Koncept otvoreného bankovníctva

Anna Sedliaková
Národná banka Slovenska

Koncept otvoreného bankovníctva je aktuálnou a naliehavou témou v oblasti rozvoja moderných finančných služieb. Tento koncept má nemalý potenciál zmeniť budúcnosť správy a vedenia financií, zvýšiť konkurenciu medzi poskytovateľmi služieb na finančnom trhu a vylepšiť skúsenosť klienta s bankou. Je to významný krok vpred tak pre banky, ako aj pre inovatívne FinTech firmy. Čo však otvorené bankovníctvo vo svojej podstate znamená? Zjednodušene ide o to, že finančné a transakčné dáta, ktoré boli donedávna prístupné jedine banke klienta a držané v tejto banke, budú dostupné aj tzv. tretím stranám. Títo noví licencovaní poskytovatelia platobných iniciačných služieb a poskytovatelia služieb informovania o účte[1] budú môcť naplno využiť svoj potenciál a ponúknuť v spolupráci s tradičnými hráčmi na trhu, ako sú bankové inštitúcie, také služby, ktoré sú vytvorené na mieru klientov a špeciálne vyvinuté pre ich individuálne potreby. Klienti budú môcť napríklad sledovať stav na platobných účtoch držaných vo viacerých bankách alebo v platobných inštitúciách a platiť prostredníctvom nových poskytovateľov platobných iniciačných služieb, čo zaujímavo rozšíri ponuku možností platenia okrem dnes už obľúbených spôsobov, ako je platba debetnou alebo kreditnou kartou online.

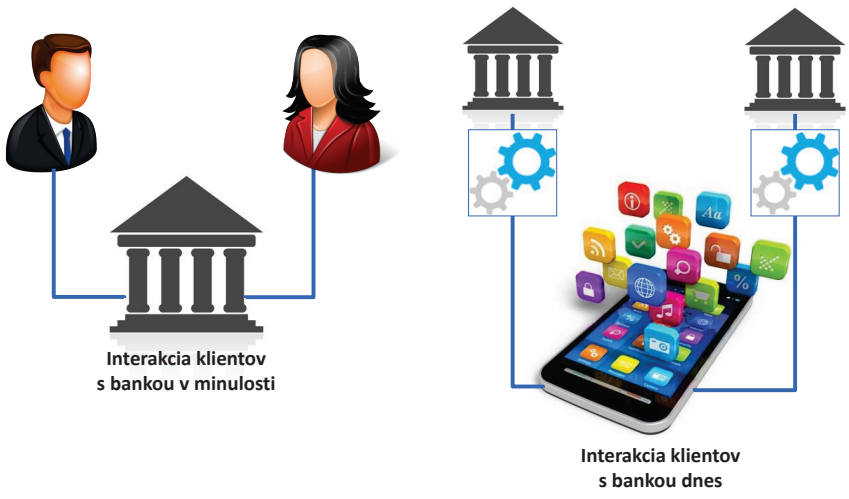
Digitalizácia finančných služieb a PSD2[2]

Bankovníctvo a platobné služby prešli za posledné roky vďaka digitalizácii veľkými transformačnými zmenami. Koncept otvoreného bankovníctva – *Open banking*, ktorý sa v európskom meradle naplno rozvíja od 13. januára 2018,[3] predznamenáva ďalšiu veľkú zmenu vpred.

Donedávna mali klienti a firmy obmedzený spôsob, ako pristupovať k svojmu platobnému účtu, napríklad kvôli platbe, a samotný prístup k informácii o stave na platobnom účte sa často poskytoval len osobne na pobočke. V celosvetovom meradle boli hotovosť, šeky a platobné karty dlhodobo a často jedinými možnosťami platenia tak v prípade klientov – fyzických osôb, ako aj firiem. Koniec dvadsiateho storočia priniesol priam prevratné zmeny. Rozvoj a hromadné rozšírenie internetu, telefonický operátor v bankách, ako aj technológia CHIP and PIN v oblasti platobných kariet podporili masový nárast e-commerce. Banky začali vyvíjať internetové bankovníctvo s online prístupom k platobnému účtu.

Ďalším významným stupňom vo vývoji moderných finančných služieb bolo rozšírenie smartfónov a následný rozvoj mobilných aplikácií. Vzniklo veľké množstvo rôznorodých platobných riešení, ako sú napríklad platby cez QR kód, *peer-to-peer* platby formou sms alebo dokonca platenie cez chatovú aplikáciu. Nové riešenia vytvárajú z platenia novú klientskú skúsenosť, zameranú na rýchlosť, prehľadnosť a vysoké používateľské pohodlie. Okrem toho tzv. PFM aplikácie (Personal Financial Management aplikácie – aplikácie osob-

Obrázok 1 Porovnanie interakcie klientov s bankou v minulosti a dnes



Interakcia klientov s bankou v minulosti

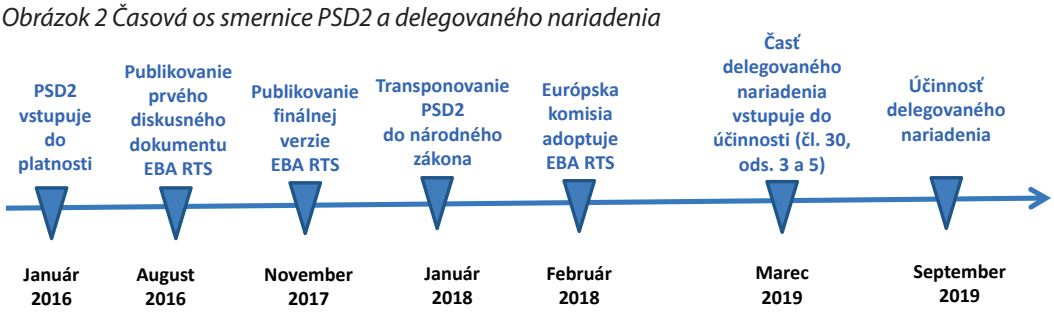
Interakcia klientov s bankou dnes

1 Viac v článku Sediaková, A.: Inovácie a zmeny v platobných službách podľa PSD2, Biatec, č. 1/2018, s. 2. (http://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2018/01-2018/Biatec_18_1_01Sedliakova.pdf)

2 Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (z angl. Payment Services Directive 2, skrátene PSD2). Na Slovensku bola smernica PSD2 transponovaná do zákona o platobných službách č. 281/2017 Z. z., ktorým sa mení a dopĺňa zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3 Dátum nadobudnutia účinnosti smernice EÚ 2015/2366 o platobných službách.

Obrázok 2 Časová os smernice PSD2 a delegovaného nariadenia



Poznámka: EBA RTS – regulačný technický predpis Európskeho orgánu pre bankovníctvo.

ného finančného manažmentu) sú vytvorené na to, aby umožnili okamžitý vizuálny prehľad o stave na platobných účtoch v agregovanej podobe. Keďže už dnes je mnoho typov PFM aplikácií, klient si môže vybrať taký, aký mu vyhovuje. Na základe takéhoto intuitívneho prehľadu bude môcť klient – fyzická osoba alebo firma – urobiť lepšie a najmä zodpovednejšie finančné rozhodnutie.

Smernica PSD2 vo svojej podstate odráža pokrok, ktorý nastal v platobnom ekosystéme v Európskej únii za posledných desať rokov. Okrem iného reaguje na otvorenie platobného trhu novým inovatívnym službám, čo je však podmienené povinnosťou získania licencie. Poskytovatelia platobných služieb budú povinní, na základe požiadavky a súhlasu klienta, poskytnúť tretej strane prístup k platobnému účtu svojich klientov v preddefinovanom rozsahu, ideálne prostredníctvom vo všeobecnosti uznávaného API rozhrania (API – *Application Programming Interface*, teda aplikačné programové rozhranie). Takýto prístup musí byť jasne odsúhlasený klientom. Okrem toho musí byť vykonaný nediskriminačným spôsobom, teda napríklad žiadna platobná iniciačná služba nemôže byť zvýhodnená, ani z časového hľadiska, pred inou a tiež nemôže byť uprednostnená na základe spoplatnenia. Na druhej strane takýto otvorený prístup môže byť odrieknutý napríklad v prípade podozrenia z podvodu.

Špeciálnou oblasťou, ktorá má veľký význam v oblasti otvoreného bankovníctva, je bezpečnosť dát. Komunikácia medzi jednotlivými hráčmi trhu sa vykoná cez zabezpečený kanál prostredníctvom kvalifikovaných certifikátov e-IDAS v súlade s delegovaným nariadením Komisie (EÚ) 2018/389 týkajúcim sa silnej klientskej autentifikácie a bezpečnej komunikácie[4] (ďalej len „delegované nariadenie"). Budúcnosť všeobecne rozšírenej praxe *screen scraping* (priamy a neriadený prístup k dátam klienta v plnom rozsahu bez informovania klienta alebo banky) sa zdá byť aspoň v teórii prekonaná vďaka široko uznávanému názoru medzi odborníkmi, že API je v súčasnosti najlepšou voľbou, a to tak pokiaľ ide o rýchlosť, štandardizáciu a bezpečnosť, ako aj o konzistentnú a komplexnú klientsku skúsenosť. Po vstupe delegovaného nariadenia do účinnosti už bude jediným akceptovaným riešením.

Tzv. nový ekosystém je po účinnosti PSD2 plný nových možností. Banky majú významnú a veľmi výhodnú pozíciu vďaka silnej základni klientov, ich dôvere a bezpečnosti, ktorá je v súčasnosti v ich prípade na vysokej úrovni. Čo sa týka FinTech spoločností alebo iných technologicky inovatívnych firiem, tie majú možnosť získať významný vplyv na trhu, ktorý bol dosiaľ otvorený výlučne bankám. A práve spolupráca medzi bankami a FinTech spoločnosťami je v centre záujmu otvoreného bankovníctva.

Časová os aplikovania vývoja jednotných pravidiel pre nový platobný ekosystém je na obrázku 2. Z časovej osi vyplýva, že v súčasnosti sa nachádzame v prechodnom období, keď delegované nariadenie týkajúce sa silnej klientskej autentifikácie a bezpečnej komunikácie je síce platné, ale účinné bude až od 14. 9. 2019. Táto situácia spôsobuje určitú neistotu na trhu platobných služieb, najmä pokiaľ ide o rôzne interpretácie dokumentov uvedených na časovej osi.

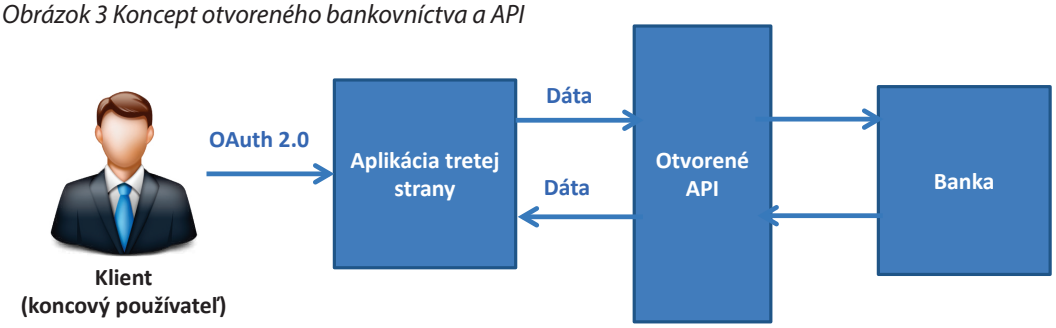
Čo je otvorené bankovníctvo

Otvorené bankovníctvo je metodický a technologický koncept, ktorý umožňuje, aby prostredníctvom jednotného štandardizovaného technologického rozhrania aplikácie tretích strán bezpečne pristupovali k bankovým produktom, procesom a službám. Banky podľa tohto konceptu vytvárajú rozhranie API, teda súbor softvérových služieb, pomocou ktorých je možné zautomatizovať štandardizovaným spôsobom komunikáciu medzi bankou a inými aplikáciami tretích strán. Vďaka tomuto softvérovému prepojeniu môžu internetové obchody, finanční poradcovia alebo účtovné systémy bezpečne a automatizovane vykonávať platobné operácie. Okrem toho vďaka API môžu napríklad vernostné schémy zabezpečiť, aby zbieranie bodov prebiehalo systematicky a kontrolovane zo zaznamenanej histórie transakcií platobnou kartou bez toho, aby musel každý obchodník vydávať vlastnú lojalitnú, resp. vernostnú kartu.

Okrem iného je otvorené bankovníctvo výzvou. Umožnilo zavedenie konkurencie bankám vo forme FinTech spoločností, mobilných operátorov a iných technologických firiem ponúkajúcich to, čo bolo v minulosti jedine výsadou bánk: nákupy, investovanie aj poskytovanie úverov. Na druhej strane ide do istej miery aj o nevyhnutný koncept, ktorý bankám pomáha udržať si svoju ponuku, čo najatraktívnejšiu pre koncového užívateľa pri vynaložení minimálnych nákladov.

4 Delegované nariadenie Komisie (EÚ) 2018/389, pokiaľ ide o regulačné technické predpisy pre silnú autentifikáciu zákazníka a spoločné a bezpečné otvorené komunikačné normy: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32018R0389&from=SK

Obrázok 3 Koncept otvoreného bankovníctva a API



V nebankovej sfére otvorených inovácií je API realitou už minimálne desať rokov. Spoločnosti ako Google, Facebook, Twitter, LinkedIn, Pinterest a mnohé iné postavili časť svojho biznisu na API. Ide o technologický pokrok porovnateľný s tým, ako keď sa v minulosti internet masovo rozšíril medzi ľudí. API sa totiž vo veľkej miere používa na rozšírenie množstva komunikačných kanálov. To znamená, že ak nejaká spoločnosť vydá a zdokumentuje svoje API verejne, môže tak nájsť partnerov na spoluprácu. Banky týmto spôsobom prostredníctvom API zjednodušia platby za mnohé služby či tovary cez e-mail, telefón, mobilnú aplikáciu a iné kanály tak, aby nadchádzajúci, čoraz populárnejší koncept, tzv. internet vecí (IoT – Internet of Things) plne zapadol do prirodzeného správania sa klienta: klient bude môcť plne využívať technologický pokrok vo forme inteligentnej domácnosti, inteligentnej televízie alebo inteligentného automobilu.

Nástup otvoreného bankovníctva si vyžaduje aj bezpečnostné nástroje a protokoly, ktoré sú často verejne dostupné a líšia sa technickým nastavením a mierou zabezpečenia. Zabezpečenie musí okrem potrebnej technickej stránky aj jednoznačne poukazovať na to, ktorá strana je za čo zodpovedná, aké sú dohody o poskytnutej spolupráci (SLA – Service Level Agreements), ktorá strana čo poskytuje, ako prebieha testovanie a ďalšie aspekty. Schematické zobrazenie konceptu otvoreného bankovníctva a API je na obázku 3.

API – APLIKAČNÉ PROGRAMOVÉ ROZHRANIE

Každý bankový API štandard vzniká so zámerom zjednodušiť integráciu a implementáciu služieb tretích strán a zadefinovať pravidlá komunikácie, najmä pre služby iniciovania platobnej operácie a poskytnutia informácie o platobnom účte, ako aj pravidlá pre poskytovateľa služieb vydávania platobných kariet.

Veľkú motiváciu implementovať API v bankovníctve spustila práve smernica PSD2. Treba však pripomenúť, že bankové API boli známe už aj v minulosti, no neboli jednotne štandardizované a ani trh im nevenoval osobitnú pozornosť.

Európske inštitúcie prejavili vôľu harmonizovať komunikáciu a bezpečný prístup so zámerom, aby trh skoncoval s rozšírenou praktikou *screen scraping*. Pri budovaní rozhrania je totiž potrebné strategicky sa rozhodnúť, ku ktorým dátam a operáciám ho treba sprístupniť povinne a ku ktorým (ak je taká možnosť) voliteľne. Navyše API prináša aj nové obchodné príležitosti a možnosť monetizácie za určitých okolností (pod podmienkou splnenia legislatívnych podmienok), a to napríklad prostredníctvom modelu *freemium*.

Ako by malo vyzerať vhodné bankové API? Odpovedať na túto otázku je náročné, a preto odborníci trhu, bánk a technologických firiem vytvorili dobrovoľné štandardy, ktorých je v Európskej únii síce viacero, no napriek tomu sú si viac-menej technicky podobné. Vybudovať jednotné univerzálne riešenie, pri ktorom je hneď na začiatku jasné, že bude mať širokú použiteľnosť, je totiž z praktického hľadiska lepšie a optimálnejšie, ako prispôsobovať sa pri každej banke (zo strany tretej strany) inej forme pripojenia. Jednotné a štandardné API tiež eliminuje riziko výberu nesprávnych parametrov (zo strany banky či platobnej inštitúcie), ktoré by tak mohli postaviť niektoré banky do nevýhodnej pozície. Do tretice, interný vývoj vlastného riešenia je finančne aj časovo náročný (na analýzu a ďalší rozvoj).

Navyše mnohé API ponúkajú okrem povinných aj voliteľné služby, vďaka ktorým sa budú môcť jednotlivé banky a platobné inštitúcie bez problémov vzájomne odlíšiť. Ako príklad možno spomenúť prémiové služby, rýchlejšie zodpovedanie dopytu, pre používateľov príjemné a pritom kvalitné zabezpečenie alebo operácie v reálnom čase. V každom prípade je voľba vhodného bankového API často otázkou stratégie, a do tej veľakrát vstupujú aj rozhodnutia matiek bankových skupín.

API, čiže aplikačné programové rozhranie, je v podstate technicky definovaný spôsob, akým dva počítače sieťovo komunikujú. Ide o softvérový produkt, ktorý je online dostupný, má svoje verzie, kompatibilitu a iné technické parametre. Je definovaný špecifikáciou, ktorá obsahuje a) popis jeho funkcionalít, b) časovú dostupnosť, c) dodatočné technické prekážky, ktoré môžu mať vplyv na jeho dostupnosť (napríklad obmedzenie dopytu užívateľa na vymedzený čas alebo maximálny počet dopytov za deň), d) dodatočné právne alebo obchodné prekážky (napríklad reklamné obmedzenia) a e) prehlásenie, že vývojári ho budú využívať len spôsobom, ktorý je popísaný v technickej špecifikácii. Okrem toho poskytovateľ API môže poskytnúť nástroje, ako sú mechanizmus prístupu k API, dokumentácia na pochopenie jeho fungovania, zdroje, ako napríklad programy

a vývojárske komunity na jeho podporu, operačné informácie o stave API a o tom, ako intenzívne sa rozhranie využíva. Štruktúra API je súčasťou kontraktu a kontrakt je záväzný a nemôže byť samovoľne pozmenený.

Z teoretického hľadiska sú dva typy API: súkromné a verejné. Prevažná väčšina API je súkromná. Verejné API sú dostupné pre každého v rámci definovaného kontraktu a špecifikácie, súkromné API sa využívajú rôznymi spôsobmi s obmedzením prístupu používateľom. Znenie alebo technická špecifikácia oboch typov je však v podstate rovnaká.

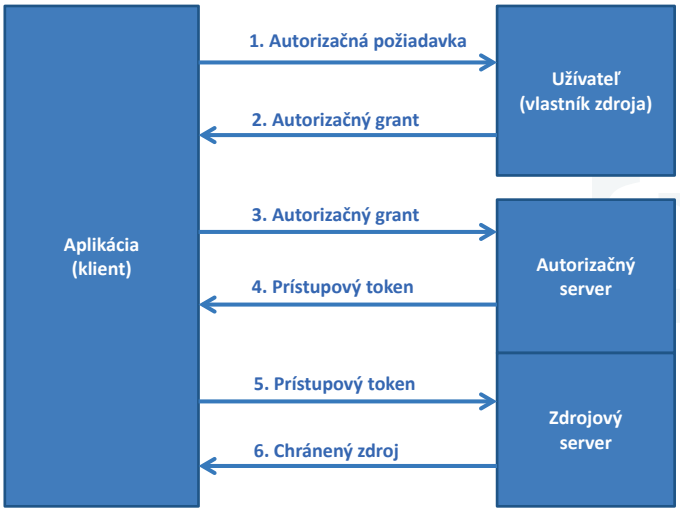
Základné charakteristiky API sa opierajú o nasledujúce prvky: v prvom rade ide o komunikačný protokol, nasleduje aplikačný protokol, ďalej autorizačný protokol, znaková sada, dátový formát a znaková konvencia. Ide však o základné prvky API, ktoré nevypovedajú o tom, aké vlastnosti poskytuje. Napríklad, či v rámci jednej komunikačnej relácie podporuje dopyt platobnej iniciačnej služby a zároveň aj služby informovania o účte.

Komunikačný protokol, ktorý API využíva, napríklad HTTP, je súbor pravidiel, ktoré využívajú programy a operačné systémy na komunikáciu, spojenie a prenos dát. Ide o pravidlá riadiace syntax, sémantiku a synchronizáciu komunikácie. Často využívaným protokolom v bankových API je práve HTTP (tzv. Hypertext Transfer Protocol) alebo HTTPS. Ide o protokol, ktorý definuje pravidlá medzi dvoma stranami, definuje tvar prenášaných informácií, možnosti, náležitosti, ako aj požiadavky a odpovede. V rámci služby WWW (World Wide Web) sa využíva od roku 1991. HTTP protokol je postavený na princípe otázky a odpovede a tento typ komunikácie prebieha medzi serverom a klientom. Každá aktivita musí byť vyvolaná klientom a má rôzne druhy žiadostí, nazývané aj metódy, ako napríklad GET, POST alebo PUT. HTTPS je zabezpečená forma HTTP, kde sa na ochranu dát používa SSL/TLS (bezpečnostný protokol výmeny informácií).

Aplikačný protokol, napríklad REST (Representational State Transfer), je architektonický spôsob pre rozvoj webových služieb. REST je jeden z frekventovaných protokolov bankových API. Je populárny a obľúbený pre svoju jednoduchosť, je postavený na existujúcich systémoch namiesto toho, aby vytváral nové štandardy, rámce a technológie. Je založený na protokole HTTP. Príkladom interakcie založenej na protokole REST je komunikačný štandard, ktorý využíva kód statusov HTTP. Kód 404 napr. znamená, že požadovaný zdroj nebol nájdený, kód 401 znamená, že požiadavka nebola autorizovaná a kód 500, že na serveri sa vyskytla chyba aplikácie. Aplikácie založené na protokole REST môžu byť napísané v akomkoľvek programovacom jazyku (Java, .NET, JavaScript a i.).

V súčasnosti najčastejšie preferovaným autorizačným protokolom je OAuth 2.0. Ide o autorizačný rámec, ktorý umožňuje aplikáciam (ako napríklad Facebook, Twitter, Flickr) limitovaný prístup k účtu používateľa. Protokol poskytuje autorizačný tok pre web, mobilné nástroje (tablet, smartfón) a aplikácie na pracovnej ploche počítača. Pracuje na princípe delegovania služby „overenia používateľa" a prostredníctvom nej autorizuje aplikácie tretích strán v rámci procesu prístupu k používateľskému kontu. Tok tohto protokolu je znázornený na obrázku 4.

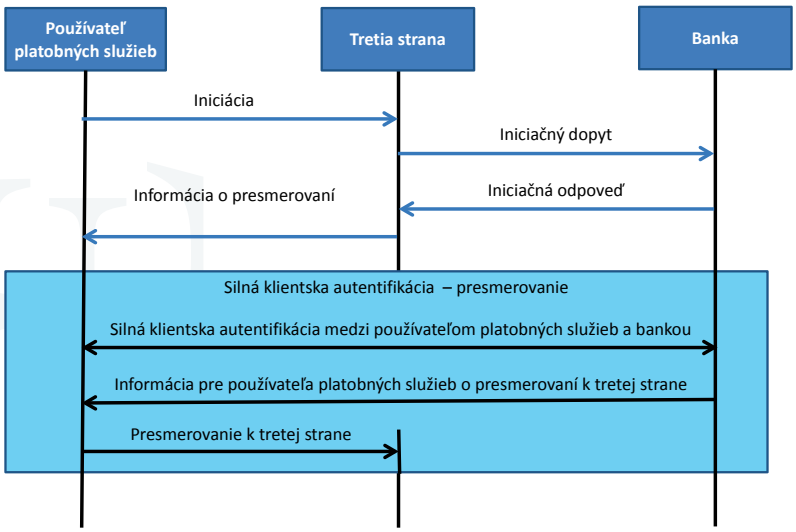
Obrázok 4 Tok protokolu OAuth 2.0



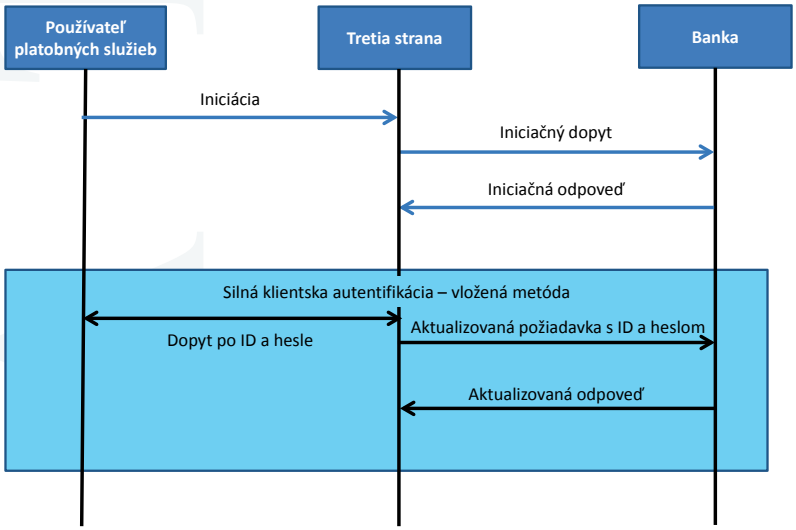
V rámci protokolu OAuth 2.0 aplikácia v prvom kroku požiada o autorizáciu na účely prístupu k zdrojovej službe zo strany používateľa. Ak používateľ v prvom kroku autorizuje požiadavku, aplikácia získa tzv. autorizačný grant. V treťom kroku si aplikácia vyžiada prístupový token (tzv. access token) z autorizačného servera API tým, že prezentuje autentifikáciu svojej vlastnej identity a autorizačný grant. Ak je identita aplikácie autentifikovaná a autorizačný grant je platný, autorizačný server API vydá vo štvrtom kroku prístupový token (tzv. access token). Následne je autorizácia ukončená. V piatom kroku aplikačné požiadavky zdroja zo zdrojového servera prezentujú prístupový token na autentifikáciu. Nakoniec, ak je prístupový token platný, zdrojový server API slúži zdroju aplikácie. Ide však o zovšeobecnený tok protokolu OAuth2.0. Skutočný a konkrétny tok operácií sa líši v závislosti od typu aplikácie.

Vo všeobecnosti je OAuth otvorený protokol, ktorý manažuje komunikáciu medzi aplikáciami a je využitý, keď vydavateľ API chce vedieť, kto má prístup do systému. Príkladom z nefinančnej oblasti je vzťah sociálnych sietí, napríklad Facebooku a Pinterestu. Ak používateľ Facebooku chce publikovať na svojej profilovej stránke fotografie z aplikácie Pinterest a nechce typovať svoje heslo z Pinterestu do Facebooku, využíva sa OAuth. Predtým, ako sa protokol OAuth začal všeobecne využívať a rozširovať, väčšina API podporovala základnú komunikáciu v HTTP. V rámci tejto komunikácie by Facebook uchoval heslo používateľa, čo je problematické najmä pre samotného používateľa. Jeho heslo by bolo totiž uchované aj v rámci mnohých iných webových stránok. Okrem toho heslo dáva každej aplikácii prístup ku všetkému, čo takéto heslo odkrýva. Táto praktika je málo

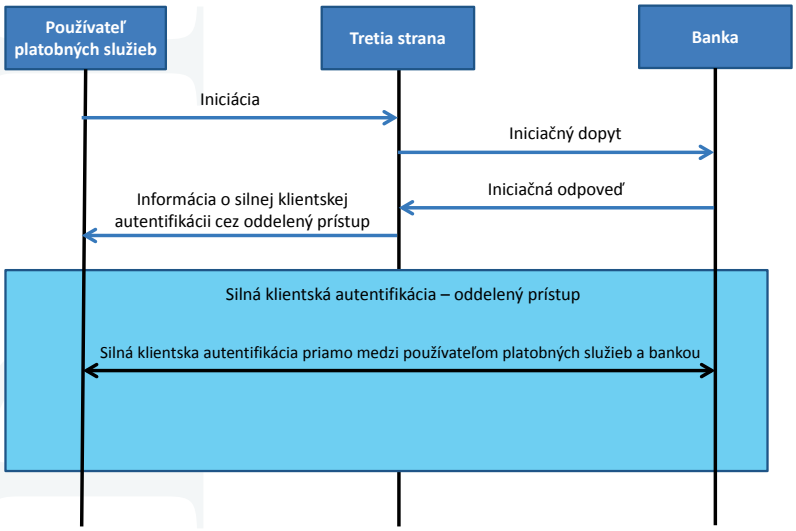
Obrázok 5 Silná klientská autentifikácia – metóda presmerovania



Obrázok 6 Silná klientská autentifikácia – vložená metóda



Obrázok 7 Silná klientská autentifikácia – metóda oddeleného prístupu



bezpečná aj preto, lebo používatelia väčšinou využívajú rovnaké heslo pre rôzne aplikácie. Preto namiesto takéhoto nedostatočného riešenia, akým je heslo, OAuth využíva token. OAuth token totiž dáva jednej aplikácii prístup k jednému API v mene jedného používateľa.

Znaková sada, dátový formát a znaková sekvencia sú ďalšie základné piliere definície API. Znaková sada definuje priradenie konkrétnych znakov k ich kódom. Dátový formát (napríklad JSON – JavaScript Object Notation alebo XML – Extensible Markup Language) alebo formát výmenných údajov umožňuje zobraziť štruktúrovanú informáciu. Znaková sekvencia je reťazec znakov alebo usporiadaná sekvencia znakov, alebo fyzicky usporiadaná sekvencia kódových jednotiek a v anglickom jazyku je označovaná aj ako *string*.

Zadefinovať hneď od začiatku, ako bude vyzerať ideálne bankové API, je takmer nemožné, keďže každé po čase potrebuje aktualizáciu alebo menšie úpravy. V rámci komunity vývojárov sú však už dnes preferované prvky, ako je tzv. pragmatický REST protokol, keďže vďaka jednoduchej štruktúre umožňuje nenáročne používanie, a teda aj šírenie, JSON ako dátový formát, keďže je jednoduchý na pochopenie a použitie, a OAuth protokol pre bezpečnosť, pretože zabráni šíreniu hesla voľne po internete (ako je to v prípade praktiky *screen scraping*) a umožňuje a podporuje rôzne druhy autentifikácie koncového používateľa.

Silná klientská autentifikácia a bezpečná komunikácia a API

Rozšírený bezpečnostný protokol OAuth2.0 podporuje všetky spôsoby silnej klientskej autentifikácie a bezpečnej komunikácie, ako sú prístup cez presmerovanie (*redirect approach*), vložený prístup (*embedded approach*) a oddelený prístup (*decoupled approach*). Všetky tri prístupy sa dnes plne využívajú, hoci niektorí trhoví hráči preferujú prístup cez presmerovanie (najmä z interných bezpečnostných príčin) a iní vložený prístup, aj kvôli tomu, aby nemuseli meniť svoje existujúce, už zabehnuté infraštruktúry.

Silná klientská autentifikácia je zadefinovaná v článku 97 smernice PSD2. Uplatňuje sa, ak platiteľ pristupuje k svojmu platobnému účtu online, iniciuje elektronickú platobnú transakciu alebo prostredníctvom diaľkového prístupu vykonáva akékoľvek kroky, ktoré môžu predstavovať riziko platobného podvodu alebo iného zneužitia. Silná klientská autentifikácia alebo dvojfaktorová klientská autentifikácia je taká, pri ktorej sa využívajú aspoň dva z nasledujúcich prvkov: vedomosť (niečo, čo používateľ platobných služieb vie, ako napríklad PIN alebo heslo), vlastníctvo (niečo, čo používateľ platobných služieb vlastní, napríklad token) a inherencia, resp. osobnostné prvky (napríklad hlasová vzorka, odtlačok prsta alebo štruktúra očnej rohovky). Jednotlivé prvky musia byť od seba nezávislé a narušenie jedného z nich nesmie ohroziť spoľahlivosť ostatných prvkov.

Delegované nariadenie týkajúce sa silnej klientskej autentifikácie a bezpečnej komunikácie

neupresňuje, aký konkrétny typ rozhrania majú banky a platobné inštitúcie implementovať. Na druhej strane článok 30 delegovaného nariadenia hovorí o tom, že *používatelia platobných služieb spravujúci účet, ktorí platiteľovi ponúkajú platobný účet, ktorý je prístupný online, majú zavedené aspoň jedno rozhranie, ktoré spĺňa všetky požiadavky* týkajúce sa najmä vzájomnej identifikácie, bezpečnej komunikácie a bezpečnej komunikácie s cieľom iniciovať platobný príkaz medzi jednotlivými hráčmi trhu, ako sú banky, platobné inštitúcie alebo tretie strany.

Metóda presmerovania (*redirect approach*) je v súčasnosti veľmi obľúbená najmä v prípade bánk, pretože silná klientská autentifikácia sa vykoná v internom prostredí banky, čo je z bezpečnostných dôvodov veľkou výhodou. Navyše tretia strana nemusí implementovať na svojej strane žiadny prvok silnej klientskej autentifikácie a od tretej strany sa nevyžadujú žiadne detailné informácie o používateľovi platobných služieb. Metóda presmerovania využíva v rámci autentifikácie preddefinovanú webovú adresu, ktorá presmeruje používateľa platobných služieb do prostredia napríklad bankového internet bankingu, kde sa môže v rámci interného prostredia bezpečne autentifikovať (obr. 5).

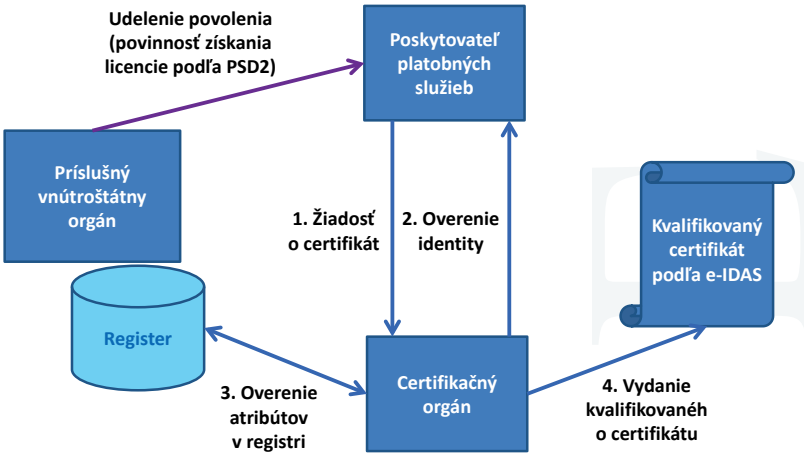
Vložená metóda (*embedded approach*) je metóda silnej klientskej autentifikácie, pri ktorej sa vyžaduje od tretej strany, aby implementovala na svojej strane časť procesu autentifikácie, ktorý banka podporuje. Táto metóda je zväčša dostatočne flexibilná a podporuje rôzne spôsoby autentifikácie (napríklad prostredníctvom ID, hesla, tokenu) a výzvy pre dáta môžu byť postavené na rôznych podporných prvkoch, ako sú animovaný obrázok, číselná matica a iné (obr. 6).

Tretia metóda, ktorá sa v súčasnosti spomína v súvislosti so silnou klientskou autentifikáciou, je metóda oddeleného prístupu, v rámci ktorej sa využíva na silnú klientskú autentifikáciu inteligentná aplikácia alebo iný externý prístroj (obr. 7). Pri tejto metóde vkladá používateľ platobných služieb svoje interné údaje priamo do aplikácie alebo na to určeného prístroja. Metóda je rozšírená v krajinách, kde bol tento spôsob zavedený aj vďaka ponuke iných administratívnych, daňových či komunálnych služieb občanom (napríklad v krajinách severnej Európy).

Silná klientská autentifikácia, ako aj technické a funkčné parametre API musia plne rešpektovať pravidlá vyplývajúce zo smernice PSD2, z delegovaného nariadenia týkajúceho sa silnej klientskej autentifikácie a bezpečnej komunikácie, no otvárajú sa aj iné otázky súvisiace s ochranou osobných údajov klienta v rámci nariadenia GDPR (General Data Protection Regulation).

Napokon, množstvo otázok v súčasnosti otvára aj možnosť príslušného vnútroštátneho orgánu udeliť výnimku z vytvorenia záložného riešenia API bankou (*fallback solution*). Banky, ktoré majú záujem o udelenie výnimky, musia splniť v rámci svojho API podmienky definované v nariadeniach a požiadať o výnimku príslušný vnútroštátny orgán, ktorý sa s danou požiadavkou obráti na Európsky orgán pre bankovníctvo (EBA). V súčasnosti má prevažná väčšina bánk záujem o udelenie výnimky, pretože záložné riešenie si vyžaduje ďalšie technické a ľudské zdroje, ako aj údržbu. Aj v dôsledku tohto faktora majú banky a platobné inštitúcie záujem o vybudovanie bezchybného API.

Obrázok 8 Schéma postupu pri vydávaní kvalifikovaného certifikátu



Register a komunikácia banky s treťou stranou

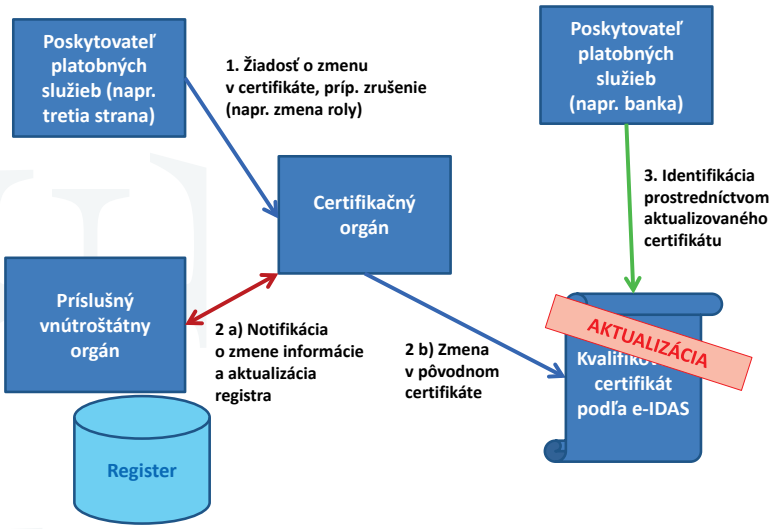
Vzájomná komunikácia banky s treťou stranou má svoje procesné nastavenie vďaka API a zvolenej metóde silnej klientskej autentifikácie. Pre správnu komunikáciu trhových hráčov na trhu platobných služieb sa na úrovni príslušných vnútroštátnych orgánov vytvoril tzv. register bánk, poskytovateľov platobných služieb a poskytovateľov elektronických peňazí (ďalej len „register"). Register je dôležitým prvkom, pretože obsahuje kľúčové dáta potrebné na správnu identifikáciu a komunikáciu jednotlivých strán trhu.

V rámci vzájomnej identifikácie tretej strany a banky sa tretia strana identifikuje voči banke kvalifikovaným certifikátom e-IDAS[5]. Certifikát obsahuje povinné prvky, ako je názov poskytovateľa platobných služieb, názov príslušného vnútroštátneho orgánu, ktorý udelil povolenie či licenciu, registračné identifikačné číslo vydané príslušným vnútroštátnym orgánom a úlohy tretej strany, resp. poskytovateľa platobných služieb. Register poskytovateľov je pravidelne aktualizovaný na webovej stránke príslušného orgánu. Registre členských štátov v Európskej únii momentálne nie sú celkom rovnaké a ani harmonizované, čo dáva priestor na vznik iných komerčných riešení. Hráči trhu očakávajú vytvorenie spoločného registra pod záštitou EBA, ktorý už síce má svoju finálnu obsahovú špecifikáciu, ale dáta bude čerpať aj tak z národných registrov.

Aktuálnou výzvou v rámci tvorby registra je okrem všeobecnej harmonizácie aj nastavenie životného cyklu kvalifikovaného certifikátu e-IDAS a nastavenie či presnosť v ňom obsiahnutých dát.

5 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

Obrázok 9 Manažment životného cyklu kvalifikovaného certifikátu



Dáta v kvalifikovanom certifikáte sú totiž vydané vydavateľmi kvalifikovaných certifikátov (ktorými sú certifikačné orgány, aktuálne ich je v Európskej únii približne osemdesiat, z toho šesť na Slovensku) (obr. 8).

Elektronický kvalifikovaný certifikát tretej strany môže totiž z rôznych príčin obsahovať nesprávne alebo už neaktuálne informácie, v dôsledku čoho môže dochádzať k zamietaniu procesu identifikácie jednotlivých protistrán, prípadne až k sporom v súvislosti s dôsledkami nesprávnej identifikácie. Pri identifikácii tretej strany, napríklad pri dopyte vo forme platobnej iniciačnej služby, totiž banka overuje informácie obsiahnuté v elektronickom kvalifikovanom certifikáte porovnávaním s informáciami obsiahnutými v strojovo čitateľnom registri. Je preto dôležité zosúladiť aktualizáciu informácií priamo v elektronickom kvalifikovanom certifikáte tretej strany s informáciami obsiahnutými v registri (obr. 9).

V súčasnosti je banková prax taká, že banky sa pri dopytoch tretích strán spoliehajú najmä na register príslušného vnútroštátneho orgánu.

Koncept otvoreného bankovníctva vo svete a na Slovensku

Ako vyzerá koncept otvoreného bankovníctva a API vo svete a doma? Technologicky vyspelá krajina Južná Kórea vytvorila od roku 2016 tzv. otvorenú FinTech platformu, ktorá sa považuje za unikátny prvok rozvoja na poli rozširovania FinTech a zároveň za jedinečnú *sandbox platformu*. Platforma prepojila šestnásť komerčných bánk a dvadsaťpäť spoločností s cennými papiermi.

Iný príklad ponúka Singapur. Od roku 2016 je zverejnená špecifikácia Finance-as-a-service: API Playbook. Dokument obsahuje usmernenia a osvedčené postupy pre tvorbu a využitie API, ktoré sú určené pre banky, poisťovne, spoločnosti správy majetku a iné.

Ďalším príkladom je Japonsko, ktoré prijalo v polovici roka 2017 tzv. stratégiu rastu krajiny. Jednou z priorít tejto stratégie je podpora otvorenej inovácie medzi finančnými inštitúciami a FinTech firmami. Japonsko pozmenilo zákon o bankovníctve a zadefinovalo do neho platobné iniciačné služby, ako aj služby informovania o platobnom účte. Cieľom je, aby sa do roku 2020 zapojilo do konceptu Open banking a API vyše osemdesiat bánk.

Európska únia sa opiera o otvorený prístup k platobnému účtu (Access to account, v skratke XS2A) zo smernice PSD2. Európska komisia zdôrazňuje, že táto metóda podporí súťaž na trhu poskytovateľov platobných služieb a ponúkne lepší a väčší výber klientom. Slovensko sa tiež aktívne zaujíma o problematiku otvoreného bankovníctva a API, a to napríklad prostredníctvom aktivít a workshopov na pôde Slovenskej bankovej asociácie, ako aj priamou participáciou expertov v pracovných skupinách európskych inštitúcií.

Budúcnosť otvoreného bankovníctva

Na otázku, ako bude vyzerať budúcnosť otvoreného bankovníctva, nie je v súčasnosti z viacerých dôvodov jednoduché odpovedať, keďže transpozícia smernice PSD2 v mnohých európskych krajinách meškala a delegované nariadenie týkajúce sa silnej klientskej autentifikácie a bezpečnej komunikácie bude účinné až od septembra 2019. V európskom prostredí sa tak vytvorilo prechodné obdobie, keď sa aplikuje to, čo v rámci európskych krajín dlhé roky bolo a existovalo, teda rôznorodosť. Výnimkou je, že banky a platobné inštitúcie musia od 13. januára 2018 poskytnúť aspoň jedno otvorené rozhranie pre dopyt tretej strany.

Ako však vyzerá ďaleká budúcnosť? Budú platby iniciované robo-poradcami namiesto klientov? Budú sčasti alebo plne automatizované v reálnom čase? Kedy bude musieť klient vyvinúť skutočne minimálne úsilie? A aký dopad to bude mať na už existujúce iné platobné nástroje a služby, ako sú úhrady, platobné karty, elektronické peňaženky a mobilné aplikácie? Odpovede na tieto otázky závisia od toho, ako si klienti zvyknú na nový platobný ekosystém. Na jednej strane digitalizácia platobných služieb a bankovníctva podnietila a zintenzívnila využívanie nových spôsobov interakcie klientov s peniazmi. Na druhej strane sú to práve obavy klientov o neoprávnené zdieľanie informácií a bezpečnosť, ktoré môžu pokrok výrazne spomaliť.

Víťazmi otvoreného bankovníctva môžu byť v každom prípade tí trhoví hráči, ktorí budú vedieť ponúknuť klientom vynikajúcu skúsenosť skombinovanú s vysokou úrovňou bezpečnosti.