

Slovak Banking API Standard

API Workshop, Bratislava, 5.2.2019



01.

Aktivita SBA v oblasti PSD2

Milena Koreňová

Nová smernica o platobných službách PSD2

- základné legislatívne piliere spolupráce bánk s tretími stranami v oblasti platobných služieb
- mnoho otvorených otázok, nutné komplexné riešenie – výzva pre tvorcov (Európsku komisiu a EBA)
- dôkazom je postupné dotváranie sekundárnej legislatívy

Zákon o platobných službách

- banky od 13.1.2018 musia umožniť komunikáciu s tretími stranami pri poskytovaní príslušných služieb, pričom pravidlá silnej autentifikácie a bezpečnej komunikácie budú účinné až od 14.9.2019 (medziobdobie)
- Slovak Banking API Standard platný od 13.1.2018
- sledovanie trendov tvorby API na európskej úrovni – zapojenie do prác API Evaluation Group



02.

Slovak Banking API Standard: Základné charakteristiky

Základné charakteristiky Slovak Banking API Standard

- bezpečná komunikácia
- minimálne požiadavky
- dobrovoľnosť
- otvorenosť

Dizajn štandardu

- každá z povinných služieb rozhrania sa viaže iba s jedným platobných účtom klienta,
- jednoznačný identifikátor účtu (IBAN) by mal byť umiestnený v tele HTTP požiadavky, prípadne v hlavičke HTTP požiadavky,
- dátový model štandardu by mal primerane používať dátové prvky, výrazy a sémantiku podľa normy ISO 20022.



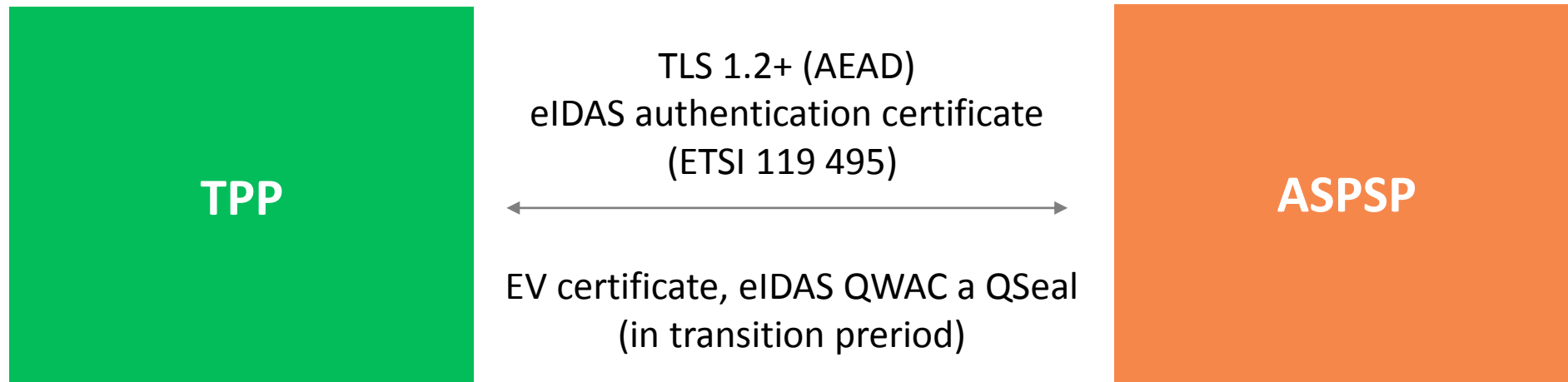
03.

Bezpečnostné charakteristiky štandardu

Peter Kopriva

TPP and ASPSP Authentication framework

- TLS version 1.2+ pre bezpečnú komunikačnú vrstvu.
- AEAD šifrovanie
- pre autentifikáciu je potrebný eIDAS certifikát



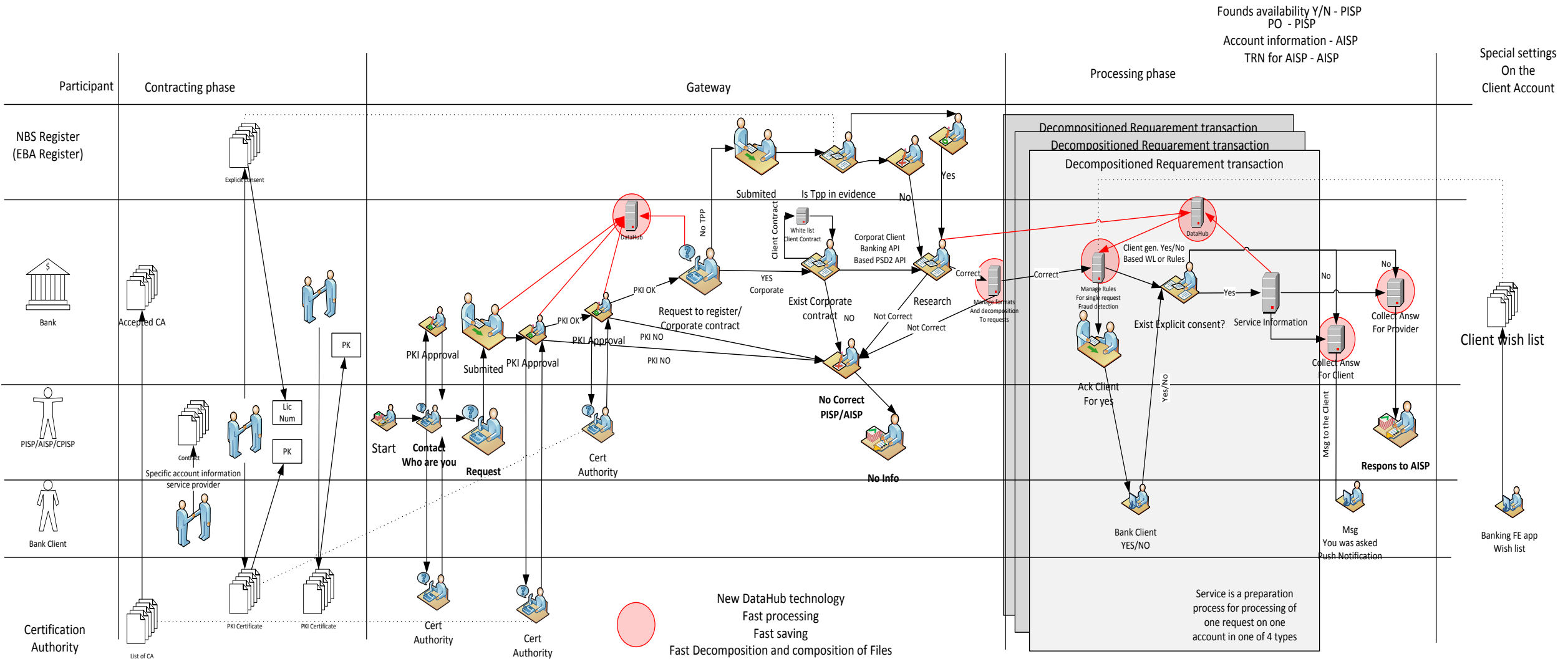
Použitie autorizačný framework-u OAuth 2.0

- automatické pridelenie technického identifikátora tretím stranám ([client_id](#), [client_secret](#), [code_verifier](#)).
- PKCE (RFC 7636) rozšírenie OAuth 2.0
- ASPSP komunikuje s TPP prostredníctvom OAuth 2.0 ([access_token](#) and [refresh_token](#)).
- SBAS podporuje získanie tokenu pomocou Authorization code grant flow a Client credentials grant flow.
- [refresh_token](#) je limitovaný na obdobie 90 dní
- [access_token](#) je naviazaný na užívateľa a platobný účet
- tokeny môžu byť previazane s viacerými účtami klienta, ak sú tieto účty k dispozícii

Pridelenie technického identifikátora („enrollment“)

API endpoint	Metóda	Popis
https://ib.banka.sk/ enroll	POST	Výstupom služby je technický identifikátor client_id a client_secret
https://ib.banka.sk/ enroll/{client_id}	PUT	Tretia strana môže pomocou tejto služby požiadať o zmenu registračných údajov.
https://ib.banka.sk/ enroll/{client_id}	DELETE	Tretia strana môže pomocou tejto služby požiadať o výmaz registračných údajov.
https://ib.banka.sk/ enroll/{client_id}/renewSecret	POST	Tretia strana môže pomocou tejto služby požiadať o nový údaj: client_secret.

PSD2 v skratke





04.

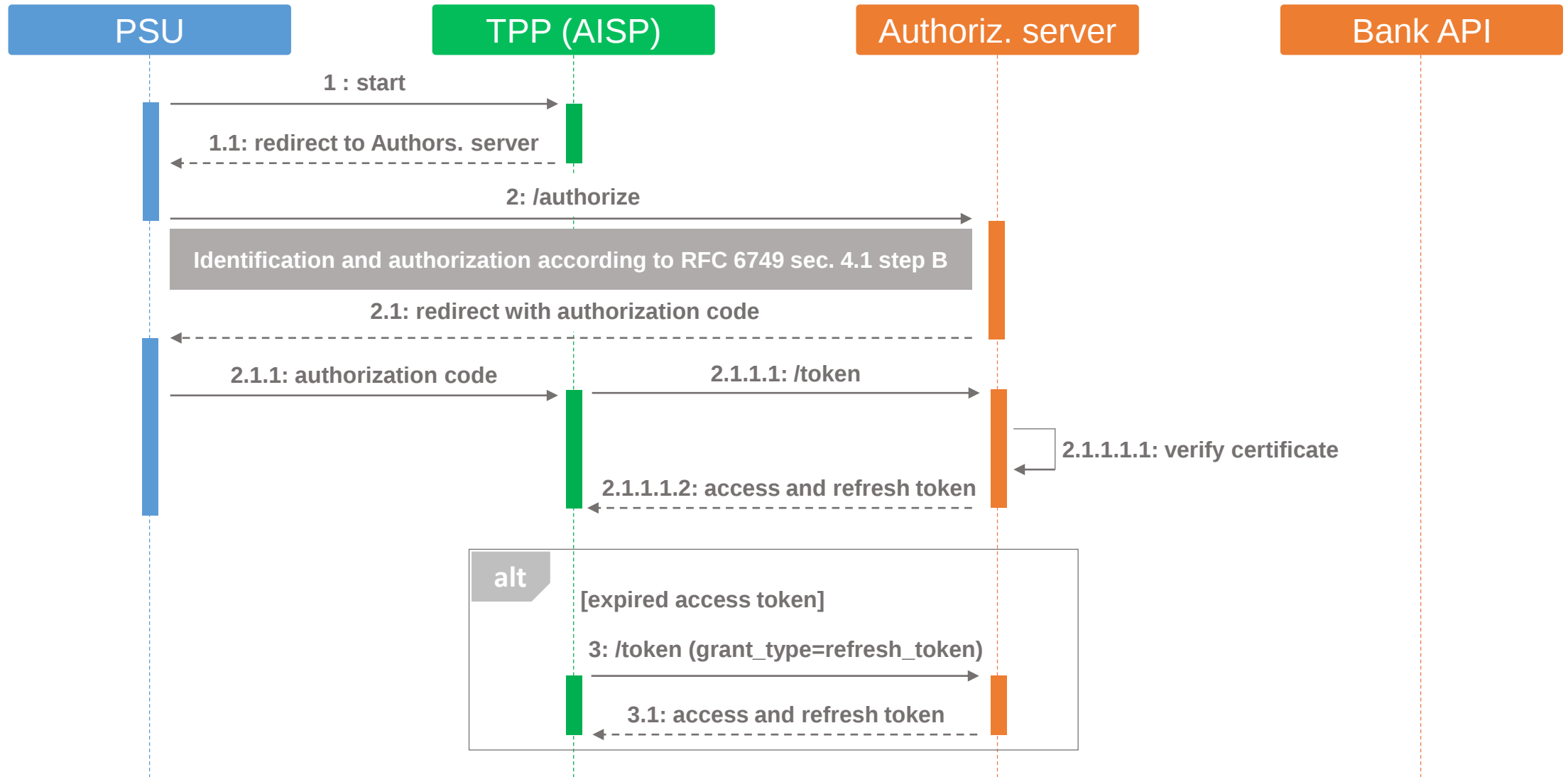
Poskytovateľ služieb informovania o účte (AISP)

Martin Špaček

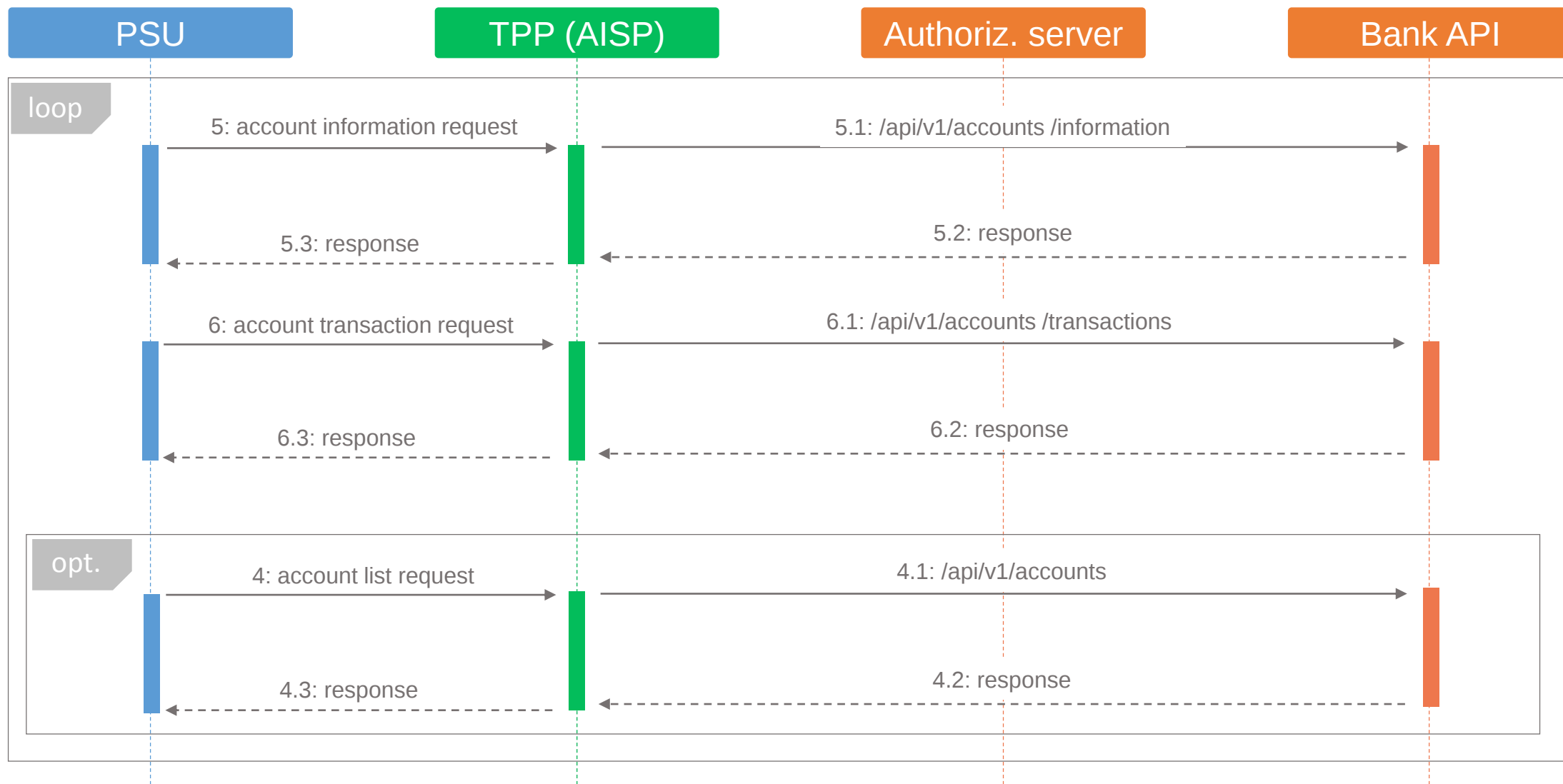
Definície endpointov pre AISP

API endpointy	Metóda	Charakter	Popis
/api/v1/ accounts/information	POST	Povinná	Informácie o účte – služba poskytuje informácie (vrátane zostatkov) o konkrétnom platobnom účte
/api/v1/ accounts/transactions	POST	Povinná	Transakcie – služba poskytuje zoznam transakcií na konkrétnom platobnom účte v JSON formáte, ktorého šematika vychádza z CAMT.054
/api/v1/ accounts	GET	Dobrovoľná	Zoznam účtov – výstupom služby je zoznam účtov, pri ktorých klient udelil dlhodobý mandát pre špecifickú konkrétnu tretiu stranu. Zoznam účtov je bez zostatkov.

Získanie tokenov pre AISP (PISP)



Volania služieb po získaní platného „access token-u“





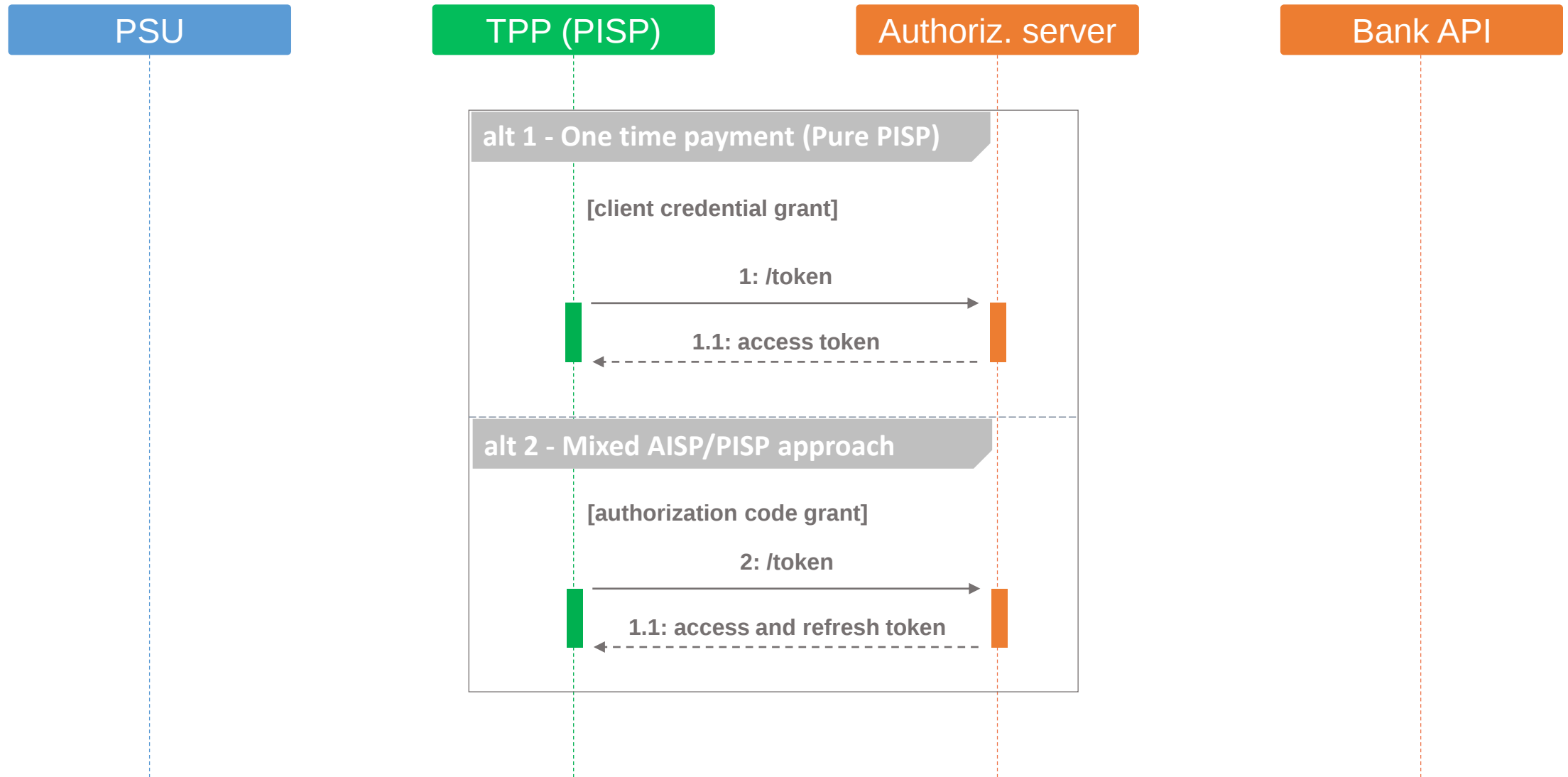
05.

Poskytovateľ služieb iniciácie
platby (PISP)

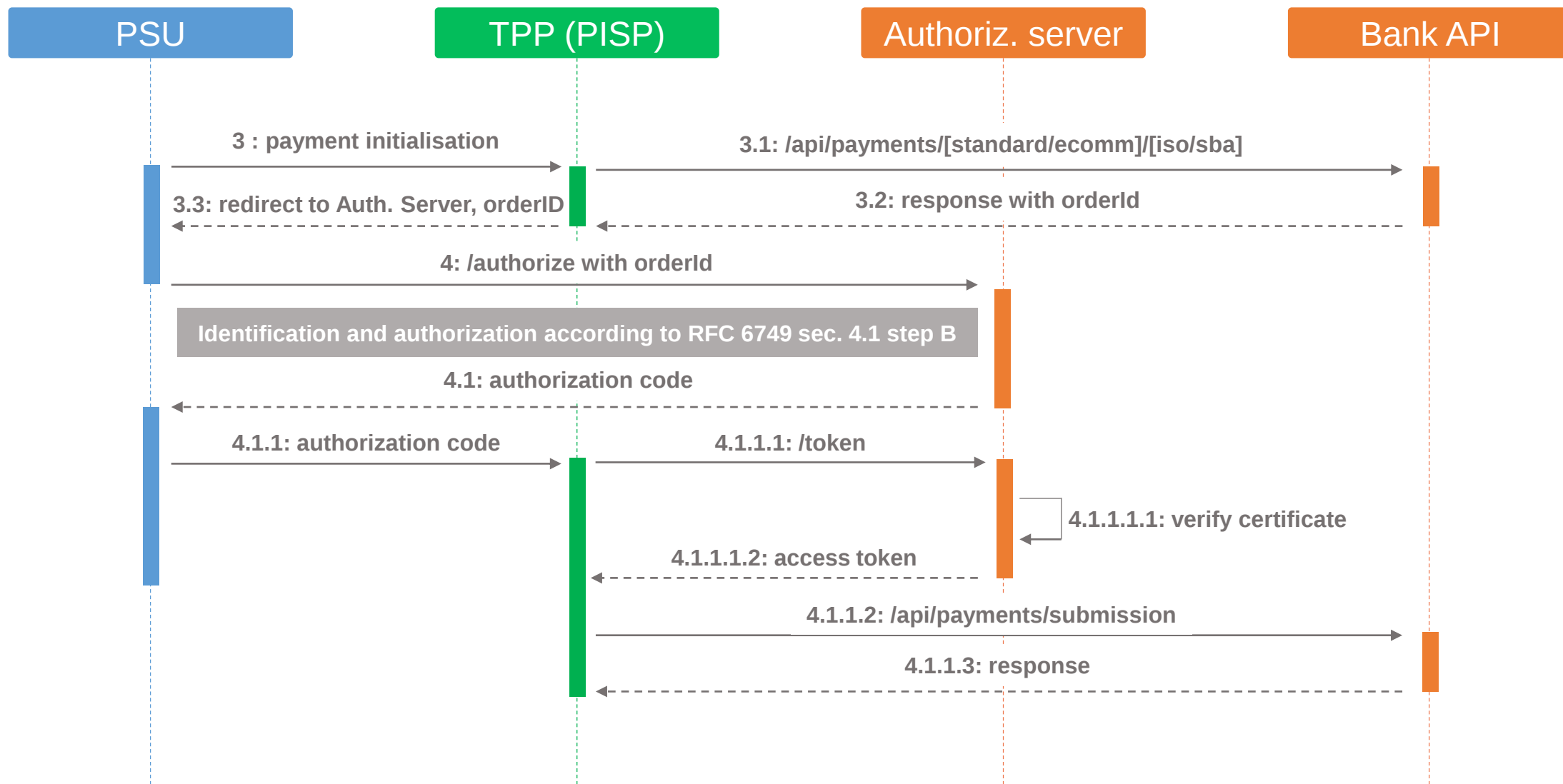
Definície endpointov pre PISP

API endpoint	Metóda	Charakter	Popis
/api/v1/ payments/standard/iso	POST	Povinná	Standard payment initialization – službou tretia strana inicializuje platbu vo formáte XML format (PAIN.001)
/api/v1/ payments/submission	POST	Povinná	Standard payment submission – služba umožňuje potvrdenie platby po získaní platného tokenu platby
/api/v1/ payments/{orderId}/status	GET	Povinná	Payment order status – služba poskytuje informáciu o aktuálnom stave inicializovanej platby
/api/v1/ payments/standard/sba	POST	Dobrovoľná	Standard payment initialization – službou tretia strana inicializuje platbu vo formáte JSON
/api/v1/ payments/ecom/iso	POST	Dobrovoľná	Ecommerce payment initialization – službou tretia strana inicializuje okamžitú platbu vo formáte XML (PAIN.001)
/api/v1/ payments/ecom/sba	POST	Dobrovoľná	Ecommerce payment initialization – službou tretia strana inicializuje okamžitú platbu vo formáte JSON

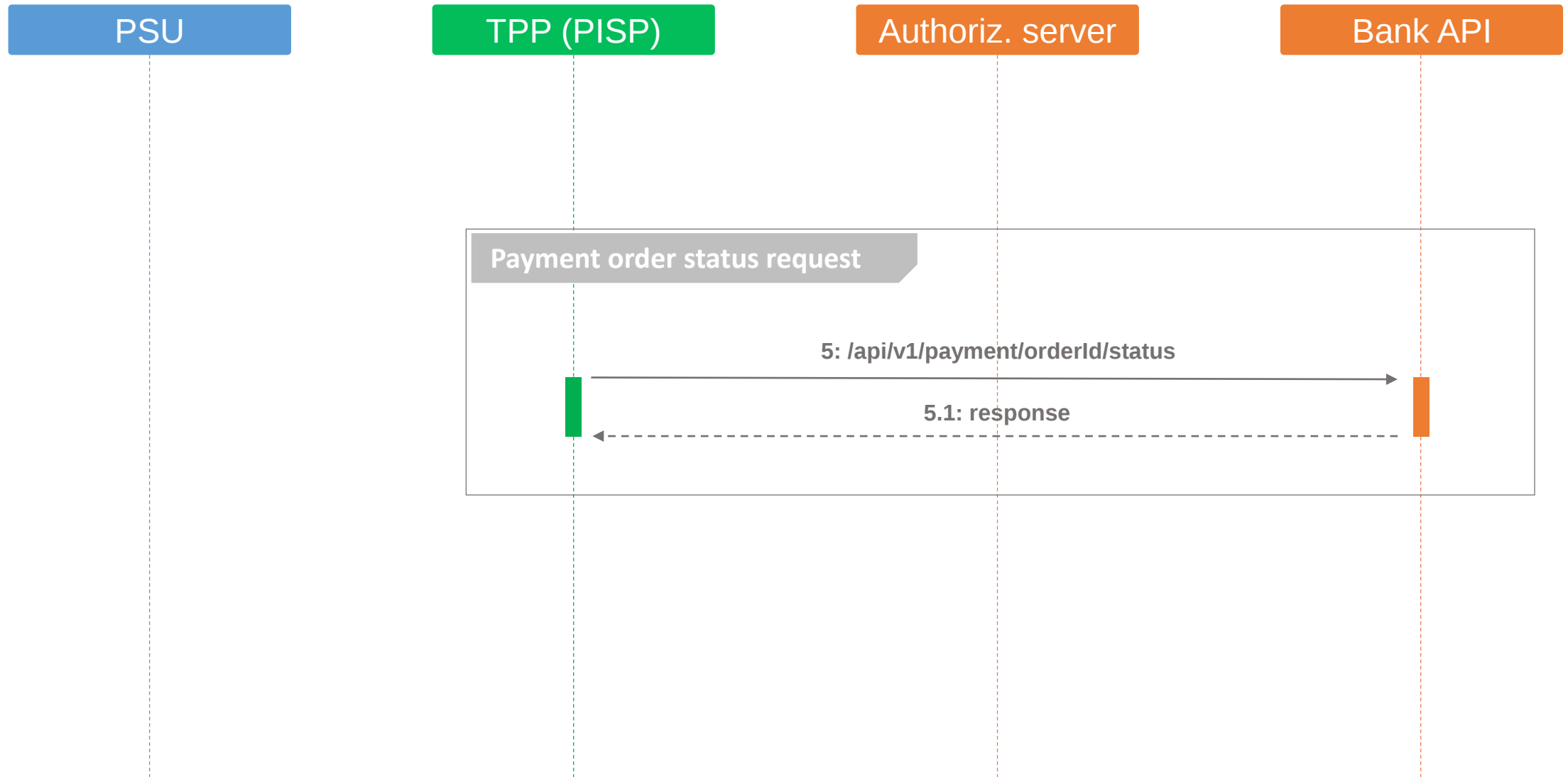
Získanie tokenov pre PISP



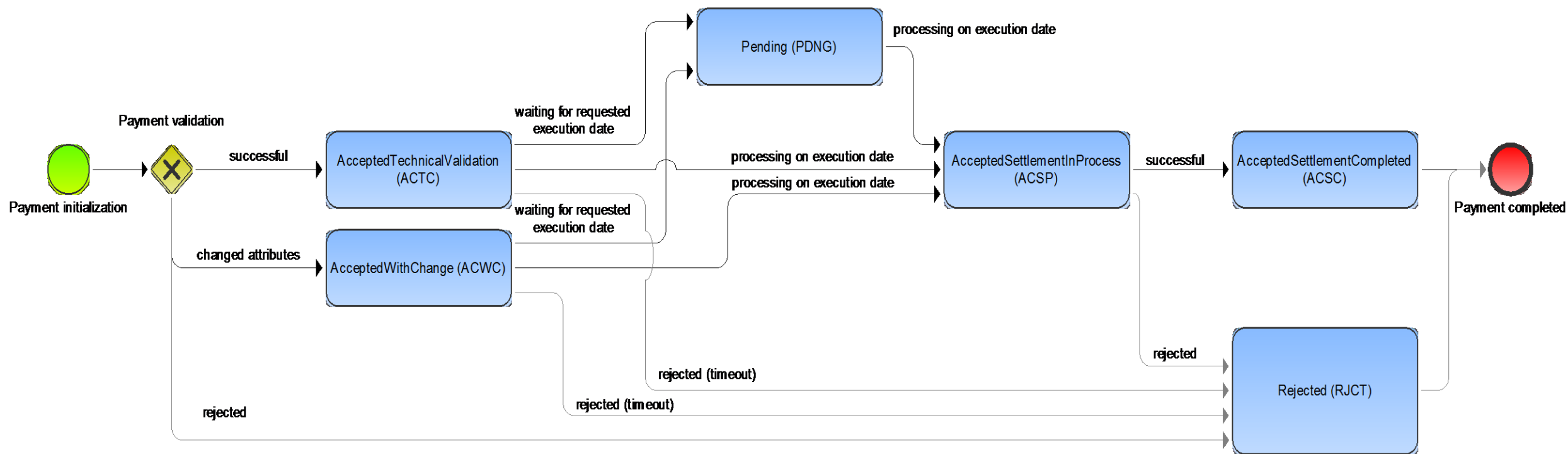
Inicializácia platby s jej potvrdením



Získanie informácie o stave platby



Stavy platby uvedené v štarde





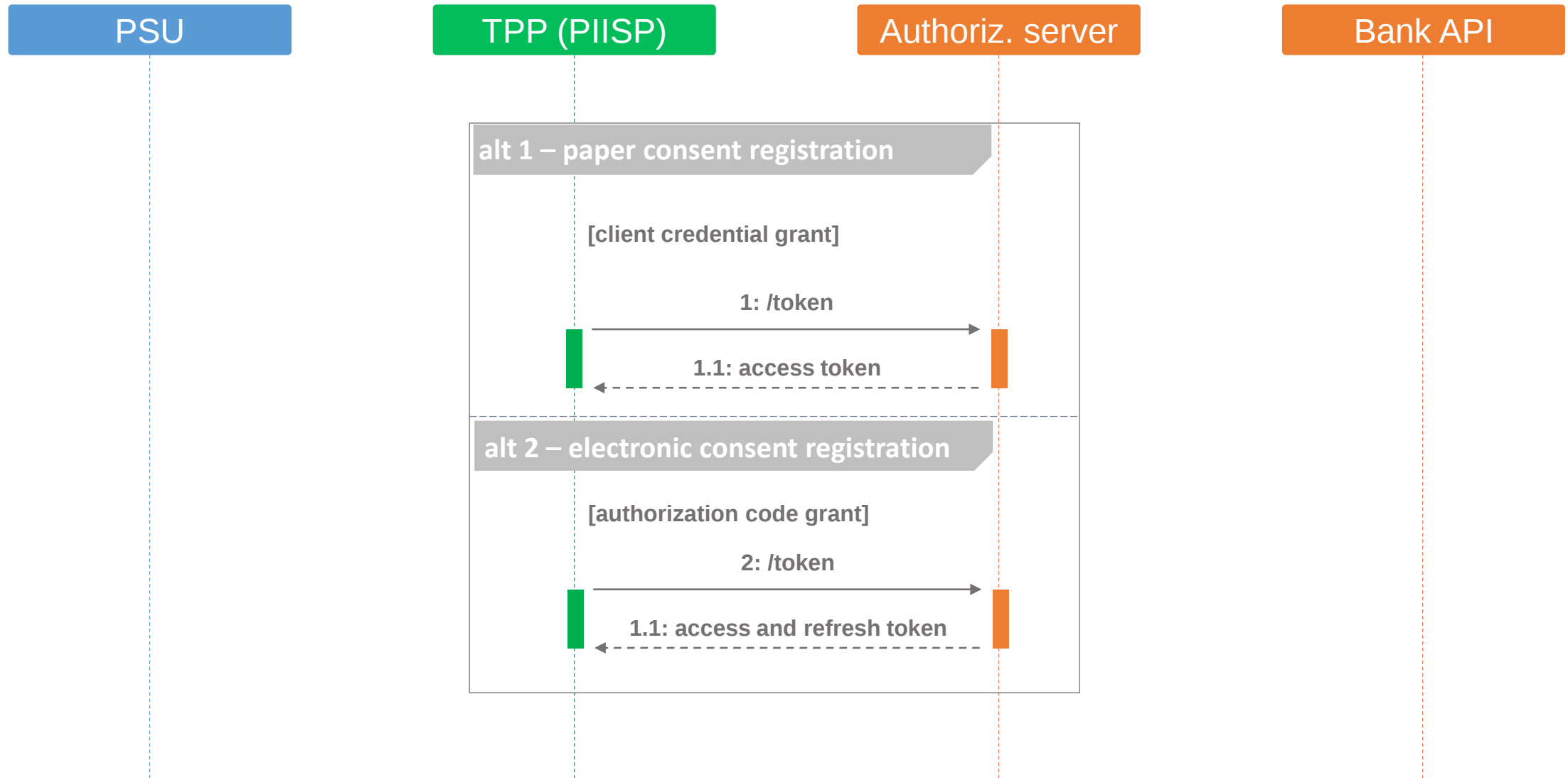
06.

Poskytovateľ plat. služieb
vydávajúci plat. prostriedok
viazaný na kartu (PIISP)

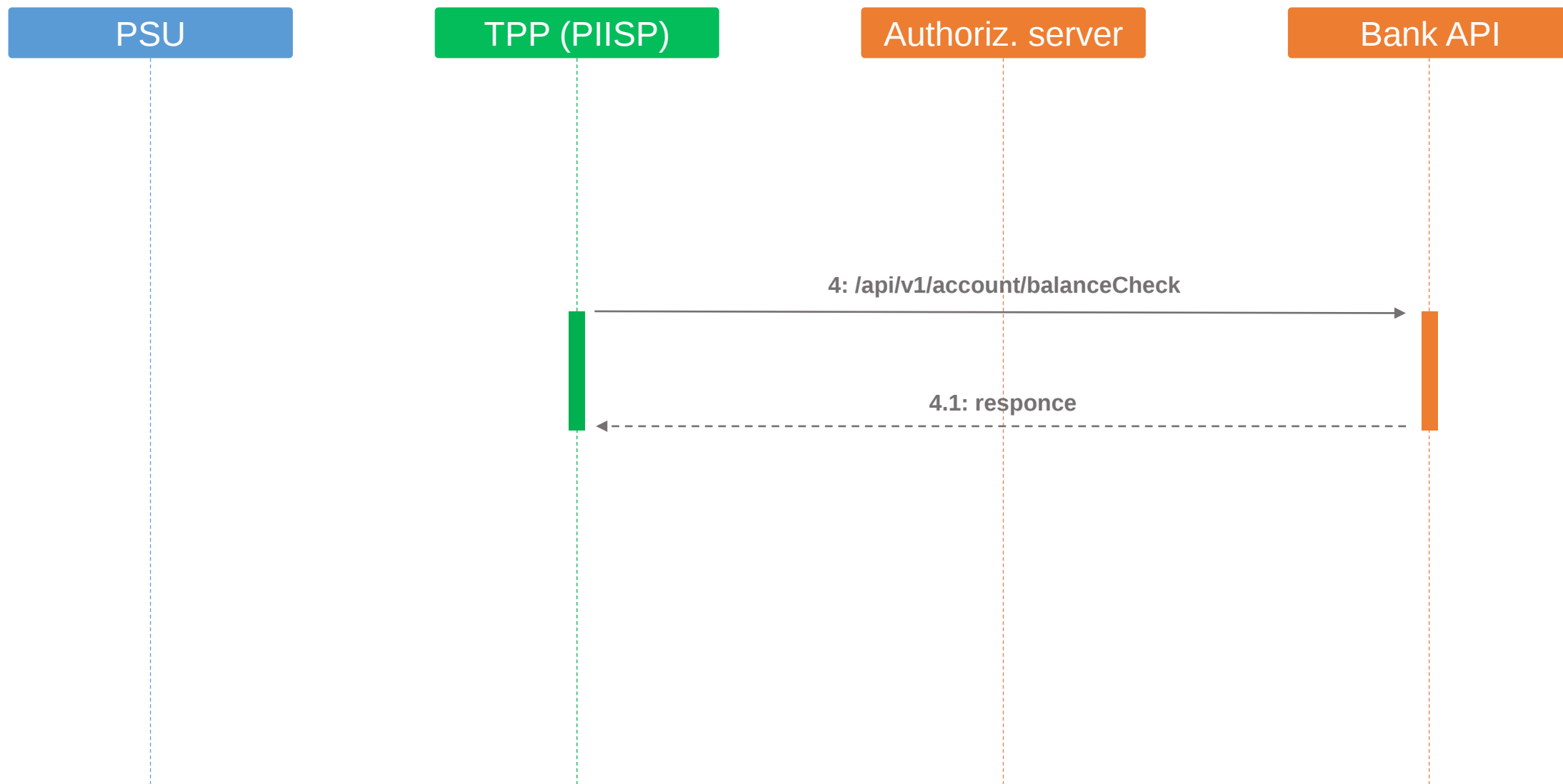
Definície endpointov pre PIISP

API endpoint	Metóda	Charakter	Popis
/api/v1/ accounts/balance Check	POST	Povinná	Balance check – služba poskytuje informácie o zostatku na účte vo formáte áno/nie

Získanie tokenov pre PIISP



Kontrola zostatku na účte



Sumár: Aktuálny zoznam služieb SBAS

Poskytovateľ	Služba	Charakter
AISP	Accounts Information	Povinná
AISP	Accounts Transactions	Povinná
AISP	Accounts List	Dobrovoľná
PISP	Standard Payment Initialization (XML)	Povinná
PISP	Standard Payment Submission	Povinná
PISP	Payment Order Status	Povinná
PISP	Standard payment initialization (JSON)	Dobrovoľná
PISP	Ecommerce payment initialization (XML)	Dobrovoľná
PISP	Ecommerce payment initialization (JSON)	Dobrovoľná
PIISP	Balance check	Povinná



07. Novinky v štarde

Marcel Laznia

Budúci zoznam služieb SBAS

Poskytovateľ	Služba	Charakter
AISP	Accounts Information	Povinná
AISP	Accounts Transactions	Povinná
AISP	Accounts List	Dobrovoľná
PISP	Standard Payment Initialization (XML)	Povinná
PISP	Request for payment cancellation	Dobrovoľná
PISP	Standard Payment Submission	Povinná
PISP	Payment Order Status	Povinná
PISP	Standard payment initialization (JSON)	Dobrovoľná
PISP	Ecommerce payment initialization (XML)	Dobrovoľná
PISP	Ecommerce payment initialization (JSON)	Dobrovoľná
PIISP, PISP	Balance check	Povinná

Odkazy

1. informácie o [Slovak Banking API Standard](#)
2. posledná verzia štandardu: [SBAS v 1.1](#)
3. [OpenAPI](#) špecifikácia štandardu
4. aktuálne [informácie](#) o slovenských bankových API podľa PSD2 (od 1. 3. 2019)

Ďakujeme

Príloha: Technické východiská SBAS

Transport protocols	TLS1.2+, HTTP
Applicative protocol	REST
Authorization protocol	OAuth 2.0 (client credential grant, authorization code grant)
Authentication methods:	Based on re-direct
Character set	UTF-8
Data structure	JSON (XML in the payment initiation services)
Data model origin	ISO 20022 is preferable used for attributes name
Character case convention	lowerCamelCase

Zoznam legislatívy: Základné normy

- [Smernica \(EÚ\) 2015/2366](#) o platobných službách na vnútornom trhu... (PSD2)
- Novela [281/2017 Z. z.](#) zákona o platobných službách [492/2009 Z. z.](#)

Zoznam legislatívy: Technické štandardy a usmernenia EBA

Predpisy k PSD2: [EBA Site](#)

1. [Guidelines for complaints-handling for the securities \(ESMA\) and banking \(EBA\) sectors](#)
2. [Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33\(6\) of Regulation \(EU\) 2018/389 \(RTS on SCA & CSC\)](#)
3. [RTS on Home-Host cooperation under PSD2](#)
4. [Guidelines on fraud reporting under PSD2](#)
5. [Technical Standards on the EBA Register under PSD2](#)
6. [Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2](#)
7. [Regulatory Technical Standards on central contact points under PSD2](#)
8. [Guidelines on security measures for operational and security risks under the PSD2](#)
9. [Guidelines on procedures for complaints of alleged infringements of the PSD2](#)
10. [Guidelines on major incidents reporting under PSD2](#)
11. [Guidelines on authorisation and registration under PSD2](#)
12. [Regulatory Technical Standards on passporting under PSD2](#)
13. [Regulatory Technical Standards on strong customer authentication and secure communication under PSD2](#)
14. [Regulatory Technical Standards on payment card schemes and processing entities under the IFR](#)
15. [Guidelines on internet payments security](#)

Zoznam legislatívy: Národné úpravy

Európsky orgán dohľadu pre bankovníctvo (ďalej len „EBA“) v spolupráci s príslušnými zainteresovanými stranami a Európskom centrálnou bankou (ďalej len „ECB“) vydal tieto vykonávacie predpisy:

1. Usmernenia k informáciám, ktoré sa majú poskytnúť pre udelenie povolenia platobným inštitúciám a inštitúciám elektronických peňazí a pre registráciu poskytovateľov služieb informovania o účte podľa článku 5 ods. 5 smernice (EÚ) 2015/2366. Usmernenia boli schválené a vydané ako usmernenie [EBA/GL/2017/09](#).
2. Usmernenia týkajúce sa kritérií na stanovenie minimálnej peňažnej sumy poistenia hmotnej zodpovednosti za škodu spôsobenú pri výkone činnosti alebo inej porovnateľnej záruky podľa článku 5 ods. 4 smernice (EÚ) 2015/2366. Usmernenia boli schválené a vydané ako usmernenie [EBA/GL/2017/08](#).
3. Usmernenia k oznamovaniu o závažných incidentoch podľa smernice (EÚ) 2015/2366 o platobných službách (PSD2). Usmernenia boli schválené a vydané ako usmernenie [EBA/GL/2017/10](#). Usmernenia sa týkajú kritérií klasifikácie závažných incidentov oznamovaných platobnými inštitúciami a kritérií posudzovania relevantnosti incidentu príslušnými orgánmi podľa článku 96 ods. 3 smernice PSD2. NBS na účely aplikácie toto usmernenie vydala informáciu na webovom sídle: (<http://www.nbs.sk/sk/dohlad-nadfinancnym-trhom/dohlad/oznamovanie-zavaznych-incidentov>).
4. Usmernenia o postupoch riešenia sťažností týkajúcich sa údajných porušení smernice o platobných službách 2. Usmerneniami sa určujú postupy riešenia sťažností, ktoré sa majú zohľadniť na zabezpečenie a monitorovanie účinného súladu s touto smernicou podľa článku 100 ods. 6 smernice PSD2. Usmernenia boli schválené a vydané ako usmernenie [EBA/GL/2017/13](#).
5. Usmernenia k bezpečnostným opatreniam vzťahujúcim sa na prevádzkové a bezpečnostné riziká platobných služieb podľa smernice (EÚ) 2015/2366 (PSD2). Usmernenie bolo schválené a vydané ako usmernenie [EBA/GL/2017/17](#). Usmernenie sa týka zavedenia, vykonávania a monitorovania bezpečnostných opatrení a v náležitých prípadoch aj postupov certifikácie s cieľom riadiť prevádzkové a bezpečnostné riziká súvisiace s platobnými službami podľa článku 95 ods. 3 smernice PSD2. Usmernenie bolo schválené a vydané ako Usmernenie EBA/GL/2017/17.

Zoznam legislatívy:

Národné úpravy... pokračovanie

Európsky orgán dohľadu pre bankovníctvo (ďalej len „EBA“) v spolupráci s príslušnými zainteresovanými stranami a Európskou centrálnou bankou (ďalej len „ECB“) vydal tieto vykonávacie predpisy:

6. Usmernenia o požiadavkách na vykazovanie podvodov podľa článku 96 ods. 6 smernice (EÚ) 2015/2366 (PDS2). Usmernenia o oznamovaní podvodov, ktoré sa vydávajú v súlade s článkom 96 ods. 6 smernice PSD2. Členským štátom z tohto usmernenia vyplýva povinnosť zabezpečiť, aby poskytovatelia platobných služieb poskytovali svojim príslušným orgánom aspoň raz ročne štatistické údaje o podvodoch súvisiacich s rôznymi platobnými prostriedkami. Uvedené štatistické údaje následne poskytne NBS orgánu EBA a ECB. [Ešte nevydaný materiál](#)
7. Regulačný technický predpis (ďalej aj „RTS“) o silnej autentifikácii a bezpečnej komunikácii. RTS ustanovujúce požiadavky na silnú autentifikáciu zákazníka a požiadavky na spoločné a bezpečné otvorené komunikačné normy podľa článku 98 smernice PSD2. RTS je kľúčovým dokumentom pre dosiahnutie účelu PSD2, ktorým je zlepšenie ochrany spotrebiteľa, podpora inovácií a zvýšenie bezpečnosti poskytovania platobných služieb v rámci Európskej únie. RTS boli schválené Európskou komisiou dňa [27. 11. 2017](#)
8. Regulačný technický štandard určujúci vhodné kritéria na zriadenie a funkcie centrálneho kontaktného miesta podľa článku 29 ods. 4 podľa smernice (EÚ) 2015/2366. Ustanovenia RTS obsahujú kritériá, ktoré sa majú uplatniť pri určovaní okolností, za ktorých je stanovenie ústredného kontaktného bodu vhodné, ako aj funkcií týchto kontaktných bodov podľa článku 29 ods. 4 smernice PSD2. Taktiež sa predpisom upravujú kritériá, pri splnení ktorých budú členské štáty vyžadovať od zahraničných platobných inštitúcií, ktoré poskytujú na ich území platobné služby prostredníctvom agentov na základe práva usadiť sa, [zriadenie centrálneho kontaktného bodu](#)
9. Regulačný technický štandard ukladajúci technické požiadavky na vytvorenie, fungovanie a zriadenie elektronického centrálneho registra a na vstup obsahujúcich informácií podľa článku 15 ods. 4 smernice (EÚ) 2015/2366 a Implementujúci technický štandard (ďalej len „ITS“) o podrobnostiach a štruktúre informácií zadávanými príslušnými orgánmi v ich verejných registroch podľa článku 15 ods. 5 smernice 2015/2366 (PSD2). V RTS sa stanovujú [technické požiadavky](#) týkajúce sa vytvorenia, prevádzky a údržby elektronického centrálneho registra a prístupu k údajom, ktoré obsahuje podľa článku 15 ods. 4 smernice PSD2, a ITS upravuje podrobnosti a štruktúru údajov, ktoré majú príslušné orgány uvádzať vo svojich verejných registroch, a oznamovať EBA podľa článku 15 ods. 5 smernice PSD2.
10. Regulačný technický štandard o spolupráci medzi príslušnými orgánmi domovského a hostiteľského členského štátu o dohľade nad výkonom činností platobných inštitúcií poskytujúcich služby cezhranične podľa článku 29 ods. 6 Smernice PSD2. V RTS sa vymedzuje [rámec spolupráce a výmeny informácií](#) medzi príslušnými orgánmi domovského členského štátu a hostiteľského členského štátu.
11. Regulačné technické štandardy o spolupráci a výmene informácií medzi príslušnými orgánmi, týkajúce sa oznamovania cezhraničného poskytovania služieb platobnými inštitúciami. Delegovaným nariadením sa ustanovuje rámec spolupráce a výmeny informácií medzi príslušnými orgánmi pri oznamovaní platobných inštitúcií, ktoré vykonávajú svoju činnosť [cezhranične podľa článku 28 ods. 5 smernice PSD2](#).