FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Směrnice PSD2 a její dopady na vývoj bankovních aplikací
Student:	Bc. Jan Alexander
Vedoucí:	Ing. Pavel Náplava
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2018/19

Pokyny pro vypracování

Analyzujte směrnici PSD2, včetně jejího dopadu na bankovní trh, a vytvořte prototyp, na kterém ukážete, jakým způsobem lze na základě směrnice vytvářet vlastní bankovní aplikace. Na základě tvorby prototypu vyhodnoťte náročnosti tvorby aplikace a vytvořte návod pro tvorbu obdobných aplikací.
Postupujte následovně:
1. Popište bankovní trh - historii bankovnictví, trendy přístupu k zákazníkům a dopady na bezpečnost bankovního styku.
2. Analyzujte aktuální trendy v bankovních aplikacích.
3. Analyzujte směrnici PSD2 a její dopad na bankovní trh a bankovní aplikace, včetně technického pohledu.
4. Na základě analýzy navrhněte vlastní aplikaci, využívající otevřené bankovní API, definované směrnicí PSD2.
5. Zvolte vhodnou implementační platformu, vytvořte a otestuje alespoň základní funkční prototyp aplikace.
6. Na základě zkušeností s vývojem vlastní aplikace vyhodnoťte obecnou náročnost tvorby obdobných aplikací, zhodnoťte jejich potenciál a vytvořte sadu doporučení pro jejich vývoj.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 28. prosince 2017

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práce

Směrnice PSD2 a její dopady na vývoj bankovních aplikací

Bc. Jan Alexander

Katedra softwarového inženýrství
Vedoucí práce: Ing. Pavel Náplava

9. května 2018

Poděkování

Děkuji panu Ing. Pavlovi Náplavovi za trpělivost s mojí nedochvilností vzhledem k harmonogramu a pomocí s efektivním posouváním práce směrem dopředu. Dále děkuji bývalému studentovi FITu Ing. Lukášovi Kořánovi za pomocnou ruku při úvodu do C# a ASP.NET, v kterém jsem před tvorbou práce ještě nikdy neprogramoval.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 9. května 2018 .....

Odkaz na tuto práci

Alexander, Jan. *Směrnice PSD2 a její dopady na vývoj bankovních aplikací.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

V diplomové práci se zabývám analýzou evropské směrnice o platebním styku, zkráceně PSD2, a otevřeného bankovního API, na základě které jsem navrhl a implementoval základní prototyp. Realizaci prototypu jsem popsal ve formě návodu sloužícímu pro další vývoj bankovních aplikací – od splnění legislativních požadavků, návrhu, implementace, až po doporučení pro produkční řešení. V první části práce zkráceně vymezuji a analyzuji obsáhlý bankovní trh, který poslouží k lepšímu pochopení směrnice a z ní plynoucích příležitostí pro vývoj bankovních aplikací.

Klíčová slova PSD2, PSD, FinTech, PSD2 prototyp, platby, API

Abstract

In my diploma thesis, I analyze the European Payments Directive, abbreviated PSD2, and the open banking API. Based on the analysis, I designed and implemented the basic prototype. I described the implementation of the prototype in the form of instructions for the further development of banking applications – from the fulfillment of legislative requirements, design, implementation, to recommendations for production solutions. In the first part of my work, I briefly define and analyze the wide banking market, which will

help to better understand the directive and the opportunities in developing banking applications.

Keywords PSD2, PSD, FinTech, PSD2 prototype, payments, API

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Bankovní trh je velmi široké téma a přijde s ním do nepřímého styku téměř každý člověk. V poslední době došlo k velkému rozmachu bankovních aplikací zvaných FinTech. Nárůst plateb přes chytré telefony a platební karty prudce roste a s tím i podvody, či obrovský zisk z poplatků u plateb kartou. Evropská unie se s problematikou snaží vypořádat pomocí platebních směrnic, již platné PSD a nyní v platnost přicházející PSD2 v době psaní mé práce.

PSD2 přináší povinnost bankám otevřít účty svých klientů třetím stranám přes API. Dále mění požadavky pro platební služby a služby agregující data z účtů. Zakáže takzvaný screen scraping a zavede povinnost dvoufázového ověření při platbách. Směrnice nebude mít dopad pouze pro nové aplikace, ale i pro stávající. Banky se rovněž směrnici nevyhnou a čekají je obrovské výdaje k přípravě požadovaného otevřeného API. Některé banky jako Česká spořitelna jsou již připravené, jiné čekají až s platností posledních technických standardů plánovaných na září roku 2019.

Mojí motivací analyzovat rozsáhle směrnici PSD2 a s tím i související bankovní trh je získání dalších praktických znalostí v oboru bankovnictví, jelikož pracuji druhým rokem jako projektový manažer v Komerční bance. Zároveň mojí malou zkušeností z praxe chci přispět radami pro další vývojáře. Snažím se nejenom vyvinout obyčejný prototyp, ale dostatečně prototyp vzhledem k PSD2 popsat, aby čtenář mohl na základě práce vyvinout svoji vlastní aplikaci splňující veškeré legislativní podmínky a přivést ji do produkčního prostředí, pokud na základě mé analýzy bankovního trhu uzná vývoj FinTech aplikace v nějaké kategorii bankovních aplikací vůbec za vhodný.

Kapitola 1

Bankovní trh

Důležitým krokem v mé diplomové práci je prvně představit základní bankovní pojmy, které v práci používám. Nicméně abych nezačal čtenáře nudit hned ze začátku, povím něco málo k historii bankovnictví. Následně uvedu zmíněné bankovní pojmy i vzhledem k předchozí kapitole. Na základě historie navážu na trendy přístupu k zákazníkům v bankovnictví současnosti uvedením základního dělení bank a jejich produktů. Představím bankovnictví v ČR i z pohledu, jenž je pro běžného zákazníka skrytý a analyzuji postavení jednotlivých bank v ČR. Na závěr vysvětlím celou problematiku finančních technologií, zkráceně FinTech, které přístup k zákazníkovi formují v dnešní době jako poslední a mění zásadně podobu bankovního trhu. Jako poslední zhodnotím bezpečnost vzhledem k současným technologiím používaným v bankovnictví. Jelikož bankovní trh je velmi obsáhlý pojem, určitě nepopíši vše důležité. Snažím se držet text ve stručnosti a relevantnosti k mé práci.

1.1 Historie bankovnictví

V kapitole historie bankovnictví dám do postupného sledu stěžejní milníky, které ovlivnily podobu bankovnictví, jak ho dnes známe. Od 20. století začnu popisovat milníky trochu detailněji a to hlavně z technologického, potažmo bezpečnostního hlediska, což bude sloužit i jako podklad pro zhodnocení bezpečnosti v kapitole 1.4 na konci.

1.1.1 Depozit *2000 př.n.l.*

Ke vzniku bankovnictví, jak ho v dnešní době známe, nejvíce vedly depozitáře, které vznikly ještě před oficiální měnou nebo bankami.

První oficiální depozity jakožto služba jsou dokumentovány v Babylonské říši v letech 2000 před naším letopočtem. Depozity byly vytvářeny u důvěryhodných lidí, kteří byli za úschovu cenností placeni.

Hlavní inspirace pro dnešní podobu depozitu v bankách vychází z Řecka, kde se měna uschovávala v chrámech kvůli nejvyšší bezpečnosti. Z důvodu ještě vyšší bezpečnosti, zejména proti krádežím, začaly v chrámech vznikat i speciální místnosti – trezory. Z počátku byly depozitáře v chrámech zdarma. Kněží dostávali akorát dary za jejich služby. S narůstajícími nároky na bezpečnost a využití služeb byly později zavedeny poplatky – stejně jako u dřívějších depozitářů v Babyloně.[8]

1.1.2 Měna *700 př.n.l.*

Přes dalších 1000 let trvalo, než vznikla oficiální měna ve formě mincí. Před oficiální měnou byl směnný obchod zboží za zboží, který byl přirozeně komplikovaný – musela být buď vzájemná poptávka nebo věřit, že vyměněné zboží bude moct člověk směnit dále za jiné, které poptává. Největší důvěru pro směnný obchod (cca 2000 B.C.) získal dobytek, následoval cenný kov jako zlato, stříbro, měď (cca 1600 B.C.), který později dal za vznik oficiálním mincím sloužícím k směně zboží (cca 700 B.C.).[8]

Bankovky vznikly až v 7. století našeho letopočtu, se kterými začala Čína.[9]

1.1.3 Bankovnictví *400 př.n.l.*

Ze správců depozitářů se přirozeným vývojem trhu stali bankéři, jelikož díky mincím mohli začít nabízet první bankovní služby s primárním záměrem zhodnotit svěřené vklady. První přerod ze správců depozitářů na bankéře započal v období římské republiky kolem roku 400 př.n.l. Nabízeli obdobné služby jako dnes:

- Otevření účtu
- Doklad o vkladu
- Výdej směnek
- Vybavování akreditivu
- Poskytování půjček
- Poskytování hypoték

Úroky byly vypláceny na termínovaných vkladech, kde peníze byly vloženy jako kredit. S tím mohli bankéři nakládat podle sebe, a proto mohli vyplácet i úroky.[8]

1.1.4 Banka *1200 n.l.*

První banku – Benátskou banku – lze datovat k roku 1157, nicméně jednalo se o státní banku formující veřejné věřitele kvůli velkému dluhu způsobeného válkou.[10] Největší rozkvět bank, jak je známe dnes, nastal v Itálii kolem roku 1400 ve městech jako Florencie, Siena, Miláno, Benátky a další. V Sieně je například dosud nejstarší fungující banka z roku 1472.[11] K rozkvětu došlo hlavně z důvodu, kromě rostoucí potřeby financovat monarchy, reakce na rostoucí mezinárodní obchod. Banky totiž přišly se směnkami za účelem úvěrových transakcí a snazšího převodu prostředků, což odstranilo potřebu nosit s sebou těžké mince v různých měnách.[12]

1.1.5 Centrální banka *1600 n.l.*

Počátkem 17. století začalo vznikat moderní bankovnictví. Nejvíce se dařilo úvěrům financující války. Dluhy se pomalu začaly stávat náhradou za měnu, čímž se z měny jako objektu spíše stával symbol pokroku. To vedlo k četným – dle někoho nutným – vládním regulacím a vzniku oficiálních centrálních bank – například první banka vzniklá v roce 1668 Sveriges Riksbank.[8][13]

1.1.6 Elektronický převod *1872 n.l.*

Bezhotovostní elektronické převody byly provázeny za využití telegrafické sítě. První telegrafický převod provedla společnost Western Union v roce 1872. Operátor telegrafu využíval seznam kódů a příslušných hesel.[14]

1.1.7 Mainframe *1950 n.l.*

V roce 1950 začaly banky nakupovat sálové počítače, respektive mainframy, pro zpracování velkého množství transakcí a s tím navazujících procesů.[12]

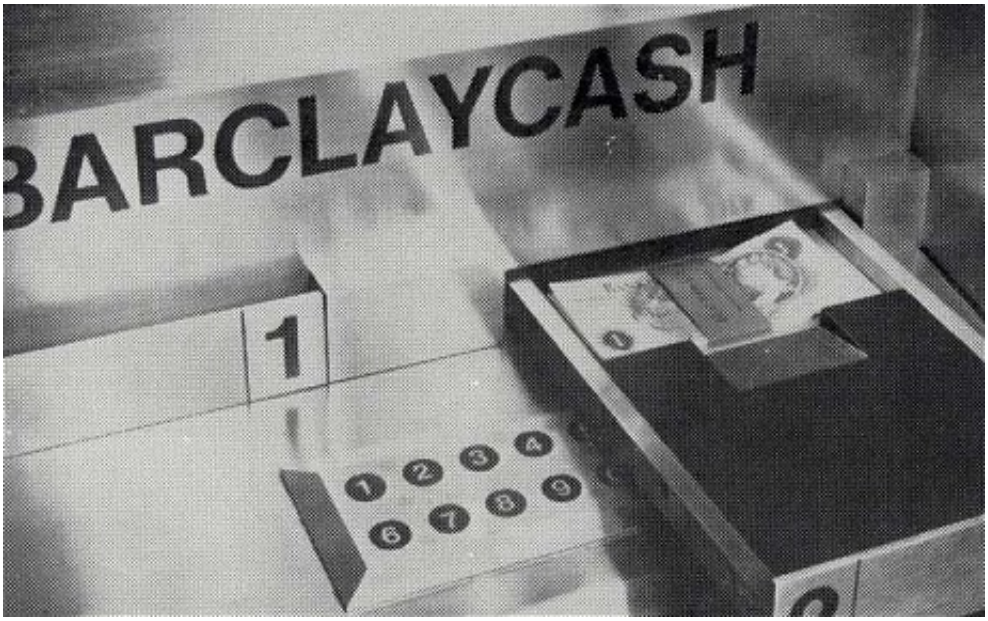
1.1.8 Kreditní karta *1958 n.l.*

U vzniku kreditní karty nebyl problém nedostačující technologie, nýbrž problematický kruh obchodník–zákazník. Obchodníci nechtěli brát karty, neboť jimi nikdo nemohl platit a zákazníci nechtěli karty, jelikož jimi neměli kde platit. S kartami přišla až Bank of America (později Visa) v roce 1958, viz obrázek 1.1, která kreditní karty masivně uvolnila do menšího města Kalifornie, aby se uchytily. S tím ale přišly první kartové podvody a nutnost vydávat kreditní kartu pouze vybraným zákazníkům, jelikož ne všichni klienti v první vlně dostávali svým úvěrovým závazkům vzniklými z nákupů kreditní kartou.[15]

1.1.9 Bankomat *1967 n.l.*

Bankomat, viz obrázek 1.2, uvedla prvně na trh banka Barclays roku 1967 v Londýně. Z počátku bankomat nevyužíval kreditní karty pro výběr peněz, ale

Obrázek 1.1: První kreditní karty z roku 1958. Vlevo BankAmericard (později Visa) od Bank of America. Vpravo kreditní karta od American Express.[1]



Obrázek 1.2: Historicky první bankomat z roku 1967 banky Barclays.[2]

vložením papírových šeků. Šeky byly označeny mírně radioaktivním izotopem uhlíku – uhlík-14 – z důvodu detekce a bezpečnosti ověřením vůči šestimístnému PIN číslu. PIN byla rovněž bezpečnostní novinka v bankovnictví právě díky příchodu bankomatů. Nicméně bankomaty se okamžitě staly terčem vandalismu za účelem krádeží.[16]

1.1.10 Clearingový systém *1968 n.l.*

Samotný clearing byl nutný kvůli cenným papírům a šekům již dávno sahajíc až do 18. století, nicméně první automatizace se clearing dočkal až v roce 1968

se systémem ve Velké Británii s názvem BACS.[1] Systém vznikl hlavně kvůli odlehčení papírování, s kterým byl spojený původní proces clearingu. Zastřešil rovněž v témže roce vymyšlené a zavedené inkasní platby.[2][17]

1.1.11 Telefonní bankovnictví *1980 n.l.*

Telefonní bankovnictví nebylo ihned automatizované – veškeré operace na druhé straně byly prováděné manuálně operátorem banky. Volající se napřed musel odpověďmi na otázky identifikovat operátorovi a následně mohl provádět různé transakce.[18] První telefonní bankovnictví spustila Girobank roku 1980 ve Velké Británii.[2]

1.1.12 Online obchod *1984 n.l.*

Online obchod ze začátku – namísto internetu – využíval Videotex systém, který byl fyzicky propojený s televizí, a přes který šlo nejenom zaplatit, ale provést celou objednávku. První objednávka byla provedena v roce 1984 ve Velké Británii nákupem v Tesco. Technologie se samozřejmě postupně vytratila se zavedením internetu.[19]

1.1.13 Debetní karta *1984 n.l.*

Debetní karty se začaly vydávat v roce 1978, nicméně fungovaly spíše jako bankou garantované šeky, které pokrývaly transakci. Proto byly karty vydávány pouze lidem z byznysu, kteří měli dostatečně velké spořící účty a dlouhou bankovní historii. Debetní karta se v pravém slova smyslu objevila až v roce 1984 společností Landmark, která implementovala celostátní debetní systém postavený na infrastruktuře kreditních karet a síti bankomatů.[20]

1.1.14 Čip a PIN *1994 n.l.*

Kreditní a debetní karty dříve používaly magnetický pruh a ověření probíhalo pouze podpisem, který byl pro účely porovnání obchodníkem na kartě. Eventuálně proběhlo ověření ještě přes telefonní hovor. Nicméně tento systém je velmi náchylný k podvodům:

- Magnetický pruh lze snadno okopírovat a tím vytvořit kopii karty.
- Podpis lze zfalšovat, navíc obchody podpis alespoň v USA moc nekontrolovaly.[21]
- Podpis je dokonce možné smazat a vytvořit vlastní.

[1] BACS anglická zkratka pro Banker's Automated Clearing Services nebo-li automatický systém pro clearingové služby.

Z důvodu velmi nízké bezpečnosti a vysoké ceně mezinárodních hovorů v Evropě nutných pro případ ověření přes telefonní hovor, se v Evropě roku 1994 zavedl technologický standard EMW, který se časem stal povinným pro ověřování transakcí kartou. U karet splňující standard EMW musí proběhnout ověření přes čip a zadání PINu.

Bezpečnost u EMW karet

Bezpečnost EMW karet je postavena na dynamické datové autentizaci (DDA). Jedná se většinou o RSA šifrování. Každá karta tedy obsahuje unikátní veřejný a privátní klíč, který je použit při autentizaci. Jedním klíčem karta vygeneruje unikátní šifrovaný kód vzhledem k transakci, který odešle terminálu a dokáže tím originalitu karty. Druhý klíč použije terminál pro validaci kódu.[22]

Nevýhoda EMW karet

Nevýhoda EMW karet, oproti kartám s magnetickým pruhem, spočívá v delší autorizaci v řádu jednotek vteřin.[23] Proto v USA mezitím obchodníci EMW karty odmítali, jelikož nechtěli zpomalit proces nakupování. Nicméně od roku 2015 Visa a MasterCard odmítli nést nadále odpovědnost za platební podvody a tím donutili obchodníky k adaptaci EMW karet, respektive podporovaných platebních terminálů.[21]

1.1.15 Internetové bankovnictví *1994 n.l.*

Internetové bankovnictví odstartovala v roce 1994 společnost Stanford Federal Credit Union. V témže roce začal nabízet integrované internetové bankovnictví Microsoft v aplikaci Microsoft Money personal finance, která uměla většinu správy bankovního účtu.[24]

Pro lepší představu rychlosti adaptace – v roce 2006 nabízelo internetové bankovnictví v USA 80% bank.[25]

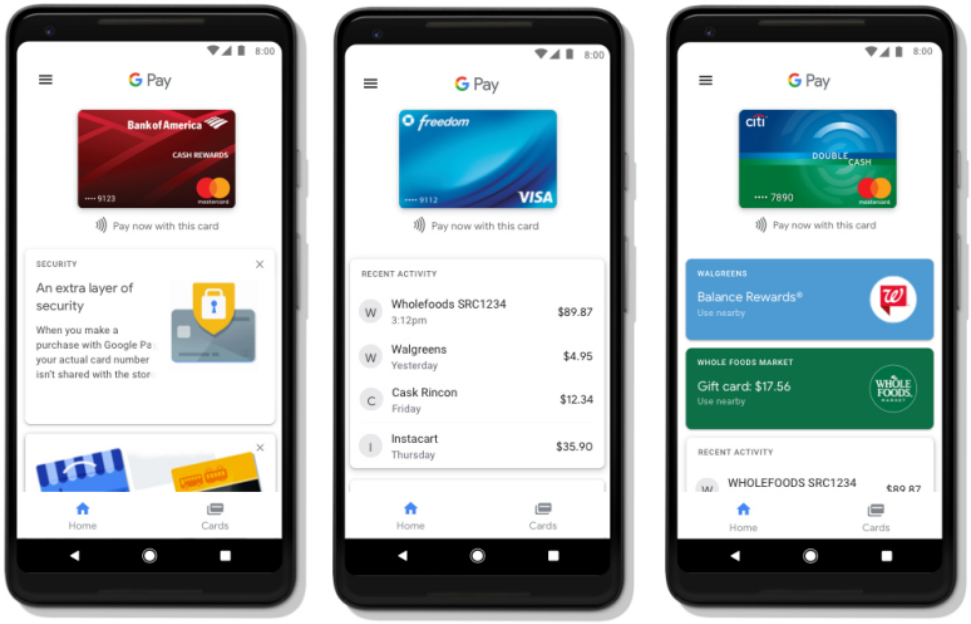
1.1.16 Agregace účtů *2000 n.l.*

Online agregace bankovních účtů přes webovou aplikaci nastoupila v USA kolem roku 2000, kde hlavním průkopníkem byla společnost Yoodle.[24] V Evropě se průkopníkem stala společnost eWise v témže roce.[26] Dá se považovat za zrod FinTech společností.

1.1.17 Bezkontaktní karta *2011 n.l.*

Bezkontaktní karta vznikla v roce 2007 v Evropě a pro věřejnost ji první spustila banka Barclays v roce 2011.[27] Čipy disponují technologií RFID, jejíž dosah závisí na frekvenci čipu. Nicméně z důvodu bezpečnosti RFID čipy v kartách mají dosah na vzdálenost kolem čtyř centimetrů.[22]

1.1.18 Platba mobilem *2011 n.l.*



Obrázek 1.3: Ukázka placení mobilem s Google Pay.[3]

V roce 2011 v USA inicializovala platby mobilem společnost Google s aplikací Google Wallet, dnes známou pod Google Pay Send. Dnes platbu mobilem z Google rodiny podporuje už jenom mobilní aplikace Google Pay, jejíž ukázku lze vidět na obrázku 1.3. Pro platbu mobilem musí být účet v aplikaci propojený s existující kartou a aplikaci musí podporovat banka uživatele, která kartu vydala.

Platby probíhají přes technologii NFC, která je jak v mobilech, tak v terminálech. Z pohledu bezpečnosti okopírování – NFC má dosah zhruba pouhých 10 centimetrů.[28] Terminály musí placení mobilem podporovat – nestačí současné terminály podporující bezkontaktní karty.[27]

Aplikace je dostupná pouze pro Android a iOS a je svázaná s Google účtem, pod kterým musí mít uživatel zařízení přihlášené. Další volitelnou bezpečnost zajistili čtyřmístným PINem pro operace s Google Pay.[29]

K nám se ve formě Google Pay dostalo placení mobilem až v roce 2017. Nicméně placení mobilem podporovaly již dříve některé banky v ČR pomocí vlastních bankovních aplikací, například ČSOB od roku 2016.[30]

1.1.19 Shrnutí historie bankovnictví

Co důležitého nebo zajímavého by čtenář měl po přečtení historie bankovnictví již vědět:

- Lidí, potažmo banky, podnikají s penězi svěřenými od klientů už od starověku.
- Podvody bankovnictví provázelo rovněž od jeho počátků. Akorát se přetransformovalo z násilí a hmotných krádeží na sofistikovanější formu podvodů.
- Tradiční banky si vlečou IT infrastrukturu již z 50 let 20. století.
- Kreditní karta není to samé jako debetní karta.
- FinTech aplikace se zrodily velmi brzo, kolem roku 2000.
- Platby mobilem nejsou až tak žhavá novinka, minimálně ne v USA.
- V USA z důvodu odporu obchodníků vůči EMW kartám výrazně zaostávají s bezpečností za EHP, kde je bankovní trh nejenom EU výrazně regulovaný.

V další kapitole i retrospektivně vysvětlím důležité pojmy bankovnictví vzhledem k mé práci.

1.2 Důležité pojmy bankovnictví

Jak jsem již zmínil, bankovní trh je obsáhlý pojem. Pojmů je tedy na bankovnictví pomálu. Vysvětlím úplné základy dělení bankovního trhu a pojmy důležité vzhledem k mé práci. Pokud je čtenář velmi znalý v bankovnictví, může kapitolu přeskočit. Nejdůležitější je pochopit clearing a dělení institucí platebního styku podle ČNB, respektive českého zákona.

1.2.1 Centrální banka

Centrální banka je nezávislou národní autoritou, která se stará o monetární politiku, reguluje banky a poskytuje finanční služby. Jejím cílem je držet stabilní měnu kontrolou inflace a nízkou nezaměstnanost. Centrální banky jsou spravovány představenstvem a komerční banky jsou jejími členy. V ČR je centrální bankou ČNB – Česká národní banka se sídlem v Praze, Na Příkopě 28 a s dalšími sedmi regionálními zastoupeními v Praze, Ústí nad Labem, Plzni, Českých Budějovicích, Hradci Králové, Brně a Ostravě.[31]

Monetární politika

- **Povinné minimální rezervy** - Množství peněz, které musí mít banky k dispozici. Slouží ke kontrole, kolik banky mohou půjčit.[32]
- **Operace na volném trhu** - Nákup a prodej cenných papírů jednotlivých bank, což mění množství peněz k dispozici bez změny povinné minimální rezervy.[32]
  - **Restriktivní měnová politika** - **Zvýšení** úrokových sazeb pomocí **prodeje** cenných papírů bankám. Zpomaluje inflaci a ekonomický růst.
  - **Expanzivní měnová politika** - **Snížení úrokových sazeb** pomocí **nákupu** cenných papírů od bank. Snižuje nezaměstnanost a stimuluje ekonomický růst.[33]
- **Nastavování úrokových sazeb** - Centrální banka nastavuje výši úrokových sazeb, které si účtuje od bank. Tím ovlivňuje výši úroků pro půjčky, hypotéky a dluhopisy. Zvýšení úrokových sazeb vede k zpomalení ekonomického růstu a snížení inflace.[32]

Regulace bank

Centrální banka reguluje své členy, tedy ostatní banky - například regulace pro rezervy pokrytí ztrát z půjček nebo za účelem finanční stability, ochrany vkladů apod.[32]

Poskytování finančních služeb

Centrální banka poskytuje služby jak bankám, tak státu. Kontrolují tok peněz a půjčují peníze svým členům. Svoji měnu uchovává v **devizových rezervách**, respektive rezervách v cizí měně, zpravidla v dolarech nebo eurech. Rezervu používá za účelem regulace kurzu, směnně mezi měnami a držení vlastní stabilní měny (fixování) kvůli kompetitivním exportním cenám.[32]

1.2.2 Finanční instituce

Mezi finanční instituce patří organizace, jejichž předmětem podnikání je obchodování s peněžními transakcemi ve formě vkladů, půjček, investic nebo převodů měny. Do hlavních kategorií finančních institucí spadají[34]:

- Centrální banky
- Komerční banky
- Internetové banky

- Družstevní záložny
- Investiční fondy a společnosti
- Makléřské firmy
- Společnosti poskytující úvěry a spoření
- Pojišťovny
- Hypotéční společnosti

1.2.3 Instituce platebního styku

Do institucí platebního styku spadají[35][36][37]:

- Instituce elektronických peněz — Můžou vydávat elektronické peníze. Licence umožňuje i činnosti spadající do platební instituce.
  - Vydavatelé elektronických peněz malého rozsahu — Můžou vydávat elektronické peníze ve stanoveném maximálním rozsahu. Licence umožňuje i činnosti spadající do poskytovatelů platebních služeb malého rozsahu. Limit pro průměrný oběh elektronických peněz v ČR za posledních 6 měsíců je stanoven na 5 000 000 EUR. Limit pro měsíční průměr provedených plateb v ČR za posledních 12 měsíců je stanoven na 3 000 000 EUR. Limit úschovy elektronických peněz pro jednotlivce je stanoven na 150 EUR. Pro vyšší objemy jednoho nebo obou případů je nutná licence instituce elektronických peněz.
- Platební instituce — Můžou poskytovat platební služby.
  - Poskytovatelé platebních služeb malého rozsahu — Můžou poskytovat platební služby ve stanoveném maximálním rozsahu. Limit pro měsíční průměr provedených plateb v ČR za posledních 12 měsíců je stanoven na 3 000 000 EUR. Pro vyšší objemy je nutná licence platební instituce.

Jednotlivé licence mají odlišné podmínky pro jejich získaní u ČNB, které lze nalézt v příslušných zákonech. Jednou z nich je například výše požadovaného základního kapitálu nebo výše počátečního kapitálu. Obecně platební služby mohou poskytovat[38]:

- ČNB
- Banky
- Spořitelní a úvěrová družstva
- Zahraniční banky nebo jejich pobočky

- Instituce elektronický peněz vč. zahraničních
- Vydavatelé elektronických peněz malého rozsahu
- Platební instituce nebo jejich pobočky vč. zahraničních
- Poskytovatelé platebních služeb malého rozsahu

1.2.4 Cenné papíry

Cenné papíry slouží jako finanční nástroj, který reprezentuje finanční hodnotu čehokoliv. Díky tomu se s cennými papíry snadno obchoduje. K obchodování s cennými papíry je zapotřebí licence. Subjekt vydávající cenný papír se nazývá **emitent**. Cenné papíry se dělí na:

- Majetkové cenné papíry – akcie.
- Dluhové cenné papíry – dluhopisy.
- Derivátové cenné papíry – spekulace založené na hodnotě jiných aktiv a jejich cenovému vývoji.[39]

1.2.5 Obchodovatelné nástroje

Ve světě mezi obchodovatelné nástroje patří směnky:

- Cizí – emitent (třetí strana, která směnku vydala), remitent (příjemce, na jehož jméno je směnka vydána), směnečník (plátce)
- Vlastní – emitent (plátce, který směnku vydal), remitent (příjemce, na jehož jméno je směnka vydána)

Nicméně v českém zákoně obchodovatelné nástroje spadají pod cenné papíry. Pod směnky se řadí například i šeky – v ČR ale opět zvlášť spadající pod cenné papíry.[40][41]

1.2.6 Clearing, clearingové centrum/středisko

V následujícím textu mluvím především o clearingu ve vztahu k bankám, nicméně clearing může být i mezi jinými subjekty - například při obchodu s cennými papíry. Clearing je operace při níž se provede započtení pohledávek a závazků pro bezhotovostní placení mezi subjekty, například bankami (z vlastních a klientských operací).[42] Pro tyto účely existují clearingová centra/střediska.[2] Clearingová centra zefektivňují transakce – subjekt nemusí nijak přijít

[2]V angličtině existuje jednotný pojem "Clearing House", nicméně v češtině se můžeme setkat s pojmy clearingové centrum nebo clearingové středisko. Pokud budu vycházet z webu ČNB[43], tak za clearingové centrum se považuje ČNB a jejich systém CERTIS, kdežto

do kontaktu s druhým subjektem. Dále snižují rizika – jsou odpovědná vůči všem svým subjektům za plnění smluv. Kvůli odpovědnosti se snaží různými regulacemi rizika mitigovat – například subjekty musejí mít u clearingového centra svůj účet s určitým minimálním zůstatkem.[44] Zúčtování přes clearingové centrum může probíhat dvěma způsoby – nettingem nebo RTGS (Real Time Gross Settlement).

Netting

Způsob clearingu, kdy z veškerých pohledávek a závazků vůči jedné bance se na konci účetního dne udělá rozdíl, na základě něhož proběhne vypořádání mezi bankou a clearingovým centrem.[45] Pro lepší představu jsem vytvořil obrázek 1.4 ukazující příklad jednoho clearingu. Jak lze například u banky Z vidět, výše odchozích plateb je 2 500 Kč a výše příchozích plateb je 3 500 Kč. Na účet banky Z je tedy clearingovým centrem připsáno 1 000 Kč.

RTGS

Způsob clearingu, který může být proveden okamžitě. Je vyžadován pro velké objemy mezibankovních transakcí a zajišťují ho většinou centrální banky. Hlavním cílem je odstranění rizika zpoždění dokončení transakcí.[46]

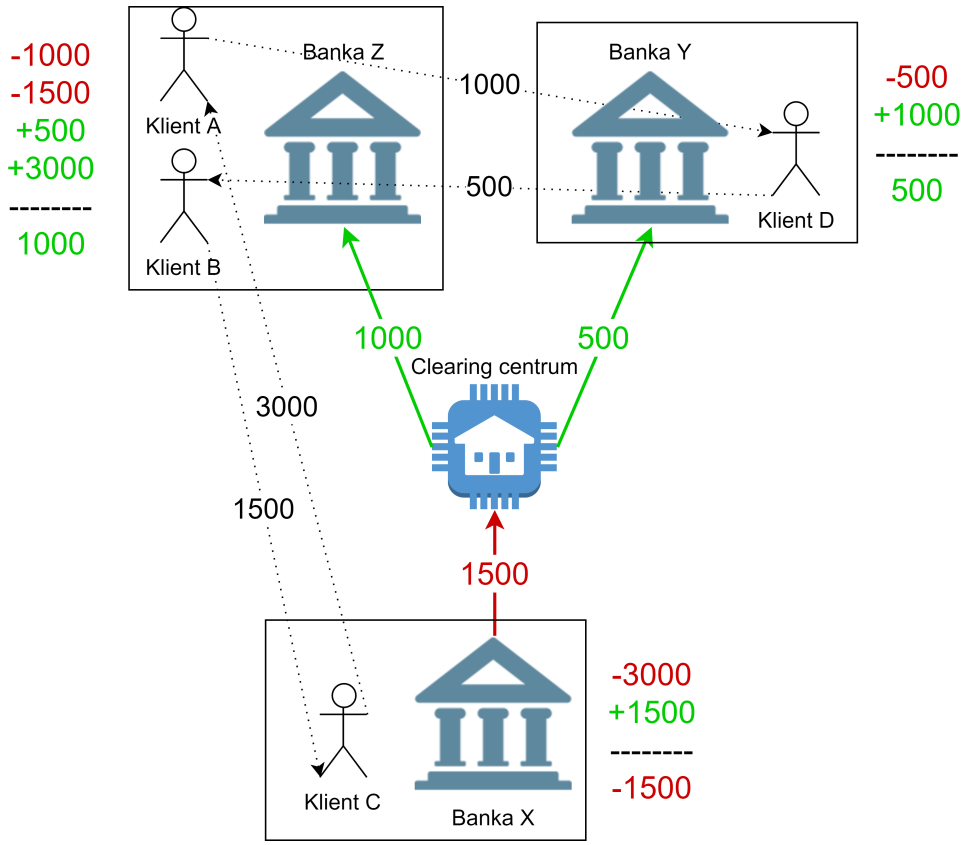
1.2.7 Platby

Platby zajišťují platební služby, viz kapitola 1.2.3. Veškeré elektronické platby mezi dvěma různými platebními službami, ať už probíhají jakoukoliv metodou, musejí projít přes clearing, viz kapitola 1.2.6. Mezi platební metody se řadí[47]:

- Kreditní karta
- Debetní karta
- Inkasní platba
- Šek
- Převod peněz

Převod peněz probíhá i z e-Peněženky, nejenom z klasických bankovních účtů. Obchodník, který umožňuje platby přes e-Peněženku, musí mít rovněž u dané společnosti e-Peněženku. Jeden z důvodů spočívá v zajištění instantní platby, jelikož se jedná o převod v rámci jedné instituce a tudíž nepodléhá clearingu.

clearingová střediska jsou ostatní instituce zajišťující zúčtování například okolo platebních karet nebo cenných papírů. Funkce je ale u obou stejná. V textu nadále používám pojem clearingové centrum a myslím tím jakoukoliv instituci poskytující clearing.



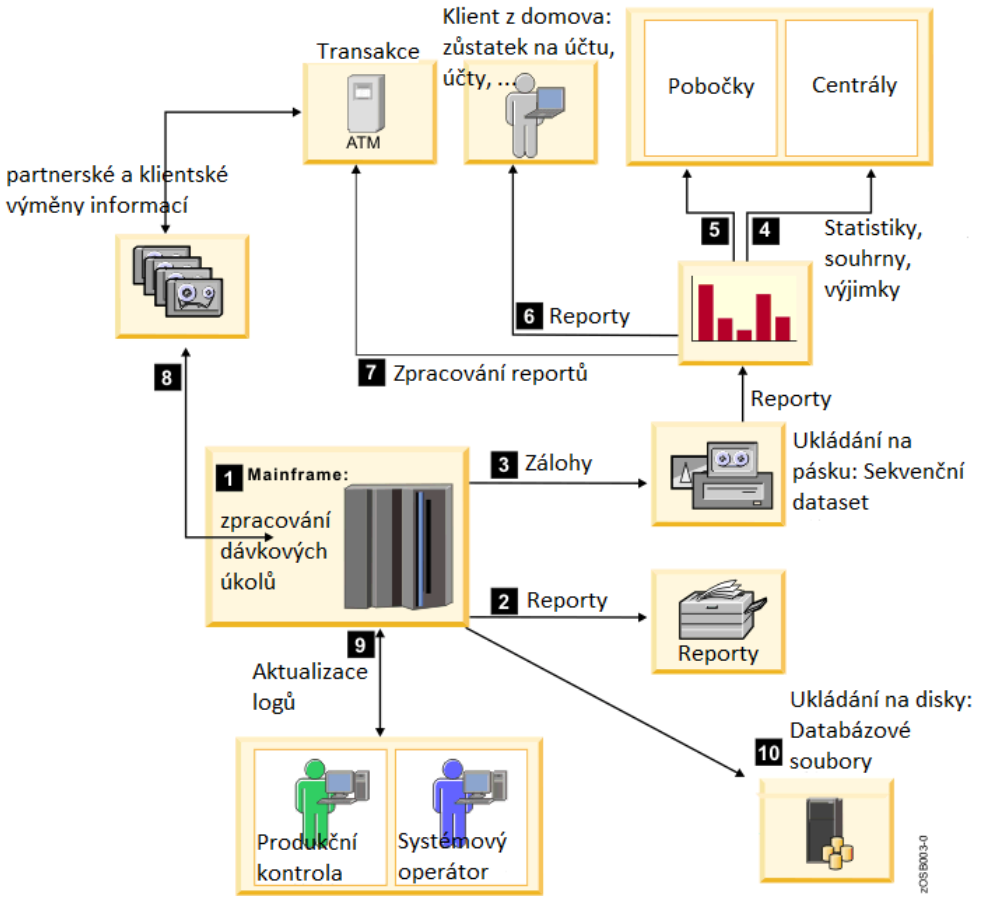
Obrázek 1.4: Ukázka jednoho clearingu mezi čtyřmi klienty, respektive třemi bankami.

1.2.8 Dávka, dávkové zpracování

Dávka, mnohdy z angličtiny nepřekládaný výraz „batch“, je soubor zpravidla velkých dat připravený pro dávkové zpracování. Dávkové zpracování nepotřebuje uživatelskou interakci, spouští se většinou skriptem.[48] Mezi výhody dávkového zpracování patří znatelně nižší náklady, jelikož se efektivně využije veškerý dostupný HW, navíc například po běžné pracovní době, kdy bývá HW méně vytížen. V bankovnictví na dávkové zpracování navazuje mnoho dalších procesů (reportů, analýz, statistik, apod.) na základě výstupů z dávkového zpracování. Zpracování takto velkého množství operací v reálném čase by nebylo možné pokrýt.[49] O dávkové zpracování se většinou stará takzvaný mainframe.[4]

1.2.9 Mainframe

Dávkové soubory zpracovává mainframe (cluster) bez interakce uživatele, viz ukázka na obrázku 1.5. Výhoda mainframu spočívá ve vysokém výkonu a



Obrázek 1.5: Typické použití mainframu pro dávkové zpracování.[4]

dostupnosti[4]:

- Dostatečné datové úložiště.
- Dostupná kapacita procesorů.
- Paralelní výpočty využívající efektivně zdroje.

1.2.10 ISO 20022

ISO 20022 představuje mezinárodní standard navržený k zjednodušení globální byznysové komunikace, zejména ve finančním sektoru. Standard zajišťuje, aby nedocházelo k mylné interpretaci pojmů díky globálnímu slovníku ve společném jazyce, kterému každý může rozumět. Slovník je určený zejména pro vytváření standardizované celosvětové komunikace mezi informačními systémy. Slovník je vedený v XML formátu.[50]

1.2.11 Shrnutí bankovních pojmů

Čtenář by si měl odnést povědomí o centrální bance, která stojí nad bankami a kupříkladu uděluje licence. Z kapitoly by mělo být dále jasné, co je to clearing a rozdíl mezi metodou netting a RTGS, aby v nadcházející kapitole mohl čtenář pochopit fungování clearingu v praxi. Dále by mělo být jasné, že pod clearing spadají veškeré platby, i když se navenek tváří jako platby instantní. Klasickým příkladem jsou platební karty, kde k zaúčtování dochází mnohem později než byla uskutečněna platba. S clearingem jsou úzce provázané dávky a mainframy. No a veškerou komunikaci v tomto kolosu propojených informačních systému zajišťuje mezinárodní standard ISO 20022.

1.3 Trendy přístupu k zákazníkům

V kapitole napřed uvedu trendy přístupu k zákazníkům z pohledu bank. Následně rozvedu bankovnictví v ČR ukázkou clearingového systému v praxi a představením bank a jejich podílu na českém trhu. Na závěr vydefinuji oblast FinTech, která poslední dobou mění trend přístupu k zákazníkům v bankovnictví nejvíce.

Banky nepřistupují ke všem zákazníkům stejně. Bankovnictví dělí na skupiny a podskupiny:

- Retailové bankovnictví
  - Osobní bankovnictví
  - Privátní bankovnictví
- Korporátní bankovnictví
  - Malé a středně velké podniky
  - Velké firmy a korporátní společnosti

Některé banky mají speciální divize a obsáhnou tak všechny skupiny klientů. Jedná se především o tradiční banky, například v ČR Česká spořitelna nebo Komerční banka. Některé banky se specializují čistě na osobní bankovnictví, například v ČR AirBank, nebo čistě privátní bankovnictví, například v ČR J&T Banka.

Většina bank umožňuje vklady hotovosti, buď na pobočce nebo poslední dobou přes takzvané vkladomaty. Většina bank rovněž umožňuje přístup k bance přes pobočky, které jsou někdy vedeny zvlášť pro retailové a korporátní bankovnictví.

1.3.1 Retailové bankovnictví

Hlavní produkty spadající pod retailové bankovnictví:

- Běžné účty — Lze z nich provádět běžné platby a obecně transakce. Nabízejí zpravidla nízký úrok.
- Spořící účty — Transakce mají omezené, většinou pouze převody a jenom za určitých podmínek. Nicméně úrok bývá vyšší jak na běžném účtu.
- Termínované vklady — Investiční produkt, který váže vklad peněz po stanovené období. Bývá zpravidla úrokováno vyšší sazbou za předpokladu dodržení vázaného období, kdy nedojde k výběru peněz.
- Úvěrové účty — Není jako samostatný produkt. Váže se ke kreditním kartám, hypotéčním úvěrům nebo úvěrům samotným.
- Úvěry — Poskytování úvěrů, jichž je celá řada. Do úvěrů spadají i hypotéční úvěry a leasingy. Vzhledem k jejich významnosti jsem je zmínil zvlášť. Mezi zbylé úvěry se nejčastější vyskytuje spotřebitelský úvěr – tedy úvěr na zboží pro osobní účely. Dále jsou časté kontokorentní úvěry, respektive účty, kde lze jít do mínusu.
- Hypotéční úvěry — Tvoří podstatnou část zisku a kapitálu bank z retailového bankovnictví.
- Leasingy — Pronájem různých zařízení, nejčastěji aut. Dělí se na finanční (po splacení se dlužník stane majitelem) a operativní (jedná se víceméně o pronájem).
- Karty — Vydávání debetních nebo kreditních karet, které pro banky tvoří rovněž značný podíl výdělku díky poplatkům za placení kartami.
- Zahraniční převody a převody měn — Vzhledem ke globalizaci se stává čím dál významnějším produktem i pro retailové bankovnictví.
- Pojištění — Pojištění osob, zejména úrazové a finanční pojištění.
- Správa financí — Kupříkladu poradci, ať už osobní nebo v dnešní době digitální, pro finanční a investiční rady.

Privátní bankovnictví se podobá osobnímu, ale banky se zaměřují v daném segmentu na movitější klientelu s vyšším čistým jměním. Služby nabízejí více osobnější, zaměřené směrem k investicím.[51]

1.3.2 Korporátní bankovnictví

Hlavní produkty spadající pod korporátní bankovnictví:

- Úvěry a kreditní produkty — Největší oblast byznysu banky – tvoří největší profit, ale zároveň risk pro banky.

- Pokladna a správa hotovosti — Využíváno společnostmi pro správu jejich operativního kapitálu a pro potřebu převodů měn.
- Leasingy — Pro vybavení společností od výrobních strojů, dopravy až po informační technologie.
- Komerční nemovitosti — Služby jako analýza aktiv, hodnocení portfolia, dluhové a kapitálové strukturování.
- Finance obchodu — Zahrnuje akreditivy, sběr účtů a fakturace.
- Zaměstnanecké služby — Služby jako mzdové vypořádání.

Mezi další okrajovější služby určené hlavně pro korporátní společnosti patří například správa aktiv a držení cenných papírů.[51]

1.3.3 Bankovnictví v ČR

Jak si již z historie bankovnictví v kapitole 1.1 šlo povšimnout, trendy přístupu k zákazníkům v České republice nejsou odlišné od těch v zahraničí – jsou jenom opožděné. Proto přiblížím bankovnictví v ČR, které se minimálně od zbytku EHP příliš neliší.

ČNB

Česká národní banka představuje centrální banku České republiky. Nejenom o činnostech centrální banky si lze více přečíst v kapitole 1.2.1 o centrálních bankách. Vzhledem k ČNB zmíním hlavně systém CERTIS, abych ukázal clearingový systém v praxi. Nutným předpokladem pro lepší pochopení následujícího textu je znalost teorie clearingu v kapitole 1.2.6 a teorie platebních metod v kapitole 1.2.7.

Systém CERTIS Banky v ČR musí využívat pro **mezibankovní** převody clearingové centrum ČNB, konkrétně jejich systém CERTIS na bázi RTGS. CERTIS má několik základních principů (pro účely DP vytyčím pouze ty nejdůležitější):

- v českých korunách bez ohledu na částku (pro platby v cizí měně musí banky využívat zahraniční clearingové systémy)
- platby probíhají na účtech bank u ČNB (slouží zároveň jako účty povinných minimálních rezerv, které musí být ve výši 2% z depozit a mohou být k platbám používány)
- položky akceptované systémem nelze již odvolat

Tabulka 1.1: Ceník a přehled účetního dne ČNB pro zpracování plateb. D je pracovní den. Ceník platný ke dni 25. 2. 2018[52]

Operace			Cena v Kč
Zpracování jedné **neprioritní** položky			0,09
Zpracování jedné **prioritní** položky			1,00
Přirážka k jedné položce podle času předání dávky.			
Od 17:00 dne D-1	do 13:00 dne D	I. pásmo	0,00
Od 13:00 dne D	do 14:30 dne D	II. pásmo	1,00
Od 14:30 dne D	do 16:00 dne D	III. pásmo	4,00

- na účtech bank není povoleno debetní saldo[3]
- platby, na které není dostatek prostředků, jsou odloženy a zúčtovány, až když je na účtu dostatek prostředků
- ČNB poskytuje bezúročný vnitrodenní úvěr pro plynulé fungování platebního styku
- není-li splacen, tak cenné papíry sloužící jako zástava jsou převedeny na účet ČNB a slouží dále jako zástava pro úvěr přes noc
- nesežene-li banka prostředky do konce účetního dne, je příkaz k platbě odmítnut a vrácen bance

Průběh účetního dne je vidět v tabulce 1.1 společně s cenami za jednu položku v dávce. ČNB poskytuje i množstevní slevy za počet položek v měsíci (v řádu milionů položek). Propustnost systému je 1 500 000 transakcí za hodinu. Proto je účetní den rozdělen do zpoplatněných pásem, čímž ČNB motivuje banky pro rovnoměrnější rozložení transakcí v rámci účetního dne. Data jsou od bank předávána zpravidla v dávkách přes síť, eventuálně na nosiči.[43]

Banky v ČR

Bankovní licenci má v ČR celkově 47 bank, mimo jiné hypotéční, exportní, stavební spořitelny a další, viz kapitola 1.2.3 o finančních institucích. Seznam udělených bankovních licencí lze nalézt na webu ČNB[4]. Do seznamu, který lze vidět v tabulce 1.2, jsem uvedl větší univerzální banky, tedy banky poskytující široké spektrum bankovních služeb. Některé banky se mohly dříve jmenovat jinak, jelikož došlo k jejich akvizici, nicméně bankovní licence bývá často součástí akvizice a není třeba ji měnit (například Equa bank původně Banco Popolare). Strukturu, respektive akcionáře bank, lze nalézt například

[3]Debetní saldo – záporný zůstatek na účtu.

[4]https://www.cnb.cz/cnb/jerrs -> Základní seznamy -> Banky a pobočky zahraničních bank.

Tabulka 1.2: Přehled jednotlivých bank, seřazených podle roku zahájení činnosti, a jejich majoritních akcionářů dle dat z let 2016 a 2017.[5]

Banka	Od	Majoritní akcionář	Sídlo	Podíl
ČSOB	1965	KBC bank	Belgie	100%
Česká spořitelna	1992	Erste Group Bank	Rakousko	99%
KB	1992	Société générale	Francie	60%
J&T BANKA	1992	J&T Finance Group SE	Česká r.	100%
Raiffeisen BANK	1993	Raiffeisen Bank I.	Rakousko	75%
Equa bank	1994	Equa Group Limited	Malta	100%
SBERBANK	1997	Sberbank Russia	Rusko	100%
MONETA Money Bank	1998	J. P. Morgan	USA	24%
Oberbank 3 Banken Gruppe	2004	CABO B. mbH	Rakousko	26%
mBank	2007	Commerzbank	Německo	70%
UniCredit Bank	2007	UniCredit Group	Itálie	100%
Expobank	2008	Igor Kim	Rusko	100%
Fio banka	2010	Marsa a Kopún	Česká r.	100%
air bank	2011	PPF Group (Kellner)	Nizozemí	89%
BANKA CREDITAS	2017	Pavel Hubáček	Česká r.	66%
Hello bank!	2017	BNP Paribas	Francie	100%

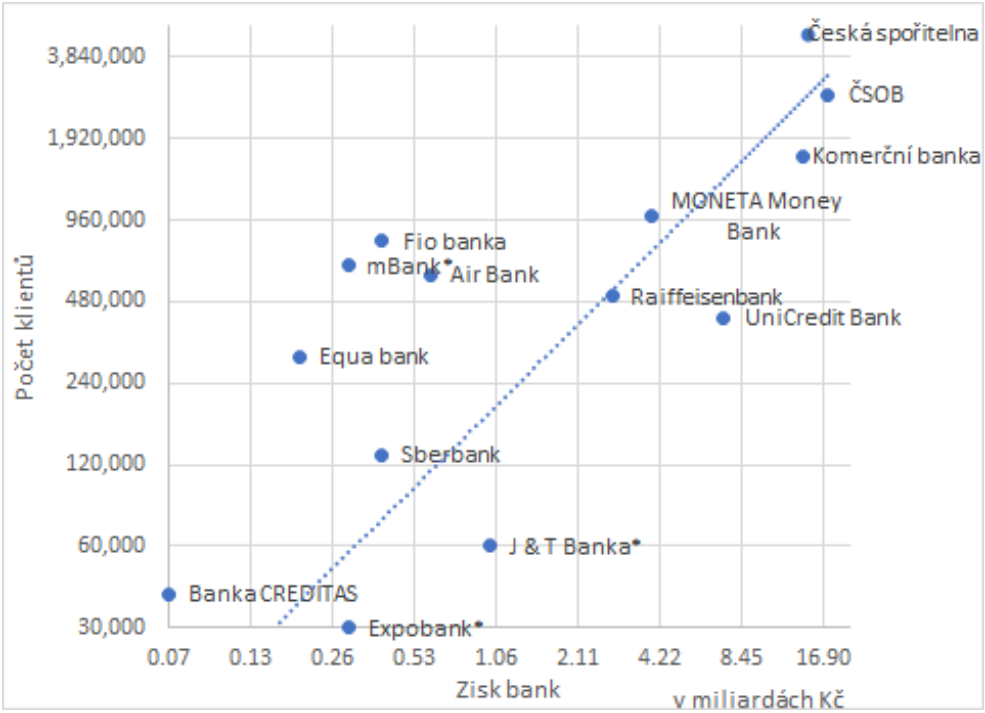
ve výročních zprávách bank v rámci informační povinnosti bank. Hello bank! v dalších statistikách vynechávám, jelikož začala působit v ČR na konci roku 2017 transformací Cetelem, která se zaměřovala primárně na úvěry. Z toho důvodu u Hello bank! není dostatek historických dat. Některé banky jsou mezi lidmi méně známé, respektive mají méně klientů, jelikož se zaměřují zejména na firemní a movitou klientelu – například J&T Banka nebo Expobank. To je dobře vidět i z obrázku 1.6.

Cílová skupina Z počátku této kapitoly 1.3 jsem ukázal, že banky se zaměřují na více cílových skupin. Z obrázku 1.6 lze do jisté míry vyčíst na jaké

[5]Tabulku jsem vytvořil na základě dat z následujících zdrojů. Majoritní akcionáři pochází ze zdroje na základě článku vycházející z výročních zpráv bank roku 2016[53], doplněné o chybějící banky a další některá aktuálnější data z jednotlivých výročních zpráv bank (rok 2017), které jsou povinně zveřejňovány na webových stránkách bank.[54][55][56][57] Sídla majoritních akcionářů vychází z článku na mesec.cz[58] a z předešlých výročních zpráv bank. Zahájení činnosti vychází primárně ze seznamu komerčních bank na finance.cz[59] a u chybějících z webových stránek bank[60][61][62].

klienty se banky zaměřují a jak se jim daná strategie daří.

Zanedbám-li různorodost klientů a kvalitu hospodaření bank, jednalo by se o ideální lineární spojnici trendu, tedy čím více má banka klientů, tím větší bude mít zisk. Nicméně to samozřejmě neplatí zcela, jak můžeme na obrázku 1.6 vidět. Zejména Expobank, J&T Banka a UniCredit banka se zaměřují na movitější klientelu (privátní bankovnictví, podnikatelé, firmy). Naopak nové nízko-nákladové banky jako Fio banka, mBank, Air Bank cílí na běžné klienty. Navíc se často může jednat pouze o vedlejší účet s menším vkladem, jelikož menší banky neposkytují tolik produktů jako tradiční banky. Pro zajímavost nízko-nákladové banky (Air Bank, Fio banka, mBank, Equa bank) měly v roce 2017 dohromady 2 350 000 klientů, ale zisk pouze 1,5 miliardy Kč. Oproti tomu například tradiční banka jako je KB měla 1 650 000 klientů, přičemž zisk 14 miliard Kč – tedy o 700 000 klientů méně, ale zisk vyšší o 12,5 miliard Kč.



Obrázek 1.6: Vztah mezi počtem klientů bank a ziskem bank z roku 2017.[6]

[6]Graf jsem vytvořil na základě dat o zisku bank ze zdroje Finparáda, který čerpal z výročních zpráv jednotlivých bank[63], a o počtu klientů z tabulky 1.3. U bank označených hvězdičkou(*) nejsou ještě dostupné hospodářské výsledky za rok 2017, a proto pro účely porovnání byly vzaty výsledky z roku 2016. Zisk banky CREDITAS pochází přímo z jejich výroční zprávy.[64]

Tabulka 1.3: Počet klientů jednotlivých bank v tisících napříč posledními třemi roky.[7]

Banka	2015	2016	15v16	2017	16v17
Česká spořitelna	4,790	4,710	-80	4,680	-30
ČSOB	2,830	2,800	-30	2,760	-40
Komerční banka	1,650	1,650	0	1,650	0
MONETA Money Bank	1,070	970	-100	1,000	30
Fio banka	550	670	120	800	130
mBank	570	630	60	650	20
Air Bank	420	520	100	600	80
Raiffeisenbank*	500	500	0	500	0
UniCredit Bank		350		420	70
Equa bank	200	250	50	300	50
Sberbank	100	110	10	130	20
J & T Banka	50	50	0	60	10
Banka CREDITAS		20		40	20
Expobank	30	30	0	30	0
Oberbank		17		17	0
Celkem		**13,277**		**13,637**	**360**

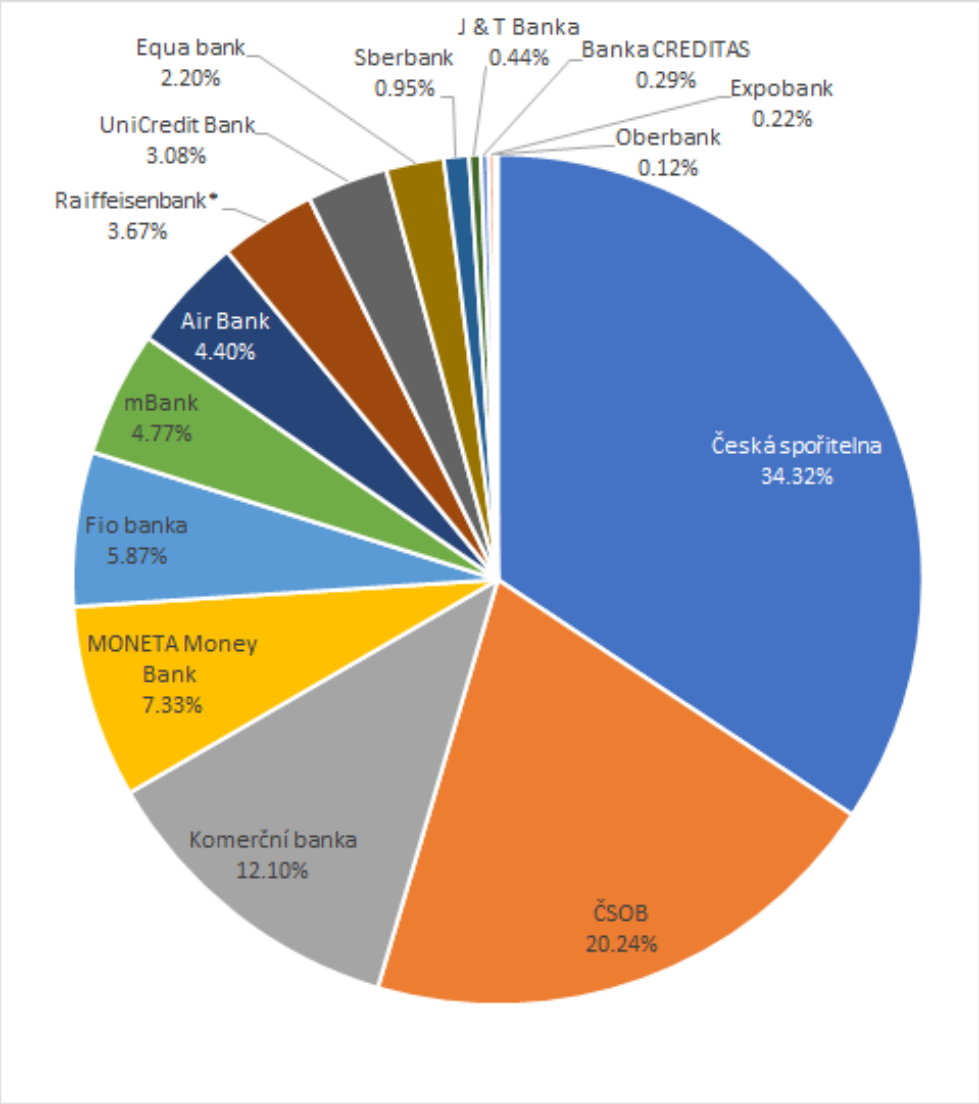
Srovnání podle počtu klientů Z tabulky 1.3 vyplývá, že mladší nízko-nákladové banky se těší každý rok nárůstu klientů v desetitisících. Drží již 17% bankovního trhu v ČR, přičemž oproti tradičním bankám mají zpoždění desítky let.[8] Můžou za to zejména následující faktory:

- Minimálně v době jejich příchodu disponovaly modernějšími službami.
- Začaly nabízet vedení osobních účtů zdarma.
- Lákají okamžitým finančním bonusem nebo dlouhodobým finančním bonusem ve formě vyšších úroků a to i na běžném účtu.
- Zaměřují se hlavně na retailové bankovnictví, takže dokážou lépe cílit na zákazníka.

Nízko-nákladové banky se i přes to, jaký mají podíl na trhu (viz obrázek 1.7), a i přesto, že ve výsledku platí klientovi, dokáží držet v zisku. Od tradičních bank jim odpadají zejména následující náklady:

[7]Tabulku jsem vytvořil na základě sloučení dat z několika zdrojů[65][66][67][68][53], jelikož každý zdroj obsahuje pouze část potřebných dat a počty klientů nejsou většinou součástí výročních zpráv bank. * – U Raiffeisenbank se jedná pouze o odhad počtu klientů, jelikož daná banka nezveřejňuje svoje čísla o počtech klientů.

[8]Řada tradičních bank vznikla vyčleněním z bývalých bank po pádu komunismu v ČR.



Obrázek 1.7: Banky v ČR a jejich podíl na trhu vzhledem k počtu klientů v roce 2017 dle tabulky 1.3.

- Informační systémy, zejména mainframe, byly vystaveny od nuly. Nenesou si tedy technologický dluh a jsou s největší pravděpodobností postaveny na mnohem lepší architektuře, což má za následek:
  - Nižší náklady na údržbu vzhledem k počtu klientů.
  - Nižší náklady na provoz vzhledem k počtu klientů.
  - Nižší náklady na rozšiřování stávajících systémů.
  - Nižší náklady na napojování nových systémů k stávajícím.

Nejvíce se dopad projeví při každé legislativní změně vyžadující zásah do IT, například GDPR nebo PSD2, kde cenový rozdíl zavedení legislativy může být v desítkách milionů.

- Zaměřují se především na retailové bankovnictví, což vede ke štíhlejší organizační struktuře.
- Mají málo nebo žádné pobočky.
- Mají malou infrastrukturu bankomatů.

1.3.4 FinTech

FinTech, zkratka pro finanční technologie, může být brán jako technologický trend přetvářejí finanční trh, bojující proti tradičnímu bankovnictví, které je zatížené regulacemi a odolné vůči změnám pro snadnější pohyb peněz. FinTech není jasně definován, jelikož tento průmysl se stále vyvíjí a je velmi mladý. Trend přístupu k zákazníkům mění ale zásadním způsobem, jelikož i banky se musí přizpůsobovat buď spoluprací s FinTech společnostmi nebo vytvářením vlastních bankovních aplikací kopírující trendy přinášené FinTech společnostmi. Skvělým příkladem je například zmíněné placení mobilem (kapitola 1.1.18), kdy banky spolupracují s Google Pay. Například ale AirBank, která z nějakého důvodu nechce příliš spolupracovat s třetími stranami, přišla s vlastní aplikací pro placení mobilem, aby držela krok s trendy.

Kdy začaly FinTech společnosti vznikat, se zdroje rozchází. Nicméně kouknuli na historii bankovnictví, zejména v kapitole 1.1.16, datoval bych začátek prvních FinTech společností kolem roku 2000. Větší vlna startupů vznikla mezi roky 2008 až 2010 (například i slavný Bitcoin[69]), nicméně k největšímu rozšíření došlo od roku 2015. Nyní se pod FinTech řadí jakákoliv technologická inovace ve finančním sektoru.[70] FinTech můžeme rozdělit do několika kategorií podle oblasti finančního sektoru, na který se aplikace zaměřují. Opět se nejedná o pevně stanovené kategorie a mohou se zdroj od zdroje lišit.

1.3.4.1 Platby a převody peněz

Platební brány Služba mezi zákazníkem a prodejcem poskytovaná přes e-shopy a obecně přes e-komerční stránky. Autorizuje kreditní karty nebo přímé platby při obchodu. Platební brána se dá představit jako virtuální místo uskutečnění prodeje. Například **GoPay**.

e-Peněženky Aplikace, které umožňují uživatelům ukládat a platit penězi z chytrého zařízení, typicky chytrého telefonu. Například **PayPal**.

Převody Služby zajišťující **přeshraniční** převod peněz. Kromě rychlosti je hlavním cílem zlomková cena oproti bankám a kamenným pobočkám (Western Union). Například **TransferWise**.

1.3.4.2 Půjčky (alternativní financování)

Přes takzvaný crowdfunding lze vybrat peníze od velkého množství lidí na půjčku, ať už pro nákup soukromé věci nebo kapitál na rozjetí byznysu, či projektu.

Odměna Byznys nebo organizace, za účelem získání peněz od fanoušků projektu, nabídne nějakou pobídku/y. Pobídek může být více, nemusí se jednat pouze o jednu ve formě hlavního produktu. Odměnou může být prakticky cokoliv od zboží, slev na služby až po vouchery. Například **Kickstarter**.

Dar Uživatelé si mohou vybrat projekt, kterému chtějí darovat své peníze výměnou za nic. Často souvisí s charitou nebo obecně pro dobro věci, kterou lidé chtějí aktivně podporovat. Například **JustGiving**.

Podíl Podnikatelé a startupy mohou nelézt malé investice od velkého počtu investorů výměnou za finanční podíl v jejich společnosti nebo aktivy společnosti odpovídající výši investice. Práva nových akcionářů se mohou lišit v závislosti na pravidlech a podmínkách. Například **Seedrs**.

Dluh Individualisté nebo skupina individualistů půjčuje peníze byznysům nebo jiným individualistům s očekáváním navrácení půjčky včetně úroků, zkráceně P2P půjčky[9]. Například **Zonky**.

1.3.4.3 Poradenství a osobní finance

Srovnávače Umožňuje uživatelům vyhledat, porovnat a zařídit finanční produkty jako jsou karty, půjčky a pojištění. Uživatelé filtrují kritéria na základě svých preferencí, aby vyhledali nejvhodnější a nejpopulárnější produkt. Například **HaloMoney**.

Správa Kombinuje správu osobních investic, finanční poradenství a plánovací aplikace pro jednotlivce vysokým čistým jměním (HNWI).[10] Některé služby jsou navržené pouze pro správu osobních financí. Například **8securities** (HNWI) nebo **Wallet** (osobní).

Umělá inteligence Robotické poradenství poskytující online rady nebo správu portfolia s téměř žádným lidským zásahem. Nabízí akční finanční a investiční návrhy založené na matematických principech, statistické analýze a vhodných algoritmech. Například **Wealthfront**.

[9] Peer-to-peer vychází z počítačové sítě, kde jsou mezi sebou klienti napojeni přímo a komunikují spolu narozdíl od komunikace klient-server, který je v modelu zcela vynechán. Analogicky se termín používá i pro sociální účely, například pro zmíněné P2P půjčky, kde je vynechána namísto serveru banka.

[10] Jednotlivce s vysokým čistým jměním, kteří investují, lze najít v angličtině pod zkratkou HNWI - High-net-worth individual.

1.3.4.4 Technologie pojištění

Pomáhá uživatelům ušetřit peníze a zajistit maximální efektivitu v současném průmyslu pojištění. Často nachází příležitosti, které mohou korporátní společnosti přehlédnout, například velmi přizpůsobenou politikou nebo využíváním dat ze zařízení uživatele pro lepší analýzu chování uživatele, díky které mohou nabídnout dynamičtější bonusy. Například **SingaporeLife**.

1.3.4.5 Technologie regulací

Softwary, které pomáhají řešit regulační problémy ve finančních službách. Pomáhají uživatelům a byznysům dodržovat regulace specifického trhu. Rovněž pomáhají společnostem bojovat proti finanční kriminalitě a snižovat v různé formě riziko, například detekcí podvodu nebo kybernetickou bezpečností. Například **RegBot**.

1.3.4.6 Kryptoměny

Kryptoměny Forma digitálních peněz. Šifrováním se reguluje generování měny a kontrolují se jednotlivé převody. Regulace a převody probíhají nezávisle na centrální bance. Regulace a centrální banky se snaží vypořádat s kryptoměnami různým způsobem, například v Číně dochází k pokusům o zakázání kryptoměn. Například **Bitcoin**.

Blockchain Základní technologie, na které jsou kryptoměny postavené. Veřejná účetní kniha sdílená na několika různých uzlech sítě. Díky tomu nemůže být nikdy smazána, odhaluje snadněji podvody a zpronevěry. Může potencionálně změnit v budoucnu celý finanční trh. Například **Digital Asset**.

1.3.4.7 Digitální banky

Banky, které jsou dostupné pouze online. Nicméně poskytují klasické služby jako jsou správa účtu, spořící účty, vklad, výběr a převody peněz a další. Například **Atom Bank**.

1.3.4.8 Podnikatelské nástroje a software

SaaS (Software-as-a-Service) Byznys model, kde aplikaci hostuje poskytovatel služby, zpravidla v cloudovém řešení pro dostupnost odevšad. Tím je zajištěna i bezpečnost dat, například při poškození počítače účetního. Například **Xero**.

POS (Point Of Sale in cloud) Systémy, které zpracovávají platby cloudovou formou. Pokladny jsou nahrazeny chytrými zařízeními připojenými

k WiFi. Podnikatelé mohou obchodovat na cestách, monitorovat aktivity obchodu a sledovat ukazatele vzdáleně v reálném čase. Například **ShopKeep**.

1.4 Bezpečnost bankovního styku

Bezpečnostní rizika v dobách před příchodem technologií byly poměrně přímočaré. Kde se ale skrývají největší bezpečnostní hrozby a podvody v dnešní době? Na tuhle otázku se pokusím odpovědět v následující kapitole. Napřed uvedu čísla v jednotlivých oblastech platebního styku a vysvětlím jejich pravděpodobný důvod. Dále vzhledem k mé práci musím zmínit Screen Scraping, který v dnešní době používají aplikace třetích stran místo API, především zhodnotím rizika této metody. Zmíním také bezpečnostní regulace, kterým podléhají platební instituce vzhledem k praní špinavých peněz. Jako poslední zmíním bezpečnost samotného internetového bankovnictví a uvedu i sadu doporučení pro lepší bezpečnost, kterou by měly dodržovat banky. Nicméně hodí se i pro aplikace třetích stran.

1.4.1 Dopady na bezpečnost v číslech

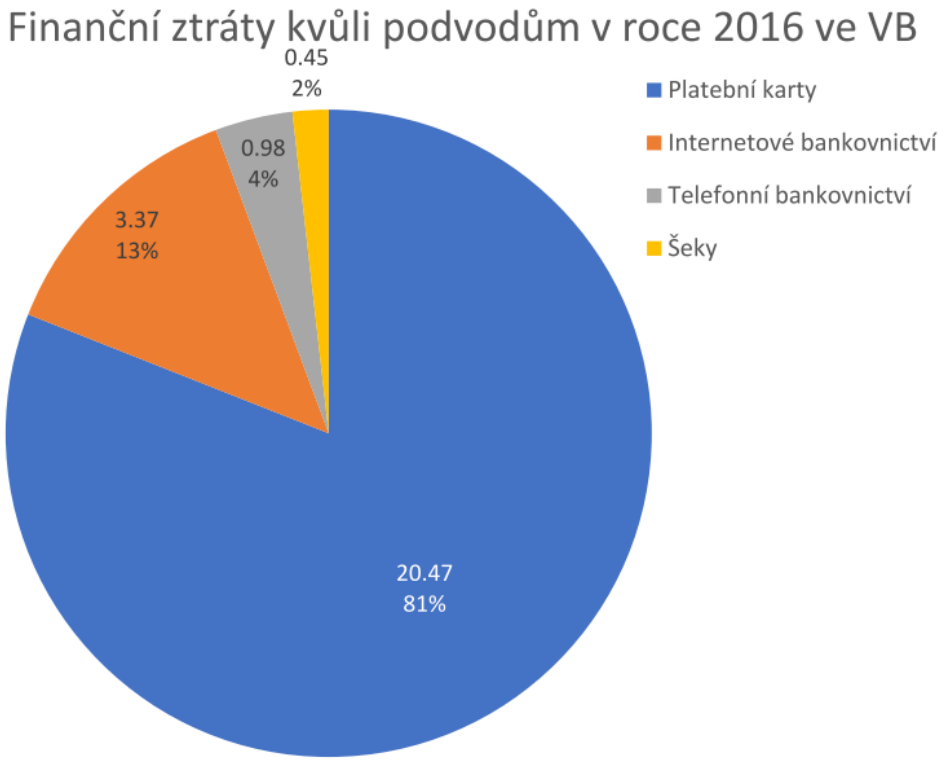
Pro ukázku dopadu na bezpečnost jsem vzal data z reportů společnosti Financial Fraud Action UK, konkrétně reportu z roku 2016.[5] Reporty mapují podvody na bankovním trhu ve Velké Británii (dále jen VB). Vzhledem k historii bankovnictví v kapitole 1.1, kde VB vedla v řadě technologických změn v bankovnictví, a vzhledem k faktu, že VB spadá do EHP, se VB hodí jako reprezentativní ukázka, jelikož trendy vyskytující se ve VB jsou následovány zpravidla postupně ve zbytku EHP.

Jak lze vidět na obrázku 1.8, k největším podvodům dochází přes platební karty, co se týče celkového objemu ukradených peněz. Rovněž do počtu identifikovaných případů zneužití, viz obrázek 1.9, vyhrávají dramaticky platební karty.

Nicméně u internetového bankovnictví dochází k odcizení větších částek v poměru na jeden podvod, v průměru 167 tisíc na jeden podvod oproti 11 tisícům na jeden podvod u platebních karet. Nepoměr vytváří zejména nastavené transakční limity, které bývají zpravidla mnohem větší u převodů peněz než u plateb kartou.

Největší nárůst nastal v oblasti CNP[11], kde počet zneužití karty z roku 2012, okolo 750 000 zneužití, narostl do roku 2016 na necelý dvojnásobek. O něco méně, ale také téměř dvojnásobek, narostl i objem ukradených peněz v oblasti CNP. Nárůst je pravděpodobně spojený s dramatickým rozšiřováním elektronického obchodování.

[11] CNP – Card Not Present, nebo-li platba kartou, kde držitel karty nemůže fyzicky nechat obchodníka kartu ověřit. Jedná se o opak POS.[71]

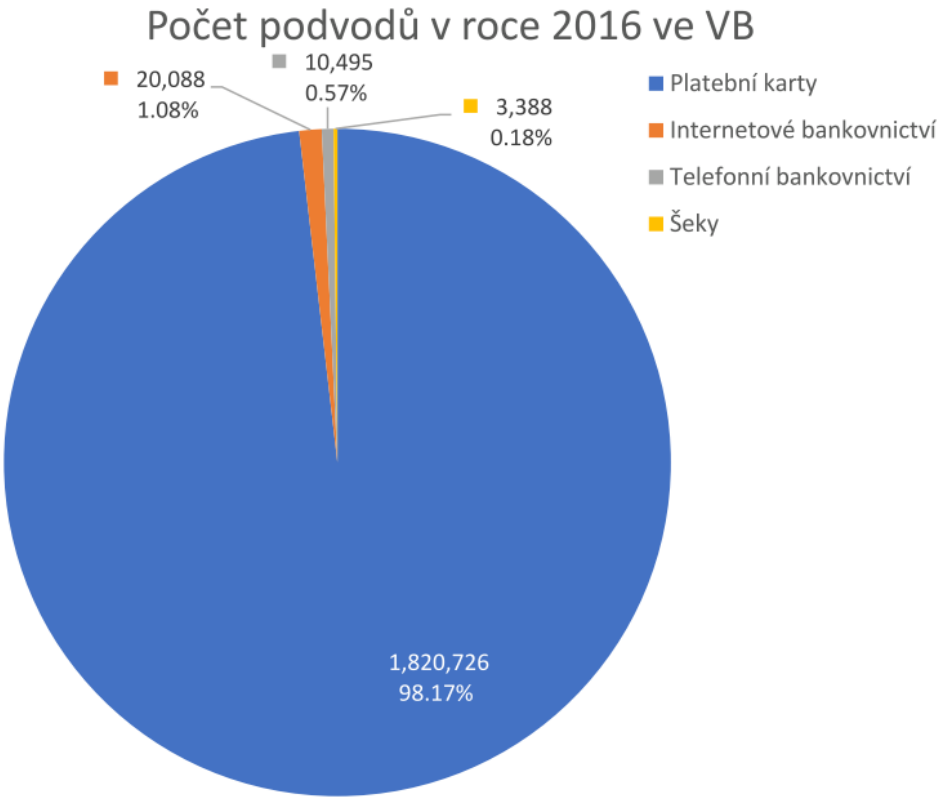


Čísla jsou v miliardách Kč vzhledem k průměrnému kurzu libry za rok 2016, který činil 33.121 Kč za 1 GBP.

Obrázek 1.8: Výše finančních ztrát kvůli podvodům v roce 2016 ve Velké Británii a jejich podíl vzhledem k typu zneužité technologie.[5]

Proč zneužití karty natolik převyšuje?

Vezmu-li dva nejčastější případy zneužití v celkovém podílu 91,7% – CNP a zneužití ztracené nebo ukradené karty – jedná se o zneužití primárně přes elektronické obchody. Na vině je proces platby přes elektronické obchody, který vyžaduje pouze jednofázové ověření zadáním čísla karty, jména držitele karty, datum ukončení platnosti karty a CVC kód na zadní straně karty. Veškeré tyto údaje jsou obsaženy na kartě, takže zloděje limituje v nakupování pouze nastavené limity na kartě, eventuálně nízký zůstatek na účtu. V poslední době se zavedla 3-D Secure technologie pro dvoufázové ověření plateb přes OTP vygenerované do emailu nebo SMS, nicméně ne všechny platební brány 3-D Secure, obzvláště v zemích mimo EHP, podporují. Dokud nebude pro všechny platební brány 3-D Secure povinný, problém se nezlepší. Nyní stačí pouze trochu vzdělanější zloděj.



Obrázek 1.9: Počet podvodů v roce 2016 ve Velké Británii a jejich podíl vzhledem k typu zneužité technologie.[5]

CNP *79%* Získání detailů karty na základě nevyžádaných mailů, telefonních hovorů nebo digitálních útoků ve formě malware a datových úniků. Následně zneužití detailů karty k CNP podvodnému obchodu, tedy elektronickému obchodu.

Zneužití ztracené nebo ukradené karty *12,7%* Zneužité karty, které byly nahlášeny držiteli karty jako ztracené nebo ukradené. Nejčastěji přes elektronický obchod nebo u obchodníků nepodporující EMW karty.

Padělek *6%* Týká se pouze kreditních karet s magnetickým pruhem, který lze snadno zkopírovat a použít například v jiné zemi, kde stále takový typ karet podporují. Detailněji jsem porovnal bezpečnost EMW karet vs. karty s magnetickým pruhem v kapitole 1.1.14.

Ukradení totožnosti *1,7%* Totožnost je využita k založení karty s osobními údaji ukradené totožnosti nebo k přihlášení účtu vázanému ke kartě.

Neobdržení karty *0,6%* Karta je zneužita dříve, než se dostane například poštou od vydavatele ke klientovi.

1.4.2 Screen Scraping

Screen Scraping automatizované programové užití webové stránky předstírající využití webové prohlížeče uživatelem. Slouží k získání dat nebo provádění operací, které by uživatel prováděl manuálně na dané webové stránce. Například portály agregující v ČR oblíbené slevy ze slevových portálů.

Nicméně u bankovních účtů potřebují od účtu přihlašovací údaje, aby mohly do bankovnictví přistoupit – například za účelem zjištění zůstatku uživatele nebo vytáhnutí transakční historie. Tím pádem třetí strana může vidět naprosto stejné data jako klient banky.

Screen Scraping je dnes preferovanou volbou pro FinTech aplikace kvůli:

- Absenci otevřeného API na straně bank.
- Není potřeba se nutně s bankou dohodnout na podmínkách. Stačí naučit algoritmus pracovat s obrazovkami bankovnictví dané banky.

Průkopníky jsou například společnosti jako SOFORT (platby), Trustly (platby), Yodlee (agregace účtů) nebo Mint.com (agregace účtů).

Bezpečnostní rizika Screen Scrapingu

Pro Screen Scraping je třeba, aby třetí strana ukládala přihlašovací údaje uživatele od jeho bank/y. Závisí tedy jakým způsobem, respektive jak bezpečně, třetí strana přihlašovací údaje ukládá. Může tím dojít k masivnímu úniku přihlašovacích údajů od tisíců klientů bank a jejich účtů.

Přihlašovací údaje jsou nutné pro přihlášení uživatele. To znamená, že v určitý moment musí být na serverové části aplikace třetí strany údaje uloženy v nešifrované podobě, aby je Screen Scraping mohl pro přihlášení využít, jelikož je zadává stejným způsobem jako uživatel. Může dojít k snadnému úniku přihlašovacích údajů například pouhým odposlechnutím.

Uživatelé se snadněji vystaví phishingu. Jelikož třetí strany využívající Screen Scraping aktuálně nepodléhají žádné regulaci, může se klient vystavit podvodným službám, které přihlašovací údaje pouze zneužijí.

Uživatelé nemohou nijak kontrolovat rozsah přístupu Screen Scrapingu. Jakmile má aplikace třetí strany přihlašovací údaje, může s účtem přes Screen Scraping dělat teoreticky cokoliv.

Uživatelé nemohou nijak kontrolovat délku období přístupu Screen Scrapingu. Jediná možnost je změnit si přihlašovací údaje v bance, pokud již dále uživatel nechce aplikaci třetí strany užívat a zároveň chce mít jistotu, že společnost si nebude uchovávat přihlašovací údaje od bankovního účtu nebo účtů uživatele.

Využívání aplikací na bázi Screen Scrapingu některé banky berou jako porušení smluvních podmínek. Může se stát, že uživatel ponese odpovědnost za jakýkoliv podvod s jeho účtem, ačkoliv podvod nemusí souviset s poskytnutím přihlašovacích údajů třetí straně.

Další nevýhodou Screen Scrapingu, nikoli ale bezpečnostní, je nutnost upravovat aplikaci při každé změně rozhraní podporované banky.[72]

1.4.3 Regulace proti praní špinavých peněz

Jeden z regulatorních bezpečnostních prvků zaměřených spíše na odhalování kriminality, než-li na bezpečnost klienta, je AML[12] framework správy:

- Řízení rolí a zodpovědností včetně rizik
  - Odhad rizika (podnik, klient, produkt, kanál, lokace)
  - Profilování rizik
  - Opakované hodnocení rizik
- Trénink výkonu personálu a jejich připravenosti
  - Screening klienta (sankce, PEPS, nežádoucí média a další)
  - Due dilligence klienta (včetně verifikace ID karty)
  - Analýza chování na základě monitoringu transakcí
  - Platební screening
- Držení záznamů, ochrana dat, management eskalace informací, schvalování SAR[13] kontrolních reportů.
  - Eskalace a schvalování
  - Vyplňování zpráv o podezřelých aktivitách
  - Management přijetí a odchodu klienta
  - Reportování

Součástí AML je KYC[14], který zastřešuje odhadování rizik klienta, screening, due dilligence a monitoring transakcí.[73]

[12] AML – Anti-Money Laundering, nebo-li opatření proti praní špinavých peněz.

[13] SAR – Zkratka pro anglický termín Suspicious Activity Report, nebo-li zpráva o podezřelých aktivitách.

[14] KYC – Know Your Customer, nebo-li znát svého zákazníka.

1.4.4 Bezpečnost internetového bankovnictví a online plateb

Mezi nejčastější podvody v online bankovnictví patří zneužití platební karty. Podvodů s internetovým bankovnictvím je výrazně méně. Útoky nemusí být vždy motivovány získáním peněz. Může se jednat například o DDoS útoky za účelem shození serveru banky, aby internetové bankovnictví nebylo dostupné. V následujících odstavcích uvádím nejčastější uživatelské chyby a možná opatření jak na straně uživatele, tak na straně banky. Nicméně opatření na straně serveru se netýkají jenom pro banku. Stačí si vzpomenout na kauzu hromadného úniku údajů o platebních kartách uživatelů PlayStationu, Xboxu a Amazonu v roce 2014.[74]

Chyby uživatele

Chyby, kterých se může dopustit uživatel při přihlašování do internetového bankovnictví nebo při vyplňování údajů karty například do platební brány při nákupu[75]:

- Zadání dat na falešnou stránku.
  - Kliknutím na odkaz v phishing e-mailu.
  - Překliknutím při psaní URL banky.
  - Přesměrování při používání nezabezpečeného připojení. Nejvíce nebezpečná je veřejná Wi-Fi.
- Používání zavirovaného zařízení. Škodlivé programy mohou:
  - Přesměrovat uživatele na phishing stránku.
  - Ukrást hesla a čísla karet uložených v zařízení.
  - Zachytit výměnu informací mezi bankou a uživatelem.
- Zachycení psaní uživatele na klávesnici.
  - Speciální malwary, které mohou zachytit, co uživatel píše.

Opatření uživatele

Opatření, které by uživatel měl provádět pro snížení rizika možného zneužití přihlašovacích údajů nebo údajů z karty[75]:

- Kontrola důvěryhodnosti stránek, zejména kontrola URL adresy.
- Používání důvěryhodného prostředí, zejména privátních sítí uživatele – domácí síť nebo mobilní internet.
- Používání důvěryhodného připojení, zejména kontrola použitého šifrování webových stránek banky a platnosti certifikátu.

- Chránění vstupu, buď zabezpečenou klávesnicí nebo eventuálně virtuální klávesnicí.

Opatření banky

Aby nedošlo například ke kompromitaci webových stránek internetového bankovnictví, používá se několik faktorů[76][77]:

- Zabezpečená komunikace přes HTTPS společně s protokolem SSL.
- Části z AML frameworku pro odhalení podezřelého chování, například přihlášení z dvou různých zemí během nemožného časového horizontu nebo napojení na FraudNet^{TM}.
- Firewally.
- Automatické odhlašování.
- Softwary aktualizované na poslední verze.
- Pravidelná změna hesel pro zaměstnance i klienty.
- OTP[15] verifikace veškerých převodů peněz, například pomocí OTP zaslaného přes SMS.
- OTP verifikace některých plateb kartami pomocí 3-D Secure, opět například pomocí OTP zaslaného přes SMS. Nicméně zde závisí na platební bráně. Ne všude je 3-D Secure podporován.
- Identifikace klienta přes telefon u větších transakcí.
- Dvoufázové nebo vícefázové ověření, ať už při přihlášení nebo provádění plateb, například při přihlašování do internetového bankovnictví vyplněním OTP z mobilní aplikace banky.

1.4.5 Bezpečnost u POS plateb

Bezpečnost u POS[16] plateb kartou je odlišná od bezpečnosti při placení kartou na internetu (CNP), proto ji uvádím zvlášť.

Bezpečnost platebních karet

Bezpečnost kreditních a debetních karet jsem již nastínil v historii bankovnictví v kapitole 1.1.14. Zkráceně řečeno podvod u POS plateb s EMW kartami je téměř nemožný, jelikož komunikace mezi čipem a termínálem probíhá šifrovaně a použité RFID čipy mají dosah okolo 4 cm.

[15] OTP – One-time password, nebo-li jednorázové heslo.

[16] POS – Zkratka pro Point-of-sale, nebo-li fyzické místo, kde proběhne platba mezi zákazníkem a obchodníkem.[78]

Bezpečnost placení mobilem

Obdobně je na tom placení s mobilem, kde na obou stranách je NFC s dosahem okolo 10 cm. Komunikace opět probíhá šifrovaně.

1.5 Shrnutí bankovního trhu

Bankovní trh je velmi starý a obzvláště s příchodem technologií se velmi změnil. Pro dnešní bankovní trh jsou nepostradatelné centrální banky a jejich clearingové systémy. Pro banky jsou zase nepostradatelné mainframy pro dávkové zpracování plateb. Z těchto důvodů je systém plateb velmi ovlivněný a je nutné při navrhování systémů na to brát zřetel, jelikož PSD2 umožňuje platby pouze inicializovat, a proto je celý proces závislý na systémech na pozadí – více ale až v nadcházející kapitole.

Pro platby minimálně v Evropě je standardní platit EMW kartami nebo mobilem. Pro komunikaci mezi systémy se používá ISO 20022 standard. FinTech společnosti s platbami nebo agregacemi informací jsou s námi již minimálně od roku 2000. Dnes už jsou tak rozšířené, že se dělí na spousty kategorií. Mě budou zajímat primárně kategorie „platby a převody peněz“ a „poradenství a osobní finance“, jelikož PSD2 má na ně největší dopad, viz následující kapitola.

Bankovní trh v ČR se hodně rozděluje podle zaměření banky na typ klientely a jejich tržní podíl je dost rozdrobený až na tři tradiční banky ČS, ČSOB a KB.

S dobou se změnilo i vnímání bezpečnosti, které je oproti minulosti velmi odlišné a vyžaduje nejenom IT specialisty na straně finančních institucí, ale digitální gramotnost na straně klientů. K největší podvodům dochází u platebních karet. Screen scraping, který je využívaný dnešními FinTech aplikacemi, je bezpečnostní hrozbou.

Kapitola 2

Směrnice PSD2

Jelikož se nejedná o první směrnici v pořadí v oblasti plateb od Evropské unie, uvedu pro lepší kontext PSD a SEPA platby – směrnice, které přišly před PSD2 a z kterých PSD2 vychází.

V samotné PSD2 se zaměřím na časování, jelikož v době psaní mé DP nejsou veškeré záležitosti okolo směrnice dořešené, schválené a finální. Je proto nutné brát na zřetel, že realita se od textu již může lišit. Dále vymezím cíle PSD2, které reagují zejména na bezpečností hrozby popsané v kapitole 1.4, ovlivněné stávající role a role nové – AISP a PISP. Práci jsem před odevzdáním aktualizoval i o čerstvě schválenou regulaci technologických standardů (RTS). Popíši rámcově jakým způsobem je možné získat licenci u ČNB potřebnou k provozování služeb obsažených v PSD2. Na závěr zhodnotím dopad na bankovní trh, zejména vzhledem k bankám v ČR, které jsem uvedl v kapitole 1.3.3.

2.1 PSD1

PSD1 nebo-li Payment Services Directive (Směrnice o platebních službách) je předchůdcem PSD2. Směrnici PSD1, z které vycházím v textu, můžete nalézt na stránkách EUR-Lex[79]. Přijata byla v roce 2007 a následně v roce 2009 zavedena.

Cílem směrnice je efektivní trh pro platební služby v rámci Evropy, zejména:

- stejná pravidla pro celou EU
- jasné informace o platbách
- rychlé platby
- ochrana zákazníka
- široká nabídka platebních služeb

Cílem EU je zajistit jednotný platební prostor, kde občané a podniky mohou provádět platby napříč státy stejně snadno jako ve svém vlastním státě, včetně poplatků.

Směrnice o platebních službách nastavila stejná pravidla pro platby napříč Evropským hospodářským prostorem.[17] Zahrnuje veškeré elektronické bezhotovostní platby jako:

- převody
- inkasa
- platby kartou
- mobilní a online platby

Směrnice rovněž položila základy pro SEPA platby.

2.2 SEPA

SEPA nebo-li Single Euro Payments Area (Jednotná oblast pro platby v eurech) zajišťuje rychlé bezhotovostní platby napříč Evropou, viz obrázek 2.1, mezi bankovními účty pro občany, byznys a veřejnou správu, se stejnými podmínkami bez ohledu na to, kde se nachází. Konkrétně se jedná o následující platby:

- převody (SCT - SEPA Credit Transfer, ukázka na obrázku 2.2)
- inkasa (SDD - SEPA Direct Debit, tedy inkasní platba)
- platby kartou

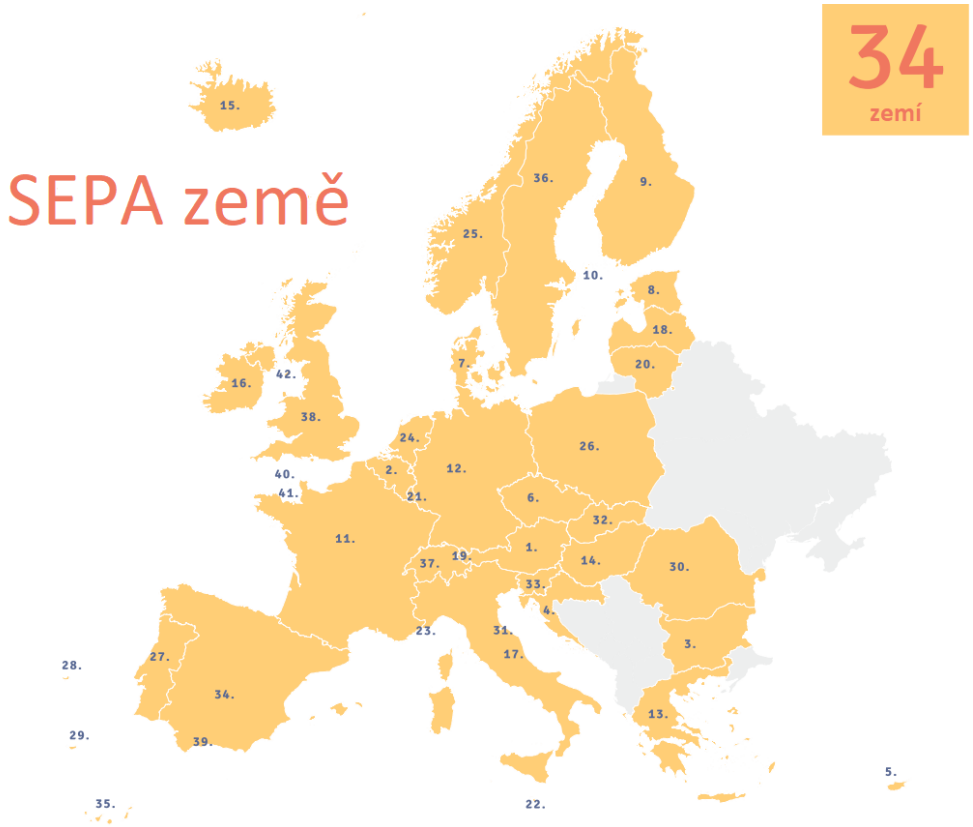
SEPA dále umožňuje používat svůj domácí účet v jiných zemích Evropy například pro mzdové příjmy nebo placení účtů.[81]

2.2.1 Technický detail SEPA SCT

1. Zboží/služba poskytnutá příjemcem původci.
2. SCT instrukce poslaná přes kanál a formát nastavený mezi bankou a původcem.
3. SCT instrukce zkontrolována a ověřena včetně BIC a IBAN.

[17] Evropský hospodářský prostor, zkráceně EHP (anglicky EEA - European Economic Area), platí od roku 1994. Cílem dohody je jednotný trh. Zaručuje tedy svobodu pohybu zboží, osob, služeb a kapitálu. Kromě členských států EU jsou součástí i Island, Lichtenštejnsko a Norsko.[80]

[18] Přeloženo a překresleno autorem ze zdroje.[82]

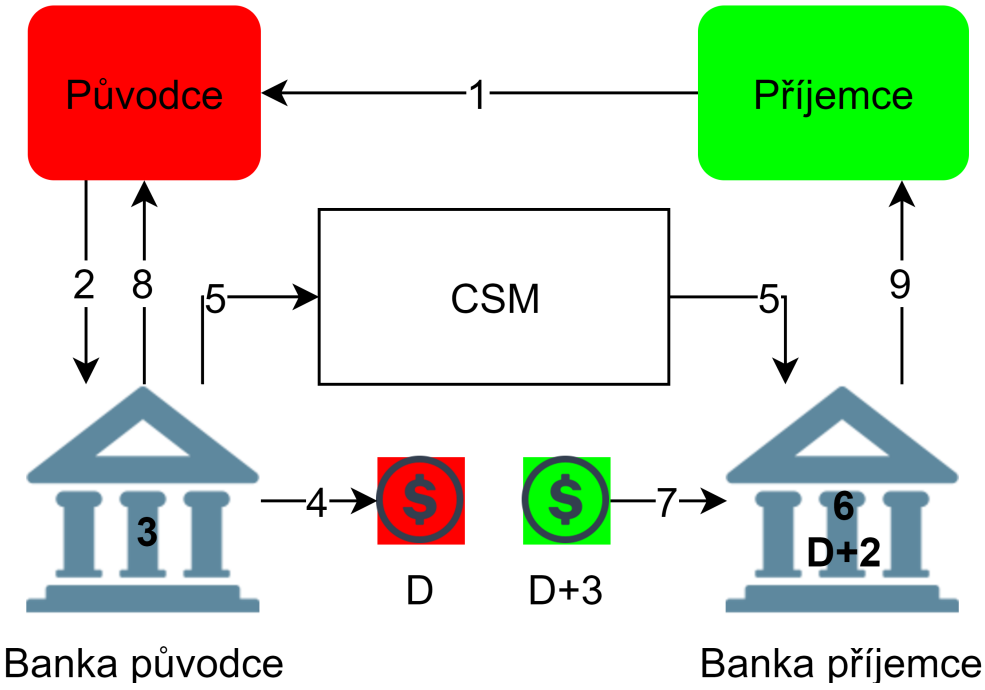


Obrázek 2.1: Mapa zemí spadající pod SEPA.[6]

4. Z účtu původce se odepíšou peníze dnem uzavření, respektive dnem splatnosti (D).
5. SCT se odešle přes CSM[19] využívající UNIFI (ISO 20022)[20] XML standardizovanou zprávu.
6. SCT přijme banka příjemce ke dni vypořádání (max. D+2) a zkontroluje ji.
7. Částka je příjemci připsána na účet max. D+3.
8. Předání informace o výsledku v nastaveném formátu mezi bankou a původcem.
9. Předání informace o výsledku v nastaveném formátu mezi bankou a příjemcem.

[19] Anglická zkratka pro „Clearing and Settlement Mechanisms“. Clearingové mechanismy vysvětluji v kapitole 1.2.6.

[20] Univerzální schéma zpráv na finančním trhu, které vysvětluji v kapitole 1.2.10.



Obrázek 2.2: Diagram SEPA převodu (SCT).[18]

Z obrázku vyplývá, že platba by měla být provedena podle směrnice do čtyř pracovních dnů, nicméně od roku 2012 by převod neměl trvat déle jak do druhého pracovního dne v závislosti, kdy je platba v daném dni zadána kvůli clearingovým institucím (1.2.6) a dávkovému zpracování (1.2.8). Další důležité vlastnosti převodu:

- Na transakce není stanoven limit, určují si ho banky samy.
- Poplatky musí být účtovány zvlášť a nesmí vycházet z převáděné částky.
- Transakce jsou prováděny v eurech, ale banka původce a příjemce může být v jiné měně (nicméně schéma nijak nepokrývá převod měny).[82]

2.2.2 Okamžité SEPA platby

Okamžité SEPA platby byly uvedeny do provozu v roce 2017 a jsou postavené na SCT schématu na obrázku 2.2. Jejich hlavní funkcí a výhodou je převod peněz do 10 vteřin na 24/7/365 bázi. Limit převáděné částky je 15 000 EUR. Zpoplatnění za platbu je čistě na bankách.[83]

2.3 PSD2

Stěžejní zkratky pro následující text:

- RTS – Regulatory Technical Standards – Regulační technické standardy
- SCA – Strong Customer Authentication – Silné ověření zákazníka
- CSC – Common and Secure open standards of Communication – Běžné a zabezpečené otevřené komunikační standardy
- PSD2 – Payment Services Directive 2 – Směrnice o platebních službách 2
- EBA – European Banking Authority – Evropský orgánu pro bankovnictví

PSD 2 je pokračovatelem PSD1. Součástí je RTS, v němž je nejdůležitější CSC a SCA.

2.3.1 Časování PSD2

- 24. července **2013** – Evropská komise zveřejnila návrh PSD2.
- Podzim **2015** – Schválení PSD2 Evropským parlamentem a následně Evropskou komisí.
- 23. prosince **2015** – PSD2 byla oficiálně zveřejněna.
- 12. ledna **2016** – PSD2 vstoupila v platnost.
- Srpen až říjen **2016** – EBA konzultovala návrh RTS na SCA a CSC.
- 23. února **2017** – EBA zveřejnila finální návrh RTS na SCA a CSC.
- 27. listopadu **2017** – Evropská komise přijala RTS na SCA a CSC. Evropský parlament a Evropská rada má tři měsíce na vyjádření.
- V průběhu roku **2017** – EBA připravovala RTS podklady pro implementaci PSD2.
- 13. ledna **2018** – Finální termín pro začlenění PSD2 do zákonů členských států Evropské unie.
- Kolem září **2019** – 18 měsíců po přijetí a zveřejnění finální verze přijde RTS na SCA a CSC v platnost.

Jak lze vidět, některé části jsou relativně čerstvé a můžou se tedy v mém textu lišit od reality vzhledem k době, kdy jsem text psal. Například finální podoba RTS byla zveřejněna teprve v březnu.[84]

Klíčový je termín v září roku 2019, kdy stávající finanční instituce a poskytovatelé platebních služeb již musí dodržovat věci zavedené v RTS. Do té doby nelze očekávat velké dopadu na trh díky PSD2.

2.3.2 Hlavní cíle PSD2

- Zajistit jednodušší a bezpečnější internetové platební služby.
- Lépe chránit spotřebitele proti podvodům, zneužívání a problémy s platbami.
- Podpořit inovativní mobilní a internetové platební služby.
- Posílit spotřebitelská práva.
- Posílit úlohu EBA s cílem koordinovat orgány dohledu návrhy technických norem.

Směrnice je součástí legislativního balíčku, který rovněž zahrnuje regulaci vícestranných mezibankovních poplatků.[21]

2.3.3 Role ovlivněné směrnicí

Pro lepší představu lze nalézt jednotlivé role a jejich návaznosti i na obrázku 2.3. PISP a AISP role jsou právě díky PSD2 přístupné pro TTP.

TTP Third Party Payment Service Providers (třetí strana poskytující platební služby) – Třetí strany získávající přístup k platebním účtům na základě souhlasu klienta. Žádným způsobem se nestanou vlastníky účtů klientů ani jejich prostředků, či převáděných částek.

ASPSP Account Servicing Payment Service Providers (správce účtu poskytující platební služby) – Jedná se o tradiční finanční instituce (například banky), které poskytují účty klientům, z kterých nebo na které může klient provádět platby.

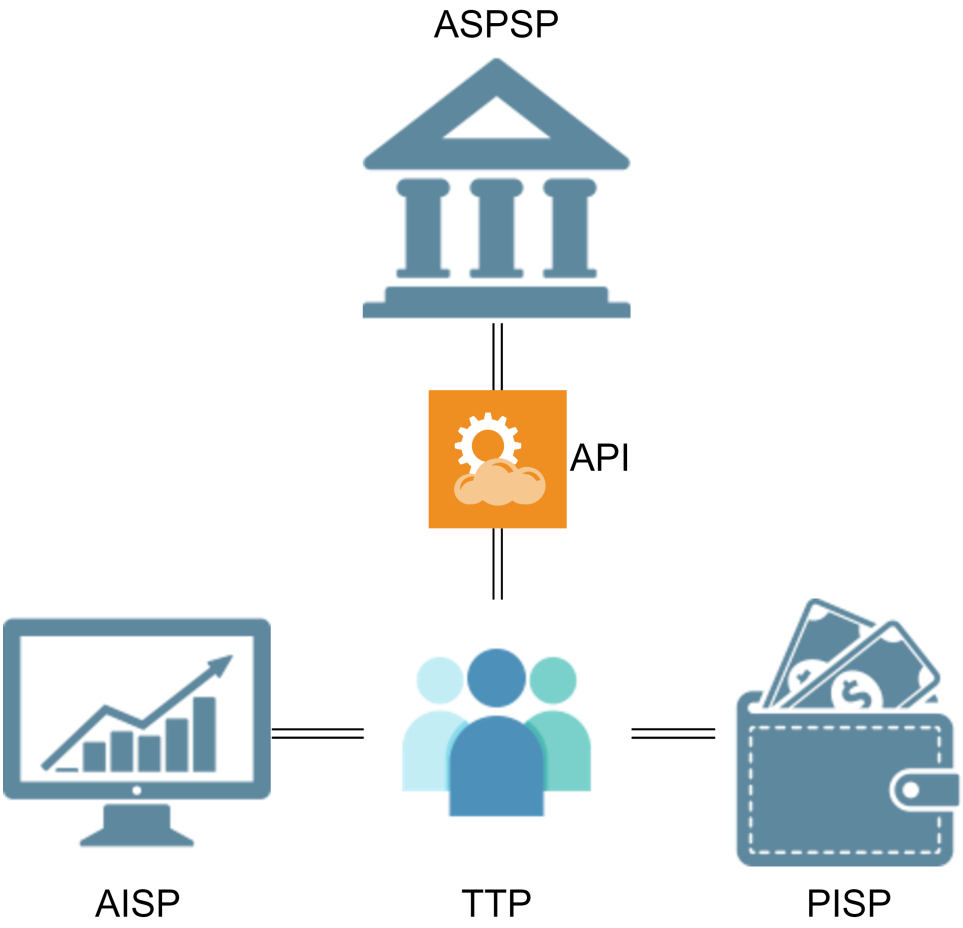
PISP Payment Initiation Service Providers (poskytovatel platebních inicializačních služeb) – Inicializuje platby na základě požadavku klienta (majitele účtu).

AISP Account Information Service Providers (poskytoval informačních služeb o účtu) – Bude mít přístup k informacím o účtu poskytnutých od ASPSP (tedy bank) na základě souhlasu klienta (majitele účtu).

PSU Payment Service User (uživatel platebních služeb) – Zákazník nebo obchodník využívající platební služby poskytované třetími stranami nebo finančními institucemi.

[21] Tato regulace například znemožňuje obchodníkům zákazníkovi účtovat poplatky navíc za platbu kartou namísto platby v hotovosti. Rovněž stanovuje limity na poplatky za transakci debetní a kreditní kartou, které může poskytovatel platebních služeb účtovat obchodníkům. Více lze nalézt přímo v „Nařízení Evropského parlamentu a rady (EU) 2015/751 ze dne 29. dubna 2015 o mezibankovních poplatcích za karetní platební transakce.“[85]

[22] Obrázek vytvořený autorem vycházející ze STET PSD2 API dokumentace.[86]



Obrázek 2.3: Přehled rolí ovlivněných směrnicí PSD2.[22]

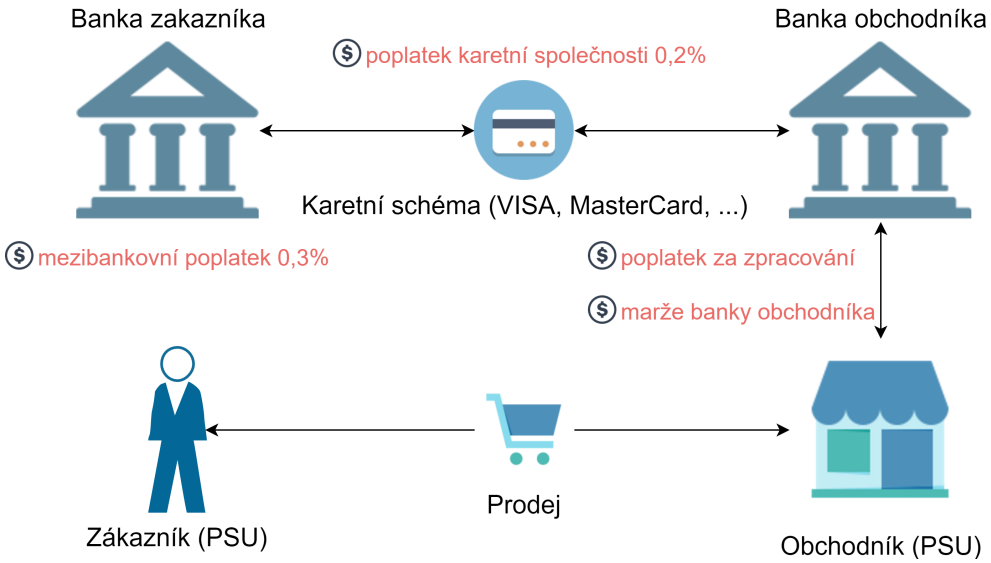
2.3.4 PISP

Abych mohl představit PISP, tak je potřeba uvést PISP do kontextu současných řešení na trhu. V současné době můžete platit u obchodníků různými způsoby, nicméně platba kartou je jeden z nejrozšířenějších způsobů (viz 1.2.7), a proto srovnání uvádím mezi PISP a platebními kartami.

Platba platební kartou

Platba kartou se skládá z několika částí skrytých zákazníkovi. Každá část je většinou spjata s poplatky (viz obrázek 2.4). Karty (VISA, VISA Electron, V Pay, MasterCard a Meastro) vydané v EHP jsou **regulované** nařízením Evropského parlamentu a Rady EU 2015/751.[85] Ostatní karty jsou **neregulované**. Regulace stanovuje maximální výši **mezibankovního poplatku** na 0,3% a **poplatku karetní společnosti** na 0,2% (u kreditní karty je ma-

ximální výše 0,3%). Ostatní poplatky, jako **poplatek za zpracování**, **marže banky obchodníka** a další, jsou neregulované. Finální výše je tedy různá a závisí primárně na smlouvě mezi obchodníkem a bankou. Například u GoPay platební brány poplatek přesahuje 2% + 3 Kč za každou transakci v závislosti na typu karty.[87]



Obrázek 2.4: Současný platební model využívající například karty.[23]

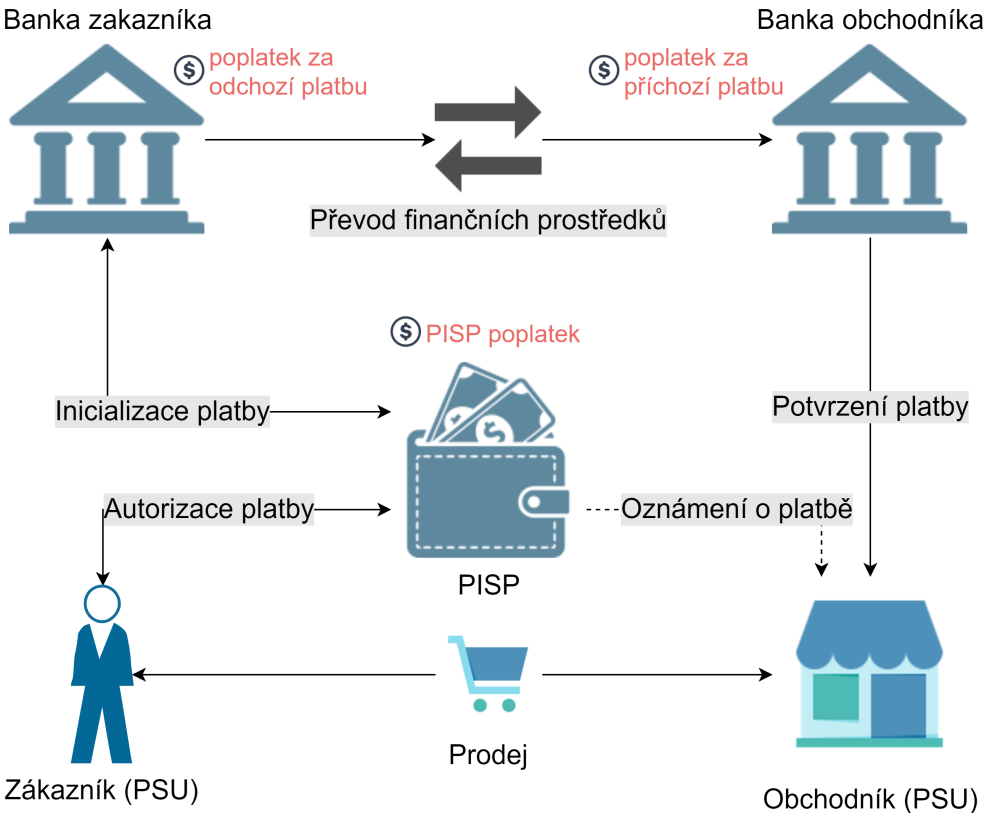
PISP versus současná řešení

Jak lze na obrázku 2.5 vidět, PISP řešení vynechává veškeré prostředníky a přes API banky zákazníka provede klasický převod finančních prostředků. Tím odpadají i veškeré poplatky, kromě poplatků u poskytovatele PISP a případně poplatků za odchozí a příchozí platbu, které ale bývají v dnešní době u většiny bank nulové. PISP tak samozřejmě může mít dopad na příjmy nejenom karetních společností, ale i bank.[87]

Klíčové požadavky na PISP určené směrnicí PSD2

- Mít PISP licenci v domovské zemi a mít práva na přeshraniční činnost v ostatních zemí EHP.
- Nedržet v žádném okamžiku peníze plátce. Pouze inicializovat platby.
- Bezpečnostní pověření uživatelů jsou přenášené přes zabezpečené a efektivní kanály a nejsou dostupné jiným stranám.

[23] Obrázek vytvořený autorem vycházející z materiálů firmy Accenture[88] a GoPay[87].
[24] Obrázek vytvořený autorem vycházející z materiálů firmy Ernst & Young.[89]



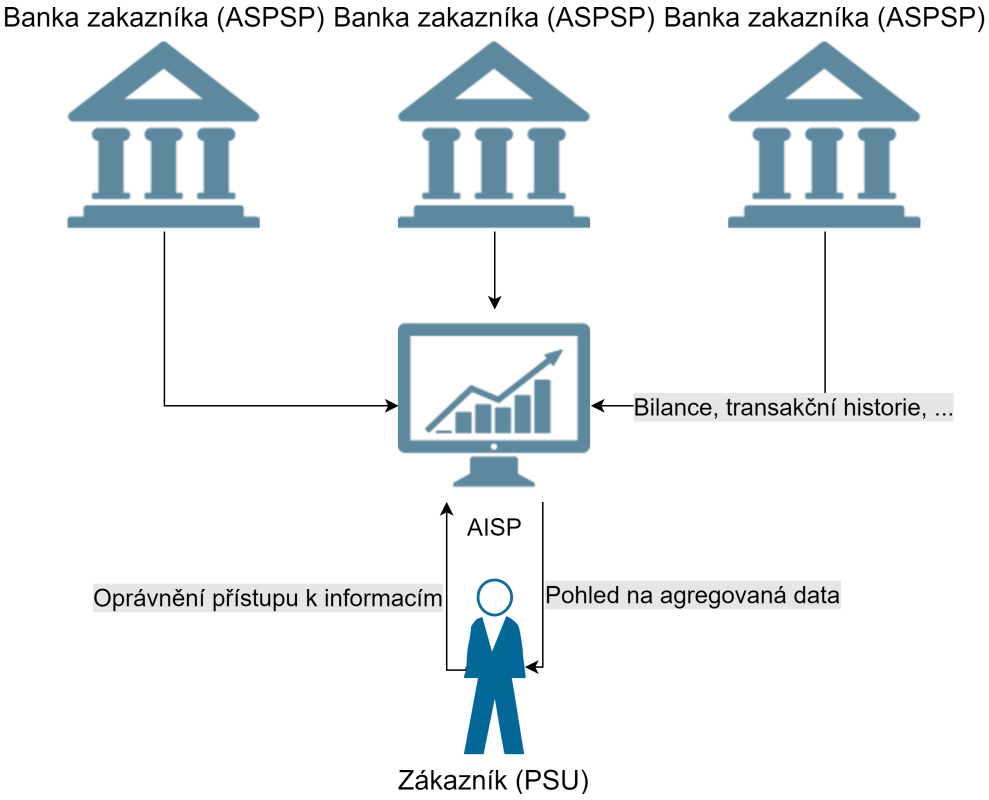
Obrázek 2.5: Platební model využívající PISP zavedený směrnicí PSD2.[24]

- Jakékoliv informace o plátci získané při provádění platby jsou dostupné pouze příjemci a to pouze s výslovným souhlasem plátce.
- Komunikace mezi jednotlivými stranami probíhá zabezpečeně.
- Neukládat citlivá data plátce o platbě.
- Vyžadovat po plátci pouze data nutná k provedení platby.
- Nepoužívat, nepřistupovat, ani neukládat získaná data pro jiné účely než k platebním inicializačním službám.
- Neupravovat částku platby, příjemce, ani jiné vlastnosti platby.[90]

2.3.5 AISP

AISP poskytuje zákazníkovi detaily k transakcím, bilanci a přístup k informacím o účtu na základě jeho souhlasu a to napříč všemi bankami v EHP, kde má zákazník účet, opět s využitím API (2.3). Jak lze vidět na obrázku 2.6,

AISP zde funguje jako agregátor dat poskytující zákazníkovi pohled na více účtů na jednom místě přes jeden portál.



Obrázek 2.6: Vazby u poskytovatele informací (AISP) o účtu zákazníka (PSU).[25]

Klíčové požadavky na AISP určené směrnicí PSD2

- Mít AISP licenci v domovské zemi a mít práva na přeshraniční činnost v ostatních zemí EHP.
- Poskytovat služby pouze na základě výslovného souhlasu uživatele.
- Bezpečnostní pověření uživatelů jsou přenášené přes zabezpečené a efektivní kanály a nejsou dostupné jiným stranám.
- Identifikovat se při každé relaci ASPSP (bankám) uživatele a komunikovat vždy zabezpečeně jak s ASPSP, tak uživatelem.
- Přistupovat pouze k informacím z určených platebních účtů a souvisejících platebních transakcí.

[25] Obrázek vytvořený autorem vycházející z materiálů firmy Ernst & Young.[89]

- Nevyžadovat citlivá platební data spojená s platebními účty.
- Nepoužívat, nepřistupovat, ani neukládat získaná data pro jiné účely než k poskytování informačních služeb o účtech požadovaných uživatelem a v souladu s pravidly ochrany dat.[90]

2.3.6 RTS – technický pohled

RTS – regulace, která by měla definovat technické standardy, popisuje tyto standardy hodně obecným způsobem. Regulace tedy neříká, jaké technologie by se měly pro zabezpečení nebo rozhraní použít. Technologické záležitosti nechává v zodpovědnosti bank.

V obecných technických standardech ale popisují následující:

API, nikoliv screen scraping Jakmile vstoupí v platnost RTS SCA, měl by být zakázaný screen scraping, který jsem popsal v kapitole 1.4.2. Veškerý přístup třetích stran do banky bude přes API.

Přihlášení přes banku Přihlášení k účtu klienta banky musí vždy proběhnout přes rozhraní klientovy banky. Tím banka může dostát své zodpovědnosti a bezpečnost bude záležet čistě na technologiích banky zajišťující bezpečnost.

Dvoufázové SCA Pro veškeré elektronické transakce, kde alespoň jedna strana se nachází v EHP, bude nutné použít alespoň dva následující bezpečnostní kroky:

- Něco, co uživatel **zná** – heslo, PIN, atd.
- Něco, co uživatel **vlastní** – karta, telefon, atd.
- Něco, co uživatel **je** – otisk prstu, rozpoznání obličeje, atd.
- Pro CNP transakce ještě unikátní ověřovací kód spárovaný s konkrétní transakcí a uživatelem.

Pro zachování dostatečné plynulosti plateb tvoří výjimku následující typy plateb:

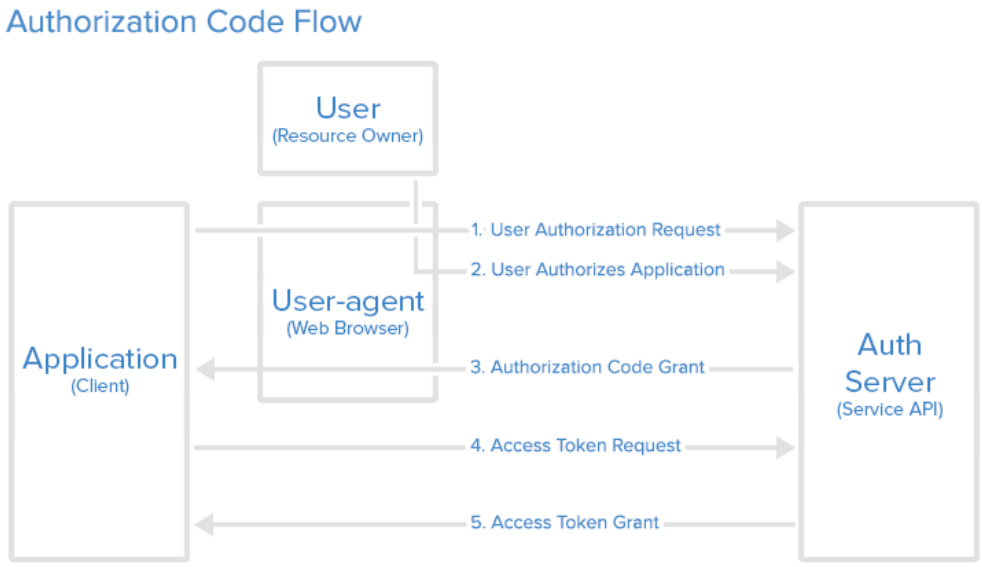
- CNP platby do částky 30 EUR, pokud nebylo provedeno již 5 plateb nebo překročeno celkově 100 EUR za den.
- Bezkontaktní platby kartou do 50 EUR, pokud nebylo provedeno již 5 plateb nebo překročeno celkově 150 EUR za den.
- Bezobslužné terminály pro dopravní a parkovací poplatky.
- Online transakce vůči ověřenému příjemci identifikovaného plátcem.

- Korporátní platby, pokud jsou použity určené platební procesy a protokoly splňující bezpečnost pro státní autority.
- Pokud míra podvodů je přes platební službu nižší než stanovené limity.

Pro přístup na účty za účelem AISP se má SCA aplikovat pouze při prvním přístupu k účtu a pak každých dalších 90 dní.[91][92]

Ověření přes OAuth 2

Při průzkumu dokumentací bank, které již v ČR API mají, jsem vypozoroval, že pro účely ověření uživatele a komunikace s aplikací třetí strany používají OAuth 2 ověřovací framework, a proto zde princip OAuth 2 více rozvedu.



Obrázek 2.7: Proces ověření pomocí frameworku OAuth2.[93]

1. Aplikace přesměruje uživatele na webové stránky poskytující API, v případě PSD2 na stránky banky.
2. Uživatel se na webových stránkách poskytující API přihlásí a následně potvrdí aplikací požadovaná oprávnění, v případě PSD2 se přihlásí do banky a potvrdí PISP, AISP nebo oboje.
3. Aplikace od poskytovatele API obdrží autorizační kód.
4. Na základě autorizačního kódu požádá poskytovatele API o přístupový token.

5. Aplikace obdrží přístupový a obnovovací token, v případě PSD2 obnovovací token musí mít platnost maximálně 90 dní, viz předchozí kapitola 2.3.6.[93]

2.3.7 Zažádání o licenci u ČNB

Každá společnost, která chce využívat přes svojí aplikaci otevřené API bank, musí zažádat o licenci u ČNB, respektive o povolení k činnosti. Žádost se liší podle toho, jestli společnost chce provozovat PISP nebo AISP. Veškeré podklady k licencím, z kterých v této kapitole vycházím, lze najít v zákoně 370/2017 Sb.[94] Vyjmenovávám ty nejdůležitější body, necituji celý zákon. Pro žádost o licenci je tedy nutné určitě záležitost konzultovat s právníkem. První uvedu žádost o AISP, jelikož obsahuje méně bodů jak žádost o PISP, u které doplním pouze rozdíly.

Žádost o AISP

Znění zákona lze najít v 370/2017 Sb., hlava 3, správce informací o platebním účtu.

Žadatel musí splňovat následující:

- Musí mít sídlo v ČR.
- Musí mít obchodní plán včetně předpokládaného rozpočtu na první 3 účetní období, který musí být podložen reálnými ekonomickými propočty.
- Musí mít zařízené pojištění pokrývající činnost společnosti.
- Měl by mít vhodné věcné, technické, personální a organizační předpoklady.
- Řídící a kontrolní systém splňuje požadavky zákona č. 370/2017 Sb.
- Vedoucí osoby jsou důvěryhodné a odborně způsobilé v oblasti AISP.
- Smí provozovat živnost.

Žádost lze podat pouze elektronicky a ČNB má na rozhodnutí po zahájení řízení lhůtu 3 měsíců.

Žádost o PISP

Znění zákona lze najít v 370/2017 Sb., hlava 2, platební instituce.

Oblast PISP spadá pod licenci platební instituce, takže se nejedná o nový proces. Od AISP licence, která má mírnější podmínky, se liší zejména v následujících bodech:

- Nemůže se jednat o fyzickou osobu, povoleny jsou pouze právnické osoby.
- Musí mít počáteční kapitál ve výši 20 000 EUR za předpokladu, že platby pouze inicializuje, tedy v žádném čase převáděnou částkou nedisponuje.
- Musí v ČR provozovat alespoň část svého podnikání.

2.3.8 Dopad na bankovní trh

V závislosti na přístupu vzhledem k PSD2 můžeme banky rozdělit na dva typy - reaktivní a proaktivní.

Reaktivní Banky, které čekají na finální verzi technických standardů regulace. Poté teprve zahájí rychlou implementaci hlavně za účelem splnění směrnice. Tímto banky riskují, že konkurence získá značnou výhodu a banka se stane pouze infrastrukturním zázemím, tedy ztratí kontakt s klientem, na základě kterého mu poskytuje například své další produkty.[95]

Proaktivní Banky, které API již mají nebo vyvíjí dříve, než přijde v platnost RTS. Jakožto první na trhu a bez dostatečných podkladů ze strany EBA musí banky dostatečně prověřit a analyzovat svoji architekturu systémů, ujistit se, že je jejich architektura skutečně orientovaná na služby a připravená pro rostoucí byznys.[95] Rovněž tím získávají výhodu, jelikož můžou sami mezi prvními nabízet vlastní PISP a AISP řešení a být připraveni na integraci jiných bank do takto svých vytvořených aplikací (CREDITAS, Česká spořitelna – viz níže). Další možností proaktivního přístupu je nabídnout API k dalším službám nad rámec PSD2, který může být například zpoplatněn nebo poskytuje zpětnou výhodu pro jejich byznys (Air Bank – viz níže).[88]

Nejenom přehled proaktivních a reaktivních bank lze nalézt v tabulce 2.1, přičemž každá banka se ujala proaktivnosti trochu jiným způsobem:[26]

Fio banka Jejich výhoda je, že API mají implementované už od roku 2012, tedy ještě dříve, než vůbec směrnice PSD2 vznikla. Náklady na přizpůsobení se směrnici budou tedy mnohem menší.

Česká spořitelna Ta se do API pustila na českém trhu nejvíce. Pro vývojáře nabízí sandbox[27] a reálný vývoj v testovacím prostředí, což značně usnadňuje tvorbu aplikací spolupracující zejména s Českou spořitelnou. Navíc sama Česká spořitelna díky této strategii navazuje řadu spolupráce

[26] Novinky do ledna 2018 včetně, z kterých lze posoudit strategii jednotlivých bank a jejich proaktivní přístup k PSD2 a API.

[27] Sandbox nebo-li pískoviště je oddělené (virtuální) vývojové prostředí od ostatních systémů, kde mohou vývojáři vytvářet a testovat nový obsah.

s FinTech firmami a přichází i s vlastními aplikacemi využívající jejich API, například Friends 24, George, rychlý výpis[28]. Od května 2018 navíc plánuje ve svém internetovém bankovnictví možnost spravovat i účty jiných bank.

Banka CREDITAS Kromě faktu, že rovněž nabízí API, jsou první bankou v ČR, která nabízí od 15. 1. 2018 AISP a PISP zároveň, jelikož integrovala do svého internetového bankovnictví účty jiných bank, konkrétně zatím FIO banky.[96]

Air Bank Již nabízí API, nicméně pouze pro vybrané partnery, s kterými je banka v úzké spolupráci, údajně kvůli testování svého API. Nabízí API pro veřejně dostupná data – umístění bankomatů banky, otevírací dobu poboček a aktuální kurzovní lístek a poté API vzhledem k směrnici PSD2, tedy klientská data.[97]

Jak je vidět v tabulce 2.1, většina bank vyčkává buď na specifikaci RTS (březen 2018, viz časování v kapitole 2.3.1), takže spustí otevřené API v Q1 nebo Q2, nebo čekají, až přijde RTS v platnost (září 2019, opět viz 2.3.1) – většina bank v ČR je tedy reaktivních a riskují, že se z nich stane pouze infrastruktura. Navíc u těchto termínů došlo k posunu, jelikož původní termín platnosti RTS se očekával dříve.

2.4 Shrnutí směrnice PSD2

PSD2 přichází po PSD a SEPA, jelikož EU shledala PSD a situaci na bankovním trhu jako nedostačující. Chce zamezit primárně potencionálně nebezpečnému screen scrapingu, snížit množství podvodů při platbách lepší bezpečnostní, chránit uživatele před zneužíváním citlivých informací a snížit množství poplatků při platbách. Toho chce dosáhnout komunikací přes API, do kterého banky legislativně přinutí, dvoufázovým ověřováním, licencováním u centrálních bank a možností vynechat prostředníky u platby jako jsou karetní společnosti, platební brány apod.

Směrnice bude platit rovněž pro stávající platební služby, které mají prostor přizpůsobit se do září roku 2019. Bohužel nedefinuje jaké konkrétní technologie pro rozhraní a bezpečnost použít. Banky v ČR pro zabezpečenou komunikaci zatím využívají framework OAuth2. Nicméně většina bank v ČR není pro otevřené API vůbec připravená a vyčkávají na zveřejnění RTS (březen 2018) nebo až na jeho uvedení v platnost (září 2019). Tím pádem začne mít PSD2 zásadní dopad na bankovní trh až koncem roku 2019.

[28] www.rychlyvypis.cz

[29] Tabulka vytvořená autorem na základě informací z 26. 3. 2018 získaných procházením oficiálních webů jednotlivých bank a posledních zpráv týkajících se spouštění API v českých bankách.[98]

Tabulka 2.1: Přehled jednotlivých bank, termínů, kdy plánují spustit otevřené API, a stavu připravenosti vůči vývojářům. Data platná k **26. 3. 2018.**[29]

Rok	Banka	API	Dokumentace	Sandbox
2012	Fio banka	✓	✓	
2015	Česká spořitelna	✓	✓	✓
Q4 2017	Banka Creditas	✓	✓	
Q4 2017	air bank	✓	✓	
13. 1. 2018	Nejzazší termín pro zahrnutí PSD2 do lokální legislativy členských států EU.			
Q1 2018	KB			
Q1 2018	Raiffeisen BANK			
Q1 2018	MONETA Money Bank			
Q4 2018	Původní možný termín, kdy začne platit RTS na SCA.			
Q4 2019	Pravděpodobný termín, kdy začne platit RTS na SCA.			
čeká na RTS	Equa bank		✓	
čeká na RTS	SBERBANK			
čeká na RTS	Oberbank 3 Banken Gruppe			
čeká na RTS	Expobank			
N/A	UniCredit Bank		✓	✓
N/A	J&T BANKA		✓	
N/A	ČSOB			
N/A	mBank			

Kapitola 3

Aktuální trendy v bankovních aplikací

V kapitole 1.3.4 jsem nastínil, co vše se skrývá pod bankovními aplikacemi, respektive FinTech aplikacemi. Nyní ukáži, jak se na FinTech dívají zákazníci. Poté některé FinTech služby a jejich případy užití ukáži zblízka zblízka.

Jak si pozorný čtenář mohl všimnout, prohodil jsem oproti zadání DP kapitolu o PSD2 s kapitolou o aktuálních trendech v bankovních aplikacích. Přišlo mi lepší napřed znát kontext směrnice, aby bylo lépe vidět dopad PSD2 a cíl snahy EU. Jednotlivé ukázky služeb vůči PSD2 i přímo porovnávám. Půjde si tak lépe představit potenciál nové aplikace nebo nutné změny pro stávající aplikace, pokud například čtenář pracuje ve FinTech společnosti.

Ze začátku analyzuji obecně FinTech trh vzhledem k zákazníkům, aby bylo jasné, kam stávající nebo nové technologie směřovat – na jaké platformy, pro jaké cílové skupiny a jaké kategorie finančního trhu volit. Poté ukáži ukázky konkrétních FinTech aplikací – PayPal (instituce elektronických peněz), Trustly (platební instituce), TransferWise (instituce elektronických peněz) a Wallet (správce informací o platebním účtu).

3.1 Adaptace FinTech mezi zákazníky

Pro nejlepší přehled díky velkému množství dat, jak využívají zákazníci FinTech, jsem vytáhl nejdůležizější věci ze studie od společnosti Ernst & Young (zkráceně EY) s názvem EY FinTech Adoption Index 2017[7], která proběhla i v roce 2015. Studie pokrývá **20 zemí** a přes **22 000 rozhovorů** s lidmi aktivními online, tedy **digitálně aktivními lidmi**. Veškerá čísla a procenta jsou tedy brány z digitálně aktivních lidí nikoliv napříč spektrem celé společnosti. Jako FinTech uživatele berou člověka, který **využil dvě nebo více FinTech služeb** za posledních **šest měsíců**. Ve studii pokrývají FinTech kategorie rozebrané v kapitole 1.3.4, konkrétně 1.3.4.1 platby a převody peněz,

1.3.4.3 poradenství a osobní finance (zde rozdělené na spoření a investice plus finanční plánování), 1.3.4.2 půjčky a 1.3.4.4 pojištění. Vzhledem k tomu, že PSD je evropská směrnice platící pro evropský trh (kapitola 2), tak jsem v detailních číslech vytáhl hlavně země EHP.

3.1.1 Přijetí FinTech zákazníky

Průměrné využití FinTech služeb dosáhlo 33% v roce 2017. Nejvyšší využití FinTech služeb je v Číně (69%) a Indii (52%). Až poté následuje první evropská země Velká Británie (42%), kterou rozeberu i v detailnějších číslech vzhledem ke všem 20 zemím, jelikož je lídrem v EHP v oblasti FinTech. V tabulce 3.1 jsou pak uvedeny všechny země EHP (dostupné ve studii) a jejich míra adaptace FinTech.

Tabulka 3.1: Země EHP a jejich míra adopce FinTech v digitálně aktivní populaci v roce 2017.[7]

Země EHP	**Míra FinTech adopce**
Velká Británie	42%
Španělsko	37%
Německo	35%
Průměr EHP	**30%**
Francie	27%
Nizozemsko	27%
Irsko	26%
Belgie a Lucembursko	13%

Strategie podporující adaptaci FinTech dle zpovědi firem:

- Přechod z placených služeb na služby zadarmo.
- Nabízení dramaticky levnějších služeb.
- Řešení problémů za jiné firmy. Zde tedy především třetí strany za banky.
- Spolupráce s firmami, které mají již existující zákazníky. Opět tedy mluvíme především o zákaznících banky třetím stranám.
- Poskytování zcela nových služeb.

Obrovský vliv v budoucnosti na adaptaci FinTech bude mít samozřejmě směrnice PSD2, viz kapitola 2.3.

Hlavní klíčem k adaptaci FinTech je růst povědomí zákazníků o FinTech. V roce 2015 nemělo ve VB povědomí o FinTech 34% zákazníků, kdežto v roce 2017 už jenom 11%. Nejenom díky tomu vzrostla adaptace

Fintech z 14% v roce 2015 na 42% v roce 2017. **Povědomí** tedy vzrostlo **o 20%** a **adaptace** ještě **o** větších **28%**. Pravděpodobně díky širší konkurenci a obeznámenosti s ní klesla i preference využívání tradičních poskytovatelů finančních služeb z 14% v roce 2015 na 5% v roce 2017.

3.1.2 Přijetí FinTech napříč kategoriemi

Adaptace FinTech je řízena zejména větší poptávkou po digitálních převodech a platbách, jak lze vidět v tabulce 3.2. Ty vzrůstají hlavně díky rozšiřování elektronického obchodu. Mezi FinTech si drží stále prvenství. Další rychlý nárůst zažívají technologie pojištění, které skočily mezi roky 2015 a 2017 o 16% a posunuly se tím před řadu jiných kategorií.

Tabulka 3.2: Porovnání FinTech adaptace napříč kategoriemi mezi roky 2015 a 2017.[7]

2015	**FinTech kategorie**	**Adaptace**	**Nárůst**
1	platby a převody peněz	18%	/
2	spoření a investice	17%	/
3	finanční plánování	8%	/
4	pojištění	8%	/
5	půjčky	6%	/
2017	**FinTech kategorie**	**Adaptace**	**Nárůst**
1	platby a převody peněz	50%	32%
2	pojištění	24%	16%
3	spoření a investice	20%	3%
4	finanční plánování	10%	2%
5	půjčky	10%	4%

Procento respondentů, kteří v dané kategorii používali alespoň jednu FinTech službu.

V tabulce 3.3 lze vidět, že v EHP není příliš velká adaptace finančního plánování, spoření a investic. Za vinu bych to dal hlavně velké uzavřenosti trhu, tudíž nemožnosti plně dané FinTech služby využívat. V zmíněných oblastech podle mě velmi pomůže AISP zahrnutý v PSD2, viz kapitola 2.3.3.

Z tabulky 3.3 lze dále vypozorovat, že Čína vede ve všech kategoriích kromě pojištění, čemuž můžou vděčit právě za otevřené API, které se v Číně za poslední roky velmi rozmáhá a od roku 2015 je v Číně dokonce vedeno jako jeden z klíčových národních projektových plánů.[99] Díky těmto datům a příkladu Číny se lze domnívat, že i v EHP adaptace FinTech služeb velmi poroste díky zavedení PSD2.

Tabulka 3.3: Porovnání pěti nejlepších trhů v každé FinTech kategorii v roce 2017.[7]

Platby a převody peněz	Ad.	**Finanční plánování**	Ad.
Čína	83%	Čína	22%
Indie	72%	Brazílie	21%
Brazílie	60%	Indie	20%
Austrálie	59%	USA	15%
Velká Británie	**57%**	Hong Kong	13%
Spoření a investice	Ad.	**Půjčky**	Ad.
Čína	58%	Čína	46%
Indie	39%	Indie	20%
Brazílie	29%	Brazílie	15%
USA	27%	USA	13%
Hong Kong	25%	**Německo**	**12%**
Pojištění	Ad.		
Indie	47%		
Velká Británie	**43%**		
Čína	38%		
Jihoafrická republika	32%		
Německo	**31%**		

Průměrné procento respondentů z každé země, kteří v dané kategorii používali alespoň jednu FinTech službu. Země EHP jsou zvýrazněny. Ad. – Adaptace.

3.1.3 Profil FinTech zákazníka

Používání FinTech služeb je přirozeně dominantou mladších. K největší průměrné adaptaci došlo mezi lidmi ve věku od **25 let do 34 let** ve výši **48%**, dále pak s každými 10 lety průměrná adaptace výrazně klesá. Věkové kategorie od 18 let do 24 let má průměrnou adaptaci 37%, což je dáno tím, že respondenti v tomto věku nejsou ještě natolik ekonomicky aktivní, aby potřebovali řešit například investice, správu financí apod. Rozdíl mezi mladší a starší generací lze ilustrovat na příkladu dvou věkových kategorií 25 až 34 let a 65 až 74 let:[30]

- Nevěděli o FinTech – 10% proti 18% – **rozdíl 8%**
- Neměli potřebu používat FinTech – 5% proti 17% – **rozdíl 12%**

[30]Otázky byly pokládány pouze respondentům, kteří nepoužili FinTech za posledních šest měsíců, nicméně data jsou přeindexována vzhledem k celé skupině respondentů, tedy i těch, co FinTech využívají. Respondenti měli povoleno volit z více možností, proč FinTech nepoužívají.

- Preferují tradiční poskytovatele finančních služeb – 3% proti 22% – **rozdíl 19%**

- Neviděli výhody FinTech oproti tradičním službám – 2% proti 14% – **rozdíl 12%**

Ačkoliv rozdíl v povědomosti o FinTech není tak značný mezi věkovými kategoriemi, „nadchnutí“ pro FinTech již rozdílné je.

V oblasti bezpečnosti jsou na tom FinTech uživatelé oproti běžným uživatelům podobně. Před využitím finančních produktů více jak polovina čte podmínky, rozdíl mezi nimi je pouze 8%. Obdobně se bojí o bezpečnost osobních dat, konkrétně 2/3 dotázaných, a rozdíl mezi nimi jsou pouze 2%. Před finančními rozhodnutími více jak polovina si nechá raději někým poradit, rozdílem o 9% mezi FinTech uživateli a běžnými uživateli.

V oblasti využívání digitálních finančních služeb se FinTech uživatelé oproti běžným uživatelům liší již významněji, konkrétně:

- Preferují co nejvíce digitálních kanálů pro správu jejich života – 64% proti 38% – **rozdíl 26%**

- Využívají hlavně chytrý telefon pro přístup k finančním službám raději než stolní počítač nebo notebook – 54% proti 29% – **rozdíl 25%**

- Jsou ochotni vzít nejvhodnější finanční službu, i když se nejedná o nejlevnější variantu – 54% proti 34% – **rozdíl 20%**

Z čísel je patrné, že FinTech by se měl zaměřovat zejména na mobilní aplikace pro chytré telefony u produktů, kde to ještě dává smysl a nabídnout široké spektrum služeb pokrývající různé životní potřeby. Nemusejí se bát nabízet dražší prémiové verze za kvalitnější službu nebo obsah.

Dále z čísel dostupných ve studii vyplývá, že FinTech uživatelé využívají dramaticky více služby na vyžádání jako je například dovoz jídla a ekonomiku sdílení jako například pronájem kola. Tyto služby mají právě ve svých aplikacích často vestavěné platební možnosti.

3.1.4 Budoucnost FinTech

V budoucnu EY očekává nárůst v průměru z 33% na 52%. Jednotlivé země lze dohledat v studii. Nepřidával jsem je, jelikož závěry respondentů o jejich využití FinTech služeb v budoucnu jsou málo věrohodné. Nicméně něco málo lze vyčíst z preferencí jednotlivých kategorií, kdy největší zájem do budoucna projevují respondenti stále v platbách a pojištění, konkrétně o 15%. Pořadí jednotlivých kategorií se nezmění, kromě finančního plánování, které zajímá do budoucna nejméně respondentů.

3.2 Ukázky FinTech služeb

V kapitole se snažím uvést nejznámější FinTech služby z jednotlivých kategorií, zejména z těch, kde bude mít dopad směrnice PSD2, viz kapitola 2.3. Dopady promítnu do stávajících případů užití dané FinTech služby. Kromě analýzy samotné služby uvedu i základní fakta o službě díky nimž si půjde vytvořit hrubou představu podoby trhu.

3.2.1 PayPal

V kapitole vycházím z informací dostupných na stránkách a podstránkách společnosti PayPal.[100] Ne všechny informace jsou dostupné na stránkách PayPal pro region České republiky.

Datum spuštění: 1998

Trh: Hlavní sídlo v USA, služby nabízeny na 200 trzích v roce 2017

Uživatelé: 227 milionů držitelů účtu (16 milionů účtů obchodníků) v roce 2017

Příjmy: 267 miliard Kč v roce 2017

O PayPal

Služba PayPal spadá do FinTech kategorie e-Peněženek, viz 1.3.4.1. PayPal je tedy licencován jako instituce elektronických peněz a musí dodržovat s tím spjaté zákony, zejména KYC a AML regulace, viz kapitola 1.4.3. K identifikaci uživatele PayPal používá propojení bankovního účtu, kde si uživatel identifikační kontrolou již projít musel.

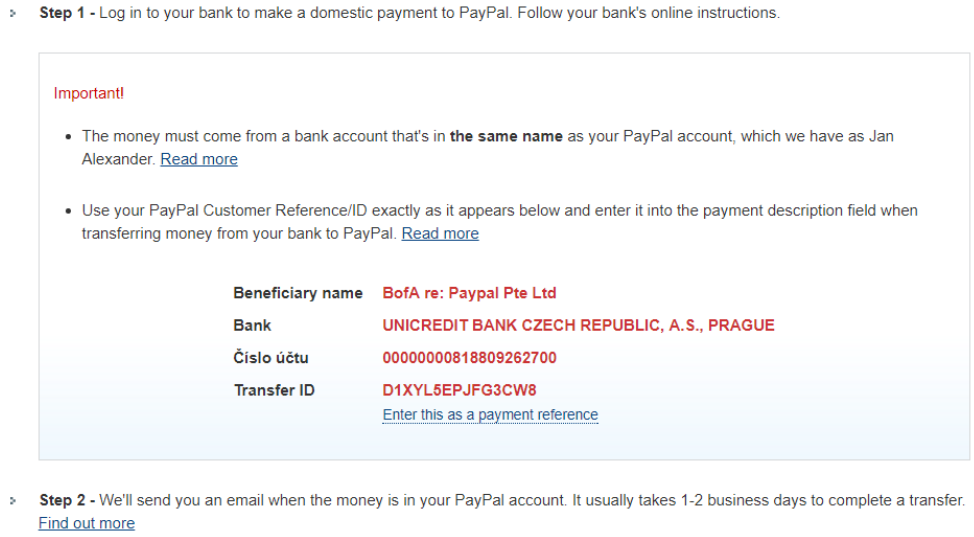
Propojení bankovního účtu

PayPal umožňuje propojení s bankovním účtem, které slouží k ověření totožnosti a k výběru peněz z PayPal peněženky, respektive převod prostředků z PayPal peněženky na propojený bankovní účet. Ve výsledku se nejedná o nic jiného, než běžný převod prostředků, akorát bez nutnosti vyplňovat údaje nutné k převodu. Další výhody propojení nemá, například pro přidání peněz do peněženky PayPalu, viz dále.

Přidání prostředků do PayPal peněženky

PayPal nabízí dvě možnosti pro nahrání prostředků do jejich peněženky.

Přidání prostředků Jedná se o klasický bankovní převod, jak lze vidět na obrázku 3.1.



Obrázek 3.1: Ukázka jednoho ze dvou způsobů přidání prostředků do PayPal peněženky.

Převod musí uživatel provést z libovolného svého bankovního účtu přes rozhraní banky nebo jiné propojené rozhraní a zadat klasické údaje pro bankovní převod, tedy číslo účtu a variabilní symbol, který je zde pod pojmem „Transfer ID“. Platba se připíše během jednoho až dvou pracovních dnů, jelikož se jedná o klasický převod bez žádných procesů na pozadí, díky kterým by se PayPal dozvěděl o zadané platbě v bance uživatele, a musí projít přes CERTIS ČNB, viz kapitola 1.3.3.

Přidání prostředků pomocí Trustly Oproti předchozí variantě mnohem rychlejší způsob, jak přidat prostředky do PayPal peněženky. K převodu využívá do PayPal integrovanou službu Trustly, o které se lze dočíst níže v kapitole 3.2.2. Vzhledem k tomu, že Trustly je opřené o směrnici PSD a bude následně přímo těžit z PSD2 nebo minimálně se bude muset adaptovat, rozebereme si tento proces detailněji. Integrovaný proces platby z pohledu uživatele probíhá následovně:

1. Zvolí možnost přidat prostředky pomocí Trustly.
2. Odsouhlasí přístup k řadě osobních údajů - viz obrázek 3.2.
3. Klikne, že chcete provést instantní platbu s využitím Trustly, což uživatele přesměruje na stránky PayPalu *https://www.paypal-dobijeni.cz*.

4. Vybere z listu bank podporovaných Trustly svoji banku, je-li v seznamu a zvolí částku. Jinak pro přidání prostředků nemůže využít tento způsob.

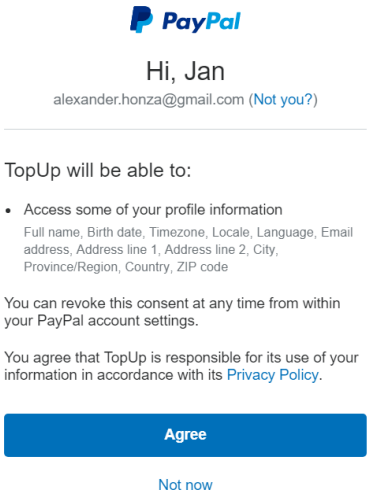
5. Následně je přesměrován na stránky služby Trustly, kde jako první krok se musí přihlásit do své banky, kterou si v předchozím kroku vybral, viz obrázek 3.4.

6. Poté vybere jeden ze svých účtů u banky, z kterého se mu peníze převedou, viz obrázek 3.5.

7. Již jenom potvrdí převod pomocí ochrany, kterou provádí banka uživatele, nikoliv Trustly samotné. Viz obrázek 3.6, kde můžeme vidět ochranu mBank pomocí SMS pro převody.

8. Následně Trustly na pozadí s bankou uživatele založí příkaz k převodu prostředků, viz obrázek 3.7.

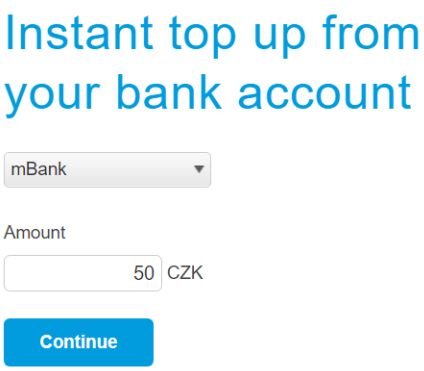
9. Během pár vteřin PayPal na základě potvrzení na pozadí od Trustly, navýší stav PayPal peněženky uživatele.



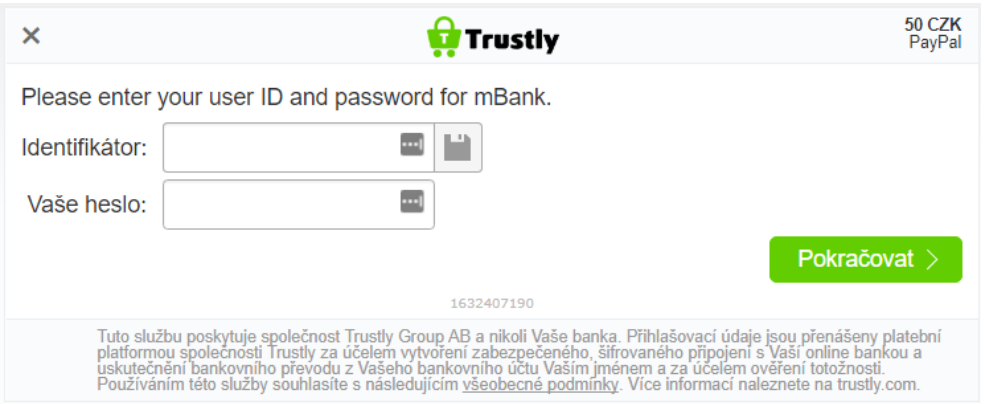
Obrázek 3.2: Souhlas s přístupem k osobním informacím ve výčtu u procesu přidání prostředků do PayPal peněženky přes Trustly.

Ve výsledku se jedná opět o klasický převod peněz z účtu na účet, akorát na pozadí. Tudíž takto připsané peníze PayPal od uživatele ve skutečnosti ještě neobdržel, jelikož musí projít transakce přes CERTIS (kapitola 1.3.3).

Ošetření stornování platby Na základě procesů popsaných výše může nejednoho napadnout zkusit tento systém obejít. Proto jsem vyzkoušel, jak tento systém má PayPal, respektive Trustly, ošetřený. Každý příkaz k převodu



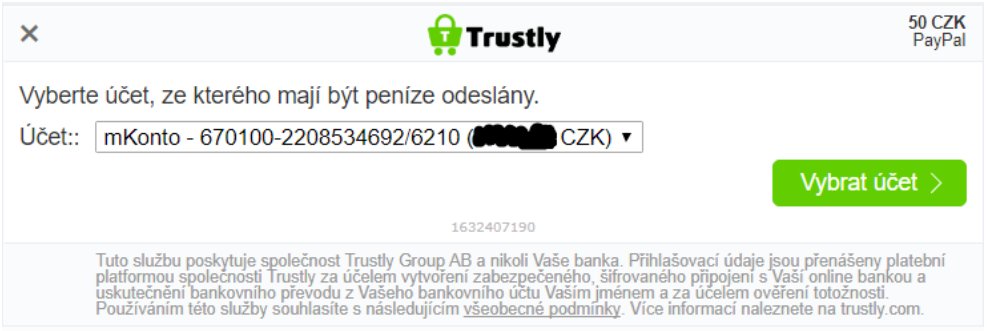
Obrázek 3.3: Výběr banky, z které chce uživatel prostředky přidat, u procesu přidání prostředků do PayPal peněženky přes Trustly.



Obrázek 3.4: Přihlášení do banky pomocí přihlašovacích údajů od banky uživatele, z které chce uživatel prostředky přidat, u procesu přidání prostředků do PayPal peněženky přes Trustly.

by v bance měl jít zrušit do doby, než je dávkově zpracován (viz kapitola 1.2.8) a odeslán do systému CERTIS, viz obrázek 3.7.

Plánovanou operaci, respektive příkaz k převodu, jsem zrušil. V PayPalu se zrušení převodu nijak nepromítlo a stále jsem danou částkou disponoval. Proto jsem ještě zkusil penězi z PayPal peněženky zaplatit, což mě PayPal nechal. Z toho plyne, že PayPal o zrušení převodu není vůbec informován Trustly, pravděpodobně ani samotné Trustly nemá nastavené žádné procesy kontroly. Dokonce ani po měsíci po testu nejsem na PayPal účtu v mínusu, ani Trustly si z banky nic nestrhlo, ani mě nikdo neinformoval přes email. Závěr je tedy takový, že jsem neprávem bohatší o 50 Kč.



Obrázek 3.5: Výběr bankovního účtu uživatele, z kterého chce prostředky přidat, u procesu přidání prostředků do PayPal peněženky přes Trustly.

Obrázek 3.6: Ověřovací mechanismus banky uživatele, z které chce uživatel prostředky přidat, u procesu přidání prostředků do PayPal peněženky přes Trustly.

Vybrání prostředků

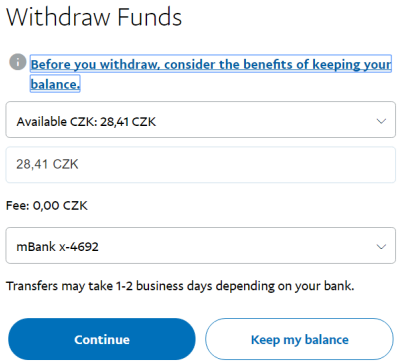
PayPal umožňuje prostředky z peněženky uživatele vybrat. Zde se uplatní propojení s bankou pro snazší výběr, respektive zadání převodu. Jedná se totiž zase o běžný převod mezi účty, tedy mezi PayPalem uživatele a vybranou bankou uživatele. Tak jako v bance musí převod peněz u PayPalu napřed projít přes CERTIS, proto převod prostředků neproběhne okamžitě.

Placení pomocí PayPal

V řadě e-shopů a jiných službách je integrovaná platba pomocí PayPalu. Při platbě si můžete vybrat, jestli chcete platit z:

- **Karty propojené v PayPal**, přičemž můžete vybrat ze dvou mož-

Obrázek 3.7: Čekající mezibankovní převody uživatele u mBank.



Obrázek 3.8: Výběr prostředků z PayPal peněženky.

ností převodu měny, platíte-li v obchodě jinou měnou, než pod kterou je vedený účet spojený s kartou:

  - Převod měny **PayPalem**
  - Převod měny **vydavatelem karty**

- **PayPal peněženky**, kde se automaticky použije převod měny pomocí PayPalu, platíte-li v obchodě jinou měnou, než disponujete v PayPal peněžence.

Kdo těží na kurzech více? Srovnání lze vidět v tabulce 3.4. Z tabulky jasně vyplývá, že PayPal má velmi nevýhodný kurz, kdy **oproti nejvýhodnějšímu kurzu u Equa bank** si připlatíte **až 3%** navíc z placené částky, nemluvě o tom, že i samotná banka prodává měnu za větší částku než je kurz ČNB. Je nutné si dávat pozor, jelikož PayPal vybírá u platby kartou převod měny pomocí PayPal jako výchozí možnost a u PayPal peněženky ani jiná možnost není.

Převody pomocí PayPal

Mezi účty PayPal můžete peníze převádět, opět buď **zdarma z PayPal peněženky** nebo **s výrazným poplatkem z karty**, viz níže v přehledu PayPal

Tabulka 3.4: Srovnání kurzů mezi PayPal, nejvýhodnější a nejméně výhodnou bankou v ČR k 20. 4. 2018. Částky jsou uvedené v Kč. Kurz je počítán za 1 USD a 1 EUR.

Srovnání kurzů	**USD**	**EUR**
mBank kurz	21.304	26.142
PayPal kurz	21.59	26.67
PayPal příplatek oproti mBank	**0.286**	**0.528**
PayPal příplatek oproti **mBank v %**	**1%**	**2%**
Equa bank kurz	20.923	25.885
PayPal příplatek oproti Equa bank	**0.667**	**0.785**
PayPal příplatek oproti **Equa bank v %**	**3%**	**3%**

poplatků. Stačí zadat **email příjemce**. Má-li příjemce PayPal, kromě notifikace mailem se mu peníze připíšou okamžitě do PayPal peněženky. Pokud příjemce PayPal nemá, vyzve ho PayPal mailem k registraci a následně mu připíše převáděnou částku.

Poplatky PayPal

Jelikož můžete přes PayPal platit za služby, jak bylo popsáno výše, poplatky jsou rozděleny pro dvě strany:

- Placení
  - Plátce (zákazník) - zdarma
  - Příjemce (obchodník) - 1,9% až 3,4% + 10 Kč (k nižším procentům lze dosáhnout větším měsíčním objemem přijímaných částek)
- Převod
  - Z PayPal peněženky - zdarma
  - Kartou - 3,4% + 10 Kč

U převodů lze v závislosti na zemi vybrat, jestli poplatky bude platit plátce nebo příjemce.

Ostatní služby ve výčtu níže jsou zdarma, jak pro osobní účet, tak účet obchodníka:

- Otevření PayPal účtu.
- Nastavení PayPal účtu (pro obchodníky).
- Vedení PayPal účtu.
- Připsání peněz do PayPal peněženky.

- Výběr z PayPal peněženky.

U mezinárodních plateb se pak ještě u placení obchodníkům i u převodů přidává cca 0,5% až 2% z částky, kde závisí hodně na zemi plátce a příjemce. Pro mezinárodní převody jsou tedy na trhu výhodnější jiné služby, například TransferWise, viz kapitola 3.2.3.

PayPal ve vztahu k PSD2

Největší potenciál pro PayPal vidím v současnosti zjednodušení plateb v rámci EHP, tedy využitím PISP.

PayPal může PISP využít pro přidání prostředků do PayPal peněženky jako náhradu současného klasického převodu, který umožňuje, a tím se vyhnout spolupráci s externími firmami jako Trustly.

Dále může PISP využít přímo pro platby u obchodníků stejně jako to dnes dělá právě Trustly. PayPal se touto záležitostí, kterou umožňuje PSD (viz kapitola 2.1) pravděpodobně nezabýval, jelikož by musel využívat screen scraping, za který PayPal nechce pravděpodobně nést odpovědnost. Nicméně díky PSD2 bude časem pro PayPal možné využít otevřené API bank, pro které si nebude muset zřizovat ani licenci, jelikož licence instituce elektronických peněz, kterou PayPal musí mít, PISP pokrývá.

Každopádně kvůli PSD2 bude muset zavést minimálně povinné dvoufázové ověření, které má aktuálně PayPal řešené dobrovolně přes mobilní aplikaci PayPal. Pro PayPal je tedy legislativní dopad minimální.

3.2.2 Trustly

Trustly

V kapitole vycházím z informací dostupných na stránkách a podstránkách společnosti Trustly.[101]

Datum spuštění: 2008

Trh: Hlavní sídlo ve Švédsku, služby nabízeny v 29 evropských zemí v roce 2018

Uživatelé: 700 obchodníků, 2 miliony transakcí měsíčně v roce 2016

Příjmy: 764 milionů Kč v roce 2016[102]

O Trustly

Trustly je platební služba využívající výhody směrnice PSD (viz kapitola 2.1) spadající do FinTech kategorie platebních bran, viz 1.3.4.1. Licenci má od švédské centrální banky jako platební instituce, což umožňuje firmě provádět

platby v EHP. Pro placení využívá podobných principů definovaných v PSD2 (viz kapitola 2.3), konkrétně PISP, akorát u většiny bank přes screen scraping (kapitola 1.4.2). Dle Trustly podporují již přes 3000 bank v 29 evropských zemích.

Trustly v ČR

Trustly je v ČR plně napojené pouze na Českou spořitelnu, UniCredit Bank, mBank a Sberbank. To mě vrací ke kapitole 2.3.8, kde jsem rozebíral připravenost bank v ČR vůči PSD2. Můžete si všimnout, že mBank ani Sberbank nemá připravené alespoň pro veřejnost žádné otevřené API – Trustly tedy s největší pravděpodobností tyto banky podporuje přes screen scraping.

Technický pohled na Trustly

Princip integrace Trustly můžeme vidět v předchozí kapitole 3.2.1, kde je Trustly integrovaný do PayPal, zpočátku přes API, díky kterému obdrží potřebné informace pro platbu, viz obrázek 3.3. Poté přesměrováním na stránky Trustly si projdete vždy postupnými kroky, které jsou vidět na obrázku 3.4, 3.5 a 3.6. Vše přes stránky Trustly, bez žádného přesměrování na banku. Pro komunikaci s bankou používá Trustly OpenPGP (RFC 4880), SHA512 a HTTPS.[31]

Poplatky Trustly

Trustly je na tom o něco lépe s poplatky, obzvláště pokud se nejedná o příliš malého obchodníka, respektive o malý měsíční objem částek:

- Nastavení služby - 200 EUR
- Měsíční poplatek - 20 EUR
- Transakční poplatek - 1,5% + 0,1 EUR

S transakčním poplatkem se dostává hluboko pod nejlepší nabídku PayPalu pro obchodníky s obrovským obratem a pro evropský trh tedy mnohem vhodnější volbou pro obchodníky jak PayPal. Navíc tato nabídka může být u Trustly dle mého názoru ještě výhodnější pro obchodníky s větším obratem. Bohužel ceník Trustly je dostupný pouze na základě poptávky. Nutno taky brát v potaz, že Trustly bere za veškeré platby plnou zodpovědnost.

[31] Více o těchto technologiích můžete najít na odkazech *https://github.com/trustly/bankapi* a *https://www.youtube.com/watch?v=CHi2RclGvIM*.

Trustly ve vztahu k PSD2

Pro Trustly vnímám PSD2 jako příležitost i hrozbu zároveň. Příležitost v tom, že bude moct bez náročných dohod s bankami využívat jejich otevřené API a propojit tím prakticky všechny banky. Nicméně pokud čísla Trustly nelžou, i tak již mají propojených hodně bank. Tím se dostáváme k hrozbě. Pokud většina propojených bank je přes technologii screen scraping, tak kvůli PSD2 budou muset do Q4 2019 všechny tyto banky propojit přes API. Je otázka, jestli to u tolika bank stihnou. Navíc příchodem PSD2 bude platební službu mnohem snazší provozovat. Větší obchodníci tím pádem můžou teoreticky začít platební služby poskytovat přímo sami a vynechají tím prostředníka jako je Trustly.

3.2.3 TransferWise

TransferWise

V kapitole vycházím z informací dostupných na stránkách a podstránkách společnosti TransferWise.[103]

Datum spuštění: 2011

Trh: Hlavní sídlo v Londýně, služby nabízeny v 59 zemí s 504 měnovými cestami

Uživatelé: Přes 2 miliony

Příjmy: 2 miliardy Kč v roce 2016[104]

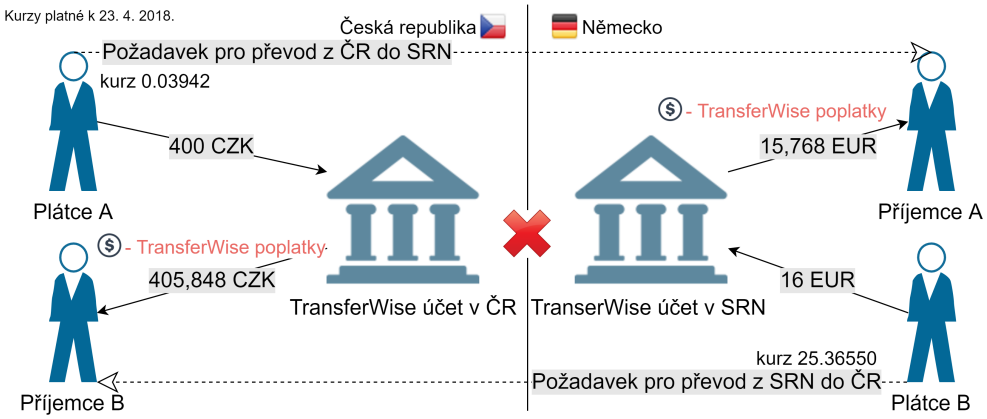
O TransferWise

TransferWise je londýnská Fintech společnost spadající do FinTech kategorie převodů a e-Peněženek, viz 1.3.4.1, která nabízí mezinárodní převody peněz a možnost držet virtuální účty v desítkách měn s možností vydat i platební kartu MasterCard k danému účtu.[32] Jelikož se jedná o virtuální účty, nikoliv skutečné bankovní účty, nemusíte účty vyplňovat do jakýchkoliv formulářů, například při získávání víza. TransferWise svými službami spadá pod licenci instituci elektronických peněz.

Převod nejde přímo příjemci definovaným plátcem, ale společnosti TransferWise na účet vedený společností v zemi plátce. Příjemci částku TransferWise převede naopak z účtu vedeného společností v zemi příjemce. K vyrovnání balančního zůstatku na svých účtech v jednotlivých zemích používá TransferWise podobný protisměrný převod prostředků jiných uživatelů. Pro lepší představu lze princip vidět na obrázku 3.9. **Ve skutečnosti se tedy žádné peníze**

[32] K 21.4.2018 dostupné pouze pro omezené množství uživatelů na základě pozvánky. Časem bude ale dostupné pro všechny ve VB a EHP.

přes hranice neposílají. Díky tomu může TransferWise nabízet velmi nízké poplatky, viz dále kapitola TransferWise poplatků, a reálný měnový kurz[33], který lze nalézt například na Googlu.



Obrázek 3.9: Princip, jakým fungují mezinárodní převody pomocí TransferWise.

Založení účtu

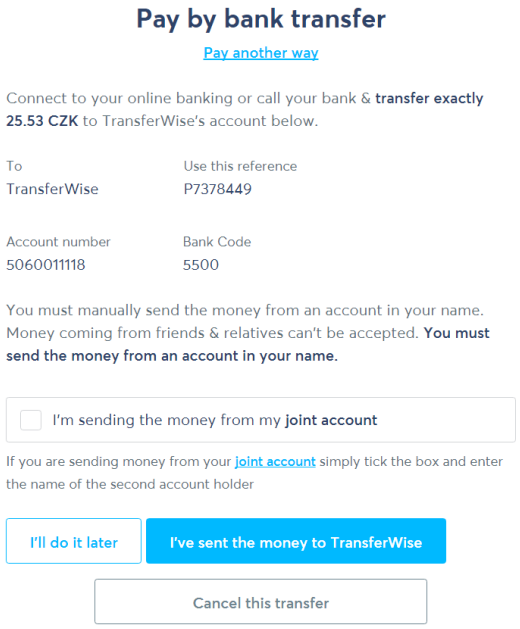
Obrázek 3.10: Virtuální účet u TransferWise vedený v EUR.

Jelikož se jedná o společnost licencovanou pro vydávání elektronických peněz, musí TransferWise dodržovat s tím spjaté zákony, zejména KYC a AML regulace, viz kapitola 1.4.3. Jelikož TransferWise nepoužívá například jako PayPal (viz 3.2.1) propojení bankovního účtu k ověření identity, založení prvního účtu u TransfeWise v jakékoliv měně není okamžité. TransferWise k těmto

[33]Kurz, který je oproštěn od prodejní marže.

účelům využívá službu Netverify od společnosti Jumio a ověření by nemělo trvat déle jak tři pracovní dny. K ověření je třeba pas nebo ID nebo řidičský průkaz a dokument potvrzující adresu uživatele, například faktura. Jakmile dojde jednou k ověření, tak pro další účty v jiných měnách není potřeba proces opakovat. U eura, britské libry, amerického a australského dolaru se jedná dokonce o účet s lokálními bankovními detaily jako je adresa, IBAN[34], apod., viz obrázek 3.10.

Převedení peněz



Obrázek 3.11: Závěrečný krok při provádění převodu prostředků přes službu TransferWise.

TransferWise umožňuje převod prostředků buď na váš účet vedený u nich, což funguje výběrem daného účtu v kontextové nabídce bez nutnosti zadávat detaily účtu, nebo převod prostředků na jiný účet v jiné zemi:

- **Účet plátce** v jiné zemi - Nutné zadat IBAN[34], plátce a příjemce musí mít stejné jméno.
- **Účet jiného uživatele** v jiné zemi - Je třeba zadat jméno vlastníka účtu příjemce a email příjemce. Nezná-li plátce IBAN[34], požádá TransferWise o IBAN[34] emailem příjemce bez nutnosti dalšího zásahu plátce.

[34]Nebo jinou identifikaci účtu v závislosti na zemi, z které účet pochází.

Vždy se jedná ale o měnový převod, nelze tedy například převést na váš účet TransferWise vedený v EUR z účtu rovněž v EUR, jelikož zde by nedošlo k převodu měny. Nicméně ve správě účtu už to již lze, viz dále správa účtu.

Pro převod si může uživatel vybrat z řady možností v závislosti na tom, z jaké měny bude peníze převádět, respektive z jaké země bude platit.

V ČR si pro převod uživatel může vybrat klasický bankovní převod, debetní nebo kreditní kartu. Vybere-li si převod pomocí karty, připočtou se ještě poplatky karetní společnosti, viz kapitola 2.3.4. TransferWise odešle částku na účet příjemce až v momentě, kdy od plátce sám částku obdrží. Nicméně mimo plateb z ČR se opět tyto poplatky mohou lišit.

Z jiných měn, respektive zemí, lze využít další možnosti převodů, například PSP jako Trustly, SOFORT, iDEAL, příkaz k inkasu a další možnosti specifické k určité zemi.

Správa účtu

Uživatel může v rámci správy účtu provádět:

- Odesílat peníze na libovolné účty způsobem, jaký je popsán v předchozí podkapitole.
- Přidávat peníze způsobem, jaký je popsán v předchozí podkapitole, ale i ve stejné měně.
- Převádět měnu, respektive prostředky, mezi svými TransferWise účty.
- Stáhnout výpis z účtu v PDF nebo CSV.

Nabídku lze vidět na obrázku 3.10.

Poplatky TransferWise

Detailní ceník lze nalézt na stránkách společnosti. Za zmínku stojí, že **všechno je zdarma** kromě:

- Převodu měny[35] - 0,35% až 1%[36] z částky, minimálně však 42 Kč
- Převod peněz na lokální účet ve stejné měně - 0,6 EUR
- Výběr z bankomatu TransferWise debetní kartou Mastercard od částky přes 200 GBP/měsíc - 2%
- Placení TransferWise debetní kartou Mastercard v nepodporované měně – poplatek Mastercard

[35]Poplatek je stejný, i když dojde k převodu měny využitím platební karty uživatele vydané TransferWise.

[36]U obvyklejších a stabilních měn. Jinak může poplatek dosahovat až 5%. Oproti PayPalu, kde dohledat některé poplatky bylo nemožné, lze v nápovědě TransferWise dohledat kompletní matici všech měnových cest a jejich poplatků.

Bezpečnost

Na TransferWise mě u bezpečnosti oproti PayPalu zaujalo dvoufázové ověření při přihlašování, které nelze vypnout, pokud máte u TransferWise vedený alespoň jeden virtuální účet. První fáze jsou klasické přihlašovací údaje do služby, druhá fáze je buď SMS ověřovací kód nebo potvrzení v mobilní aplikaci TransferWise.

Přihlášení je nutné pokaždé, pokud uživatel nezaškrtne volbu zapamatování. Poté zůstanete na zařízeních přihlášený po dobu dvou týdnů. Při přístupu z nového zařízení musí projít znovu dvoufázovým ověřením.

TransferWise ve vztahu k SEPA

Hodně lidí by si řeklo, že u převodů po Evropě díky SEPA platbám (více o SEPA v kapitole 2.2) nemá smysl TransferWise používat. Nicméně například dle ceníků SEPA plateb u bank v ČR[105] se pohybují poplatky od 40 Kč do 450 Kč.[37]

SEPA platba v EUR

- **SEPA** - Od 40 Kč do 450 Kč.
- **TransferWise** - Přidání peněz na virtuální účet ve stejné měně zdarma. Převedení peněz na lokální bankovní účet ve stejné měně **15,26 Kč**.[38]
- **Závěr** - TransferWise vyjde vždy levněji v desítkách korun.

SEPA platba v Kč

- **SEPA** - Od 40 Kč do 450 Kč + marže banky na prodeji měny.
- **TransferWise** - Poplatek **0,7%** z převáděné částky, avšak minimálně 42 Kč. Reálný kurz bez marže za prodej měny.
- **Závěr** - Když započtu u bank poplatek za SEPA platbu, vždy vyjde levněji TransferWise. Navíc u částek od stokorun výše, kde už hraje roli marže banky na prodeji měny, si u SEPA platby **klient banky připlatí** cca **1,3% až 2,2%**[39] z převáděné částky podle banky. SEPA platby jsou z tohoto důvodu oproti TransferWise velmi nevýhodné. Další prodražení

[37] Pro lepší srovnání jsem sečetl poplatky za odchozí i příchozí platby. Předpokládám, že poplatky za příchozí platby v bankách jiných evropských zemí se příliš neliší od bank v ČR.

[38] Převedeno z EUR do Kč. Kurz platný ke dni 24.4.2018. Poplatek je 0,6 EUR.

[39] U menších částek v tisících je procentuální příplatek ještě vyšší v řádu 0,1% a klesá mezi uvedené hodnoty příplatků až v desetitisících. Důvodem je výše poplatku za SEPA platbu, který z převáděné částky odečítám. Oproti tomu TransferWise od určité částky přejde ze stabilního poplatku 42 Kč na procentuální poplatek a ten je vždy výhodnější jak marže banky na prodeji měny.

by nastalo, pokud by účet příjemce rovněž nebyl vedený v EUR a muselo by dojít u SEPA platby k dvojímu převodu měny.

TransferWise ve vztahu k PSD2

Díky PSD2 bude moct TransferWise zavést vlastní PISP pro převody a přidávání peněz do e-Peněženky a tím uživatelům dramaticky zjednodušit a zrychlit celý proces z jakékoliv země EHP oproti běžnému převodu peněz, viz obrázek 3.11, a pro TransferWise za stejných cenových podmínek, odhlédnu-li od nákladů spojených s implementací řešení PSD2. Navíc z pohledu RTS SCA jsou již připraveni a potřebnou licenci, jakožto instituce elektronických peněz, již mají. Proč by stávající přístup měli změnit až s příchodem PSD2? Opět dle mého názoru díky tomu, že oproti současnosti, tedy PSD, budou moci využít otevřené API bank, nikoliv screen scraping.

3.2.4 Wallet

Wallet

V kapitole vycházím z informací dostupných na stránkách a podstránkách společnosti BudgetBakers.[106]

Datum spuštění: 2010

Trh: Hlavní sídlo v Praze, služby nabízeny celosvětově (uživatelé aktuálně z 140 zemí)

Uživatelé: Přes 1,5 milionu, nicméně aktivních 160 tisíc[107]

Příjmy: Přesné čísla jsem nenašel, nicméně do černých čísel se překlonili teprve nedávno

O Wallet

Wallet je FinTech aplikace spadající do kategorie správy osobních financí, viz 1.3.4.3. Wallet vytvořil český Startup BudgetBakers.

Wallet slouží k evidenci příjmů a výdajů uživatele, případně celé rodiny, pokud si peněženky propojíte. Z těchto dat pak uživatel může sledovat grafy a reporty. Díky možnosti propojení s bankou může Wallet bezhotovostní platby synchronizovat bez asistence uživatele. V aplikaci může uživatel vést několik účtů ať už hotovostních nebo bezhotovostních. V jednotlivých částech aplikace pak lze filtrovat dle účtů nebo zobrazit souhrn ze všech. Účty lze vést v jakékoliv měně, dokonce i v řadě virtuálních (viz kryptoměny v kapitole 1.3.4.6).

Hlavní konkurencí nabízející prakticky stejné služby jsou například rovněž česká společnost se Spendee, Mint, MoneyLover a mnoho dalších.

Základní funkcionality

Záznamy Transakční historie příjmů a výdajů napříč účty. Lze vytvořit nový záznam nebo peníze převést mezi účty. U záznamu je možné pro usnadnění vytvořit šablonu. Veškeré záznamy lze kategorizovat. K záznamům lze přidávat účtenky, faktury nebo jiné doklady, dokonce i místo nákupu přes GPS.

Grafy Různé formy grafů vycházející ze záznamů.

Reporty Souhrn záznamů za určité časové období, které je plně nastavitelné.

Plánované platby Seznam plateb, které ještě nebyly provedeny.

Rozpočty Maximální částka pro kategorii nebo skupinu kategorií, kterou uživatel za nastavitelné období nechce překročit. Lze uživatele upozornit při hrozbě překročení rozpočtu nebo jeho překročení.

Dluhy Evidence dluhů oběma směry (věřitel nebo dlužník). Lze propojit s kontakty v telefonu, nastavit datum splatnosti a další.

Cíle Cíle, kterých by uživatel chtěl dosáhnout a jejich průběh, například šetření na auto. Není propojené nijak se záznamy.

Wallet Life Různé notifikace, například na možnosti odškodnění a rovnou možnost jejich řešení.

Sdílení se skupinou Možnost propojit Wallet s ostatními uživateli, například rodinou.

Věrnostní karty Evidence věrnostních karet od obchodníků. Skenuje pouze čárový kód přes fotoaparát. Nijak nespolupracuje s ostatními funkcionalitami aplikace, takže snadno nahraditelné specializovanými aplikacemi pro tyto účely, například Stocard.

Exporty Export záznamů nastaveného časového období s možností dalších filtrů. Export je možný do PDF, XLS nebo CSV.

Umístění Dle záznamů, u kterých byla zapnutá GPS, může vytvářet teplotní mapu[40] transakcí. Na základě ní může uživatel vidět místa, kde utrácí nejvíce.

Nákupní lístky Skládá se z editovatelných nákupních seznamů, kam lze přidávat položky (bez žádného detailu kromě názvu). Seznam lze sdílet nebo z něho generovat záznam o zadané částce. Lepší než poznámkový

[40]Grafická reprezentace dat používající systém barev reprezentující různé hodnoty. Nemusí nutně být na reálné mapě. Používá se například pro analýzu používání webu uživateli.[108]

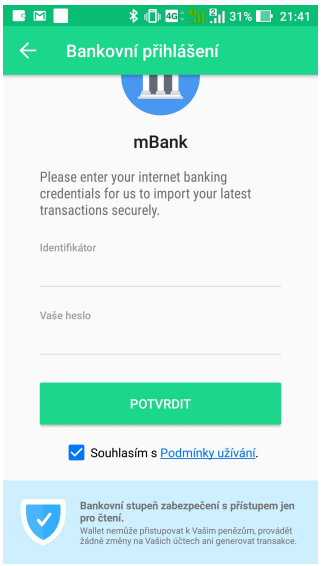
blok, nicméně na nákupní seznamy jsou případně lepší specializované aplikace, například Out of Milk.

Záruky Seznam záruk, respektive dokladů, které uživatel přidal k záznamům. U jednotlivých záruk je vidět stav k aktuálnímu dni. Něco podobného nabízí například AirBank, nicméně AirBank dokáže z dokladu vyčíst částku, případně vyplnit příkaz k zaplacení faktury. Pokud se jedná ale o hotovostní platbu, nijak částku nezahrne do historie, takže se AirBank nedá používat pro celkovou správu osobních financí.

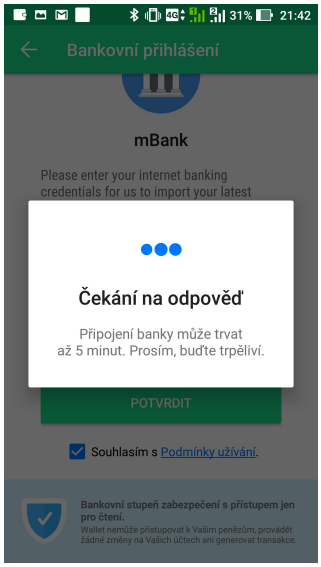
Propojení bank

Proces propojení banky s aplikací Wallet uživatel zvládne ve dvou krocích:

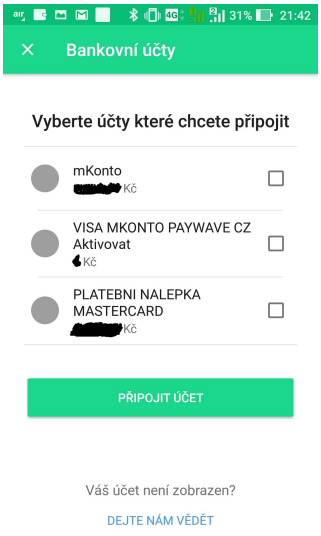
1. Vyplnění přihlašovacích údajů do banky, viz 3.12.
2. Výběr účtu nebo účtů banky uživatele, které chce uživatel propojit, viz 3.14.



Obrázek 3.12: Vyplnění přihlašovacích údajů do mBank kvůli propojení banky s aplikací Wallet.



Obrázek 3.13: Čekání na propojení banky s aplikací Wallet.



Obrázek 3.14: Výběr účtu nebo účtů banky uživatele, které chce uživatel propojit s aplikací Wallet.

Podporované banky v ČR

- Česká spořitelna

- ČSOB
- Equa Bank
- Fio Bank
- mBank
- PPF Banka[41]
- Raiffeisenbank
- Sberbank
- UniCredit Bank

Bezpečnost

Aplikace umožňuje dobrovolně nastavit PIN nutný k otevření aplikace.

Fyzická bezpečnost Využívají Amazon a Linode datová centra, tedy od specializovaných firem zajišťující následující bezpečnost:

- Biometrické skenování pro přístup k datovému centru
- Bezpečnostní kamery monitorující veškerá datová centra
- 24/7 ochranka objektů
- Datová centra skryta pro veřejnost
- Fyzická bezpečnost auditována nezávislou firmou

Data Veškerá jejich data jsou přenášena přes SSL. Zajištěny mají dva databázové systémy - pro uložení profilu a pro individuální uživatelská data s přístupem opět přes SSL.

Propojení bank Aplikace je naprogramována pouze pro čtení dat z bankovního účtu a tudíž nemůže z účtu provádět platby ani modifikovat nebo odesílat jakékoliv jiné informace.

Poplatky Wallet

Aplikace je nabízená zdarma ořezaná o řadu funkcionalit. Nejdůležitější funkce, tedy propojení bank, v základu chybí. Prémiové funkce jsou nabízeny za měsíční poplatek 65 Kč nebo 21 Kč při roční platbě, kde lze připojit až dvě banky. Za 100 Kč nebo 33 Kč měsíčně lze propojit Wallet s ostatními uživateli a propojit s neomezeným počtem podporovaných bank.

[41] Ačkoliv AirBank spadá do skupiny PPF, tak podporovaná není.

Wallet ve vztahu k PSD2

Wallet opět u většiny bank s největší pravděpodobností využívá screen scraping. Ačkoliv tedy tvrdí, že data pouze čtou, můžou ve skutečnosti účet i ovládat, jelikož musí mít pro screen scraping přihlašovací údaje. Wallet díky PSD2 bude moct podporovat více bank. Na druhou stranu do Q4 2019 u stávajících podporovaných bank bude muset technologii změnit ze screen scrapingu na API, což bude časově náročné. Navíc bude muset zažádat u ČNB o licenci správce informací o platebním účtu.

3.3 Shrnutí aktuálních trendů v bankovních aplikacích

Využívaní platebních služeb, které jsou nejžádanější, a dalších kategorií FinTech výrazně rostlo i v předchozích letech bez PSD2. Po příchodu PSD2 lze očekávat ještě vyšší nárůst FinTech a jeho využívání v EHP, po vzoru Číny. Do cílové skupiny patří zejména mladší generace lidí. Nejužívanější platforma jsou chytré zařízení, zejména telefony.

PSD2 bude mít dopad i na stávající poskytovatele platebních služeb jako jsou společnosti PayPal, Trustly, TransferWise, zejména v oblasti RTS SCA a přechodu ze screen scrapingu na otevřené API, a agregační služby jako je Wallet, kde největší problém bude opět přechod ze screen scrapingu a navíc žádost o udělení licence.

Poznatky se hodí nejenom pro vytvoření nové aplikace, ale i pro zaměstnance společností, které provozující stávající FinTech aplikace.

Velké zaměření bude muset směřovat na ošetření procesů u plateb, respektive převodů, které musí proběhnout teoreticky instantně, nicméně prakticky instantně kvůli ČNB a CERTIS nikdy proběhnout nemůžou.

Kapitola 4

Návrh aplikace využívající otevřené API definované směrnicí PSD2

Jelikož se jedná o základní prototyp pro představení propojení s bankou a ukázku některých operací přes otevřené API, případy užití i doménový model jsou méně obsáhlejší. V kapitole ještě rozeberu architekturu systému.

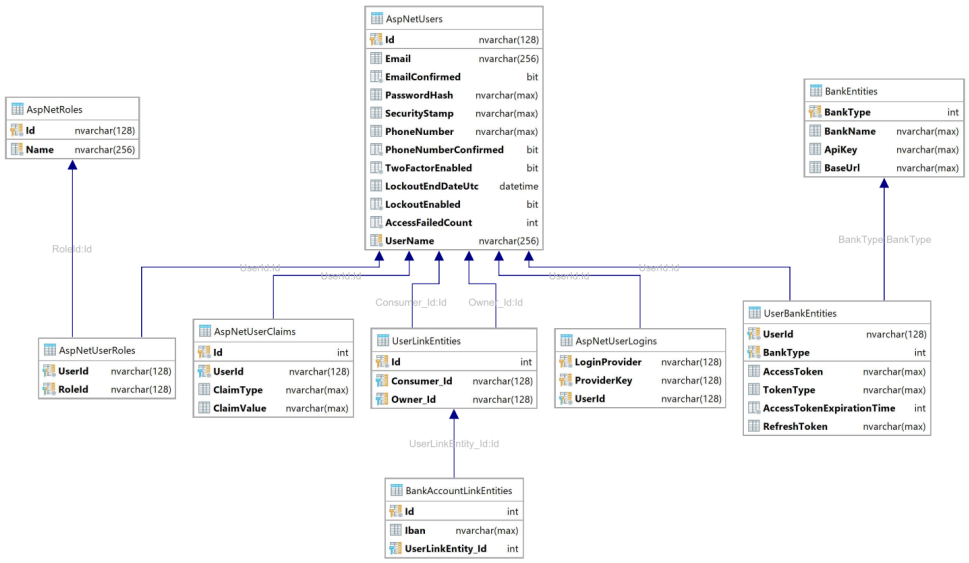
4.1 Doménový model

Doménový model mého základního prototypu vytvořeného na základě směrnice PSD2 a dokumentace otevřeného API bank s využitím frameworku OAuth2 pro ověření komunikace lze vidět na obrázku databázového modelu 4.1.

Pro pochopení modelu je nutnou podmínkou mít z kapitoly o PSD2 nastudovaný minimálně OAuth2 framework, který jsem rozebral v kapitole 2.3.6. Vlastnosti týkající se PSD2 jsem zvýraznil kurzívou.

4.1.1 Model nutný vzhledem k PSD2

- **Bank** Evidované banky poskytovatele služby, u kterých podporuje propojení přes otevřené API. U jednotlivých bank jsou pak evidováni uživatelé aplikace, s kterými je banka propojená, viz `UserBank`.
  - **BankType** ID banky, pod kterým je banka evidována. ID je výčtový typ `enum`, ve kterém jsou zkratky pro jednotlivé banky podporované aplikací. Například pod `BankType cs` lze dohledat v `Bank` Českou spořitelnu.
  - **BankName** Plný název banky.
  - ***ApiKey*** API klíč, který poskytovatel služby dostane od dané banky.



Obrázek 4.1: Databázový model základního prototypu mé aplikace navrženého na základě PSD2 a dokumentace otevřeného API bank.

  - ***BaseUrl*** Základní část URL pro komunikaci s danou bankou.

- **UserBank** Seznam propojených uživatelů a bank. Seznam je tím pádem vázaný na seznam uživatelů `AspNetUsers` a seznam bank `Bank`. Každý uživatel může být svázán pouze jedenkrát s určitou bankou, vícekrát by nedávalo smysl.

  - ***AccessToken*** Přístupový token přidělený danou bankou určený jako „heslo“ pro komunikaci s bankou.
  - ***TokenType*** Typ tokenu, nicméně zaznamenal jsem vždy jenom typ „Bearer“.
  - ***AccessTokenExpirationTime*** Čas platnosti přiděleného přístupového tokenu. Může se banka od banky lišit, není v RTS SCA definováno.
  - ***RefreshToken*** Obnovovací token pro opětovné získání přístupového tokenu. Platnost obnovovacího tokenu by měla být a rozhodně by neměla přesáhnout 90 dní podle RTS SCA.

4.1.2 Model k sdílení účtu

Umožňuje sdílet propojené bankovní účty uživatele na základě IBAN identifikátoru, který se váže k specifickému účtu, nikoliv bance. Bylo by vhodné rozšířit minimálně ještě o specifikaci práv k účtu.

- **UserLink** Eviduje, kdo je vlastníkem účtu a kdo je jeho konzumentem, respektive kdo bude mít přístup k účtům vlastníků. Slouží pouze k propojení uživatelů, výčet bankovních účtů a případných práv se nachází dále v `BankAccountLink`.
  - **Owner** Vlastník jako uživatel aplikace, který poskytuje přístup ke svým účtům konzumentovi.
  - **Consumer** Konzument jako uživatel aplikace, který má přístup k účtům vlastníka.
- **BankAccountLink** Bankovní účty, které jsou sdílené vzhledem k danému propojení evidovanému v `UserLink`.
  - **Iban** Identifikátor účtu IBAN, ke kterému chce vlastník dát přístup konzumentovi.

4.1.3 Systémový model

Tvoří základ frameworku .Net pro správu uživatele aplikace a s tím spojené funkcionality. Jedná se o knihovny poskytnuté v rámci ASP.NET frameworku a jsou tedy spjaté pouze s výběrem technologie pro implementaci, nikoliv s ukázkou využití otevřeného API bank a obecného návrhu aplikace. Nicméně lze samozřejmě dále popsaný model vytvořit od základu v jakékoliv technologii. Model v práci uvádím hlavně kvůli inspiraci, jakým způsobem může být provedeno například oddělení prémiových funkcí přes `AspNetUserClaims`, metody přihlášení do aplikace přes třetí strany s `AspNetUserLogins` nebo obyčejná bezpečnost účtu přes bezpečnostní razítka nebo blokování účtu a mnoho dalšího.

- **AspNetUsers**
  - **Email** E-mail uživatele.
  - **EmailConfirmed** Informace, jestli E-mail uživatele byl ověřený.
  - **PasswordHash** Hash z osoleného hesla uživatele.
  - **SecurityStamp** Náhodná hodnota, která by se měla změnit pokaždé, když dojde ke změně přihlašovacích údajů.
  - **PhoneNumber** Telefonní číslo uživatele.
  - **PhoneNumberConfirmed** Informace, jestli telefonní číslo uživatele bylo ověřené.
  - **TwoFactorEnabled** Informace, jestli je povoleno uživatelem dvoufázové ověření například při přihlášení. Lze nastavit jako výchozí na serveru nebo nechat volbu uživateli - závisí na konkrétní implementaci.

  - **LockoutEndDateUtc** Datum a čas, kdy skončí blokace uživatele. Například po určitém počtu špatných přihlášení.
  - **LockoutEnabled** Informace, jestli je blokace uživatele povolena. Podobně jako u TwoFactorEnabled závisí poté na konkrétní implementaci.
  - **AccessFailedCount** Počet špatných přihlášení uživatele pro účel blokace uživatele.
  - **UserName** Uživatelské jméno uživatele.

- **AspNetUserRoles** Seznam veškerých uživatelů a jejich rolí. Seznam je tím pádem vázaný na seznamy uživatelů `AspNetUsers` a seznamy rolí `AspNetRoles`.

- **AspNetRoles** Seznam dostupných uživatelských rolí, které lze k uživateli přiřadit v `AspNetUserRoles`.

  - **Name** Název role.

- **AspNetUserClaims** Seznam tvrzení uživatele získané ideálně důvěryhodnou stranou. Hodí se například pro oddělení obsahu pro prémiové účty od běžných účtů nebo pro oddělení obsahu pro osoby starších 18 let.

  - **ClaimType** Druh tvrzení. Například „AccountType“ nebo „DateOfBirth“.
  - **ClaimValue** Hodnota tvrzení. Například „premium“ nebo „10.2.1996“.

- **AspNetUserLogins** Seznam dostupných externích přihlášení, přes které se daný uživatel může přihlásit. Například přes Facebook, Google, Twitter a mnoho dalších.

  - **LoginProvider** Název poskytovatele umožňující přihlášení přes jejich službu. Například Facebook.
  - **ProviderKey** Unikátní klíč od poskytovatele externího přihlášení spojený s uživatelem služby poskytovatele. Například klíč od Facebooku spojený s profilem uživatele na Facebooku.
  - **UserId** ID uživatele aplikace z `AspNetUsers`.

4.2 Architektura systému

Aplikaci jsem vytvořil pouze jako serverou část. Pro serverou část jsem použil MVC architekturu. Frontend aplikace je tedy tvořený takzvanými views, které jsou generovány z controlleru, funkční logika aplikace se odehrává v servicech, případně controllech a přes doménový model se řeší data ve spolupráci s databází.

Frontend aplikace je dostupný přes webový prohlížeč. Webovou platformu jsem zvolil, jelikož je jednodušší pro vytvoření funkčního prototypu, než například mobilní platforma, pro zamýšlené pouhého představení otevřeného API postaveného na PSD2. Jak vyplývá z analýzy bankovního trhu v kapitole 1.3, pro komerční užití je jinak vhodnější mobilní platforma. U mobilní platformy se hodí, kromě serverové části, zavést ještě klientskou část, ať už přes tenkého klienta nebo normálního klienta například s REST API.

Kapitola 5

Vytvoření základního prototypu

V kapitole napřed uvedu jaké všechny technologie jsem k vývoji základního prototypu použil. Poté ukáži na ukázce s propojením sandboxu České spořitelny, jak klíčové části otevřeného API fungují vzhledem k ověření komunikace přes OAuth2 a následně komunikace k AISP a PISP.

Pokud čtenář dodrží přesné postupy, bude pro čtenáře snadné vytvořit si rovněž základní prototyp od nuly.

5.1 Výběr technologií

Technologie jsem rozdělil na vývojové prostředí, které je nepodstatné a pak na obecné technologie k implementaci a technologie speciálně využité k otevřenému API, které nemusí být jenom implementační. Technologie vždy uvádím v nadpisu stylem k čemu je technologie dobrá a jak se jmenuje.

5.1.1 Vývojové prostředí

IDE pro vývoj jsem zvolil Visual Studio 2017, jelikož se jedná o výchozí program pro programovací jazyk C# a dle mého názoru nemá smysl zkoumat jiná IDE. Do IDE jsem si ještě doinstaloval doplněk ReSharper Ultimate pro využívání pomůcek z ostatních IDE společnosti JetBrains.

5.1.2 Obecné implementační technologie

ASP.NET webový framework

Pro aplikační server jsem zvolil ASP.NET webový framework[109] postavený na .NET frameworku[110]. .NET framwork slouží vývojářům pro vytváření aplikací pro řadu dostupných platforem – web, mobil, stolní počítač, hry, strojové učení a internet věcí. ASP.NET webový framework slouží pro webovou platformu jakožto soubor nástrojů a knihoven pro vytváření webových aplikací postavených na .NET frameworku. ASP.NET i .NET jsou bezplatné open

source technologie od Microsoftu. Serverové části jsou na OS Windows, Linux a macOS. Technologie využívají jazyky C#, HTML, CSS a JavaScript.

Technologie od Microsoftu jsem zvolil, jelikož jsou opět jedny z nejjednodušších pro vytvoření funkčního prototypu dostupném přes webové rozhraní. Pro účely například mobilní platformy, z důvodů popisovaných v kapitole 4.2, by ASP.NET v C# poté reprezentoval serverou část a komunikoval by řekněme přes REST API s klientskou částí reprezentovanou třeba Android SDK v Javě.

Práce s databází *Entity Framework*

Entity Framework[111] umožňuje vývojářům pracovat s daty v doménových modelech a jejich vlastnostech, zjednodušeně řečeno metodami s gettery a settery.[42] Jedná se tedy o mapovací nástroj mezi objekty a relačními daty (O/RM), díky kterému nemusí vývojáři psát většinu kódu pro přístup k datům uloženým v databázi. Pro dotazy nad databází používá LINQ[43] syntaxi (dotazy[44]), viz ukázka 5.1, kde vyfiltruji z databáze dostupné banky, které uživatel nemá ještě propojené.

```
var availableBanks = db.BankEntities.Where(banks =>
    !currentUserBankEntities
                .Any(userBanks => banks.BankType ==
                    userBanks.BankType));
```

Algoritmus 5.1: Dotazy v LINQ převáděné pomocí Entity Framework do SQL.

Na další ukázce 5.2 lze vidět uložení nového propojení banky s uživatelem. Napřed dojde v konstruktoru objektu z doménového modelu k jeho naplnění, konkrétně objektu `UserBankEntity` (viz 4.1.1), a poté se objekt přidá a uloží do databáze.

```
var linkEntity = new UserBankEntity
                {
                    UserId = CurrentUser.Id,
                    BankType = userBankEntity.BankType,
                    ApplicationUser =
                        db.Users.Find(CurrentUser.Id),
                    BankEntity =
                        db.BankEntities.Find(userBankEntity.BankType),
                    Token = retrievedToken
                };
                db.UserBankEntities.Add(linkEntity);
                db.SaveChanges();
```

Algoritmus 5.2: Práce s Entity Framework pro uložení dat z objektu do databáze.

[42] V angličtině k nalezení pod termínem *properties*.
[43] .NET Language-Integrated Query[112]
[44] V angličtině pod známějším *query*.

Uživatelská oprávnění *Identity* a *Security*

Ke správě uživatele jsem použil nástroj od Microsoft s názvem Identity[113] skládající se ze tří integrovaných částí:

- **Identity.Core** Základ celé správy uživatele.
- **Identity.EntityFramework** Využití O/RM frameworku pro práci s daty vzhledem ke správě uživatele, viz předchozí kapitola Entity Framework.
- **Identity.Owin** Middleware umožňující aplikaci použít cookies k autentizaci, či třetí strany, například Facebook.[114]

Identity od Microsoftu umožňuje řadu funkcionalit jako jsou role nebo tvrzení[45], které jsem již načal v kapitole 4.1.3. Díky rolím můžete části views nebo celé controllery generující views zobrazovat pouze pro některé uživatele pomocí Security[115], která je součástí ASP.NET Core. Příklady atributů Security na základě definovaných rolí a tvrzení v Identity:

- [**Authorize**] Jednoduché ověření – Přístup pro jakéhokoliv ověřeného uživatele.
- [**Authorize(Policy = "tvrzení")**] Ověření podle tvrzení – Přístup pouze pro uživatele splňující dané tvrzení.
- [**Authorize(Roles = "role")**] Ověření podle role – Přístup pouze pro uživatele mající přiřazenou danou roli.

Užití v praxi lze vidět v ukázce 5.3, kde Index view nebude přístupný pro uživatele, který nemá přiřazenou roli premium a od jeho data narození neuplynulo 18 let. Jsou-li atributy a jejich parametry pod sebou, musí být splněny všechny. Je-li více parametrů v jednom atributu, stačí splnit jeden z nich pro přidělení přístupu.

```
[Authorize(Policy = "18")]
[Authorize(Roles = "premiumUser")]
public class UserBankController : Controller
{
     // Access only for users with role premiumUser which
        are claiming, that they are over 18 yers old.
     public async Task<ActionResult> Index()
     {
        return View();
     }
}
```

Algoritmus 5.3: Autorizace uživatele přes role a tvrzení.

[45] V angličtině známěji jako *claims*.

Dynamické webové stránky *Razor*

Razor[116] slouží k vytváření dynamických webových stránek v HTML na základě C# jazyka. Soubory mají příponu .cshtml a bloky kódu začínají pomocí @ a nejsou nijak ukončeny, viz ukázka použití v praxi 5.4, kde se vytvoří stránka s tabulkou, respektive list propojených bank uživatele. Tabulku vytvořenou na stránce lze vidět na obrázku 5.1.

Email	BankName	
alexander.honza@gmail.com	Česká spořitelna	Delete
alexander.honza@gmail.com	Mock Bank	Delete

Obrázek 5.1: Ukázka listu propojených bank uživatele na webové stránce aplikace.

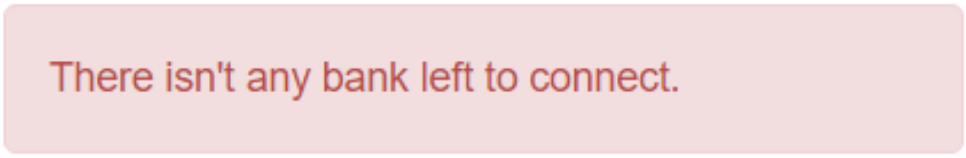
```
<table class="table">
    <tr>
        <th>@Html.DisplayNameFor(model =>
            model.ApplicationUser.Email)</th>
        <th>@Html.DisplayNameFor(model =>
            model.BankEntity.BankName)</th>
    </tr>

    @foreach (var item in Model)
    {
        <tr>
            <td>@Html.DisplayFor(modelItem =>
                item.ApplicationUser.Email)</td>
            <td>@Html.DisplayFor(modelItem =>
                item.BankEntity.BankName)</td>
            <td>@Html.ActionLink("Delete", "Delete", new
                { bankType = item.BankType })</td>
        </tr>
    }
</table>
```

Algoritmus 5.4: Vytvoření dynamické stránky pomocí Razor

Vzhled aplikace *Bootstrap*

Jelikož se jedná pouze o základní prototyp, použil jsem Bootstrap knihovnu.[117] Bootstrap je jedna z nejpopulárnějších knihoven pro frontend, plně responzivní. V rámci ASP.NET se používá ve views, což jsou dynamické HTML stránky vykreslované pomocí Razor popsaného v předchozí kapitole. Na ukázce

5.5 lze vidět mapování přes třídu `alert alert-danger` pro zobrazení červeného boxu na stránce, viz obrázek 5.2.



Obrázek 5.2: Ukázka chybové zprávy (za účelem představení užití Bootstrap) při snaze uživatele propojit aplikaci s další bankou, jelikož již všechny dostupné banky uživatel připojil.

```
<div class="alert alert-danger">
    @TempData["Message"]
</div>
```

Algoritmus 5.5: Využití Bootstrapu pro zobrazení červeného boxu z jejich CSS přes mapování. Jedná se o část kódu z view.

5.1.3 Implementační technologie k využití otevřeného API

Budování URL *Flurl*

Pro komunikaci přes otevřené API, nejenom s bankami, se používá URL odkaz, do kterého vyplníte parametry. Normálně by se musela URL složit z několika stringů různými metodami. Knihovna Flurl[118] skládání URL mnohem usnadňuje díky svým metodám knihovny. Veškeré metody pro skládání URL lze řetězit. Mezi nejpoužívanější metody vzhledem ke komunikacemi s bankami patří:

- `var url = "http://www.some-api.com"` Základní část URL, z které chcete čerpat přes API data.
- `.AppendPathSegment(parametr)` Připojení parametru na konec URL jako segment URL. Bude-li se dále skládat URL, tak přirozeně parametr nebude již na konci URL ale součástí url *https://.../parametr/...*
- `.SetQueryParams(new {nazevParametru1 = hodnotaParametru1, nazevParametru2 = hodnotaParametru2})`
  Nastavení parametrů v dotazech, které jsou v URL na konci za symbolem **?**
  https://...?nazevParametru1=hodnotaParametru1&nazevParametru2=hodnotaParametru2 Jako oddělovače mezi jednotlivými dotazy slouží symboly **&**.

Volání URL *Flurl.Http*

Po složené URL je třeba ještě naplnit HTTP požadavek zbylými daty do hlavičky, eventuálně těla HTTP požadavku, je-li třeba a následně HTTP požadavek odeslat na složenou URL z předchozí kapitoly. K zjednodušení těchto kroků poslouží knihovna Flurl.Http[119], která navazuje řetězově přímo na Flurl knihovnu z předchozí kapitoly. Mezi nejpoužívanější metody vzhledem ke komunikacemi s bankami patří:

- `.WithOAuthBearerToken(token)` Přidání OAuth 2.0 bearer tokenu.
- `.WithHeader(1. hlavička požadavku, 2. hlavička požadavku)` Přidání vyžadovaných hlaviček. Hlavička může být přímo nějaká hodnota nebo proměnná.
- `.GetAsync()` Pošle asynchronně HTTP požadavek přes složené URL a dostane nazpět hrubou HTTP odpověď.
- `.ReceiveJson<Objekt>()` Z těla HTTP odpovědi následně vezme JSON a způsobem popsaným v další kapitole vloží data do vlastností objektu.
- `.PostJsonAsync(Objekt)` Pošle asynchronně HTTP požadavek, kde v těle požadavku bude JSON vytvořený z vlastností objektu, opět viz kapitola dále.

Serializace a deserializace JSON *Newtonsoft.Json*

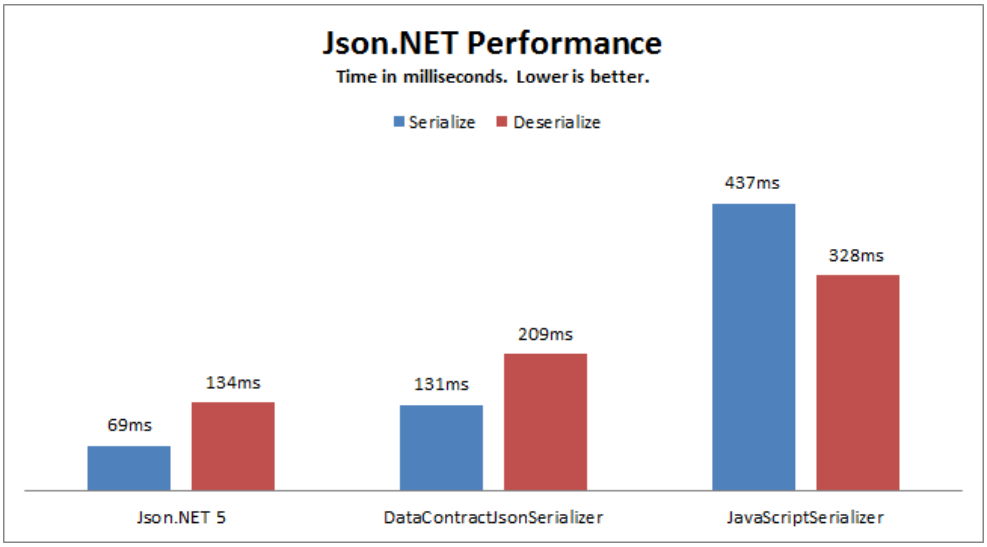
V předchozí kapitole jsem ukazoval komunikaci přes API s JSON, nicméně data v .NET jsou v objektech. Mezi JSON a objekty musí tedy fungovat nějaký převod:

- **Serializace** Převod JSON do vlastností objektu.
- **Deserializace** Převod vlastností objektu do JSON.

.NET má pro tyto účely třídu DataContractJsonSerializer v systémové knihovně. Nicméně existují i rychlejší řešení (viz obrázek 5.3), například knihovna Json.NET od společnosti Newtonsoft.[120]

5.1.4 Další technologie vzhledem k otevřenému API

V předchozích kapitolách jsem uvedl technologie, které jsem použil k implementaci. Jednalo se zejména o frameworky a knihovny. Nicméně pro implementaci se velmi hodí minimálně ještě jeden nástroj.



Obrázek 5.3: Srovnání rychlosti serializace a deserializace JSON mezi použitou Json.NET knihovnou, která je nalevo a konkurencí napravo. Menší hodnoty jsou lepší.

Vygenerování objektu na základě JSON *JSON Utils*

Generátor objektů JSON Utils na základě JSON je webová služba. Tělo HTTP odpovědi, které je v JSON, nástroj snadno převede do objektu v jazyce C#. Vstupy pro převod:

- Jazyk, ve kterém se z JSON vytvoří objekt. V mém případě C#.
- Název objektu.
- Atributy vlastností. V mém případě JsonProperty.
- JSON text, tedy jakékoliv tělo HTTP odpovědi nebo URL.

Vygenerování lze vidět v následující ukázkách JSON 5.6 → objekty 5.7.

```
{"JsonNameProperty1": "hodnota",
"JsonNameProperties": [ "JsonNameProperty2": hodnota ]}
```

Algoritmus 5.6: JSON pro ukázku vygenerování objektů z daného JSON za pomoci nástroje JSON Utils.

```
public class ListOfObjects
{
        [JsonProperty("JsonNameProperty1")]
        public string JsonNameProperty1 { get; set; }
```

```
        [JsonProperty("JsonNameProperties")]
        public IList<ObjectInList> JsonNameProperties {
            get; set; }
}

public class ObjectInList
{
        [JsonProperty("JsonNameProperty2")]
        public int JsonNameProperty2 { get; set; }
}
```

Algoritmus 5.7: Vygenerované objekty na základě JSON pomocí nástroje JSON Utils.

5.2 Ukázky použití otevřeného bankovního API

K ukázkám použiji jako protistranu například Českou spořitelnu, která poskytuje na stránkách *https://developers.erstegroup.com* sandbox, eventuálně po schválení bankou produkční prostředí, má-li žadatel již vyřízenou licenci u ČNB. Sandbox ve skutečnosti není až příliš sandboxem, jelikož na HTTP požadavky vrací API České spořitelny zamockované data.

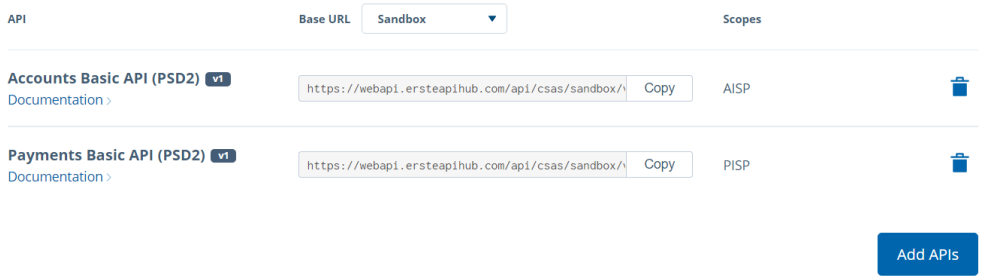
5.2.1 Nastavení sandboxu České spořitelny

Po vytvoření projektu jsem si vybral, přes jaké všechny API chci v aplikaci s Českou spořitelnou komunikovat. Na výběr jsem měl z následujících:

- **Accounts Basic API (PSD2)** – Základní informace o účtech definované PSD2, tedy čtení – AISP.
- **Payments Basic API (PSD2)** – Inicializování základních plateb z účtů definovaných PSD2, tedy čtení a psaní – PISP.
- **Corporate Accounts API** – Detailní informace ohledně jakéhokoliv typu účtu vedených středními nebo většími firmami.
- **Exchange rates API** – Kurzovní lístek České spořitelny, současný nebo historický až dva roky zpátky.
- **Know-your-customer API** – Verifikace uživatelů na základě tokenu, jestli jsou klienty České spořitelny.
- **Mortgage calculator API** – Umožňuje integrovat hypotéční kalkulačku České spořitelny do jiných aplikací.
- **Personal Accounts API** – Detailní informace ohledně jakéhokoliv typu účtu vedených osobami nebo malými firmami.

- **Places API** – Detailní informace o více jak 560 pobočkách a 1 600 bankomatech, například GPS lokace, adresy, otevírací doby apod.
- **Transparent accounts API** – Umožňuje integrovat transparentní účet do jiných aplikací.

Pro účely DP jsem si přidal AISP a PISP API. Obě API jsou pro moji aplikaci třeba, proto jsem v rozsahu zaškrtl, že AISP i PISP jsou mojí aplikací vyžadovány, nikoliv dobrovolné nebo zcela nepoužívané. Na základě výběru API a prostředí Sandbox jsem obdržel **základní URL** pro API, viz obrázek 5.4.



Obrázek 5.4: Souhrn přidaných APIs v projektu u České spořitelny v sandbox prostředí.

Pro komunikaci jsou potřeba dané základní **URLs**:

- **AISP** *https://webapi.ersteapihub.com/api/csas/sandbox/v1/account-information*
- **PISP** *https://webapi.ersteapihub.com/api/csas/sandbox/v1/payment-initiation*

V nastavení u České spořitelny pro mojí aplikaci, viz obrázek 5.5, je pro mě další důležitá hodnota **API klíč** pro sandbox prostředí, konkrétně *4b7142e5-3fe1-4fe6-ac68-270d1c6eb71a*. Ještě jednou je zde shrnuto, jaký rozsah po České spořitelně požaduji.

Obrázek 5.5: Nastavení pro mojí aplikaci u České spořitelny.

Nyní to jsou všechny údaje, které potřebuji, abych mohl v čistě serverové části aplikace (odhlédnu od toho, že v mém projektu žádná klientská část není, pouze frontend) vyplnit konstruktor objektu `UserBankEntity`, viz ukázka 5.8. Díky naplněné inlinecodeUserBankEntity klíčovými vlastnostmi může nyní moje serverová aplikace komunikovat s Českou spořitelnou přes API.

```
var newBank = new BankEntity
{
        BankType = BankType.Cs,
        BankName = "Ceska sporitelna",
        ApiKey = "4b7142e5-3fe1-4fe6-ac68-270d1c6eb71a",
        BaseUrl =
            "https://webapi.ersteapihub.com/api/csas/sandbox/v1"
};
db.BankEntities.Add(newBank);
```

Algoritmus 5.8: Konstruktor a ukládání objektu UserBankEntity do DB které slouží k uložení banky a klíčových vlastností pro komunikaci s Českou spořitelnou přes API.

Jak je možné si v kódu všimnout, jako základní URL využívám necelou. Takhle můžu URL použít jak pro AISP, tak pro PISP. Nakonec přidám pro rozlišení pouze *account-information* pro AISP nebo *payment-initiation* pro PISP.

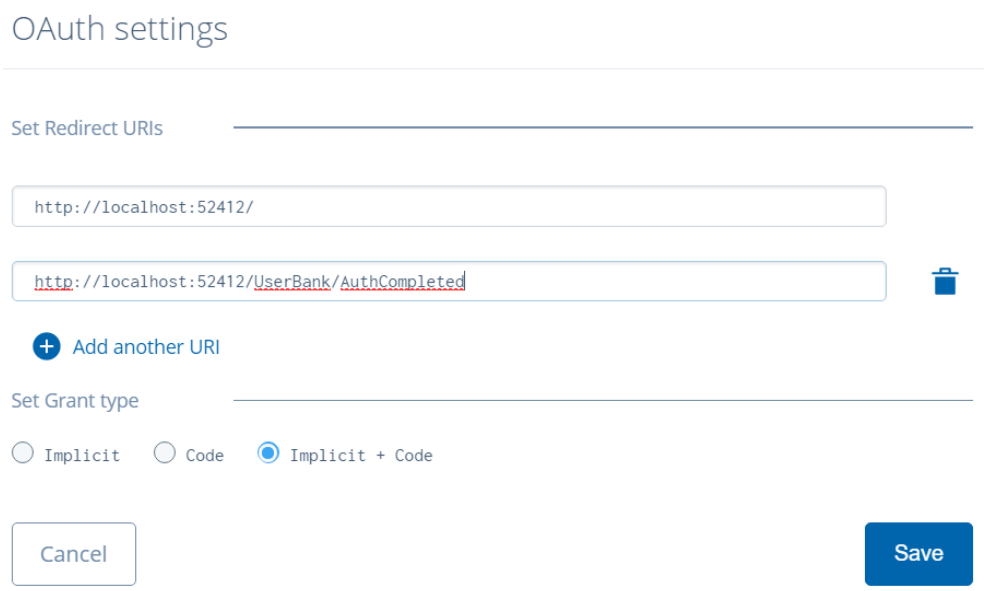
Kromě nastavení komunikace na obou stranách je zapotřebí u České spořitelny, viz obrázek 5.6, nastavit ještě OAuth2, konkrétně nastavit seznam URL, na které je možné ze stránek České spořitelny vůči aplikaci přesměrovávat, a vybrat typ přístupu:

- **Implicit** - Jednorázový přístupový token.
- **Code** - Přístupový token a token určený k obnovování přístupového tokenu.

5.2.2 Ověření uživatele a získání oprávnění

V předchozím bodě jsem nastavil komunikaci serveru aplikace vůči serveru České spořitelny. Další krok pro využití dat některých z klientů je zapotřebí získat nějakou formou přístup k účtu uživatele u banky. Pro účely oprávnění k uživatelskému účtu klienta banky používá Česká spořitelna framework pro oprávnění OAuth2. Více OAuth2 probírám v kapitole 2.3.6.

Popíši typ přístupu přes kód, jelikož implicitní typ přístupu je prakticky stejný, jenom zkrácený. Jak už jsem zmínil, sandbox České spořitelny není úplně sandboxem v pravém slova smyslu, takže první dva kroky v mé ukázce lze otestovat až na produkčním prostředí České spořitelny, tudíž následující ukázky algoritmů jsou pouze částečně otestované.



Obrázek 5.6: Editace nastavení OAuth2 pro mojí aplikaci u České spořitelny.

1) Přesměrování uživatele na OAuth2 přihlašovací stránku

produkční prostředí

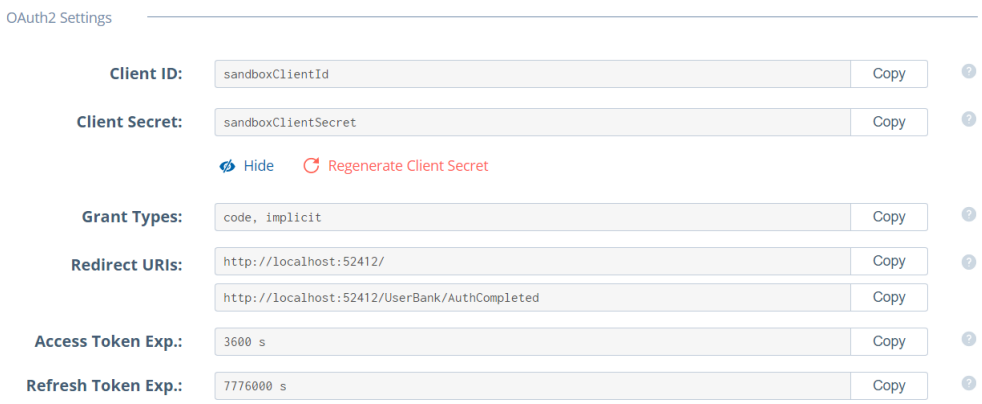
Jakmile si uživatel při procesu propojování banky vybere banku k propojení, vrátím v metodě controlleru přesměrování na stránky České spořitelny, viz 5.9.

```
return RedirectToAction("https://bezpecnost.csast.csas.cz/
mep/fs/fl/oauth2/auth?
state=csas-auth&
redirect_uri=http://localhost:52412/UserBank/AuthCompleted&
client_id=sandboxClientId&
response_type=code&
access_type=offline&
approval_prompt=force");
```

Algoritmus 5.9: Přesměrování uživatele po výběru banky k propojení na stránky banky – konkrétně České spořitelny. Jedná se o jednu URL pro lepší přehled rozdělenou do řádků po parametrech.

Důležité parametry a odkud jsem jsem vzal:

- **state** – Libovolný řetězec pro ověření, že na konci procesu se vrátí stejný řetězec. Kvůli identifikaci při více probíhajících ověřeních najednou.
- **redirect_uri** – Základ by měl být stejný dle nastavení OAuth2 v České spořitelně, kam jsem si nastavil *http://localhost*, viz obrázek 5.7.



Obrázek 5.7: Přehled nastavení OAuth2 pro mojí aplikaci u České spořitelny.

- **client_id** – ID mojí aplikace v České spořitelně, viz obrázek 5.7.

Dobrovolné parametry, které lze nastavit:

- **scope** – Typy API, které chci uživateli poskytnout. Jako výchozí poskytne všechny nastavené, viz obrázek 5.7.
- **language_id** – V jakém jazyce má být stránka s OAuth2 pro uživatele.

2) Získání kódu z přesměrování *produkční prostředí*

Česká spořitelna uživatele přesměruje na `http://localhost:52412/UserBank/AuthCompleted?code=returned-code&state=csas-auth`, jelikož jsem takovou URL požadoval v přesměrování, viz 5.9, a URL je mezi schválenými u České spořitelny, viz obrázek 5.7. Následně vyextrahuji kód z URL pomocí `var code = Request.QueryString["code"];` za předpokladu, že se vrácený řetězec `state` rovná tomu v HTTP požadavku v předchozím kroku. Kód je platný pouze pár minut, takže s dalším krokem se nesmí otálet.

3) Výměna kódu za přístupový a obnovovací token *produkční i testovací prostředí*

Po získání kódu mohu požádat Českou spořitelnu o přístupový a obnovovací token, viz algoritmus 5.10.

```
await (_baseUrl + "/sandbox-idp/token")
        .WithHeader("Content-Type",
            "application/x-www-form-urlencoded")
        .PostUrlEncodedAsync(new
        {
```

```
                grant_type = "authorization_code",
                code = code,
                client_id = "sandboxClientId",
                client_secret = "sandboxClientSecret"
        })
        .ReceiveJson<UserBankAuthentication>();
```

Algoritmus 5.10: Požadavek na přístupový a obnovovací token.

Další důležité parametry, které jsou potřeba až teď, a odkud jsem jsem vzal:

- **grant__type** – Typ přístupu. Požaduji přístup přes kód.
- **client__secret** – Tajný kód mé aplikace u České spořitelny, viz obrázek 5.7. Tajný kód nesmí být nikomu prozrazen a musí být držen pouze na serverové části aplikace. Z důvodu bezpečnosti lze u České spořitelny tajný kód i obměnit.

Na základě odpovědi si pak uložím z JSON do objektu svázaného s uživatelem a bankou `UserBankEntity` získaný přístupový token `access_token` s určenou platností na hodinu a obnovovací token `refresh_token` s určenou platností 90 dní, viz obrázek 5.7. Expirační časy nelze nijak editovat, nastavuje si je banka.

V odpovědi v JSON Česká spořitelna vrací ještě expirační dobu přístupové tokenu, nicméně připadá mi zbytečné čas ukládat. Stačí při HTTP požadavku uživatele odchytit špatnou HTTP odpověď banky kvůli neplatnému přístupovému tokenu a na základě toho přístupový token obnovit, viz další krok. Dále ještě vrací typ tokenu, který jsem si ale nevšiml, že by byl někdy jiný kromě typu `bearer`, proto nikam neukládám. Jako poslední vrací typy povolených API pro uživatele, ale opět mi připadá zbytečné ukládat, jelikož seznam chtěných API k povolení vím již z mého HTTP požadavku.

4) Použití obnovovacího tokenu k získání nového přístupového tokenu *produkční i testovací prostředí*

Odchytím-li při HTTP požadavku uživatele, že mu vypršel přístupový token, zažádám si pomocí obnovovacího tokenu o nový přístupový token, viz algoritmus 5.11. Od prvotního získávání tokenů z předchozího kroku se liší hodnota parametru přístupu na `refresh_token` a za kód zaměním parametr `refresh_token` s hodnotou obnovovacího tokenu, kterou získám z entity propojení mezi daným uživatelem a bankou, tedy `userBankEntity`.

```
await (_baseUrl + "/sandbox-idp/token")
        .WithHeader("Content-Type",
            "application/x-www-form-urlencoded")
        .PostUrlEncodedAsync(new
        {
```

```
grant_type = "refresh_token",
refresh_token =
    userBankEntity.RefreshToken,
client_id = "sandboxClientId",
client_secret = "sandboxClientSecret"
})
.ReceiveJson<NewAccessToken>();
```

Algoritmus 5.11: Požadavek na nový přístupový token na základě obnovovacího tokenu.

Nicméně v sandboxu se přístupový token vrací vždy `test-token`, takže čtvrtý krok není pro testování nutný.

Kdy a jak zažádat o nové tokeny

Při každém HTTP požadavku uživatele by se měl kontrolovat vrácený kód stavu v HTTP odpovědi.

Vrátí-li se od České spořitelny kód `403 UNAUTHORISED`, který znamená chybějící nebo špatný přístupový kód, je třeba zažádat o nový přístupový kód, viz krok 4 v předchozí kapitole.

Obdobně se bude kontrolovat HTTP odpověď u procesu získávání nového přístupového tokenu kvůli kontrole vypršení obnovovacího tokenu. Vrátí-li se při tomto procesu od České spořitelny kód `401 UNAUTHORISED`, který znamená chybějící nebo špatný obnovovací kód, je třeba provést celé ověření uživatele, respektive klienta banky, znovu od kroku jedna v předchozí kapitole.

5.2.3 Ukázka AISP

AISP České spořitelny podporuje získání následujících dat:

- Seznam účtů uživatele (osobní, spořící, v cizí měně a další).
- Zůstatek na účtu uživatele.
- Transakční historie účtu uživatele.

HTTP odpovědi vrací v těle ve formátu JSON.

V mé práci ukáži AISP na seznamu účtů uživatele, jelikož rozepisovat kód všech možností API pro AISP by bylo příliš dlouhé. Nicméně v mé aplikace lze rovněž vypsat historii transakcí. Zůstatek na účtu zobrazuji přímo v listu účtů. Ukázku z aplikace lze vidět na obrázku 5.8.

Česká spořitelna v rámci dotazů v URL u HTTP požadavku na list účtů umožňuje:

- stránkování, parametry:
  - `size` pro počet účtů na stránku

BankAccountIdentification	Currency	Servicer	Name|18N	Product|18N	Bank Account Balance	Payments
Iban CZ1208000000000259459101 Other 259459101	CZK	BankCode 0800 CountryCode CZ Bic GIBACZPX	Jiří Spokojený	Osobní účet ČS II	48923.15	Pay by iban | Pay by email
Iban CZ4108000000000782553098 Other 782553098	CZK	BankCode 0800 CountryCode CZ Bic GIBACZPX	Jiří SPokojený - CM	Cizoměnový účet		Pay by iban | Pay by email

Obrázek 5.8: Ukázka listu veškerých bankovních účtů propojených bank uživatele na webové stránce aplikace.

  - `page` pro požadované číslo stránky

- řazení, parametry:
  - `sort` podle čeho se list má třídit
  - `order` jakým směrem se má list seřadit

Příklad lze vidět v algoritmu 5.12.

```
private const string TracingKey = "WEB-API-key";
public async Task<BankAccountList>
    ListUserAccounts(string token)
{
        try
        {
                return await (_baseUrl +
                    "/account-information/my/accounts")
                .SetQueryParams(new
                {
                        size = 100,
                        page = 0,
                        sort = "iban",
                        order = "desc"
                })
                .WithOAuthBearerToken(token)
                .WithHeader(TracingKey, _apiKey)
                .GetAsync()
                .ReceiveJson<BankAccountList>();
        }
```

```
        catch (FlurlHttpException)
        {
                return new BankAccountList();
        }
}
```

Algoritmus 5.12: Požadavek na list účtů uživatele u jedné banky. Volání metody opakuji pro každou propojenou banku uživatele.

Další důležité parametry a odkud jsem jsem vzal:

- **Typ tokenu a jeho hodnota** – Požadovaný je bearer. V algoritmu 5.12 využívám rovnou Flurl metodu bearer autorizací, do které vkládán potřebný přístupový token `.WithOAuthBearerToken(accessToken)`.
- **API klíč** – Parametr s názvem `WEB-API-key` a hodnotou klíče, který mám v aplikaci od České spořitelny, viz obrázek 5.5.

Obecně dotazy v URL do HTTP požadavku se liší API od API a ještě ke všemu banka od banky. Je proto nutné zkoumat poskytnutou dokumentaci od banky k jednotlivým API. Alespoň bankovní terminologie se drží podle ISO 20022 standardu, viz kapitola 1.2.10. Česká spořitelna obecně umožňuje pro základní třídění dat (v závislosti na datech):

- Stránkování
- Řazení
- Filtrování

V aplikaci odchytávám HTTP odpovědi a při špatném požadavku účet nevypíši, viz algoritmus 5.12. Bez odchytávání HTTP odpovědí by se nevypsal celý list, ačkoliv by chyba nastala například jenom u jedné banky. Po odchycení HTTP odpovědi by ideálně mělo nastat řada procesů v závislosti na typu odpovědi. Je-li odchycená odpověď 401 nebo 403, lze zkusit provést procesy popsané v předchozí kapitole 5.2.2 „Kdy a jak zažádat o nové tokeny“.

5.2.4 Ukázka PISP

Data pro PISP se posílají v JSON, takže používám deserializaci, viz knihovna popsaná v kapitole 5.1.3.

Zadání platby v aplikaci umožňuji buď podle IBAN nebo dle emailu emailu jiného uživatele, viz volby na obrázku 5.8. Nicméně pro vytvoření platby ve výsledku vždy odesílám HTTP požadavek s IBAN.

Ve všech HTTP požadavcích opět nezapomenout na:

- `.WithOAuthBearerToken(token)` – přístupový token uživatele.
- `.WithHeader("WEB-API-key", _apiKey)` – parametr WEB-API-key s API klíčem od ČS, viz obrázek 5.5.

1) Vytvoření platby

Z view formuláře vyplněného uživatelem naplním objekt `PaymentViewModel`. Nejedná se o entitu, kterou bych přes O/RM ukládal do databáze nebo kamkoliv jinam kromě RAM. Stejně tak by měl dělat kdokoliv jiný, aby naplnil požadavky definované směrnicí PSD2 pro PISP, viz kapitola 2.3.4. Data o platbě pro PISP se České spořitelně posílají v rámci HTTP požadavku v jeho těle. Proto v následujícím kroku použiji deserializaci, viz knihovna popsaná v kapitole 5.1.3. Nyní platbu vytvořím přes HTTP požadavek, viz algoritmus 5.13.

```
public async Task<CreatePaymentResponse>
    CreatePayment(CreatePaymentRequest request, string
    token)
{
return await (_baseUrl +
    "/payment-initiation/my/payments")
         .WithOAuthBearerToken(token)
         .WithHeader(TracingKey, _apiKey)
         .PostJsonAsync(request)
         .ReceiveJson<CreatePaymentResponse>();
}
```

Algoritmus 5.13: Vytvoření platby s parametry v JSON

Pro vytvoření platby je podobný HTTP požadavek jako u AISP. Liší se přidanou metodou `.PostJsonAsync(request)`, v které se musí poslat docela obsáhlý JSON s vyplněnými atributy dle typu platby:

- Domácí platba.
- SEPA platba, více o SEPA v kapitole 2.2.
- SWIFT platba.[46]
- Platba do Ruska.

V rámci HTTP odpovědi je důležité získat ID platby `signId` v `signInfo` pro další krok.

2) Autorizace platby

Autorizace platby se skládá z několika kroků:

[46]SWIFT je systém pro mezinárodní platby po celém světě.

I) Zjištění typu autorizace Napřed zjistím, jaké autorizaci platba podléhá. Je-li k dispozici více možností, dám uživateli na výběr. K zjištění dostupných možností autorizace přidám do URL v rámci HTTP požadavku **ID platby k autorizaci** `.AppendPathSegment(signId)` získané z HTTP odpovědi v předchozí kapitole (algoritmus 5.14). Poté přesměruji aplikaci na potřebný view vzhledem k typu autorizace. U ČS je výběr z:

- OTP obdržené přes SMS – `TAC` - podporuje moje aplikace.
- Autorizace přes mobilní aplikaci – `MOBILE_CASE`.
- Bez další autorizace – `NO_AUTHORIZATION`.

```
public async Task<SigningInit> DetailSigning(string
    signId, string token)
{
return await (_baseUrl +
    "/payment-initiation/my/payments/sign/")
  .AppendPathSegment(signId) // ID platby k autorizaci
  .WithOAuthBearerToken(token)
  .WithHeader(TracingKey, _apiKey)
  .PostAsync(null)
  .ReceiveJson<SigningDetail>(); // typ autorizace, stav
     autorizace
}
```

Algoritmus 5.14: První krok u autorizace platby - zjištění typu autorizace.

II) Zahájení autorizace platby Pro zahájení autorizace musím zaslat HTTP požadavek (algoritmus 5.15) stejný jako v předchozím kroku, ale rozšířený o JSON s parametrem **typu autorizace** a nepřijde-li nějaká výjimka, přesměruji aplikaci na view s procesem dané autorizace.

OTP obdržené přes SMS Přesměruji uživatele na view s formulářem pro vyplnění hesla, které uživatel obdrží od České spořitelny přes SMS.

```
public async Task<SigningInit> InitSigning(string signId,
    string token)
{
return await (_baseUrl +
    "/payment-initiation/my/payments/sign/")
  .AppendPathSegment(signId) // ID platby k autorizaci
  .WithOAuthBearerToken(token)
  .WithHeader(TracingKey, _apiKey)
  .PostJsonAsync(request) // typ autorizace
  .ReceiveJson<SigningInit>(); // typ autorizace, stav
     autorizace, stav sms
}
```

Algoritmus 5.15: Druhý krok u autorizace platby - inicializace autorizace.

III) Finalizace autorizace platby Odešlu HTTP požadavek (algoritmus 1.3.3) jako v předchozích bodech, akorát JSON bude obsahovat parametry kromě typu autorizace ještě **OTP**. V HTTP odpovědi dostanu stav autorizace.

- `OPEN` – Autorizace stále probíhá.
- `DONE` – Autorizace skončila v pořádku a platba se provedla, respektive zařadila se do plánovaných operací, viz problematika clearingu v kapitole 1.2.6 a příklad fungování clearingu v ČR v kapitole 1.3.3.

OTP obdržené přes SMS Do parametru pro heslo vložím OTP heslo vyplněné uživatelem ze SMS.

```
public async Task<SigningInit> FinalizeSigning(string
    signId, string token)
{
return await (_baseUrl +
    "/payment-initiation/my/payments/sign/")
  .AppendPathSegment(signId) // ID platby k autorizaci
  .WithOAuthBearerToken(token)
  .WithHeader(TracingKey, _apiKey)
  .PostJsonAsync(request) // typ autorizace, OTP (heslo)
  .ReceiveJson<SigningFin>(); // stav autorizace
}
```

Algoritmus 5.16: Třetí krok u autorizace platby - finalizace autorizace.

5.3 Shrnutí vytvoření základního prototypu

Pro používání otevřeného API doporučuji využívat řadu knihoven, které jsem v kapitole vyjmenoval – hlavně pro práci s JSON a HTTP požadavky. Neumí-li čtenář v jazycích pro mobilní platformy, doporučuji si naprogramovat prototyp v ASP.NET. Měl jsem již například zkušenosti s frameworkem Spring postaveným na Javě z bakalářské práce, ale daná technologie je výrazně složitější. Tím ale určitě netvrdím, že by C# byl nutně vhodnější řešení na serverové části v produkčním řešení. Bavím se čistě o prototypu.

U každé banky bude mít společnost účet na jejich vývojářském portálu, kde je nezbytně nutné provést základní nastavení:

- Výběr rozsahu – PISP, AISP a další.
- Nastavení URLs k přesměrovávání.

- Nastavení OAuth2 autorizace – implicitní nebo kódové nebo kombinace.

a získat potřebné údaje pro komunikaci:

- URLs pro jednotlivé rozsahy – PISP, AISP a další.
- API klíč.
- Klientské ID.
- Klientský tajný kód.

Kapitola 6

Vyhodnocení vývoje FinTech aplikace

V poslední kapitole se pokusím na základě zkušeností z vývoje vlastní FinTech aplikace, kterou jsem popisoval v předchozí kapitole, nastínit, kolik tvorba nejenom prototypu může zabrat času. Srovnán částečně dostupné dokumentace bank k jejich otevřenému API a jaký to bohužel bude mít dopad na náročnost vývoje.

Na základě analýzy trhu, náročnosti vývoje a připravenosti bank zhodnotím ze svého pohledu potenciál FinTech aplikací s příchodem PSD2.

A pokud čtenáře například potenciál těchto aplikací přesvědčí také k tvorbě vlastní FinTech aplikace, shrnu sadu doporučení pro jejich vývoj.

6.1 Náročnost vývoje

Nejtěžší na vývoji FinTech aplikace využívající otevřené bankovní API bylo navrhnout rozumnou architekturu, která je plně připravená na rozšiřování zejména kvůli přidávání podpory nových bank. Jak jsem například uvedl v kapitole 3.2.2, Trustly podporuje propojení pro platby s více jak 3000 bankami napříč Evropou. Časová náročnost propojení nové banky tedy v případě vývoje FinTech aplikace hraje velkou roli. Například v mém řešení neefektivně řeším URL pro HTTP požadavky, jejichž struktura se bude banka od banky lišit, nicméně já připojuji na konec URL statický text od ČS. Kromě zmíněného mi ale pro propojení banky teoreticky stačí naplnit entitu s bankou a upravit objekty pro serializaci/deserializaci JSON.

Proč teoreticky? Zde se dostávám k velkému problému u otevřeného API bank – každá banka má své API dost odlišné, jelikož RTS nepopisuje technologické detaily (viz kapitola 2.3.6), a dle mého názoru ani nejlepší architektura to nezachrání. Výčet některých razantnějších odlišení při porovnávání dokumentací bank k otevřenému API, zejména dokumentace mezi ČS a AirBank:

- Operace s listem (kapitola 5.2.3). Například od jedné banky můžete historii transakcí filtrovat, u jiné už ale ne. Šlo by možná zlepšit ukládáním si k bankám, jaké operace u jednotlivých listů podporují.
- Některé banky nepodporují získat list plánovaných operací, ba dokonce ani vyhledat stav jednou zadané platby dle ID. Naráží na obrovský problém kontroly stornování platby v jejím průběhu, který jsem popisoval u PayPal vs. Trustly v kapitole 3.2.1 .
- Některé banky nepodporují PISP. Ale asi se jedná o dočasný problém.
- JSON v HTTP odpovědi se u každé banky drobně liší. Dle mého názoru nelze nijak ošetřit. Je nutné mít připravené objekty pro serializaci/deserializaci pro každou banku zvlášť. Odhadovaná pracnost 1 MD vývoje + testy, eventuálně méně, pokud aplikace bude umět nějakou formou vlastní překladač z JSON do C# (viz kapitola 5.1.4) v reálném čase.

Celková moje pracnost na prototypu dle záznamů dosahuje 100 hodin čistého času, přičemž se jedná pouze o základní prototyp umožňující:

- Bezpečné přihlášení do aplikace, připravené pro dvoufázové ověření.
- Připojení nové banky.
- Výpis všech účtů včetně zůstatku.
- Transakční historie všech účtů.
- Zadání platby podle emailu nebo IBAN včetně dalších detailů potřebných k platbě, včetně OTP banky.
- Sdílení účtů s dalšími uživateli aplikace.

Nejvíce náročné bylo vypořádat se s architekturou mezi entitou uživatele a entitou banky. Dále bylo náročné připravit mocky pro otestování funkcionalit, které při propojení jedné banky nestačí. Mocky je totiž třeba připravit na jiném serveru, aby šlo komunikaci přes API řádně otestovat. Samotná komunikace přes API pak patří mezi ty snadnější části, pokud se používají vhodné knihovny.

6.2 Potenciál FinTech aplikací

Potenciál FinTech aplikace mají určitě. Závisí ale v jaké kategorii, jelikož každá FinTech kategorie je dost rozdílná, i z pohledu případného zisku. Dále závisí na počtu již stávající konkurence v dané kategorii, jelikož jak jsem již řekl, FinTech je tu s námi od roku 2000. PSD2 pouze usnadňuje a zlepšuje bezpečnost komunikace s bankami.

6.2.1 AISP

Například pro AISP si lze v kapitole 3.2.4 povšimnout, že i přes to, jak dlouho jsou na trhu, co všechno jejich aplikace nabízí, včetně moderního designu, tak je společnost sotva v zisku. V kategorii správy osobního financí a plánování osobního financí moc příležitostí nevidím.

Data tak budou sloužit spíše k hodně specifickým účelům a nepůjde tolik o zdroje z uživatele samotného, ale o zdroje z jím poskytnutých dat, které se využijí pro další účely, pokud to směrnice PSD2 nějakou formou umožní.

6.2.2 PISP

Pro PISP vidím mnohem více příležitostí a to ve několika směrech.

Samostatná platební služba

Jedna z příležitostí se mi jeví založit vlastní platební službu, například využívající platby přes QR kódy. Tento druh služby je například velmi oblíbený v Číně, který dominuje v platbách přes mobilní telefon, viz kapitola 3.1. Platby by díky tomu byly stejně rychlé jako v případě platebních karet. Obchodníky by motivovalo využití těchto služeb kvůli nižším poplatkům, které jsou v současné době v řádu několika procent, viz kapitola 2.3 ohledně obecného procesu platby platební kartu a kapitola 3.2 ohledně konkrétních FinTech aplikací.

Integrované platební služby obchodníků

Větší obchodníci, kteří snadno splní podmínky pro získání licence u ČNB, si mohou PISP implementovat sami a tím se kompletně vyhnout jakékoliv třetí straně, kterým by platily procentuální poplatky za využití platební služby. Pro zákazníka obchodu se nic nezmění, ale obchodníkům se tím razantně zvedne marže, která se dnes ponižuje o zmíněné poplatky při platbě kartou. Implementaci nemusí ani provádět přímo obchodník, může využít služby dodavatele poskytující hotová řešení jako jsou například šablony e-shopů.

Platební služby v rámci sociálních sítí

PISP může dále usnadnit převody mezi samotnými lidmi. Kdyby sociální síť propojila účty uživatelů s bankami a využívala jak AISP, tak PISP, mohla by umožnit odesílat platby jenom na základě jiného uživatele v kontaktech – bez jakéhokoliv složitého vyplňování čísla účtu a instantně nezávisle na bance obou uživatelů.

6.3 Sada doporučení pro vývoj aplikace využívající otevřené API PSD2

Postupoval bych v následujících krocích:

1. Zjistil bych si něco o FinTech a prozkoumal celý trh. FinTech aplikací je na trhu obrovské množství v mnoha kategoriích. Svět FinTech není založený jenom na platbách a už vůbec ne na správě osobních financí – ty jsou jenom špička ledovce, viz kapitola 1.3.4 a kapitola 3.2.
2. Zjistil bych si v rychlosti, co je vlastně PSD2, viz kapitola 2.3.
3. Zhruba bych si nastudoval, co je třeba pro získání licence u ČNB. Licence pro AISP je mnohonásobně snazší, než licence pro PISP, kde musíte disponovat minimálním kapitálem 20 000 EUR, viz kapitola 2.3.7.
4. Naprogramoval bych si prototyp využívající veškeré možnosti otevřeného API, například v doporučeném ASP.NET, viz kapitola 5 a využil ideálně z některých dostupných sandboxů bank.
5. Provedl bych hlubokou analýzu trhu.
6. Nastudoval bych si, co všechno mi nařizuje RTS SCA a CSC z PSD2, viz kapitola 2.3.6.
7. Na základě analýzy navrhl a naprogramoval prototyp již konkrétní aplikace, rovnou bych připravoval aplikaci na fungování v celém EHP, viz kapitola 1.3.3 – český trh je příliš malý, vhodný maximálně pro PISP.
8. Zažádal bych si o licenci u ČNB, abych mohl aplikaci otestovat na produkčním prostředí – například na svých bankovních účtech.

Závěr

Cílem mé diplomové práce bylo vytvořit prototyp bankovní aplikace využívající otevřené bankovní API vycházející ze směrnice PSD2. Na základě prototypu následně navrhnout sadu doporučení pro ostatní vývojáře, respektive návod, pro vývoj dalších aplikací využívající výhody směrnice PSD2.

Abych mohl analyzovat aktuální trh bankovních aplikací, popsal jsem ze široka jak vlastně bankovní trh vznikl a jak vypadá v současnosti. Vydefinoval jsem pojem FinTech, který pokrývá bankovní aplikace.

V analýze trendů přístupu k zákazníkům jsem se zaměřil na současné moderní technologie, která bankovní trh nabízí a zhodnotil jejich bezpečnostní rizika, jejichž znalost byla zásadní pro pochopení záměru a analýzy PSD2. Zjistil jsem, že hlavním záměrem je skutečně bezpečnost, jak avizuje směrnice Evropské unie a to z důvodu velmi velkého objemu podvodů rostoucího s čím dále větší oblíbeností FinTech aplikací, zejména platebních služeb a z důvodu potencionálně nebezpečné screen scraping technologie, která bude směrnicí PSD2 zakázána.

Analyzoval jsem samotnou směrnici PSD2 a její časování, než přijde v platnost kompletní směrnice z důvodu teprve nedávno Evropským parlamentem schválených technologických standardů pro silně zabezpečenou autorizaci, které jsem v mé práci ještě stihl aktualizovat k aktuálním požadavkům. Dále jsem analyzoval dopady směrnice na bankovní trh vzhledem k stávajícím aplikacím, ale i vzhledem k příležitostem pro vznik nových aplikací.

Na základě získaných znalostní o bankovním trhu a PSD2 jsem analyzoval již současná řešení platebních služeb a agregačních služeb, jejich bezpečnost a nutná opatření i příležitosti vzhledem k směrnici PSD2.

V druhé části práce jsem na základě bankovního trhu, jeho analýzy a analýzy směrnice PSD2 vytvořil základní prototyp aplikace ukazující jak AISP, tak PISP v praxi v napojení na API České spořitelny.

Ze zkušeností vývoje prototypu jsem napsal návod pro další vývojáře a zhodnotil náročnost vývoje takové aplikace, která minimálně z pohledu prototypu není příliš náročná. Návod a zhodnocení by mělo vývojářům pomoci

nejenom pro samotný vývoj, ale rozhodnout se, jestli vůbec má smysl bankovní aplikace vyvíjet vzhledem k tomu, co všechno s vývojem aplikace je spojené, zejména náročné legislativní podmínky a nejednotné API bank.

Literatura

[1] Credit Cards Compare: Credit Cards History (The History of Credit Cards). [cit. 2017-12-30]. Dostupné z: https://www.creditcardscompare.co.nz/credit-cards/

[2] The Telegraph: A history of banking: from coins to pings. Červen 2015, [cit. 2017-12-30]. Dostupné z: https://www.telegraph.co.uk/sponsored/finance/your-bank/10912973/history-banking-early-coins-contactless.html

[3] Gerardo Capiel, V. C.: Say hello to a better way to pay, by Google. Únor 2018, [cit. 2018-5-6]. Dostupné z: https://www.blog.google/topics/shopping-payments/say-hello-to-google-pay/

[4] IBM: Mainframes working after hours: Batch processing. 2010, [cit. 2018-02-25]. Dostupné z: https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zmainframe/zconc_batchproc.htm

[5] Financial Fraud Action UK: Fraud The Facts 2017. Září 2017, [cit. 2018-02-24]. Dostupné z: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf

[6] European Payments Council: Map of SEPA Scheme Countries and Territories. 2016, [cit. 2018-02-01]. Dostupné z: https://www.europeanpaymentscouncil.eu/document-library/other/map-sepa-scheme-countries-and-territories

[7] Ernst & Young: EY FinTech Adoption Index 2017. 2017, [cit. 2018-04-17]. Dostupné z: http://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/$FILE/ey-fintech-adoption-index-2017.pdf

[8] Hoggson, N. F.: *Banking Through the Ages*. New York : Dodd, Mead & Company, 1926, ISBN 1602061998, [cit. 2017-12-29]. Dostupné z: https://archive.org/details/bankingthroughag00hogg

[9] Jones, C.: The history of paper money [online]. *Financial Times*, září 2013, [cit. 2017-12-29]. Dostupné z: https://www.ft.com/content/f11c6126-1a39-11e3-93e8-00144feab7de

[10] Gilbart, J. W.: *The history and principles of banking*. London : Longman, 1837. Dostupné z: https://archive.org/details/historyprinciple00gilb

[11] Pohl, M.: *Handbook on the History of European Banks*. Elgar Original Reference Series, E. Elgar, 1994, ISBN 9781781954218. Dostupné z: https://books.google.cz/books?id=eXvfNDHpfWwC

[12] BNP Paribas: A brief history of banking. Únor 2016, [cit. 2017-12-30]. Dostupné z: https://group.bnpparibas/en/news/history-banking

[13] TietoCorporation: History of Banking. Prosinec 2016, [cit. 2017-12-29]. Dostupné z: https://www.youtube.com/watch?v=sN_17yVDj80

[14] PDM: What Is a Wire Transfer & How Do They Work? Prosinec 2017, [cit. 2017-12-30]. Dostupné z: https://www.veem.com/wire-transfers/international-wire-transfer/

[15] Mayyasi, A.: How Credit Cards Tax America. Leden 2016, [cit. 2017-12-30]. Dostupné z: https://www.veem.com/wire-transfers/international-wire-transfer/

[16] Milligan, B.: The man who invented the cash machinea. Červen 2007, [cit. 2017-12-30]. Dostupné z: http://news.bbc.co.uk/2/hi/business/6230194.stm

[17] Nye, C.: How Direct Debit began in the UK. Duben 2014, [cit. 2017-12-30]. Dostupné z: https://www.youtube.com/watch?v=HLpIbRLi_x4

[18] wiseGEEK: What is Telephone Banking? [cit. 2017-12-31]. Dostupné z: http://www.wisegeek.com/what-is-telephone-banking.htm

[19] The Telegraph: First Online Home Shopping: 1984! Květen 2013, [cit. 2017-12-31]. Dostupné z: https://www.zdnet.com/article/first-online-home-shopping-1984/

[20] Tilden, E.: A Detailed History of Debit Cards. Červenec 2017, [cit. 2017-12-31]. Dostupné z: https://pocketsense.com/detailed-history-debit-cards-5462528.html

[21] Millward, D.: Don't bank on credit card security in the USA. Květen 2016, [cit. 2017-12-31]. Dostupné z: https://www.telegraph.co.uk/expat/money/dont-bank-on-credit-card-security-in-the-usa/

[22] Gemalto: Contactless payment: how it works. [cit. 2017-12-31]. Dostupné z: https://www.gemalto.com/financial/cards/contactless/how-it-works

[23] Olson, J.: A Brief History Of EMV Technology. Červen 2017, [cit. 2017-12-31]. Dostupné z: https://fattmerchant.com/blog/brief-history-emv-technology/

[24] Pilcher, J.: Infographic: The History Of Internet Banking (1983 – 2012). Říjen 2012, [cit. 2017-12-31]. Dostupné z: https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/

[25] Sarreal, R.: History of Online Banking: How Internet Banking Went Mainstream. Říjen 2017, [cit. 2017-12-31]. Dostupné z: https://www.gobankingrates.com/banking/history-online-banking/

[26] eWise: A PIONEER OF FINANCIAL DATA AGGREGATION. [cit. 2017-12-31]. Dostupné z: http://www.ewise.com

[27] Moneris: A 30-Second History Lesson in Contactless Payments [Infographic]. Listopad 2015, [cit. 2017-12-31]. Dostupné z: https://insights.moneris.com/payment-news-trends/a-30-second-history-lesson-in-contactless-payments-infographic

[28] Triggs, R.: What is NFC & how does it work? Leden 2018, [cit. 2018-5-6]. Dostupné z: https://www.androidauthority.com/what-is-nfc-270730/

[29] Trends, D.: How to use Google Pay and Google Pay Send. Březen 2018, [cit. 2018-3-11]. Dostupné z: https://www.digitaltrends.com/mobile/how-to-use-google-pay/

[30] Sýkora, F.: Jednoduché placení mobilem dobývá Česko. Google Pay spustí další banky, chystají i alternativu. Duben 2018, [cit. 2018-5-6]. Dostupné z: https://zpravy.aktualne.cz/finance/sluzba-google-pay-pro-bezkontaktni-platby-telefonem-se-osved/r~b1d325da38da11e885e30cc47ab5f122/

[31] ČNB: O ČNB. 2003, [cit. 2018-02-24]. Dostupné z: https://www.cnb.cz/cs/o_cnb/

[32] Amadeo, K.: Central Banks' Function and Role [online]. *The Balance*, leden 2018, [cit. 2018-01-10]. Dostupné z: https://www.thebalance.com/what-is-a-central-bank-definition-function-and-role-3305827

[33] Amadeo, K.: Open Market Operations [online]. *The Balance*, prosinec 2017, [cit. 2018-01-10]. Dostupné z: https://www.thebalance.com/open-market-operations-3306121

[34] Horton, M.: The 9 Major Financial Institutions. Březen 2018, [cit. 2018-3-30]. Dostupné z: https://www.investopedia.com/ask/answers/061615/what-are-major-categories-financial-institutions-and-what-are-their-primary-roles.asp

[35] ČNB: Platební instituce a instituce elektronických peněz, poskytovatelé platebních služeb malého rozsahu a vydavatelé elektronických peněz malého rozsahu. [cit. 2018-3-17]. Dostupné z: https://www.cnb.cz/cs/dohled_financni_trh/legislativni_zakladna/platebni_instituce_a_instituce_el_penez/

[36] Stuchlíková & Partners: Vydavatelé elektronických peněz malého rozsahu. Květen 2016, [cit. 2018-3-17]. Dostupné z: https://www.stuchlikova.com/cs/aktuality/vydavatele-elektronickych-penez/

[37] Stuchlíková & Partners: Poskytovatelé platebních služeb malého rozsahu. Květen 2016, [cit. 2018-3-17]. Dostupné z: https://www.stuchlikova.com/cs/aktuality/poskytovatele-platebnich-sluzeb-maleho-rozsahu/

[38] JUDr. Ing. Otakar Schlossberger, P.: Kdo může poskytovat platební služby. [cit. 2018-3-17]. Dostupné z: https://www.stuchlikova.com/cs/aktuality/poskytovatele-platebnich-sluzeb-maleho-rozsahu/

[39] Amadeo, K.: Securities and Their Effect on the U.S. Economy. Leden 2018, [cit. 2018-3-11]. Dostupné z: https://www.thebalance.com/securities-definition-and-effect-on-the-u-s-economy-3305961

[40] Hanák, M.: Cenné papíry. Únor 2001, [cit. 2018-3-11]. Dostupné z: https://www.epravo.cz/top/clanky/cenne-papiry-1785.html

[41] Maverick, J.: What is the difference between a bill of exchange and a promissory note? [cit. 2018-3-11]. Dostupné z: https://www.investopedia.com/ask/answers/042415/what-difference-between-bill-exchange-and-promissory-note.asp

[42] Business Center: businesscenter.cz. 2018, [cit. 2018-02-02]. Dostupné z: https://business.center.cz/business/pojmy/

[43] ČNB: Popis systému CERTIS. 2017, [cit. 2018-02-24]. Dostupné z: https://www.cnb.cz/cs/platebni_styk/certis/certis_popis.html

[44] Investopedia: Clearing House. [cit. 2018-02-24]. Dostupné z: https://www.investopedia.com/video/play/clearing-house/

[45] Japan Securities Clearing Corporation: Netting. [cit. 2018-02-24]. Dostupné z: https://www.jpx.co.jp/jscc/en/cash/cash/assumption-obligation/netting.html

[46] Investopedia: Real Time Gross Settlement. [cit. 2018-02-24]. Dostupné z: https://www.investopedia.com/terms/r/rtgs.asp

[47] business.gov.au: Choosing payment methods. Květen 2018, [cit. 2018-5-6]. Dostupné z: https://www.business.gov.au/Info/Run/Finance-and-accounting/Payments-and-invoicing/Choosing-payment-methods

[48] IBM: What is batch processing? 2010, [cit. 2018-02-25]. Dostupné z: https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zconcepts/zconc_whatisbatch.htm

[49] HelpSystems: Batch Processing: How It Evolved and How Your Business Benefits. březen 2017, [cit. 2018-02-25]. Dostupné z: https://www.helpsystems.com/resources/articles/batch-processing-how-it-evolved-and-how-your-business-benefits

[50] ISO 20022 Registration Authority: About ISO 20022. [cit. 2018-02-25]. Dostupné z: https://www.iso20022.org/faq.page

[51] Norris, E.: Retail Banking vs. Corporate Banking. Leden 2018, [cit. 2018-3-11]. Dostupné z: https://www.investopedia.com/articles/general/071213/retail-banking-vs-commercial-banking.asp

[52] ČNB: Ceník peněžních a obchodních služeb České národní banky, Část V. leden 2017, [cit. 2018-02-25]. Dostupné z: https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/o_cnb/hospodareni/cenik/cenik_cast_V.pdf

[53] Bureš, M.: Víte, kdo vlastní vaši banku? Ital, Rus, Rakušan, nebo Čech? srpen 2017, [cit. 2018-03-30]. Dostupné z: https://www.finance.cz/496071-kdo-vlastni-ceske-banky/

[54] Oberbank AG: Oberbank Shares. prosinec 2017, [cit. 2018-04-01]. Dostupné z: https://www.oberbank.com/oberbank-shares

[55] Equa bank: Consolidated annual report 2016. 2016, [cit. 2018-04-01]. Dostupné z: https://m.equabank.cz/download/1019-vz-equabank-2016-en.pdf

[56] Banka CREDITAS: Povinně uveřejňované informace k 30. 9. 2017 - 1 (XSLX) (XLSX, 1,11 MB). září 2017, [cit. 2018-04-01]. Dostupné z: https://www.creditas.cz/povinne-uverejnovane-informace

[57] J&T Banka: Povinně uveřejňované informace k 30. 9. 2017, příloha 1, datum zveřejnění - 13. 11. 2017. listopad 2017, [cit. 2018-04-01]. Dostupné z: https://www.jtbank.cz/informacni-povinnost/

[58] Prchalová, K.: Komu patří banky? Z padesátky společností je českých třetina. únor 2016, [cit. 2018-04-01]. Dostupné z: https://www.mesec.cz/clanky/komu-patri-banky/

[59] finance.cz: Seznam komerčních bank. [cit. 2018-04-01]. Dostupné z: https://www.finance.cz/ucty-a-sporeni/seznamy-a-adresare/komercni-banky/

[60] Fio banka: Historie společnosti. [cit. 2018-04-01]. Dostupné z: https://www.fio.cz/o-nas/fio-banka/historie

[61] Banka CREDITAS: Představení Banky CREDITAS. [cit. 2018-04-01]. Dostupné z: https://www.creditas.cz/predstaveni-banky

[62] Hello bank!: O BNP PARIBAS. [cit. 2018-04-01]. Dostupné z: https://www.hellobank.cz/paticka/povinne-informace-o-nas/

[63] Bubák, Z.: Výsledky bank za rok 2017. Největší zisk měla ČSOB následovaná Českou spořitelnou a Komerční bankou. březen 2018, [cit. 2018-04-02]. Dostupné z: http://www.finparada.cz/4921-Vysledky-bank-za-rok-2017.aspx

[64] Banka CREDITAS: Banka CREDITAS a.s., Výroční zpráva 2017. březen 2018, [cit. 2018-04-02]. Dostupné z: https://www.creditas.cz/documents/20705/68155/Výroční+zpráva_20180321.pdf/d3ebd159-709d-46cd-a62a-d22ae409b284

[65] Pokorný, O.: Banky podle velikosti? Počty klientů a aktiva v roce 2018! únor 2018, [cit. 2018-03-30]. Dostupné z: https://www.duofinance.cz/banky-cr-podle-poctu-klientu

[66] Olga Skalková, D. C.: Banky ruší část svých poboček. Stále více Čechů do nich přestává chodit. březen 2018, [cit. 2018-03-30]. Dostupné z: https://infografiky.ihned.cz/pobocky-banky/r~f7f1552e31c211e8a72bac1f6b220ee8/

[67] Mašek, F.: Přiměje konkurenční boj velké banky zvednout úročení spořicích i termínovaných účtů? leden 2018, [cit. 2018-03-30]. Dostupné z: http://www.finparada.cz/4839-Primeje-konkurencni-boj-velke-banky-zvednout-uroceni-sporicich-i-terminovanych-uctu.aspx

[68] Sovová, E.: Věrnost jedné bance se už nenosí, nové banky dál zvyšují počty klientů. únor 2018, [cit. 2018-03-30]. Dostupné z: https://finance.idnes.cz/analyza-nove-banky-pocty-klientu-inovace-novy-trend-f9d-/sporeni.aspx?c=A180222_114720_sporeni_sov

[69] Marr, B.: A Very Brief History Of Blockchain Technology Everyone Should Read. Únor 2018, [cit. 2018-5-6]. Dostupné z: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#643f6c0b7bc4

[70] LANDERS, R.: How FinTech Is Changing Business (and Bank Accounts). Únor 2017, [cit. 2018-04-10]. Dostupné z: https://www.business.com/articles/how-fintech-is-changing-business-and-bank-accounts/

[71] Harris, L.: Card not present transactions – the absolute basics for merchants. Březen 2018, [cit. 2018-03-30]. Dostupné z: https://www.mobiletransaction.org/card-not-present-transactions/

[72] GoCardless: Screen scraping 101: Who, What, Where, When? Červenec 2017, [cit. 2018-02-25]. Dostupné z: https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712

[73] Wright, M.: The Difference Between AML and KYC. Říjen 2016, [cit. 2018-02-25]. Dostupné z: https://www.linkedin.com/pulse/difference-between-aml-kyc-malcolm-wright-finstlm

[74] Zakrzewski, C.: Anonymous Leaked A Massive List Of Passwords And Credit Card Numbers. [cit. 2018-02-25]. Dostupné z: https://techcrunch.com/2014/12/27/anonymous-leaked-a-massive-list-of-passwords-and-credit-card-numbers/

[75] AO Kaspersky Lab: Internet Banking Security to Keep Fraudsters Away. [cit. 2018-02-25]. Dostupné z: https://usa.kaspersky.com/resource-center/preemptive-safety/internet-banking-security-keep-fraudsters-away

[76] Australia and New Zealand Banking Group Limited: Internet Banking Security. [cit. 2018-02-25]. Dostupné z: http://www.anz.com/auxiliary/security-centre/fraud-security-centre/protection/internet-banking-security/

[77] Fiserv: Security Guidelines and Best Practices for Internet Banking for Precision and Cash Management for Precision. Březen 2013, [cit. 2018-02-25]. Dostupné z: https://www.fiserv.com/resources/13-0305_Security_Guidelines_and_Best_Practices_Online_Banking_for_Precision.pdf

[78] Moore, M.: 4 DIFFERENT TYPES OF POINT OF SALE SOLUTIONS. Září 2016, [cit. 2018-02-25]. Dostupné z: http://www.bnasmartpayment.com/blog/4-different-types-of-point-of-sale-solutions

[79] European Parliament, Council of the European Union: Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. 2007, [cit. 2018-01-31]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007L0064

[80] EFTA: European Economic Area (EEA) / Relations with the EU. 1994, [cit. 2018-01-31]. Dostupné z: http://www.efta.int/eea/eea-agreement

[81] European Commission: Single euro payments area (SEPA). [cit. 2018-03-11]. Dostupné z: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en

[82] Treasury Today: SEPA payment instruments [online]. *Treasury Today*, březen 2008, [cit. 2018-02-01]. Dostupné z: http://treasurytoday.com/2008/03/sepa-payment-instruments

[83] European Payments Council: Questions and Answers on the SEPA Instant Credit Transfer Scheme. listopad 2017, [cit. 2018-03-10]. Dostupné z: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2017-11/EPC090-16%20v2.0_QA_SCT%20Inst%20scheme_Updated%20November%202017.pdf

[84] European Payments Council: PSD2 Explained. listopad 2017, [cit. 2018-04-29]. Dostupné z: https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2017-11/EPC_Infographic_PSD2_March-2017_Updated%20November%202017.pdf

[85] European Parliament, Council of the European Union: Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions. [cit. 2018-03-11]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0751

[86] Hervé, R.: STET PSD2 API Documentation. [cit. 2018-03-12]. Dostupné z: https://www.stet.eu/assets/files/PSD2/API-DSP2-STET_V1.2.3_final.pdf

[87] GoPay: Z čeho se skládá poplatek při platbě kartou? [cit. 2018-03-18]. Dostupné z: https://help.gopay.com/cs/tema/podminky-a-ceny/aktualni-podminky/z-ceho-se-sklada-poplatek-pri-platbe-kartou

[88] Light, J.; McFarlane, A.; Barry, K.; aj.: Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive. 2016, [cit. 2018-03-18]. Dostupné z: https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive.pdf

[89] Ernst & Young Accountants LLP: Payment Services Directive 2 for FinTech & Payment Service Providers. [cit. 2018-03-18]. Dostupné z: http://www.ey.com/Publication/vwLUAssets/EY-payment-services-directive-2/$FILE/EY-payment-services-directive-2.pdf

[90] HSBC: Payment Services Directive II (PSD2). 2017, [cit. 2018-03-18]. Dostupné z: http://www.gbm.hsbc.com/-/media/gbm/reports/insights/payment-services-directive-ii-psd2.pdf

[91] European Payments Council: Understanding the final regulatory technical standards. listopad 2017, [cit. 2018-03-29]. Dostupné z: https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-04/rts-infographic_April%202018.pdf

[92] Hay, T.: The PSD2 Final RTS: 10 Things You Need to Know. duben 2017, [cit. 2018-03-29]. Dostupné z: https://gomedici.com/psd2-final-rts-10-things-you-need-to-know/

[93] Anicas, M.: An Introduction to OAuth 2. červenec 2014, [cit. 2018-03-30]. Dostupné z: https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

[94] Parlament České republiky: Zákon č. 370/2017 Sb. leden 2018, [cit. 2018-03-30]. Dostupné z: https://www.mesec.cz/zakony/zakon-o-platebnim-styku/uplne/

[95] PwC: The communication between Third Party Providers and Banks. 2016, [cit. 2018-03-26]. Dostupné z: https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n02.pdf

[96] Bubák, Z.: Bankovní revoluce je tu: Účty od více bank od teď můžete obsluhovat z jednoho místa. leden 2018, [cit. 2018-03-26]. Dostupné z: http://www.finparada.cz/4822-Bankovni-revoluce-je-tu-Ucty-od-vice-bank-v-jedne-aplikaci.aspx

[97] Bubák, Z.: Air Bank se připojila ke třem bankám nabízejícím bankovní rozhraní třetím stranám. říjen 2017, [cit. 2018-03-26]. Dostupné z: http://www.finparada.cz/4668-Air-Bank-se-pripojila-k-bankam-nabizejici-bankovni-rozhrani-tretim-stranam.aspx

[98] Bubák, Z.: Banka CREDITAS spouští API. Klientská data tak budou k dipozici FinTech společnostem a IT oddělením firemních klientů banky. říjen 2017, [cit. 2018-03-26]. Dostupné z: http://finparada.cz/4642-Banka-CREDITAS-spousti-API-Klientska-data-tak-budou-k-dispozici-FinTech-firmam-a-dalsim.aspx

[99] Ma, Y. J.: Why Open Data Is Good For China. Březen 2017, [cit. 2018-04-21]. Dostupné z: https://gijn.org/2017/03/28/why-open-data-is-good-for-china/

[100] PayPal: PayPal. 2018, [cit. 2018-04-21]. Dostupné z: https://www.paypal.com

[101] Trustly: Trustly. 2018, [cit. 2018-04-21]. Dostupné z: https://trustly.com

[102] Turula, T.: Fintech startup Trustly was just acquired by a Swedish PE firm - with a huge jump in valuation. Březen 2018, [cit. 2018-04-21]. Dostupné z: https://nordic.businessinsider.com/a-hyped-startup-that-had-20000-swedes-apply-for-095-mortgages-just-cleared-a-major-regulatory-hurdle--/

[103] TransferWise: TransferWise. 2018, [cit. 2018-04-21]. Dostupné z: https://transferwise.com/

[104] Kharpal, A.: Western Union rival TransferWise says it will record its second year of profit. Březen 2018, [cit. 2018-04-21]. Dostupné z: https://www.cnbc.com/2018/03/21/transferwise-says-it-will-record-a-profit-in-its-2018-fiscal-year.html

[105] Budín, J.: Jak na zahraniční platby? Duben 2017, [cit. 2018-04-21]. Dostupné z: https://www.banky.cz/clanky/jak-na-zahranicni-platby/

[106] BudgetBakers: Wallet. 2018, [cit. 2018-04-22]. Dostupné z: https://budgetbakers.com

[107] Brejčák, P.: Infografika: Jak se daří BudgetBakers a aplikaci Wallet, kterou si stáhlo již 1,6 milionu lidí. Únor 2017, [cit. 2018-04-22]. Dostupné z: https://tyinternety.cz/startupy/infografika-jak-se-dari-budgetbakers-a-aplikaci-wallet-kterou-si-stahlo-jiz-16-milionu-lidi/

[108] Optimizely: Heatmap. 2018, [cit. 2018-04-22]. Dostupné z: https://www.optimizely.com/optimization-glossary/heatmap/

[109] Microsoft: ASP.NET Web Framework and Tools 2017. 2017, [cit. 2018-04-27]. Dostupné z: https://www.asp.net/

[110] Microsoft: .NET. 2017, [cit. 2018-04-27]. Dostupné z: https://www.microsoft.com/net/

[111] opensource: Entity Framework. 2017, [cit. 2018-04-27]. Dostupné z: https://github.com/aspnet/EntityFramework6/wiki

[112] Microsoft: Language Integrated Query (LINQ). 2017, [cit. 2018-04-27]. Dostupné z: https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/concepts/linq/

[113] Microsoft: ASP.NET Core Identity. 2015, [cit. 2018-04-27]. Dostupné z: https://github.com/aspnet/Identity

[114] opensource: Welcome to Katana. 2018, [cit. 2018-04-27]. Dostupné z: https://github.com/aspnet/AspNetKatana/

[115] opensource: ASP.NET Security. [cit. 2018-04-27]. Dostupné z: https://github.com/aspnet/AspNetKatana/

[116] Microsoft: Razor. 2018, [cit. 2018-04-27]. Dostupné z: https://getbootstrap.com

[117] The Bootstrap Authors, Twitter Inc.: Bootstrap. 2018, [cit. 2018-04-27]. Dostupné z: https://getbootstrap.com

[118] Menier, T.: Flurl. 2018, [cit. 2018-04-27]. Dostupné z: http://tmenier.github.io/Flurl/fluent-url/

[119] Menier, T.: Flurl.Http. 2018, [cit. 2018-04-27]. Dostupné z: http://tmenier.github.io/Flurl/fluent-http/

[120] Newton-King, J.: Json.NET. 2018, [cit. 2018-04-27]. Dostupné z: https://www.newtonsoft.com/json

Příloha **A**

Seznam použitých zkratek

XML Extensible markup language

AISP Account Information Service Providers

AML Anti-money laundering

API Application programming interface

ASPSP Account Servicing Payment Service Providers

BIC Bank Identifier Code

ČNB Česká národní banka

CNP Card not present transaction

ČR Česká republika

ČS Česká spořitelna

CSC Common and secure communication

ČSOB Československá obchodní banka

DDoS Distributed Denial of Service

EHP Evropský hospodářský prostor

EMW Europay MasterCard and Visa

EU Evropská unie

EUR Euro

EY Ernst & Young

FinTech Finanční Technologie

GBP Britská libra

GPS Global Positioning System

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IBAN International Bank Account Number

ID Identity

IT Informační technologie

KB Komerční banka

KYC Know your customer

LINQ Language Integrated Query

O/RM Object-relational mapping

OTP One-time password

PEPS Politically exposed person

PISP Payment Initiation Service Providers

POS Point of sale transaction

PSD Payment services directive

PSD2 Payment services directive 2

PSU Payment service user

Q Kvartál

RTS Regulatory technical standards

SAR Suspicious activity report

SCA Strong customer Authentication

SEPA Single Euro Payments Area

SQL Structured Query Language

SWIFT Society for Worldwide Interbank Financial Telecommunications

TTP Third party providers

UK United Kingdom

URL Uniform Resource Locator

VB Velká Británie

XML eXtensible Markup Language

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `exe` ..... adresář se spustitelnou formou implementace
- `src`
  - `Psd2ConceptDiplomaThesis` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
- `Excel` ..... zdrojové data pro tabulky a grafy ve formátu XLSX
  - `Banky_klienti` ..... klienti bank, zisk bank
  - `Banky_prehled` ..... přehled bank v ČR
  - `exchangeRates` ..... kurzy měn TransferWise, PayPal a bank
  - `FinTechAdoption` ..... adaptace FinTech na bankovním trhu
  - `ukFrauds` ..... míra podvodů ve VB