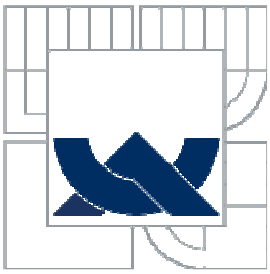


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT

INSTITUTE OF INFORMATICS

ANALÝZA A NÁVRHY ELEKTRONICKÉHO BANKOVNICTVÍ

ANALYSIS AND DESIGN OF ELECTRONIC BANKING

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — LUBOMÍR MAŤÁK

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZUZANA NĚMCOVÁ, PhD.

SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Maťák Lubomír, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Analýza a návrhy elektronického bankovnictví

v anglickém jazyce:

Analysis and Design of Electronic Banking

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrh řešení
Zhodnocení návrhu
Závěr
Seznam použitých informačních zdrojů
Rejstřík
Přílohy

Seznam odborné literatury:

MÁČE, M. Platební styk klasický a elektronický. 1. vyd. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.
MARK L. MURPHY. Průvodce programováním mobilních aplikací. Albatros Media, 2011. 376 s. ISBN 978-80-251-3194-7.
POLČÁK, R. Internet a proměny práva. Auditorium. 2012. 388 s. ISBN 978-80-872-8422-3.
ROONEY, A. Velká kniha o počítačích. Internet a mail, databáze a texty, obrázky a prezentace, grafy a schémata. MLADÁ FRONTA, 2010. 160 s. ISBN 978-80-204-2220-0.
SCHLOSSBERGER, O. Elektronické platební prostředky. Praha: Bankovní institut, 2005. 276 s. ISBN 80-7265-073-4.

Vedoucí diplomové práce: Ing. Zuzana Němcová, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 22.04.2013

Abstrakt

Obsahem diplomové práce je analýza zvoleného bankovního sektoru pro Komerční banku a vytvoření návrhu a zhodnocení problematiky internetového a převážně mobilního bankovnictví..

Abstract

The content of the thesis is an analysis of selected banking for Komercni banka and create the design and evaluation of the issue of online and mobile banking mainly.

Klíčová slova

elektronické bankovnictví, internetbanking, elektronické podnikání, smartbanking

Keywords

electronic banking, Internet banking, e-business, smartbanking

Bibliografická citace mé práce

MAŤÁK, L. *Analýza a návrhy elektronického bankovnictví.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 80 s. Vedoucí diplomové práce Ing. Zuzana Němcová, Ph.D..

Prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 20.5.2013

Poděkování

Rád bych touto cestou poděkoval vedoucí své diplomové práce Ing. Zuzaně Němcové, PhD. za ochotu, cenné rady a připomínky, které mi poskytla při zpracování práce.

Obsah

Úvod

Elektronický obchod a vše s ním spojené, dnes hraje ve světě businessu a podnikání velice významnou roli. Ne každá firma ale potenciálu, který tato forma obchodování nabízí, využívá naplno. V posledních letech se vývojáři stále více a více zaměřují na miniaturizaci zařízení a snaží se poskytnou maximální volnost a mobilitu uživatele. Není tomu tak dávno, co stolní počítače nahradily menší a trasportnější notebooky a ty teď pomalu vytlačují tablety. Využívat připojení k internetu odkudkoli je dnes tak běžné, jako před deseti lety telefonovat. Mobilní telefony už dnes nejsou jen mobilními telefony určeny primárně k telefonování a zasílání krátkých zpráv, ale jsou to i jakési kapesní počítače, díky kterým dnes nemusí spousta uživatelů trávit hodiny sezením u stolu, ale běžné záležitosti vyřizovat přímo v terénu. Společnosti ze všech odvětví musí na tento trend okamžitě reagovat. Musí vyvíjet a upgradovat své produkty tak, aby vyhovovaly dnešnímu rychlému životnímu stylu.

Zásadní oblast, která musí na tento trend reagovat je oblast bankovnictví. Lidé dnes nejsou ochotni stát dlouhé fronty u přepážek aby provedli platbu či zjistili stav svého účtu. Chtějí mít možnost, využívat těchto služeb kdykoli a kdekoli. Díky rozmachu smartphonů, tabletů a mobilního internetu, je dnes možnost spravovat své finance kdykoli a kdekoli, dostupná v podstatě každému.

Tato práce se zabývá a rozebírá přístup Komerční banky ke konceptu online bankovnictví a zaměřuje se hlavně na nejmodernější formu přímého bankovnictví, smartbanking. Výstupem práce pak bude zhodnocení a srovnání její aplikace s aplikacemi konkurenčních bank na českém trhu a návrh na možné změny, vylepšení a doladění chyb a nedostatků, kterými tato aplikace disponuje.

1. Vymezení problému a cíle práce

1.1. Vymezení problému

Diplomová práce je koncipována jako analýza a zhodnocení současného a budoucího stavu nabídky elektronického a mobilního bankovnictví Komerční banky a.s., z pohledu jejich nezaujatého klienta. Cílem je, pomocí výsledků analýz, navrhnout opatření, které mohou napomoci vyšší konkurenceschopnosti banky a vytvoření stabilnějšího postavení v době vzniku velkého množství konkurence, díky nízkým bariérám vstupu do odvětví.

V loňském roce, v době vývoje aplikace, jsem se aktivně podílel na vývoji a testování nových prostředků elektronického bankovnictví pro Komerční banku. Ta jako jedna z prvních na světě vůbec, připravila pro své klienty možnost obsluhy svých produktů skrze mobilní telefon. Od toho okamžiku jakoby se zastavil čas a KB pro své klienty nic dalšího, co by překonalo očekávání, nepřipravila. Spíše držela krok s konkurencí a po čase začala dokonce zaostávat.

Tato práce pojednává o okamžiku, kdy se KB usilovně snaží opět získat vedení v rozsahu a kvalitě nabízených služeb a stát se jedničkou mezi tuzemskými bankami, co se technické stránky týče.

1.2. Cíl práce

Cílem této diplomové práce je provést analýzu zvoleného bankovního segmentu a na základě této analýzy vytvořit návrh případných změn a hodnocení elektronického bankovnictví. Dílčími cíly pak bude analýza stávajícího stavu elektronického bankovnictví vybrané banky a zhodnocení připravovaných změn a tyto změny pak porovnat s konkurencí.

Kapitola **Teoretická východiska práce** se zaměřuje na uvedení do problematicky elektronického bankovnictví. Ve stručnosti ukazuje vývoj internetu a internetového bankovnictví až do současnosti.

V následující kapitole **Analýza problému a současné situace** budou nejdříve provedeny analýzy oborového prostředí prostřednictvím Porterova modelu konkurenčních sil, dále SWOT analýzy, která odhalí silné a slabé stránky, příležitosti a hrozby společnosti. V rámci SWOT analýzy bude provedeno rovněž její matematické zhodnocení. V neposlední řadě je analýza zaměřena na přímé bankovnictví Komerční banky.

Poslední kapitola je zaměřena na zhodnocení a zpracování výsledků analýz a navržení doporučení na zlepšení konkurenceschopnosti zmíněné banky.

2. Teoretická východiska práce

V této kapitole bude stručně shrnut historický vývoj internetu, jako takového, dále se zaměřuje na problematiku elektronického obchodování, internet bankingu, smartbankingu a především jejich zabezpečení.

2.1. Historický vývoj internetu

Za skutečný historický počátek Internetu lze požadovat rok 1958, kdy prezident Eisenhower požádal o přidělení fondů na vytvoření Agentury moderních výzkumných projektů – ARPA (Advanced Research Projects Agency). Cílem této agentury měl být vývoj decentralizované počítačové sítě, která by umožnila komunikaci řídících středisek obranného systému USA a vybraných výzkumných pracovišť v případě jaderného útoku proti USA. Prostředky byly vyhrazeny z rozpočtu amerického vojenského letectva. (17)

Až do poloviny osmdesátých let se Internet rozvíjel pozvolna a je omezen především na vládní a vojenské organizace. Významnou posilu dostává Internet v polovině osmdesátých let, kdy se k němu začínají připojovat americké univerzity. Zásadní impuls přichází v roce 1986, kdy vzniká síť NSFNET, páteřní síť Internetu v USA. Provoz této páteřní sítě byl financován z rozpočtu vládní agentury NSF (National Science Foundation). Tato síť nahradila dosavadní ARPANET a MILNET (Military Network). Obě tyto starší sítě se vrátily ke svému původnímu určení a začaly opět sloužit výhradně armádě. Vytvoření páteřní sítě NSFNET podnítilo další připojování do Internetu. Ten se stává ověřenou doménou pro vzdělání a výzkum. Postupně se do Internetu připojují všechny významnější americké univerzity a výzkumné ústavy. Počátkem devadesátých let vstupuje do děje i český internet. Vznikl a propojil se se světem a začal jím být ovlivňován. Od roku 1993 prožívá Internet v USA veliký rozmach. O dva roky později, v roce 1995, je na Internet připojen dvojnásobek počítačů v porovnání s rokem 1993. Jde již o dva miliony počítačů.

Internet začíná v poslední době zásadním způsobem ovlivňovat nejen přístup k informacím, ale i rozvoj obchodu. E-business – využití internetu pro obchodní účely se stává denní součástí našeho života. (24, 30)

2.2. Bezpečnost na internetu

Kapitola se zaměřuje na problematiku bezpečnosti ve virtuálním prostředí. Rozsah práce nedovoluje detailní rozbor všech možných typů útoků a zabezpečení, proto je cílem této časti lehce nastínit možné základní hrozby a jejich řešení.

2.2.1. Tři základní notace

Autentizace

Autentizace je proces ověření identity subjektu. Potřebujeme potvrdit, že druhým účastníkem komunikace, transakce jsme právě my a nikdo jiný. Potřebujeme vědět, že v určitých transakcích se za nás nemůže nikdo jiný vydávat. Subjekt vydá prohlášení o své identitě – 1:1. (6)

Autorizace

Autorizace obvykle následuje po autentizaci. Je to souhlas, schválení, umožnění přístupu či provedení konkrétní operace daným subjektem. Je to povolení přístupu někam, k někomu nebo něčemu (nejen ve smyslu přístupu do konkrétních prostor nebo k nějaké osobě, ale také přístup k informacím, funkcím, programovým objektům a podobně). (6)

Identifikace

Identifikace je porovnání nezaměnitelných charakteristik předmětu s následným určením nebo vyloučením shodnosti. Systém prochází všechny záznamy v databázi, aby našel shodu – 1:n. (6)

Vícefaktorová autentizace

Jednou z nejúčinnějších metod bezpečné autentizace, je kombinace více faktorů. Těmito faktory jsou:

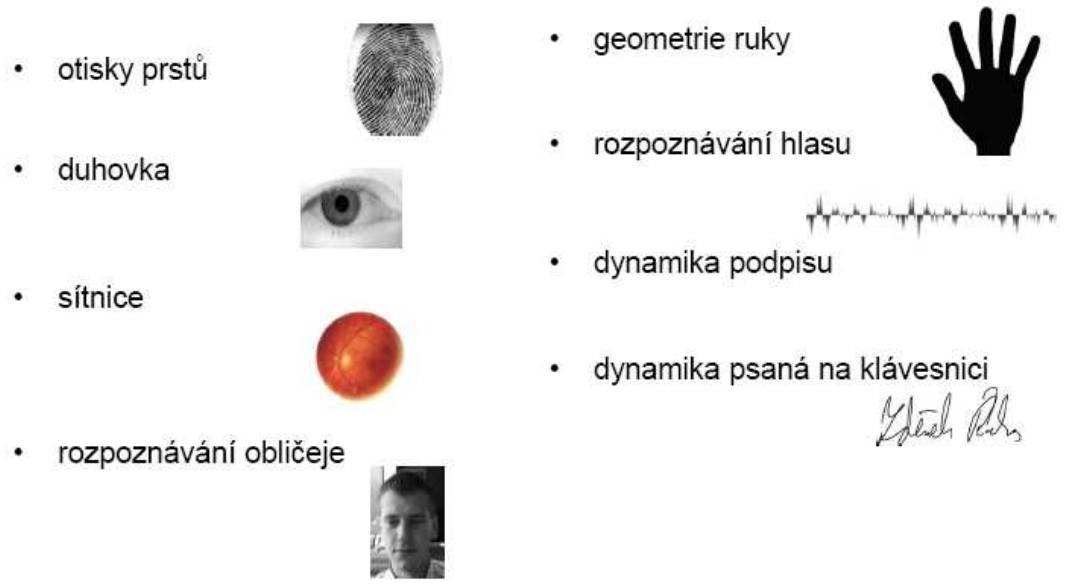
- něco co znám
- něco co mám
- něco co jsem

Dvoufaktorová autentizace

V praxi vypadá dvoufaktorová autentizace tak, že kromě klasického hesla nebo PINu, přidáme něco, co uživatel má, např. token. Token je malý předmět, který musí mít klient u sebe ve chvíli přihlašování k internetovému bankovnictví. Tokenem může být i čipová karta, USB token, mobilní telefon nebo autentizační kalkulátor. Využívají se také certifikáty, nebo jednorázová hesla. Evropské i tuzemské banky se snaží dvoufaktorovou autentizaci klientům nabízet.

Třífaktorová autentizace

Zřídka se také můžeme setkat s třífaktorovou autentizací, kde třetí faktor je biometrika. Biometrické metody autentizace vycházejí z předpokladu, že mnohé charakteristiky jsou jedinečné pro každého živého člověka a zároveň jsou průběhu času minimálně proměnné. (19)



Obrázek 1: Biometrické technologie
Zdroj: (9)

2.2.2. Zabezpečení proti útoku Man-In-The-Middle

Man in the middle (dále jen MITM) patří mezi nejznámější problémy v informatice a kryptografii. Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Důležitým faktem je, že v prostředí současných běžných počítačových sítí není nutné, aby Malory (útočník) ležel fyzicky na cestě mezi Alicí a Bobem, protože lze síťový provoz snadno přesměrovat.

Útok MITM lze řešit několika způsoby:

- vzájemnou výměnou veřejných klíčů jiným bezpečným kanálem (požadavkem na bezpečný kanál pro výměnu klíčů ovšem přicházíme o zásadní výhodu asymetrické kryptografie, kde ideálně takový kanál nepotřebujeme),
- ověřením získaných veřejných klíčů jiným bezpečným kanálem, nejlépe pomocí jejich otisku (např. telefonicky),
- ověřením klíčů pomocí elektronického podpisu Alice i Boba pomocí certifikační autority nebo sítě důvěry (tzv. digitální certifikát).

Kvantová kryptografie umožňuje připravit takový kanál, který je z principu neodposlouchávatelný, neboť každou snahu o odposlouchávání dokáže pravý příjemce detekovat. (6)

2.2.3. Elektronický podpis

Elektronický podpis je identifikační údaj autora (odesílatele) elektronického dokumentu, k němu připojeného. Za elektronický podpis se v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (například jména a adresy, názvu a sídla, rodného nebo jiného identifikačního čísla atd.) na konci textu v elektronické (digitální) podobě, které zaručuje identifikaci (tedy jednoznačné určení) označené osoby, avšak nikoliv integritu podepsaného dokumentu ani autentizaci podepsaného.

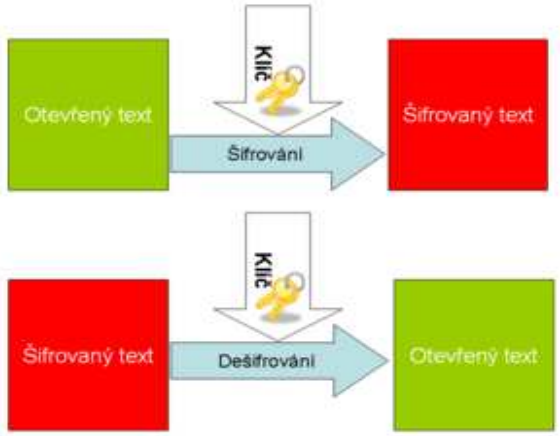
Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Zaručený elektronický podpis je aplikací asymetrické kryptografie. (2, 36)

2.2.4. Symetrická a asymetrická šifra

Symetrická šifra

Symetrická šifra, někdy též nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Tím se liší od algoritmů s veřejným klíčem, které mají dvojici klíčů – tajný a veřejný.

Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší. Na druhou stranu velkou nevýhodou je nutnost sdílení tajného klíče, takže se odesilatel a příjemce tajné zprávy musí předem domluvit na tajném klíči. (2)

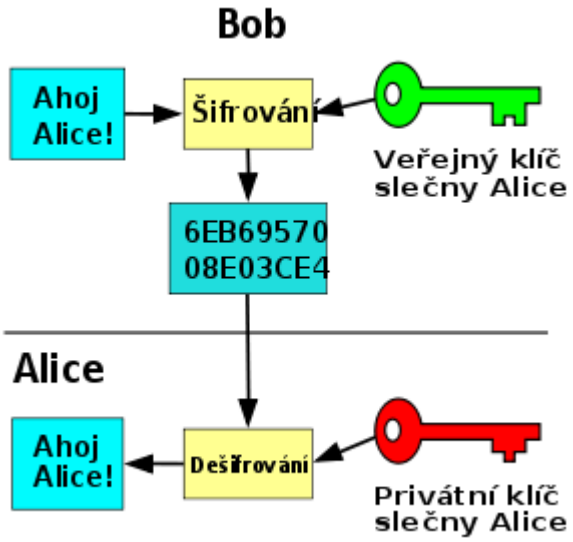


Obrázek 2: Šifrování a dešifrování pomocí jediného klíče
Zdroj: (2)

Asymetrická šifra

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče. To je základní rozdíl oproti symetrické kryptografii, která používá k šifrování i dešifrování jediný klíč.

Kromě očividné možnosti pro utajení komunikace se asymetrická kryptografie používá také pro elektronický podpis, tzn. možnost u dat prokázat jejich autora. (2)



Obrázek 3: Asymetrické šifrování
Zdroj: (2)

2.2.5. Certifikáty

Digitální certifikát je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita. Uchovává se ve formátu X.509, který (kromě jiného) obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. certifikační autoritě). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN atp.). Na základě principu přenosu důvěry je možné důvěřovat neznámým certifikátům, které jsou podepsány důvěryhodnou certifikační autoritou. (13)

2.2.6. Šifrovací standardy a protokoly

DES

Date Encryption Standard je v kryptografii symetrická šifra vyvinutá v 70. Letech společností IBM. V roce 1977 byla zvolena za standard pro šifrování dat v civilních státních organizacích v USA a následně se rozšířila i do soukromého sektoru. V současnosti je tato šifra považována za nespolehlivou, protože používá klíč pouze o délce 64 bitů, z toho 8 je kontrolních a 56 efektivních. Navíc její algoritmus obsahuje slabiny, které dále snižují bezpečnost šifry. Díky tomu je možné šifru prolomit útokem hrubou silou za méně než 24 hodin. (6)

AES

Advanced Encryption Standard je symetrická bloková šifra, která nahradila dříve užívanou šifru DES. Dnes je používána například pro bezdrátové Wi-Fi sítě v rámci zabezpečení WPA2 dle standardu IEEE 802.11i. (3)

WEP

Wired Equivalent Privacy (soukromí ekvivalentní drátovým sítím) je v informatice označení pro zastaralé zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997. Cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím (např. kroucená dvojlinka), protože rádiový signál je možné snadno odposlouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí. WEP byl prolomen v srpnu 2001, a proto bylo jeho nasazení nahrazeno zabezpečením pomocí WPA2 podle standardu IEEE 802.11i. (13)

WPA

Wi-Fi Protected Access (chráněný přístup k Wi-Fi) je v informatice obchodní označení pro zabezpečení bezdrátových sítí. Po prolomení zabezpečení WEP v roce 2001 definovala Wi-Fi Alliance v roce 2002 zabezpečení WPA pro Wi-Fi sítě jako část tehdy připravovaného standardu IEEE 802.11i. (7)

WPA2

IEEE 802.11i, také známý jako WPA2, je dodatek k IEEE 802.11 standardu vylepšující autentizační a šifrovací algoritmus pro bezdrátové sítě Wi-Fi. Byl schválen 24. června 2004 a zneplatňuje tak původní zabezpečení Wired Equivalent Privacy (WEP), které má mnoho bezpečnostních slabin. Wi-Fi Protected Access (WPA) je předchůdce WPA2, ale místo implementace plného IEEE 802.11i implementuje pouze 3. návrh tohoto standardu, tedy pouze podmnožinu 802.11i.

WPA2 používá blokovou šifru Advanced Encryption Standard (AES), zatímco dřívější WEP a WPA používají proudovou šifru RC4. 802.11i architektura obsahuje následující komponenty: IEEE 802.1X pro autentizaci (používá tedy Extensible Authentication Protocol (EAP) a autentizační server), Robust Security Network (RSN) pro udržování záznamu asociací a na AES založený Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), který poskytuje utajení,

integritu a autentizaci. Dalším důležitým prvkem autentizačního procesu je čtyřcestný handshake. (7)

SSL

Secure Sockets Layer (vrstva bezpečných socketů) je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran. Následovníkem SSL je protokol Transport Layer Security (TLS). (11)

HTTPS

Hypertext Transfer Protocol Secure je v informatice nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. HTTPS používá protokol HTTP, přičemž přenášená data jsou šifrována pomocí SSL nebo TLS a standardní port na straně serveru je 443.

Základy pro dnešní podobu HTTPS sahají do devadesátých let minulého století. Tehdy společnost Netscape Communications přišla s první verzí protokolu SSL, který vytvořila pro svůj webový prohlížeč. Tento protokol pak umožnil aplikačním protokolům možnost šifrovaného přenosu informací a ověření identity. (18)

2.3.Elektronický obchod

Pod pojmem „elektronický obchod“ rozumíme podnikání elektronickými prostředky. To zahrnuje obchodování se zbožím hmotným i nehmotných (potraviny, hudební nahrávky atd.) i službami (informačními, právními atd.). Zahrnuje všechny kroky od reklamy přes uzavření smlouvy, její plnění, a to včetně prodejní podpory a služeb. Z právního hlediska jde zásadně o projevy vůle – právní úkony, směřující k uzavírání smluv, které jsou realizovány pomocí počítačových sítí. (16)

Dokument Bílá kniha elektronického obchodu definuje tento pojem jako obchod, při němž komunikace mezi jeho účastníky probíhá z části nebo zcela po standardních datových sítích, prostřednictvím počítačů, jejich příslušenství a telekomunikačních zařízeních. Zahrnuje jak výrobky, které jsou prodávány, příp. i placeny přes datové sítě,

ale doručovány v hmotné podobně, tak i produkty, které jsou přes datové sítě doručovány v digitální, tedy nemateriální podobě, jako například software. (22, 42)

2.3.1. Historie elektronického obchodu

První nákupy na Internetu se uskutečnily v USA již v roce 1992. První prodejní komoditou se staly hudební nahrávky na CD, následovaly dárkové předměty a knížky. Teprve poté přišla na řadu elektronika, hračky a například nábytek. Internetové nakupování v České republice má dnes již více než desetiletou historii, ale jeho vývoj je hodně odlišný. Elektronické obchody se totiž ubíraly různými směry nejen v Česku a v Americe, ale i jinde v Evropě.

V Evropě se projevovala nedůvěra zákazníků v on-line platby, ve Spojených Státech se internetový business rozvíjel právě díky jejich oblibě. Jedno měl vývoj v obou částech světa společné. Jak v Evropě tak i v USA se začaly na internetu prosazovat velké obchodní řetězce s vlastními internetovými obchody. Většinou se setkáváme s tím, že cena výrobků je levnější na internetu něž v kamenných prodejnách.

Internet přinesl do světa nákupů zásadní průlom. Fantazie se změnila ve skutečnost ještě ve dvacátém století. Z pohodlí domova či kanceláře se ve Spojených Státech začalo nakupovat již v roce 1992. S boomem protokolu http a www začaly v letech 1994 a 1995 vznikat elektronické obchody dnešního typu.

Česká republika má navíc svůj vlastní fenomén – dobírku. Ještě dnes platí zákazníci za více než 60 % objednaného zboží hotově při jeho předání. V USA naopak dobírku v českém provedení neznají vůbec. Jedním z důvodů stálosti dobírky je především nedůvěra a historicky špatná zkušenost českých zákazníků s nákupem.

Češi teprve na začátku třetího tisíciletí začínají vnímat nákup přes internet jako relativně bezpečný. Důvodem je především mnohem více profesionální přístup některých on-line prodejců. Obecně se začíná zkracovat doba dodání zboží zákazníkům a silnější elektronické obchody začínají fungovat na smluvní bázi nad velkoobchody. (31)

2.3.2. Základní dělení elektronického obchodu

E-obchody se dělí do kategorií, a to podle subjektů, které mezi sebou uzavírají smluvní vztah, dále podle otevřenosti použitého média a nakonec podle způsobu plnění.

Dělení podle účastníků e-obchodování

B2B – Business to Business (obchodník→obchodník)

Koncept B2B je nejstarší složkou elektronického obchodování. Tento koncept se týká obchodních vztahů a vzájemné komunikace mezi dvěma společnostmi (obchodníky) navzájem. Český obchodní zákoník ve svém platném znění definuje v § 2 podnikání jako soustavnou činnost, prováděnou samostatně podnikatelem vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku. (20)

Podnikatelem podle tohoto zákona je:

- osoba zapsaná v obchodním rejstříku,
- osoba, která podniká na základě živnostenského oprávnění,
- osoba, která podniká na základě jiného než živnostenského oprávnění podle zvláštních předpisů,
- osoba, která provozuje zemědělskou výrobu a je zapsána do evidence podle zvláštních předpisů.

Tyto vztahy většinou fungují na principu výměny dat. Těmito mohou být základní informace (např. objednávky, faktury), jejichž elektronická podoba umožňuje snížit náklady, automatizovat celý proces a zvýšit jeho rychlost. Vyšším stupněm B2B obchodování jsou různá B2B elektronická tržiště, jejichž hlavním úkolem je zprostředkování obchodů. Nejsložitější B2B systémy potom fungují jako komunikační a distribuční sítě, sloužící především k regulaci již navázaných obchodních vztahů. Nemusí jít vždy nutně o transakce závislé na internetu, neboť řada podniků vytváří vlastní specializované sítě pro omezený okruh obchodních partnerů. (20)

B2C – Business to Cutomer (obchodník →zákazník)

Je to patrně nejrozšířenější model internetového podnikání. Segment B2C zahrnuje především přímý prodej koncovým spotřebitelům či alespoň jeho podporu. (20)

Obvykle se rozlišují tři úrovně tohoto modelu. Základem služeb B2C je snaha informovat o produktech, webová stránka zde vlastně plní funkci jakéhosi letáku či elektronického katalogu. Vyšší úroveň B2C služeb přidává interaktivní formuláře, kde

je například možnost zpětné vazby. Nejvyšší úrovní B2C je potom samozřejmě samotný internetový obchod, nejlépe s možností rovnou zaplatit objednané zboží online. (20)

C2C - Customer to Customer (zákazník→zákazník)

Jedná se o typ e-obchodů, kdy mezi sebou komunikují dva zákazníci bez přímé účasti obchodníka. Nejčastěji se jedná o prodej nebo nákup použitého zboží. K provozování těchto operací většinou slouží e-inzeráty, e-bazary, e-aukce apod. Mezi světově nejrozšířenějším zástupce tohoto modelu je internetový aukční portál eBay. (20)

C2B – Customer to Business (zákazník →obchodník)

Jde zatím o nejméně rozšířený typ e-obchodů. Jedná se o obchody, kdy zákazník oslovuje podnikatele, např. kdy definuje zboží maximální cenu a využívá obchodníky k podání nabídek na uzavření smlouvy. Nejčastěji se tento typ uplatňuje u on-line nákupů letenek a ubytování. (20)

B2G – Business to Government (obchodník→správa)

Vedle klasických obchodních vztahů se do e-obchodu zahrnují i vztahy ke státní správě. Do segmentu B2G tedy patří nabídka produktů institucím státní správy a také veškerá komunikace s těmito zařízeními. Typickým již fungujícím příkladem konceptu B2G může být stále se rozšiřující možnost podávat daňová přiznání s využitím elektronického podpisu. (20)

G2B – Government to Business (správa→obchodník)

Týká se obchodních vztahů a komunikace mezi správou a obchodníkem. Spadá sem např. zadávání veřejných zakázek, podávání informací o grantech, dotacích apod. (20)

Dělení podle otevřenosti použitého média

Podle otevřenosti použitého média dělíme transakce, které se mezi subjekty uskutečňují na uzavřené a otevřené.

Uzavřené transakce

Jde o transakce, které probíhají po uzavřených sítích mezi omezeným okruhem partnerů. Prostředí, ve kterém se tyto transakce uskutečňují, jsou dostupné jen vybraným a přesně specifikovaným subjektům. Jde například o firemní, klubové nebo univerzitní sítě. (17)

Otevřené transakce

Tyto transakce probíhají mezi otevřeným počtem účastníků v prostředí rozsáhlé a obecně dostupné počítačové sítě. V dnešní době se bude jedna především o transakce přes Internet. (17)

Dělení podle způsobu plnění

Přímé e-obchody

Tyto obchody jsou plně on-line. Objednávka, placení a zároveň dodávka nehmotných statků se uskutečňuje výhradně prostřednictvím elektronických prostředků v reálném čase. Nehmotnými statky se zde myslí např. software, informace a mediální produkty. (17)

Nepřímé obchody

Zde on-line probíhá pouze objednávka či uzavření smlouvy, nejvýše ještě platba, ale plnění smlouvy ze strany prodávajícího, tj. dodávka zboží, probíhá tradičními prostředky. (17)

2.3.3. Výhody a nevýhody elektronického obchodování

Nakupování na internetu nabízí svá pozitiva, ale i negativa, jak z pohledu firmy, tak z pohledu zákazníka. Stojíme-li před rozhodnutím, zda-li si pořídit internetový obchod, je dobré si uvědomit, co můžeme ztratit a co naopak získat. Stejně jako u každého podnikatelského záměru můžeme ztratit peníze nebo čas. (25)

Výhody z pohledu prodávajícího

- komunikace se zákazníkem přes Internet výrazně snižuje náklady transakce (odpadá práce prodavačů, nutnost stavět kamenné obchody)

- zpětná vazba od zákazníka, který vyplní formulář, případně zašle e-mailovou zprávu nebo se spojí s obchodem telefonicky (zvláště v případě zelených linek),
- podrobné informace o návštěvách obchodu (v závislosti na nich lze obchod přizpůsobit),
- šance pro menší firmy, které nemají dostatek prostředků na vybudování sítě klasických obchodů.

Nevýhody z pohledu prodávajícího

- vzhledem k obrovskému rozsahu a dosahu Internetu může ztráta pověsti dosáhnout velkých rozměrů, avšak úspěšný obchod tuto hrozbu promění v příležitost,
- připojením podniku na Internet se zvyšují šance na získání přístupu do podnikových sítí neoprávněné osobě, může dojít k narušení nebo ke zneužití interních podnikových dat. (25, 41)

Výhody z pohledu kupujícího

- zákazník nakupuje zboří často přímo od výrobce, a tím pádem za nižší cenu (odpadá nutnost platit zprostředkovateli poplatky všem článkům v distribučním řetězci),
- zpřístupnění neustále aktualizovaných informací (oproti klasickým reklamním letákům, kde informace velice rychle zastarávají),
- velké množství informací na jednom místě,
- obchod je otevřen 24 hodin denně, 365 dní v roce,
- možnost přístupu z libovolného místa, např. z domova, což může ušetřit spoustu stráveného času ve frontách, cestováním apod..

Nevýhody z pohledu kupujícího

- veškerá marketingová činnost zákazníka je podrobně monitorována za účelem následného použití v marketingu, což někteří zákazníci považují za nežádoucí narušení soukromí,

- existuje možnost vystupovat pod jménem někoho jiného a uskutečnit za něj finanční transakce, případně objednat nežádoucí zboží,
- údaje posílané po síti může někdo odposlouchávat a následně zneužít,
- zákazníci se v záplavě informací nedokáží dostatečně zorientovat a nenaleznout zboží, které hledají, případně na vyhledávání určitého zboží musí vynaložit neadekvátní úsilí,
- neexistuje jednoduchý způsob zabezpečení plateb,
- neosobnost nákupu, to se týká především starších lidí, pro něž je nakupování jedna z mála příležitostí sociálního kontaktu. (1, 38)

2.3.4. Obchod a elektronické obchodování

Nová ekonomika je založena především na informacích a znalostech. Na svět klasické staré ekonomiky působí nová ekonomika razantně. To je dáno především rychlostí, množstvím a dostupností informací, které dělají z celého světa jednotný globální trh. Konkurence je v dnešní době téměř pro každou firmu globální. Tento trend se bude nadále neodvratitelně stupňovat.

„Klasická ekonomika“ je spojena s možností relativně snadného předvídání vývoje, s určitou stabilitou práce a podnikání. Klíčem k úspěchu je dnes schopnost inovovat a neustále zdokonalovat, pružně podnikat a vzdělávat. Nová ekonomika implikuje restrukturalizační procesy dodavatelského řetězce, řízení vztahů se zákazníky a systémy údržby a podpory pro zákazníka. Vznikají nové typy společností se značným podílem elektronického obchodu. Vzniká prostor pro nové produkty a služby nabízené prostřednictvím Webu. Komerční transakce prováděné přes Web vytlačují tradiční obchodní kanály staré ekonomiky. (4)

2.4. Elektronické bankovnictví

Jednotlivé banky se v posledních letech odvrací od známého konzervatismu a ve stále větší míře se soustředí na nové typy komunikace s klientem. Období dominance vkladních knížek a nekonečných front před přepážkami se tak stává minulostí a jejich místo nahrazuje elektronické (neboli přímé) bankovnictví. (14)

„Přímé bankovnictví znamená, že klient může být díky elektronickým prostředkům se svými penězi v kontaktu 24 hodin denně, 365 dnů v roce, ať je

v zaměstnání, doma nebo uprostřed oceánu. Zkrátka odkudkoliv a kdykoliv. Je to možné díky moderním technologiím.“ (14)

Většina pozornosti jednotlivých bankovních ústavů se v posledních letech soustředí právě na vývoj a propagaci přímého bankovnictví, a to zejména na úkor svých poboček. V přímé komunikaci s klientem vidí většina institucí správnou cestu, jak snížit vlastní náklady a zároveň poskytnout svým zákazníkům nejen rychlejší, ale i pohodlnější přístup k jejich finančním prostředkům. Pobočková síť se však svého zániku bát nemusí. Elektronické bankovnictví přebírá pouze tzv. servisní činnost, zabývající se obsluhou účtu spojenou s nákupem produktů a služeb. (26)

Využitelnost novodobých technologických vymožeností, jako je internet či mobilní telefon, neunikla pozornosti ani manažerům jednotlivých bank. Po letech následného vývoje a testování služeb mohou klienti většiny tuzemských bank spravovat své peníze z pohodlí domova. Nabídka produktů přímého bankovnictví je v České republice považována za bohatou, takže každý z klientů může najít vhodnou kombinaci služeb, jakoby právě jemu ušitých na míru. Pokrok však jde stále kupředu a banky se snaží své produkty vylepšovat a vycházet tak vstříc požadavkům zákazníků. (26)

Klasická forma bankovnictví i přes finanční nevýhodnost však přežívá. Stále se zmenšující skupina konzervativních klientů tuto možnost správy peněz preferuje a jistě ještě nějakou dobu preferovat bude. Pobočka se však stává hlavně místem pro vyřízení složitých operací, které vyžadují poradenství a které klienti nechtějí vyřizovat po internetu ani po telefonu. Osobní kontakt s bankou je i v dnešní době vysoce ceněn a dodává majiteli účtu větší pocit bezpečí. (26)

2.4.1. Historický vývoj elektronického bankovnictví

V 70. letech 20. Století docházelo ke znatelnému poklesu cen počítačové techniky, což byl prvotní impuls pro masivní rozvoj počítačových technologií. První banky nabídly svým klientům nejprve nepřetržitý přístup k jejich finančním prostředkům prostřednictvím bankomatů. Nové zkušeností začaly ukazovat, že část

klientů upřednostňuje neustálý přístup k účtu přes moderní komunikační kanály před osobním kontaktem na pobočce banky. (14)

Historicky prvním skutečně přímým komunikačním kanálem (nepočítaje platební karty a bankomaty) je tzv. *phone banking*. Telefonní bankovnictví vzniklo v 80. letech minulého století v USA a Velké Británii, ke zlomu však došlo až 1. října 1989, a to vstupem First Direct Bank, instituce orientující se na přímé bankovnictví, na finanční trh. Charakter služby doznal během její existence mnoha změn, ta nejzásadnější přichází s nástupem digitálních mobilních sítí. (14)

Phone banking byl a stále je pro firemní klientelu vzhledem k objemu prováděných transakcí nepoužitelný. Peněžní instituce tak těmto významným zákazníkům nabídly novou možnost komunikace, označovanou souhrnně jako *homebanking*. Nástup nových generací stolních počítačů a Internetu vedl ke vzniku nové, nejmladší formy elektronického bankovnictví, tzv. *internet banking*. Správa účtu běžných klientů tak získala na pohodlí a jediná nevýhoda v podobě špatné dostupnosti celosvětové počítačové sítě se v posledních letech díky nezastavitelnému technickému rozvoji téměř vytratila. (14)

2.4.2. Základní formy elektronického bankovnictví

GSM Banking

GSM Banking umožňuje ovládat bankovní účet prostřednictvím mobilního telefonu. Obliba této formy přímého bankovnictví je založena na její mobilitě, klient může ovládat svůj účet ze všech míst, na kterých má potřebný signál. (33)

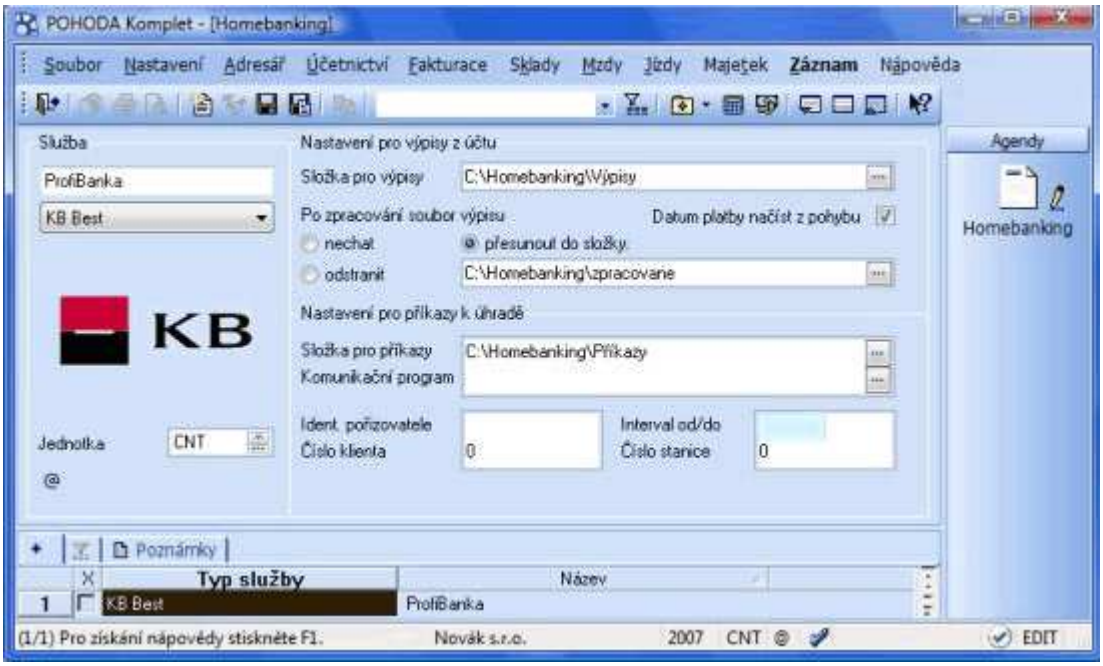
Bezpečnost komunikačního kanálu je díky svému šifrování obecně považována za minimálně dostačující. GSM Banking je již v dnešní době zpravidla založen na SMS zprávách sestavovaných mobilním telefonem v aplikace SIM Toolkit. Spektrum podporovaných služeb se u jednotlivých bank výrazně liší, některé z nich nabízí pouze pasivní operace s účtem (zůstatek na účtu, informace o pohybech na účtu, úrokové sazby apod.), jiné umožňují i aktivní ovládání peněžních prostředků (povolení SIPO, jednorázový či trvalý platební příkaz apod.). (33)

Obrázek 4: GSM Banking: Jednorázový platební příkaz
Zdroj: (43)

Home banking

Home Banking se od klasického internetového bankovnictví odlišuje nutností instalace speciálního softwaru na přístupovém počítači, který přes internet komunikuje s bankovním systémem. (32)

Poptávka ze strany firemních klientů dala základy právě Home bankingu, formě elektronického bankovnictví, která umožňuje zpracování většího objemu bezhotovostních plateb či nabízí přehled o aktuálním stavu účtu. Aplikaci je možné propojit s účetním systémem firmy, což umožňuje nejen generování platebních příkazů, ale i zpětné načítání výpisů do ekonomického softwaru klienta. (32)



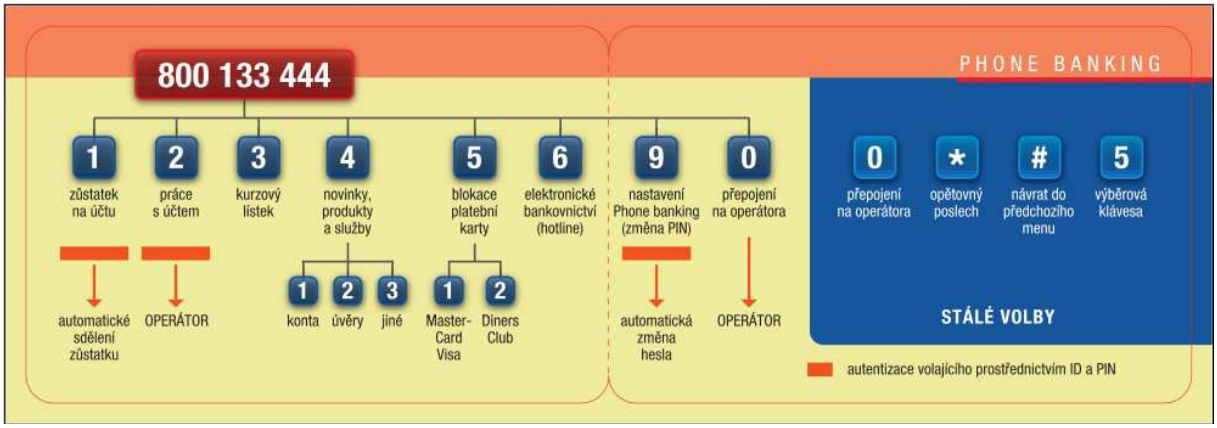
Obrázek 5: Home banking
Zdroj: (39)

Vysoké náklady a vazba na počítače s nainstalovaným bankovním programem zabraňují masového využívání tohoto typu bankovnictví. Z jeho existence tak těží firemní klientela, komunikující s bankou prostřednictvím modemu a telefonu nebo internetu.

Phone banking

Telefonní bankovnictví slouží ke správě účtu prostřednictvím mobilního telefonu, ale i běžného telefonu vybaveného zvukovou tónovou volbou. Phone banking je založen na telefonickém kontaktu buď s automatem, nebo telefonním bankéřem. Zatímco v prvním případě dostává klient instrukce, které potvrzuje prostřednictvím klávesnice telefonu (princip je shodný s infolinkou mobilního operátora), v tom druhém majitel účtu zadává příkazy hlasem. (5)

Bezpečnost je založena na identifikaci klienta PIN kódem nebo heslem, který si zákazník zvolí zpravidla sám. Některé z bank nabízí v oblasti zabezpečení nadstandardní služby založené např. na autentizačním kalkulátoru, příp. jednorázových transakčních heslech TAN. (5)



Obrázek 6: Phone banking: Nabídka hlasového stromu
Zdroj: (44)

Internet banking

Přístup k bankovnímu účtu prostřednictvím Internetu se po jeho rychlém rozvoji doslova nabízel. Po několikaletém vývoji a testování této formy přímého bankovnictví byl spuštěn jeho komerční provoz. Internetové bankovnictví, které je chápáno jako nejlevnější alternativa správy bankovního účtu, získalo během své existence nemalé množství věrných klientů. (37)

Uživatel pocítí pohodlí internetového bankovnictví hned při prvním přístupu ke svému účtu. Stolní počítač či notebook stačí pouze vybavit podporovaným internetovým prohlížečem (Internet Explorer, Mozilla Firefox atd.), tudíž se v tomto případě zákazník obejde bez instalace jakéhokoli bankovního programu. Na speciální webovou stránku se tak majitel účtu může přihlásit z jakéhokoli počítače na světě, a to v běžném internetovém rozhraní. Jednotlivé ústavy se staví k otázce bezpečnosti rozdílným způsobem, např. KB používá pro tento účel certifikát, eBanka používá autentizační kalkulátor. Samotný datový přenos je stejně jako v předchozím případě vždy kódovaný. (37)

Obrázek 7: Internet banking KB
Zdroj: (35)

Transakce prováděné prostřednictvím internetového bankovnictvím jsou ve srovnání s telefonním o poznání levnější, o poplatcích u přepážek ani nemluvě. Finanční politika peněžních ústavů zpravidla preferuje přímé bankovnictví a snaží se své klienty motivovat k používání těchto komunikačních kanálů. Rozdílná výše poplatků účtovaných za stejné úkony na bankovní přepážce a pomocí internetového bankovnictví mluví sama za sebe. (10)

2.4.3. Metody zabezpečení elektronického bankovnictví

„Bezpečnost by měla mít u bank maximální prioritu a měla by být naprostou samozřejmostí. Nejde přeci o nic menšího než o reálné peníze. Bohužel i banky mají jistý podíl na tom, že uživatelé jejich služeb volí méně bezpečné metody ochrany. Ty lepší a účinnější jsou mnohdy zpoplatněny zvláštními poplatky, které mnoho zákazníků odradí.“ (29)

Internet se od svého zrození potýká s problémy napadnutelnosti a zneužitelnosti. Tato skutečnost ovlivnila také začátky internetového bankovnictví. Nedůvěra v bezpečnost nového komunikačního kanálu nebyla kompenzována ani nižšími poplatky,

větší rychlostí či komfortem, takže lidé stále plnili bankovní přepážky a stáli si tradiční dlouhé fronty. Současná vysoká míra zabezpečení internet bankingu je tak výsledkem mnohaleté práce a nemalých investic. (40)

Základem manipulace s účtem přes internet je dodržování bezpečnostních zásad zpracovaných bankou. Nezbytnou součástí počítače pro využití služeb internetového bankovnictví je internetový prohlížeč. Potenciální nebezpečí se skrývá i v tomto typu softwaru, nejúčinnější ochrana před zneužitím třetí stranou spočívá v pravidelné aktualizaci nejen prohlížeče, ale i celého operačního systému. (40)

Prostřednictvím plně aktualizovaného počítače si klient otevře speciální webovou stránku určenou pro vstup do aplikace internetového bankovnictví. Správa finančních prostředků je možná ihned po přihlášení, tedy po dalším z bezpečnostních opatření. Identifikace klienta je založena na ověření přihlašovacích údajů, jejichž správnost posuzuje systém instituce. Jednotlivé banky většinou upřednostňují některé z následujících typů autorizací:

- **Uživatelské jméno a heslo** – Tyto údaje představují základní a nejpoužívanější metodu přístupu k bankovnímu účtu. Za pojmem Přihlašovací jméno se zpravidla skrývá klientské (příp. identifikační) číslo. Bezpečnost přihlášeni však stojí a padá kvalitou hesla, které je buď nově vygenerováno čistě za účelem využití internetového bankovnictví, nebo shodné s přiděleným PIN kódem.
- **Uživatelské jméno a heslo a potvrzovací kód z autentizačního kalkulátoru** – Použití autentizačního kalkulátoru[1] poskytuje zákazníkovi vyšší úroveň bezpečnosti. Výhodou tohoto zařízení je nezávislost na distribučním kanálu a na jakémkoliv dalším zařízení. Používá se na místech, která neumožňují implementaci žádné jiné bezpečnostní technologie. V případě internetového bankovnictví může klient bez rizika využívat jakýkoli počítač, a to i v tolik obávaných internetových kavárnách.

[1] Univerzální řešení v oblasti autentizace uživatelů a ochrany přenášených dat představují autentizační kalkulátory, známé též pod názvy PIN kalkulátor, elektronický klíč či generátor jednorázových hesel. Jedná se o zařízení, která umožňují ověření klienta a přenášené zprávy a splňují i nejvyšší nároky na bezpečnost. (21)

Obrázek 8: Autentizační kalkulátory
Zdroj: (21)

Banka při komunikaci s klientem musí mít jistotu, že do posílaných informací nikdo nenahlíží a nedegeneruje je. Pro zajištění důvěryhodnosti používá instituce proces šifrování, který je založen na vygenerování kombinačního klíče, s jehož pomocí se z čitelné zprávy stává během přenosu posloupnost znaků neobsahující žádnou logickou souvislost. (21)

2.4.4. Smartbanking

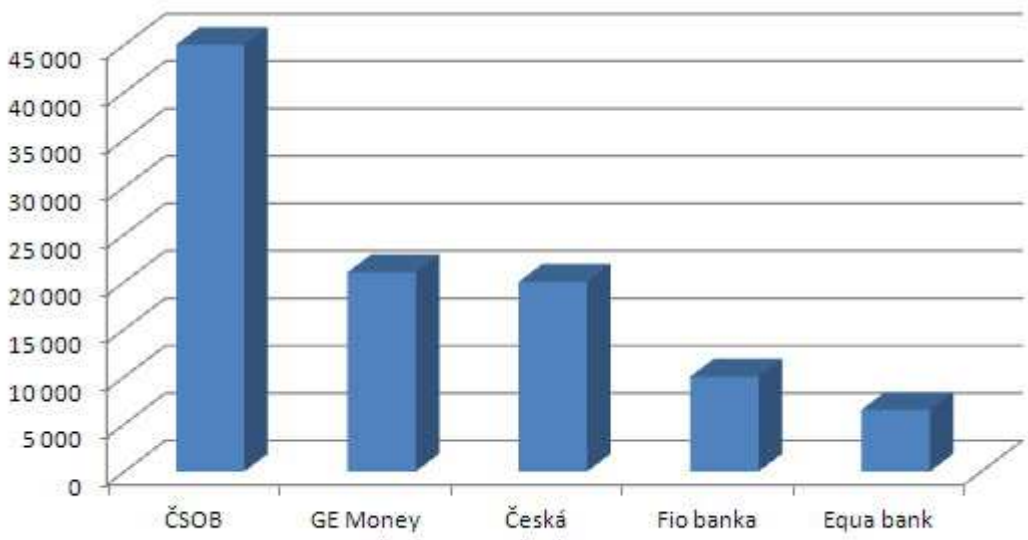
Trendy v posledních letech jsou jednoznačné, stále více telefonů, které se prodají má operační systém (nejčastěji Android, iOS či některý další) a disponují přístupem na internet, což je služba, která se vzhledem ke snižujícím se cenám za připojení a zvyšujícím se požadavkům na přístup k informacím kdykoli a odkudkoli těší poměrně velké oblibě.

Uživatelé vyžadují, aby mohli ke svým účtům přistupovat z mobilních zařízení. V zásadě nemusí jít jen o obyčejné získávání informací o aktuálním stavu peněz na účtu, ale také o realizaci plateb, změnu limitů nebo celkovou komunikaci s bankou. Samozřejmě by neměl chybět přístup k aktivaci služeb jako je pojištění, blokace karty či žádosti o zřízení nové karty. (34)

Smartbanking by mohl také nabídnout velice pěknou podporu pro různé účetní aplikace, takže byste mohli jedním či dvěma kliknutími dostat data z jedné aplikace (smartbankingové) do druhé (nástroje na správu osobních financí). (34)

Dobře pojatý smartbanking není jen o pohodlném a rychlém přístupu k informacím, ale také představuje velice důležitý pilíř bezpečnostní, například onou možností pružně měnit limity pro výběr či platbu kartou, realizovat pokročilé autorizace plateb nebo rychle zablokovat zcizenou kartu. (34)

Velice zajímavou kategorií služeb jsou pak ty, které s bankovnictvím přímo nesouvisí, ale uživateli mohou přijít vhod jako dobrý zdroj informací – může jít o spojení s GPS a poskytnutí informací o nejbližším bankomatu, pobočce nebo informaci, že je třeba do banky donést potvrzení o studiu. Zajímavé možnosti se nabízejí také v kombinaci s kartami, které nabízejí různé slevy a benefity. Aplikace by mohla klienta informovat o tom, kde se podobný „výhodný“ obchod nachází v jeho nejbližším okolí. (34)



Obrázek 9: Počet klientů smartbankingu podle bank k dubnu 2013
Zdroj: (23)

Bezpečnost smartbankingu

Metod zabezpečení aplikace pro mobilní bankovnictví je nepřeberné množství. Ne každá je použitelná a ne každou jsou uživatelé ochotni přijmout. Při obsluze bankovních účtů skrze mobilní telefon, může být aplikace zabezpečena několika různými stupni bezpečnosti. Vývojáři však musí brát zřetel na nepřímo-úměrnost dvou veličin. Bezpečnosti a použitelnosti. Čím více je aplikace zabezpečená, tím méně je zpravidla pro uživatele použitelná a příjemná. (23)

První stupeň bezpečnosti

Jedná se pouze o tzv. jednofaktorou autentizaci uživatele. V praxi to znamená, že pro přihlášení do aplikace a provádění transakcí, je zapotřebí pouze jednoho bezpečnostního prvku a to zpravidla hesla nebo PINu. PIN je čtyřmístné identifikační číslo. To znamená, že existuje 10 000 kombinací tohoto čísla. Pro dnešní, běžně výkonný hardware, není problém pomocí speciálního softwaru tuto kombinaci zjistit během poměrně krátkého časového okamžiku.. Bezpečnost PINu je dána omezeným počtem pokusů. Po třetím chybném zadání se účet zablokuje. (23)

Druhý stupeň bezpečnosti

Někdy také nazýván „zlatá střední cesta“. Tento stupeň bezpečnosti kombinuje prvky autentizace „něco, co znám“ a „něco, co mám“. Zpravidla se jedná o kombinaci hesla nebo PINu a autentizačního kalkulátoru, certifikátu nebo mobilního telefonu. Jedná se o nejčastěji používaný typ zabezpečení. (23)

Třetí stupeň bezpečnosti

Nejvyšší, ale ne běžně použitelný stupeň bezpečnosti. K výše zmíněným prvkům se přidá „něco, co jsem“. Může se jednat o otisk prstu, sken sítnice nebo např. porovnání hlasu. U mobilních aplikací je ale tato metoda autentizace uživatele nemyslitelná. (23)

Další metody zabezpečení

Mezi jiné nejpoužívanější, ale zároveň velmi omezující metody zabezpečení, patří tzv. White-list, což je seznam předem definovaných účtů, na které lze peněžní prostředky převést. (23)

2.5. Použité metody analýzy

2.5.1. SWOT analýza

Jedním ze nejčastěji používaných nástrojů analýzy je SWOT analýza. Tato metoda se nejčastěji používá při hodnocení podniku, avšak lze použít i na jiné objekty. Faktory, které působí na podnik, rozděluje jako interní (silné a slabé stránky) a externí (příležitosti a hrozby). Je důležité identifikovat hlavní faktory a rozdělit je do těchto čtyř skupin. Vzájemnou interakcí silných a slabých stránek, příležitostí a hrozeb se specifikují strategie, které by podniku měly zajistit prosperitu.

2.5.2. Porterův model 5 konkurenčních sil

Model konkurenčních sil na trhu popsal Michael E. Porter na univerzitě Harward School of Business Administratic. Vytvořil síť, pomáhající manažerům analyzovat konkurenční síly v okolí firmy a odhalit příležitosti a hrozby podniku. Model definuje a popisuje podstatu konkurenčního prostředí uvnitř každého jednotlivého odvětví a tak vytváří informační model pro rozhodování o tvorbě konkurenční výhody podniku. (20)

1. riziko vstupu potenciálních konkurentů – Zjišťuje, jak snadné nebo obtížné je pro nového konkurenta vstoupit na trh.
2. rivalita mezi stávajícími konkurenty – Hodnotí rivalitu mezi stávajícími konkurenty.
3. smluvní síla odběratelů – Určuje, jak silná je pozice odběratelů.
4. smluvní síla dodavatelů – Zjišťuje, jak silná je pozice dodavatelů.
5. hrozba substitučních výrobků – Hodnotí jak snadno mohou být produkty a služby nahrazeny jinými.

3. Analýza problému a současné situace

Tato kapitola má za úkol analyzovat a rozebrat segment Komerční banky zaměřen na přímé bankovnictví, tzn. obsluhování bankovních produktů elektronickými prostředky. Zaměřuje se převážně na internetové a mobilní bankovnictví.

3.1. Popis společnosti Komerční banka, a.s.

„Komerční banka, a.s., (dále také „KB“ nebo „Banka“) je mateřskou společností Skupiny KB (dále také „Skupina“) a je součástí mezinárodní skupiny Société Générale. Komerční banka patří mezi přední bankovní instituce v České republice a v regionu střední a východní Evropy. KB je univerzální bankou se širokou nabídkou služeb v oblasti retailového, podnikového a investičního bankovnictví. Společnosti Skupiny Komerční banky nabízejí další specializované služby, mezi které patří penzijní připojištění, stavební spoření, faktoring, spotřebitelské úvěry a pojištění, dostupné prostřednictvím sítě poboček KB, přímého bankovnictví a vlastní distribuční sítě. Prostřednictvím pobočky poskytuje KB své služby rovněž ve Slovenské republice.“ (27)

V letech 2004, 2005, 2007 a 2011 získala Komerční banka, a.s. prestižní ocenění **Banka roku.** Tato soutěž byla v letech 2002-2008 označována jako *MasterCard Banka roku*, od ročníku 2009 nese název *Fincentrum Banka roku*.

Historie společnosti

„Komerční banka byla založena v roce 1990 jako státní instituce a v roce 1992 byla transformována na akciovou společnost. Akcie KB jsou kótovány na Burze cenných papírů Praha i v RM-Systému již od jejich vzniku. Globální depozitní certifikáty (GDR) zastupující akcie KB se obchodují na Burze cenných papírů v Londýně (London Stock Exchange) od roku 1995. V roce 2001 koupila státní 60% podíl v Komerční bance Société Générale. Po této privatizaci začala KB kromě své tradičně silné pozice na trhu podniků a municipalit výrazně rozvíjet aktivity také pro individuální zákazníky a podnikatele. Součástí rozvoje retailových aktivit byl i nákup zbývajícího 60% podílu v Modré pyramidě v roce 2006, kterým Komerční banka získala plnou kontrolu nad třetí největší stavební spořitelnou v České republice. Dne 31. 12. 2010 nabyla účinnosti

přeshraniční fúze sloučením mezi Komerční bankou a Komerční bankou Bratislava s tím, že nástupnickou společností se stala Komerční banka, která pokračuje v aktivitách na Slovensku prostřednictvím pobočky.“ (27)

3.2. SWOT analýza

SWOT analýza zkoumá aktuální postavení firmy. Jedná se o analýzu vnějšího a vnitřního okolí. V této části jsou rozděleny jednotlivé faktory do skupin podle toho, zda vycházejí z vnitřního (přímo ovlivnitelného) nebo z vnějšího (nepřímo ovlivnitelného) prostředí firmy.

Tabulka 1: SWOT analýza

S	**S - Silné stránky (strengths)**	**W**	**W - Slabé stránky (weaknesses)**
S1	Jednoduchost používání	W1	Stoprocentní ověření uživatele není možné
S2	Žádné HW úpravy pro uživatele	W2	Nutnost pravidelné aktualizace
S3	Nevyžaduje instalace SW při každém přihlášení	W3	Počítačové viry
S4	Uživatel se může přihlásit odkudkoliv	W4	Nutnost zapamatování přístupového hesla
S5	Jednoduchost spravování	W5	Nutná IT gramotnost
S6	Pohodlné		
S7	Operativní		
S8	Snadno zapamatovatelné		
S9	Ušetření času pro uživatele		
S10	Zdarma		
O	**O - Příležitosti (opportunities)**	**T**	**T - Hrozby (threats)**
O1	Rychlejší chod aplikace	T1	Možnost okopírování
O2	Zamezení zablokování hesla	T2	Softwarové chyby
O3	Registrace překlepových domén bankou	T3	Zneužití různých chyb v aplikaci
		T4	Většina uživatelů používá pro přístup do různých systému stejná hesla
		T5	Prolomení hesla
		T6	Phishing
		T7	Typosquatting

Zdroj: vlastní

3.2.1. Popis jednotlivých faktorů SWOT analýzy

Silné stránky (strengths)

Mezi silné stránky elektronického bankovnictví patří hlavně jeho jednoduchost používání. Uživatel nepotřebuje žádné speciální softwarové instalace při každém přihlášení. Můžeme se připojit odkudkoli. Elektronické bankovnictví se velice jednoduše spravuje. Je to pohodlné a rychle, uživatel si zpracovává příkazy z pohodlí domova. Šetří to jeho čas a nemusí jít fyzicky do banky. Další výhodou je, že banka poskytuje tyto služby zdarma.

Slabé stránky (weaknesses)

Do slabých stránek můžeme započítat, že není vždy stoprocentně možné ověřit uživatele. Aplikaci musíme pravidelně aktualizovat. Můžou ji napadnout počítačové viry. Každý uživatel si musí pamatovat svoje přístupové heslo. A také je nutná IT gramotnost.

Příležitosti (opportunities)

Mezi příležitosti zařadíme zapracování na rychlejším chodu aplikace. Další důležitou příležitostí je registrace překlepových domén bankou, kdy banka eliminuje parazitování typosquattingu.

Hrozby (threats)

Velký problém přináší to, že si uživatel nemění hesla a používá jedno do různých systémů nebo je heslo příliš jednoduché, že dojde k jeho prolomení. Další, velmi významnou hrozbou, je phishing, jedná se o podvodnou techniku používanou na internetu k získávání citlivých údajů (hesla) v elektronické komunikaci. Typosquatting patří mezi neméně významné hrozby, je to forma cybersquattingu, která je postavena na překlepech při psaní internetové adresy. Na překlepové adrese na nás můžou čekat ohrožení v podobě virů apod. Dalšími hrozbami můžou být softwarové chyby, či dokonce okopírování celé aplikace.

3.2.2. Bilance SWOT analýzy

U Silných stránek a Příležitostí použijeme kladnou stupnici od 1 do 5 s tím, že 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost. U Slabých stránek a Hrozeb je použita záporná stupnice od -1 (nejnižší nespokojenost) do -5 (nejvyšší nespokojenost).

Tabulka 2: Bilance SWOT analýzy

S - Silné stránky (strengths)	**Váha**	**Hodnocení**	
Jednoduchost používání	0.1	4	0.4
Žádné HW úpravy pro uživatele	0.03	3	0.09
Nevyžaduje instalace SW při každém přihlášení	0.03	3	0.09
Uživatel se může přihlásit odkudkoliv	0.1	5	0.5
Jednoduchost spravování	0.07	3	0.21
Pohodlné	0.2	5	1
Operativní	0.1	4	0.4
Snadno zapamatovatelné	0.07	4	0.28
Ušetření času pro uživatele	0.2	5	1
Zdarma	0.1	4	0.4
Součet	1		**4.37**
W - Slabé stránky (weaknesses)			
Stoprocentní ověření uživatele není možné	0.2	-4	-0.8
Nutnost pravidelné aktualizace	0.1	-3	-0.3
Počítačové viry	0.1	-4	-0.4
Nutnost zapamatování přístupového hesla	0.3	-5	-1.5
Nutná IT gramotnost	0.3	-4	-1.2
Součet	1		**-4.2**
O - Příležitosti (opportunities)			
Rychlejší chod aplikace	0.3	3	0.9
Zamezení zablokování hesla	0.2	4	0.8
Registrace překlepových domén bankou	0.5	1	0.5
Součet	1		**2.2**
T - Hrozby (threats)			
Možnost okopírování	0.1	-4	-0.4
Softwarové chyby	0.1	-3	-0.3
Zneužití různých chyb v aplikaci	0.1	-3	-0.3
Opakující se hesla	0.1	-5	-0.5
Prolomení hesla	0.1	-4	-0.4
Phishing	0.2	-5	-1
Typosquatting	0.3	-5	-1.5
Součet	1		**-4.4**

Zdroj: vlastní

Tabulka 3: Výsledek bilance

Interní	0.17
Externí	-2.2
Celkem	2.37

Zdroj: vlastní

Bilance SWOT analýzy je 2.37 bodů. Při důkladné prohlídce je zřejmé, že nejvyššího zlepšení dosáhneme v interní části. Největší potenciál ke zlepšení celkové bilance SWOT analýzy představuje podchycení typosquattingu. Je nutné, aby si banka registrovala největší možný počet překlepových domén, případně usilovala o odkoupení již stávajících.

3.3. Porterův model 5 konkurenčních sil

Tento model patří k základním a zároveň nejvýznamnějším nástrojům pro analýzu konkurenčního prostředí firmy a jejího strategického řízení. Model se snaží odvodit sílu konkurence v analyzovaném odvětví a tím pádem také ziskovost daného sektoru trhu. K dosažení tohoto cíle rozebírá pět klíčových vlivů, které konkurenceschopnost firmy přímo či nepřímo ovlivňují.

3.3.1. Konkurenční rivalita

První Porterovou silou je konkurenční rivalita. Při analýze této síly je nutné sledovat konkurenční tlaky na daném trhu. V dnešní době je konkurenční boj opravdu silný. Je zde tlak na snižování cen na úkor kvality služeb. Komerční banka patří mezi silné články na trhu bankovnictví. Svým zákazníkům nabízí kvalitní služby. Mnohé ostatní, nové banky, tlačí cenu dolů na úkor pohodlí v kamenné pobočce. Nabízejí méně automatů. Mnoho věcí nelze zařídit z domova. Klientský servis, či online podpora není natolik pochycená.

3.3.2. Ohrožení ze strany nových potenciálních konkurentů

Další Porterovou silou je hrozba vstupu nových konkurentů na trh. Ta je obzvláště důležitá v nových, progresivně se rozvíjejících oborech, kde není zcela znám objem trhu jako celku anebo kde objem trhu rychle roste. Příkladem takového trhu může být trh elektronického bankovnictví.

Bariéry vstupu na trh nejsou příliš velké. Největší část zabírají náklady na neustálý vývoj, update aplikací. Další část jsou investice do důvěry zákazníků či počáteční pokrytí možných ztrát.

U Komerční banky nastává ohrožení přírůstkem nových konkurentů hlavně v podobě poplatků. Komerční banka má jedny z nejvyšších poplatků. Konkurence přitahuje potenciální zákazníky hlavně díky nižším cenám či službám zdarma. Na druhou stranu KB patří ke solventní bance s dlouhou historií a kvalitními službami. Většina stávajících zákazníků ji jen tak nevymění.

3.3.3. Náhradní (nové) produkty

Třetí silou z kategorie konkurenčního prostředí je hrozba vzniku substitutů. Substituty se v tomto případě myslí cokoliv, co nějakým způsobem nahradí zákazníkovi službu nebo produkt, který poskytuje.

Komerční banka často bojuje s přírůstkem nových konkurenčních produktů, substitutů, které poskytují jiné banky. Kupříkladu méně bezpečný, ale o to dostupnější produkty. Pokud bude zajímavější poměr cena-kvalita, substitut může částečně KB ohrozit. V dnešní době je spousta věcí otázka prestiže, takže většina stávajících zákazníků zůstane u osvědčené společnosti.

3.3.4. Odběratelé

Silou kupujících se myslí zejména jejich vyjednávací síla o ceně. Síla kupujících je od vzniku krize velice důležitým faktorem, který se nevyplatí podceňovat. Dnes už je totiž běžné, že zákazník zcela otevřeně a významně ovlivňuje cenu takových komodit jako je pojištění a bankovní služby.

Významný vliv mají v Komerční bance odběratelé více druhů produktů, existují zde možnosti výhodnější podmínek, propojené produkty, víceúčelové produkty apod. Pokud přijde 10 zákazníků se zájmem o hypotéku, tak se s cenou nestane vůbec nic. Pokud přijde zákazník, který má zájem o hypotéku, spořící účet a životní pojištění najednou, dostane výhodnější podmínky. Konkurence má v dnešní době významný vliv. Potenciální zákazník si v dnešní době může vybírat z mnoha nabídek produktů od různých bank.

3.3.5. Dodavatelé

Dodavatelé jsou silní, pokud je na trhu jen malé množství dodavatelů. Mohou si tak lépe manipulovat s cenou. Taktéž síla závisí na závislosti odběratelů a na poptávce.

3.3.6. Zhodnocení

Komerční banka je silná společnost s dlouhou historií. Hrozba konkurence v bankovním sektoru je vysoká. Avšak taková společnost, jako je KB, bude vždy přitahovat klientelu, která spoléhá na dlouhodobou historii, sílu a kvalitu. Vstup nových konkurentů do bankovního sektoru je nyní trend. K získání klientely používají, jako nástroj konkurenční rivality, nulové poplatky a výhodné produkty. Tento trend, ale není dlouhodobě udržitelný. S dobou rostou i nároky klientů. Na trh přichází stále nové produkty k uspokojení poptávky a potřeby zákazníků. Banka reaguje flexibilně a neustále sleduje potřeby klientů.

3.4. Průzkum trhu

Pro potřebu průzkumu využití mobilního bankovnictví Komerční banky byl oslovenému vzorku lidí z různých věkových a sociálních skupin, předložen jednoduchý dotazník (viz příloha č.), který si dává za úkol zjistit praktickou použitelnost smartbankingové aplikace Komerční banky Mobilní banka 2. Věkový průměr oslovených respondentů byl 31 let. Na dotazník celkově odpovědělo, během 4 měsíců, téměř 3000 lidí. Výběr dotázaných byl filtrován první otázkou, která není součástí dotazníku. Otázka zní: *Jste klientem Komerční banky?*

3.4.1. Distribuce dotazníků a sběr dat

Dotazníkové šetření bylo provedeno následujícími distribučními kanály:

a) internet (sociální sítě)
b) papírová forma
c) e-mailing

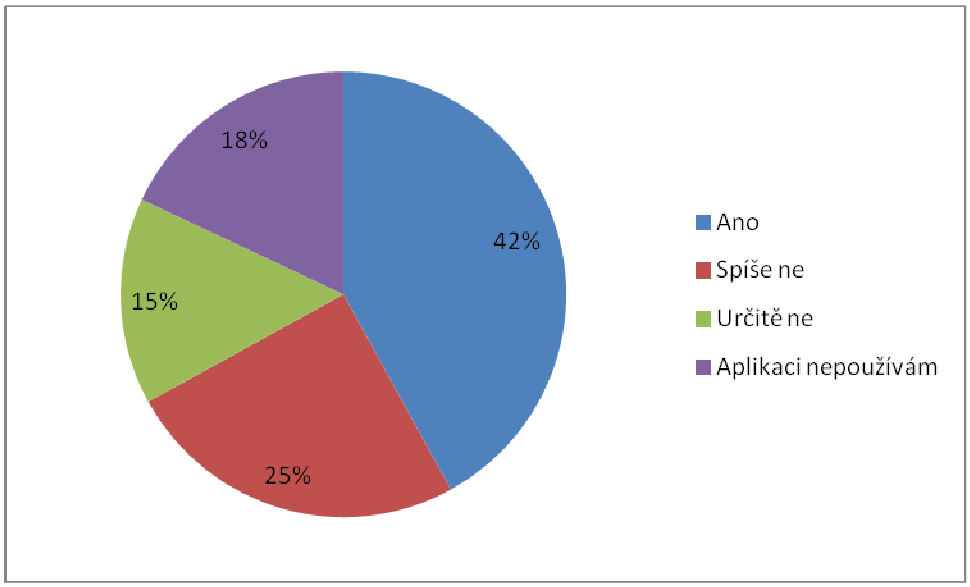
Nejmasovější distribuce proběhla pomocí internetu a to hlavně kvůli pohodlnosti a jednoduchosti sběru dat. Pokud by byl použit pouze tento kanál, byl by výsledek značně zkreslený, z důvodu nižšího věkového průměru dotázaných. Tato nepřesnost

byla částečně ošetřena distribucí dotazníků v tištěné formě se zaměřením na vyšší věkový průměr dotázaných.

3.4.2. Dotazníkový průzkum

Otázka č. 1 - Je pro vás aplikace užitečná?

Zatímco u dotazníků získaných pomocí internetu byl počet dotázaných, kteří aplikaci nepoužívají vůbec zanedbatelný, u respondentů vyššího věku, tj. 50 let a více, byl téměř každý desátý překvapen, že tato aplikace vůbec existuje. Z výzkumu vyplývá, že téměř polovina dotázaných aplikaci zná a používá. Čtvrtina dotázaných si aplikaci stáhla do svého zařízení, ale dále ji již nepoužívá.

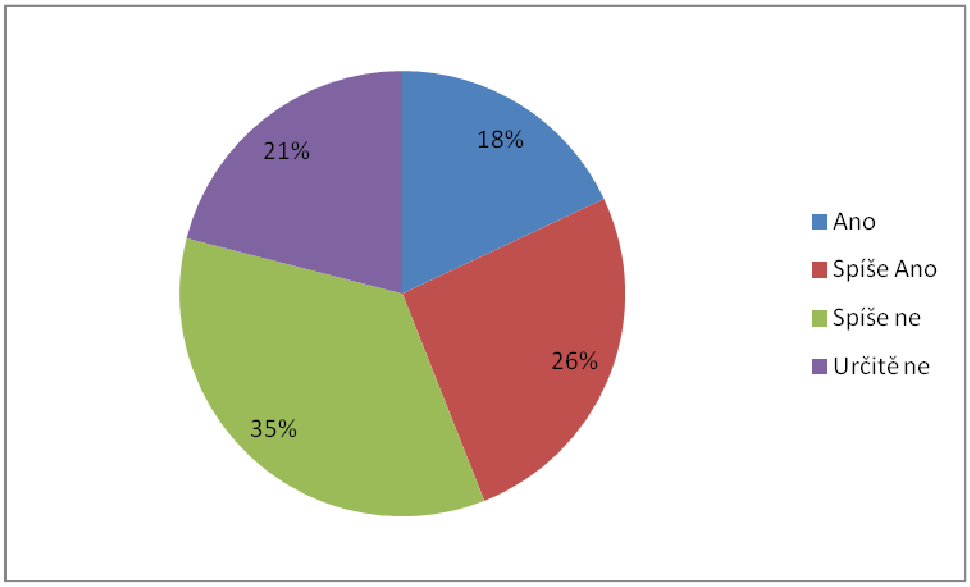


Graf 1: Poměr odpovědí na otázku č.1
Zdroj: vlastní

Otázka č. 2 - Myslíte si, že je aplikace dostatečně zabezpečena?

Otázka bezpečnosti je velice kontroverzní téma. Lehce zarážející je zjištění, že aplikaci nepoužívá ani polovina dotázaných, jejímu zabezpečení však nedůvěřuje více než 60 procent uživatelů. Tento paradox je pravděpodobně způsoben věkovým zkreslením, kdy lidé kolem 20 až 25 roku věku nedisponují vyššími disponibilními finančními prostředky a jsou ochotni podstoupit možné riziko ztráty, výměnou za mobilitu a časovou úsporu, kterou jim aplikace nabízí. Většina mladších uživatelů si ale plně uvědomuje, že riziko je tím nižší, čím zodpovědněji k ovládání aplikace přistupují.

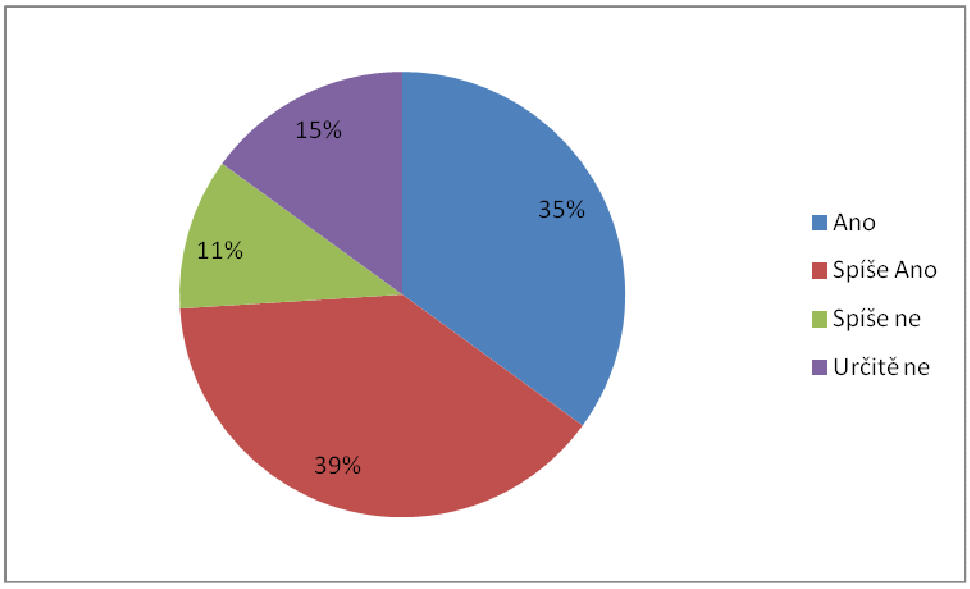
Naopak starší skupina obyvatelstva více důvěřuje sobě a svým dovednostem finanční prostředky přechovávat, než technickému zabezpečení, kterému nerozumí.



Graf 2: Poměr odpovědí na otázku č.2
Zdroj: vlastní

Otázka č. 3 – Provádíte platby s připojením přes domácí Wi-Fi?¨

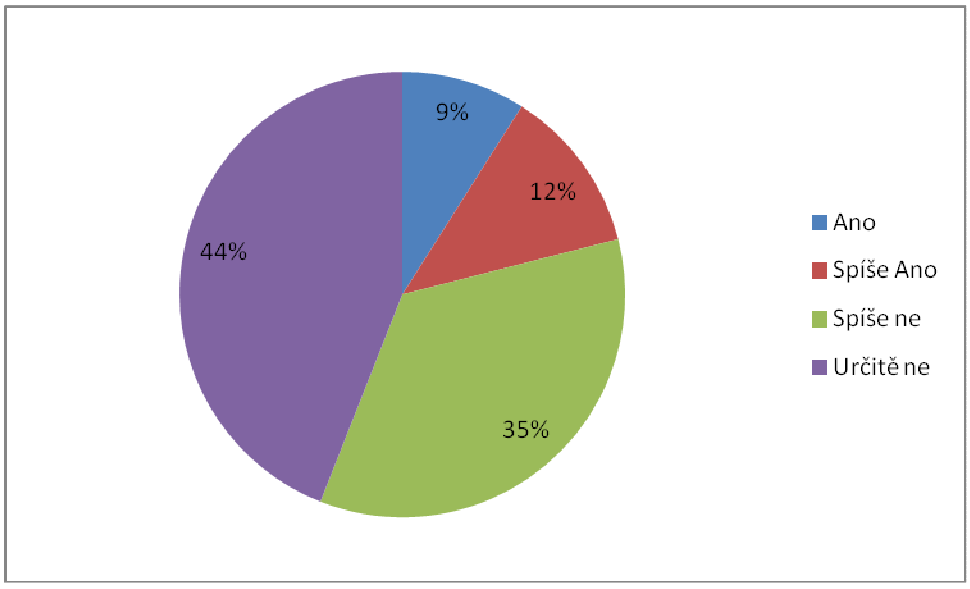
Ze tří možností připojení k internetu, pomocí kterého může uživatel online s aplikací pracovat, jednoznačně zvítězila domácí Wi-Fi síť. Pokud je domácí síť správně nastavena a dostatečně zabezpečena, jedná se skutečně o nejbezpečnější způsob připojení k serverům banky. Nevýhodou této metody je, že se uživatel nemůže vzdálit z dosahu signálu, a je tak omezen prostorem. V tomto případě je lepší, pokud to situace dovolí, použít raději aplikaci internetového bankovnictví MojeBanka.



Graf 3: Poměr odpovědí na otázku č.3
Zdroj: vlastní

Otázka č. 4 - Provádíte platby s připojením přes veřejnou Wi-Fi?

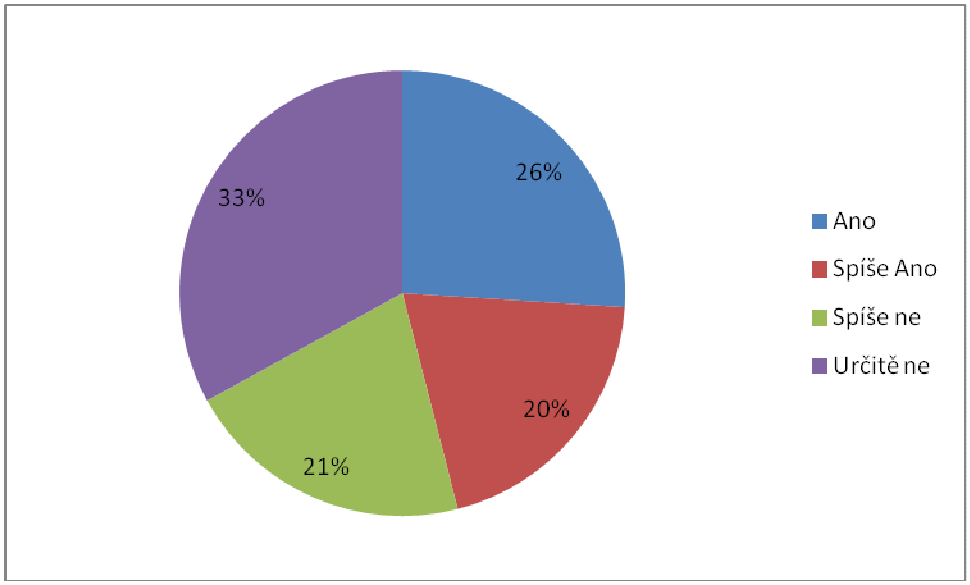
Jednoznačně nejnebezpečnější způsob práce online, při kterém existuje reálné riziko odposlouchání přenosu a získání citlivých údajů. Nejčastější chybou je zadávání přístupového kódu či hesla v přítomnosti cizí osoby a následná nepozornost, která může vést k odcizení zařízení a následného zneužití. Uživatelé jsou si tohoto rizika vědomi a jen malá část z nich používá aplikaci s připojením k veřejné Wi-Fi.



Graf 4: Poměr odpovědí na otázku č.4
Zdroj: vlastní

Otázka č. 5 - Provádíte platby s připojením přes mobilní data?

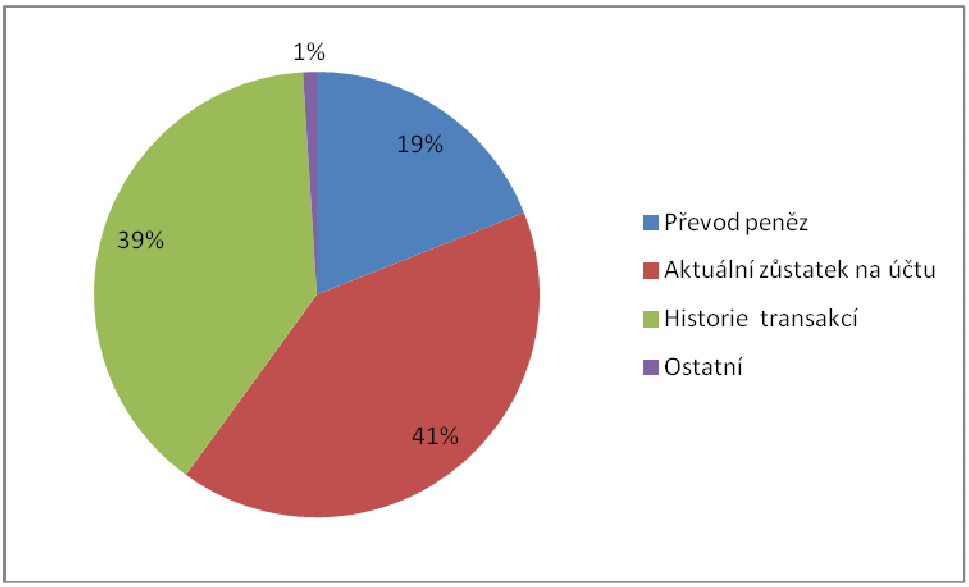
Kompromis mezi dvěma výše uvedenými způsoby připojení. Tato metoda je tak bezpečná, jak zodpovědný je přístup uživatele. Pro některé jedince může být stejně nebezpečná jako při připojení k nezabezpečené veřejné Wi-Fi. Pokud ale uživatel dodržuje zásady práce s aplikacemi mobilního bankovnictví (viz 4.6), je tato metoda velice účinná a to díky mobilitě, resp. rozsahu pokrytí mobilní datové sítě.



Graf 5: Poměr odpovědí na otázku č.5
Zdroj: vlastní

Otázka č. 6 - Jakou funkci Mobilní banky 2 používáte nejčastěji?

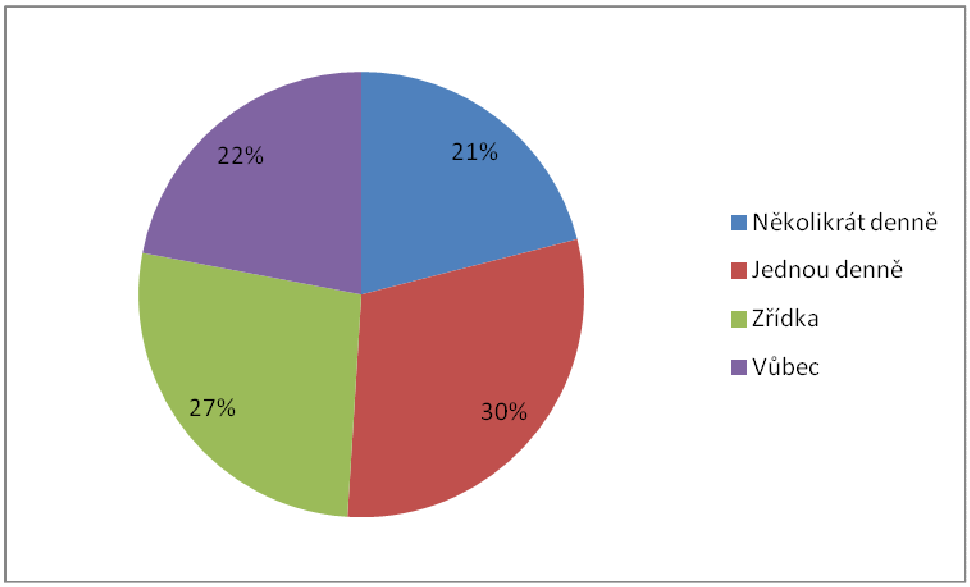
Z výzkumu vyplývá, že většina uživatelů svou mobilní aplikaci používá hlavně na zjištění aktuálního použitelného zůstatku na účtu a zobrazení historie transakcí. Pětina z nich pak využívá nejvíce převod finančních prostředků, což má pravděpodobně na svědomí malá důvěra k zabezpečení transakcí.



Graf 6: Poměr odpovědí na otázku č.6
Zdroj: vlastní

Otázka č. 7 – Jak často aplikaci používáte?

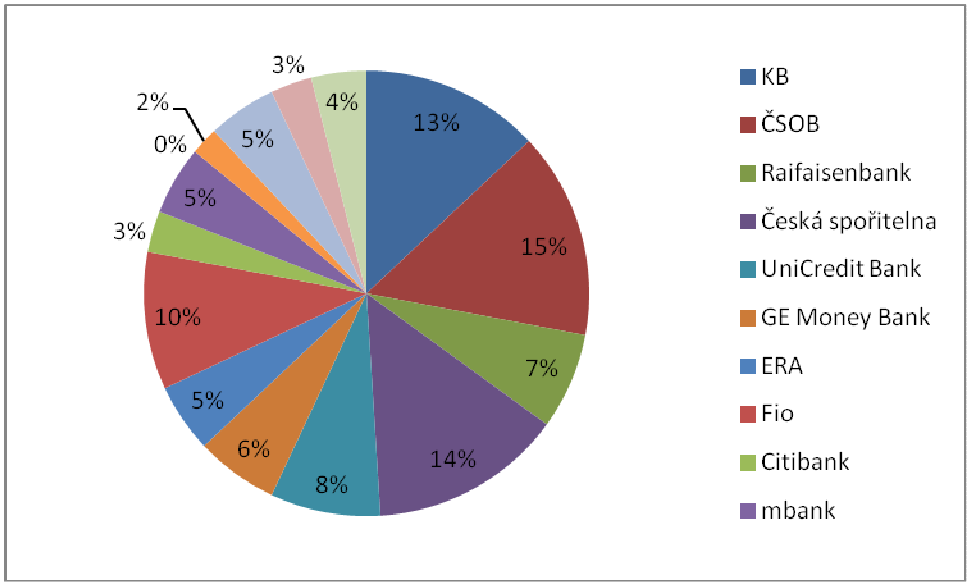
Průzkum ukazuje velice vyrovnané skupiny uživatelů podle použitelnosti. Podle výsledků by se daly jednotlivé čtvrtiny rozdělit podle věkového průměru. Odpověď a) zvolilo 21% dotázaných a tuto tvoří skupina zejména mladí lidé od 18 do 25 let. Největší skupina volila odpověď b) a tvoří lidé v produktivním věku mezi 26 a 36 rokem věku. Další významnou skupinu tvoří lidé mezi 37 a 50 rokem věku, kteří používají aplikaci jen zřídka. Poslední skupinu tvoří zejména lidé starší 50 let a převážně senioři, kteří nepoužívají aplikaci vůbec. Nedá se ale samozřejmě říci, že každý mladý člověk používá aplikaci několikrát denně nebo každý člověk nad 50 let nepoužívá aplikaci vůbec. Jedná se pouze o jakousi průměrnou hodnotu.



Graf 7: Poměr odpovědí na otázku č.7
Zdroj: vlastní

Otázka č. 8 – Smartbankingové aplikace kterých bank používáte?

Výsledky průzkumu u testované otázky č. 8, jsou silně závislé na velikosti banky a počtu jejich klientů. Uživatelé měli možnost vybrat libovolný počet bank, jejichž aplikace používají a i přesto jsou výsledky téměř přímým odrazem velikosti banky podle počtu jejich klientů.



Graf 8: Poměr odpovědí na otázku č.8
Zdroj: vlastní

3.5. Analýza přímého bankovnictví Komerční banky

Tato kapitola zkoumá jednotlivé metody konceptu přímého bankovnictví Komerční banky a dává základ pro celkové hodnocení konkurenceschopnosti banky v oblasti poskytování bankovních služeb bez nutnosti osobní návštěvy pobočky.

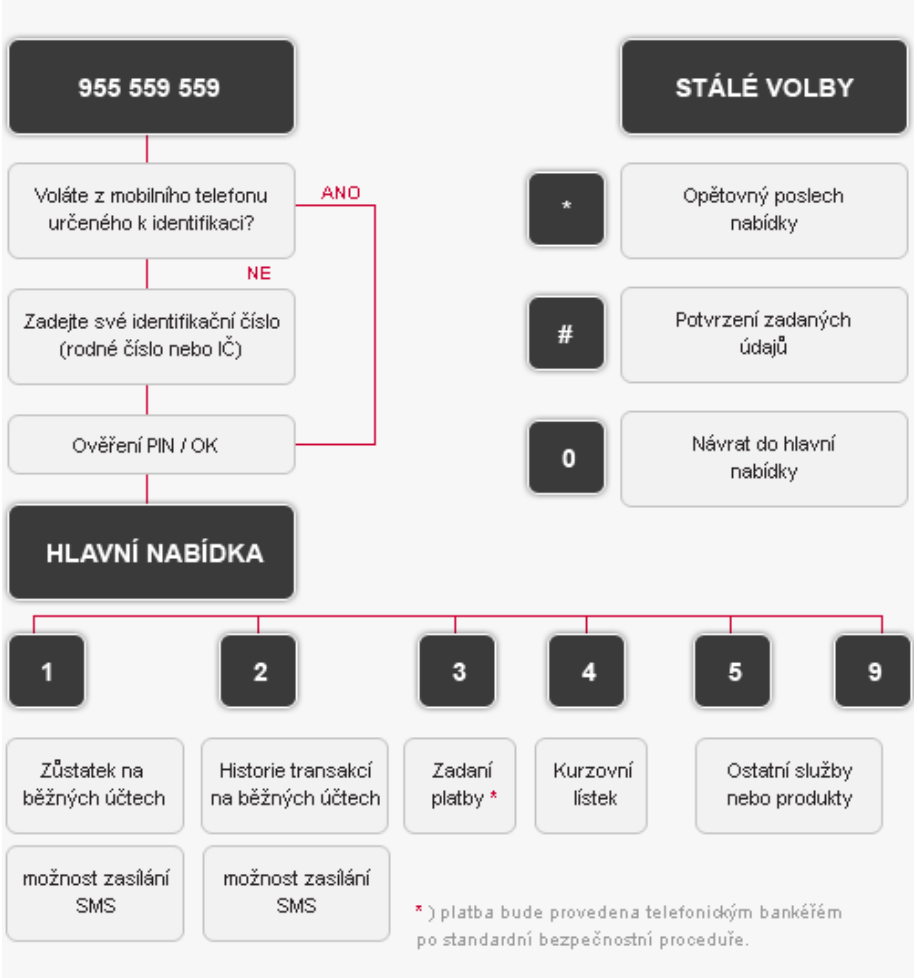
3.5.1. Expresní linka

Tato služba přímého bankovnictví je určena zejména občanům a drobným podnikatelům jak nástroj obsluhy svého účtu pomocí telefonu. Dříve bylo volání na expresní linku pro klienty zdarma, nyní je podle nového ceníku zpoplatněna jako klasický hovor na pevnou linku. Výhodou tohoto typu přímého bankovnictví je naprostá nenáročnost na HW vybavení. K obsluze postačí jakýkoli mobilní telefon nebo pevná linka. Další, a pro někoho zásadní výhoda je to, že komunikuje s operátorem, který mu může zodpovědět i netradiční dotazy a plnit netradiční přání, které např. systém *MojeBanka* nedovoluje.

I v dnešní době informačních technologií, existuje stále spousta domácností bez internetové přípojky nebo dokonce osobního počítače či notebooku a proto je pro ně expresní linka naprosto zásadní nástroj přímého bankovnictví.

Služby poskytované Expresní linkou

- → Získání informací o zůstatcích a pohybech na všech účtech, s nimiž uživatel disponuje
- → Zadávání příkazů k úhradě
- → Vytváření šablon, pro zadávání opakovaných příkazů k úhradě
- → Zadávání, rušení a změna trvalých příkazů k úhradě
- → Povolení, změna čí zrušení inkasa
- → Podání žádosti o vydání platební karty
- → Podání žádosti o vydání kreditní karty
- → Založení termínovaného účtu
- → Obchodování s cennými papíry
- → Uzavření smlouvy doplňkového penzijního spoření nebo důchodového spoření
- → a řadu dalších služeb



Obrázek 10: Schéma Expresní linky
Zdroj: (28)

Bezpečnost Expresní linky je zajištěna dvou-faktorovou autentizací.

Identifikace klienta – ta probíhá pomocí identifikačního čísla, což může být rodné číslo, IČO, číslo mobilního telefonu apod.

Autentizace - ověření totožnosti, pomocí vybraného typu bezpečnosti. Buď čtyřmístný PIN v kombinaci s heslem nebo karta OPK.

3.5.2. MojeBanka

Tento produkt dává klientům Komerční banky možnost spravovat svůj účet prostřednictvím internetu skrze webové rozhraní. Tento druh přímého bankovnictví je nejrozšířenější a nejpohodlnější, z důvodu snadného přístupu z téměř jakéhokoli počítače připojeného k síti internet. Veškerá komunikace probíhá pod zabezpečeným SSL a každou aktivní operaci uživatel podepisuje.

Minimální požadavky na PC

Operační systém	Verze prohlížeče	Verze Java
Microsoft Windows XP SP 3	MS Internet Explorer 7.0 MS Internet Explorer 8.0 Mozilla Firefox 6 Opera 11.0X* Google Chrome 13*	SUN 1.6.0_27*
Microsoft Windows Vista SP 2, 32 i 64 bit Česká nebo anglická jazyková verze	MS Internet Explorer 7.0 MS Internet Explorer 8.0 MS Internet Explorer 9.0 Mozilla Firefox 6 Opera 11.0X* Google Chrome 13*	SUN 1.6.0_27*
Microsoft Windows 7 SP1, 32 i 64 bit Česká nebo anglická jazyková verze	MS Internet Explorer 8.0 MS Internet Explorer 9.0 Mozilla Firefox 6 Opera 11.0X* Google Chrome 13*	SUN 1.6.0_27*
Microsoft Windows SERVER 2008 SP1	MS Internet Explorer 8.0 MS Internet Explorer 9.0	SUN 1.6.0_27*
Linux Ubuntu 11.04 „Natty Narval“*	Mozilla Firefox 6	SUN 1.6.0_27*
MacOS X 10.7 Lion*	Mozilla Firefox 6 Safari 5.1	JAVA for Mac OS X 1.6.0_26

Obrázek 11: Minimální požadavky na systém
Zdroj: (28)

Přihlášení

Přihlášení do aplikace probíhá pomocí dvou-faktorové autentizace. Pro přihlášení uživatel potřebuje něco co zná (heslo) a něco co má (certifikát a mobilní telefon). Uživatel nejdříve nahraje do aplikace certifikát, který si vyzvedl na internetových stránkách KB, pomocí certifikačního průvodce a poté zadá heslo pro přihlášení. Pokud se klient přihlašuje poprvé z IP adresy, ze které se předtím ještě nepřihlašoval, vyzve ho aplikace k zadání jednorázového autorizačního SMS kódu, který mu byl zaslán, na předem definované telefonní číslo.

Obrázek 13: Certifikát na čipové kartě
Zdroj: (28)

Obrázek 12: Certifikát v souboru
Zdroj: (28)

Pro úspěšné přihlášení do aplikace Mojebanka pomocí certifikátu uloženého na čipové kartě je zapotřebí provést dva kroky. Prvním krokem je instalace ovladačů čipové karty a rozhraní Crypto plus KB (tento proces se provádí pouze 1x). Druhým krokem je samotné přihlášení a zadání bezpečnostního kódu PIN.

Pro přihlášení pomocí certifikátu uloženého v souboru, stačí přes prohlížeč tento soubor nahrát do webového rozhraní a zadat heslo.

Po úspěšném přihlášení nám aplikace na úvodní obrazovce zobrazí přehled účtů, vedených u KB, kde okamžitě vidíme stav debetního, popř. kreditního či termínovaného účtu. Přímo z hlavní obrazovky, po kliknutí na kterýkoli účet můžeme zjistit použitelné peněžní prostředky daného účtu, zadat platbu, či zobrazit historii transakcí nebo dnešní činnost.

3.5.3. Mobilní banka

Mobilní banka, je služba přímého bankovnictví, určena především občanům a drobným podnikatelům, která umožňuje využívat bankovních služeb kdykoli a kdekoli prostřednictvím speciální aplikace nainstalované v mobilním telefonu, za použití stejných bezpečnostních prvků, které klient používá pro Expresní linku KB - jedná se o identifikační číslo, PIN a heslo, nebo kartu OPK. Komunikace je zabezpečena šifrovací metodou AES.

Služba byla spuštěna na začátku roku 2005. Aplikace byla ve své době špičkou a Komerční banka patřila mezi 3 banky na světě, které Java Banking rozšířili mezi své klienty. V té době nebyl ještě datový tarif samozřejmostí a připojení bylo pomalé.

Vývoj se však ubíral jiným směrem. Uživatelé, kteří však aplikaci nainstalovali, byli spokojeni, neboť je velmi jednoduchá a transparentní. Aplikace se však nikdy nestala masovou záležitostí.

Služba je nabízena pouze jako součást telefonního bankovnictví Expresní linka KB. Aktivací služby Mobilní banka je klientovi umožněno využívat stejných operací a přistupovat ke stejným produktům jako u Expresní linky KB. Pro úspěšnou instalaci a provoz aplikace Mobilní banka musí mít uživatel mobilní zařízení splňující technické podmínky, aktivovány datové přenosy u mobilního operátora a správně nastaveny parametry datových přenosů GPRS v mobilním telefonu.

Tabulka 4: Minimální konfigurace telefonu

Mobilní telefon	
Splňující standard nebo kompatibilní s	J2ME MIDP 1.0
Paměť telefonu (pro aplikaci)	min. 64 KB
HEAP (paměť pro běh aplikace)	min 200 KB
RMS (paměť pro uložení dat)	min 20 KB
Komunikace (podporováno)	http komunikace přes CSD, GPRS nebo EDGE
Komunikace (doporučená)	GPRS, EDGE
Barevný display	počet barev min. 256, rozlišení min. 128 x 128 bodů
Velikost stahovaných aplikací	Min. 64 KB

Zdroj: (28)

První přihlášení do aplikace

Po spuštění aplikace Mobilní banka, je uživatel vyzván k zadání znaků z PINu a hesla, případně k zadání sériového čísla karty optického klíče, a aktivačního kódu. Po ověření správnosti zadání jsou v mobilním telefonu vygenerovány přístupové klíče, sloužící k navázání spojení při dalších přihlášeních. Tato operace může trvat až několik desítek sekund, v závislosti na rychlosti procesoru telefonu. Klíče jsou uloženy v zašifrované podobě v paměti telefonu a nejsou uživateli přístupné. Pro každé přihlášení je použit a spotřebován jeden klíč. Po jejich spotřebování je nutné obnovit přístupové klíče telefonátem na Expresní linku KB. Uživateli je sdělen nový aktivační kód a při dalším přihlášení do aplikace provádí stejnou proceduru jako při prvním přihlášení do aplikace. Na nutnost generace nových přístupových klíčů je uživatel s předstihem

aplikací opakovaně upozorněn. Po úspěšném vygenerování klíčů je možné se přihlásit do aplikace stejným způsobem jako při následných přihlášeních.

Obrázek 14: Mobilní banka – přihlášení
Zdroj: (28)

Obrázek 15: Mobilní banka – přehled
Zdroj: (28)

Funkčnosti přístupné z hlavního menu

Po výběru subjektu a účtu se uživateli zobrazí hlavní menu aplikace. V záhlaví je zobrazen vybraný účet. V menu jsou pak zobrazeny volby:

- Použitelný zůstatek,
- Platební příkazy,
- Přehledy,
- Jiný účet/subjekt,
- Odhlásit se.

Platební příkazy je možné zadávat pouze na vrub účtů vedených v CZK, ve prospěch účtů vedených také v CZK, a to jak v rámci KB, tak do jiných bank v ČR. Prostřednictvím aplikace Mobilní banka není možné zadávat platby ve prospěch termínovaných účtů vedených u KB. Příkazy s dopřednou splatností (tj. zpracovávají se až v den splatnosti) nelze zadat. Pro snazší zadávání příkazů k úhradě je možné použít připravené šablony platebních příkazů. Funkci je možné využít pouze pro běžné účty vedené v CZK. Podmínkou úspěšného odeslání platebních příkazů ke zpracování

bankou, je dostatečný bezpečnostní limit uživatele a dostatečný použitelný zůstatek účtu. Je možné získat přehled o zúčtovaných transakcích na vybraném účtu a dále si zobrazit detail jednotlivé položky.

Dnes už je tato aplikace přežitkem a v podstatě se již nepoužívá. Nahradila jí nová verze Mobilní banka 2, která je určena pro „chytré“ telefony s dotykovým displejem a operačním systémem Android či iOs. Pro jiné operační systémy je zapotřebí webový prohlížeč s podporou JavaScriptu.

3.5.4. Mobilní banka 2

Komerční banka druhou verzi aplikace vydává v červenci roku 2011 a jako jedna z prvních tuzemských bank, tak reaguje na vzrůstající poptávku po funkčních aplikacích pro chytré telefony. Aplikace v té době zatím nenabízí zabezpečený přístup k účtu a slouží pouze jako pomocný nástroj pro vyhledávání bankomatů a poboček či jako měnová kalkulačka.

V květnu roku 2012, pak, jako jedna z posledních bank, přichází s aktualizací, která již nabízí přístup do zabezpečené sekce. Tato první aktualizace se však nesetkává s kladným ohlasem uživatelů, a to hlavě proto, že nenabízí základní funkci, která dělá mobilní bankovnictví mobilním. Touto funkcí je zasílání plateb na libovolná čísla účtů. Nabízí toto pouze omezeně, a to na čísla účtů přednastavená v internetovém bankovnictví jako šablony.

3.5.5. Jiné nástroje přímého bankovnictví

Profibanka

Aplikace Profibanka Komerční banky je velmi podobný produkt jako MojeBanka. Hlavní rozdíl je, že Profibanka je určena pro podnikatele a firmy. Profibanka je programována přímo na míru. Z toho důvodu je zřízení služby zpoplatněno.

Veškeré nabízené služby jsou totožné s produktem MojeBanka. Uspořádání odkazů a záložek je víceméně totožné. Profibanka přizpůsobuje své ovládací prvky potřebám podnikatelů, kdy například účet banky obsluhuje účetní firmy, ale platnost

odesílaných příkazů k úhradě musí svým elektronickým podpisem odsouhlasit více lidí. Bez souhlasu všech mezičlánků nemůže požadovaná operace proběhnout.

MojePlatba

Služba MojePlatba je určena uživatelům internetového bankovnictví MojeBanka s platným certifikátem v souboru nebo na čipové kartě. Jedná se o internetový platební nástroj pro klienty Komerční banky formou bezhotovostní platby přímo z internetových stránek obchodníka. Po rozhodnutí využít služby MojePlatba pro zaplacení zboží nebo služeb je nakupující při požadavku na úhradu přesměrován na stránky banky. Aplikace uživateli zobrazí před-vyplněný platební příkaz, uživatel jej podepíše svým certifikátem a po úspěšné autorizaci je přesměrován zpět na stránky obchodu. Platba obchodníkovi je garantována, obchodník tedy může ihned expedovat zboží.

Jedná se v podstatě o obdobu světoznámého platebního systému PayPal. Hlavní výhodou tohoto typu platby je, že obchodník vidí platbu okamžitě a odpadá tak až třídenní čekací lhůta pro převod peněz z účtu na účet.

3.6. Bezpečnost přímého bankovnictví KB

Problematika bezpečnosti přímého bankovnictví je velmi ošemetná věc. Uživatelé si jsou vědomi rizik s ním spojených a i přesto stále více lpí na jednoduchosti a použitelnosti produktů a nejsou ochotni přistoupit na mnohdy těžkopádná řešení autentizace uživatele.

3.6.1. Bezpečnost internetového bankovnictví KB

Komerční banka vsadila na relativně silnou, dvou-faktorovou autentizaci uživatele. Pro úspěšné přihlášení musí mít uživatel k dispozici svůj certifikát umístěný v souboru nebo na čipové kartě, heslo a mobilní telefon.

Certifikát umístěný v souboru lze použít kdekoli a kdykoli, ale největší bezpečnostní problém, skýtá jeho transfer a uložení. Velmi špatná volba je zasílání nezabezpečeného certifikátu nešifrovanými nebo špatně šifrovanými kanály, jako je

e-mail, bluetooth, ftp nebo třeba pomocí infra-portu, kde je odposlouchávání přenosu reálnou hrozbou.

Certifikát na čipové kartě řeší problém uložení. Lze jej v podstatě skladovat vedle platební karty, která je též chráněna dalším bezpečnostním prvkem a mít jej tak neustále k dispozici. Problém ale nastává v případě, že uživatel nemá k dispozici čtečku čipových karet.

Pro adekvátně silné heslo, je důležité, aby kromě velkých a malých písmen obsahovalo číslice a speciální znaky. Nedoporučuje se v hesle používat kombinace znaků, jakýmkoli způsobem souvisejících s danou osobou. Např. data narození, jména svých dětí, názvů ulic či dokonce vlastní příjmení. V žádném případě se nedoporučuje zapisovat si heslo do mobilního telefonu, lepit na papírku na monitor či jej mít poblíž certifikátu nebo čipové karty (stejně jako nemít zapsán PIN poblíž platební či kreditní karty).

Komunikace mezi klientem a bankou, je zabezpečena pomocí šifrovacího protokolu HTTPS. Bezpečnost je dále podporována automatickým odhlašování v případě, že byl uživatel delší dobu nečinný. Pro provedení jakékoli transakce, je opět nezbytné, mít k dispozici všechny bezpečnostní součásti pro úspěšnou autorizaci, a to certifikát, heslo a mobilní telefon. Bez jakéhokoli jednoho či více chybějících členů nebude provedena autorizace uživatele a nebude možné provést žádnou transakci.

3.6.2. Bezpečnost mobilního bankovnictví KB

Komunikace mezi zařízením a bankou, je zabezpečena šifrovacím protokolem AES. U mobilní banky je odolnost vůči útoku MITM (viz kapitola 2.2.2) zajištěna tzv. white-listem, tzn. možností transakcí peněžních prostředků pouze na předem definované účty. Uživatelé mobilního bankovnictví hledí více na jednoduchost a okamžitou použitelnost než na bezpečnost. Tu berou jako samozřejmost a domnívají se, že banka veškerou bezpečnost zajistí. S dobrým úmyslem pak vývojáři a bezpečnostní experti omezí zasílání plateb pouze na předem definované účty, což ale vede k silné degradaci a nepoužitelnosti aplikace.

Bohužel, nebo bohudík je za 90% úspěšných útoků zodpovědný právě uživatel, který svým nezodpovědným chováním ohrožuje bezpečnost svých finančních prostředků. Bohudík proto, že pokud si uživatel uvědomí rizika a své chování tomu přizpůsobí, je pravděpodobnost prolomení bezpečnosti velmi nízká.

U Mobilní banky 2 je kromě white-listu jediný bezpečnostní prvek heslo. Na správné zadání hesla má uživatel 3 pokusy. Poté se účet zablokuje a odblokovat jej je možné pouze přes aplikaci MojeBanka nebo osobní návštěvou pobočky (nikoli přes telefonního operátora, kvůli nedostatečné autorizaci).

Dotázaní uživatelé při průzkumu zcela zavrhli jakýkoli další prvek autentizace jako např. kalkulačku na challenge – response nebo obdobu certifikátu jako u internetového bankovnictví. Autentizace pomocí SMS je zase drahá varianta a uživatel je závislý na operátorovi, kteří SMS negarantují a může se stát, že SMS přijde až za dlouhou dobu, což způsobuje velké operační riziko. Navíc SMS by ve většině případů přišla na stejné zařízení, ze kterého se transakce realizuje. Z toho důvodu je tato metoda neúčelná.

4. Vlastní návrh řešení, přínos návrhu řešení

Tato část diplomové práce se převážně zaměřuje na zpracování získaných údajů analýz a pokouší se naznačit směr, kterým je možno internetové a hlavně mobilní bankovnictví směrovat.

4.1. Srovnání jednotlivých verzí aplikací

Kapitola obsahuje srovnání původní a současné verze internetového bankovnictví MojeBanka a v dalším bodu se zaměřuje na obdobné srovnání smartbankingové aplikace Mobilní banka 2. Závěrem této kapitoly bude zhodnocení současné verze aplikace MojeBanka a Mobilní banka 2 a jejich vzájemné porovnání.

4.1.1. Starší verze webové aplikace MojeBanka

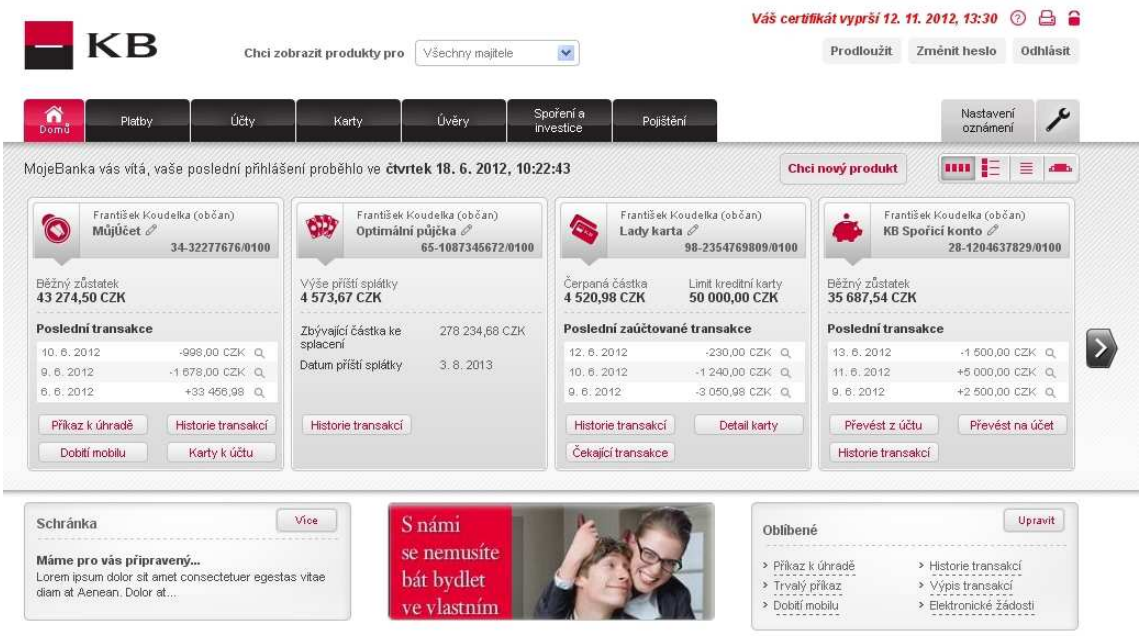
Grafický vzhled starší verze aplikace působí zastaralým dojmem a nedává uživateli pocit, že se jedná o produkt jedné z nejdynamičtější a nejsilnějších bank na českém trhu. Kladem této grafické verze je přehlednost

Obrázek 16: Hlavní obrazovka MojiBanky
Zdroj: (28)

4.1.2. Nová verze webové aplikace MojeBanka

Komerční banka současně s mobilní aplikací, vydává i kompletně novou internetovou aplikaci MojeBanka. Nejedná se přitom pouze nové grafické pojetí, ale i o přepracování backendových systémů. Nová frontendová technologie si vyžádala i úpravu aplikační vrstvy. Z designu nové MojiBanka pak vychází i design aplikace Mobilní Banka 2 (viz 0). t.j. kartičky a použité spektrum barev. U barev však moc možností není, jelikož jsou vývojáři svázáni korporátní identitou.

Zásadní vylepšení se týkají zejména zjednodušení ovládání, kdy 80% nejčastěji používaných funkcí je dostupných přímo z hlavní obrazovky. Mění se koncept z funkční orientace na produktovou. Znamená to, že uživatel nejdříve vybírá produkt a poté teprve akci, kterou chce provést.



Obrázek 17: Připravovaná verze MojiBanky
Zdroj: (28)

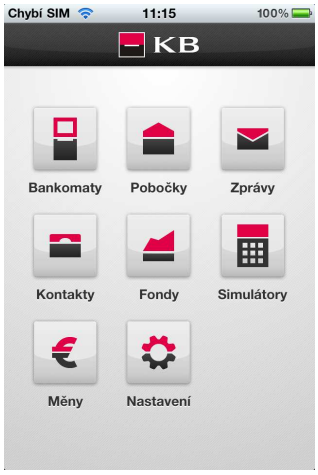
4.1.3. Mobilní banka 2 – původní verze

Aplikace Mobilní banka 2 se od svého vydání v červenci 2011 až po verzi 2.0.2 vydanou 8.prosince 2011 nestala u uživatelů příliš populární a oblíbenou (viz obrázek č.19). Bylo tomu tak zejména z důvodu chybějících součástí plnohodnotného mobilního

bankovnictví. Aplikace v základní verzi nenabízela svým klientům žádným, ani omezeným způsobem přístup ke svým účtům. Vzhledem k tomu, že je KB, a.s druhou největší bankou v ČR, očekává se od ní, že součástí nabízených služeb, bude kvalitní mobilní bankovnictví. Bohužel tomu, až do konce května 2012, nebylo. KB byla jednou z posledních větších bank, která tuto službu pro chytré telefony nenabízela. Základem mobilního bankovnictví, je nejen přístup k důležitým informacím, ale hlavně možnost kdykoli a odkudkoli přistupovat a obsluhovat svůj účet. Až na pár výjimek, byly informace nabízené touto aplikací nepotřebné, irelevantní a mnohdy i redundantní a aplikace jako taková byla v podstatě nepoužitelná.

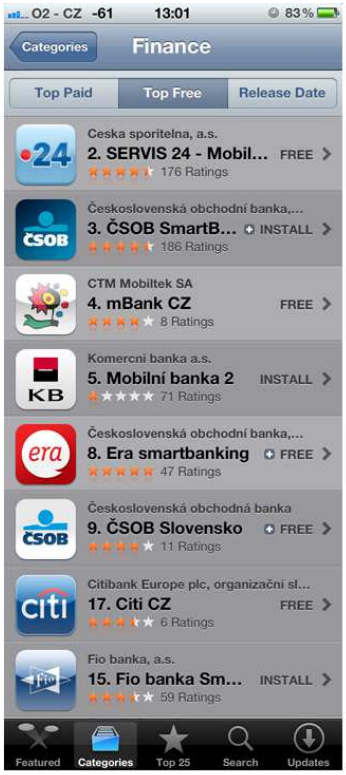
Nabízené funkce první verze Mobilní banky 2

- Bankomaty
- Pobočky
- Zprávy
- Kontakty
- Fondy
- Simulátory
- Měny
- Nastavení



Obrázek 18: Hlavní obrazovka
Zdroj: (28)

Po vydání aktualizace v květnu roku 2012 se ale situace příliš nezměnila. Sice již bylo k dispozici přihlášení do zabezpečené sekce, aplikace však nabízela provádění plateb pouze na čísla účtů z tzv. White-listu, vytvořeném v internetovém bankovnictví. Toto omezení aplikaci degradovalo a v podstatě narušilo celkový koncept mobilního bankovnictví. Praktická použitelnost byla omezena hlavně kvůli



Obrázek 19: Seznam dostupných smartbankingových aplikací
Zrdoj: vlastní

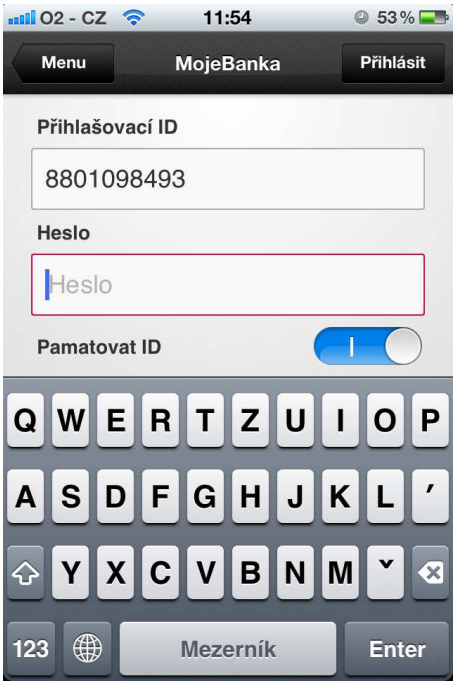
4.1.4. Mobilní banka 2 - nová verze

Tlak ze strany klientů, donutil Komerční banku investovat nemalé finanční prostředky do vývoje nové, vylepšené verze Mobilní banky 2.

Aplikace byla oficiálně zveřejněna dne 25.5.2012 a KB se tak stala jednou z posledních bank na českém trhu, která začala poskytovat přístup ke klientským účtům prostřednictvím chytrého telefonu. Aktivace služby probíhá přes internet banking a provádí ji každý uživatel samostatně, není tedy nutná návštěva pobočky. Ta je nutná pouze v případě, že uživatel nemá internetové bankovnictví. V současné době je tato služba klientům nabízena zdarma. Zpočátku neměla aplikace mezi uživateli příliš velký úspěch a to hlavně kvůli omezeným službám. První vydaná verze nenabízela zasílání volných finančních prostředků na libovolné účty. Platbu bylo možné zaslat pouze na čísla účtů předdefinovaná v internetovém bankovnictví. K dnešnímu dni je již tento zásadní nedostatek odstraněn a aplikace se tak bez problémů vyrovná konkurenčním službám. Nejnovější verzi mobilní aplikace Komerční banky již můžeme označit jako plnohodnotný produkt. Nabízí téměř všechny důležité součásti, které by měly mobilní

aplikace obsahovat. Některé součásti je nutné dotáhnout do konce, aby mohla být aplikace použitelná v maximální možné míře. Výčet doporučení je v kapitole 4.5.

V současné době je aplikace schopna zasílat finanční prostředky na libovolná čísla účtů, zobrazit historii nebo přehled příkazů, zaplatit fakturu za mobilní služby Vodafone nebo dobít kredit libovolného operátora. Pokud jakákoli faktura obsahuje QR kód, je aplikace schopna tento kód načíst a ušetřit tak uživateli čas, který by strávil vyplňováním údajů. Podobným způsobem dokáže aplikace načíst údaje ze složenky.



Obrázek 21: MB2 – přihlášení
Zdroj: vlastní

Obrázek 20: MB2 - hlavní obrazovka
Zdroj: vlastní

4.1.5. Internetové bankovnictví vs. mobilní bankovnictví

Z technického hlediska je Mobilní banka bezpečnější, protože není triviální záležitost dostat na zařízení oběti útočníkův škodlivý kód. Na Android i iPhone je potřeba aplikaci instalovat a explicitně povolit. Na iPhone je to ještě složitější, neboť každá aplikace, která je na AppStore, prochází schvalovacím procesem Apple (na Google Play nikoliv). Ovšem pokud uživatel provede root nebo jailbreak, pak i tento bezpečnostní prvek ztrácí na významu.

Z pohledu uživatelského je bezpečnější internetové bankovnictví a to hlavně z důvodu několika bezpečnostních prvků. Když uživatelská zodpovědnost selže na dvou stupních, stále existuje možnost odražení útoku, kdežto u mobilního bankovnictví stačí zadávat heslo v přítomnosti útočníka, který jej odposlouchá a pak pro něj v mnoha případech není problém zařízení odcizit a zneužít. V době vydání první verze aplikace byla bezpečnost posílena tzv. White-listem. Uživatelé ale na tento bezpečnostní prvek reagovali velmi negativně a KB byla nucena White-list zrušit. V současné době používá aplikace pro autorizaci uživatele pouze heslo, a zároveň musí být zařízení povoleno v internetové aplikaci MojeBanka pomocí jednoznačného identifikátoru UDID (iPhone) nebo IMEI (ostatní zařízení).

Tato problematika je sama o sobě velice kontroverzní. Vždy záleží na mnoha aspektech lidského chování, které je jednoznačně největší bezpečnostní hrozbou. Z tohoto důvodu, musí banka na každé zařízení nahlížet jako na kompromitované.

4.2. Srovnání s konkurencí

Cílem této kapitoly je postavit nejnovější verzi aplikace Mobilní banka 2 proti jednotlivým konkurenčním aplikacím a zhodnocení jednotlivých online a offline funkcí.

4.2.1. Srovnání online funkcí

Tabulka 5: Online funkce

Banka	Stav a historie účtu	Nová platba	Šablona platby	Přehled karet	Skenování složenky	Čtení QR kódů na fakturách	Dobití kreditu mobilu	Grafický náhled pohybu na účtu	Změna hesla	Celkový dojem	Hodnocení
Komerční banka	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ne	9%	87%
Česká spořitelna	Ano	Ano	Ano	Ne	Ano	Ano	Ne	Ne	Ne	6%	50%
ČSOB	Ano	Ano	Ano	Ano	Ne	Ano	Ano	Ne	Ne	10%	87%
UniCredit Bank	Ano	Ano	Ano	Ano	Ne	Ne	Ne	Ne	Ano	7%	63%
Raiffeisenbank	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ne	Ano	9%	87%
GE Money Bank	Ano	Ano	Ano	Ano	Ne	Ne	Ano	Ano	Ne	5%	72%
Era	Ano	Ano	Ne	Ano	Ne	Ano	Ano	Ne	Ne	8%	64%
Fio banka	Ano	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne	7%	40%
Citibank	Ano	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ne	6%	28%
mBank	Ano	Ano	Ano	Ano	Ne	Ne	Ne	Ne	Ne	5%	49%
ZUNO Bank	Ano	Ano	Ano	Ano	Ano	Ne	Ne	Ano	Ne	6%	73%
Equa bank	Ano	Ano	Ano	Ne	Ne	Ne	Ne	Ne	Ne	6%	39%
ING Bank	Ano	Ano	Ano	Ne	Ne	Ne	Ne	Ano	Ano	6%	62%

Zdroj: vlastní

4.2.2. Srovnání jednotlivých offline funkcí

Tabulka 6: Offline funkce

Banka	Hledání bankomatu, pobočky	Kontakty	Kurzovní lístek	QR Platba	Kalkulačka úvěrů	Návrh obrázku na kartu	Podílové fondy	Slevy	Zprávy z banky	Nápověda	Celkový dojem	Hodnocení
Komerční banka	Ano - i cizích bank	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ne	8%	88%
Česká spořitelna	Ano - jen vlastní	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Ne	7%	37%
ČSOB	Ano - i cizích bank a pošty	Ano	Ano	Ano	Ne	Ano	Ne	Ne	Ano	Ne	10%	70%
UniCredit Bank	Ano - jen vlastní	Ano	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ne	6%	36%
Raiffeisenbank	Ano - i cizích bank	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ano	Ano	8%	68%
GE Money Bank	Ano - jen vlastní	Ano	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ano	6%	56%
Era	Ano -i cizích bank a pošty	Ano	Ano	Ano	Ne	Ano	Ne	Ne	Ano	Ne	8%	68%
Fio banka	Ano - jen vlastní	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ano	Ne	6%	36%
Citibank	Ano - jen vlastní	Ano	Ano	Ne	Ne	Ne	Ne	Ano	Ne	Ano	5%	55%
mBank	Ano - jen vlastní	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ano	Ne	5%	35%
ZUNO Bank	Ano - i cizích bank a pošty	Ano	Ano	Ne	Ano	Ne	Ne	Ne	Ano	Ano	6%	66%
Equa bank	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ano	Ano	7%	37%
ING Bank	Ano - jen vlastní	Ano	Ne	Ne	Ne	Ne	Ano	Ne	Ano	Ano	6%	56%

Zdroj: vlastní

4.2.3. Výsledné hodnocení

Největším konkurentem Mobilní Banky 2, je aplikace pro mobilní bankovnictví Československé obchodní banky ČSOB Smartbanking. Aplikace nabízí široké portfolio služeb a přitom si zachovává přehlednost a uživatelskou přívětivost. Na začátku roku 2013 získala ČSOB prestižní ocenění Mobilní aplikace roku 2012. Uživatelské hodnocení v obchodech pro jednotlivé operační systémy jsou hromadně kladné. Naproti tomu uživatelská hodnocení aplikace Komerční banky jsou velice protichůdné. Téměř 90% uživatelů hodnotí aplikaci jako velice povedenou a komplexně dobře řešenou. Zbylých 10% uživatelů má s aplikací zásadní problém a jejich hodnocení je velice nízké. Ve většině případů se jedná o funkční nedostatky, které banka v nových verzích nabízí, ale u uživatelů se objevují individuální chyby problémy s fungováním.

Tabulka 7: Výsledné hodnocení

Banka	Výsledné hodnocení
Komerční banka	87,4%
Česká spořitelna	43,7%
ČSOB	83,3%
UniCredit Bank	49,3%
Raiffeisenbank	72,4%
GE Money Bank	63,8%
Era	65,8%
Fio banka	38,2%
Citibank	41,6%
mBank	42,2%
ZUNO Bank	69,3%
Equa bank	38,2%
ING Bank	58,8%

Zdroj: vlastní

4.3. Zhodnocení nové verze Mobilní banky 2

Komerční banka sice přišla na trh mobilních aplikací s plnohodnotným produktem jako jedna z posledních, ale o to kvalitněji zpracované řešení přináší. Tuto pozici nebere jako nevýhodu. Naopak se ji snaží využít ve svůj prospěch. Hledá chyby a nedostatky u konkurenčních aplikací, snaží se z nich poučit a ve své nově vydané

aplikaci tyto nedostatky eliminovat. Analýza a srovnání s jinými smartbankingovými aplikacemi poukazuje na velkou konkurenceschopnost a silný potenciál, který aplikace bezpochyby má.

4.4. Zhodnocení dotazníkového průzkumu

Výsledky dotazníkového průzkumu poukazují na skutečnost, že se mobilní bankovnictví stává v České republice stále více oblíbené. Uživatelé si stále nejsou jisti dostatečným zabezpečením. Tato reakce je však naprosto běžná. S příchodem internetového bankovnictví byla uživatelská skepse naprosto stejná a v dnešní době je již internetové bankovnictví masovou záležitostí. S velkou pravděpodobností bude situace u mobilního bankovnictví velice podobná.

4.5. Návrh na změny a vylepšení

Jako klient KB, uživatel a nadšenec pro mobilní a obecně IT technologie přikládám návrh na doplňující služby a funkce, které by mohly budoucí verze aplikace obsahovat a napomohly by tak zvýšit funkčnost a konkurenceschopnost aplikace a banky obecně.

4.5.1. Investiční portfolio

Mezi významné funkce patří sledování vývoje svého portfolia přímo v aplikace mobilního telefonu. Základním kamenem je sledování vývoje investičního životního pojištění Vital Invest, které investuje prostředky do různě rizikových IKS fondů Komerční banky.

4.5.2. Potvrzení odeslané platby

Pro maximální efektivitu smartbankingových aplikací je nutné, aby komunikace mezi uživatelem, bankou a ostatními klienty probíhala v reálném čase. Banka v mobilu má napomáhat uživateli, mít neustále k dispozici potřebné disponibilní zůstatky v kooperaci s maximálním zabezpečením. Aby byly tyto prostředky ihned použitelné, je nutné vyřešit problematiku okamžité zpětné vazby z banky. K tomu by měl sloužit, v reálném čase zaslaný, elektronicky podepsaný dokument, potvrzující odeslání platby na konkrétní účet, s možností okamžitého zaslání tohoto dokumentu protistraně.

4.5.3. QR platba

Zajímavou funkcí, kterou Komerční banka nabízí, je platba pomocí QR kódu, který si může uživatel sám vygenerovat přímo v aplikaci pouhým zadáním platebních údajů. Funkce má ale jednu zásadní nevýhodu, a to absenci čtení čárových kódů přímo z galerie obrázků. Reálná situace pak může vypadat následovně. Příjemce platby zašle QR kód obsahující platební informace odesílateli. Ten jej pomocí e-mailového klienta přijme, uloží do galerie obrázků a tím celá situace končí. Odesílatel takto přijatý QR kód není schopen přečíst. Jediná možnost je mít v tu chvíli u sebe dvě zařízení (další mobilní telefon s přístupem k internetu či notebook) nebo tiskárnu, na které si QR kód vytiskne a načte. Téměř všechny aplikace sloužící ke čtení QR kódů obsahují funkci načtení kódu přímo z galerie obrázků bez nutnosti použití integrovaného fotoaparátu. Čtečka v aplikaci KB však tuto možnost nenabízí.

4.6. Doporučené zásady bezpečnosti mobilního bankovnictví

Z výsledků analýz v kapitolách … byl sestaven následující seznam doporučení, který má napomáhat ke zvýšení bezpečnosti při obsluze aplikace mobilního bankovnictví:

- Nezadávat PIN či heslo v přítomnosti další osoby.
- Nepřechovávat PIN či heslo v blízkosti zařízení pro obsluhu aplikace.
- V pravidelných intervalech měnit PIN či heslo.
- Neinstalovat na zařízení podezřelý software, který může odposlouchávat zařízení.
- Před ukončením aplikace provést odhlášení.
- Nepouštět z dohledu zařízení přihlášené do aplikace mobilního bankovnictví.
- Pravidelně zařízení kontrolovat antivirových softwarem.
- Mít zařízení uzamčeno bezpečnostním prvkem pro případ odcizení či ztráty.

5. Zhodnocení návrhu

Vzhledem k tomu, že Komerční banka investovala do vývoje internetové i mobilní aplikace finanční prostředky v řádek milionů korun, je bezpředmětné navrhovat zásadní změny. Kapitola 4.5 zobrazuje pouze přehled postřehů z pohledu nezaujatého klienta Komerční banky, ale i klienta konkurenčních bank. Internetové i mobilní bankovnictví má bezpochyby slibnou budoucnost, ale vše záleží na přístupu uživatelů. Jednoznačně největší překážkou v masovém používání služeb je jejich zabezpečení. Postupem času ubývá počítačově negramotných lidí a tento trend bude jistě pokračovat, až se skupina, která nedokáže s IT nástroji pracovat, zmenší na zanedbatelný počet. Vývojáři pak budou moci vyvíjet aplikace, které jsou složitější a komplexnější.

Závěr

Mobilní bankovnictví je v první řadě o flexibilitě a neomezených možnostech bezhotovostní platby. Tato oblast má obrovský budoucí potenciál a s postupujícím vývojem nových technologií, jde o cestu správným směrem. Dnes stojíme téměř na začátku, ale nebude dlouho trvat a hotovostní peníze, tak jak je známe, přestanou existovat a budou plně nahrazeny bezhotovostními převody přes mobilní zařízení a bezkontaktními čipovými kartami počínaje a skenováním biometrických údajů konče.

Krátkodobý a i dlouhodobý vývoj těchto technologií závisí především na lidské psychice. Čím je člověk starší, tím větší problém má se zásadními změnami a to hlavně v oblastech, kterým dokonale nerozumí a je nucen věřit, „že to tak prostě funguje“, aniž by věděl proč a jak. Je nutné mít na paměti, že systém mobilního bankovnictví je v ČR a obecně ve světě teprve na svém počátku a masové používání mobilních služeb bankovnictví je otázkou času. Stejně jako s příchodem internetu, byli lidé k používání internetového bankovnictví skeptičtí, dnes si většina z nich nedokáže představit neustálou nutnost osobní návštěvy pobočky banky.

Celá práce byla směrována do hodnocení hlavně technické stránky služeb banky. Bankovnictví ale není jenom o technickém zázemí. Klienty si získává a udržuje hlavně svým přístupem. Co se Komerční banky týče, zpětná vazba byla profesionální a na vysoké úrovni. Při zpracování kapitoly 0 jsem si jako zdroj informací vybral přímo konkrétní banky a informace sbíral e-mailovým kanálem. Žádal jsem o poskytnutí demo nebo testovacích verzí mobilních aplikací. Ve dvou případech jsem dostal odpověď a pouze jedna banka mi poskytla testovací verzi. Jiné banky na e-mail nereagovaly. Druhý, nezávisle zaslaný dopis téže bankám, obsahoval seznam otázek ke konkrétních aplikacích. Od jedné banky jsem dostal odpověď do 15 minut, jiná banka mi odpověděla do druhého dne, přičemž se jednalo o stejné banky jako v předchozím případě, ale jiné pracovníky. Reakce těchto dvou bank, mne velice potěšila, resp. jsem byl zklamaný z přístupu zbylých bank. Jedná se o maličkosti, ale právě tyto maličkosti dnes hrají významnou roli v konkurenčním boji o klienta.

6. Seznam použité literatury

6.1.Monografie

(1) BLAŽKOVÁ, M. *Jak využít internet v marketingu: krok za krokem k vyšší konkurenceschopnosti*. 1. vyd. Praha: Grada, 2005. 156 s. ISBN 80-247-1095-1

(2) BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc: ANAG, 2008. 157 s. ISBN 80-726-3465-8.

(3) DAEMEN, J., RIJMEN, V. *The Design of Rijndael: AES--the Advanced Encryption*. Praha: Springer, 2002. 238 s. ISBN 35-404-2580-2.

(4) DVOŘÁK, J. *Elektronický obchod*. MSD s.r.o. Brno: Ing. Zdeněk Novotný, CSc - Brno, 2005, 116 s. ISBN 80-214-2236-X

(5) DVOŘÁK, P. *Komerční bankovnictví pro bankéře a klienty*. 1.vyd. Praha: Linde, 1999. 244 s. ISBN 80-7169-859-8.

(6) HARPER, A., HARRIS, S., EAGLE, CH., NESS, J., LESTER, M. *Hacking – manuál hackera*. Praha: Grada, 2008. 399 s. ISBN 80-247-1346-2.

(7) HORSKÝ, R. *Bezdrátové sítě Wi-Fi v rekordním čase*. Praha: Grada, 2006. 84 s. ISBN 80-247-1790-5.

(8) KALABIS, Z. Bankovní služby v praxi. 1. vyd. Brno: Computer Press, 2005. 148 s. ISBN 80-251-0882-1.

(9) MALINKA, K. *Kryptografie a informační bezpečnost.* (Přednáška). Brno: VUT, 2008. 42s.

(10) MÁČE, M. Platební styk klasický a elektronický. 1. vyd. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.

(11) OPPLIGER, R. Ssl and Tls: *Theory and Practice*. London: Artech House, 2009. 257 s. ISBN 15-969-3447-6.

(12) POLIDAR, V. Management bank a bankovních obchodů. 2. vyd. Praha: Ekopress, 1999. 450 s. ISBN 80-86119-11-4.

(13) POUR, J., TOMAN, P. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi : technologie informačních systémů : řízení a rozvoj podnikové informatiky*. Praha: Expert (Grada), 2006. 482 s. ISNB 80-247-1278-4.

(14) PŘÁDKA M., KALA, J. *Elektronické bankovnictví.* Praha: ComputerPress, 2000. 166 s. ISBN 8072263285.

(15) SCHLOSSBERGER,O. Elektronické platební prostředky. Praha: Bankovní institut, a.s., 2005. 276 s. ISBN 80-7265-073-4.

(16) SVOBODA, P., KROFT, M., BERAN, K., EMR, D., FRÝZEK,L.VÁŇA, R., VÍT, M., *Právní a daňové aspekty e-obchodu*. 1. vyd. Praha: Linde, 2001. s. 461. ISBN 80-7201-311-4.

(17) SVOBODA, P. a kol. *Právní a daňové aspekty e-obchodu*. 1. vyd. Praha: Linde Praha a.s., 2001. 462 s. ISBN 80-7201-311-4.

(18) TILBORG, H., JAJODIA, S. *Encyclopedia of Cryptography and Security*. Praha: Springer, 2011. 1500 s. ISBN 14-419-5905-X.

6.2. Elektronické zdroje

(19) ACCESS.CZ *Autentizační metody založené na biometrických informacích.* [online]. 2012 [cit. 2012-03-04]. Dostupné z:http://access.feld.cvut.cz/view.php?cisloclanku=2010110002.

(20) *ADAPTIC.*CZ. *Účastnící e-obchodování*. [online]. 2011 [cit. 2012-03-02]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/.

(21) ALSOFT .CZ. *Autentizace*. [online]. 2011 [cit. 2012-04-10]. Dostupné z: http://www.alsoft.cz/cz/Products/Security/Vasco/Strong-Authentication-and-e-Signatures/.

(22) ASOCIACE PRO ELEKTRONICKOU KOMERCI. *O Asociaci*. [online]. 2009 [cit. 2012-03-12]. Dostupné z: http://www.apek.cz/8459/sekce/o-asociaci/.

(23) BANKOVNÍ POPLATKY. Smartbanking. [online]. 2011 [cit. 2012-04-11]. Dostupné z: http://www.bankovnipoplatky.com/smartbanking-v-ceskych-bankach-v-roce-2012-17181.html.

(24) ENETSYSTEM.CZ. *Internet.* [online]. 2005 [cit. 2012-03-24]. Dostupné z: http://www.enetsystem.net/index_308.htm.

(25) IKAROS.CZ. *Obchodování po sítí může přinést řadu výhod pro koncového zákazníka*. [online]. 2010 [cit. 2012-03-13]. Dostupné z: http://www.ikaros.cz/obchodovani-po-siti-muze-prinest-radu-vyhod-pro-koncoveho-zakaznika.

(26) KAFKA, J. *Přímé bankovnictví v Česku*. [online]. 2006 [cit. 2012-03-02].Dostupné z: http://www.finexpert.cz/default.aspx?section=17&server=1&article=17385.

(27) KB.CZ. Výroční zpráva 2011. [online]. 2012 [cit.2012-02-02]. Dostupné z: http://www.kb.cz/file/cs/o-bance/vztahy-s-investory/publikace/vyrocni-zpravy/kb-2011-vyrocni-zprava.pdf?eeb75525319871a5caeff01b1e417d1a.

(28) KB.CZ. [online]. 2012 [cit.2012-02-02]. Dostupné z: http://www.kb.cz/.

(29) KRČMÁŘ, P. *Bezpečnost českého internetového bankovnictví.* [online]. 2005 [cit. 2012-03-04] Dostupné z: http://www.root.cz/clanky/bezpecnostceskehointernetovehobankovnictvi/.

(30) LUPA.CZ. *Historie českého Internetu*. [online]. 2007 [cit.2012-03-21]. Dostupné z: http://www.lupa.cz/clanky/historie-ceskeho-internetu/.

(31) MARKETINGOVÉNOVINY.CZ. *Historie elektronických obchodů*. [online]. 2006 [cit. 2012-02-13]. Dostupné z: http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4391.

(32) MĚŠEC.CZ. *Home banking.* [online]. 2007 [cit. 2012-04-04] Dostupné z: http://www.mesec.cz/texty/homebanking/.

(33) MĚŠEC.CZ. *Elektronické bankovnictví.* [online]. 2007 [cit. 2012-20-4]. Dostupné z: http://www.mesec.cz/texty/elektronickebankovnictvi/.

(34) MĚŠEC.CZ. *Smartbanking* [online]. 2011 [cit. 2012-04-01]. Dostupné z: http://www.mesec.cz/clanky/smartbanking-daleko-za-svymi-moznostmi/.

(35) MOJEBANKA.CZ.*Internet Banking*. [online]. 2012 [cit. 2012-04-13]. Dostupné z: https://www.mojebanka.cz/InternetBanking/?L=CS

(36) MVCR.CZ. *Informace k používání elektronického podpisu*. [online]. 2012 [cit. 2012-04-05]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx.

(37) NACHER, P. *Internetové bankovnictví pod lupou.* [online]. 2007 [cit. 2012-04-04] Dostupné z: http://www.nasepenize.cz/clanek655internetovebankovnictvipodlupou.

(38) *Online obchody.* [on-line]. 2005 [cit. 2012-02-20]. Dostupné z: http://www.onlineobchody.com/.

(39) POHODA 2008. *Swmag* [online]. 2009 [cit. 2012-03-08]. Dostupné z: http://www.swmag.cz/213/pohoda-2008/

(40) RYBKOVÁ, H. *Internetbanking: bezpečnost na úkor pohodlí*. [online]. 2006 [cit. 2012-07-04] Dostupný z: http://aktualne.centrum.cz/finance/clanek.phtml?id=137692.

(41) SHOPFINDER.CZ. *Nákup na internetu pro začátečníky*. [online]. 2010 [cit. 2012-03-02]. Dostupné z: http://www.shopfinder.cz/svet/clanek.asp?ID=3#4.

(42) ŠKRDLA, V., *Právní aspekty elektronické komerce v ČR.* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http//www.bfco.eu/dokumenty-info/pravni-aspekty-elektronicke-komerce-v-cr.doc.

(43) T-MOBILE.CZ *Platby mobilem.* [online]. 2006 [cit. 2012-04-13]. Dostupné z: http://www.tmobile.cz/web/cz/zivnostnici.a.podnikatele/sluzby.a.reseni/platby.mobilem/gsm.banking.

(44) VOLKSBANK.CZ *Phone Banking.* [online]. 2009 [cit. 2012-03-13]. Dostupné z: http://www.volksbank.cz/volksbank/404.aspx?item=%2fvb%2fjnp%2fcz%2fobcane%2fcz-obcane-phone_banking&user=extranet\Anonymous&site=websit)

7. Seznam obrázků a tabulek

7.1.Seznam obrázků

7.2. Seznam tabulek

7.3. Seznam grafů