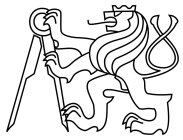
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Bankovní platforma pro provádění Peer to Peer plateb
Student:	Bc. Petr Pešta
Vedoucí:	Ing. Pavel Krejčí
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2016/17

Pokyny pro vypracování

Vymezte pojem „peer to peer“ plateb v kontextu běžného platebního styku i nových platebních metod. Zmapujte současný stav služeb pro provádění P2P plateb v ČR, EU, USA a Asii, a to z pohledu bankovních a i nebankovních subjektů. Vyberte několik existujících platforem, zhodnoťte klíčové faktory jejich úspěchu a popište jejich použitelnost v ČR. Ve vybrané bance navrhněte platformu pro provádění P2P plateb. Analyzujte příležitosti a hrozby spojené s implementací – ze strany banky i uživatele. Navrhněte vhodné začlenění platformy do distribučních kanálů. Odhadněte náklady na implementaci a spuštění této platformy a stanovte způsob měření úspěchu platformy na trhu. Analyzujte a posuďte bezpečnostní rizika spojená s ověřováním identity, finančními podvody a dalšími hrozbami, spojenými se zavedením této platformy. Výstupem práce bude studie hodnotící možnosti, přínosy a rizika spojená s vytvořením platformy pro provádění P2P plateb ve vybrané organizaci, a to včetně návrhu této platformy.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 2. února 2016

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra Softwarového Inženýrství

Diplomová práce

Bankovní platforma pro provádění Peer to Peer plateb

Bc. Petr Pešta

Vedoucí práce: Ing. Pavel Krejčí

8. ledna 2017

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, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

Praha dne 8. ledna 2017 .....

Odkaz na tuto práci

Pešta, Petr. *Bankovní platforma pro provádění Peer to Peer plateb.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2017.

Abstrakt

Tato diplomová práce se zabývá tématem peer to peer plateb. Hlavním cílem je provést analýzu poskytovatelů P2P služeb v zahraničí a navrhnout vhodné řešení pro implementaci v dané bance. Zároveň je nutné zhodnotit všechna úskalí, která průběh projektu doprovází a uvést jejích řešení.

Klíčová slova P2P, platba, trh, služba, banka, bezpečnost, aplikace

Abstract

This diploma thesis is dealing with peer to peer payments. The main goal of the work is to analyze service providers in abroad and propose corresponding solution for implementation in given bank. It is necessary to evaluate all riscs which follow the project and propose their solution too.

Keywords P2P, payment, market, service, bank, security, application

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V současné době postupuje rozvoj technologií neuvěřitelným tempem a stává se čím dál více dostupný široké veřejnosti. Z principu fungování trhu je jasné, že s rostoucí poptávkou roste i nabídka. Proto i bannkovní sektor musí na tyto výzvy reagovat a dříve než konkurence. Nejinak tomu je v případě P2P plateb. Jedná se o službu, která v zahraničí již nějakou dobu funguje a nabízí se tedy otázka, zda by tato služba mohla fungovat i v českém prostředí a za jakých podmínek. Odpovědět na tuto otázku je jedním z cílů této diplomové práce. Po provedené nezbytné analýzy následuje průzkum trhu, který představuje nejznámější služby, princip jejich fungování a úskalí jejich provozu. Tyto poznatky jsou dále aplikovány na prostředí českého trhu. V rámci tohoto projektu je třeba stanovit základní postup při implementaci služby, zhodnotit klíčová rizika a jejich řešení a navrhnout platformu pro provozování P2P plateb.

Kapitola 1

Analýza

Pro účely této práce je nutné nejprve uvést nezbytné definice a pojmy, které s touto prací úzce souvisí. Cílem této kapitoly je vysvětlit pojmy peníze a platba a ukázat jejich historický vývoj. Blíže se seznámit se samotným procesem platby, zejména platby bezhotovostní. V další kapitole pak definujeme a blíže rozebereme hlavní téma této práce, P2P platby.

1.1 Peníze a jejich vývoj

Peníze můžeme definovat jako statek, který ve společnosti slouží jako všeobecně přijímaný prostředek směny, tedy tzv. platidlo a v dnešní době jsou téměř nepostradatelné. Peníze představují společného jmenovatele, na který lze převést odlišné statky jako např. lidská práce, surovinové zdroje či kapitálové vybavení. Dále mají schopnost zprostředkovat a usnadnit směnné akty. V neposlední řadě uchovávají hodnoty v čase (mohou být použity v budoucnu). V makroekonomické rovině jsou peníze vyjádřeny jako aktiva, která mají vysokou likviditu a zároveň jsou spojeny s nízkou mírou výskytu rizik. Jestliže peníze ztrácejí svoji hodnotu, lidé jim přestávají věřit a raději zvolí jinou formu bohatství (cenné papíry, pozemky, atd.) [1].

Formy peněz:

- Plnohodnotné (komoditní) peníze – jejich hodnota je založena na hodnotě kovu, ze kterého byly raženy (měď, stříbro, zlato)
- Papírové peníze a mince z obecného kovu – náhrada plnohodnotných peněz
- Elektronické peníze – elektronické bankovnictví, kreditní karta

Peníze začaly vznikat postupně s rozvojem dělby práce, směny a obchodu, avšak přesné období vzniku není známo. Už v pravěku lidé směňovali různé

druhy zboží za jiné (kůže, zvěř, nástroje, atd.). Postupem času se začaly zvyšovat požadavky a potřeby lidí, množství statků narostl a tím vznikla i směna zboží za zboží, které bylo na jedné straně přebytečné a na druhé nedostačující. Jedná se tedy o směnný obchod neboli barter, který v omezené míře funguje dodnes.

1.1.1 Barterový obchod

Barter můžeme chápat jako tzv. směnu zboží, služeb či produktů bez využití peněz. Barterové obchody jsou považovány za nejzákladnější formu kompenzačních obchodů. Před vznikem peněz, jakožto univerzálního prostředku směny, bylo barterové obchodování jedinou možností jak uskutečnit obchod. Výhodou tohoto typu obchodu je, že platidlo, v tomto případě zboží, má stále svou reálnou hodnotu. Naopak nevýhodou tohoto typu platby je potřeba tzv. dvojí shody, která by vyhovovala oběma stranám. Prodávající musí najít takového vhodného kupujícího, který nabízí dané zboží a zároveň by byl ochotný přijmout i jeho produkt. I dnes dochází k tomuto druhu obchodu, a to ve společnostech, kde neexistují peněžní prostředky anebo tam, kde je z důvodu vysoké inflace nestálá měna. Postupem času k jednoduššímu obchodování napomohly „zbožové peníze“, které tento problém částečně vyřešily.

1.1.2 Zbožové peníze

Zbožové (komoditní) peníze měly svou vnitřní hodnotu nezávislou na peněžní (směnné) funkci. Řadily se mezi ně drahé kovy (zlato a stříbro), neboť se dají snadno dělit a v malém množství je obsažena velká hodnota. Dále pak další komodity jako kůže, mušle či vzácné kameny. V historii plnily funkci peněz, kdy je lidé určité skupiny státního celku obchodovali svým zbožím. Nevýhodou komoditních peněz byla však v některých případech nízká trvanlivost, přenosnost mezi trhy nebo dělitelnost, kromě kovů.

1.1.3 Mince

Mincovní systém se spojuje s oběhem plnohodnotných mincí z drahého kovu, zejména zlatých a stříbrných mincí či mincí z platiny. Jejich množství bylo omezeno zásobami drahých kovů, které měly jednotlivé země k dispozici. Ražba mincí byla zpravidla výsadou panovníka. Kolem roku 600 př. n. l. na dnešním území Turecka vznikl první předchůdce mincí. Jednalo se o přírodní slitinu stříbra a zlata, do které byl vyražen obrázek vyjadřující hodnotu této mince. Důvodem proč si lidstvo vybralo za referenční materiál kov, byl ten, že se dá snadno roztavit a použít na výrobu něčeho jiného. Nominální hodnota takové mince se v podstatě zpočátku rovnala hodnotě reálné. Neboli hmotnost kovu obsaženého v minci se rovnala hodnotě zboží, za které ji bylo možné „vyměnit“. Ruku v ruce s novou měnou přišlo i její padělání. Mince v té době ještě

neměly klasický kulatý charakter. První formou padělání tak bylo obrušování hran mincí za účelem získání dalšího materiálu pro tvorbu mincí. V situaci kdy bylo stanoveno jednotné platidlo v rámci panství, se mohla začít snižovat jeho skutečná hodnota. Zejména v situaci kdy panovník potřeboval vynaložit veškeré dostupné prostředky na válečná tažení, přestala být měna závislá na materiálu, místo toho její hodnotu určoval panovník. Znak panovníka, tak na minci představoval záruku pravosti. Cenová revoluce v 16. století zaznamenala příliv drahých kovů do Evropy z nově objevených území (američtí Indiáni). Obchodování s mincemi z drahého kovu je nyní omezené. Vzhledem k velkému objemu vytěženého stříbra začaly mince nabývat vyšší hodnotu a byly nahrazeny papírovými penězi, nebo mincemi jejichž nominální hodnota se nerovná reálné. Mezi nejznámějšími mince se řadí American Eagle, Canadian Maple Leaf, South Africa Kruggerand a Australian Kangaroo.

1.1.4 Papírové peníze

K urychlení oběhu drahých mincí se začalo používat uložení těchto kovů u zlatníků, kteří vystavili na uložení drahých kovů potvrzení. Stvrzenka (směnka) obsahovala údaj o uloženém množství kovů a jejich ryzosti a řadí se mezi první formu bankovky. Tento systém se stal více oblíbeným a následným převzetím stvrzenkového systému dostaly stvrzenky pevné hodnoty. Prvními papírovými penězi se začalo platit v Číně. K prvnímu vydání došlo za vlády čínského císaře Hien Tsunga v letech 806-821 a následující emise byla vydána v r. 910 a r. 960 se papírové bankovky začaly vyrábět pravidelně. V Evropě se poprvé objevují v 17. století. Mezi významné období se řadí vláda Marie Terezie, kdy která oficiálně zavedla papírové peníze (tvz. bankocedulí). Nepříjemností byl v 19. století státní bankrot, který vyřešila Wallisova peněžní reforma. [1] V r. 1892 proběhla v Rakousku-Uhersku měnová reforma, kdy se peněžní jednotkou stává koruna, dělící se na 100 haléřů [2].

1.1.5 Elektronické peníze

Inovativní metodou platby je vvyužití technologie, které nám dnešní doba nabízí. Tou metodou jsou peníze elektronické. Těmi se rozumí číslená hodnota, která je rovna nominální hodnotě hotovostních peněz (bankovky, mince). Aby bylo možně toto platidlo přijmou za ofociální, musí na jejich definici myslet i zákon. V České republice je definice uvedena v zákoně č.284/2009 o platebním styku. Definuje elektronické peníze jako:

a) představují pohledávku vůči tomu, kdo ji vydal

b) jsou uchovávají se elektronicky

[1] Wallisova reforma - stání zadlužení a prudká inflace (důsledek bojů s císařem Napoleonem) vyústily ve státní bankrot. Podepsal ji František I. dne 20. února 1811 a následně zavedl novou papírovou měnu - směnné listy.

c) jsou vydávány proti přijetí peněžním prostředků za účelem provádění platebních transakcí a

d) jsou přijímány jinými osobami než tím, kdo je vydal

[3]

Druhů elektronických peněz je samozřejmě celá řada. Například téma této práce P2P platby, či kontroverzní bitcoin.

1.2 Banka a bankovní systém

Chrámy v minulosti tvořili tvz. úschovnu, kam si lidé mohli ponechat své prozatím nevyužité zdroje. Postupně se bankovní operace začaly přesouvat i mimo církévní objekty a největší nárůst bankovnictví je považováno období starověkého Říma.

1.2.1 Banka

Banka = peněžní ústavy (il banco - neboli lavice, stůl) jsou místem, kam si lidé chodí ukládat své úspory, obchodující na peněžním trhu. Ve 13. století v Itálii seděl jeden člen z rodu Medicejů na lavici před domem a lidé si k němu chodili ukládat přebytečné zlato a mince. On jim na oplátku vystavil doklad o množství uloženého bohatství. Jiní lidé k němu naopak chodili s žádostí o půjčku a on jim za své služby a určitou míru rizika počítal úrok. Na počátku 19. st. se pomalým tempem první banky objevují i v českých zemí. R. 1824 byla v Praze založena Česká spořitelna a r. 1847 vznikla rakouská National Bank a 1868 Živnostenská banka. Velký vliv na bankovnictví měl vznik Československa v r. 1918. Od r. 1938 situace bankovnictví na našem území bylo na vysoké úrovni. Tato situace však netrvala dlouho, neboť po 2. sv. v. došlo k přesunu vlastnistvví ve prospěch německého kapitálu. V r. 1965 vznikla Československá obchodní banka a na konci 90. let na našem území působilo 5 bank - Státní banka československá, ČSOB, St. spořitelna, Živnostenská banka a Investiční banka.

Rozdělení bank:

- centrální banka - jedná se o instituci, která je zřízena vládou (v ČR = Česká národní banka. Neposkytuje běžné bankovní služby. Vydává peníze a reguluje jejich množství v oběhu. Pečuje o stabilitu měny a určuje podmínky pro poskytování úvěrů. Dozoruje komerčním bankám.

- komerční (obchodní) banka - patří nezi nejpočetnější složku bankovní soustavy (v ČR např. ČSOB). Poskytují půjčky uživatelům, přijímají vklady a nabízi úvěry. Vystupují jako zprostředkovatelé (umoňují převody peněz z účtu na účet).

1.2.2 Bankovní systém

Bankovní systém tvoří soustava finančních institucí, zabývající se bankovními operacemi. [4]

Rozdělení:

- jednostupňový - hlavně pro centrálně plánovanou ekonomiku, v čele centrální banka, ostatní banky jsou na ni závislé. Tento typ bankovního systému je typycký pro Československo do r. 1989 nebo pro jiné komunistické země.
- dvojstupňový - v tržní ekonomice, v čele je také centrální banka, avšak ostatní banky jsou na ni nezávislé a vystupují jako samostatné subjekty.
- specializované finanční instituce - do tohoto sektoru se řadí investiční, hypotéční banky, spořitelny, pošty, soukromé směnárny či kampeličky.

1.2.2.1 Centrální banka

Už v r. 1816 na území Rakouska-Uherska vznikla první centrální banka a to "Privilegovaná Rakouská národní banka". O několik let později vznikla nová centrální banka Rakousko-Uherská, která začala vydávat první hotovostní peníze na celém území. Se vznikem Československé republiky vznikla "Národní banka Československá". Její činnost však skončila v r. 1950, neboť funkci centrální banky přebírá nově vzniklá "Státní banka československá". Tato banka plně fungovala až do r. 1989. Vlivem sametové revoluce se banka rozdělila na tři subjekty:

- Státní banka Československá
- Komerční banka Praha
- Všeobecná úvěrová banka Bratislava

Česká národní banka vznikla rozdělením Státní banky československé 1. 1. 1993 [5], tedy současně se vznikem České republiky. Podle zákona č. 6/1993 Sb. o České národní bance [5] je zřízena Ústavou České republiky. ČNB je samostatná právnická osoba působící v Praze. Nezapisuje se do obchodního rejstříku a jsou jí svěřeny některé kompetence správního úřadu. Hlavním orgánem je bankovní rada, která zřizuje bankovní politiku státu. Je to sedmičlenný orgán, který tvoří guvernér, dva víceguvernéři a čtyři další členové. Členy bankovní rady jmenuje prezident ČR na 6 let, nikdo však nesmí zastávat danou funkci více než dvakrát. Bankovní rada určuje měnovou politiku, schvaluje rozpočet ČNB, stanovuje mzdové požitky guvernéra či uděluje souhlas k podnikatelské činnosti zaměstnanců. Hlavním cílem ČNB je péče o cenovou stabilitu, podporuje hospodářskou politiku, vydává bankovky a mince, řídí peněžní oběh, zúčtování bank. Také spravuje zlaté a devizové rezervy (vydává devizové

licence). Dvakrát ročně musí ČNB podávat zprávu o měnovém vývoji Poslanecké sněmovně a jednou za tři měsíce je povinna o tomto vývoji informovat i veřejnost. Stanovuje úrokové sazby, dává do prodeje státní dluhopisy či vede evidenci cenných papírů vydávaných Českou republikou. [6]

1.2.3 Platební karta

Platební karta je identifikační doklad, jehož rozměry a fyzikální vlastnosti stanoví mezinárodní norma ISO 3554 [2]. Na přední straně je číslo karty, období její platnosti a jméno držitele. Na zadní straně je podpisový a většinou i magnetický proužek. Na většině karet se také nachází číslo karty, mnohdy rozšířené o další trojčíslí, které slouží jako heslo při některých elektronických transakcích. Karta je vždy majetkem banky, nikoli držitele. Proto často banky žádají její navrácení po skončení doby platnosti.

Rozdělení bankovních karet [7]

1. Podle zůčtování
   - Deberní karta - vázana na běžný účet držitele, ze kterého lidé čerpají prostředky při platbách. Při operacích je na kartě zablokována částka na účtu a následně se ověřuje v kartovém systému (ověření limitu, dostatek finančních prostředků).
   - Kreditní karta - není vázána na běžný účet. Držitelé těchto karet mohou provádět bankovní operace, ale za cenu úvěru a případnému následnému zadlužení. Úvěr po dobu 45 dní je bezúročný, poté si banka začne účtovat vysoké úroky.
   - Charge karta - podobné jako kreditní. Charge karty lze přirovnat k fakturám, neboť platba je odložena o několik dnů. Výhodou těchto karet je, že držiteli nevzniká úvěr.
   - Co-branded karta - v ČR není tento typ karty rozšířen. Můžeme jej popsat tak, že jde o spolupráci nějaké bankovní instituce s nebankovní. Držitelům, nebankovní instituce, jsou nabízeny výhodné balíčky, bonusové body a slevy.
2. Podle způsobu provedení
   - Ebosovaná karta - údaje o držiteli a číslo karty je vytlačeno nad povrch reliéfním písmem. Při placení dochází k ověření pomocí imprinteru, který provede otisk karty a identifikačního štítku. Držitel karty vše potvrdí svým podpisem a ochodník následně provede

[2] ISO 3554 - platební karta má přesně definovanou mezinárodní normu. Plast je vyroben s třívrstvého PVC, který má velmi přísná kritéria (elastičnost, tepelná stálost, odolnost vůči chemickým vlivům atd.). Platební karta musí umožnit přístup k hotovosti / bezhotovostní placení.

platbu. Vlastní ji pouze ten, u koho banky nepředpokládají nižší zůstatek méně než 10 000 Kč / měsíc).

- Elektronická karta - tyto karty vydávají banky zdarma ke každému běžnému účtu. Patří mezi nejčastější typ karty. Pomocí těchto karet lze vybírat hotovost z bankomatů či lze s ní platit u obchodníků, kteří mají elektronický platební terminál. Na zadní straně je magnetický pásek nebo čip.

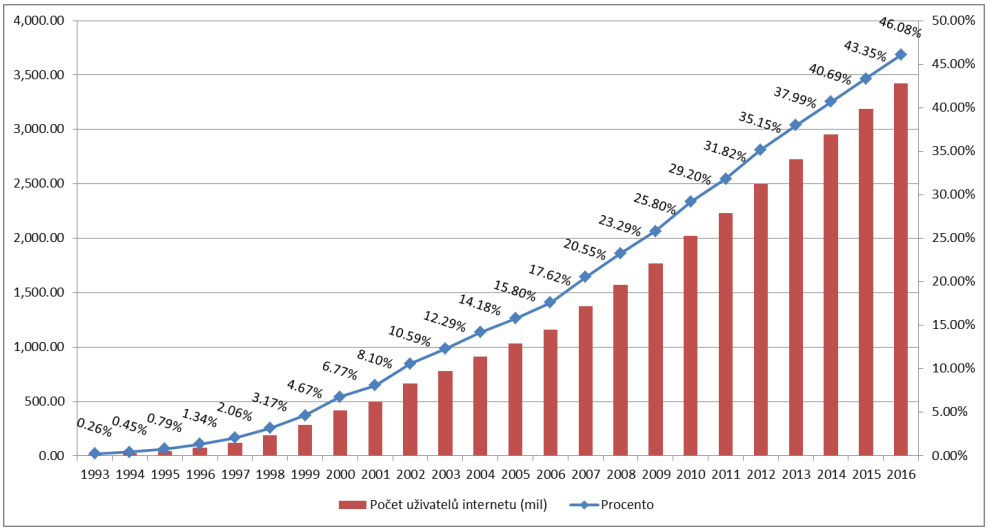
3. Podle použité technologie

   - Hybridní karty - výhodou je, že karty mají jak magnetický proužek, tak čip a lze je využít ve všech obchodních místech.
   - Internetové karty - jedná se o virtuální provedení karty, neexistují ve fyzické podobě. Je vygenerována pouze platnost a CVV2/CVC2 kód [3]. Tuto kartu může držitel využívat pouze při platbě zboží a služeb v kamenných proejnách.
   - Optické karty - tyto karty umožňují ukládání dat s tím, že údaje mohou být na tyto karty nahrány jen jednou a nelze je z nich odstranit.
   - Čipové karty - karty obsahují mikroprocesor, který kontroluje přístup k informacím na nich uložených. Dále se dělí na paměťové a modernější procesorové. Mezinárodními asociacemi byl stanoven termín 1. 1. 2005, od kterého musí všechny platební karty používané v Evropě nést v sobě čip a být standardu EMV (Europay-MasterCard-Visa standard).
   - Karty s magnetickým proužkem - u platebních karet tohoto typu proužek čten protažením karty čtecí hlavou

První bankovní karta pojmenovaná "Charg-it" byla představena r. 1946 Brooklynským bankéřem Johnem Bigginem [8]. Když s ní zákazník zaplatil, účet byl poslán do Bigginsovy banky. Bohužel v té době mohly být platby prováděny pouze lokálně a držitelé karty museli mít samozřejmě účet u Bigginsovy banky. Dalším krokem ve vývoji platebních karet byl vznik debetních karet. První debetní kartu představila Western Union Telegraph Company r 1914. Tato karta umožnila zákazníkům telegrafní společnosti posílat telegramy bez okamžiého placení.

První univerzální platební karta byla vydána r. 1950 společností Diners Club International. Tato společnost poskytla kartu svým 200 vybraným zákazníkům. Její univerzálnost spočívala v širokém využití. Zákazníci ji mohli používat pro krytí cestovních nákladů a zábavy. O rok později vydala první univerzální platební kartu i Franklinova národní banka v New Yorku (The

[3] CVV2/CVC2 kód - slouží jako bezpečnostní prvek. Je složen ze tří číslic na podpisovém proužku.



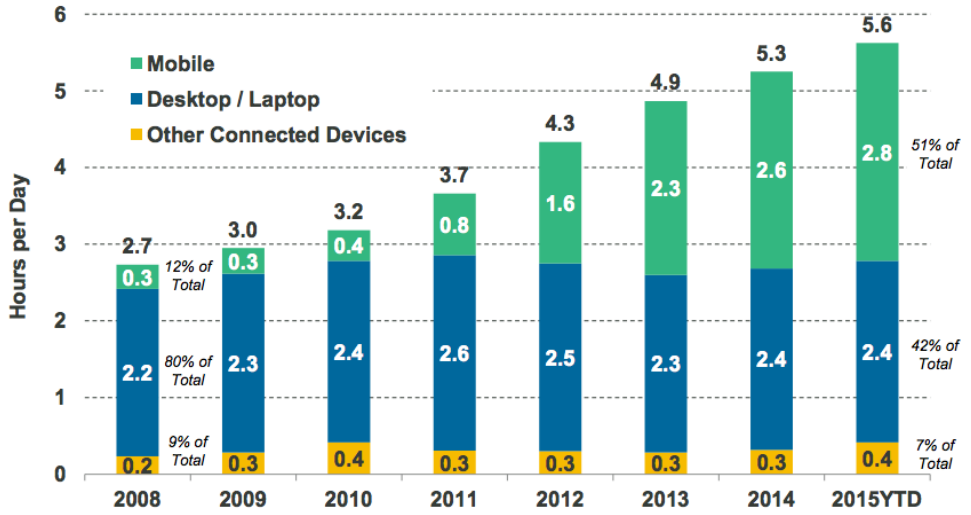
Obrázek 1.1: Vývoj počtu uživatelů internetu

Franklin National bank in New York). Při placení předložili klienti banky identifikační kartu a účet potvrdili podpisem. Obchodník ověřil podpis zákazníka v porovnání se vzorem na kartě. Později ještě přibyla kontrola přítomnosti karty na seznamu zablokovaných karet. Úplné počátky bankovních karet se tak obešly kompletně bez výpočetní techniky.

1.2.4 Vymezení pojmu internetové bankovnictví a mobilní bankovnictví

Od roku 1990 se začal rozvíjet internet a bylo jasné že tato technologie znamená nový pokrok pro lidstvo. Již roku 1993 používalo internet kolem 14 milionů lidí. A trend byl od roku 1990 exponenciální. Každým rokem přibývali noví uživatelé. Osa Y následujícího obrázku 1.1 znázorňuje jednak počet lidí s přístupem k internetu (v mil.) a zároveň procentuální podíl k celkové populaci na zemi. V současnosti tak má přístup k internetu téměř polovina populace. Dalším krokem pro bankovní sektor bylo logicky využít možností nového trhu [9].

Celý začátek internetové revoluce v bankovním sektoru začal v USA, coby kolébce celého internetu. Prvním milníkem pro vstup bankovního sektoru do prostředí internetu byl rok 1994, kdy Stanford Federal Credit Union jako první spustila své webové stránky. Další banky ji samozřejmě následovaly. Již v roce 1995, kdy přístup k internetu mělo bez mála 45 milionů lidí, přidala společnost Wells Fargo do svých internetových stránek možnost spravovat své bankovní účty. Na konci roku 1999 používalo tyto služby méně než 0.4% domácností. Na začátku roku 2004 tomu však již bylo 33%.[10]



Obrázek 1.2: Čas strávený před monitorem (smartphone, pc,..)
Zdroj: `http://techpp.com/2015/07/24/mobile-internet-usage-report/`

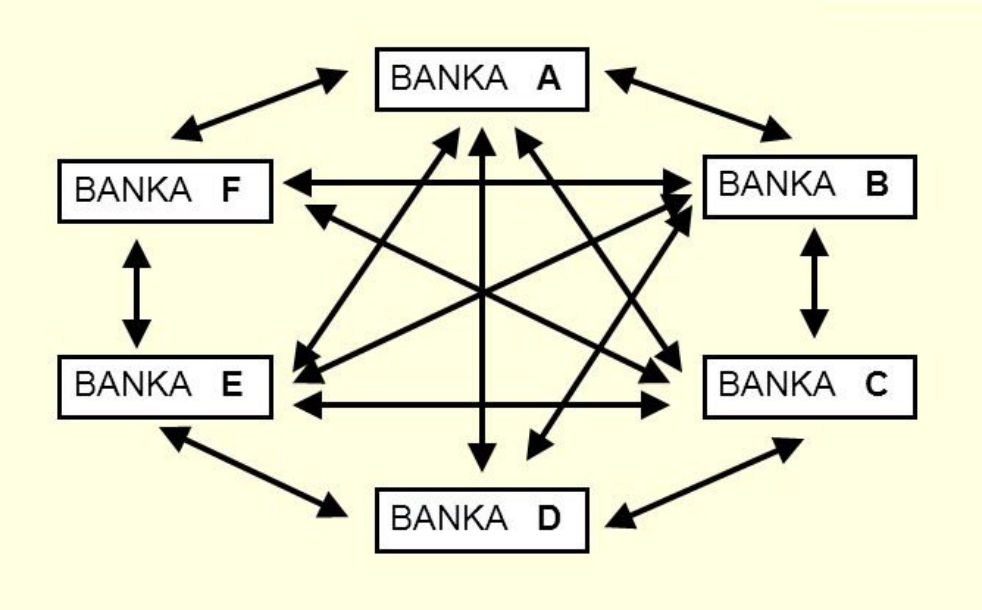
1.2.4.1 Internetové bankovnictví

Internet banking dosahuje vrcholu oblíbenosti v oblasti bankovnictví. Na počátku 90. let tuto službu začaly poskytovat první banky v USA. Podmínou je vlastnit zařízení s připojením k internetu a na jakémkoli internetovém prohlížeči se přihlásit pod přihlašovacím jménem a heslem ke do svého bankovnictví. V internetovém bankovnictví lze hradit veškeré účty v pohodlí domova a netrávit tak čas ve frontách na pobočkách bank či jiných institucí. Kromě sledování aktuálního zůstatku na účtu, uživatelé mohou snadno využít i dalších služeb, záleží co nabízí daná banka.

1.2.4.2 Mobilní bankovnictví

Obdobná revoluce jako se odehrála v případě internetu následovala o dekádu později v oblasti mobilního bankovnictví. Následující graf 1.2 ukazuje, jak se v průběhu let od roku 2008 změnil čas strávený před obrazovkou mobilních zařízení v porovnání s klasickými počítači.

Je patrné, že čas strávený před monitorem se v případě klasického PC příliš nezměnil, zatímco v případě mobilních zařízení vzrostl z 0,3 hodiny denně na 2,8 hodiny. Bavíme-li se o používání bankovních služeb na mobilních zařízeních nabízí se dva způsoby. První z nich je přístup přes klasické webové rozhraní a pak samozřejmě pomocí mobilní aplikace. V dobách, kdy mobilní telefony začaly umožňovat přístup na internet, se možnost přístupu přes webové rozhraní jevila jako klíčová. První banka, která s touto možností přišla na trh byla Americká banka “Bank of America”. Obdobnou službu nabídla i společ-



Obrázek 1.3: Korespondentský platební systém
Zdroj: Dvořák,Bankovnictvíprobankéřeaklienty

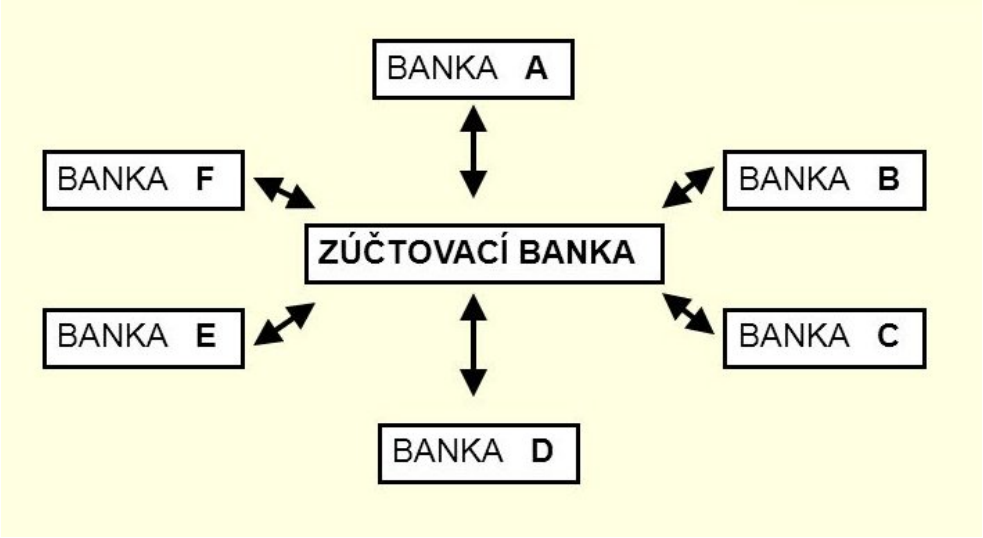
nost Wells Fargo, která navíc přidala možnost spravovat své bankovnictví prostřednictvím SMS. Druhá možnost umožňuje lepší optimalizaci pro rozlišení mobilního zařízení a dokáže lépe provázat více služeb najednou. Klasickým příkladem jsou aplikace, jak je známe dnes. Aplikace nejenže poskytuje možnost připojit se na internetové bankovnictví, ale i umožňuje například využití kamery pro scanování QR kódů nebo například spárování se sociálními sítěmi. Aplikaci tohoto typu, jako první představila polská Wachovia v roce 2006. O dva roky později v roce 2008 už je mobilní aplikace pro správu internetového bankovnictví standardem i pro menší banky.

1.2.5 Clearing

Součástí každého mezibankovního platebního styku je proces vzájemného vyrovnání závazků zúčastněných bank. Existují dva způsoby vzájemného vyúčtování.

První z nich je korespondentský platební systém 1.3. Princip tohoto sytému je ten, že každá banka si musí založit účet u všech ostatních existujících bank. Mezibankovní převod tak prakticky funguje jen jako převod v rámci jedné banky. Tento systém jak je již patrné z obrázku má nevýhodu v množství nezbytných účtů a nutnosti vlastnit dostatečné množství prostředků na každém z nich. Jejich počet narůstá geometrickou řadou v případě založení nové finanční instituce.

Druhý systém je pomocí prostředníka, zúčtovací banky. Tento systém má



Obrázek 1.4: Clearingový platební systém
Zdroj: Dvořák,Bankovnictvíprobankéřeaklienty

samozřejmě výhodu v množství účtů potřebných pro fungování celého bankovního ekosystému. V tomto případě je postačující založení jednoho účtu každé banky u této centrální zúčtovací. Jediným systémem, který zpracovává mezibankovní převody finančních prostředků a splňuje podmínky podle zákona č.284/2009 Sb., o platebním styku [3], je systém CERTIS (Czech Express Real Time Interbank Gross Settlement System). Tento systém byl založen v roce 1992 v rámci Státní banky Československé. Po rozdělení Československa, počátkem roku 1993 bylo na Slovensku vytvořeno nové zúčtovací centrum, zatímco bývalé federální zúčtovací centrum zůstalo v ČNB.

Clearing ČNB jak bývá tento proces v České republice označován, je i jednou z hlavních příčin dlouhé doby mezibankovního převodu. Hlavním cílem systému je odhalit praní špinavých peněz, kdy se pachatel tohoto trestného činu snaží zamaskovat nelegální původ finančních prostředků. Celý bankovní systém má kromě samotných převodů peněz za úkol sledovat chování svých klientů a jakékoliv podezřelé odchylky prověřit. V případě podezření z páchání trestného činu je povinností podstoupit takové informace Ministerstvu financí k dalšímu prošetření. Zákon ovšem opět stanovuje jaká je maximální délka mezibankovní finančního převodu. Pro tento typ bankovní transakce platí opět zákon č.284/2009 Sb., o platebním styku [3].

Provádí-li převádějící instituce příkazce převody na území České republiky v české měně

a) Poskytovatel plátce zajistí, aby částka platební transakce byla připsána na účet poskytovatele příjemce nejpozději do konce následujícího pracovního dne po okamžiku přijetí platebního příkazu.

b) Plátce a jeho poskytovatel si mohou dohodnout lhůtu o 1 pracovní den delší, než je lhůta uvedená v odstavci 1 (Za daných podmínek).

c) Plátce a jeho poskytovatel si mohou dohodnout lhůtu o 3 pracovní dny delší, než je lhůta uvedená v odstavci 1 (Za daných podmínek).

Platí tak lhůta D+1, kde se dnem D myslí den, ve kterém banka odepíše platbu z účtu odesílatele. Číslice udává, kolik času má banka na převod peněz. Do 31. října 2009 platila pro převod peněz z účtu na účet lhůta D+2.

Problémem celkové doby zpracování požadavku ovšem není průběh jeho zpracování, ale celé nastavení systému. Bankovní den účetního centra systému CERTIS začíná v 17.00 předchozího dne (D-1) a končí v 16.00 hodin (D). Za své služby si clearingové centrum účtuje poplatky, přičemž nejnižší jsou na začátku bankovního dne. Kde se cena pohybuje kolem 0.09 Kč za transakci. Čim více se blíží konec dne, tím více se částka zvyšuje až na 25Kč za transakci. Tento čas je většinou vyhrazen větším bankovním transakcím, ČNB se tak snaží motivovat banky, aby posílaly platby co nejdříve a nečekaly na konec bankovního dne. Bohužel o víkendech a státních svátcích je tento systém vypnutý a probíhá údržba. Podle vyjádření zástupce ČNB by klidně mohl systém fungovat 7/24, ale musely by to banky vyžadovat.

Každá banka má také specifikovaný bankovní den, který se v každě bance liší. Například v případě Komerční banky jsou platby odesílané téhož dne přijímány do 20 hodin 30 minut. Pokud klient pošle bance požadavek na provedení transakce do této doby, bude požadavek odeslán do clearingového centra ještě téhož dne. Za současného stavu tak může dojít k několika situacím. První situací je již zmíněný příklad, kdy je požadavek odeslán do lhůty dané bankou. Požadavek je tak hromadně odeslán s ostatními ještě téhož dne na zpracování do zúčtovací banky. Jelikož ČNB označuje dobu od 17.00 do půlnoci jako D-1 znamená to, že bude stejně zpracován až následujícího dne (D). Transakce bude tak dokončena nejdříve druhý den ráno a nejpozději druhý den o půlnoci. Druhá situace, která může nastat, je pokud klient odešle transakci po zúčtovací lhůtě své banky. Některé banky odesílají transakce v několika dávkách denně, ale častěji se stane že všechny transakce budou odeslány až následující den po ukončení dalšího bankovního dne. Peníze tak budou doručeny nejdříve za dva dny po odeslání transakce. V tuto chvíli se nabízí otázka, zda banka neporušuje zákonem stanovený limit D+1. Odpověď zní ne. Transakce musí být dokončena následující bankovní pracovní den po dni účinnosti příkazu, a nikoliv následující pracovní den. V praxi tak dochází i k třetí situaci, kdy klient odešle příkaz k transakci v pátek po skončení bankovního dne. Transakce tak bude odeslána do ČNB až následující bankovní den, to znamená v ponděli a dokončení transakce lze očekávat v úterý v dopoledních hodinách a nejpozději do půlnoci. To znamená tři dny od zadání příkazu.

Není zřejmé proč jsou příkazy zpracovány dávkově a ne v okamžiku zadání příkazu. Když dle internetových stránek banky je systém CERTIS dimenzován

na propustnost 1 500 000 transakcí za hodinu a clearingovým centrem ČNB projde denně kolem 2 500 000 transakcí. Pro převod platebních prostředků v rámci téhož poskytovatele na území České republiky v české měně musí být částka připsána příjemci nejpozději na konci dne v němž nastal okamžik přijetí příkazu [11].

1.3 Platba a její druhy

V následující kapitole se zaměříme na technické provedení jdnotlivých typů plateb. Platbu lze rozdělit do dvou kategorií na hotovostní a bezhotovostní. Bezhotovostní platba se pak dále dělí podle technologie kterou využívá.

- Hotovostní
- Bezhotovostní
  - Platba kontaktní platební kartou
  - Platba prostřednictvím aktivní a pasivní NFC technologie
  - Internetový a mobilní bankovní převod

1.3.1 Hotovostní platba

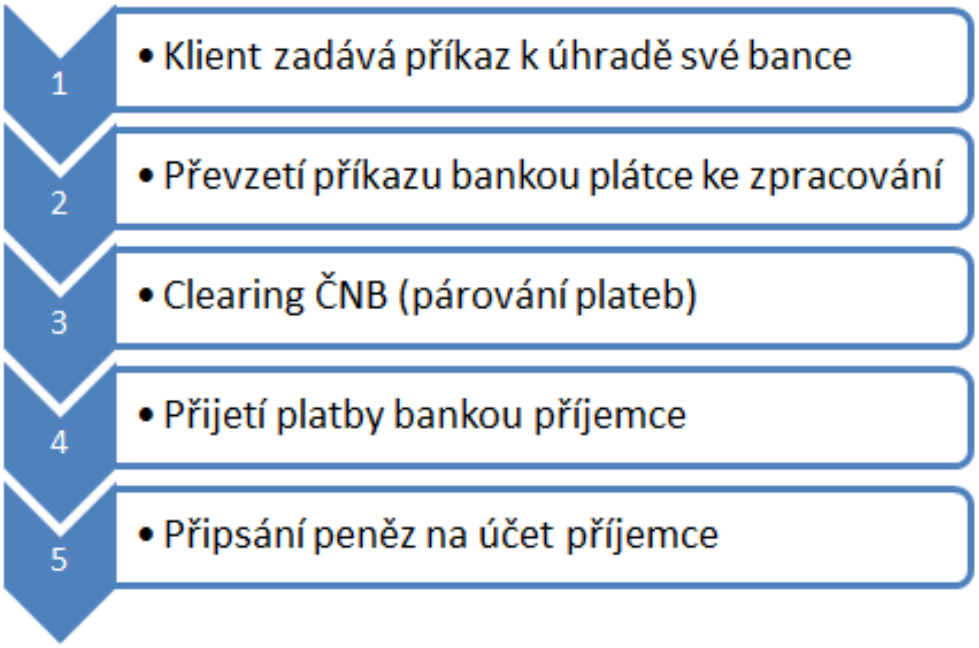
Zákon č.254/2004 Sb. definuje platbu jako předání nebo převedení peněžních prostředků poskytovatelem platby příjemci platby [12]. V tomto případě se jedná o platbu hotovostní neboli o platbu, kde je předmětem finanční hotovost v podobě bankovek či mincí.

1.3.2 Bezhotovostní platba

Bezhotovostní platbou se dle zákona rozumí platba provedená převodem peněžních prostředků na území České republiky prostřednictvím peněžního ústavu v české nebo cizí měně. Nebo převodem peněžních prostředků prostřednictvím peněžního ústavu v české nebo cizí měně z území České republiky na území jiného státu [12]. Pro ilustraci proces bezhotovostní platby se dá vyjádřit následujícím obrázkem 1.5. Dále se liší i proces platby v rámci jednoho poskytovatele účtu a tzv. mezibankovní platební styk, tj, mezi různými poskytovateli. Obrázek tak popisuje platbu z účtu jedné banky do účtu banky jiné. Na první pohled je patrné v čem spočívá onen podstatný rozdíl. Je jím již zmíněný Clearing ČNB 1.2.5.

1.3.2.1 Platba kontaktní platební kartou

Platba platební kartou je komplexní posloupnost jednotlivých kroků. Během platební transakce si musí platební karta s terminálem vyměnit informace o jejích dostupných aplikacích, dále informace o jejím držiteli, provést ověření



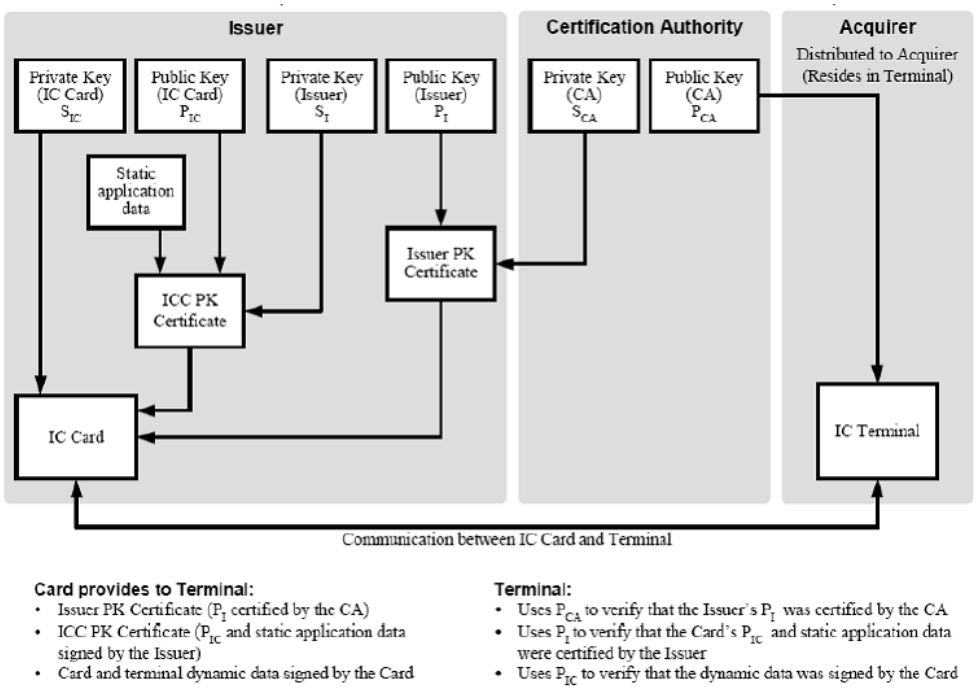
Obrázek 1.5: Proces bezhotovostní platby

Zdroj: http://www.tivit.cz/poradime-vam/financni-poradenstvi/penize/zpusoby-placeni/zpusoby-placeni-hotovostni-a-bezhotovostni

a poslední řadě schválit či zamítnout transakci. Každá platební karta označovaná jako EMV v sobě obsahuje platební aplikace. Například Bonuscard, Visa Credit, Visa Debit atp. Proto při komunikaci karty s platebním terminálem musí nejprve dojít k výběru požadované aplikace na kartě. V dalším kroku může dojít k offline autentizaci. V této fázi existuje několik způsobů provedení, SDA (Static Data Authentication), DDA (Dynamic data authentication) a CDA (Combined data authentication). Na následujícím obrázku 1.6 si přiblížíme funkčnost DDA, coby standardu pro offline authentizaci. DDA v porovnání s SDA znamená, že karta má v sobě obsažený privátní RSA klíč, kterým jsou podepsána dynamická data [13]. Tento přístup v porovnání s SDA má zabránit útoku opakováním [4].

Karta v sobě obsahuje svůj privátní klíč, veřejný certifikát karty (veřejný klíč karty s aplikačními daty podepsaný privátním klíčem vydavatele karty). A v neposlední řadě také veřejný certifikát vydavatele karty (veřejný klíč podepsaný privátním klíčem certifikační autority). Terminál tak použije veřejný klíč certifikační autority, aby ověřil veřejný klíč vydavatele karty. Tento klíč tak použije k ověření veřejného klíče karty a statických aplikačních dat. Dále pak použije získaný veřejný klíč karty k ověření dat podepsaných klíčem pri-

[4] útok opakováním ("reply attack"), útok, při kterém je využito shodných dat v každé transakci, pro rozklíčování informací



Obrázek 1.6: DDA, Dynamic data authentication

Zdroj: `http://emvfunctionalflow.blogspot.cz/2015/07/card-inserted-in-terminalposatm.html`

vátním. Tento krok ovšem není prováděn vždy, ale pouze v případě, kdy může být transakce provedena offline. V případě online ověřovací fáze komunikuje platební terminál přímo s bankou. Má-li klient na kontě dostatečné množství prostředků a pokud úspěšně dojde k ověření indentity držitele karty, karty samotné i jejího vydavatele, nebrání nic dokončení platby.

Celý proces NFC platby je samozřejmě o poznání složitější, pro naše potřeby tento zkrácený popis postačí. Přesto jej pro přehlednost naznačuje následující obrázek 1.7.

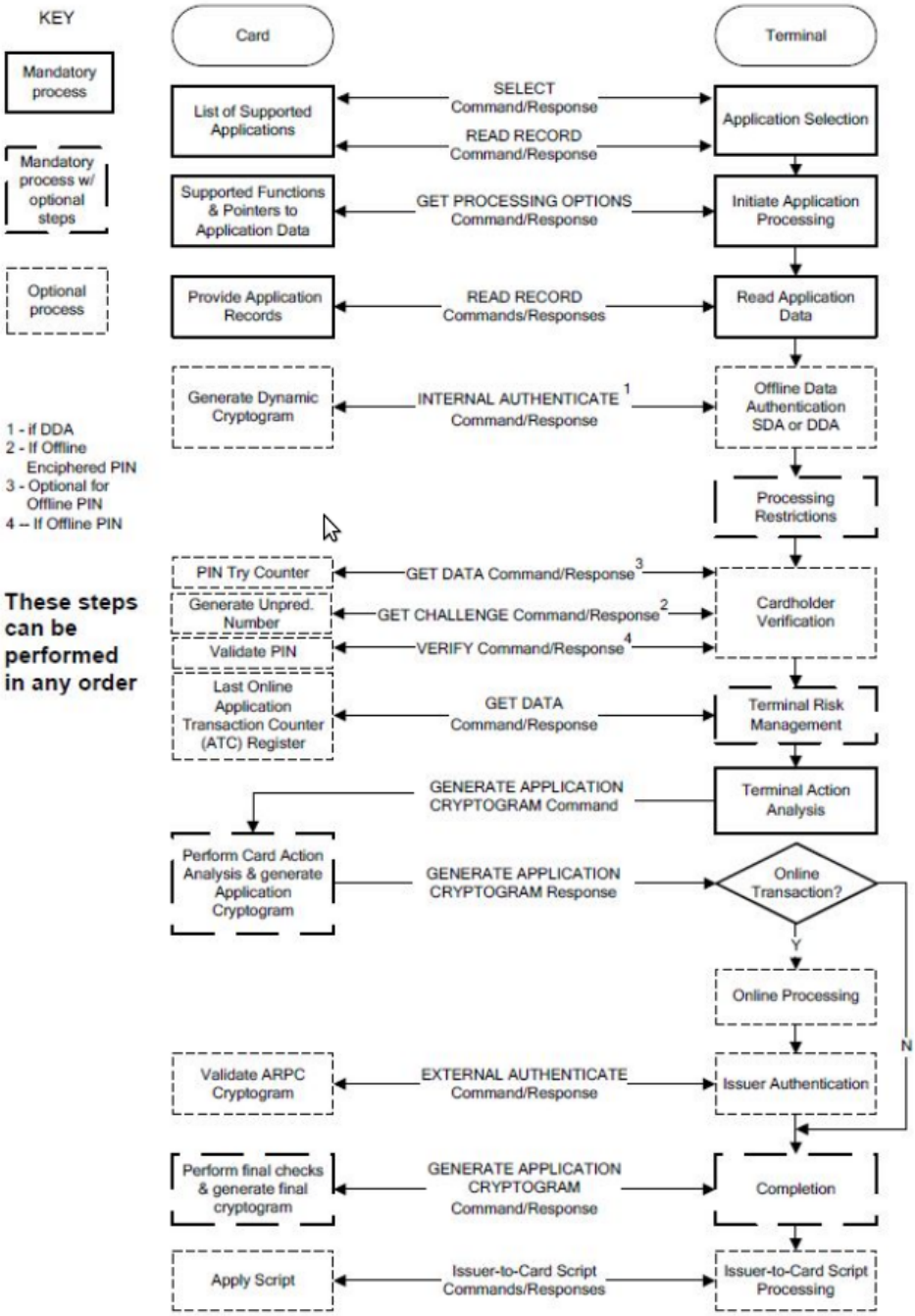
1.3.2.2 Platba prostřednictvím aktivní a pasivní NFC technologie

Aktivní a pasivní NFC je typ technologie pro provedení bezkontaktní platby. V případě pasivní NFC platby se jedná o klasickou bezkontaktní EMV [5] platební kartu. Tento typ karty v obsahuje zabudovaný RFID [6] chip 1.8, který funguje na principu elektromagnetické indukce. Jakmile se takový typ karty přiblíží k platebnímu terminálu, který je sprárovaný s POS [7], dojde k indukci elektrického napětí v kartě a je tak napájen její mikroprocesor. Dokud je RFID chip

[5] EMU je zkratka pro Europay, MasterCard, Visa. Jedná se o mezinárodní standard pro platební karty

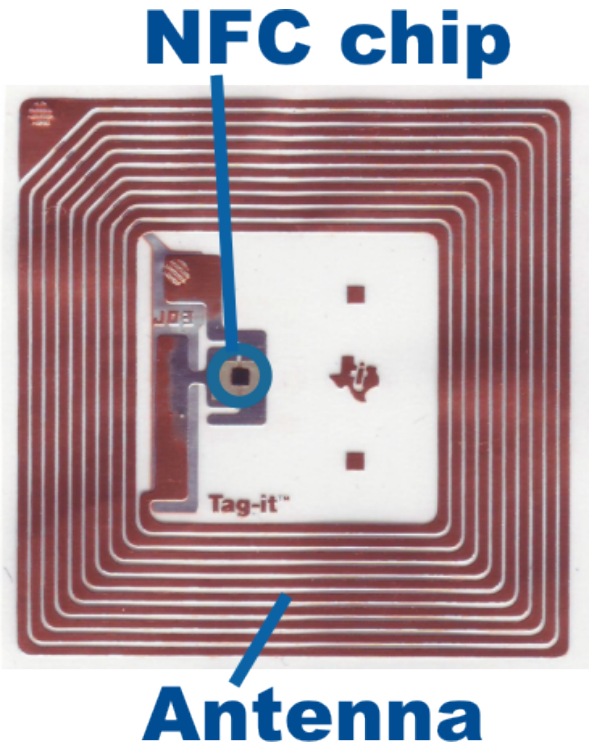
[6] RFID je zkratka pro "Radio frequency identification

[7] POS, "Point of sale"je pokladní místo, neboli pokladna



Obrázek 1.7: Proces platby EMV

Zdroj: Tomáš Bublík, Stručný úvod do EMV transakcí



Obrázek 1.8: NFC tag

Zdroj: http://www.bonwal.fi/wp-content/uploads/2015/04/nfc-tag.png

v elektromagnetickém poli terminálu, je schopen rádiové komunikace. První platba pomocí využití pasivního RFID chipu přišla jako forma Speedpasu v roce 1997. Mobilní stanice na plyn nabízela platební zařízení, které bylo přpevněné k prstenu. Stačilo tak jen mávnout rukou nad terminálem a platba proběhla okamžitě. Na český trh s touto novinkou přišla v roce 2011 Česká spořitelna ve spolupráci s karetní asociací Visa. Jejich cílem bylo během tří let převést všechny platební karty na bezkontaktní. Nutno podotknout, že se to podařilo nejen České spořitelně, ale dnes již nabízí bezkontaktní placení EMV kartou všechny větší banky, a jedná se tudíž o jakýsi standard. Pro placení stačí platební kartu přiblížit do vzdálenosti cca 5 cm odd platebního terminálu a platby do hodnoty 500Kč jsou autorizovány bez potřeby zadávat PIN. Po zvukovém signálu je transakce ukončena. Své využití nalezl tento RFID chip nejen v bankovním sektoru ale i v mnoha dalších odvětvích průmyslu, od oděvního po logistiku. RFID chip je pro představu na následujícím obrázku.

S první platbou s aktivním RFID chipem přišla na český trh Fio banka ve spolupráci s mobilním operátorem. Jedná se o chip, který je aktivně napájen z připojeného zdroje napětí. Typickým příkladem tohoto typu je právě technologie NFC v telefonu, která v podstatě dokáže plnit jak funkci chipu tak i čtečky. Krátce po implementaci prvních nfc chipů do mobilních telefonů se

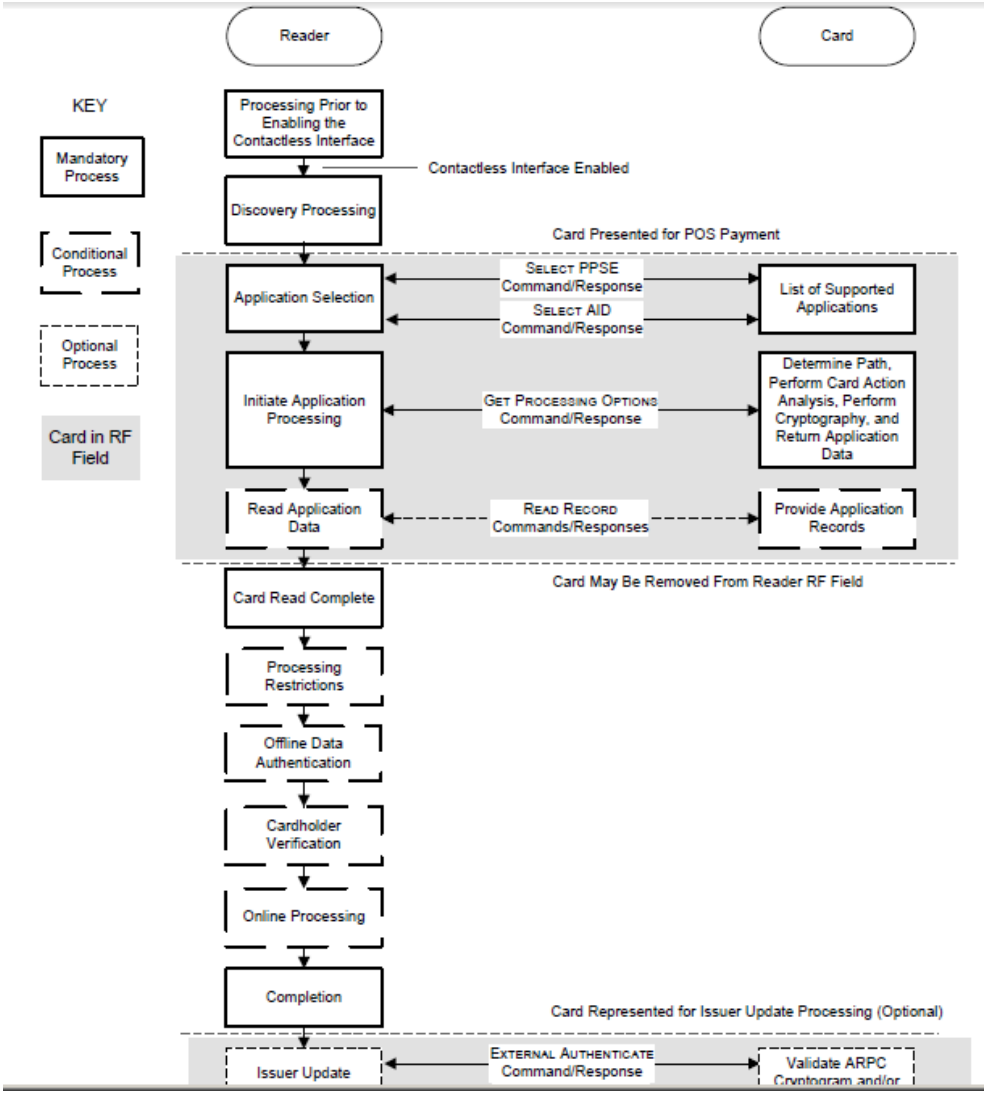
mluvilo o možnosti placení mobilním telefonem. Od verze Androidu KitKat (4.4) se v operačním systému vyskytuje technologie HCE neboli "host card emulation". Mobilní operační systém iOS tuto technologii začíná podporovat až ve své nejnovější verzi. Tato technologie umožňuje importování platebních karet do systému mobilního telefonu. Jedná se o klasický příklad technologie, která v zahraničí již nějaký čas úspěšně funguje, ale k nám se dostává až dnes. K datu 20. října 2016 tento typ placení podporují v českém prostředí dvě banky. Jedná se o ČSOB a KB. Proces platby je obdobný jako v případě klasické plastové karty. Důkazem zájmu klientů o tento typ placení je statistika uveřejněná Komerční Bankou. Ta uvádí, že po prvním měsíci existence služby využívá mobilní kartu KB kolem 3000 klientů [14]. Pro tento typ platby prakticky stačí, aby telefon podporoval technologii NFC a zákazník tak může platit pouze přiložením telefonu k platebnímu terminálu. Není potřeba žádné spárování se SIM kartou mobilních operátorů.

Jelikož se v obou případech stále jedná o platby platební kartou, jednotlivé kroky vykazují jistou míru podobnosti s klasickou kontaktní platební transakcí. Následující obrázek 1.9 popisuje platební transakci prováděnou NFC EMV platební kartou. Jak je vidět i v tomto případě dochází k výběru aplikace na kartě. Rozdíl je ovšem v tom, že po načtení aplikačních dat z karty již není přítomnost karty v magnetickém poli terminálu vyžadována, neboli zbytek transakčního procesu provádí pouze již jen jedna strana. Tato vlastnost je zejména z důvodu použitelnosti této metody během platby u obchodníka. Těžko si lze představit, že by během provádění platby bylo nutné držet platební kartu v adekvátní vzdálenosti od terminálu po dobu delší než 5 vteřin. Jakmile je aplikace zvolena dochází k offline ověřovacímu procesu. Po ověření identity karty a jejího vydavatele dojde k přečtení dat. Dále dojde k ověření omezení na platbu, offline dat a potřeby zadat PIN. Někdy je třeba provést znovu i online ověřovací fázi. Pokud úspěšném ukončení všech fází dojde k schválení samotné platby. Celý proces však trvá pouhých pár vteřin.

1.3.2.3 Internetový a mobilní bankovní převod

Tuto kategorii nelze striktně rozdělit na dvě kategorie, protože v případě mobilního bankovního převodu se v podstatě jedná o internetový bankovní převod prostřednitvím mobilního bankovnictví. Do této kategorie řadíme samozřejmě patří i platba virtuální měnou Bitcoin či téma této práce P2P platby. Popularita mobilního bankovnictví má proti klasickému přístupu přes internetový prohlížeč rostoucí tendenci. Průzkum internetového portáu novinky.cz ukázal, že mobilní bankovnictví využívá letos 27% klientů oproti loňským 24%. [15].

Bitcoin je digitální měna, kterou v rámci své práce "Bitcoin" A Peer-to-Peer Electronic Cash" vytvořil v roce 2009 autor pod pseunonymem Satoshi Nakamoto. Název bitoin je též označení pro open-source software a peer-to-peer síť. Pro provádění transakcí je využívána distribuovaná databáze mezi všemi uzly této sítě. K zabezpečení se je využita kryptografie. Bitcoiny, coby

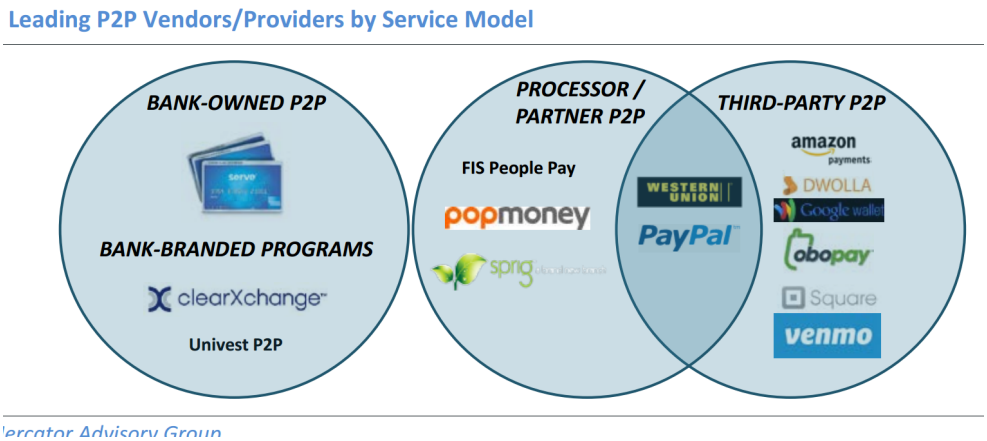


Obrázek 1.9: Proces bezkontaktni platby EMV

Zdroj: Tomáš Bublík, Stručný úvod do EMV transakcí

elektronická měna, jsou uloženy na počítači ve formě souboru nebo uchovávány službami třetích stran. Vzhledem k decentralozovanosti měny a faktu, že množství mincí je předem dané, je bitoin odolný vůči intervencím ze strany bank a vlád. Celkové množství Bitcoinů, které mohou být vytěženy, je přibližně 21 000 000. Každý bitoin je dálě dělitelný až na osm desetinných míst. Tato kryptoměna ale představuje, coby způsob financování nelegálních aktivit, dle mnohých problém. Je to způsoběno tím, že jednotlivé transakce nepodléhají kontrole a jsou nedohledatelné. Již bylo prokázáno, že tuto měnu v určité míře používají i teroristické organizace k financování svých aktivit. Druhý problém, který tato měna přináší, je nepřipravenost zákonů na obchodování s touto měnou. V minulosti byly zaznamnány velké výkyvy v hodnotě Bitcoinu, ale pokud by například obchodník zbohatnul při převodu z BTC, měl by dle platných zákonů být držitelem licence pro směnárenskou činnost [16].

Do této kategorie samozřejmě spadá i P2P platba. Znamená v překladu person-to-person, neboli "člověk člověku" či je občas označována jako peer-to- peer. Některé služby však spíše než peer-to-peer využívají klasický model client-server, proto je toto označení v mnoha případech zavádějící. Jedná se o online technologii, která umožňuje zákazníkům převádět platby z jejich bankovního účtu, či platební karty na účet jiné osoby přes internet či sms. Přímým předchůdcem tohoto typu platby je klasická v platba v hotovosti či použití šeků. Snaha nalézt podobně řešení v moderním pojetí a rozmach internetových aukčních portálů dala za vznik právě této službě. Původně služby fungovaly pomocí webového prohlížeče v přenosném počítači. Dnes je však samozřejmým předpokladem úspěchu rozvoj vysokorychlostního internetu a chytrých mobilních telefonů. Data webového portálu businessinsider.com z roku 2014 udávají, že se celková cena celosvětových ročních p2p plateb pohybuje kolem $1 bilionu. Z toho p2p platby z mobilních zařízení tvoří pouhé 1 procento celkové částky. Dle jejich předpovědi by však do roku 2020 měl tento podíl tvořit cca 30 procent. Jedná se ovšem jen o odhady závislé na mnoha faktorech a proto se v případě dalších portálů zásadně liší. Jednotlivé služby se dají rozdělit do několika kategorií [17]. P2P jako bankovní služba, dále jako služba třetích stran a jako služba využívající platebních karet. Jako službu třetích stran představila P2P platby první společnost PayPal v roce 1999. Tyto společnosti vystupují jako prostředníci mezi zákazníkem a bankou. Ve chvíli, kdy chce člověk zaplatit, předá tuto instrukci této službě a ta samotnou transakci zprostředkuje. Výhodou využívání služeb třetích stran je prvotně jejich univerzálnost. Uživatel není omezen na bankou. Rovněž se dá považovat za bezpečnější, pokud je samotná platba abstrahována od dat klienta uložených v bance. Jednotlivé kategorie jsou znázorněny na následujícím obrázku 1.10. Odpovědí bank na služby třetích stran se jejich klienti dočkali až po roce 2010. V této skupině jsou služby klientům poskytovány přímo jejich bankou. Přináší to s sebou opět řadu výhod i nevýhod. Jako výhoda tohoto přístupu je ta, že data klienta jsou bezpečně uložena, předpokládá se totiž vysoká úroveň zabezpečení bankovních subjektů. Dále klient banky nemusí používat aplikaci od jiného poskytovatele,



Obrázek 1.10: P2P kategorie

Zdroj: `http://www.paymentsjournal.com/WorkArea/DownloadAsset.aspx?id=22928`

ale vše potřebné funkce nalezne v aplikaci své banky. První službou tohoto druhu byla síť ClearXChange. ClearXChange která vznikla jako společné dílo Bank of America, Capital One, JPMorgan Chase, US Bank a Wells Fargo. Banky tak chtěly získat klienty zpátky pod svoji kontrolu. Poslední skupinou z jmenovaných jsou služby, které poskytují služby bankám. Jedná se tak prakticky o opačný přístup, než v případě aplikací třetích stran, kde služby pod sebe sdružují klienty jednotlivých bank. Typickým zástupce v této skupině je například Popmoney nebo PayPal.

Všechny hlavní metody byly zmíněny v předchozích odstavcích, přesto stále existuje prostor pro inovace. Například pro placení u obchodníka lze využít například spojení s geolokalizačním systémem. Tato metoda má ovšem spoustu nedostatků. Nové možnosti může přinést využití biometrických údajů. Společnost Fujitsu úspěšně vyvinula technologii PalmSecure na ověřování osob pomocí struktury krevního řečiště. Jelikož je tato struktura unikátní pro každého jedince, naprosto odpadá nutnost s sebou nosit jakékoliv platební médium. V takovém případě by stačilo při placení natáhnou ruku. Tato technologie je již úspěšně používána ve vybraných přenosných počítačích této společnosti a dokonce byl na Fujitsu Forum 2016 prezentován první bankomat s touto technologií.

1.4 Bezpečnost mobilních aplikací

Využívání každé mobilní aplikace s sebou přináší vždy řadu výhod i nevýhod. Pokud ale aplikace nakládá s osobními údaji uživatele, je potřeba být zvláště na pozoru v otázce bezpečnosti. V této kapitole se tak seznámíme s obecnými doporučeními pro uživatele a pro vývojáře aplikace.

1.4.1 Uživatelský pohled

Nejprve se podíváme na doporučení pro uživatele mobilních aplikací od instalace přes nastavení hesla až po samotné používání. Na pozoru by se měl mít uživatel už v okamžiku instalace aplikace. Neinstalovat aplikace z jiného než z ověřeného zdroje by mělo být samozřejmostí. Nejen v případě bankovních aplikací, ale i v případě jakékoliv aplikace. Zvláště pokud na zařízení chceme využívat službu, která spravuje naše osobní údaje. Dále je třeba dávat dobrý pozor na to jaká oprávnění, která aplikace požaduje. Při nedostatečné obezřetnosti si uživatel do svého zařízení může nainstalova škodlivý software. Po samotné instalaci platí pro uživatele doporučení ohledně používání hesel. Následující vydala společnost CERN Computer Security [18].

- **soukromé:** je používáno a známo pouze jedné osobě
- **tajné:** není součástí jakéhokoliv textu v libovolném programu ani na kusu papíru přilepeném k monitoru
- **jednoduše zapamatovatelné:** není potřeba si jej zapisovat nejméně 8 znaků
- **obsahuje minimálně 3 kategorie znaků:** velká písmena, malá písmena, čísla a symboly
- **není ve slovníku** žádného z hlavních jazyků
- **není uhodnutelné programem** v rozumném čase, například méně než týden.

Těchto doporučení je celá řada, ale rozhodně se vyplatí je mít na paměti nejen při vytváření hesla. Dalšími pravidly, které nejsou uvedena na seznamu je například používání jednoho hesla pro jednu službu. V dnešní době, kdy je do každé webové stránky požadováno přihlášení, se doporučuje používat zvláštní heslo pro každou službu, jejíž kompromitování by nám mohlo způsobit újmu. Pro všechny ostatní služby klidně může být používáno heslo jedno.

1.4.2 Vývojářský pohled

Pohled vývojářů na bezpečnost mobilních aplikací je velmi důležitým aspektem vývoje software. Těmto lidem dávají uživatelé k dispozici své osobní údaje a předpokládají jistou úroveň ochrany. Abychom se mohli v následujícím odstavci věnovat zabezpečení, je nejprve důležité se seznámit s tématy, které se bezpečnosti týkají.

1.4.2.1 Zabezpečení přístupu

Už od prvního přihlášení jsou uživatelé vystaveni riziku, že jejich data mohou být ukradena a následně zneužita. Vývojáři aplikací by proto měli nejprve myslet na zabezpečení celé komunikace mezi aplikací a serverem. Protokol, který toto umožňuje, se nazývá SSL/TLS [8]. Celá komunikace probíhá šifrovaně. Ovšem i používání tohoto protokolu má své nevýhody. Například pokud klient (mobilní aplikace) neověřuje certifikát proti listu certifikačních autorit. Může pak dojít k situaci, kdy se podvodná CA dostane do ověřených CA a nic nebrání podvržení serveru a k provedení MITM útoku. Internetový magazín Infosecurity prezentoval výsledky průzkumu 40 mobilních bankovních aplikací [19]. Výsledky byly poněkud alarmující.

- 12.5% zkoumaných aplikací nekontroluje pravost SSL certifikátu, což je činí náchylné na MITM útoky.
- 35% aplikací obsahovalo nezabezpečené (non SSL) odkazy v rámci aplikace. To umožní útočníkovi injektovat škodlivý Javascript/HTML kód, který se může pokusit vytvořit podvržené přihlašovací údaje.
- 30% aplikací nekontroluje příchozí data, tak je činí náchylné na JavaScript injekce přes nezabezpečené UIWebView implementace.

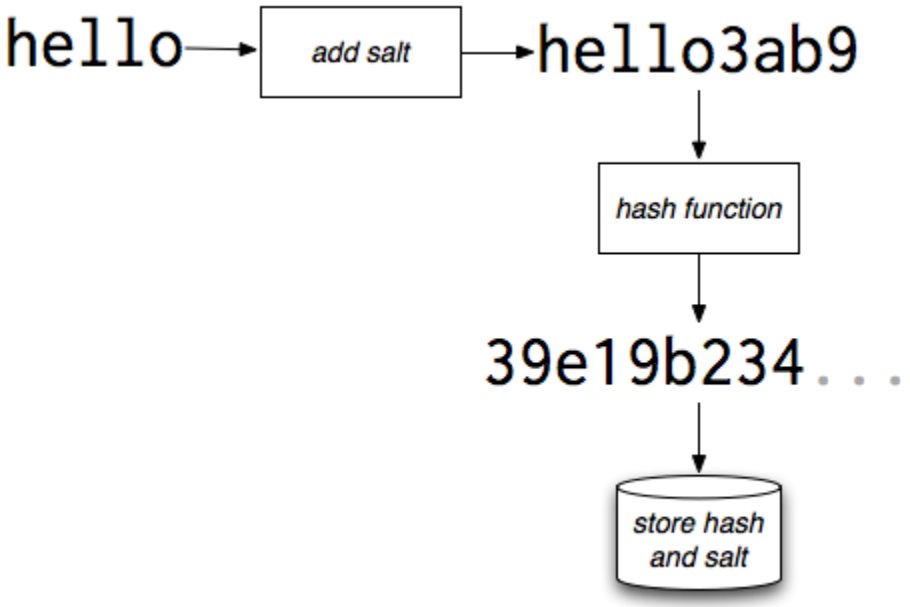
1.4.2.2 Uložení dat uživatele

Data uživatelů jsou pro jakoukoliv aplikaci klíčová. Nejen že tvoří aplikaci jako takovou, ale ohrožení jejich bezpečnosti může kriticky ohrozit celý projekt. Hlavní zásadou pro ukládání dat je zamezit uložení jakýchkoliv citlivých dat přímo v mobilním zařízení v plain/textové podobě. Pokud se jedná o uložení dat na serverech banky můžeme předpokládat, že číslo účtu se chová podobně jako PAN platební karty, k němuž se vztahuje PCI 1.4.2.4. Během prvního přihlášení uživatele je vytvořeno heslo, se kterými je třeba nakládat s nejvyšším zabezpečením. Hesla by nikdy neměla být uložena v textové podobě, ale jako hash. Při vytváření hashe je nutné použít tzv. solení, aby databáze s hesly byla odolná vůči útoku s Rainbow tables [9]. Solení hesla popisuje následující obrázek 1.11.

Jak i z obrázku vyplývá, po použití solení je v databázi uložen hash hesla a sůl. Pro ověření hesla je pak použit stejný hashovací algoritmus s přidanou solí na vytvoření hashe. Následně dojde pouze k ověření hashů. Architekti databáze by však kromě zabezpečení hesel, měli dbát i na vyžadování pravidel pro tvorbu hesel, popsané v předchozí kapitole 1.4.2.2.

[8] Secure Socket Layers/ Transport Layer Socket - transportní protokol

[9] Rainbow tables - předem vypočtené hodnoty určené k usnadnění prolomení hashovací funkce útočníkem



Obrázek 1.11: Solení hesla

Zdroj: `https://www.codeproject.com/Articles/844722/Hashing-Passwords-using-ASP-NETs-Crypto-Class`

1.4.2.3 Aplikační bezpečnost

V této kapitole se podíváme na základní bezpečnostní prvky zejména při vývoji a nasazení android aplikací. Android aplikace se od aplikací pro mobilní operační systém do jisté míry liší, zejména pokud se jedná o bezpečnost. Společnost Apple má propracovaný systém nahrávání aplikace do webového marketu, který má zamezit falšování aplikací. Každá aplikace musí projít verifikací, kdy se může programátorovi několikrát vrátit dokud není vše v naprostém pořádku. Pro vývojáře na platformě android je samotné nahrávání na google store o poznání jednodušší. Kromě toho v případě iOS je pro uživatele této platformy obtížné nahrát vlastní aplikaci do telefonu bez přístupu k apple store. K tomu je potřeba vývojářský účet u společnosti Apple nebo root práva k zařízení. Uživatelé mobilních zařízení s OS Android mohou instalovat libovolné aplikace, pokud tuto možnost povolí v nastavení svého telefonu. Kromě nahrávání je potřeba zabezpečit, aby se nikdo nedostal k datům aplikace. Na android zařízeních se s root právy dá snadno dostat do aplikační databáze pomocí příkazu sqlite3. Proto některé platební společnosti neumožňují instalaci aplikací na taková zařízení. Otázkou je zda se jedná o správný přístup, zda by nebylo efektnější zabezpečit data aplikace tak, aby neoprávněný přístup do databáze jakkoliv neohrozil uživatele. Stejná situace platí pro reverse

engineering aplikací. Některé nejsou proti tomuto zpětnému procesu sestavování aplikace chráněny. Kdokoliv tak se prakticky může dostat ke zdrojovým kódům aplikace. Nejedná se o zdrojový kód, který by se dal normálně použít, ale dovolí analýzu potencionálních chyb v aplikaci.

Další významnou součástí bezpečnosti aplikací je jejich podepisování. Pokud není aplikace dostatečně chráněná podpisem může být snadno podvržena a vydávána za originální. Každá aplikace by tak měla být chráněna dostatečně silným hashovacím algoritmem. Pro iOS mobilní aplikace tento proces do zajišťuje proces publikování aplikací na marketplace. Vývojáři mobilních aplikací pro mobilní operační systém Android musí aplikace podepisovat sami. Nástrojem k podepisování je tzv. jarsigner. Jedná se o binární archiv, který po zadání parametrů podepíše archiv požadovaným certifikátem. Celý proces podepisování nepodepisuje archiv jako takový, ale je rozdělen do tří dílčích souborů v aplikaci. První z nich se jmenuje MANIFEST.MF, v něm jsou po dvojicích uloženy cesta k souboru včetně názvu s hashem tohoto souboru. Druhý soubor s názvem CERT.SF obsahuje hashe řádků z MANFEST.MF. Poslední soubor je označen jako CERT.RSA. Tento soubor je kontainerem pro veřejný klíč aplikace z javového podepisovacího nástroje a pro podpis z CERT.SF souboru.

Každá aplikace dál vyžaduje systémová oprávnění, aby mohla používat různé prvky operačního systému. Například přístup na externí úložiště nebo na rozhraní fotoaparátu. Tato oprávnění jsou pro Android apliace specifikovány v AndroidManifest.xml souboru. Je dobré, jak při vydávání aplikace, tak při jejím samotném používání dávat dobrý pozor, jaké oprávnění potřebuje a podle toho jí povolení udělit. Pro nejnovější verze mobilních operačních systémů platí, že oprávnění mohou být udělována a odebírána i v průběhu samotného používání aplikace. V praxi to funguje tak, že aplikace si zažádá o přístup až ve chvíli, kdy jej fakticky potřebuje. Uživatel tak má lepší kontrolu nad tím, co aplikace vykonává.

Nedílnou součástí vývoje jakéhokoliv softwarového produktu je důkladné testování v celém průběhu vývoje software. S testováním je samozřejmě důležité začít ihned v okamžiku započetí vývoje, tím se dokáže zmírnit dopad případných chyb, pokud budou včas odhaleny. Každý developper by měl samozřejmě po sobě kontrolovat napsaný kód, ale takové testování nestačí, zejména podílí-li se na vývoji více lidí. Musí být provedeno také integrační testování, zda spolu jednotlivé komponenty či kusy kódu dokáží spolupracovat. Dalšími typy testů, které je třeba nepodcenit, je testování výkonu, či v případě bankovní aplikace všechna testování, která souvisí s bezpečností. Těmi jsou stress testování, penetarční testování, kdy se tester snaží využít známých chyb k prolomení do zabezpečení aplikace a další.

Nejde ale jen o implementaci, mnohdy může způsobit problémy i na první pohled neškodné logování do externích souborů moblního zařízení. Nesmí se stát, aby v případě pádu aplikace byla jakákoliv citlivá data zahrnuta do logovacích zpráv. V ideálním případě by měly být tyto reporty zakryptovány

a použitelné pouze pro oprávněné osoby.

1.4.2.4 Certifikace

Certifikace je ve světě platebních aplikací důležitou součástí jejího vývoje, zejména v případě, kdy je nakládáno s karetními daty. V tu chvíli je třeba rozlišovat mezi dvěma hlavními typy, PCI- DSS a PA-DSS. Protože aplikace, které jsou součástí zahraničního trhu používají platební karty, vztahuje se na ně povinnost splnit tyto standardy.

- PCI-DSS (Payment Card Industry Data Security Standard) - standard pro nakládání s daty držitelů platebních karet, které jsou uloženy na platební kartě. Dodržování těchto mezinárodních pravidel je vyžadováno karetními asociacemi. Tento standard je určen pro organizace, které zpracovávají, přechovávají či uchovávají data držitelů platebních karet.
- PA-DSS (Payment Application Data Security Standard) - globální bezpečnostní standard vytvořený PCI-SCC (Payment Card Industry Security Standards Council). Cílem tohoto standardu je zabránit aplikacím třetích stran, aby ukládaly zakázaná bezpečnostní data, například. data z magnetického pásku, CVV2, či PIN. Pokud aplikace jakkoliv ukládá, zpracovává, nebo přenáší citlivá karetní data, pak je tato aplikace považována za platební a spadá do rozsahu PA-DSS.

Oba standardy mají za úkol, co nejvíce ochránit držitele platebních karet. Snaží se zamezit tvůrcům aplikace, aby ukládali data v nezakryptované podobě, nepoužívali nedostatečné hashovací stanardy atp.

Kapitola 2

Mapování trhu

Pro provedení návrhu služby P2P plateb pro český trh, je dobré nejprve provést mapování trhu. Zejména abychom získali přehled o konkurenci a případně se vyvarovali chyb, se kterými se možná již ostatní poskytovatelé potýkali. Vzhledem k tomu, že český trh v současnosti žádné služby obdobného druhu nenabízí, zaměříme se na trh zahraniční. Co se zahraničních poskytovatelů týče, P2P platby jsou populární ve vyspělejších státech, což je dáno do jisté míry technologickou vyspělostí a dále i vyšší životní úrovní obyvatel. Tyto služby tak fungují ve Spojených státech, ve spojeném Království a dále Číně. Poté si rozebereme základní benefity a rizika P2P služeb, klíčové faktory úspěchu. Dále následuje kapitola o bezpečnosti dostupných aplikací. V závěru se zaměříme na specifika českého trhu a provedeme celkové shrnutí.

2.1 Rozbor existujících sluzeb

V následující kapitole je proveden rozbor populárních zahraničních služeb. Původním záměrem bylo zmapovat všechny služby, jenže vzhledem k jejich nedostupnosti na našem trhu se jedná o krok téměř nemožný. Dalším důvodem jsou shodné znaky, které jednotlivé aplikace vykazují. Byly tak vybrány pouze aplikace některé. U těch, které jsou nejvíce specifické je provedeno mapování procesu registrace a platby. Jak již bylo zmíněno v kapitole P2P platby 1.3.2.3, poskytovatelé P2P plateb se dají rozdělit do několika kategorií. Z hlediska mapování tak byly vybrány zejména aplikace třetích stran a dále aplikace jejichž poskytovateli jsou bankovní instituce.

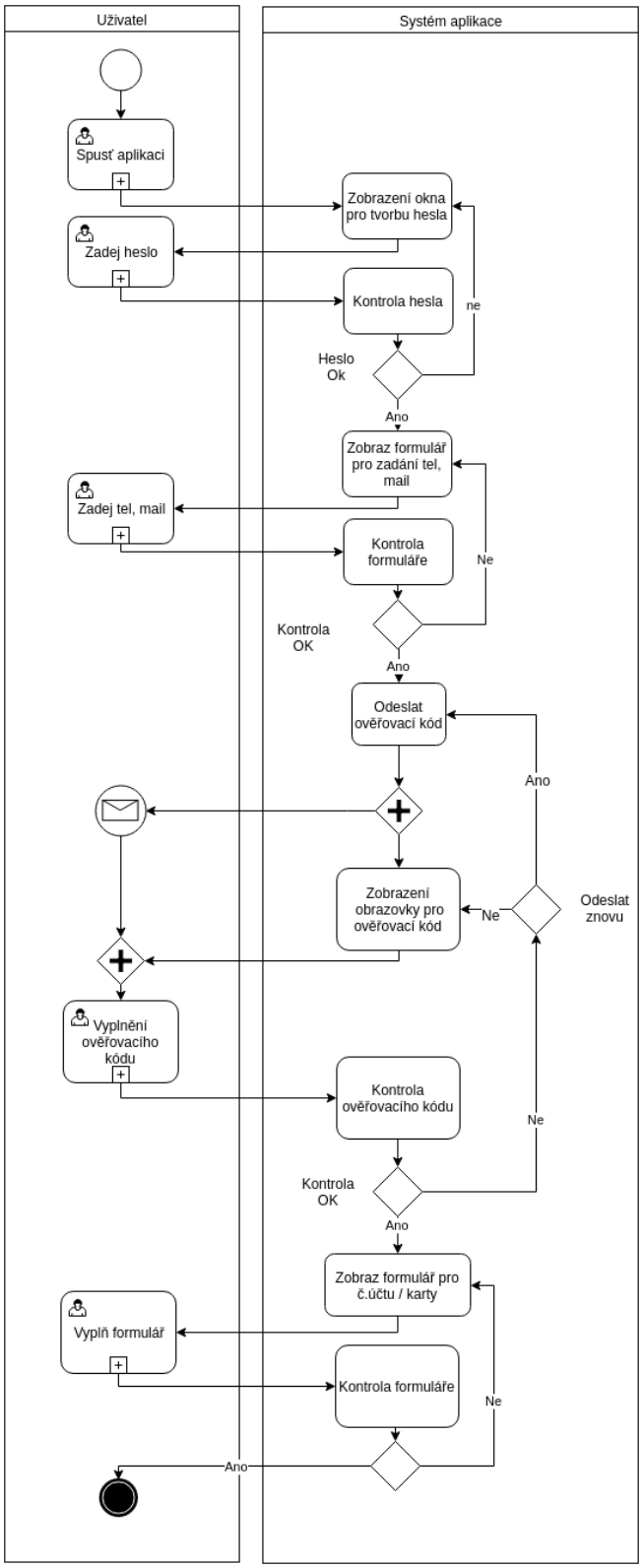
2.1.1 Venmo

Tato služba vnikla jako startup stejnojmenné společnosti v roce 2009. Zakladateli této společnosti jsou Andrew Kortina a Iqram Magdon-Ismail. Původním záměrem tvůrců bylo vytvořit službu, která by umožňovala placení za multimediální obsah pomocí SMS. Teprve v pozdějších fázích vývoje dostala služba

podobu aplikace. Venmo se jako online služba objevila již v roce 2009, ale zůstala pro širokou veřejnost nedostupná po dva roky jejího testovacího provozu. Jejími klienty se mohli lidé stát pouze na pozvání. Službu si její tvůrci ponechávali v tajnosti, dokud se jim nepodaří snížit čas potřebný k uskutečnění převodu peněz z účtu na účet. Což se jim nakonec z původních několika dní podařilo snížit na hranici jednoho dne. Platba v rámci této služby tak probíhá prakticky přes noc. Díky pilotnímu provozu získala zpočátku i jakýsi punc exkluzivity a tak ještě před samotným spuštěním již zpracovávala $10 milonů měsíčně na mobilních platbách. Po jejím spuštění se stala virální a počet jejích uživatelů raketově rostl. V současnosti je služba využívána kolem 550 000 uživateli a zpracovává přes $3,2 miliardy ročně. Plánem společnosti je nahradit kreditní karty, a přímo spolupracovat s POS. Společnost již není dávno startupem, v srpnu roku 2012 ji za $26,2 milionu koupila společnost Braintree. A dokonce společnost Braintree se dočkala akvizice se společností Paypal za celkovou částku kolem $800 milionu [20].

Tato aplikace má samozřejmě svá specifika, která ji činí unikátní. Vzhledem k popularitě sociálních sítí v době vzniku aplikace, vnáší služba do finanční transakce jakýsi sociální faktor. To znamená, že aplikace obsahuje stránku, kde se uživatel může dozvědět, kdo komu a za co zaplatil a to nejen v okruhu jeho přátel, ale dokonce globálně. Nabízí se otázka, do jaké míry je tato vlastnost výhodou a do jaké míry se jedná o narušení soukromí a nadužívání sociálních sítí. Naštěstí tvůrci aplikace mysleli i na skeptické uživatele vůči této vlastnosti a v nastavení aplikace je možnost si nastavit úroveň soukromí. Od možnosti zveřejňovat vše, přes zveřejnění okruhu známých a přátel po kompletní zákaz sdílení informací. V rámci této sociální sítě samozřejmě nejsou sdíleny žádné citlivé informace jako telefonní číslo, číslo karty či placená částka. Jedná se pouze o informaci kdo je plátcem, kdo příjemcem a co je předmětem platby, neboli poznámka, která je v rámci každé platby možná specifikovat. Navíc má tato vlastnost pozitivní přínos pro službu i z psychologického hlediska. Toto chování popsal ve své knize “Psychologie davu” francouzský psycholog Gustav le Bone. Můžeme aplikovat jeho poznatky na funkcionalitu ekosystému aplikace. Dospějeme tak k závěru, že pokud uživatel služby má pocit, že ji vyžívá velká spousta dalších uživatelů, dostává se mu do jisté míry pocitu bezpečnosti a sounáležitosti s ostatními uživateli. Tato služba tak i díky sociálnímu faktoru zjevně cílí na mladé uživatele pod 30 let. Díky viralitě se dokonce stává, že uživatelé používají název aplikace jako synonymum pro samotnou platební transakci (“Venmo me”). Jsou zde ovšem i další vlastnosti kterými je tato služba specifická. Jednou z nich je proces registrace, který je pro každou službu klíčový. Tento proces je představen na následujícím diagramu 2.1.

Jak z obrázku 2.1 vyplývá, po spuštění aplikace je zobrazena tabulka pro specifikaci hesla. V dalším kroku zadá uživatel svoje telefonní číslo či e-mailovou adresu. Na tento kontakt je zaslána ověřovací zpráva. Smyslem tohoto kroku je vytvořit klíčové spojení kontaktu se samotným číslem účtu. Jelikož se jedná službu třetích stran, je v posledním kroku registrace rovněž



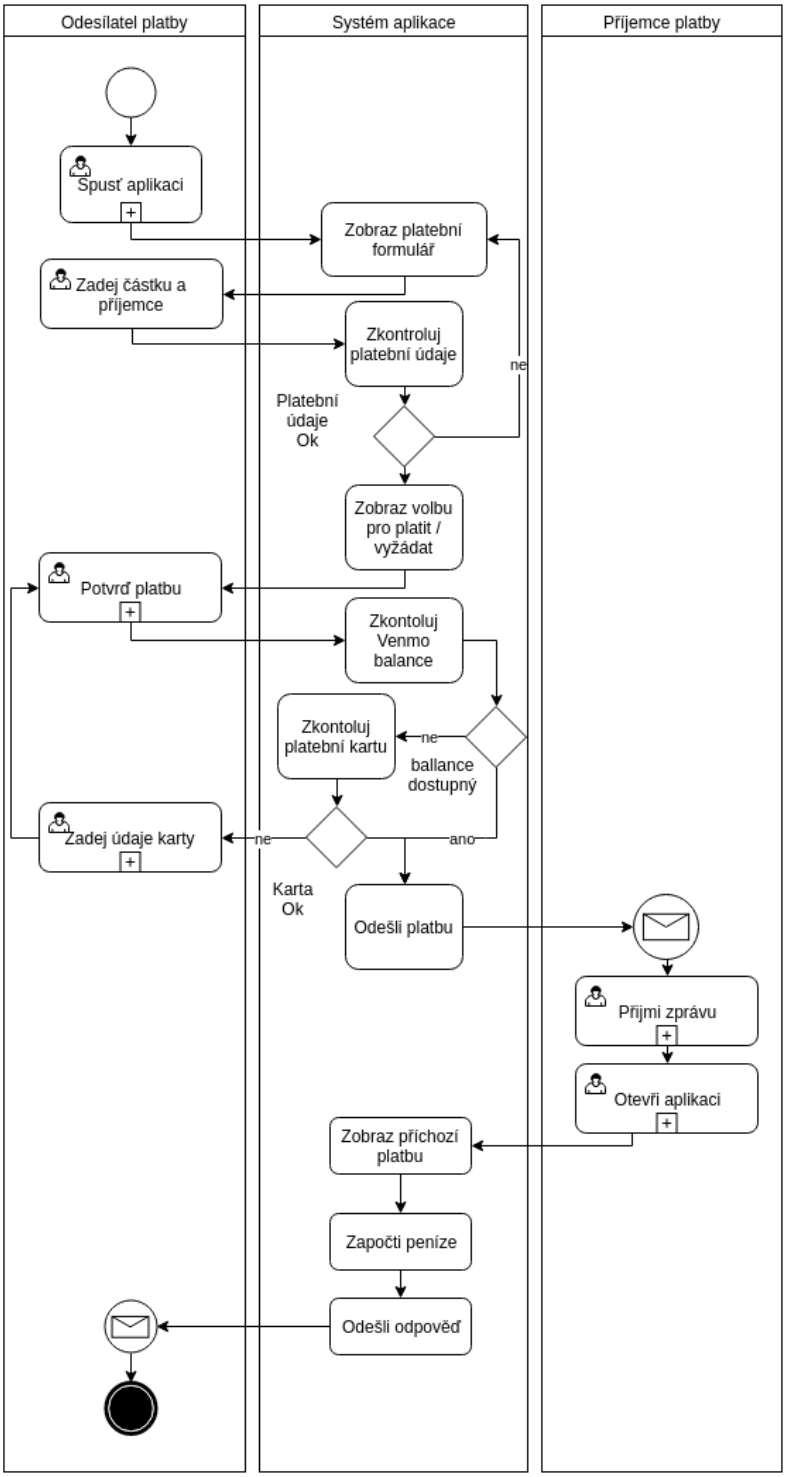
Obrázek 2.1: Proces registrace Venmo

nutné zadat číslo účtu či bankovní karty. Pro provádění plateb musí být registrován jak odesílatel, tak i příjemce. V případě příjemce platby je vlastník telefonního čísla či e-mailové schránky vyzván k registraci v okamiku obdržení platby.

Druhý obrázek 2.2, který se vzahuje k této službě, popisuje proces platby. Aby mohla být služba úspěšná, musí být posloupnost jednotlivých kroků intuitivní a neměl by obsahovat žádné zbytečné kroky. Jak lze vidět z obrázku, jednotlivé kroky jsou opodstatněné. Elektronické peníze jsou v rámci služby uloženy ve virtuální peněžence, Venmo ballance. I v případě nedostatečného množství "peněz" ve virtuální peněžence, není uživatel při platbě příliš omezen. Transakce může být prováděna rovněž přímo z primárního zdroje financování, který si může uživatel nastavit. V tom případě samozřejmě transakce trvá déle. V případě transakce z penženky do peněženky se jedná o transakci instantní. Pro usutečnění transakce musí druhá strana platbu přijmout. Pokud tak neučiní, peníze se vracejí po určité době zpět odesílateli. Prováděné transakce jsou zdarma, jedinou vyjímku ale tvoří platba kreditní kartou, která je zpoplatněna 3%. Tento poplatek není určen pro autory služby, ale jedná se pouze o přenesení bankovního poplatku banky.

Aplikace je certifikována podle standardu PCI 1.4.2.4. Přesto její uživatelé od počátku jejího fungování reportovali řadu chyb, které by se do produkční varianty aplikace neměly dostat. Jedna z nejzávažnějších chyb byla ve spojitosti s hlasovou asistentkou Siri na mobilních telefonech společnosti Apple. Při zaslání požadavku k platbě existovala možnost i v případě zamčeného displaye telfonu odpovědět na SMS zprávu a dokončit tak provedení samotné platby. Nejedná se o chybu v implementaci, zde lze spíše mluvit o chybě v návrhu aplikace. Společnost samozřejmě vydala záplatu, která znemožňuje provádět platby na zamčené obrazovce a dále zakazuje provádění hromadných plateb pomocí hlasové asistentky. Další bezpečnostní chybou, kterou uživatelé hlásili bylo naprosté ignorování změny hesla či důležitých nastavení aplikace. Poslední zásadní věcí kterou by měla obsahovat každá platební aplikace je snadná dostupnost aplikačního helpdesku s 7/24 podporou.

Služba byla založená v US a je dostupná pouze pro občany Spojených států. Narozdíl od konkurenční služby stejného vlastníka PayPal, která je dostupná celosvětově. Využití služby nacházejí její uživatelé zejména při potřebě rozdělit účet mezi více osob. Sociální faktor aplikace je zajímavou vlastností, ale uživatel musí být přinejmenším opatrný jaký typ plateb zveřejňuje do sociální sítě. Po dobu působnosti služby se její funkčnost, vzhled i bezpečnost rapidně zlepšily. V současnosti poskytuje společnost krytí každě neoprávněné transakce, pokud její vlastník splní stanovené podmínky. Přesto a právě proto vybízí uživatele k pravidelným kontrolám prováděných transakcí, aby nedocházelo ke kompromitaci osobních údajů a krádeži elektronických peněz.



Obrázek 2.2: Proces platební transakce Venmo

2.1.2 Square cash

Druhým velice významným hráčem na poli P2P služeb je společnost Square Inc. se svým produktem Square Cash. Společnost Square Inc. založil výkonný ředitel společnosti Twitter, Jack Dorsey. Podobně jako v případě Venmo si společnost nechávala čas na průběh pilotního provozu, ale v tomto případě šlo pouze o 4 měsíce. Služba byla do pilotního provozu spuštěna v květnu roku 2013, ale pro širokou veřejnost byla dostupná již v září. V průběhu pilotního projektu se lehce lišil i způsob účtování za provedení transakce. Původně si společnost nechal platit $0.50 za jednu transakci. V produkční variantě služby již tyto poplatky nadobro zmizely.

Hlavním specifikem, kterým se tato služba pyšní, je neuvěřitelná snadnost použití. Aplikace jako taková je velmi minimalistická, neobsahuje žádné dodatečné funkce a z jejího používání je zřejmý její primární účel. V porovnání s konkurenční službou Venmo nemá tato služba žádný účet fungující jako peněženka. Celý proces platby funguje jako převod z jednoho bankovního účtu (nebo kreditní karty) odesílatele do druhého účtu příjemce. Produkt manažer Brian Grassadonia popořil tuto myšlenku vyjádřením, že lidé nechtějí používat jejich peníze na sekundárním účtu. Ale chtějí je mít k dispozici tam, kde se ve skutečnosti nacházejí, na bankovním kontě. Celá aplikace tak působí jako zjednodušený e-mailový klient. Zásadní vlastností tohoto produktu je možnost maskování uživatelů za tzv. cashtagy. Jedná se o způsob mapování čísla účtu či karty za unikání název. Například $DonateMe123. Obdobná vlastnost je typická i pro sociální síť Twitter, kde uživatelé mohou vyžívat tzv. hashtagy (#neco) pro vyjídření klíčových slov v jejich sdělení. Nespornou výhodou v jednoduchosti použití je jiná politika pro registraci příjemců platby. Pokud ze svého Square Cash pošlete platbu osobě, která není v této službě zaregistrována, příjemce obdrží zprávu o přijetí finančního obnosu. Jediné co příjemci pro dokončení platby stačí učinit, je zadat číslo debetní nebo kreditní karty. Není potřeba žádné registrace. Registrace je vyžadována až v okamžik platby.

Jednoduchost aplikace občas má tendenci budit podezření ohledně zabezpečení aplikace. Kromě toho e-mail komunikace není obecně považována za dostatečně zabezpečený platební kanál. Odpůrci služby by mohli namítnout, že dostávají tisíce spamových zpráv a celý koncept tak pro ně působí nedůvěryhodně. Společnost se s pochybami o bezpečnost vypořádala uveřejněním zprávy o existenci systému, zabraňujícímu podrvržení e-mailové komunikace. Přesto odmítla poskytnout jakékoliv další detaily. Pomyslnou útěchou uživatelům může být alespoň informace o certifikaci aplikace PCI Data Security Standard (PCI-DSS) Level 1 a zabezpečení komunikace pomocí SSL s PGP klíčem o minimální délce 128 bitů [21].

První diagram 2.3 opět popisuje proces registrace do této služby. Jak lze vidět, po spuštění aplikace je zobrazen formulář pro vyplnění všech nezbytných údajů. Po ověření formuláře je klientovi odeslána potvrzovací sms na zadané telefonní číslo. Po jeho ověření následuje krok z něhož není na první pohled

zřejmý jeho záměr. Aplikace je dostupná ve dvou variantách, pro firemní zákazníky a pro běžné uživatele. V tomto kroku je tak zvolena požadovaná varianta. Problém nastává ve chvíli pokud by uživatel měl zájem použít účet pro oba účely. Po potvrzení volby musí uživatel přejít do nastavení aplikace, aby mohl specifikovat dodatečné informace propojení s požadovaným bankovním účtem či debetní platební kartou.

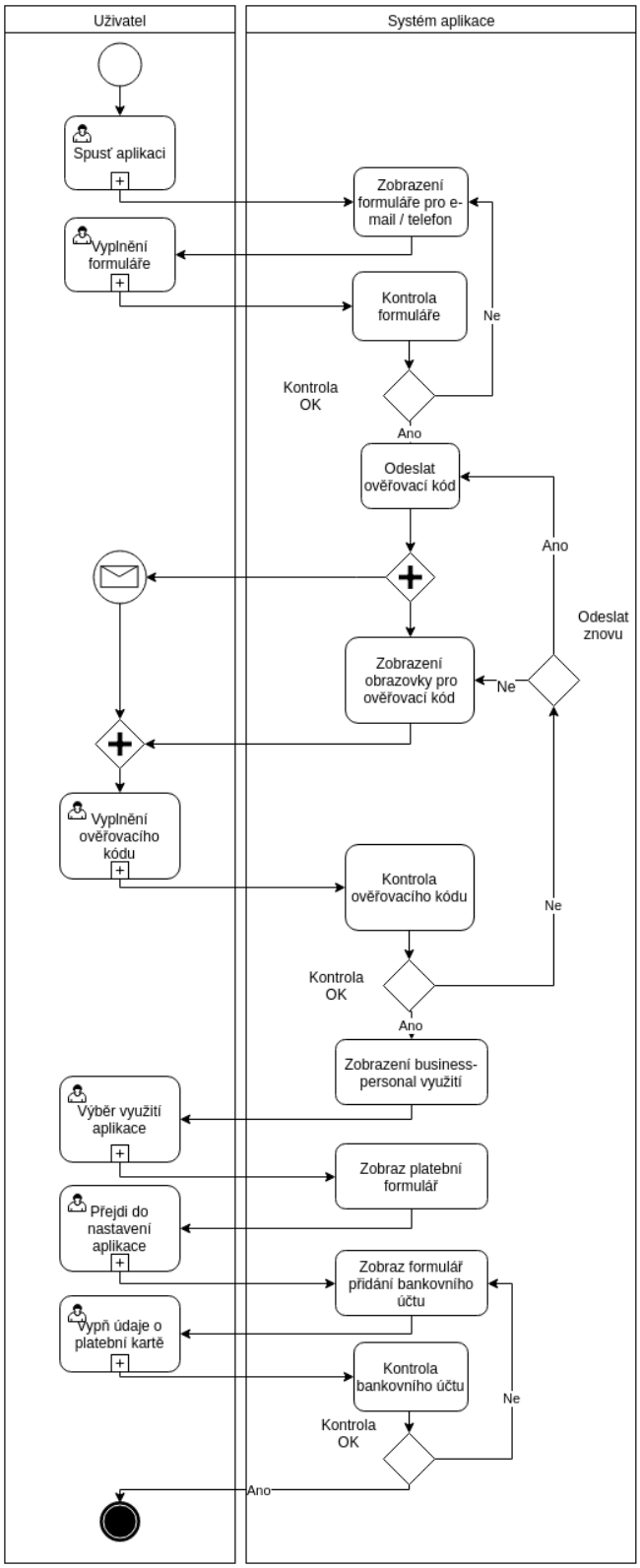
Druhý diagram 2.4 popisuje proces platby se Square Cash. Až do okamžiku odeslání platby se proces neliší od procesu v případě Venmo. Zde je zřejmé, že uživatel musí explicitně přijmout či zamítnout platbu. Bez tohoto kroku je platba po určité době vrácena zpět odesílateli. To má vliv i na situaci kdy není příjemce zaregistrován. V tom případě mu je doručena zpráva o příchozí platbě a je na uživateli, zda vyjádří svůj souhlas s příjetím platby instalací aplikace. Nebo tacitně vyjádří své zamítnutí transakce ignorováním přijaté zprávy. V každém případě je odesílatel informován o průběhu transakce. V případě schválení transakce jsou příjemci připsány na debetní kartu finanční prostředky, které byly předmětem transakce. V opačném případě se elektronické peníze vrátí zpět k odesílateli.

2.1.3 Barclays Pingit

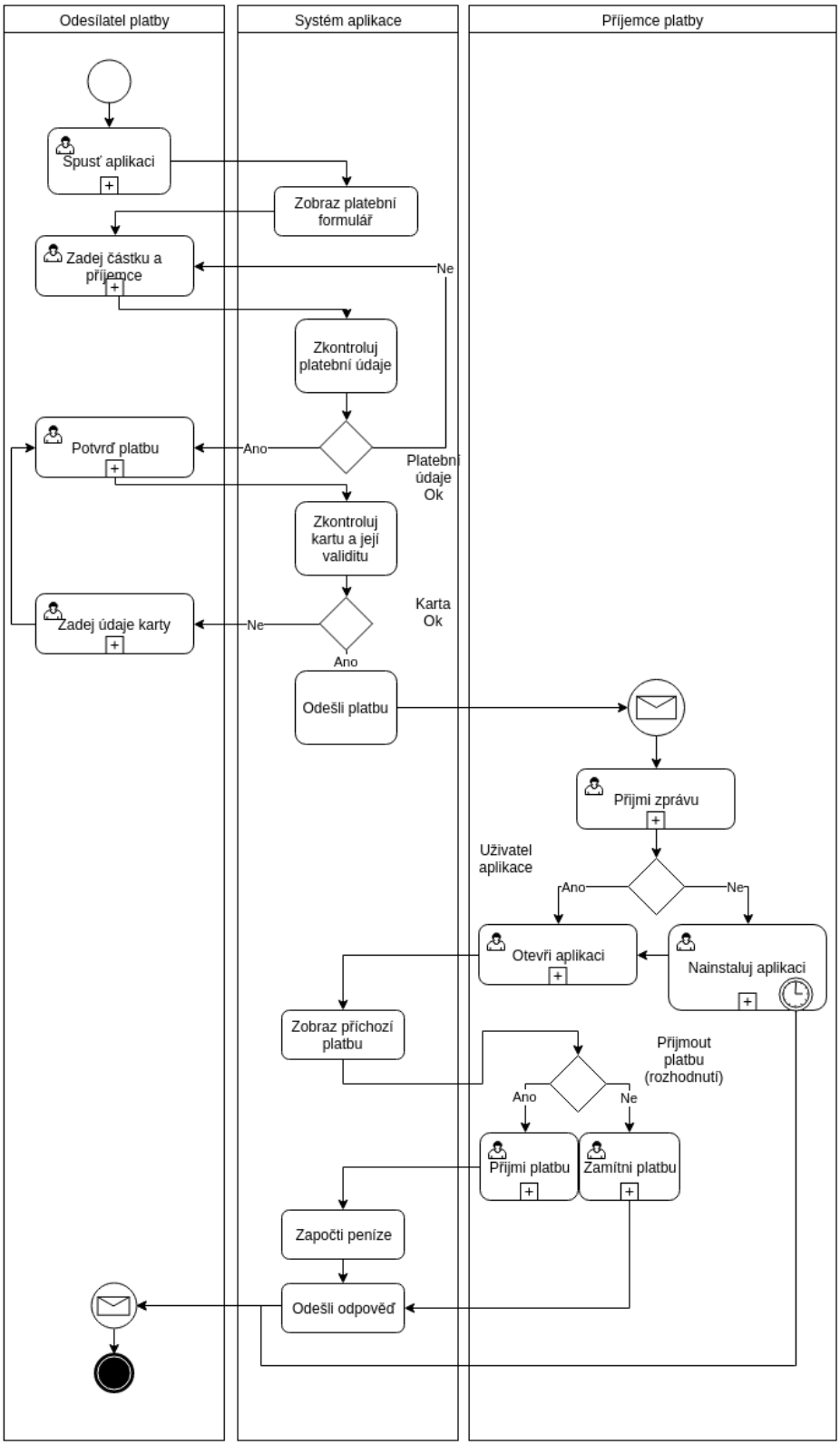
Pingit je P2P služba, kterou nabízí nadnárodní finanční společnost Barclays jako jeden z produktů svého portfolia. Služba vznikla v únoru roku 2012. Společnost prezentovala svou projekt “Schopnost platit přátelům a obchodníkům jednoduše používáním telefonu” jako první na evropském trhu. Ostatní banky ji v tomto záměru brzy následovaly. Původním záměrem banky byla služba dostupná pouze pro vlastní klienty s věkovým limitem nad 18 let. U každé platební aplikace je ovšem klíčová její univerzálnost. Proto ji později rozšířili na všechny klienty s UK bankovním kontem. S tímto krokem zároveň snížili věkovou hranici na 16 let.

V červnu roku 2015 se služba spojila se službou Zapp, aby umožnili použití Pingit s POS a pro internetové transakce, kde je zobrazen symbol zaplatit bankovní aplikací. V té době už tuto službu používalo kolem 2 milionů aktivních uživatelů. Což se za tříleté působení v této oblasti dá považovat za obrovský úspěch. Takovýto výsledek si samozřejmě žádá pozornost i od ostatních nejen platebních společností. V témže roce tak došlo ke spuštění podpory Pingit plateb v Národní loterii. Pořád se ale jednalo projekt v rámci jedné banky. Finanční instituce (Payments Council) tak později přišly s nápadem umožnit jednotlivým službám spolu komunikovat, tak aby z každého účtu založeného v UK šlo platit na všechny ostatní pouze se znalostí telefonního čísla. Vznikla tak služba PayM. Uživatelé, kteří již mají založený účet u společnosti Barclays si ovšem nemusí zakládat účet nový, ale mohou plynule přejít na používání aplikace PayM [22].

Nyní se dostáváme k samotnému využívání aplikace. První fází je opět registrace, která je popsána na následujícím obrázku 2.5. Registrace do této



Obrázek 2.3: Proces registrace Square Cash

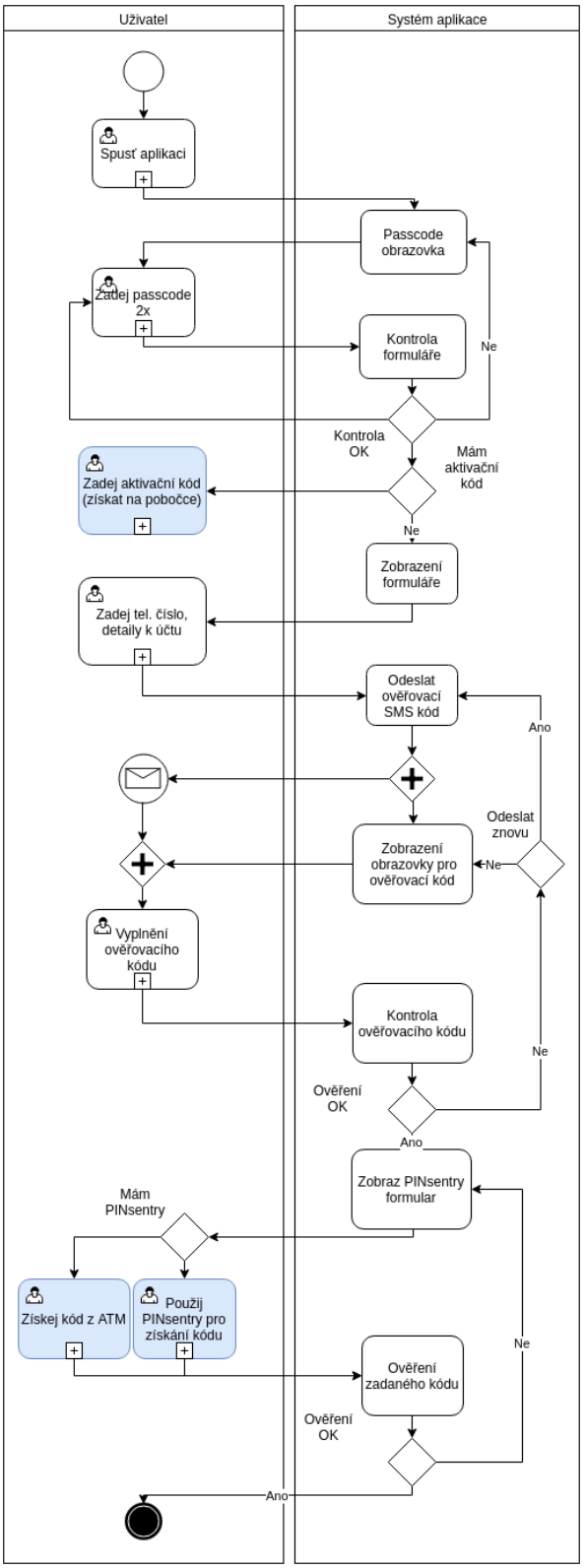


Obrázek 2.4: Proces platební transakce Square Cash

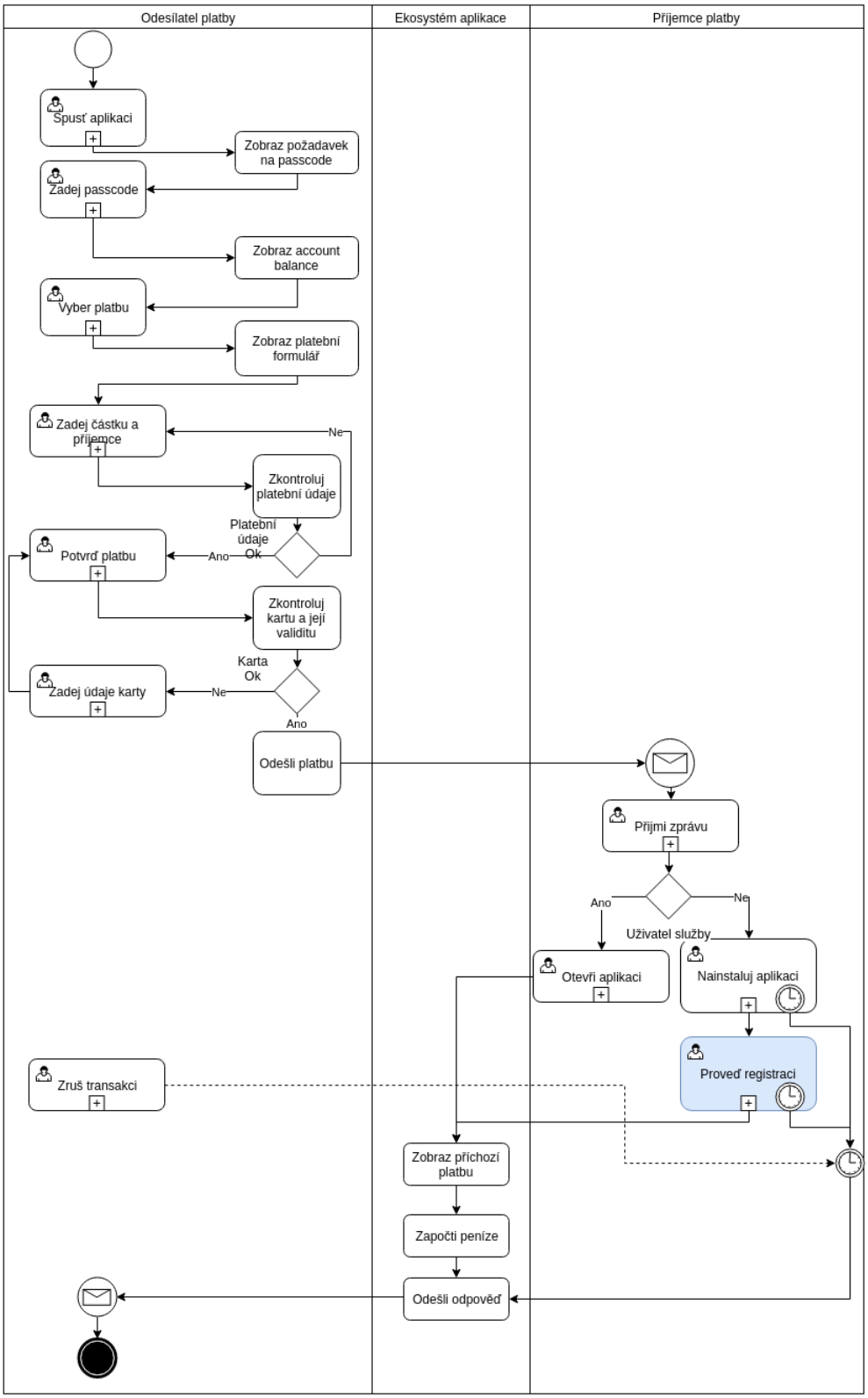
služby, není rozhodně tak přímočará jako tomu je v případě ostatních služeb a do jisté míry ji tak lze označit za unikátní v rámci zkoumané množiny služeb. Jak lze vidět na tomto diagramu, samotný začátek procesu je stejný jako v případě ostatních služeb. Dojde ke zvolení hesla a jeho následného ověření. Jedná se o pětimístné heslo a musí splňovat určitá pravidla. Jelikož se jedná čistě o numerické heslo, nesmí proto obsahovat například více jak tři po sobě jdoucí shodné znaky. Nesmí také obsahovat jednoduché kombinace jako 12345. Smyslem tohoto požadavku na zabezpečení je především zamezit okamžitému neoprávněnému přístupu do aplikace. Dále následuje obrazovka, která dává uživateli možnost výběru dalšího postupu. Je zde možnost zadání kódu, pro jehož obdržení je potřeba navštívit kamennou pobočku banky. Nebo pokračování v získávání osobních informací o klientovi jako v případě ostatních služeb a jejich následné ověření. V případě druhé volby je v dalším kroku potřeba ověřit platební kartu. V tuto chvíli je zapotřebí vlastnit zařízení PIN Setry, do kterého je vložena karta a po zadání PIN vygeneruje klíč, který je nutné následně zadat zpět do aplikace. Nebo je možné navštívit jakýkoliv bankomat, a poté opět vložit získaný kód.

Následující obrázek 2.6 stejně jako v předchozích případech popisuje proces platby. Prvním krokem po spuštění aplikace je zadání kódu, který je vyžadován při každém spuštění aplikace. Dále následuje požadovaný výběr typu transakce (platba či požadavek), zadání částky a příjemce. Po odeslání platby dostane její příjemce zprávu. Zde se aplikace liší oproti ostatním. Aby příjemce platby obdržel odesílanou placenou částku, musí se po obdržení zprávy do 24 hodin zaregistrovat, jinak bude platba zrušena. Což znamená poskytnout bance své mobilní telefonní číslo. Pokud příjemce nemá chytrý mobilní telefon, může se zaregistrovat rovněž přes webový prohlížeč svého počítače. Pokud blíže nahlédneme do obchodních podmínek společnosti, zjistíme, že banka má oprávnění použít poskytnuté údaje k obchodním a marketingovým účelům. To znamená, že jakmile se příjemce zaregistruje aby obdržel zaslané peníze, otevírá dveře svého mobilního telefonu spamovým zprávám od společnosti Barclays. Pokud by se tedy chtěl následně z této služby odhlásit a vymazat tak své telefonní číslo z databáze, musí poslat dopis zákaznickému oddělení Barclays, nebo osobně navštívit pobočku banky.

Používání služby společnosti Barclays s sebou stejně jako v ostatních případech přináší i řadu problémů, se kterými se služba musela nebo musí potýkat. Prvním problémem je postup v případě výměny mobilního telefonu. Služba se přímo váže na telefonní přístroj, proto v okamžiku jeho výměny je potřeba znovu projít procesem registrace 2.5. Pokud bude příjemci v době, kdy si mění svůj přístroj poslána platba, nemůže mu být doručena a může se stát, že zůstane v systému služby 24h a poté bude odeslána zpět jako zamítnutá. Kromě toho banka opět ve svých obchodních podmínkách uvádí, že není zodpovědná za platby provedené na špatné telefonní číslo. V případě že se odesílatel splete a rychle tuto skutečnost bance ohlásí, je pouze na ní jak se s touto transakcí vypořádá. Další vlastností této služby je její nedostupnost na telefonech s root



Obrázek 2.5: Proces registrace Barclays Pingit



Obrázek 2.6: Proces platební transakce Barclays Pingit

právy. Jedná se o do jisté míry bezpečnostní opatření, ale pro mnohé uživatele to bude důvodem k využití služeb konkurence.

2.1.4 PayM

PayM je mobilní platební systém, který byl představen ve Spojeném království. Opět se jedná o P2P službu která má cíl zpřístupnit placení mobilním telefonem pouze se znalostí telefonního čísla příjemce. Hlavním specifikem a dá se říci i výhodou této služby je fakt, že vznikala v mezibankovním prostředí. Službu v dubnu 2014 uvedl na trh britský Payments Council a podílelo se na ní devět velkých bank. Jedná se o Bank of Scotland, Barclays, Cumberland Building Society, Danske, Halifax, HSBC, Lloyds Bank, Santander a TSB. Během jednoho roku se k této úmluvě přidaly další banky jako The Royal Bank of Scotland, Yorkshire Bank a další. Službu PayM tak v současnosti podporuje 9 z 10 britských bank. Tím si mohla vybudovat obrovskou uživatelskou základnu, kterou v roce 2016 tvoří 3,2 milionu uživatelů. Přestože byla vyvinuta ve spolupráci všech velkých bank, byl i zde velký prostor pro optimalizaci času potřebného pro uskutečnění mezibankovního převodu. Hranice se tak zastavila na 2 hodinách. Služba je běžně zdarma, ale její použití může být dále zpoplatněno v závislosti na podmínkách podílejících se bank. Jak již bylo zmíněno, například společnost Barclays nabízela podobný produkt již před spuštěním této služby, projekt byl ale pro banku natolik výhodný, že se přesto rozhodla se do projektu zapojit a uchovat obě služby. Nacházejí se mezi nimi ale rozdíly. Například pro používání PayM musí mít všechny zainteresované strany banku v UK zatímco pro Barclays Pingit toto pravidlo neplatí.

2.1.5 Radius Pay a friend

Následující služba je opět zástupcem kategorie čistě bankovní aplikace. Služba vznikla teprve na začátku roku 2016 v USA, jedná se tedy o poměrně mladou službu. Služba je produktem banky Radius Bank. Narozdíl od ostatních služeb se nejedná o samostatnou aplikaci pro P2P, ale tuto funkcionalitu implementovala přímo do mobilního bankovnictví. V menu “transakctions” volbou “Pay a Friend”, přejde klient na požadovanou funkcionalitu. I přes fakt, že se jedná o službu bankovního subjektu, banka nepožaduje po příjemci platby registraci, ani být klientem stejné banky. Pro příjem platby stačí po obdržení upozornění vyplnit informace o bankovním účtu či debetní kartě. Pokud si příjemce zvolí debení kartu, jsou elektronické peníze připsány na účet téměř okamžitě. Příjemce platby má 10 dní od obdržení oznámení o probíhající platbě na zadání svých údajů. Pokud tak neučiní peníze jsou poslány zpět odesílateli, na jehož účet budou přípsány během 1-2 pracovních dnů. Pro odesílání platební transakce existuje samozřejmě více omezení. První z nich je nutnost vlastnit Radius debetní platební kartu prolinkovanou s osobním účtem v Radius bance. Druhé omezení je, že uživatel musí být být zaregistrován do mobilního

a online bankovnictví. Bez splnění těchto dvou podmínek nemůže uživatel provádět platební transakce pomocí P2P služby této banky. Při přihlašování do aplikace je po uživateli vyžadováno heslo. Neobvyklý je však následně fakt, že číslice nejsou pokaždé na stejném místě, ale dochází k jejich promíchání. Toto má zabránit možnosti odhadnout heslo pro přístup do aplikace pomocí otisků na dotykovém displeji mobilního zařízení. Služba je jinak poskytována klientům zdarma.

2.1.6 Google Wallet

Google Wallet je službou všeobecně známé společnosti Google, která poskytuje celou řadu služeb po celém světě. Služby od této společnosti poskytují do jisté míry záruku kvality, a tudíž již v okamžiku vzniku jeví zájemci o službu zájem. Google Wallet je služba, která za dobu její existence prošla velkým vývojem. Poprvé byla představena na tiskové konferenci v květnu 2011 a následně první aplikace vznikla v září 2011. Původním cílem služby bylo použití platebních karet v mobilním telefonu a použití technologie NFC. Google Wallet v sobě tak obsahovala emulaci platebních karet a dále možnost nahrát věrnostní karty obchodníků. Samotná integrace P2P do služby přišla až v květnu 2013, kdy Google přišel s nápadem propojit Google Wallet a Gmail a umožnit zákazníkům odesílat elektronické peníze prostřednicvím Gmail příloh. V roce 2015 došlo k rozdělení Google Wallet na dvě samostatné aplikace. Google Wallet si uchovala P2P platební službu a umožnila přístup zákazníkům s provedeným "root" telefonu. Platba prostřednictvím bankovních karet a využití věrnostních karet byla odsunuta do nové aplikace s názvem Android Pay. Hlavním důvodem tohoto kroku byla schopnost konkurovat službě společnosti Apple s názvem Apple Pay. Mimo jiné tento krok umožnil zpřístupnit P2P i jiným zákazníkům než jenom vlastníkům zařízení s operačním systémem Android. Faktem však je, že nepotěšil celou řadu do té doby spokojených zákazníků. Původní záměr univerzální aplikace pro platbu pomocí HCE a zároveň P2P byl pro mnohé důvodem k využívání této služby.

Google Wallet aplikace je dostupné pouze pro klienty v USA, zatímco integrace s Gmailovým klientem je dostupné i pro zákazníky ze zemí Spojeného Království. S Google Wallet je tak možné posílat transakci na libovolný emailový účet. Služba pracuje s tzv. "Wallet Ballance", jedná se o virtuální účet u společnosti Google, kam si klient může nahrát své elektronické peníze a zároveň je z něj odesílat. Využití tohoto účtu není povinné, klient může využít přímého převodu ze spárovaného bankovního účtu či platební karty. V případě bankovního účtu, Wallet Ballance či debetní karty je služba zdarma. Při převodu z kreditní karty se účtuje 2,95% poplatek. Nevýhodou služby je nejasně definovaná doba převodu finančních prostředků, kdy na stránkách poskytovatele je uvedena standardní doba převodu jako 3 dny, ale bohužel není nikde naspecifikována maximální garantovaná doba převodu. Zkušenosti zákazníků služby z internetových fór však hovoří i o převodech trvajících 10 dní. Přijetí

platby probíhá obdobně jako v případě služby Square Cash, příjemce se tak nemusí registrovat ale stačí mu vyplnit formulář pro zaslání peněz.

I taková společnost jako je Google se ve svém produktu potýkala s vážnými chybami, které mohly ohrozit uživatele mobilní aplikace. Existovala totiž možnost jak se dostat přes zabezpečení aplikace. Stačilo vymazat data aplikace, následně opět spustit aplikace. Ta si znovu vyžádala nastavení. Jelikož je ale již spárovaná s telefonem, stačilo nastavit nový pin a původní karty přítomné v aplikaci byly obnoveny.

2.1.7 PayPal.me

Internetová platební společnost PayPal s 170 miliony aktivních klienty spustila v roce 2015 službu s názvem PayPal.me, která je přímým konkurentem společnosti Venmo. Nabízí se proto srovnání s touto službou. PayPal je v porovnání s Venmo spojený s emailovou adresou a platba trvá 3 dny. Dále cílem Paypal.me nebylo vytvořit kopii Venmo, ale přinést i něco navíc, jedná se proto o službou dostupnou i za hranicemi US. Konkrétně je PayPal.me dostupná ze 17 států kromě U.S. Z uživatelského pohledu přináší Venmo lepší uživatelský zážitek. Paypal.me je součástí běžné aplikace a je tak její použití o něco komplikovanější. Pro posílání a příjem plateb je nutné mít založený účet. Při registraci si uživatel vytvoří jedinečný internetový odkaz ve tvaru paypal.me/ <jedinečný řetězec>, který je možný dále používat jako náhradu za telefonní číslo či emailovou adresu. Služba využívá opět virtuálního účtu PayPal Ballance, na který jsou účtovány všechny platby. Služba je mimo posílání elektronických peněz mezi přáteli určena také obchodníkům, kteří tak mohou jednoduše dostat zaplaceno. Garantovaná doba doručení platby jsou 3-4 hodiny [23].

Paypal jako společnost je proti Venmo daleko větší a nevynakládá takové prostředky na marketingové účely. Hlavním důvodem je zejména fakt, že vzhledem k velikosti klientské základny společnosti PayPal, jsou P2P platby zanedbatelnou částí jejich příjmů.

Zabezpečení služby je opět na relativně vysoké úrovni. Služba je držitelem certifikátu PCI. Komunikace probíhá přes SSL s klíčem o minimální délce 128 bitů. Ještě před samotnou registrací server kontroluje zabezpečení spojení včetně verze prohlížeče a dále iniciuje spojení pouze pokud klient podporuje SSL ve verzi 3.0 a vyšší.

2.1.8 ClearXChange

ClearXChange je služba, která vznikla ve spolupráci velkých národních bank v US. V současnosti se na celém ekosystému podílejí Bank of America, Capital One, Chase, FirstBank, Frost, U.S. Bank a Wells Fargo. Zakládajícími členskými bankami byly Wells Fargo, Bank of America a Chase. ClearXChange neprovádí platby v pravém slova smyslu, ale spíše předává informace, které

banky potřebují pro uskutečnění transakce. Aby klient mohl posílat platby, potřebuje US bankovní číslo jedné z podporovaných bank zmíněných výše. Pro příjem platby existuje navíc možnost se zaregistrovat přímo u ClearXChange. Tato možnost je důležitá zejména pokud banka u které má klient svůj účet není zapojena do partnerské sítě. Je tak zřejmé, že pro příjem plateb musí být klient zaregistrován. ClearXChange nemá žádnou svou vlastní aplikaci. Pro podporované banky platí, že mají nabídku platby přes tohoto poskytovatele přímo ve svém internetovém bankovnictví či ve vlastní mobilní aplikaci. ClearXchange je konkurentem služeb jako PayPal a jako Popmoney, ale není existenciální hrozbou pro tyto služby. Pouze vrací P2P platby zpět na úroveň bankovních operací. A snaží se nastavit benchmark pro cenu těchto služeb, která je v tomto případě zdarma [24].

Bezpečnost takového typu poskytovatele plateb je také na vysoké úrovní, protože se shoduje se standardy, které běžně používají banky samotné. ClearXChange používá ochranu proti náhodnému ponechání otevřené webové stránky i v případě kdy uživatel není přihlášen. V praxi to znamená, že stránce vyprší platnost pokud je ponechána bez jakékoliv uživatelské interakce.

2.1.9 Ostatní

Existuje samozřejmě celá řada dalších služeb. U mnohých z nich nejsou k dispozici dostatečné informace. Patří mezi ně například švýcarský Swish, který vzniknul v roce 2012, již v roce 2014 reportoval 1 milion aktivních uživatelů a nárůst 120 000 nových uživatelů měsíčně. Dále například Popmoney, americká služba, která stejně jako Square Cash posílá peníze přímo z účtu na účet bez jakýchkoliv virtuálních peněženek. Velkou nevýhodou této služby je ovšem její cena, kde si její provozovatelé účtují $0,95 za transakci. Nebo například opět americká služba Dwolla, která je určena spíše než platbám mezi kamarády platbám za drobné zboží. Dalším hlavním specifikem je například absence využití platebních karet. Pro provádění plateb využívá čistě bankovního konta uživatele. Poslední ze služeb, které stojí za zmínku je polský Blik. Jedná se opět o službu, která vznikla jako výsledek spolupráce několika místních bank. Jmenovitě Alior, Millennium, BZ WBK, ING BSK, mBank a PKO BP. Platba pomocí Blik je akceptována v 35 000 obchodech včetně 12 000 internetových a bankomatů. Služba pracuje na poněkud odlišném způsobu. V aplikaci vlastní banky klient zvolí možnost platby touto službou. Je vygenerován jednorázový kód, který například může uživatel vložit do bankomatu či při platbě u obchodníka. Služba opět vyžaduje registraci pro odeslání i příjem plateb.

2.2 Benefity a rizika P2P služeb

P2P platby jsou ve většině případů úzce spjaty s mobilními aplikacemi. Principem P2P plateb je posílat peníze druhé osobě bez znalosti jejího čísla účtu a

jak již bylo zmíněno, technologie v elektronickém odvětví přináší nové a možnosti neuvěřitelným tempem. Používání chytrých mobilních telefonů a tedy i aplikací se tak stalo součástí našich životů stejně kdysi televizní obrazovka. Využívání této služby tak s sebou přináší řadu výhod i nevýhod jak z pohledu uživatele tak provozovatele.

2.2.1 Benefity

Hlavním benefitem z pohledu uživatele je samozřejmě možnost placení bez znalosti čísla účtu příjemce. Typickou situací, kterou všechny uvedené služby popisují je placení s kamarády nebo kolegy za oběd, kdy obchodníkovi může zaplatit jeden z nich a ostatní mu během okamžiku pošlou peníze zpět na jeho účet, aniž by si museli vyměňovat čísla účtu nebo je zadávat manuálně. Některé ze služeb dokonce umožňují v rámci aplikace platit i obchodníkovi. Tato výhoda ovšem nezáleží jen na provozovateli aplikace, ale i na samotných prodejcích, zda chtějí službu podporovat. Typicky se tak stává až v okamžiku, kdy vědí, že by u nich byl o službu zájem. Další výhodou pro klienty je jednoduché vyřízení pohledávek a kontrola nad závazky. V situaci, kdy uživateli někdo dluží finanční obnos, je nepříjemné prosit osobu o včasné zaplacení. S touto službou jednoduše pošle žádost o zaplacení, což je pro obě strany jednodušší.

Pro provozovatele služby, je hlavní výhodou získání výnosů z provozování této služby. Můžeme uvažovat zejména o primárním zisku či zisku z druhotných faktorů. V případě primárního zisku, je aplikace či služba schopna pokrýt náklady na její provoz a dále generuje zisk. V případě, kdy služba není primární aktivitou společnosti, ovšem častěji nastává generování zisku až z druhotných faktorů. V tuto chvíli je zisk generován například z nárůstu klientů společnosti, kteří mimo využívání této službu mají zájem i o další produkty.

2.2.2 Rizika a nevýhody používání aplikace

Opakem benefitů, jsou nevýhody, či rizika spojená s provozem a používáním. U posytovatele služby asi není vhodné zvažovat nevýhody, ale spíše rizika, které tato služba může přinést. Hlavním rizikem pro provozovatele služby je nedostatečné pokrytí nákladů na projekt nebo minimální výnosnost. Dalším rizikům z pohledu provozovatele je věnována kapitola 3.5.

Nevýhody služby z pohledu uživatele se liší dle poskytovatele služby. V jednom případě je to vysoká cena za prováděnou transakci. Dále nevýhoda, která vychází ze situace, kdy služba vyžaduje po příjemci platby registraci. Dochází tak prakticky k tomu, že uživateli někdo půjčí finanční obnos, ale místo vrácení hotovosti obdrží žádost o registraci do služby, o kterou nemusí jevit zájem. Proto by před každým provedením transakce měl takový uživatel kontaktovat příjemce, zda souhlasí s takovýmto přístupem. Dále je nevýhodou úzká návaznost na provoz mobilního zařízení, které má velmi omezenou

kapacitu baterie. Nebo obecně nevýhody spjaté s používáním mobilního zařízení, jako například krádež, či poškození telefonu. V tu chvíli ovšem klientům aplikace nic nebrání použít již osvědčené metody placení.

Pro obě jmenované skupiny existuje množina rizik která má dopad na obě strany. Například nedostatečné zabezpečení a následný unik citlivých informací, či finančních prostředků klientů.

2.3 Klíčové faktory úspěchu

Z provedené analýzy lze odvodit několik pohledů na klíčové faktory k úspěchu P2P služeb. Pohled ze strany potencionálních uživatelů, reálných uživatelů a poskytovatelů.

Jako první se zaměříme na pohled potencionálních uživatelů, neboli lidí, kteří vyjádřili obavy z používání podobných aplikací [25]. Tyto obavy jsou uvedeny v následujícím seznamu, ohodnocené procenty, kolik lidí sdílí podobné obavy.

- Bezpečnost – 71%
- Preferují tradiční způsob – 42%
- Kráděž telefonu – 39%
- Platba špatné částky/osobě – 32%
- Nevlastní smartphone - 27%
- Čeká jak se situace vyvine – 13%

Jak lze vidět, nejčastější obavy se týkají bezpečnosti. Dále 42% respondentů preferuje tradiční působ placení. A Poslední z top 3 obav je obava z krádeže telefonu. Dá se předpokládat, že část těchto lidí by se dala přesvědčit pro tento typ produktu, pokud by měli dostatečný důvod jí věřit. To znamená, že pokud by služba poskytovala dostatečné bezpečí svým uživatelům a jejich penězům, zvýšila by se pravděpodobnost, že tito lidé budou více otevření novým možnostem. Mnohdy ale nejde o samotné zabezpečení aplikace, ale o neznalost konceptu zabezpečení služby, jež brání lidem upustit od těchto obav. Blíže se bezpečnosti věnuje kapitola tomu určená 1.4.2.4. Co se týče krádeže telefonu, musí existovat dostupný a dobře popsaný postup, co dělat v takové situaci. K celkovému mínění potencionálních uživatelů také nepřispívají mnohdy nejasné způsoby účtování poplatků za poskytované služby. Tento jev se častěji týká bankovních aplikací, než aplikací třetích stran. Banky obecně málokdy poskytují naprosto transparentní přehled jednotlivých poplatků a tím můžou odradit potencionální klienty, kteří nabudou dojmu, že nová služba je pouze dalším pokusem jak z nich vylákat prostředky.

Druhým pohled je názor uživatelů se špatnými zkušenostmi se stávajícími službami. Hlavním faktorem úspěchu služby v takovém případě je její univerzálnost. Tím se rozumí možnost platit lidem, kteří nejsou registrováni u té samé služby nebo nemají stejnou banku. I za cenu toho, že se příjemce bude muset registrovat. Pořád existuje možnost, že se příjemce i odesílatel domluví a jde o menší problém, než když tato možnost neexistuje vůbec. Samozřejmě absence nutnosti příjemce se registrovat je výhodou pro takovou službu. Dalším faktorem je její rychlost. Služby, které jsou schopné vyřídit platební transakci za 3 a více dní, postrádají smysl. Aby mělo význam používat placení mezi lidmi v kavárně, nebo na obědě, což je hlavním záměrem P2P plateb, musí být platba provedena okamžitě.

Třetí pohled je ze strany provozovatele P2P plateb. Hlavním faktorem úspěchu je vždy přilákání dostatečného počtu uživatelů. Z pohledu poskytovatele se jedná o vlastnost, které uživatelé přímo nevyžadovali, ale ukázalo se, že jsou stěžejní pro zásadní pro získání pozornosti. Každá služba se s tímto vypořádala jinak. Například společnost Venmo vsadila na sociální faktor. Jak již bylo zmíněno, jedná se o krok poněkud kontroverzní. Mnozí uživatelé jej přivítají, mnozí odsoudí. Ale faktem zůstává, že sociální sítě v současnosti stále mají co říct. Bohužel tento prvek nemůže být aplikován pro každou společnost. Druhým faktorem, který upoutá na první pohled, je jednoduchost aplikace. Lidé nechtějí zkoumat manuály, obchodní podmínky a ceníky služeb, chtějí jen přijít a začít používat. Proto musí mýt služba jednoduchá a dávat pocit přímočarosti a transparentnosti. A to nejen při běžném používání, ale i během první registrace a nastavování.

Každá nová služba by se primárně měla snažit zaujmout skupinu, která nejeví přehnaný zájem. Protože skupina, která projevuje zájem "z angl. early adopeters", má velké tendence, že bude službu využívat i bez jakékoliv mediální prezentace. A je velká pravděpodobnost, že pokud se podaří přesvědčit pro aplikaci konervativnější uživatele, méně konzervativní se nechají přesvědčit také. Přesto z povahy aplikace je zřejmé, že má potenciál oslovit zejména mladší uživatele, kteří jednak k novým technologiím přistupují s nadšením. Ale jsou i otevřenější rizikovým způsobům placení za předpokladu zjednodušení jejich každodenního života. A v otázce bezpečnosti by se měli tvůrci aplikace a služby jako takové snažit vyvážit zabezpečení s použitelností. Vhodné proto je nastavit výchozí míru zabezpečení a poté umožnit uživatelům nastavení dodatečných bezpečnostních prvků.

2.4 Bezpečnost zkoumaných aplikací

Následující kapitola shrnuje poznatky týkající se bezpečnosti v průběhu zkoumání aplikací. Bezpečnost je pro bankovní aplikace klíčová, proto by jí měla být věnována zvláštní pozornost. Výše zmíněné aplikace se mnohdy v průběhu jejich používání potýkaly s problémy a cílem této kapitoly je tak identifikovat

potencionální bezpečnostní hrozby a následně se jim vyvarovat.

První problém je informování uživatelů. Na první pohled se může dát, že se ani tolik nejedná o problém. Bohužel některé firmy razí strategii utajování vzniklých problémů ve snaze minimalizovat dopady na jejich společnost. Do jisté míry se jedná o pochopitelný krok, rozhodně není potřeba šířit paniku při sebemenším incidentu. Vždy je nutné zvážit míru rizika a rozsah potencinálních dopadů. Koneckonců jde primárně o zákazníky, kteří pokud se dozvědí že společnost utajovala informace a vystavila tak své klienty zbytečnému riziku, mohou ztratit důvěru v poskytovatele. V každém případě by ale měl poskytovatel služby vždy podniknout všechny adekvátní kroky k minimalizaci rizika, popřípadě dopadu. Například pokud se provozovatel dozví o úniku přihlašovacích údajů, není rozhodně důvod čekat co bude následovat, ale jít s pravdou ven a přimět klienty k jejich změně. Dále by měli v každém případě informovat uživatele v případě změny jakýchkoliv důležitých údajů. Například při změně hesla je nezbytné informovat klienta prostřednitvím emailové adresy nebo sms s informací o provedené akci a rovnou přidat kontakt pro případ, že uživatel bude považovat aktivitu za neoprávněnou. Tím se automaticky dostáváme k problému druhému. Klienti bance, či aplikaci poskytovatele třetí strany projevují důvěru svěřením svých osobních údajů. Proto by poskytovatel měl ke svým klientům přisupovat s pokorou. A jelikož spravuje jejich osobní údaje a finanční prostředky, neměla by nastat situace kdy se klient nemůže obrátit na zákaznickou podporu. Podpora je u takovéhoto typu služeb nezbytnou součástí.

Dále je důležitá kontrola přístupu k datům uživatele. To zahrnuje jednak samotné oprávnění aplikace, ale například i přístup do aplikační databáze. Alespoň pro aplikace operačního systému Android platí, že musí mít nadefinovaná oprávnění v AndroidManifest.xml, který je uložen v jar archivu. Po kontrole těchto oprávnění ve všech dostupných aplikacích nebylo odhaleno žádné zbytečné oprávnění. Co se ale přístupu do aplikační databáze týče, některé aplikace nebyly v tomto ohledu vůbec zabezpečené a uživatel s root právy se tak jednoduše dostane k uživatelským datům, včetně transakční historie. Naštěstí zde nebyly ani v jednom případě data v plain/textové podobě. Dále bylo provedeno reversní inženýrství [10] na vybraných aplikacích a v některých případech bylo možné se dostat k zdrojovému kódu. Tento proces není vyloženě nebezpečný pro samotná data aplikace, umožňuje ale dostatečně zkušenému útočníkovi analyzovat zdrojový kód aplikace a hledat případné zadní vrátka do aplikace. Například lze takto odhadout možnost použití SQL injection v produkční aplikaci. Samozřejmě nelze pokládat zamezení přístupu ke zdrojovm kódům aplikace za zabezpečení, tím by v tomto případě měl být kvalitní, čistý kód. Dále některé aplikace při pokusu o registraci akceptovaly nekonečný počet pokusů. V tomto případě je velmi snadné použít brute-force

[10] Způsob zpětné kompilace aplikace, ve snaze získat zdrojové kódy již ze zabaleného binárního archivu

útok pro prolomení zabezpečení.

Jak již bylo zmíněno, podepisování je nedílnou součástí publikace mobilní aplikace. Vždy by však mělo být použito nejvyšší možné zabezpečení, zvláště pokud to neúměrně nezvyšuje zátěž systému, či nároky na implementaci aplikace. Některé aplikace ze zkoumaného výběru byly podepisovány dnes již zastaralým hashovacím algorimem, který v například v rámci PCI certifikace není považován za dostatečně zabezpečený. V tomto případě je tak minimálním požadavkem na hashovací algoritmus SHA1, v ideálním případě pak SHA256.

Jak již bylo naznačeno v popisu jednotlivých služeb, se aplikace potýkaly i s dalšími problémy. Například hlasová asistentka SIRI/Cortana na první pohled nepředstavuje žádné riziko. Pokud však jakkoliv dokáže operovat s aplikací přes zamčenou obrazovku, jedná se o bezpečností díru.

Uživatel i poskytovatel služby by vždy měl myslet na dostatečné vyvážení uživatelského pohodlí a zabezpečení. Provozovatel by měl nastavit minimální akceptovatelnou hranici zabezpečení a uživatel by dále měl mít možnost toto zabezpečení dále rozšířit, například o dvoufaktorové ověření. Co se týče služeb, které jakkoliv manipulují s karetními daty, by měly projít certifikací PCI. V případě zkoumaných aplikací nebylo v tomto ohledu shledáno žádné pochybení.

2.5 P2P platby na českém trhu

Žádná ze zkoumaných služeb nepochází z českého trhu, protože v současné chvíli zde žádná služba obdobného charakteru nefunguje. Přesto by se nejednalo o premiéru P2P aplikace v českém prostředí. Několik let fungovala služba Mobito. Bohužel od 1.prosince roku 2015 byl její provoz zastaven. Nabízí se tedy otázka, co vedlo provozovatele k zrušení jejího provozu, do jaké míry je český trh na podobné služby připraven a jaká jsou specifika místního trhu. V této kapitole tak rozebereme obecné informace týkající se P2P na českém trhu. Specifické informace pro implementaci nové aplikace budou rozebrány v kapitole 3.6.

2.5.1 Mobito

Služba Mobito [26] vznikla v září roku 2012 jako projekt mladé společnosti MOPET.cz. Zakladateli společnosti jsou dlouholetí bankéři, Tomáš Salomon a Viktor Pešek. Mobito není projekt, který by vznikl přes noc, předcházelo mu dlouholeté plánování. Služba dále vznikala ve spolupráci se všemi mobilními operátory a s podporou od České Spořitelny, GE Money Bank a Reiffeisen Bank. Záměrem společnosti bylo vytvořit mobilní platformu, která umožní provádění plateb velkému množství klientů. V době před pár lety, se začínaly více rozvíjet chytré telefony, ale aplikace přesto necílila pouze na majitele těchto zařízení. Podporovala i ovládání služby pomocí textových zpráv. Služba měla několik možností jejího využití. Jednalo se o platbu mezi lidmi,

nabíjení kreditu a platba u obchodníka. Pilotní část projektu byla spuštěna již v červnu 2012, kdy jejími uživateli byli vybraní zájemci. Šest týdnů po jejím oficiálním uvedení službu využívalo kolem 11000 klientů a po bezmála půl roce téměř 20000. Start služby se tak zdál být na dobré cestě k úspěchu. Dokonce se aplikace pro chytré mobilní telefony objevila na několika soutěžích. Byla finalistou v soutěži České inovace a probojovala se do TOP5 na Global Mobile Awards v Barceloně. Podle dostupných informací však v roce 2013, byl počet uživatelů pouze kolem 25000. Jelikož jednou z hlavních funkcionalit systému měla být možnost platby u obchodníka, snažili je její tvůrci bojovat za prosazení mezi klasické platby. Bohužel projekt nesplnil daná očekávání a byl v roce 2015, tedy po třech letech ukončen z důvodu nedostatečného zájmu klientů.

Celý projekt byl v té době velice ambiciózní, společnost předpokládala, že po prvním roce bude službu používat kolem 150 000 uživatelů a přes 1000 obchodníků. Vzhledem k číslům prezentovaným výše, se po roce k těmto číslům, alespoň co se počtu uživatelů týče, ani nepřiblížila. Mobilní telefony nebyly na takové úrovni, aby mohly zastoupit klasické platební metody. Služba podporovala dokonce platbu pomocí protokolu USSD. V případě že chtěl klient zaplatit vytočil na svém zařízení číslo ve tvaru *135*# a dále postupovat podle textových instrukcí. Tento způsob představuje zajímavou alternativu, nikoliv však použitelnou. Je zřejmé, že tvůrci služby se snažili vytvořit univerzální službu a pokrýt tak co největší část trhu. Možná právě to bylo nakonec důvodem skončení služby. Podpora tohoto typu platby ze strany obchodníků je v tomto případě klíčová. Bohužel se je však autorům nepodařilo přesvědčit, služba proto nemůže nahradit klasické platby. Dokonce monetizační strategie reflektovala problémy v průběhu fungování služby. V roce 2013 služba zvýšila poplatek pro převádění elektronických peněz na bankovní účet, v případě že převáděná částka byla vyšší než 2000. Ve snaze přilákat více zákazníků hlavně ze strany obchodníků, tento poplatek v roce 2014 zrušila.

Důvodem pro zrušení byl samozřejmě nezájem koncových uživatelů. Samotní uživatelé reagovali na internetové recenze tohoto produktu s komentáři a důvodů jejich nespokojenosti uváděli hned několik. Většinu z nich lze shrnout pod výraz “smysl služby”. Při platbě u obchodníka byl potřeba opisovat kódy buď z mobilního telefonu obchodníkem, nebo například při platbě v taxi, musel naopak klient opisovat mobito číslo obchodníka. V takovém případě by dávalo smysl použití QR kódů pro jednodušší manipulaci s čísly. Bez tohoto prvku je použití o poznání složitější, než v případě bezkontaktní karty nebo ekvivalentní platbě přes internetové bankovnictví. Druhým hlavním důvodem, který vyplynul po skončená služby, byla velice minimalistická marketingová kampaň. Dalo by se říci, že službu používali lidé, kteří sami projevovali zájem o podobné služby a aktivně je vyhledávali. Internetový portál finparada.cz po skončení služby prezentoval článek shrnující působení Mobito na českém trhu a rovněž publikovat závěr šetření pravidelně prováděného mobilními operátory, ze kterého vyplynulo že téměř 1/2 čechů by o podobné služby zájem měla. [26]

2.5.2 Přístup k inovacím

Nutné je ovšem uvázit všchny faktory, které mají na provozování této služby na českém trhu vliv. Hlavním problémem při zavádění služby na trh je konzervatismus českých uživatelů. Nelze předpokládat, že zavádění platební služby bude mít stejný průběh jako například v USA, kde jsou lidé více otevření novým možnostem a aktivně se zajímají o inovativní způsoby platby. Většina Čechů věří pouze osvědčeným metodám placení a jakékoliv inovace jsou přijímány velmi pomalu. Nejinak tomu bylo v případě bezkontaktních karet. Jejich nárůst byl zpočátku velmi pomalý, po překonání počáteční nedůvěry jeji popularita raketově roste. To samé platí pro mobilní bankovnictví.

2.5.3 Legislativa

V případě České republiky zákon č. 284/2009 Sb., o platebním styku stanovuje maximální možnou dobu provádění transakce při splnění určitých podmínek (viz. 1.2.5). Dalším předpisem, který ovlivňuje stav na českém trhu bude directiva Evropské komise, týkající se bankovních plateb [27], PSD2. Hlavním cílem této direktivy je přizpůsobit se rozvíjejícím se požadavkům a možnostem inovativních platebních metod. Jedním z bodů je například zpřístupnění aplikačního rozhraní internetového bankovnictví třetím stranám. To znamená, že pokud poskytovatel služby získá souhlas uživatele, pak může přistupovat k bankovnímu účtu uživatele jeho jménem. Banka v tom případě nebude mít na výběr, zda informace dá poskytovateli k dispozici, ale tato povinnost bude dána zákonem. Díky tomuto předpisu bude snazší přijít s novou platební službou, lze tak očekávat vznik konkurence současným platebním aplikacím bank. V tomto případě se však nejedná o kompletní výčet právních předpisů, pouze o souhrn těch, které přímo ovlivňují vývoj P2P mobilní platformy.

2.6 Trendy v oblasti P2P

Jak předeslala předchozí kapitola 2.5.3, s příchodem nové evropské direktivy, lze očekávat nárůst inovativních platebních metod, které budou využívat bankovní API. Další zajímavou inovací v oblasti plateb je například platba pomocí osobního automobilu. Například při průjezdu čerpací stanicí auto samo pozná množství natankovaného paliva a uživatel tak pouze potvrdí placenou částku. Stejná situace platí pro parkování v označených zónách. [28]

Dále lze samozřejmě očekávat další rozvoj bezkontaktních platebních metod prostřednictvím technologie NFC v mobilním telefonu. Dále již zmíněná technologie identifikace pomocí krevního řečiště je určitě zajímavým prvkem pro bankovní sektor. Rovněž lze předpokládat další rozvoj dnes již známe digitální měny bitcoin. Všechny nové metody mají ale společný cíl, usnadnit placení uživatelům do takové míry, aby je platby začaly bavit a zpětně tak vrátily počáteční investici bance.

Tabulka 2.1: Shrnutí specifik jednotlivých služeb

Název	Místo	Start	Platforma	Poplatky	Rychlost
SquareCash	US	2013	iOS,Android	Zdarma (Platba kreditní kartou 3%)	1-2d
Barclays Pingit	UK	2012	iOS,Android	Zdarma	1d
Venmo	US	2012	iOS,Android	Zdarma (Platba kreditní kartou 3%)	1d
Radius Pay a Friend	US	2016	iOS,Android	Zdarma	debet-instant, účet-1-2d
Dwolla	US	2010	iOS,Android	Zdarma	3-4d
Google Wallet	US	2013	iOS,Android	Zdarma	3d
PayPal.me	US	2015	iOS,Android, Windows Mobile	Zdarma	3-4h
Swish	SWISS	2012	iOS,Android	1,5%/ transakce	12h
Blik	PL	2015	iOS,Android, Windows Mobile	Zdarma	neznámé
Circle	US	2015	iOS,Android	Zdarma (Platba kreditní kartou zpoplatněna)	1-4d
Popmoney	US	2010	iOS,Android	$0,95/ transakce	debit-1d, účet-3d

2.7 Shrnutí

Platba na kontakt je zejména v Americe a asijských státech rozšířenou platební metodou. Pomalu se její vliv začíná dostávat i do států západní Evropy.

Následující tabulka 2.1 představuje souhrn porovnatelných parametrů dostupných služeb. Všechny služby podporují mobilní platformu s operačními systémy Android a iOS. Pouze dvě služby podporují i mobilní operační systém společnosti Microsoft, Windows mobile. První P2P aplikace se začaly objevovat v průběhu roku 2010, nejedná se tedy v rámci celosvětového trhu o žádnou novinku. Služby jako jsou Venmo či Square cash jsou v USA velmi populární, což bohužel nezaručuje popularitu obdobých služeb i na tuzemském trhu. Americký trh je hodně zaměřen na tento typ služeb zřejmě z důvodu počáteční absence bezkontaktních plateb. Ty jsou dnes již standardem v Evropě, zatímco v Americe je vrchol teprve čeká. Služba, která ale může představovat

jistou paralelu s českým trhem, je polský Blik. Můžeme uvážit počet klientů tohoto poskytovatele, který v tomto roce činí kolem 2 milionu klientů, zatímco v předchozím "pouhých" 500 000. Dále uvážíme velikost polského trhu, a aplikujeme poměr na český trh, jednalo by se v případě 2 milionů polských klientů o cca 500 000 klientů na českém trhu. Pokud by se plánovanému projektu podařilo dosáhnout tohoto čísla, můžeme mluvit o neuvěřitelném úspěchu. Pro dosažení maximálního možného počtu klientů je možné se těmito službami inspirovat, případně poučit z jejich chyb. Co se zpoplatnění služeb týče, je většina nabízených k dispozici zdarma, popřípadě za poplatek za platbu kreditní kartou. Tento poplatek není připisován na účet provozovatele služby, ale karetním asociacím. Poskytovatelé pouze přenáší odpovědnost za tuto platbu na klienta. Doba převodu finančních prostředků je prakticky v rozmezí několika dní až po několik hodin. Samozřejmě se jedná pouze o faktický převod elektronických peněz mezi klientem a klientem nebo mezi klientem a aplikací. Převody mezi virtuálními peněženkami jsou připisovány instantně. Nejlepší časy za reálný převod peněz platí pro švýcarský Swish, či americký PayPal. Některé americké služby přinášejí inovace do platebního sektoru, jako například aplikace Venmo a její sociální aspekt. Zůstává otázkou jak by na tento prvek reagovali zákazníci na českém trhu. Situací na tuzemském trhu může zamíchat příchod nové evropské regulativy, která otevře dveře novým poskytovatelů třetích stran a vytvoří lepší prostředí pro konkurenční boj.

Hlavní využití této aplikace představuje platba za nájem, dále pak sdílení účtů a neméně významné využití například při platbě v restauraci s kolegy. Lze očekávat, že toto rozložení by v rámci české republiky vypadalo odlišně. Zejména v případě, kdy majoritní část Čechů preferuje vlastní byt před pronájmem, by právě první kategorie utrpěla největší ztrátu.

Kapitola 3

Návrh

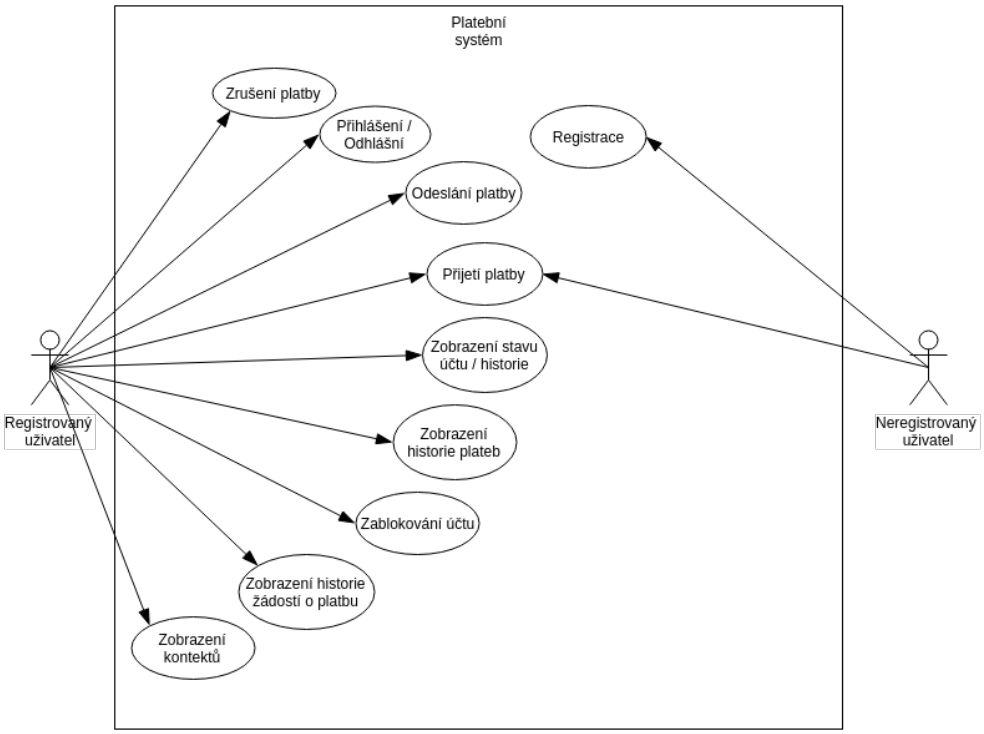
Následující kapitola má za úkol navrhnout službu, která má potenciál oslovit cílovou skupinu uživatelů a představit kroky k její úspěšné realizaci. Abychom mohli obdobný projekt realizovat, je potřeba nejprve nadefinovat co je hlavním cílem, následně specifikovat požadavky a provést prvotní návrh. Následuje finanční analýza, která slouží k získání představy o celkových nákladech a očekávaném zisku. S ohledem na předešlé kroky je zhodnocena proveditelnost projektu. Dále, pokud je zjištěno, že realizace je možná, je dobré se připravit na možné hrozby a na metody jejich řešení. V poslední části je navržen procesní a databázový model aplikace.

3.1 Definice hlavních cílů a příležitostí pro KB

Pokud společnost zvažuje implementaci nějaké služby pro své klienty, musí jí tento krok samozřejmě přinést nějaký profit. Těchto přínosů existuje celá řada. Jako první člověka napadne přínos finanční. Mohlo by se tak na první pohled zdát že služba, která nepřinese přímý zisk se společnosti nevyplatí. Existuje však i nepřímý zisk z provozování služby. Typickým příkladem je větší zájem uživatelů o produkty dané společnosti, kteří jsou za své služby ochotní zaplatit. Takoví klienti byť nemusí přímo generovat zisk z již zmíněné služby, rozšiřují klientskou základnu společnosti a využíváním běžných služeb zvyšují zisk také. Primární přínosy aplikace rozebereme blíže v kapitole týkající se finančního plánu projektu 3.4.

Co se týče dalších příležitostí s implementací této služby, má projekt potenciál oslovit zejména mladé lidi, protože se jedná o novou službu, která není příliš rozšířená v Evropě. Následující obrázek 3.1 popisuje uživatelské scénáře aplikace.

Obrázek 3.1 popisuje funkční požadavky služby, abychom ale mohli projekt naplánovat a zadat požadavek na realizaci, musí být dostatečně specifikované jak funkční tak i nefunkční požadavky.



Obrázek 3.1: Use Case model pro P2P aplikaci KB

- Platby musí být prováděny instantně
- Aplikace je vyvíjena multiplatformě
- Systém je dostatečně škálovatelný
- Komunikace probíhá přes TLS
- Aplikace splňuje nejvyšší bezpečnostní standardy a certifikace
- Aplikace je dostupná pro iOS(7.x+) a Android (ICS+)
- Reakční čas přihlášení/odeslání požadavku je max 3s
- Aplikace je jednoduchá na používání
- Aplikace využívá existujícího API banky
- Modulární architektura aplikace
- Aplikace má dostatečná oprávnění
- Databáze splňuje CIA (confidentiality, integrity, availability)
- Aplikace podporuje biometrické údaje jako metodu ověření identity

- Pro uživatele mobilní banky je číslo automaticky spárované s účtem

3.2 Návrh P2P aplikace KB

Po provedení analýzy funkčních a nefunkčních požadavků následuje samotný návrh aplikace. Návrh platformy byl specifikován v rámci nefunkčních požadavků. Jedná se o mobilní operační systémy iOS a Android. Volba mobilní platformy byla samozřejmostí vzhledem k povaze služby. Tyto byly vybrány na základě jejich podílů na trhu. Mobilní telefony s OS Android představují cca 71% a iOS kolem 11%. Ostatní operační systémy mají zanedbatelný podíl a implementace aplikace pro tyto systémy by nepokryla její náklady. Zbývá zvážit implementaci do současných aplikací či vývoj nové. Dále následuje návrh uživatelského rozhraní a procesního modelu.

3.2.1 Koncepce aplikace

V případě zakomponování nové funkcionality do stávající mobilní banky se samozřejmě jedná o jednodušší variantu. Lze předpokládat, že aplikace jež implementuje rozhraní aplikačního serveru a splňuje bezpečnostní normy pro bankovní aplikace. Dále není potřeba návrhu uživatelského rozhraní celé aplikace, postačí pouze dílčí část týkající se samotné funkcionality. Nevýhodou ovšem je, že nově vyvinutá funkcionalita má tendenci zapadnout do množiny již existujících vlastností a nezíská tak potřebné množství uživatelů pro generování zisku. Samostatná aplikace má více možností jejího marketingu a proto potenciál zaujmout.

Pro KB je tak výhodnější variantou implementace samostatné aplikace. Pro provoz Android aplikace jsou tak potřeba určit nezbytná oprávnění. V aplikaci pro operační systém iOS má aplikace právo přístupu na všechna veřejná API. Jediný okamžik kdy aplikace požaduje oprávnění je při přístupu k poloze zařízení. Požadavek na povolení je odeslán uživateli v okamžiku jejího prvního vyžádání. Posílání sms nebo emailů je prováděné pomocí standardních controlerů, takže uživatel jejích používání, pozná. Oprávnění pro Android aplikaci jsou potřeba následující:

- ACCESS_FINE_LOCATION
- ACCESS_NETWORK_STATE
- INTERNET
- READ_CONTACTS
- WRITE_EXTERNAL_STORAGE
- USE_FINGERPRINT

- VIBRATE
- WAKE_LOCK

Veškerá komunikace probíhá přes internet, proto aplikace potřebuje i oprávnění k jeho přístupu. Oprávnění k čtení otisku prstu je opět určeno jako alternativní možnost při přihlašování do aplikace. Dále je vhodné aby aplikace měla možnost pozastavit uspání zařízení, například při probíhající transakci.

Pro dosažení co nejnižší ceny za vývoj aplikací bude použit framework, který umožňuje multiplatformní vývoj. Jako optimální pro tyto potřeby se jeví například React Native framework.

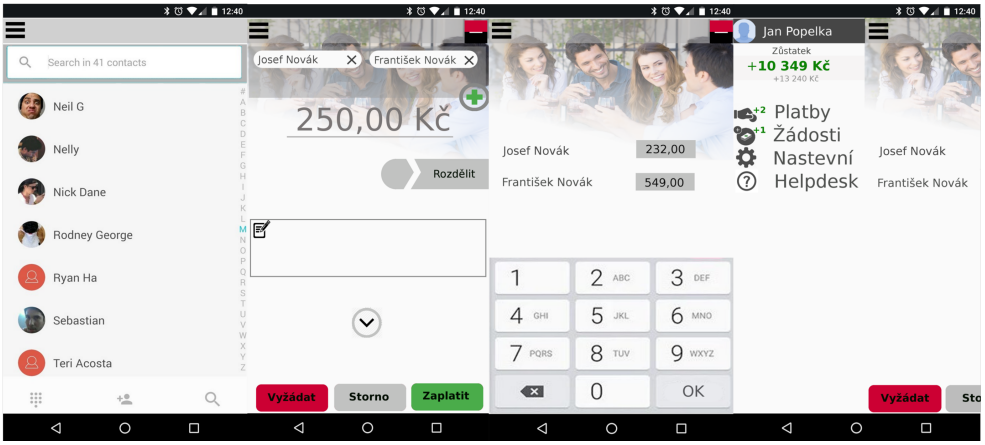
3.2.2 Uživatelské rozhraní

Tato podkapitola má znázornit grafické rozhraní aplikace. Aplikace by měla být jednoduchá na používání. Jednotlivé kroky by měly být dostatečně intuitivní. Zákazník musí být schopen provést či vyžádat platbu a nastavit základní parametry i bez čtení dokumentace či návodu. Ihned po přihlášení je klient přímo zaveden do kontaktního seznamu 3.2a. Pro provedení platby či žádosti stačí vybrat požadovaný kontakt. Po výběru příjemce následuje obrazovka pro specifikaci požadované částky. Na této obrazovce je dále možné nastavit více příjemců či plátců. Po výběru požadované částky pro více příjemců je každému z nich přednastavena stejná zadaná částka. Po tažení prstem z pravé části displeje do levé, se objeví obrazovka, která umožňuje změnit tyto přednastavené hodnoty. Po stisku požadovaného tlačítka je provedena platba či odeslána žádost o provedení platby.

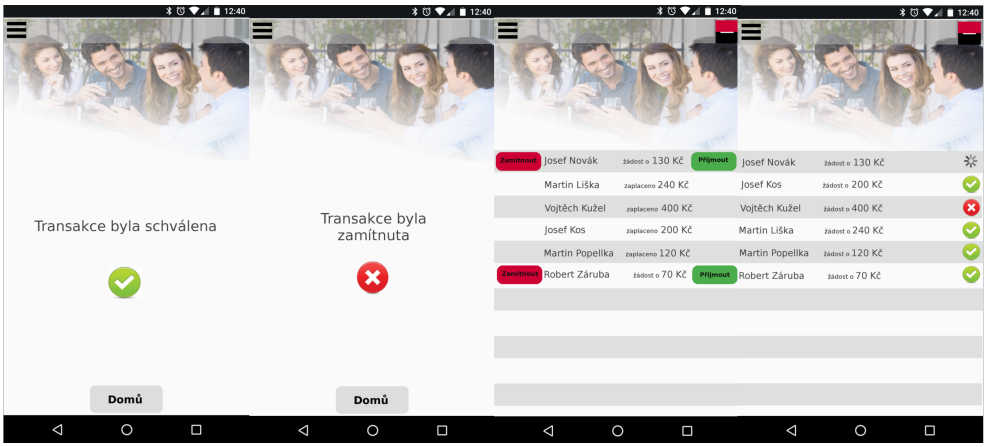
Druhá sada obrázků 3.2b znázorňuje oznámení uživateli o dokončené transakci. Dále pak obrazovku informující uživatele o odchozích a příchozích platbách. V rámci odchozích plateb jsou dále zobrazeny žádosti o zaplacení od ostatních uživatelů služby. Jednotlivé žádosti je možné přijmout, kdy poté dojde k zaplacení pohledávky nebo zamítnout. V obou případech je uživatel informován o stavu jeho požadavku. Poslední obrázek ukazuje příchozí platby, včetně stavu odeslaných žádostí. Lze de vidět zamítnuté transakce, transakce, které čekají na vyjádření protistrany a samozřejmě přijaté.

3.2.3 Princip systému

Pro funkčnost systému existují dvě varianty. Jako první varianta je využití bankovního API, které by podle evropské regulativy PSD2 2.5.3 mělo být dostupné od ledna 2018. To znamená, že systém by po nezaregistrovaném uživateli vyžadoval souhlas s přístupem do banky pře výše zmíněné API. Jedná se ovšem poněkud o novinku a proto implementace aplikace v tuto chvíli s touto variantou nepočítá. Po zavedení PSD2 by prakticky nebylo zapotřebí imeplementace serverové infrastruktury. Stačilo by vytvořit klienta schopného komunikovat se všemi dostupnými API. Klient by pouze spravoval komunikaci



(a) Platba a její provedení



(b) Kontrola provedených plateb a požadavků

Obrázek 3.2: Návrh uživatelského rozhraní

mezi API jednotlivých bankovních institucí. Zabezpečení přístupu lze očekávat na straně banky. Tato varianta předpokládá existenci instantních plateb.

Druhou variantu lze považovat za dočasné řešení před zavedením varianty předchozí. Smyslem tohoto systému je zamezit mezibankovním převodům. Banka ale může převádět platby v rámci svých účtů bez nutnosti spolupráce clearingového centra. Provedení platby je tak možné v reálném čase. Aby tohoto banka dosáhla, založí si své účty u všech dostupných bank na českém trhu. Na tyto účty převede část svých prostředků. Při provedení mezibankovní platby, tak pouze informuje banku klienta o převedení finančního obnosu z vlastního účtu na účet příjemce.

3.2.4 Návrh procesních modelů

Stejně jako v případě zkoumaných aplikací následují procesní modely registrace a provedení platby. Návrh je upraven tak, aby použití aplikace bylo co nejjednodušší.

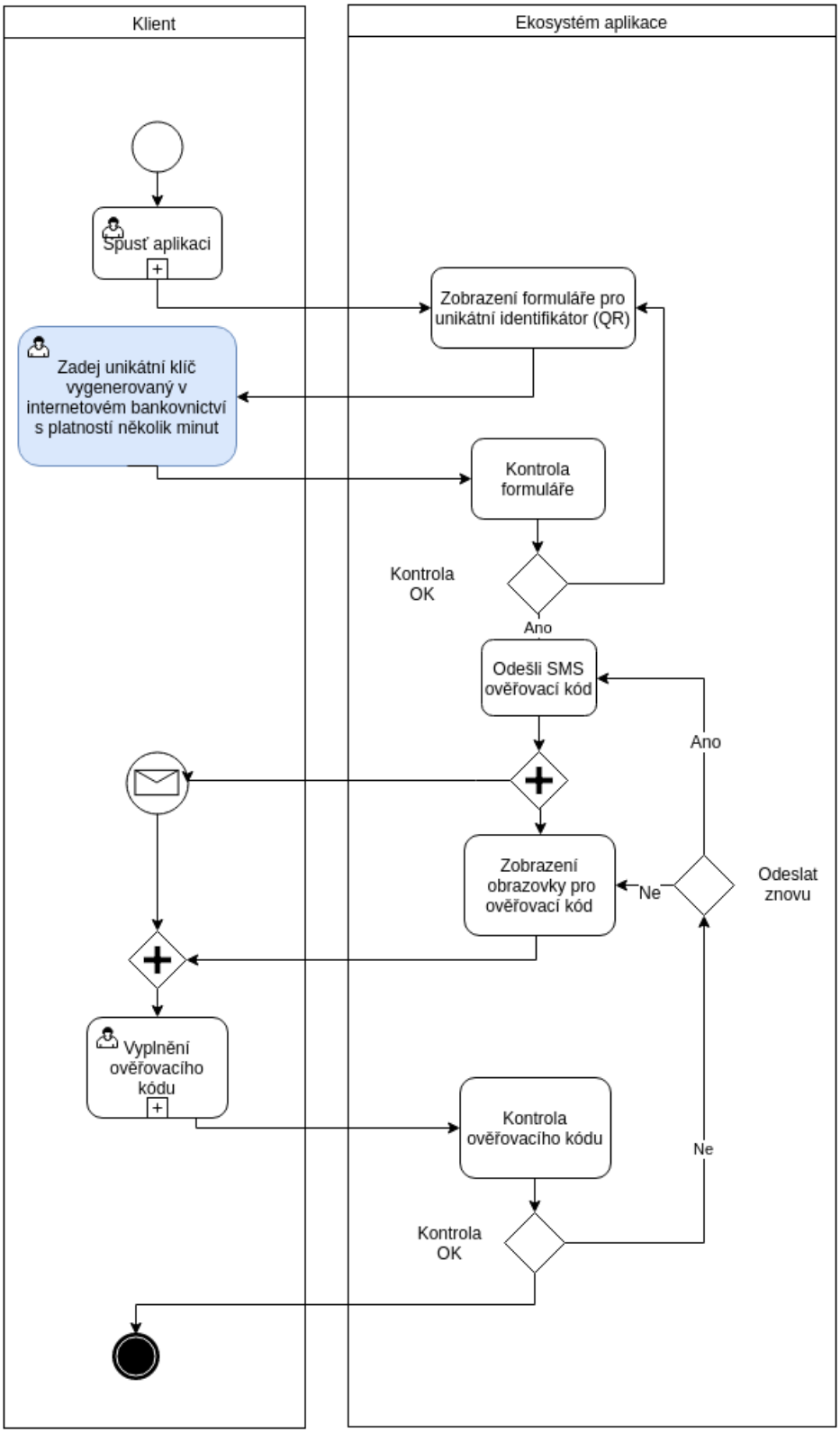
Proces registrace je znázorněn na následujícím obrázku 3.3. Pro zjednodušení procesu a usnadnění uživateli registraci do systému bez nutnosti zadávat manuálně potřebné informace je využito skenování QR kódu. Jako první obrazovka při započetí procesu registrace je uživateli v aplikaci zobrazena čtečka QR kódu. Potřebný kód se uživateli zobrazí v nastavení při přihlášení do elektronického bankovnictví. Tím je dosaženo vyšší úrovně zabezpečení. Po nascanování QR kódu je provedena kontrola a zaslán ověřovací SMS kód na mobilní telefon. Tím je zajištěno dvojí ochrany. Při prolomení ochrany první instance přihlášení je tak majitel bankovního účtu informován SMS zprávou. Po ověření kódu ze zprávy je úspěšně zaregistrován.

Druhý model 3.4 představuje proces platby. Proces je do jisté míry zřetelný i z návrhu uživatelského rozhraní. Po spuštění aplikace je uživatel vyzván pro zadání příjemce z kontaktního seznamu. Poté následuje zadání částky, po němž uživatel pouze potrvrdí platby pro dokončení transakce. Uživatel samozřejmě má možnost zadat více příjemců a následně specifikovat částku pro každého zvlášť, tento podproces na diagramu znázorněn není. Po zkontrolování parametrů transakce je odeslána zpráva jejímu příjemci. Pokud je příjemce zaregistrován, platba je přijata automaticky. Pro její zobrazení stačí otevřít aplikaci a platba je zaúčtována a viditelná v přehledu přijatých plateb. Nezaregistrovanému příjemci je odeslána zpráva SMS, po jejímž doručení se musí pro obdržení platby zaregistrovat do služby. Příjemce z jiné banky má na výběr registraci pouze pro příjem. V takovém případě je příjemci v okamžíku otevření aplikace zobrazena možnostzaregistrovat pouze pro příjem. V ten okamžik stačí zadání čísla účtu. Ihned po dokončení registrace je uživateli poslána částka na účet.

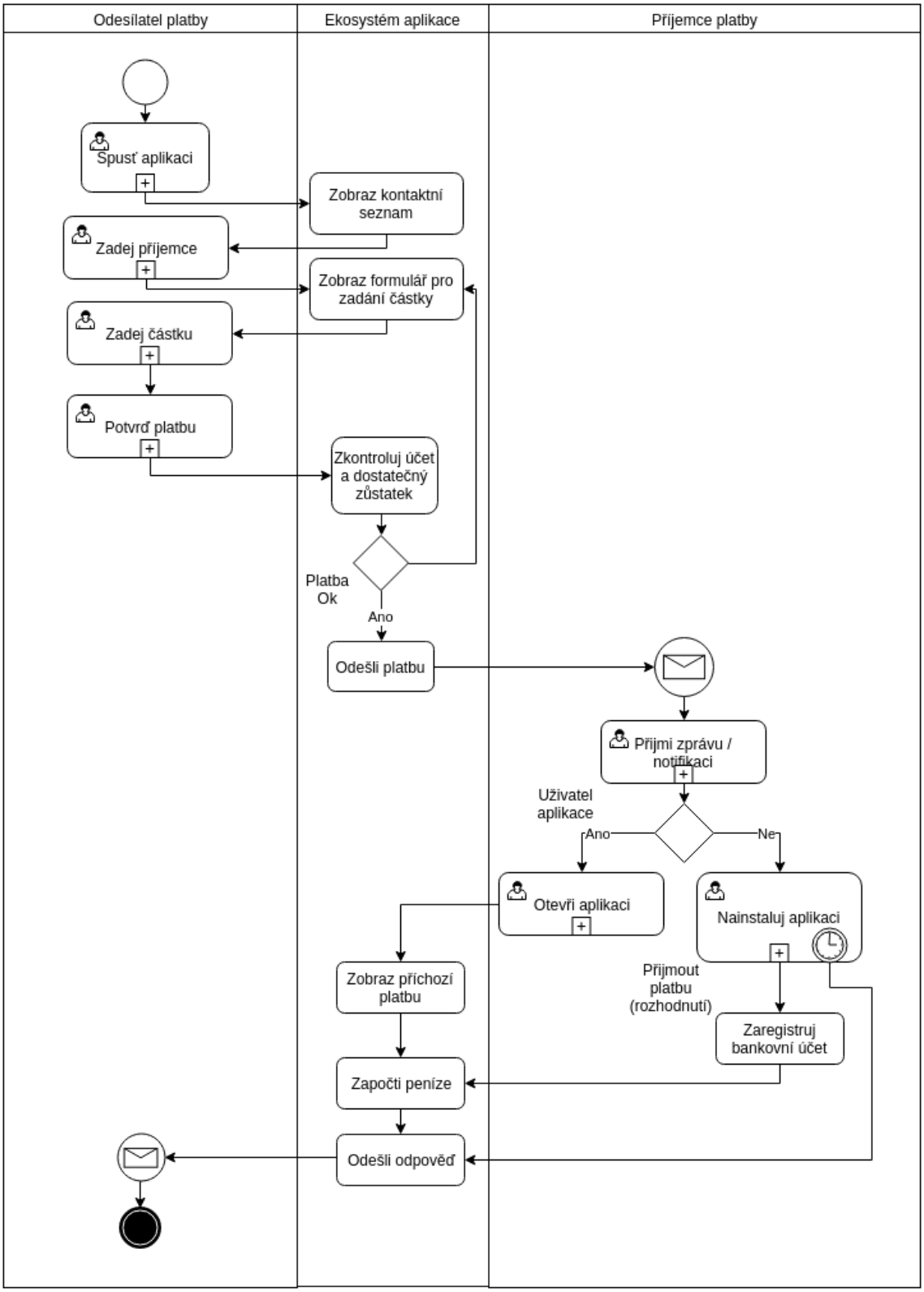
3.3 Harmonogram projektu

Abychom mohli provést finanční plán projektu je důležité nejprve stanovit harmonogram A.1. Z něj je vypočítán finanční plán a následně a předpokládané výnosy v několika možných scénářích. Projekt je rozdělen na tří hlavní fáze. Hlavním důvodem tohoto rozdělení je potřeba strukturovat projekt a zmenšit části po kterých může následovat retrospektiva a případné hodnocení průběhu projektu případně jeho následné směrování.

1. Vývoj web API a serverové části
2. Vývoj základních funkcionalit mobilní aplikace
3. Implementace dodatečných funkcí mobilní aplikace



Obrázek 3.3: Návrh procesu registrace



Obrázek 3.4: Návrh procesu platební transakce

Každá fáze má svůj vlastní SDLC [11]. Ten spočívá v analýze, návrhu, implementaci a testování.V analytické části první iterace je nejprve provedeno mapování trhu. Smyslem této fáze je zjistit co trh v současnosti nabízí a jaké jsou možnosti oslovit novým produktem. Špatný přístup při zavádění nového produktu je pouze snaha o vytvoření konkurence cenou. Vždy by měl nabídnout něco, co je pro něj specifické, a čím má šanci si vytvořit svoji cílovou skupinu. Proto je jako další krok projektu definice hlavních cílů. Po jejich stanovení musí být jasné jakým směrem se aplikace bude ubírat. V našem případě jde o mobilní aplikaci pro operační systém iOS a Android, která bude umožňovat využití P2P služby. Teprve poté je možné začít plánovat finance. Následuje analýza proveditelnosti, kde je cílem zjistit, zda je projekt realizovatelný a jaké jsou jeho potencionální výnosy. Druhá, návrhová fáze první iterace je vyhrazena návrhu architektury a datového modelu. V tomto bodě by mělo být poskytnuto dostatečné množství informací na implementaci první iterace, tedy serverové části aplikace a potřebných rozhraní pro komunikaci aplikace se servery. V závěru každé ze tří částí je testování. To musí probíhat po celou dobu implementace aby chyby, které při vývoji vzniknou, byly odhaleny dříve, než bude jejich odstranění nákladnější.

Druhá iterace je zaměřena na vývoj základních funkcí aplikace. Zde se opakují jednotlivé fáze SDLC. Jako první krok je tedy opět analýza zmapovaných aplikací z pohledu vývojářů. Cílem je nyní zjistit aplikaci co nejefektivnější. Snahou je získat dostatečné množství informací o fungování aplikací, získat zpětnou vazbu od klientů konkurenčních aplikací. Následuje návrh samotné aplikace. Od procesního modelu, přes vizuální návrh aplikace až po konkrétní třídní model. V implementační fázi je vytvořeno uživatelské rozhraní aplikace a následně samotná funkcionalita. V této fázi stačí dojít do bodu kdy jsou vytvořeny základní funkcionality. Na konci implementační fáze druhé iterace by tedy aplikace měla být schopna provádět registraci, platební příkaz nebo žádost a přijímat notifikace. Stejně jako v předchozí iteraci musí po celou dobu vývoje probíhat testování. Které odhalí nedostatky aplikace již na začátku. Po skončení testování by měl být vytvořen prototyp, který umožňuje provést testování reálného provozu aplikace.

Poslední iterace začíná analýzou požadavků na změnu, které mohly vyvstanout během vývoje. Může se například stát, že se změní situace na trhu, nebo se přijde na funkcionalitu, která je tzv. “nice to have”. Poté již následuje přímo implementační fáze, jelikož návrh aplikace by již měl být hotov z předchozí iterace. Dále testování a spuštění produkčního pilota, po kterém samozřejmě je třeba počítat s podporou vývojářů v případě odhalení chyb v aplikaci.

V rámci harmonogramu je naznačena návaznost jednotlivých kroků projektu a počet dní strávených na různých částech projektu.

[11] SDLC - Software Development Life Cycle - vývojový cyklus projektu

Tabulka 3.1: Personální zdroje na projektu

Zaměstnanec	Superhrubá mzda/h	Počet osob	Počet člověkodní	Cena (Kč)
Projekt manažer	1000	1	20	160 000
Analytik	600	2	88	422 400
Architekt	1200	1	22	211 200
Programátor	800	3	207	1 324 800
Bezpečnostní expert	1000	1	6	48 000
Tester	400	2	190	608 000
Designer	600	1	4	19 200

3.4 Finanční plán

Finanční plán by se dal rozdělit na dvě části. Plánovaná finanční náročnost projektu a očekávaný zisk z provozování aplikace.

3.4.1 Finanční náročnost projektu

Pro finanční náročnost projektu budeme vycházet z naplánovaného harmonogramu. Z času stráveného na projektu byla spočítána očekávaná účast členů týmu na jednotlivých úkolech. Samotná realizace projektu se dá tak rozdělit na tři části. První částí je vývoj aplikace a vše s tím spojené. Druhá část je vybavení potřebné pro testování implementace. Třetí část tvoří nezbytná propagace. Následující tabulka tak představuje čas strávený na projektu jednotlivými členy vývojového týmu a cenu za jednu hodinu přepočítanou na celkové náklady. Cena jedné osoby v rámci projektu je spočítána z počtu dní v harmonogramu, převedených na hodiny, vynásobena superhrubou mzdou na hodinu a počtem osob podílejících se na projektu.

Jelikož se jedná o softwarový produkt, největší položkou na seznamu je samotný vývoj a testování. Dále pak samozřejmě propagace celé služby, bez které by vývoj neměl šanci naplnit předpokladánaé výnosy. Jednou z nejčastějších příčin neúspěchu vývoje softwarového produktu je špatný odhad finančních zdrojů. Je potřeba proto počítat s dostatečnou rezervou, která by měla být schopna pokrýt náklady v případě prodloužení doby vývoje.

- Cena za implementaci: 2 793 600 Kč
- Testovací zařízení: 50 000 Kč
- Propagace produktu: 1 000 000 Kč
- Finanční rezerva: 500 000 Kč

Celková cena: **4 343 600 Kč**

Celková cena za projekt je dána prostým součtem jednotlivých položek. a je do ní započítána již zmíněná finanční rezerva. Výsledná částka tedy činí 4 343 600 Kč.

3.4.2 Očekávaný zisk z provozování služby

Pro určení finančního plánu je nutně určit počet potencionálních uživatelů služby. Budeme vycházet z údaje za minulý rok, kdy měla Komerční banka kolem 1 647 000 klientů. Není ale možné brát v úvahu všechny klienty banky jako potencionální uživatele. Budeme dále tedy uvažovat, že klienty aplikace se stanou jen lidé ve věkovém rozmezí 18-40 let. Ostatní věkové kategorie můžeme zanedbat. Abychom ale zjistili kolik klientů banky se v tomto věkovém rozpětí nachází. Vezmeme data z českého statistického úřadu o rozložení populace v České republice a toto rozložení aplikujeme na klienty banky. Za rok 2016 naměřil ČSÚ 10 553 843 osob.

První odhad počtu klientů banky ve věkové skupině, je podíl počtu obyvatel za rok 2015 a počtu osob v dané věkové skupině za rok 2015 vynásobený celkovým počtem klientů banky. Pro tento případ je tak počet klientů ve věkové skupině dán vztahem:

$$\begin{matrix}\text{počet klientů}\\ \text{ve skupině}\end{matrix} = \frac{poč\ obyvatel}{poč.\ obyvatel\ ve\ věkové\ skup.} \times poč.\ klientů\ banky$$

Tento odhad ale není příliš přesný, protože předpokládá existenci klientů banky, kteří jsou mladší 18 a starší 70. Mezi klienty banky se tak řadí i kojenci. Proto vzniknul odhad druhý který se toto snaží odstranit. Je větší pravděpodobnost, že klientům banky bude minimálně 18 a maximálně 70 s jistou mírou zanedbání. Každá věková kategorie tak byla následně vydělena procentuálním podílem věkové kategorie v rámci počtu obyvatel. Vzorec tak vypadá následovně.

$$\begin{matrix}\text{počet klientů}\\ \text{ve skupině}\end{matrix} = \frac{\frac{poč.\ obyvatel}{poč.\ obyvatel\ ve\ věkové\ skup.}}{\sum_{i=18}^{70} \frac{poč.\ obyvatel}{poč.\ obyvatel\ ve\ věkové\ skup.}} \times poč.\ klientů\ banky$$

Jak již bylo zmíněno, nelze však nyní počítat se všemi klienty banky jako s potencionálními klienty služby. V následující tabulce je proto proveden odhad počtu klientů aplikace v následujících letech. Hodnoty v prvních dvou sloupcích jsou založen na výsledcích předchozího odhadu, který se vztahuje k roku 0. V následných výpočtech je potřeba ještě započítat roční nárůst klientů KB (ve zvoleném rozsahu), který činí 1%. V posledním sloupci je počet odvozen podle počtu současných uživatelů mobilní banky. Dá se totiž předpokládat, že lidé, kteří již používají mobilní aplikaci pro správu svých bankovních účtů,

Tabulka 3.2: Odhady počtu klientů ve věkové skupině

Věkové skupiny	**Počet obyvatel**	**Počet klientů (odhad1)**	**Počet klientů (odhad2)**
18<x>20	284 937	44 466	62 361
20<x>30	1 326 588	207 023	290 335
30<x>40	1 667 227	250 182	264 886
40<x>50	1 528 705	238 565	334 570
50<x>60	1 340 612	209 212	293 404
60<x>70	1 337 349	214 945	301 444
Celkem 18<x>70	3 278 752	511 672	717 582

Tabulka 3.3: Procentuální odhady počtu klientů v prvních pěti letech pro několik scénářů

Počet klientů KB 18<x>40	**Odhad 1 (511 672 rok 0)**	**Odhad 2 (717 582 rok 0)**	**Odhad 3 (132 000 rok 0)**
0.rok(%)	0,1%	0,1%	0,1%
1.rok(%)	5%	4%	30%
2.rok(%)	7%	5%	32%
3.rok(%)	9%	7%	35%
4.rok(%)	12%	10%	37%
5.rok(%)	13%	12%	39%

budou mít větší tendence věnovat pozornost i nové aplikaci. Spíše než klienti, kteří například jakékoliv mobilní bankovnictví odmítají úplně. Procenta v tomto sloupci jsou proto vyšší. Současný počet uživatelů mobilní banky se pohybuje kolem hodnoty 132 000 a má tendenci každoročního 20% růstu.

Po provedení těchto odhadů se již můžeme věnovat samotným výnosům aplikace. Výnosy jsou určeny pro všechny zvolené odhady v následujících pěti letech. Ve všech případech je počítáno s procentuálními odhady z předchozí tabulky. Do počtu uživatelů je dále započítán předpokládaný 1% nárůst počtu klientů KB. Roční náklady v nultém roce se skládají z hodnoty investice a dále z nákladů za tříměsíční provoz služby podle stanoveného harmonogramu. Provoz služby za ostatní roky je stanoven na 500 000 ročně. Do tohoto provozu se počítá uživatelská podpora, popřípadě práce vývojového týmu na potřebných opravách a provoz infrastruktury. Částka za jednu transakci je stanovena na 3Kč. Hodnota je stanovena tak, aby měla šanci přinést požadovaný zisk, ale stále neodradit potencionální zájemce o službu. 3 Kč se pro tyto účely zdá být optimální. Druhým scénářem je měsíční paušál, který by se vyplatil zejména lidem, kteří plánují posílat více než 1 transakci měsíčně. Částka je stanovena

na 5Kč měsíčně. Průměrný počet transakcí na osobu byl stanoven na 1,3. Zisk je počítán pro dva scénáře. První z nich je zpoplatnění transakce, druhý měsíční paušál. Pro výpočet zisku při platbě za transakci zisku při zavedení paušálu byly použity následující vzorce.

$$ZiskT = (poč.uživ. \times prům.poč.transakcí \times cena za transakci \times 12) - náklady$$

$$ZiskP = (poč.\ uživ. \times měsíční\ paušál \times 12) - náklady$$

Dále je v tabulkách počítána návratnost investice ROI (Return of investment), která je finančním ukazatelem zda se investice společnosti vyplatí či nikoliv za předpokládaných podmínek. ROI je počítána podle vzorce:

$$ROI(\%) = (\frac{čistý\ zisk}{investice}) \times 100$$

Posledním ukazatelem je NPV (Net present value), neboli čistá současná hodnota. Jedná se o diskontovanou finanční hodnotu všech peněžních toků souvisejících s investičním projektem. Výsledná hodnota udává, kolik peněz realizace investice podniku přinese. Pokud vyjde NPV kladné, je projekt přípustný. Oproti tomu pokud vyjde hodnota záporná, projekt je nepřijatelný. Vzorec je tak následující:

$$NPV = \sum_{i=0}^{t} \frac{CF}{(1+r)^t} kde\ r\ je\ 5\%$$

První sada tabulek 3.4 a 3.5 popisuje situaci prvního odhadu. Jak lze vidět, za rok 0 nemohou výnosy pokrýt náklady, naopak náklady za provoz ještě vzrostou. Druhý rok ale již generuje dostatečné výnosy v obou scénářích, aby pokryl provozní náklady služby a dále generoval zisk. Do zisku se projekt dostane během 5. roka své existence v případě zpoplatnění transakce a již v 4. roce při zavedení měsíčního paušálního poplatku. Z tabulky lze zjistit průměrnou návratnost investice, která se pohybuje kolem 8.75% pro zpoplatnění transakce a 18.77% pro paušální poplatek. Je zřejmé, že projekt se i při takto pesimisticky odhadnutém počtu klientů banky a posléze i počtu uživatelů aplikace po pěti letech vyplatí realizovat.

Druhá sada tabulek 3.6 a 3.7 ukazuje výsledky pro počet klientů podle optimističtějšího druhého odhadu. Pořád se ale počet předpokládaných klientů pohybuje pod hranicí současného počtu uživatelů mobilního bankovnictví Komerční banky. Projekt se začne dostávat do kladných čísel během čtvrtého roka v obou případech financování. Návratnost investice je 14,44% pro platbu za transakci a 26,05 v případě paušálního poplatku. Během pátého roku má projekt šanci překonat 4 milionovou hranici čistého zisku pro první případ a bez mála 8 milionovou hranici v případě druhém. Opět je zřejmé že se projekt i v tomto případě vyplatí.

Tabulka 3.4: Finanční ukazatele pro první odhad počtu klientů při měsíčním paušálním poplatku 5Kč

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	512	4 468 600	-4 443 733	-102,31%	-5 486 089
1	25 839	500 000	755 796	17,40%	-4 562 246
2	36 533	500 000	1 275 522	29,37%	-3 018 556
3	47 432	500 000	1 805 194	41,56%	-855 465
4	63 857	500 000	2 603 433	59,94%	2 233 236
5	69 843	500 000	2 894 380	66,64%	5 633 116

Tabulka 3.5: Finanční ukazatele pro první odhad počtu klientů při zpoplatnění transakce 3Kč a průměrném počtu 1.3 transakcí na osobu

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	512	4 468 600	-4 449 204	-102,43%	-5 492 843
1	25 839	500 000	479 521	11,04%	-4 906 703
2	36 533	500 000	884 907	20,37%	-3 835 752
3	47 432	500 000	1 298 052	29,88%	-2 280 349
4	63 857	500 000	1 920 678	44,22%	-1 666
5	69 843	500 000	2 147 616	49,44%	2 521 029

Tabulka 3.6: Finanční ukazatele pro druhý odhad počtu klientů při měsíčním paušálním poplatku 5Kč

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	718	4 468 600	-4 441 398	-102,25%	-5 483 207
1	28 990	500 000	598 965	13,79%	-4 751 066
2	36 597	500 000	887 307	20,43%	-3 677 209
3	51 738	500 000	1 461 271	33,64%	-1 926 227
4	74 629	500 000	2 329 018	53,62%	836 909
5	90 415	500 000	2 927 464	67,40%	4 275 652

Tabulka 3.7: Finanční ukazatele pro druhý odhad počtu klientů při zpoplatnění transakce 3Kč a průměrném počtu 1.3 transakcí na osobu

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	718	4 468 600	-4 433 726	-102,07%	-5 473 735
1	28 990	500 000	908 929	20,93%	-4 362 710
2	36 597	500 000	1 278 599	29,44%	-2 815 296
3	51 738	500 000	2 014 450	46,38%	-401 462
4	74 629	500 000	3 126 946	71,99%	3 308 332
5	90 415	500 000	3 894 185	89,65%	7 882 633

Tabulka 3.8: Finanční ukazatele pro třetí odhad počtu klientů při měsíčním paušálním poplatku 5Kč

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	132	4 468 600,00	-4 462 185	-102,73%	-5 508 870
1	39 996	500 000	1 443 806	33,24%	-3 744 042
2	43 085	500 000	1 593 921	36,70%	-1 815 011
3	47 586	500 000	1 812 680	41,73%	357 048
4	50 794	500 000	1 968 569	45,32%	2 692 549
5	54 054	500 000	2 127 024	48,97%	5 191 057

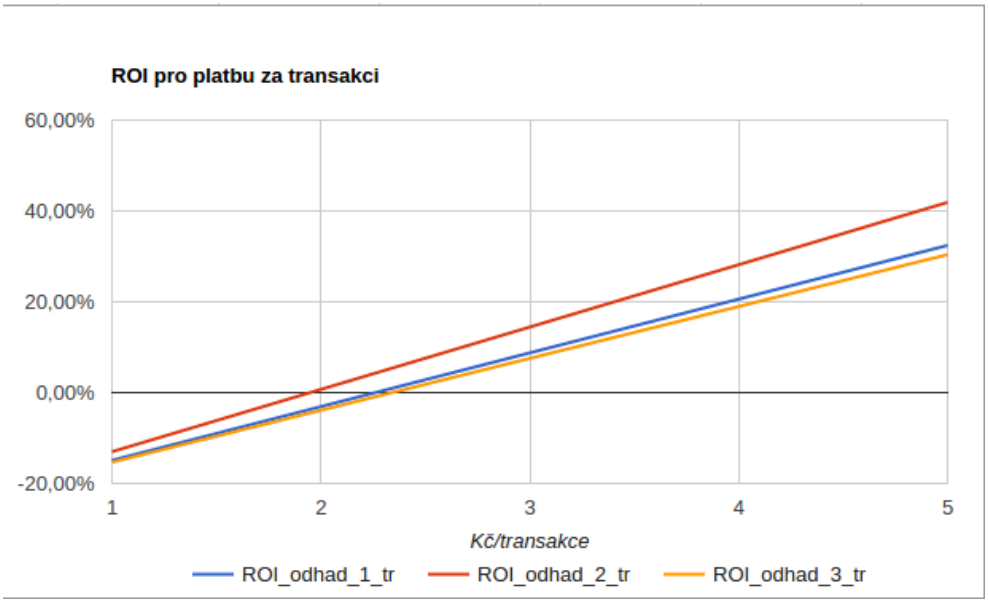
Poslední sada tabulek 3.8 a 3.9 reflektuje situaci, která je přímo odvozena od současného počtu klientů mobilního bankovnictví Komerční banky. Jedná se nejpesimističtější scénář ze všech tří zkoumaných. Cílem bylo zjistit zda projekt i případě nejvíce nepříznivého scénáře přinejmenším pokryje náklady na jeho relizaci. Jak je vidět do plusových hodnot se projekt dostane ve čtvrtém, nebo dokonce třetím roce v případě paušálního poplatku, ovšem výsledná částka kterou po pěti letech vygeneruje bude menší než v prvním odhadu. Průměrná návratnost investice je 7,54 potažmo 17,20%.

Z výsledků je zřejmé, že pokud se počet klientů služby přiblíží alespoň jedné z zkoumaných variant, dostane se v pětiletém intervalu při zavedených poplatcích vždy do kladných čísel. Nabízí se ale otázka, kde je v takovém případě ta hranice pro zavedení poplatku pod kterou se v žádném případě nevyplatí jít. Odpovědí jsou následující dva grafy 3.5 a 3.6.

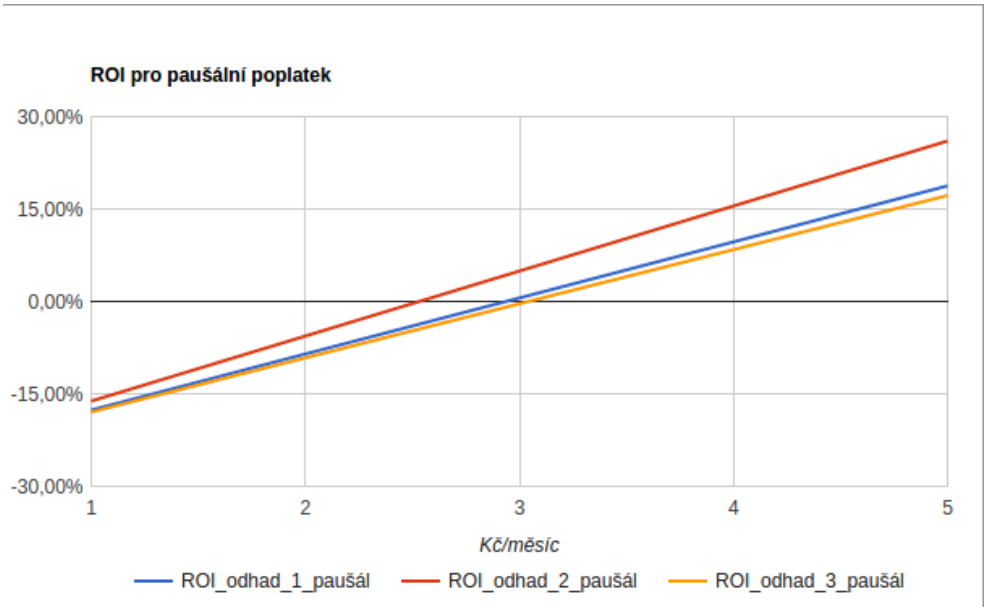
Z prvního grafu 3.5 lze vidět, že minimální částka za jednu transakci, tak aby zisk pokryl všechny náklady a byl schopen dále generovat výnosy společnosti je 3Kč. Takže prvotní odhad byl správný. Může být účtována i vyšší částka za jednu transakci, ale pak vzrůstá riziko, že odradí potencionální

Tabulka 3.9: Finanční ukazatele pro třetí odhad počtu klientů při zpoplatnění transakce 3Kč a průměrném počtu 1.3 transakcí na osobu

Rok	Počet uživ.	Roční náklady (Kč)	Zisk (Kč)	ROI	NPV (Kč)
0	132	4 468 600,00	-4 463 596	-102,76%	-5 510 612
1	39 996	500 000	1 016 168	23,39%	-4 268 504
2	43 085	500 000	1 133 259	26,09%	-2 896 987
3	47 586	500 000	1 303 890	30,02%	-1 334 588
4	50 794	500 000	1 425 484	32,82%	356 598
5	54 054	500 000	1 549 079	35,66%	2 176 222



Obrázek 3.5: Návratnost investice při různých hodnotách poplatku za transakci pro všechy odhady



Obrázek 3.6: Návratnost investice při různých hodnotách měsíčního paušálního poplatku pro všechny odhady

klienty a ve finále na tom banka prodělá. Graf tak představuje situaci právě při zachování stále stejného počtu klientů. V případě platby za transakci nelze doporučit vyšší částku.

Druhý graf 3.6 ilustruje změnu ROI pro výši měsíčního poplatku. Graf opět reflektuje situace při zachování stejného počtu klientů. Je jasné že tato částka bude nepatrně vyšší než v případě jednoduchého poplatku za transakci. Měsíční poplatek je samozřejmě pro banku výhodnější, což vyplývá i s předchozích tabulek. Jednak má banka v tomto případě k dispozici prostředky předem, ale zároveň generuje vyšší zisk. Pokud zůstává průměrný počet transakcí na 1,3, minimální hranice pod kterou se nevyplatí službu provozovat jsou 3 koruny měsíčně. Za 3 koruny dochází prakticky jen k pokrytí nákladů. V případě měsíčního poplatku je volba trochu volnější, neboť 5 korun měsíčně nemá takový negativní efekt jako 5 korun za transakci. Pro optimální vyvážení minimálního poplatku a maximálních zisků je doporučená hranice 5 Kč měsíčně. Lze očekávat, že se tato hodnota bude nacházet velmi blízko maximální částky, kterou je klient ochoten za tuto službu zaplatit.

Ideální je zkombinovat výhody obou strategií a nabídnout zákazníkovi možnost volby. Samozřejmě cílem banky by mělo být přesvědčit klienta ve výhodnost paušálního poplatku.

3.5 Rozbor reálných rizik

Nejprve je dobré rozlišit mezi hrozbou a rizikem. Hrozba je přírodní nebo člověkem podmíněný proces, který představuje možné ohrožení pro lidskou společnost. Riziko je potom pravděpodobnost, že nastane událost, kterou hrozba představuje.

Nyní si tedy rozebereme jednotlivá rizika, která ohrožují průběh projektu. Ke každému z nich je nutné přiřadit jeho pravděpodobnost, jeho popis. Dále pak kroky, které je potřeba podnikout ve snaze minimalizovat riziko a v poslední řadě také krizový plán. Smyslem tohoto plánování je snížit pravděpodobnost výskytu rizika a připravit případnou likvidaci následků incidentu. Existují mnohé případy, kde společnosti nevěnovaly mnoho pozornosti těmto přípravám a v okamžiku incidentu nebyly na řešení připraveny. V případě incidentu je po skončení likvidace následků potřeba opět analyzovat krizový plán a kroky k minimalizaci rizika.

Název rizika	**Příchod konkurence**
Pravděpodobnost	70%
Popis rizika	Na českém trhu v současnosti není žádná aplikace tohoto typu. Dokonce ani na kontinentálním evroském trhu se zatím nedá mluvit o rozšíření P2P plateb. Lze tedy očekávat, že již existující služby budou zvětšovat své pole působnosti zejména po zavedení PSD2.
Mitigace	Kvalitní PR připravované aplikace, získání povědomí klientů banky o službe ještě před samotným spuštěním, bonusy za pozvání
Krizový plán	Analýza konkurenceschopnosti. Zaměřit se na klíčové skupiny uživatelů. Podporovat příchod nových klientů, přehodnotit cenovou politiku

Název rizika	**Konzervatismus trhu**
Pravděpodobnost	65%
Popis rizika	Český trh je specifický svou konzervativností, je třeba počítat s nezájmem klientů o podobné aplikace. V takovém případě je potřeba překonat počáteční nedůvěru.
Mitigace	Důraz na celkovou bezpečnost aplikace. Kvalitní PR, důkladné proškolení personálu. Analýza existujícíh služeb.
Krizový plán	Určení cílové skupiny nejměné konzervativních uživatelů a přizpůsobení podmínek služby jejich potřebám

Název rizika	**Nízká výnosnost projektu p2p platformy**
Pravděpodobnost	20%

Popis rizika	O platby mobilním telefonem je zájem a jejich podíl na trhu zjevně roste, otázkou zůstává jak se český trh postaví k nové metodě placení s přihlédnutém k jeho zpoplatnění
Mitigace	Nalákat zákazníky vstupním bonusem, a bonusem za doporuční. Průběžné sledování popularity služby a školení zaměstnanců na podporu. Průzkum trhu před implementací služby. Hledání klientů v průmyslové oblasti
Krizový plán	Posílit PR, zhodnocení monetizační strategie.

Název rizika	**Protahování implementace, vyčerpání zdrojů**
Pravděpodobnost	20%
Popis rizika	Vývoj softwarového produktu je projektem u kterého se velmi obtížně odhaduje časová náročnost, zvláště pokud se jedná o projekt, který není standartním portfoliem společnosti.
Mitigace	Rozdělení projektu na iterace. Vytvoření finanční rezervy při plánování očekávaných zdrojů na projekt.
Krizový plán	Zhodnotit současnou situaci, identifikovat klíčovou komponentu projektu která generuje neočekávané výdaje. Vtvořit nový finanční plán a rozhodnout o pokračování či skončení projektu s ohledem na již vynaložené zdroje.

Název rizika	**Incident v datovém centru (povodeň, požár, výpadek proudu, připojení..)**
Pravděpodobnost	10%
Popis rizika	Datové centrum může ohrozit velká spousta okolnách vlivů, je potřeba se připravit na jejich řešení.
Mitigace	Pravidelné zálohování produkčních dat. Záložní servery musí být umístěny v jiné lokalitě aby se zmenšila pravděpodobnost vlivu jedné hrozby na všechny serverové instance.
Krizový plán	Přechod na záložní server, náhrada poškozeného serveru

Název rizika	**Kritická chyba v aplikaci**
Pravděpodobnost	7%
Popis rizika	Mobilní aplikace jako softwarový produkt je dílo složené z mnoha částí na kterých se podílel celý projektový tým. Může tedy dojít k situaci, kdy se kritická chyba dostane do produkční verze aplikace.

Mitigace	Aplikace by měla být testována již v průběhu jejího vývoje. Počínaje code review, přes funkční testování až po testování UI
Krizový plán	Zhodnocení závažnosti situace, zda zastavit službu nebo jen omezit některou funkcionalitu. Simulace vzniklého incidentu, identifikace krizového místa, vydání záplaty

Název rizika	**Nedostupnost člena týmu**
Pravděpodobnost	5%
Popis rizika	Vývoj produktu je závislý na činnosti jednotlivých členů, může proto dojít k situaci, kdy jeden nebo více členů týmu onemocní, zemře či podá výpoveď.
Mitigace	Tvorba projektové dokumentace, tvorba programové dokumentace včetně komentářů kódu. Finanční záloha.
Krizový plán	Zhodnotit do jaké míry je situace kritická a jestli se vyplatí alokovat jednoho člověka jako náhradu či více lidí (v případě že jeden odejde).

Název rizika	**Výpadek internetového připojení**
Pravděpodobnost	5%
Popis rizika	Internetové připojení je klíčové pro běh internetové služby.
Mitigace	Podpora více internetových linek různých poskytovatelů
Krizový plán	Zjištění důvodu výpadku, kontaktování poskytovatele, automatický přechod na sekundární linku připojení. Obnova původní linky

Název rizika	**Neočekávaný nárůst uživatelů popř. DDoS**
Pravděpodobnost	5%
Popis rizika	Byť vše nasvědčuje pozvolnému růstu klientů mobilní aplikace, je potřeba počítat i s případem kdy počet uživatelů vzroste exponenciálně nad očekávání dimenzace stávající infrastruktury
Mitigace	Připravit infrastrukturu na možné škálování jejího výkonu. Důraz na celkové zabezpečení v případě zahlcení
Krizový plán	Zapojit připravené servery, vydat prohlášení informující uživatele o dočasné nedostupnosti aby banka neztratila jejich důvěru. Zkontrolovat případné aktivity spojené s náhlým nárůstem provozu

Název rizika	**Nedostatečné zabezpečení, únik informací**
Pravděpodobnost	5%

Popis rizika	V dnešní době dochází k útoku na webové služby téměř na denním pořádku. Aplikace a celá její infrastruktura by na takovéto situace měla být připravena.
Mitigace	Důraz na zabezpečení aplikace, testování v celém průběhu SDLC. Dostatečné šifrování. Monitorování podezřelých transakcí.
Krizový plán	Neprodleně informovat klienty. Indentifikovat místo úniku informací, podstoupit kroky k zastavení úniku. Provést kroky k minimalizaci škod.

Název rizika	**Výpadek telefonické podopory**
Pravděpodobnost	2%
Popis rizika	Telefonická podpora je důležitá pro komunikaci se zákazníkem. Zákazník nesmí nabýt pocitu že je v problému sám, podpora musí být funkční 24/7
Mitigace	Opět je důležité více telefonních linek. Konfigurace centrály na přesměrování na krizová telefonní čísla.(např. mobilní telefony odpovědných zaměstnanců)
Krizový plán	Identifikace problému, záložní řešení na centrále

3.6 Analýza proveditelnosti

Ze získaných poznatků a provedené analýzy lze usoudit, že projekt má potenciál stát se úspěšným, nelze však očekávat masový zájem o produkt. Z velké části bude záležet na provedení aplikace a na jejím marketingu. Ze získaných monetizačních scénářů lze jasně vidět, že při získání očekávaného počtu klientů se pokryjí náklady a projekt začne generovat zisk do pátého roka jeho existence. Zvolené částky za provedení platby jsou reálné a do jisté míry akceptovatelné ze strany uživatelů. Z předchozí kapitoly vyplývá, že očekávané míry rizika jsou na hranici přijatelosti, v případě realizace je nutné podniknout kroky k jejich mitigaci. Zejména z hlediska bezpečnosti a PR.

3.7 Bezpečnost aplikace

Pro vytvoření dostatečně zabezpečené aplikace je potřeba integrovat bezpečnostního experta do vývojového týmu. Aby aplikace mohla provádět finanční operace, musí být bezesporu zajištěna ochrana uživatelů a jejich osobních dat. Veškerá komunikace bude probíhat v zašifrované podobě přes zabezpečený kanál HTTPS. Pro zvýšení bezpečnosti bude vyžadován minimální hashovací algoritmus sha2 a dálka klíče 2048 bitů. Nejde ale jen o zabezpečení komunikace, bezpečnostní parametry musí splňovat i samotná aplikace. V průběhu vývoje bude probíhat několik vln testování. Revize vyvinutého kódu bude sou-

částí vývojového procesu, ve snaze zamezit chybám programátora. Aplikace bude dostupná pouze pro zařízení která nejsou odemčena dalším úpravám, tzv. root.

Standardní metodou přihlášení bude jednofaktorové ověření pomocí hesla. Zákazník však bude mít možnost zpřísnit přidaná zabezpečení v nastavení aplikace. K dispozici bude volba dvoufaktorového ověření, nebo validace platby pomocí polohy.

Jelikož aplikace nepracuje s platebními kartami, není potřeba ji certifikovat PCI certifikátem. Pravidla pro udělení tohoto certifikáu ovšem zahrnují i obecná "best practices", je proto doporučené tato pravidla také respektovat.

Pokud se mluví o bezpečnosti aplikace, je dobré taktéž vzpomenout OWASP projekt. Jedná se o zkratku pro Open Web Application Security Project, open source komunitu, která se zaměřuje na zlepšování bezpečnosti software. Výsledkem jejich práce jsou studie, doporučení a softwarové nástroje, jejichž použití naplňuje ideu open source. Nejedná se pouze o bezpečnost webových služeb, ale i například mobilních aplikací. Pro vývoj bankovní aplikace je proto dobré vzít v úvahu již existující nástroje, a to z pohledu bezpečnostního experta, vývojáře či testera.

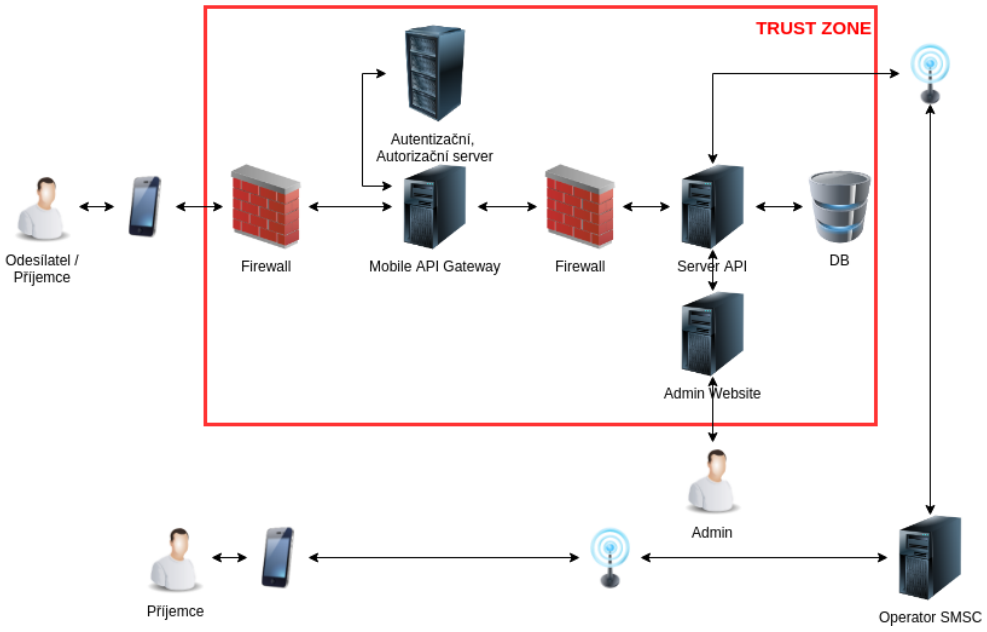
3.8 Návrh architektury

V následující kapitole je znázorněn návrh systému a databázový model aplikace. Je zřejmé že aplikace musí komunikovat s jejím uživatelem a zároveň si uchovat vysokou úroveň zabezpečení.

3.8.1 Nárvh systému

Návrh systému spočívá v určení návaznosti jednotlivých prvků síťové infrastruktury, do té míry aby bylo jasné jakým způsobem spolu budou komunikovat. Samozřejmě se nejedná o detailní model, tento musí být následně zpracován pro konkrétní nasazení na dané síti.

Následující model 3.7 si lze rozdělit na několik menších částí. První částí je samotný uživatelský vstup. Původním nápadem bylo vytvořit kromě mobilní platformy i platformu webovou, ale vzhledem k nákladnosti projektu, jeho výnosům a k faktu, že klient své prostředky mimo jiné může spravovat přímo na svém bankovním účtu bylo od tohoto záměru upuštěno. Zůstává tak pouze rozhraní mobilního zařízení. Druhá část je samotná funkcionalita systému, kterou uživatel vnímá jako tzv. "black box". To znamená, že systému předává vstupy a dostává od něj požadované odpovědi. Samotná implementace by měla uživateli zůstat utajena. Této části se dále budeme věnovat v dalším odstavci. Poslední částí je možnost využít sms brány poskytovatele signálu telefonního přístroje. Přes tuto bránu by měli být nezaregistrovaným příjemcům posílány zprávy o potřebné registraci do systému, popřípadě další nezbytné informace. Tento kanál již není potřeba mít chráněn zvláštním zabezpečením. Příjemci



Obrázek 3.7: Návrh architektury systému

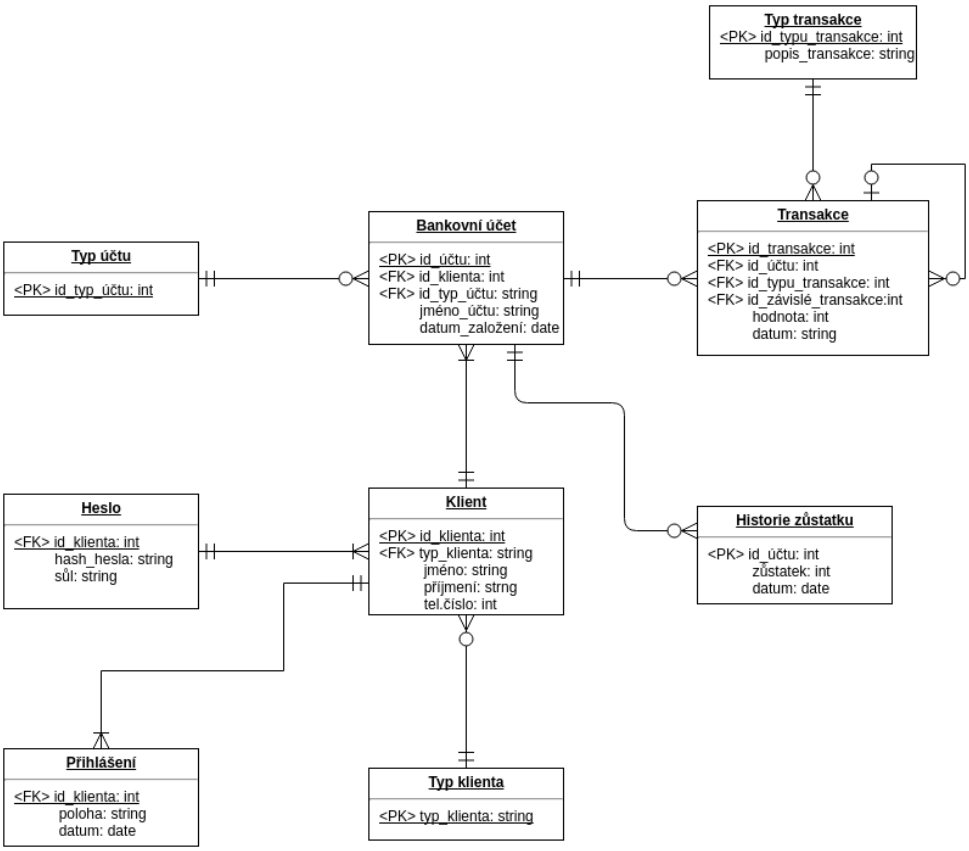
platby přijde SMS zpráva a on je následně nucen se zaregistrovat, aby se dostal k potřebným informacím či k elektronickým penězům.

Opět se vrátíme k samotné funkcionalitě systému. Na obrázku vyznačená jako "trust zone". Jedná se o část systému, kterou spravuje poskytovatel služby, v našem případě Komerční banka. Po navázání spojení klienta se serverem je komunikace vedena přes firewall na aplikační rozhraní. Zde dojde k autentizaci klienta pomocí autentizačního/autorizačního serveru. Aplikační rozhraní samozřejmě komunikuje se samotným aplikačním serverem, který má za úkol spravovat data uživatelů. Na tomto serveru by tak měla běžet služba která dokáže zpracovat požadavky o zaplacení a následně je zpracovávat. Na tento server je napojena samotná databáze.

3.8.2 Databázový model

V následující kapitole se budeme věnovat databázovému modelu aplikace. Databázový model je důležitý pro stanovení provázanosti jednotlivých databázových entit. Zejména při implementaci aplikačního serveru je třeba znát které tabulky jsou na sobě závislé.

Jak z následujícího obrázku 3.8 vyplývá, hlavní databázovou entitou je entita Klient. Ta k sobě vztahuje tabulku bankovní účet v relaci 1..n, neboli jeden klient může mít jeden a více účtů. Zároveň ale platí opačná relace, kde každý bankovní účet je vázán právě na jednoho klienta. Primárním klíčem klienta je jeho jednoznačné identifikační číslo, stejně jako pro číslo účtu. V



Obrázek 3.8: Návrh databázové struktury platebního systému

diagramu jsou vyznačené pouze informace potřebné pro funkčnost systému. Například pro klienta tak banka eviduje také jeho kontaktní informace, popřípadě číslo dokladu totožnosti. Tyto informace jsou vyžadovány zákonem při zakládání bankovního účtu. Pro každého klienta je v evidenci právě jedno heslo které je uloženo v samostatné tabulce. Zde samozřejmě nejsou uložena hesla v plain textové podobě ale pouze jejich hashe. Další tabulkou, která je provázána s klientem, je tabulka přihlášení. Tato tabulka je důležitá jednak vzhledem k evidenci přihlášení uživatele pro jeho samotné potřeby. Mimo jiné by nad databází měla být implementována funkcionalita evidující podezřelá přihlášení. Například, pokud se klient jednou ze svého účtu přihlásí v Praze a druhý den například v Moskvě, měl by obdržet upozornění o přihlášení z takového umístění.

Na bankovní účet se váže tabulka transakcí. V této tabulce je provázáno číslo bankovního účtu s bankovním účtem příjemce. Není potřeba v této tabulce evidovat dvě čísla. Neboť číslo odesílatele je provázané relací. Jedna transakce se vztahuje právě k jednomu bankovnímu účtu. Dále existuje závislá transakce. Jedná se o transakci, kterou eviduje příjemce platby. Samozřejmě

dalším nezbytným údajem je hodnota transakce a datum jejího plnění. Poslední tabulkou která se váže k bankovnímu účtu je tabulka historie zůstatku. Díky této tabulce tak klient může sledovat stav svého konta před několika dny a může tak lépe optimalizovat své výdaje a příjmy.

Zhodnocení

Banka zvažovala implementaci P2P služby jako nového produktu svého portfolia. Na výběr platformy mělo v konečném důsledku vliv několik faktorů. Hlavním z nich byla potřeba mobility, proto byla vybrána platforma mobilní. Dále byl s příhlédnutím na podíl jednotlivých mobilních operátorů vybrán mobilní operační systém Android a iOS. Na těchto platformách je možné vybudovat uživatelsky přívětivou aplikaci, která umožní správu bankovních plateb s pouhou znalostí telefonního účtu příjemce. Jako monetizační strategie byly zvoleny platba za transakci a měsíční paušál. Ostatní strategie se pro použití v bankovním produktu zdají být nevhodné. Jediná reklama, která je pro bankovní produkt akceptovatelná, je reklama dalších vlastních produktů banky. Ideální částky při vyvážení výhodnosti pro klienta i banku byly zvoleny na 3Kč za transakci nebo 5Kč měsíčně. Pro zjištění výnosnosti případně realizace projektu bylo vybráno několik scénářů potencionálního počtu uživatelů. První dva scénáře byly vybrány na základě věkového rozdělení populace a za předpokladu cílové skupiny starší 18 let a mladší 40. Do třetího scénáře byl zohledněn současný počet uživatelů již existující mobilní aplikace banky. Na základě dříve provedené analýzy předpokládané ceny projektu bylo zjištěno, že projekt má s odhadnutým počtem uživatelů šanci na úspěch.

Pro případného realizátora je však vždy nejprve nutné uvážit, zda míra některých rizik nepřevyšuje očekávání. Ze zjištěných rizik hraje nejvýznamější roli příchod konkurence a konzervatismus trhu. Příchod konkurence lze očeká-

Tabulka 3.11: Shrnutí návratnosti investice projektu

Název	Odhad 1	Odhad 2	Odhad 3
ROI transakce	8,75%	14,04%	7,54%
ROI paušální poplatek	18,77%	26,05%	17,20%

vat vzhledem k nové evropské direktivě PSD2. Lze také očekávat, že mezibankovní aplikace bude mít větší potenciál uspět, než aplikace zaměřená pouze na klienty jedné banky. Případné vytvoření mezibankovní platformy není součástí návrhu, ale pro obsažení celého trhu by bylo ideálním řešením i vzhledem k budoucí konkurenci. Konzervatismus trhu je faktorem, který přináší vysokou míru rizika zvláště v případě zpoplatněných služeb a je s ním tedy nutné dopředu počítat. Pro zajištění službě dostatečného množství klientů je nutné podpořit kvalitní marketingovou kampaň, která rozšíří povědomí lidí o nové bankovní aplikaci a rozptýlí jejich potencionální obavy ohledně bezpečnosti. Té je během implementace a testování potřeba věnovat velkou pozornost. Implementace by dle harmonogramu měla trvat přibližně půl roku. Její průběh je rozdělen do tří iterací, pro zajištění jednodušší správy celého procesu.

Závěr

Cílem diplomové práce bylo provést analýzu P2P služeb na celosvětovém trhu z pohledu bankovních i nebankovních subjektů. Dále vybrat několik existujících služeb, zhodnotit klíčové faktory úspěchu a jejich aplikovatelnost na českém trhu pro vybranou banku, coby realizátora projektu.

Po definici pojmu P2P služby a specifikování funkce bankovního systému v České republice jsem provedl průzkum poskytovatelů P2P služeb na zahraničních trzích. Na základě této analýzy jsem vybral několik klíčových produktů u nichž bylo provedeno mapování procesu platby a registrace nového klienta. Z analýzy dostupných služeb také byly stanoveny klíčové faktory jejich úspěchu. U těchto faktorů byla následně zhodnocena jejich aplikovatelnost na český trh. Zejména z hediska legislativy a specifik cílové skupiny. Po dokončení analýzy byla navržena cílová platforma pro implementaci služby a zvoleny konkrétní monetizační strategie. Na jejich základě bylo vypočítána návratnost počáteční investice. Vzhledem k výsledkům jsem dospěl k závěru, že případná implementace projektu pokryje náklady a je schopna dále generovat bance zisk. Po tomto finančním zhodnocení byla navržena aplikační infrastruktura a databázový model systému. Zároveň zhodnocena veškerá bezpečnostní rizika spojená s vývojem mobilní aplikace, coby cílové platformy.

Stanovené cíle se mi podařilo splnit, niceméně provedená studie byla z části založena na předpokladu získání minimálního počtu klientů. Dále z důvodu nedostupnosti zahraničních služeb pro český trhu bylo při provádění analýzy nutné vycházet z informací o službách dostupných pouze z internetových zdrojů.

Přínosem této práce pro čtenáře je přehled služeb fungujících v zahraničí a informace důležité k dosažení obdobného úspěchu na trhu tuzemském. Dalším přínosem pro banku je kalkulace možných výnosů dle zvolených scénářů přizpůsobených současné situaci. Dále může být práce považována za ucelený návod při plánování nasazení této služby.

Pokračování práce bych případně viděl v hlubší analýze zahraničního trhu s přístupem k zkoumaným aplikacím. Dále pak samotné pokračování projektu

od podrobnějšího návrhu po samotnou implementaci.

Literatura

[1] Dorová, Š. *Vývoj peněz na našem území*. Master's thesis, Bankovní institut vysoká škola Praha, 2014.

[2] Cvrčková, M. *Peníze v ČR - historie a současnost*. Master's thesis, Bankovní institut vysoká škola Praha, 2009.

[3] Zákon o platebním styku. 2009, [cit. 2016-27-12]. Dostupné z: `https://www.zakonyprolidi.cz/cs/2009-284`

[4] Ing. Dana Forišková, P. *Základy komerčního bankovnictví (Texty pro distanční studium)*. Master's thesis, Ostravská univerzita, 2008.

[5] Zákon České národní rady o České národní bance. 1993, [cit. 2016-27-12]. Dostupné z: `https://www.zakonyprolidi.cz/cs/1993-6`

[6] a kol., M. B. *Finanční právo*. C.H.Beck, 6th edition, 2012, ISBN 978-80-7400-440-7.

[7] Rozdíl mezí platební a kreditní kartou. 2012, [cit. 2016-27-12]. Dostupné z: `http://www.cfi.cz/aktuality/5-rozdil-mezi-platebni-a-kreditni-kartou`

[8] Ben Woolsey, E. S. G. The history of credit cards. 2016, [cit. 2016-27-12]. Dostupné z: `http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php`

[9] Pekárková, L. *Elektronické bankovnictví, jeho možnosti a další vývoj*. Master's thesis, Masarykova univerzita, 2008.

[10] Marková, B. S. *Elektronické bankovnictví, jeho prvky a vývojové tendence*. Master's thesis, Masarykova univezita, 2009.

[11] ČNB. Popis systému CERTIS. -, [cit. 2016-27-12]. Dostupné z: `https://www.cnb.cz/cs/platebni_styk/certis/certis_popis.html`

[12] Zákon o omezení plateb v hotovosti. 2004, [cit. 2016-27-12]. Dostupné z: http://business.center.cz/business/pravo/zakony/omezeniplateb/cast1.aspx

[13] EMV Payment Security. 2014, [cit. 2016-27-12]. Dostupné z: https://crypto.stanford.edu/~dabo/courses/cs255_winter14/lectures/EMV.pdf

[14] Přes tři tisíce klientů Komerční banky už platí kartou v chytrém telefonu. 2016, [cit. 2016-27-12]. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/pres-tri-tisice-klientu-komercni-banky-uz-plati-kartou-v-chytrem-telefonu-1215/

[15] Naprostá většina Čechů neře'v sí zabezpečení mobilů proti napadení. *Novinky.cz [online]*, září 2016, [cit. 2016-27-12]. Dostupné z: https://www.novinky.cz/finance/415233-naprosta-vetsina-cechu-neresi-zabezpeceni-mobilu-proti-napadeni.html

[16] Ha, T. T. T. *Bitcoin jako platební a investiční nástroj*. Master's thesis, Mendelevova univerzita v Brně, 2016.

[17] Terri Brandford, W. R. K. New Person-to-Person Payment Methods: Have Checks Met Their Match? -, [cit. 2016-27-12]. Dostupné z: https://www.kansascityfed.org/publicat/econrev/pdf/12q3Bradford-Keeton.pdf

[18] CERN. Password Recommendations. -, [cit. 2016-27-12]. Dostupné z: https://security.web.cern.ch/security/recommendations/en/passwords.shtml

[19] Raywood, D. Mobile App Research Shows Major Flaws Persist. 2015, [cit. 2016-27-12]. Dostupné z: http://www.infosecurity-magazine.com/news/mobile-app-research-shows-major/

[20] Seth, S. Venmo: Its Business Model and Competition. 2015, [cit. 2016-27-12]. Dostupné z: http://www.investopedia.com/articles/personal-finance/010715/venmo-its-business-model-and-competition.asp

[21] Square. Serious about Security. -, [cit. 2016-27-12]. Dostupné z: https://squareup.com/security

[22] Green, T. Zapp andr Paym - just what is the difference? 2014, [cit. 2016-27-12]. Dostupné z: http://www.mobilemoneyrevolution.co.uk/zapp-and-paym-just-what-is-the-difference/

[23] Paul, I. PayPal launches PayPal.me, a person-to-person payment service. 2015, [cit. 2016-27-12]. Dostupné z: http://www.pcworld.com/article/

2978809/web-apps/paypal-launches-paypal-me-a-person-to-person-payment-service.html

[24] ClearXChange Review. 2015, [cit. 2016-27-12]. Dostupné z: http://www.toptenreviews.com/business/payment-processing/best-p2p-payments/clearxchange-review/

[25] Innofis. Mobile Payments trends. 2014, [cit. 2016-27-12]. Dostupné z: http://www.innofis.com/mobile-payments-trends/

[26] Zdeněk Bubák, H. K. Proč Mobito letos v prosinci končí? Co nabízí jeho konkurence? 2015, [cit. 2016-27-12]. Dostupné z: http://www.finparada.cz/3118-Proc-Mobito-letos-v-prosinci-skonci-Co-nabizi-konkurence.aspx

[27] Směrnice evropského parlamentu a rady 2007/64/ES o platebních službách na vnitřním trhu. 2015, [cit. 2016-27-12]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[28] Zeman, M. Platby protřednictvím auta. Nový směr v bankovních inovacích. 2016, [cit. 2016-27-12]. Dostupné z: http://www.bankovnipoplatky.com/platby-prostrednictvim-auta-novy-smer-v-bankovnich-inovacich-33584

[29] Khan, F. How do contactless payment cards work. 2014, [cit. 2016-27-12]. Dostupné z: https://www.quora.com/How-do-contactless-payment-cards-work

[30] History of Mobile & Contactless Payment Systems. -, [cit. 2016-27-12]. Dostupné z: http://nearfieldcommunication.org/payment-systems.html

[31] Bebusinessed. The history of money. -, [cit. 2016-27-12]. Dostupné z: http://bebusinessed.com/history/the-history-of-money/

[32] Mošnička, M. Bezkontaktní platby nastupují na český trh. 2011, [cit. 2016-27-12]. Dostupné z: http://www.finparada.cz/215-.aspx

[33] Obržálková, B. V. Bankovní systém. -, [cit. 2016-27-12]. Dostupné z: http://www.soudom.cz/files/financovani_obchodniho_podniku/vy-62-inovace-02.05.pdf

[34] Iveta, H. *Banky a bankovní systém*. Master's thesis, Masarykova univerzita, 2008.

[35] Způsoby placení hotovostní a bezhotovostní. 2008, [cit. 2016-27-12]. Dostupné z: http://www.tivit.cz/poradime-vam/financni-poradenstvi/penize/zpusoby-placeni/zpusoby-placeni-hotovostni-a-bezhotovostni

[36] Novotný, M. *Elektronické bankovnictví ve veřejném sektoru*. Master's thesis, Vysoká škola ekonomická v Praze, 2007.

[37] Müller, J. Proč to penězům z účtu na účet i v dnešní době internetu tak trvá. *finexpert.e15.cz [online]*, duben 2013, [cit. 2016-27-12]. Dostupné z: http://finexpert.e15.cz/proc-to-penezum-z-uctu-na-ucet-i-v-dobe-internetu-tak-trva

[38] Pegueros, V. Security of Mobile Banking and Payments. 2012, [cit. 2016-27-12]. Dostupné z: https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062

[39] Google. Frequently Asked Questions. -, [cit. 2016-27-12]. Dostupné z: https://www.google.com/wallet/faq/

[40] PayPal. PayPal.me requently Asked Questions. -, [cit. 2016-27-12]. Dostupné z: https://www.paypal.me/pages/faqs

[41] Salmon, F. Why ClearXChange is great for payments. 2011, [cit. 2016-27-12]. Dostupné z: http://blogs.reuters.com/felix-salmon/2011/05/25/why-clearxchange-is-great-for-payments/

[42] Griswald, A. Venmo Money, Venmo Problems. 2015, [cit. 2016-27-12]. Dostupné z: http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.html

[43] Seth, S. Venmo: Its Business Model and Competition. 2015, [cit. 2016-27-12]. Dostupné z: http://www.investopedia.com/articles/personal-finance/010715/venmo-its-business-model-and-competition.asp

[44] Ph.D., D. I. P. D. *Bankovnictví pro bankéře a klienty*. Linde Praha a.s., third edition, 2005, ISBN 80-7201-515-X.

[45] Wen-ChenHu, W. K., Chung-wei Lee. *Advances in Security and Payment Methods for Mobile Commerce*. Idea Group, first edition, 2004, ISBN 1-59140-345-6.

[46] Person-To-Person Payments: An Update. 2014, [cit. 2016-27-12]. Dostupné z: http://www.paymentsjournal.com/WorkArea/DownloadAsset.aspx?id=22928

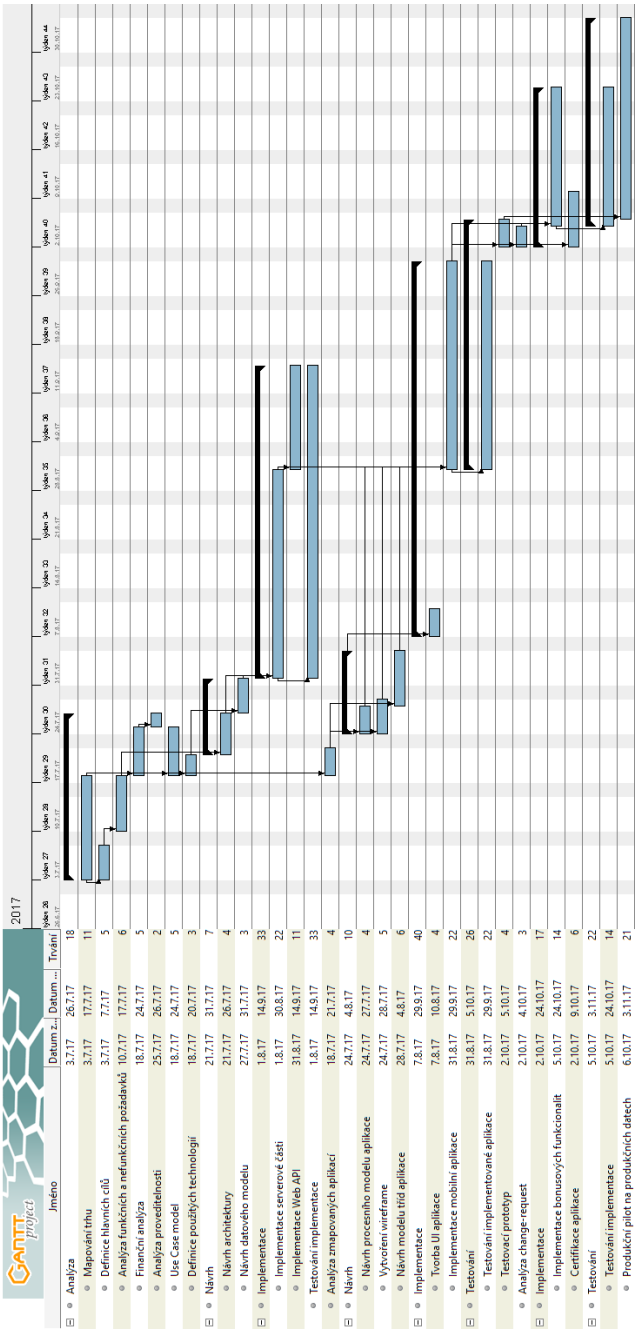
[47] Sucháčková, N. *Srovnání bankovního systému ČR a vybrané země*. Master's thesis, Bankovní institut vysoká škola Praha, 2014.

[48] ČSÚ. Vekové složení obyvatelstva - 2015. 2015, [cit. 2016-27-12]. Dostupné z: `https://www.czso.cz/csu/czso/vekove-slozeni-obyvatelstva`

[49] Sanchez, A. Personal banking apps leak info throufgh phone. 2015, [cit. 2016-27-12]. Dostupné z: `http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html`

Příloha A

Obrázky



Obrázek A.1: Odhad časové náročnosti projektu, včetně návaznosti dílčích kroků

Příloha B

Seznam použitých zkratek

P2P Peer To Peer

PSD2 The Second Payment Services Directive

OS Operating System

QR Quick Response

PAN Primary Account Number

RFID Radio Frequency Identification

POS Point Of Sale

ISO International Organization for Standardization

NFC Near Field Communication

SDA Static Data Authentication

DDA Dynamic Data Authentication

SIM Subscriber Identity Module

PCI-DSS Payment Card Industry Data Security Standard

PA-DSS Payment Application Data Security Standard

HCE Host Card Emulation

MITM Men In The Middle

SSL/TLS Secure Sockets Layer/Transport Layer Security

CERTIS Czech Express Real Time Interbank Gross Settlement System

OWASP Open Web Application Security Project

CIA Confidentiality, Integrity, Availability

API Application Interface

ČSÚ Český Statistický Úřad

SMS Short Message Service

USSD Unstructured Supplementary Service Data

NPV Net Present Value

ROI Return Of Investment

CA Certification Authority

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `DP_Pesta_Petr_2017.tex` .... zdrojová forma práce ve formátu LaTeX
- `přílohy`
  - `gantt_diagram.png` ..... diagram časového plánu projektu
- `text`
  - `DP_Pesta_Petr_2017.pdf` ..... text práce ve formátu PDF
  - `DP_Pesta_Petr_2017.ps` ..... text práce ve formátu PS