": "1111111111",
    "specificSymbol": "2222222222",
    "constantSymbol": "0968",
    "paymentPurpose": "Poznamka",
    "noteForBeneficiary": "Správa pre príjemcu"
  }
}
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "id": 10004890,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```


3.2.4.12 (PUT api/v1/standingOrders/{Id}) Trvalý príkaz – zmena

HTTP request:

Header

```
PUT api/v1/standingOrders/2216267 HTTP/1.1
Host: api.srzrb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "sequence": 1,
  "standingOrderData":
  {
    "iban": "SK8230000000000123123123",
    "partner":
    {
      "name": "Meno partnera",
      "address":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      },
      "iban": "SK308120000000000272727",
      "bic": "BSLOS22XXX",
      "bankname": "meno",
      "bankaddress":
      {
        "street": "Ulica",
        "city": "Mesto",
        "country": "SK"
      }
    },
    "currency": "EUR",
    "amount": 2.80,
    "periodicity": "21",
    "dayOfPayment": 15,
    "failureRetries": 1,
    "dateFrom": "2022-06-08",
    "dateTo": "2022-12-30",
    "variableSymbol": "1111111111",
    "specificSymbol": "2222222222",
    "constantSymbol": "0968",
    "paymentPurpose": "Poznamka",
    "noteForBeneficiary": "Správa pre príjemcu"
  }
}
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "id": 10004891,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```

3.2.4.13 (DELETE [api/v1/standingOrders/{Id}](#)) Trvalý príkaz – zrušenie

HTTP request:

Header

```
DELETE api/v1/standingOrders/2216267 HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "id": 10004892,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```

3.2.4.14 (POST [api/v1/payments](#)) Payment initialization – Vytvorenie platby (JSON)

HTTP request:

Header

```
POST api/v1/standingOrders HTTP/1.1
Host: api.srzrb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "paymentIdentification": {
    "instructionIdentification": "F111222",
    "endToEndIdentification": "/VS1111111111/KS0968/SS2222222222"
  },
  "paymentTypeInformation": {
    "instructionPriority": "NORM" /* táto položka nemusí byť zadaná */
  },
  "amount": {
    "instructedAmount": {
      "value": 10.0,
      "currency": "EUR"
    }
  },
  "chargeBearer": "SHAR", /* táto položka nemusí byť zadaná */
  "requestedExecutionDate": "2022-12-16",
  "debtorAccount": {
    "identification": {
      "iban": "SK823000000000123123123" /* táto položka nemusí byť zadaná */
    }
  },
  "creditor": {
    "name": "Meno partnera",
    "postalAddress": {
      "streetName": "Ulica",
      "buildingNumber": "23",
      "postCode": "12345",
      "townName": "Mesto",
      "country": "SK"
    }
  },
  "creditorAccount": {
    "identification": {
      "iban": "SK308120000000000272727"
    }
  },
  "creditorAgent": {
    "financialInstitutionIdentification": {
      "bic": "BSLOS22",
      "name": "Meno banky partnera",
      "postalAddress": { /* táto sekcia nemusí byť zadaná */
        "streetName": "Ulica",
        "buildingNumber": "111",
        "postCode": "12345",
        "townName": "Mesto",
        "country": "SK"
      }
    }
  },
  "remittanceInformation": {
    "unstructured": "Text remittanceInformation > unstructured"
  },
  "purpose": {
    "proprietary": "Text purpose > proprietary (účel platby)."
  }
}
```

HTTP response:**Header**

```
HTTP/1.1 200 ok  
Content-Type: application/json;charset=UTF-8
```

Body

```
{  
  "id": 10004890,  
  "status": "ACTC",  
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"  
  "paymentTypeInformation": {  
    "code": "ESCT"  
  }  
}
```

3.2.5 (api/) PIISP

3.2.5.1 Všeobecná definícia hlavičiek

HTTP request:**Header**

```
Host: api.srzrb.sk  
Content-Type: application/json;charset=UTF-8  
Authorization: Bearer IDWJJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
```

```
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351  
PSU-IP-Address: 192.168.0.100  
PSU-Device-OS: iOS 12.1.4  
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:**Header**

```
Content-Type: application/json;charset=UTF-8  
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

3.2.5.2 (POST [api/v1/accounts/balanceCheck](#)) Balance check

HTTP request:

Header

```
POST api/v1/accounts/balanceCheck HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "instructionIdentification": "9b76608457de48b2be531bd2804ae0b7",
  "creationDateTime": "2019-05-27T18:00:00+01:00",
  "iban": "SK8230000000000123123123",
  "amount": {
    "value": 123.56,
    "currency": "EUR"
  },
  "relatedParties": {
    "tradingParty": {
      "identification": "AAA-GG-SSSS",
      "name": "Merchant ID",
      "address": "Ulica 123123, Mesto",
      "countryCode": "SK",
      "merchantCode": "3370"
    }
  },
  "references": {
    "chequeNumber": "**** * 1111",
    "holderName": "Jan Dopek"
  }
}
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "response": "APPR",
  "dateTime": "2022-06-06T15:14:50.0564144+02:00"
}
```

3.2.6 ([api/](#)) Súhlasy

3.2.6.1 Všeobecná definícia hlavičiek

HTTP request:

Header

```
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:**Header**

```
Content-Type: application/json;charset=UTF-8  
Response-ID: 7deb90a9-9900-4c90-a91c-3ecc888c2c88
```

3.2.6.2 (POST [api/v1/consents/global](#)) Vytvorenie žiadosti na súhlas typu Global Consent**HTTP request:****Header**

```
POST api/v1/consents/global HTTP/1.1  
Host: api.srzb.sk  
Content-Type: application/json;charset=UTF-8  
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX  
  
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351  
PSU-IP-Address: 192.168.0.100  
PSU-Device-OS: iOS 12.1.4  
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body**HTTP response:****Header**

```
HTTP/1.1 200 ok  
Content-Type: application/json;charset=UTF-8
```

Body

```
{  
  "id": 10004892,  
  "status": "ACTC",  
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"  
}
```

3.2.6.3 (POST [api/v1/consents/bankOffered](#)) Vytvorenie žiadosti na súhlas typu Bank Offered Consent**HTTP request:****Header**

```
POST api/v1/consents/bankOffered HTTP/1.1  
Host: api.srzb.sk  
Content-Type: application/json;charset=UTF-8  
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX  
  
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351  
PSU-IP-Address: 192.168.0.100  
PSU-Device-OS: iOS 12.1.4  
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body**HTTP response:****Header**

```
HTTP/1.1 200 ok  
Content-Type: application/json;charset=UTF-8
```

Body

```
{
```

```
{
  "id": 10004892,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```

3.2.6.4 (POST [api/v1/consents/detailed](#)) Vytvorenie žiadosti na súhlas typu Detailed Consent

HTTP request:

Header

```
POST api/v1/consents/detailed HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
```

```
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

Body

```
{
  "accounts": ["SK823000000000123123123", "SK113000000000111111111"],
  "scopes": ["AISP", "PISP"]
}
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "id": 10004890,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```

3.2.6.5 (POST [api/v1/consents](#)) Ukončenie platného súhlasu

HTTP request:

Header

```
POST api/v1/consents HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer IDWJJBCHQ5DZJWEMO7ZWM4DLYWOFWKXX
```

```
Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "id": 10004890,
  "status": "ACTC",
  "createdDate": "2022-12-21T14:06:58.3681146+01:00"
}
```


3.2.6.7 (POST [auth/oauth/token](#)) Získanie tokenu pre požiadavku Request of consent submission

HTTP request:

Header

```
POST auth/oauth/token HTTP/1.1
Host: api.srzb.sk
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
TmV3X2NlcnRfMzIzMzNj01VzVWTF5ajNGWGY5cVBUZHo3cTJ5UE4wZ1dVWkFmeDNmZnNpQXBGX3Z0MDE2MzNncEd4cU
9zTGdoUnRldUtiWXN6VW5Ea3FXQ1pFc0VocXpQM1JYQQ //Basic BASE64 (CLIENT_ID + ":" + CLIENT_SECRET)
```

Body

```
grant_type=authorization_code&
code=IDPCyAymoimg0L1bEI&
redirect_uri=http://www.tpp.sk/TPPTest/Home/LoginReturn&
code_verifier=yDWNhLugLI3BqUvXDYWE3DPrggSEyXCR
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "access token": "wmszcjFUOWJGRWpkRV1hSjhFZTRPekZHaGJGMU1GdcEftWU5PdkI0aU91N315",
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token": null,
  "scope": "PISP"
}
```

3.2.6.8 (POST [api/v1/consents/submission](#)) Request of consent submission

HTTP request:

Header

```
POST api/v1/consents/submission HTTP/1.1
Host: api.srzb.sk
Content-Type: application/json;charset=UTF-8
Authorization: Bearer wmszcjFUOWJGRWpkRV1hSjhFZTRPekZHaGJGMU1GdcEftWU5PdkI0aU91N315

Request-ID: c2c48fc8-1f79-4934-a47b-56d61a28f351
PSU-IP-Address: 192.168.0.100
PSU-Device-OS: iOS 12.1.4
PSU-User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
```

HTTP response:

Header

```
HTTP/1.1 200 ok
Content-Type: application/json;charset=UTF-8
```

Body

```
{
  "orderId": "10004851",
  "status": "PDNG",
  "reasonCode": "Authorized",
  "statusDateTime": "2022-06-06T14:40:08.2478907+02:00"
}
```

4. 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/files/slovak-banking-api-standard-2_0-2.pdf