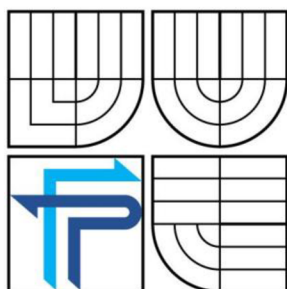


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

MODEL HODNOCENÍ ELEKTRONICKÉHO BANKOVNICTVÍ

EVALUATION MODEL OF ELECTRONIC BANKING

DIPLOMOVÁ PRÁCE

DIPLOMA THESIS

AUTOR PRÁCE

AUTHOR

LUBOMÍR MAŽÁK

VEDOUCÍ PRÁCE

SUPERVISOR

prof. Ing. JIŘÍ DVOŘÁK, DrSc.

BRNO 2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

Maťák Lubomír

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:

Model hodnocení elektronického bankovníctví

v anglickém jazyce:

Evaluation Model of Electronic Banking

Pokyny pro vypracování:

Úvod

Vymezení problému a cíle práce

Teoretická východiska práce

Analýza problému a současné situace

Vlastní návrh řešení, přínos návrhu řešení

Závěr

Seznam použité literatury

Přílohy

Seznam odborné literatury:

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

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

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

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

Vedoucí diplomové práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2011/2012.

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkan fakulty

V Brně, dne 19.04.2012

Abstrakt

Obsahem práce je vytvoření modelu hodnocení elektronického bankovníctví pro KB a vyjádření přínosu z pohledu ekonomického a technického.

Abstract

The thesis is a model evaluation of electronic banking for KB expression and benefit from the economic and technical.

Klíčová slova

elektronické bankovníctví, elektronické podnikání, smartbanking

Keywords

e-banking, e-business, smartbanking

Bibliografická citace mé práce

MAŤÁK, L. *Model hodnocení elektronického bankovníctví*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 81 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc..

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 19.5.2012

Poděkování

Rád bych touto cestou poděkoval vedoucímu své práce prof. Ing. Jiřímu Dvořákovi, DrSc. za ochotu, cenné rady a připomínky, které mi poskytl při zpracování diplomové práce a zejména pak panu Petru Jandovi za trpělivost, obětavost a poskytnutí všech důležitých informací.

Obsah

Úvod.....	10
1. Vymezení problému a cíle práce.....	11
1.1. Vymezení problému.....	11
1.2. Cíl práce.....	12
2. Teoretická východiska práce.....	13
2.1. Historický vývoj internetu.....	13
2.2. Bezpečnost na internetu.....	14
2.2.1. Tři základní notace.....	14
2.2.2. Zabezpečení proti útoku Man-In-The-Middle.....	15
2.2.3. Elektronický podpis.....	16
2.2.4. Symetrická a asymetrická šifra.....	16
2.2.5. Certifikáty.....	17
2.2.6. Šifrovací standardy a protokoly.....	18
2.3. Elektronický obchod.....	20
2.3.1. Historie elektronického obchodu.....	20
2.3.2. Základní dělení elektronického obchodu.....	21
2.3.3. Výhody a nevýhody elektronického obchodování.....	24
2.3.4. Obchod a elektronické obchodování.....	26
2.4. Elektronické bankovníctví.....	27
2.4.1. Historický vývoj elektronického bankovníctví.....	28
2.4.2. Základní formy elektronického bankovníctví.....	29
2.4.3. Metody zabezpečení elektronického bankovníctví.....	33
2.4.4. Smartbanking.....	35
3. Analýza problému a současné situace.....	38
3.1. Popis společnosti Komerční banka, a.s.....	38
3.2. Přímé bankovníctví.....	39
3.2.1. Expresní linka.....	39
3.2.2. MojeBanka.....	41
3.2.3. Nově připravovaná verze MojeBanka.....	47
3.2.4. Mobilní banka.....	48
3.2.5. Mobilní banka 2 – původní verze.....	53
3.2.6. Mobilní banka 2 - nová verze.....	56
3.2.7. Jiné nástroje přímého bankovníctví.....	59
3.3. Bezpečnost přímého bankovníctví KB.....	60
3.3.1. Bezpečnost internetového bankovníctví KB.....	60
3.3.2. Bezpečnost mobilního bankovníctví KB.....	61
3.3.3. Internetové bankovníctví vs. mobilní bankovníctví.....	62

4. Vlastní návrh řešení, přínos návrhu řešení	63
4.1. Srovnání s konkurencí.....	63
4.1.1. Fio banka	64
4.1.2. Česká spořitelna	65
4.1.3. Československá obchodní banka	66
4.1.4. ERA Poštovní spořitelna	67
4.1.5. UniCredit Bank	67
4.1.6. GE Money Bank.....	68
4.1.7. mBank	69
4.1.8. Citibank	71
4.2. Výsledné hodnocení	72
4.3. Zhodnocení nové verze Mobilní Banky 2	72
4.4. Návrh na změny a vylepšení	72
4.4.1. Odstranění White-listu	73
4.4.2. Investiční portfolio	73
4.4.3. Potvrzení odeslané platby	73
Závěr.....	74
Seznam použité literatury.....	75
Monografie	75
Elektronické zdroje.....	77
Seznam obrázků a tabulek	80
Seznam obrázků	80
Seznam tabulek	81

Úvod

Elektronický obchod a vše s ním spojené, dnes hraje ve světě businessu a podnikání velice významnou roli, akšak ne každá firma naplno využívá potenciálu, který tato forma obchodování nabízí. Práce je zaměřena na oblast poskytování bankovních produktů skrze e-commerce a speciálně pak soustředěna na právě vyvíjenou aplikaci Komerční banky, pro obsluhu jejich produktů pomocí relativně nové záležitosti, a to „chytrých“ telefonů s operačním systémem iOS nebo Android.

Práce si dává za cíl zhodnotit tuto aplikaci s konkurenčními aplikacemi ostatních bank, působících na tuzemském trhu, vymezit její nedostatky a navrhnout opatření, která by vedla k posílení konkurenceschopnosti banky v tomto odvětví.

1. Vymezení problému a cíle práce

1.1. Vymezení problému

Celá práce je koncipována jako analýza a zhodnocení současného a budoucího stavu elektronického bankovníctví KB, z pohledu nezaujatého klienta Komerční banky, a.s., která, jakožto jedna z největších tuzemských bank, stojí na přelomu moderního přístupu k elektronickému bankovníctví.

Měl jsem tu čest, jako jeden z mála, se osobně podílet na vývoji a testování nových prostředků elektronického bankovníctví pro zmíněnou 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 zlomovém okamžiku, kdy se KB usilovně snaží překonat vcelku vyspělou konkurenci a stát se opět jedničkou mezi tuzemskými bankami, co se technické stránky týče.

1.2. Cíl práce

Na základě informačních zdrojů světa a analýzy zvoleného bankovního segmentu vytvořit model hodnocení elektronického bankovníctví pro KB. Navržený model hodnocení elektronického bankovníctví vyjádřit přínosem z pohledu ekonomického a technického.

Dílčí cíle práce

- Analýza stávajícího stavu elektronického bankovníctví vybrané banky
- Zhodnocení připravovaných změn a vylepšení
- Srovnání s konkurencí

2. Teoretická východiska práce

Teoretické část diplomové práce se zaměřuje na historii a vývoj internetu, ale především na problematiku elektronického obchodování, internet bankingu, smartbankingu a 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 řídicích 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

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

Nejúčinnější metodou jak vylepšit autentizační metodu je, že místo klasického hesla nebo PINu, přidáme navíc další faktor, např. token. Token je malý předmět, který musí mít klient v držení, aby se mohl přihlásit do své internetové banky. Tokenem může být čipová karta, USB token, mobilní telefon, autentizační kalkulátor. Využívají se certifikáty, jednorázová hesla. Evropské i tuzemské banky se snaží dvoufaktorovou autentizaci klientům nabízet. Můžeme se také 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)

- otisky prstů 
- duhovka 
- sítnice 
- rozpoznávání obličeje 
- geometrie ruky 
- rozpoznávání hlasu 
- dynamika podpisu 
- dynamika psaná na klávesnici

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.

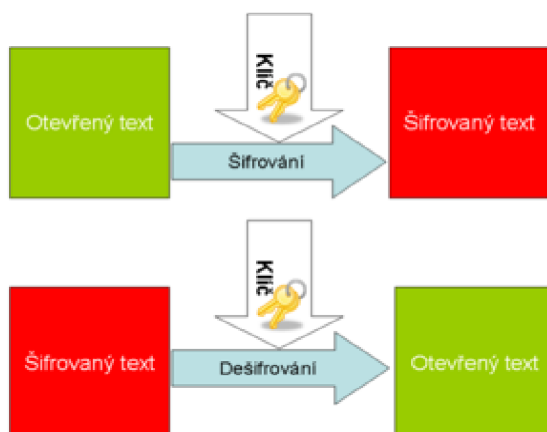
Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Zaručený elektronický podpis je aplikací asymetrické kryptografie (viz 3.2.4). (2, 36)

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 mohou být i stotisíckrát pomalejší. Na druhou stranu velkou nevýhodou je nutnost sdílení tajného klíče, takže se odesílatel a příjemce tajné zprávy musí předem domluvit na tajném klíči. (2)



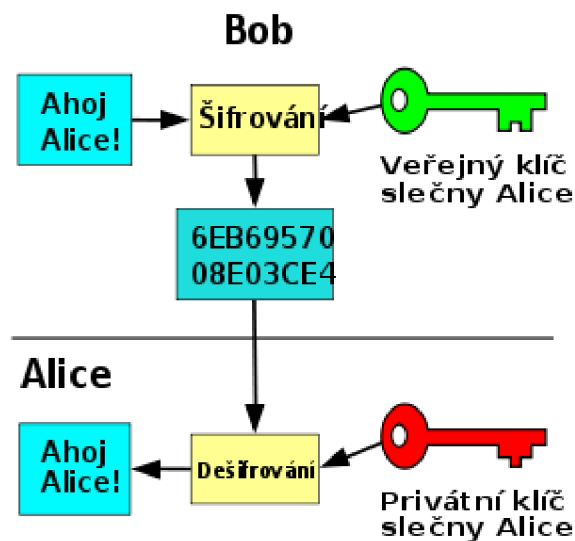
Obrázek 2: Šifrování a dešifrování pomocí jediného klíče

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

Data 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 autentizací 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 (potravin, 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 podobě, 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 než 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 Customer (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 úroveň 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 zboží 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 předvídaní 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 bankovníctví

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) bankovníctví. (14)

„Přímé bankovníctví 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 bankovníctví, 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 bankovníctví 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 bankovníctví 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 bankovníctví 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 bankovníctví

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 zkušenosti 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 bankovníctví 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 bankovníctví, na finanční trh. Charakter služby doznal během její existence mnoha změn, ta nejzásadnější přichází s nástupem digitálních mobilních sítí. (14)

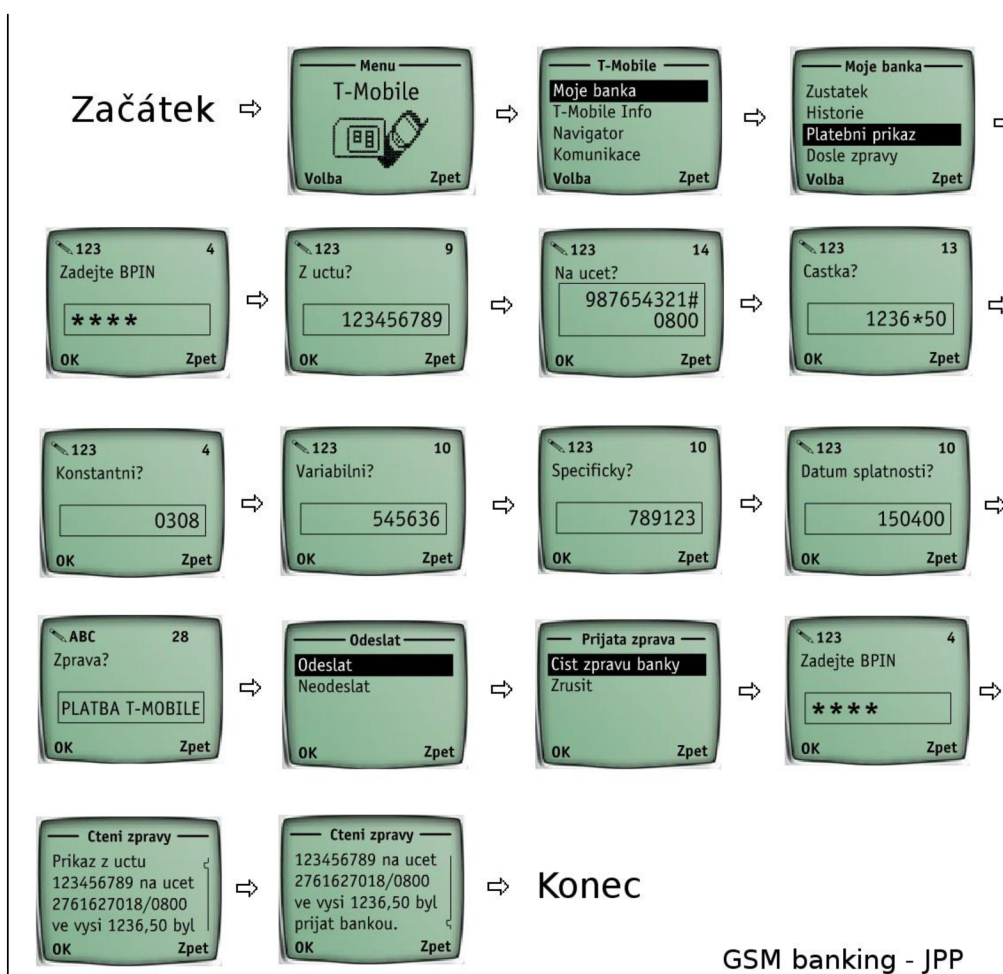
Phone banking byl a stále je pro firemní klientelu vzhledem k objemu prováděných transakcí nepoužitelný. Peněžní instituce tak těmto významným zákazníkům nabídly novou možnost komunikace, označovanou souhrnně jako *homebanking*. Nástup nových generací stolních počítačů a Internetu vedl ke vzniku nové, nejmladší formy elektronického bankovníctví, 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 bankovníctví

GSM Banking

GSM Banking umožňuje ovládat bankovní účet prostřednictvím mobilního telefonu. Obliba této formy přímého bankovníctví 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 aplikaci 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)



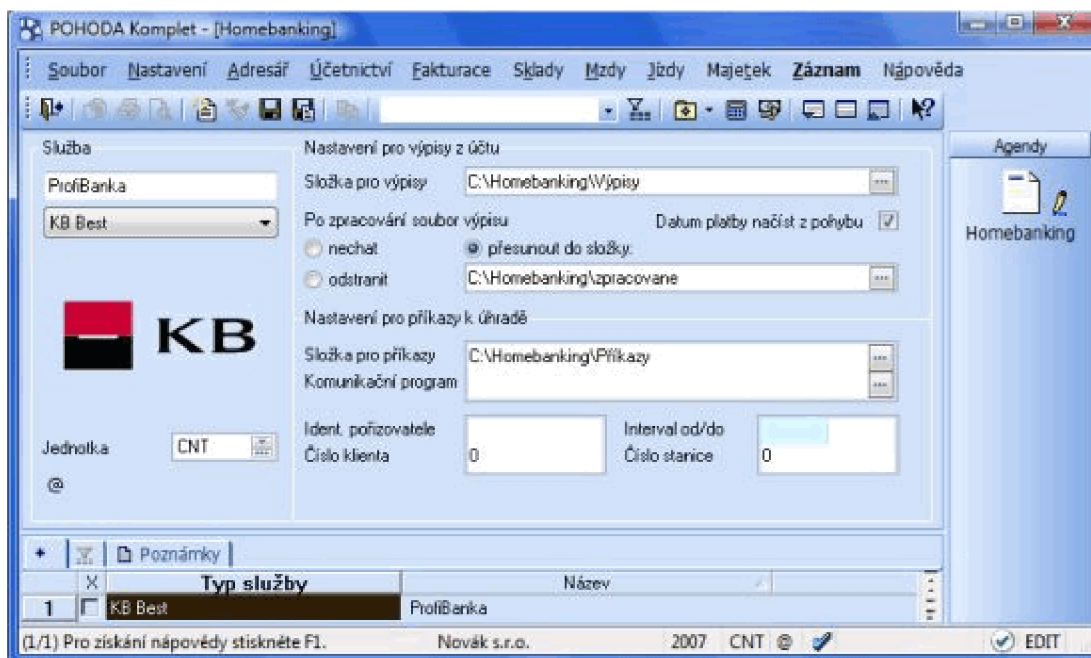
Obrázek 4: GSM Banking: Jednorázový platební příkaz

Zdroj: (43)

Home banking

Home Banking se od klasického internetového bankovníctví 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 bankovníctví, 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

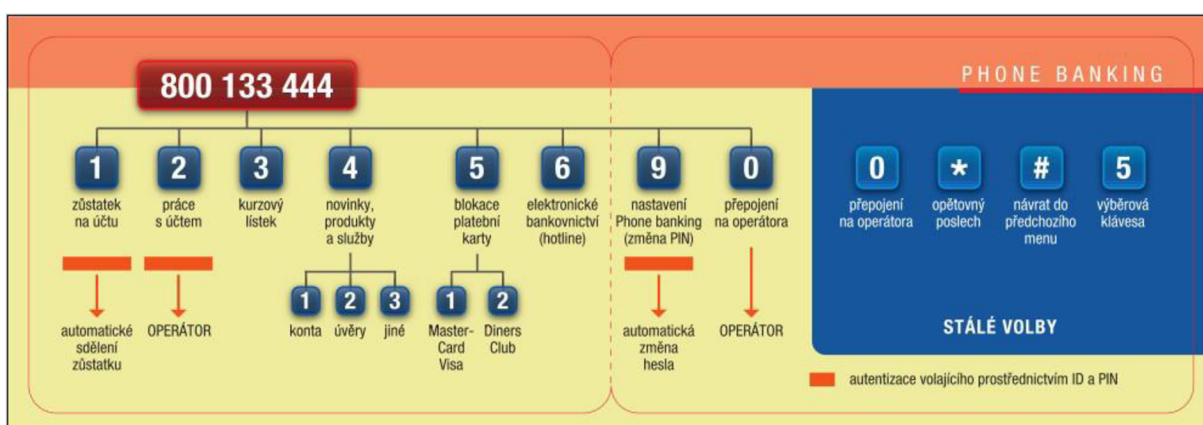
Zdroj: (39)

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

Phone banking

Telefonní bankovníctví 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 bankovníctví byl spuštěn jeho komerční provoz. Internetové bankovníctví, které je chápáno jako nejlevnější alternativa správy bankovního účtu, získalo během své existence nemalé množství věrných klientů. (37)

Uživatel pocítí pohodlí internetového bankovníctví 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)

Platba internetovému obchodu: PayMyway

Číslo účtu: **43-768384023/0100** [nápověda](#)

Číslo protiúčtu: Kód banky protiúčtu:

Částka: CZK

Datum splatnosti:

Variabilní symbol:

Konstantní symbol:

Specifický symbol:

Popis příkazy (zobrazuje se i protistraně):

Popis pro příjemce (zobrazuje se i protistraně): [Oznámení o platbě >>>](#)

Ukončit platbu **Podpis a odeslání...**

Obrázek 7: Internet banking KB

Zdroj: (35)

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

2.4.3. Metody zabezpečení elektronického bankovníctví

„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 bankovníctví. 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 bankovníctví 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 bankovníctví. 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 přihlášení však stojí a padá kvalitou hesla, které je

bud' nově vygenerováno čistě za účelem využití internetového bankovníctví, nebo shodné s přiděleným PIN kódem.

- **Uživatelské jméno a heslo a potvrzovací kód z autentizačního kalkulátoru** – Použití autentizačního kalkulátoru¹ 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 bankovníctví může klient bez rizika využívat jakýkoli počítač, a to i v tolik obávaných internetových kavárnách.



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)

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)

2.4.4. Smartbanking

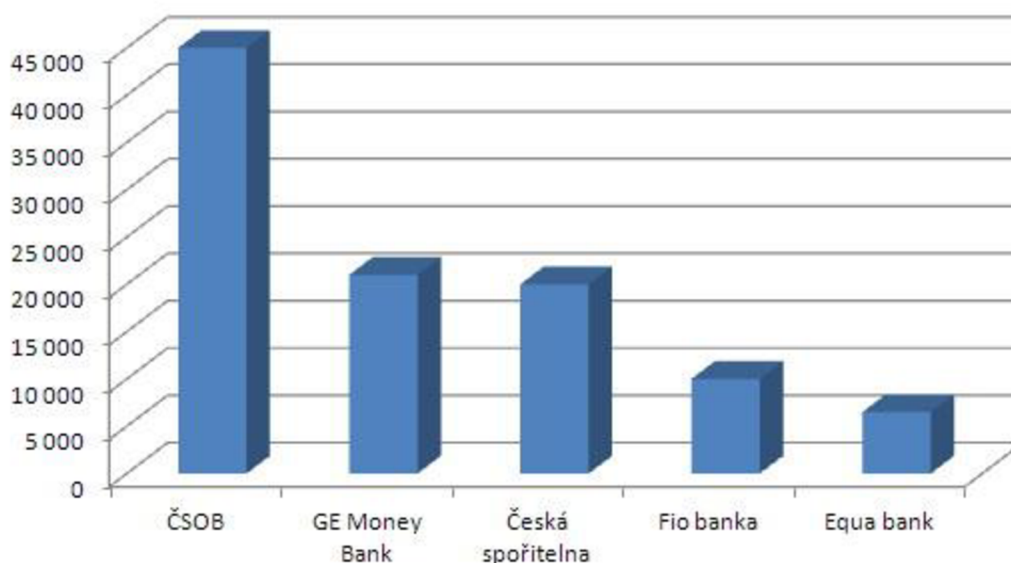
Trendy v posledních letech jsou jednoznačné, stále více telefonů, které se prodají má operační systém (nejčastěji Android, iOS či některý další) a disponují přístupem na internet, což je služba, která se vzhledem ke snižujícím se cenám za připojení a zvyšujícím se požadavkům na přístup k informacím kdykoli 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 bankovníctvím přímo nesouvisí, ale uživatelé 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 2012
Zdroj: (23)

Bezpečnost smartbankingu

Metod zabezpečení aplikace pro mobilní bankovníctví je nepřehledné 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 nepřímoúměrnost dvou veličin. Bezpečnosti a použitelnosti. Čím více je aplikace zabezpečena, tím méně je zpravidla pro uživatele použitelná a příjemná. (23)

První stupeň bezpečnosti

Jedná se pouze o tzv. jednofaktorovou 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 nepoužívanější, ale zároveň velmi omezující metody zabezpečení, patří tzv. White-list, což je seznam předem definovaných účtů, na které lze peněžní prostředky převést. (23)

3. Analýza problému a současné situace

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 Sociétés 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 bankovníctví. 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 bankovníctví 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 Sociétés 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 zbývajících 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. Přímé bankovníctví

3.2.1. Expresní linka

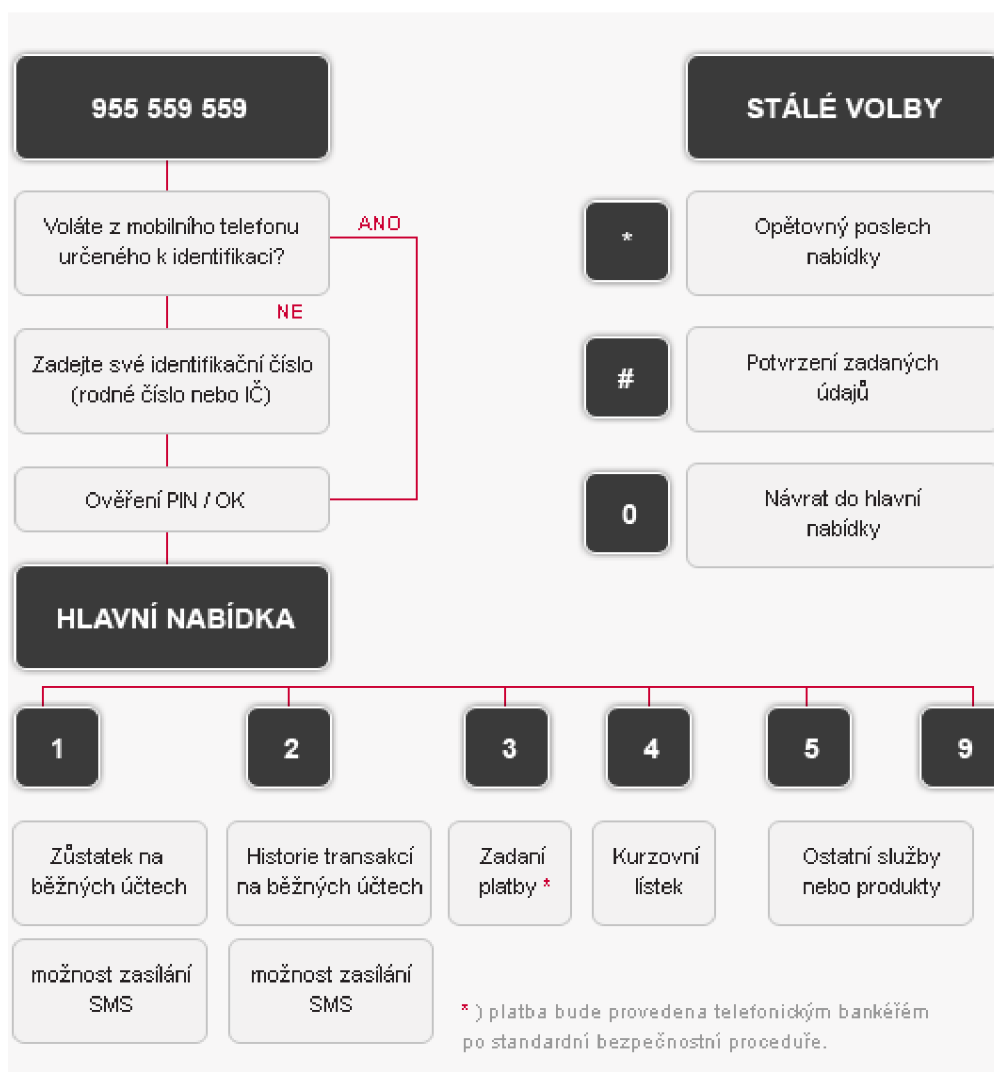
Tato služba přímého bankovníctví je určena zejména občanům a drobným podnikatelům jak nástroj obsluhy svého účtu pomocí telefonu. Dříve bylo volání na expresní linku pro klienty zdarma, nyní je podle nového ceníku zpoplatněna jako klasický hovor na pevnou linku. Výhodou tohoto typu přímého bankovníctví 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 bankovníctví.

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 či zrušení inkasa
- Podání žádosti o vydání platební karty
- Podání žádosti o vydání kreditní karty
- Založení termínovaného účtu
- Obchodování s cennými papíry
- Uzavření smlouvy na penzijní připojištění
- a řadu dalších služeb



Obrázek 10: Schéma Expressní linky
Zdroj: (28)

Bezpečnost Expressní 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.

3.2.2. MojeBanka

Tento produkt dává klientům Komerční banky možnost spravovat svůj účet prostřednictvím internetu skrze webové rozhraní. Tento druh přímého bankovníctví 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 dvoufaktorové 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.



The screenshot shows a login interface with two tabs: 'Certifikát v souboru' and 'Certifikát na čipové kartě'. The active tab is 'Certifikát na čipové kartě'. Below the tabs, there is a text instruction: 'Vložte čipovou kartu do čtečního zařízení a zadejte PIN.' Below this is a text input field labeled 'PIN:'. A red arrow points to the input field, and another red arrow points to the 'Přihlásit' button.

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



The screenshot shows a login interface with two tabs: 'Certifikát v souboru' and 'Certifikát na čipové kartě'. The active tab is 'Certifikát v souboru'. Below the tabs, there is a text label 'Certifikát:' followed by the file path 'C:\KBCertifikat\MAŘÁK_LUBOMÍR.p12'. Below this is a button labeled 'Jiný certifikát'. Below the button is a text input field labeled 'Heslo:' containing several dots. A 'Přihlásit' button is located at the bottom right.

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.

Prostředí aplikace MojeBanka

Po úspěšném přihlášení nám aplikace na úvodní obrazovce zobrazí přehled účtů, vedených u KB, kde okamžitě vidíme stav debetního, popř. kreditního či termínovaného účtu. Přimo z hlavní obrazovky, po kliknutí na tlačítko „Aktuální použitelný zůstatek“ můžeme zjistit použitelné peněžní prostředky daného účtu.

Jedna z nejpoužívanějších funkcí aplikace MojeBanka je výpis transakční historie účtu. Můžeme se k ní dostat jednoduše přímo z úvodní obrazovky nebo z oblíbených položek hlavního menu a nebo po proklikání hlavního menu v nabídce „Přehledy“

The screenshot displays the MojeBanka main interface. On the left is a navigation menu with sections: 'Oblíbené' (Favorites) containing 'Přehled účtů', 'Příkaz k úhradě v CZK', 'Aktuální použitelný zůstatek', 'Transakční historie', and 'Dostupné výpisy'; and 'Hlavní menu' (Main menu) containing 'Přehled účtů', 'Platební příkazy', 'Mobilní služby', 'Dávkové příkazy', 'Trvalé příkazy', 'Inkaso', 'Přehledy', 'Výpisy transakcí', 'eVýpisy', and 'Informace KB'. The main content area is titled 'Přehled účtů' (Account Overview) and shows details for 'MAŤÁK LUBOMÍR'. It lists two accounts: a 'BĚŽNÉ ÚČTY' (Current Account) with IBAN CZ600100000086333820227, a balance of 515 716,16 CZK, and an interest rate of 20,20%; and an 'ÚVĚROVÉ ÚČTY' (Credit Account) with IBAN CZ5401000000513257321357, a credit limit of 200 000,00 CZK, and an interest rate of 0,00%. Each account entry has buttons for 'Profil účtu', 'Aktuální použitelný zůstatek', 'Přehled příkazů', and 'Transakční historie'.

Obrázek 14: Hlavní obrazovka MojiBanky
Zdroj: (28)

Navigační menu

V levém sloupci jsou přehledně seřazeny kategorie menu, pomocí kterých se aplikace snadno ovládá. Nejpoužívanější funkce lze snadno přidat do kategorie „Oblíbené“ a mít tak jednoduchý přístup k hlavním funkcím, bez zdlouhavého proklikávání. Pomocí navigačního menu si můžeme např. zobrazit přehled uzavřených smluv pojištění, spoření či investování a nebo si přes aplikaci přímo zažádat o uzavření smlouvy či sjednání hypotéky.

Hlavní menu

V nabídce hlavního menu se nacházejí všechny nejpoužívanější tlačítka pro ovládání aplikace. Menu je přehledně uspořádáno a seřazeno podle využití. Nachází se zde jedna z nejdůležitějších a nejpoužívanějších funkcí internetového bankovníctví, příkazy k úhradě. Po rozkliknutí nabídky „*Platební příkazy*“ nám aplikace nabídne platební příkazy v CZK, cizí měně, zahraniční platbu, příkaz k inkasu a mnoho dalších.

Položky hlavního menu

- Přehled účtů
- Platební příkazy
- Mobilní služby
- Dávkové příkazy
- Trvalé příkazy
- Inkaso
- Přehledy
- Výpis transakcí
- eVýpisy
- Informace KB

Oblíbené
Hlavní menu
Platební karty
Investování
Spoření a pojištění
Úvěrové obchody
Schránka
Nastavení oznámení
Administrace
Mám zájem o ...
Schůzky v bance
Odhlášení
Certifikační průvodce
Nápověda

Obrázek 15: Navigační menu

Zdroj: (28)

Platební karty

Po kliknutí na odkaz „*Přehled karet*“ přehledně vidíme debetní karty k běžným účtům, vedených u KB. Přes tuto nabídku, jde např. požádat o znovuzaslání PINu, změnit týdenní limity subjektu nebo povolit či zablokovat platby kartou přes internet.

Číslo karty	543 402 ***** 270
Jméno držitele karty	LUBOMÍR MAŤÁK
Typ karty	MC, debetní, embosovaná
Služby	Cestovní pojištění k embosovaným kartám
Platnost karty	12/13
Automatická výměna karty	ANO
Tisk zůstatku z bankomatu	ANO
Status karty	Aktivní
Týdenní limity	Bankomaty 20 000,00 CZK Změnit Obchodníci 20 000,00 CZK Souhrnný 20 000,00 CZK
Platby přes internet	ANO Změnit



Údaje na kartě jsou pouze informativní.

Transakce čekající na zaúčtování

Žádost o znovuzaslání PINu

Obrázek 16: Přehled platebních karet

Zdroj: (28)

Investování

Pomocí tohoto nástroje může uživatel sledovat vývoj hodnot svého portfolia, uzavřít novou smlouvu, operovat s podílovými listy apod. Většina běžných klientů tuto možnost s největší pravděpodobností nevyužije, je však důležité tu možnost mít.

Spoření a pojištění.

Pomocí této nabídky má uživatel možnost sledovat stav svého penzijního fondu, pokud má u KB zřízeno. Dále si pak může online sjednat cestovní pojištění či stavební spoření

Úvěrové obchody

Vcelku zajímavé možnosti skýtá položka „*Úvěrové obchody*“, pomocí kterého si uživatel může např. podat žádost o hypotéku, spotřebitelský úvěr či kreditní kartu a odlehčit a zkrátit si tak zdlouhavou osobní návštěvu pobočky banky.

Schránka

Jedná se o jednosměrnou informační schránku, do které banka posílá nabídky na nové produkty, hlášení výpadků přímého bankovníctví, či změny v obchodních podmínkách.

Nastavení oznámení

V této části aplikace si uživatel sám nastavuje frekvenci, periodu a kanál pro různá oznámení, jako jsou oznámení o platbách, zůstatcích, přečerpání aj.

Administrace

Administrace obsahuje informace o subjektu, uživateli a účtu. Dále je zde možno editovat uživatele, přístupující a obsluhující účty, či přidat zmocněnou osobu.

Mám zájem o...

Velmi šikovně zpracovaná sekce s přehledně uspořádanými dokumenty s informacemi o produktech, o které může uživatel projevit zájem. Jedná se v podstatě o formu cílené reklamy na podporu prodeje jednotlivých produktů.

Schůzky v bance

Intuitivně a účelně zpracovaná aplikace pro sjednávání schůzek se svým osobním bankéřem. Nabízí uživateli možnost volby data a času a stručně bankéři naznačit důvod osobní schůzky.

The screenshot shows a web form for scheduling a meeting. It includes a dropdown for the reason, a text area for a detailed description (max. 250 characters), a date selector set to 09.05.2012, and a time selector for the start (10:00) and end (10:30). A horizontal bar chart shows the time slots from 8:00 to 19:00, with a shaded area indicating the selected meeting time. Below the chart are input fields for the email address (matak.l@centrum.cz), phone number (+420 721262434), and branch address (Merhautova 1, Brno, 63132). The name of the bank advisor, Lenka Brzobohatá, is displayed. At the bottom, there are two buttons: 'Zpětný kontakt' and 'Odeslat návrh schůzky bankovnímu poradci'.

Obrázek 17: Plánování schůzky v bance

Zdroj: (28)

Odhlášení

Klasický odkaz na bezpečné ukončení zabezpečené session. Doporučuje se po skončení aktivity ukončovat aplikaci MojeBanka tímto odkazem, nikoli pouhým zavřením okna prohlížeče.

Certifikační průvodce

Používá se výhradně v případě vypršení platnosti, ztráty či porušení bezpečnosti certifikátu, k vygenerování nového certifikátu. Certifikát se používá k autorizaci uživatele při přihlášení či odesílání plateb (viz kapitola 2.2.5).

Nápověda

Obsahuje základní informace o obsluze aplikace MojeBanka.

3.2.3. Nově připravovaná verze MojeBanka

KB připravuje novou verzi webové aplikace internetového bankovníctví pro obsluhu uživatelských účtů. 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 (viz 3.2.6). 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.

The screenshot displays the KB MojeBanka user interface. At the top, there is a navigation bar with the KB logo, a search bar for products, and utility links like 'Prodloužit', 'Změnit heslo', and 'Odhlásit'. Below this is a secondary navigation bar with tabs for 'Domů', 'Platby', 'Účty', 'Karty', 'Úvěry', 'Spoření a investice', and 'Pojistění'. The main content area is titled 'MojeBanka vás vítá, vaše poslední přihlášení proběhlo ve čtvrtek 18. 6. 2012, 10:22:43'. It features four main account cards for František Koudelka (občan):

- Můj účet** (34-32277676/0100): Běžný zůstatek 43 274,50 CZK. Poslední transakce: 10. 6. 2012 (-998,00 CZK), 9. 6. 2012 (-1 678,00 CZK), 6. 6. 2012 (+33 456,98 CZK).
- Optimální půjčka** (65-1087345672/0100): Výše příští splátky 4 573,67 CZK. Zbývající částka ke splacení 278 234,68 CZK. Datum příští splátky 3. 8. 2013.
- Lady karta** (98-2354769809/0100): Čerpaná částka 4 520,98 CZK, Limit kreditní karty 50 000,00 CZK. Poslední zaúčtované transakce: 12. 6. 2012 (-230,00 CZK), 10. 6. 2012 (-1 240,00 CZK), 9. 6. 2012 (-3 050,98 CZK).
- KB Spořicí konto** (28-1204637829/0100): Běžný zůstatek 35 687,54 CZK. Poslední transakce: 13. 6. 2012 (-1 500,00 CZK), 11. 6. 2012 (+5 000,00 CZK), 9. 6. 2012 (+2 500,00 CZK).

At the bottom, there are sections for 'Schránka' (Máme pro vás připravený...), a promotional banner 'S námi se nemusíte bát bydlet ve vlastním', and 'Oblíbené' (Příkaz k úhradě, Trvalý příkaz, Dobití mobilu, Historie transakcí, Výpis transakcí, Elektronické žádosti).

Obrázek 18: Připravovaná verze MojiBanky

Zdroj: (28)

3.2.4. Mobilní banka

Mobilní banka, je služba přímého bankovníctví, 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 bankovníctví 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 1: 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)

Aktivace služby

Aktivace služby probíhá u telefonního bankéře na Expresní lince KB. Uživatel při aktivaci zadává:

- telefonní číslo pro zaslání SMS s internetovou adresou,
- jazykovou verzi
- denní bezpečnostní limit pro aktivní operace.

Telefonní bankéř uživateli sdělí aktivační kód, který uživatel musí zadat při prvním přihlášení do aplikace Mobilní banka. Po obdržení SMS si může uživatel stáhnout aplikaci ze zasláné adresy URL. Tímto je aplikace připravena k prvnímu použití. Službu Mobilní banka je možné aktivovat i bez zaslání aplikace na mobilní zařízení klienta. V tom případě zadá uživatel pouze jazykovou verzi a bezpečnostní limit, a ke svým účtům přistupuje z mobilního zařízení jiného uživatele, který má službu Mobilní banka aktivovanou a aplikaci stáhnul (např. manžela/manželky). Každý z uživatelů zadává své bezpečnostní prvky pro Expresní linku. (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 19: Mobilní banka – přihlášení
Zdroj: (28)



Obrázek 20: Mobilní banka – přehled
Zdroj: (28)

Následná přihlášení do aplikace

Uživatel je vždy vyzván nejprve k zadání svého identifikačního čísla pro Expresní linku KB. Aplikace si pamatuje poslední zadané identifikační číslo a zobrazuje ho při dalším přihlášení. Podle zvoleného typu bezpečnosti na Expresní lince KB (PIN+heslo nebo OPK) je zobrazena buď tabulka pro zadání náhodně vybraných znaků z PINu a hesla, nebo tabulka pro zadání odpovědi OPK. Po vyplnění znaků odešle uživatel zadané údaje do banky stisknutím tlačítka „Přihlásit se“. Proběhne ověření správnosti zadaných údajů a poté je zobrazen formulář pro výběr obsluhovaného subjektu.

Během přihlášení může uživatel využívat veškerých nabízených služeb v rozsahu svého oprávnění (bezpečnostního limitu) a smluvních vztahů s Komerční bankou. V rámci jednoho přihlášení však nemůže službu využívat více uživatelů zároveň, byť by měli oprávnění k nakládání se stejnými účty - pro takový případ se každý z nich musí přihlásit za použití svých bezpečnostních prvků. Jestliže uživatel neprovede po dobu 10 minut žádnou akci, která by požadovala data z banky (např. dotaz na zůstatek, historii transakcí...) nebo data do banky předávala (např. odeslání příkazu,...), bude přihlášení ukončeno z důvodu bezpečnosti. Pro pokračování je potřeba se přihlásit znovu. Pro odhlášení se z aplikace se používá tlačítko „Odhlásit se“ v hlavním menu. Přihlášení se ukončí i uzavřením aplikace v mobilním telefonu.

Chybné pokusy o přihlášení

Při chybném zadání údajů se čítač chybných pokusů o přihlášení zvýší o jeden, a systém se vrátí na přihlašovací stranu a umožní uživateli další pokus, kterých má maximálně 3. V případě, že uživatel uzavře aplikaci, aniž by se korektně přihlásil, počet chybných pokusů se nenuluje.

Počet chybných pokusů o přihlášení se nuluje okamžikem korektního přihlášení do Mobilní banky, nebo znovu zaktivováním zablokovaného přístupu uživatele do Mobilní banky. Odblokování lze provést pouze prostřednictvím Expresní linky KB po průchodu bezpečnostní procedurou.

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

Příkaz k úhradě

Ty 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.

Dobití telefonu

Prostřednictvím této volby je možné zadat příkaz na dobítí kreditu předplacené SIM karty mobilních operátorů.

Platba faktury za telefon

Tato volba slouží tarifním zákazníkům mobilních operátorů pro platbu faktur za telekomunikační služby a pro další typy plateb.

Šablony

Pro snazší zadávání příkazů k úhradě je možné použít připravené šablony platebních příkazů. Funkci je možné využít pouze pro běžné účty vedené v CZK.

Zbývající limit

Podmínkou úspěšného odeslání platebních příkazů ke zpracování bankou, je dostatečný bezpečnostní limit uživatele a dostatečný použitelný zůstatek účtu.

Přehledy

Transakční historie

Je možné získat přehled o zúčtovaných transakcích na vybraném účtu a dále si zobrazit detail jednotlivé položky.

Blokace z operací PK

Je možné získat přehled o dosud nezaúčtovaných transakcích pořízených platební kartou a dále si zobrazit detail vybrané položky.

Jiný účet/subjekt

Výběr subjektu a Výběr účtu

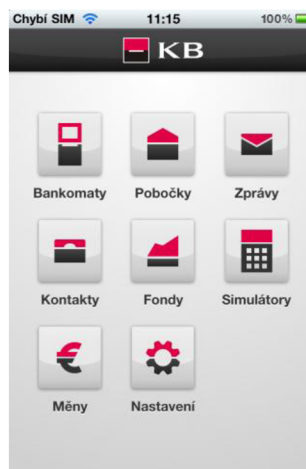
Slouží pro změnu aktuálně vybraného subjektu nebo účtu. Pokud uživatel obsluhuje pouze jeden subjekt, po stisknutí volby Výběr subjektu se zobrazí informující hláška.

3.2.5. 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. Bylo tomu tak zejména z důvodu chybějících součástí mobilního bankovníctví. Aplikace v základní verzi nenabízela svým klientům žádným, ani omezeným způsobem kontrolu nebo obsluhu svých produktů. Vzhledem k tomu, že je KB, a.s druhou největší bankou v ČR, očekává se od ní, že součástí nabízených služeb, bude kvalitní mobilní bankovníctví. Bohužel tomu, až do konce května 2012, nebylo. KB byla jednou z posledních větších bank, která tuto službu pro chytré telefony nenabízela.

Aplikace rozhodně nedělala dobré jméno svému názvu. S mobilní bankou neměla téměř nic společného. Základem mobilního bankovníctví, 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. K dispozici byly následující položky:

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



Obrázek 21: Hlavní obrazovka
Zdroj: (28)

Bankomaty

Pro mnohé nejpoužívanější funkce aplikace. Pomocí polohových služeb zobrazuje nejbližše položené bankomaty, u nich nejmenší vydávanou bankovku a adresu.

Pobočky

Naprosto redundantní položka v menu. Zobrazuje pobočky stejným způsobem jako předešlá funkce. Informace o poloze bankomatů a poboček lze sloučit do jednoho menu a řešit např. barevným rozlišením nebo různou ikonou pro bankomat a pobočku.



Obrázek 22: Pobočky
Zdroj: vlastní

Zprávy

Tato položka v sobě skrývá tiskové zprávy, ekonomické analýzy a různé nabídky pro klienty. Nejedná se o schránku s osobní komunikací mezi bankou a klientem, nýbrž o jakousi formu zpravodajské části aplikace.

Kontakty

V této části jsou přehledně seřazeny důležité kontaktní informace od infolinky přes kontakt pro zablokování platební karty až po clientskou linku přímého bankovníctví.

Fondy

Grafická část aplikace, zobrazující vývoj fondů KB Amundi a IKS. Zobrazená data jsou pouze informativního charakteru a nelze je přímo využít k nákupu či zobrazení svého portfolia.

Simulátory

Tato část umožňuje nasimulovat uzavření hypotečního či osobního úvěru a poskytně uživateli lehký informativní základ o úroku, výši měsíční splátky a době splácení podle uživatelem vyplněných dat.

Měny

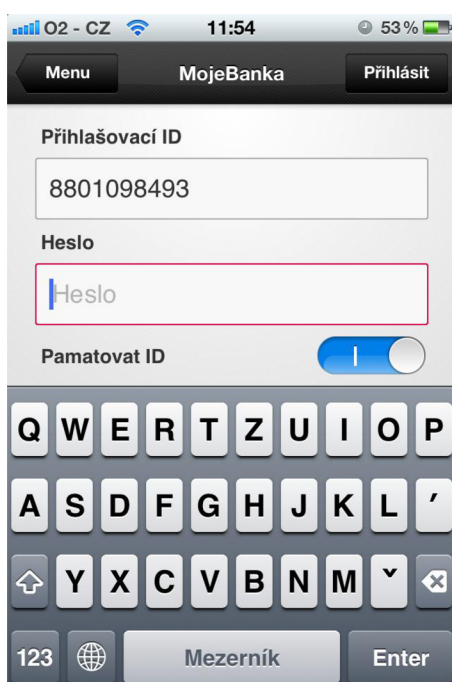
Podobně jako odkaz „*Fondy*“ zobrazuje vývoj kurzu měn vůči české koruně. K dispozici je i konvertor, pomocí kterého lze lehce převést jednu měnu na druhou.

Nastavení

Zajímavou funkcí, kterou nastavení nabízí, je vyhledávání bankomatů konkurenčních bank. Změna motivu vzhledu aplikace je zanedbatelnou položkou nastavení.

3.2.6. Mobilní banka 2 - nová verze

Vývojáři KB usilovně pracují na vydání nové verze aplikace Mobilní banka 2, která bude eliminovat největší nedostatek původní verze, a to absenci zabezpečeného přístupu k individuálním uživatelským účtům. Plánované vydání nové verze se připravuje na 25.5.2012. Komerční banka je jedna z posledních tuzemských bank, která možnost obsluhy svých účtů skrze „chytrý“ telefon dosud nenabízí. 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 bankovníctví. V současné době je tato služba klientům nabízena zdarma.



Obrázek 24: MB2 – přihlášení
Zdroj: vlastní



Obrázek 23: MB2 - hlavní obrazovka
Zdroj: vlastní

Přihlášení do zabezpečené sekce

Pro přihlášení do zabezpečené sekce, je nutno mít k dispozici následující údaje:

Přihlašovací ID - Bude přiděleno bankou. Ve většině případů, se bude jednat o rodné číslo majitele účtu, z důvodu snadné zapamatovatelnosti. U uživatelů bez rodného čísla, bude přihlašovací ID generované bankou.

Heslo - Přihlašovací heslo si uživatel zvolí po aktivování služby v internetovém bankovníctví, kde jej může zároveň libovolně měnit. Heslo musí obsahovat 6 znaků, výrazně se však doporučuje zvolit heslo alespoň o 8 znacích s obsahem malých písmen, velkých písmen, speciálního znaku a alespoň jedno čísla.

Funkce aplikace

Po přihlášení do zabezpečené sekce nám aplikace na úvodní obrazovce přehledně zobrazí běžný a aktuální použitelný zůstatek a nabídne zadání platby, zobrazení historie, či vypsání přehledu zůstatků. Přetažením obrazovky vlevo či vpravo může uživatel přepínat mezi jednotlivými produkty jako je debetní, kreditní či termínovaný účet.

Platba

Uživatel si nejdříve zvolí, s jakým účtem chce pracovat a poté si z přednastavených čísel účtů zvolí příjemce platby. Poté zvolí částku a datum splatnosti. To vše nabízí základní nabídka. Po rozkliknutí odkazu „*Více detailů*“, nám aplikace nabídne vyplnění identifikačních údajů, jako je variabilní, konstantní a specifický symbol. Dále je možno vyplnit políčka „*Zpráva pro mě*“ a „*Zpráva pro příjemce*“. Jako poslední lze zvolit, zda chce uživatel dostat oznámení o platbě formou sms nebo e-mailu, tato položka je však nepovinná. Po stisknutí tlačítka pokračovat se zobrazí kontrolní obrazovka se všemi vyplněnými údaji a zbývajícím bezpečnostním limitem. Pro odsouhlasení a odeslání platby, slouží tlačítko potvrdit, po jehož zmáčknutí aplikace vyzve k zadání autorizačního hesla.

Historie

Jednoduchý, ale velice přehledný a uživatelsky přívětivý seznam zaúčtovaných odeslaných a přijatých plateb. Jedná se o platby, tedy příkazy, které jsou ve stavu „*zaúčtovaný*“ a zároveň prošli nočním zúčtováním, tedy ovlivnily účetní zůstatek účtu. V základním zobrazení jsou vidět informace o čísle účtu, částce, datu zaúčtování a popisu. Po rozkliknutí jednotlivých záznamů se pak navíc zobrazují informace o variabilním, konstantním a specifickém symbolu. Seznam historie lze filtrovat podle čísla účtu, kódu banky či data zaúčtování.

Přehled příkazů

Jedná se o přehled zadaných plateb s různými stavy. Nemusí se vždy jednat o zaúčtované platby, ale třeba o platby, které mají splatnost až v budoucnu, čekají na dalšího autorizátora nebo jsou zamítnuté ze strany banky a nebo je uživatel smazal sám.

Mobilní služby

Tato položka jednak nabízí dobítí kreditu předplacených telefonních karet pro tři největší tuzemské operátory v rozsahu 200 – 9900,- Kč, druhá umožňuje provést platbu za fakturu u operátora Vodafone.

Čekající transakce

Jedná se o právě provedené transakce, které čekají na zaúčtování a poté jsou automaticky přesunuty do „*Historie*“.

Tenký klient

Jedná se o webovou stránku, která je přizpůsobena malému displeji telefonu. Dostupné jsou v podstatě všechny služby jako v aplikaci, pouze s několika malými omezeními. Současná a po vydání i nová verze je dostupná na www.mobilnibanka.cz.

Výjimky v tenkém klientovi

- není kartičkový přehled, ale řádkový (v prohlížeči nejdou využívat nativní funkce, které daný telefon poskytuje přímo pro na míru ušitou aplikaci)
- není k dispozici „picker“ pro výběr měny v kalkulačce kurzů

3.2.7. Jiné nástroje přímého bankovníctví

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.

Služby produktu Profibanka

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 bankovníctví 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 předvyplněný 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 třídní čekací lhůta pro převod peněz z účtu na účet.

Nezbytnosti ke zřízení MojePlatba

- internetové bankovníctví MojeBanka
- platný průkaz totožnosti
- osobní certifikát

3.3. Bezpečnost přímého bankovníctví KB

Problematika bezpečnosti přímého bankovníctví 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.

3.3.1. Bezpečnost internetového bankovníctví KB

Komerční banka vsadila na poměrně silnou, třífaktorovou 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 lokace. 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.

3.3.2. Bezpečnost mobilního bankovníctví 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 bankovníctví 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 malá.

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 zavrhlí jakýkoli další prvek autentizace jako např. kalkulačku na challenge – response nebo obdobu certifikátu jako u internetového bankovníctví. 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.

3.3.3. Internetové bankovníctví vs. mobilní bankovníctví

Z technického hlediska je Mobilní banka bezpečnější, protože není triviální záležitost dostat na zařízení oběti útočníkův škodlivý kód. Na Androidu i na 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.

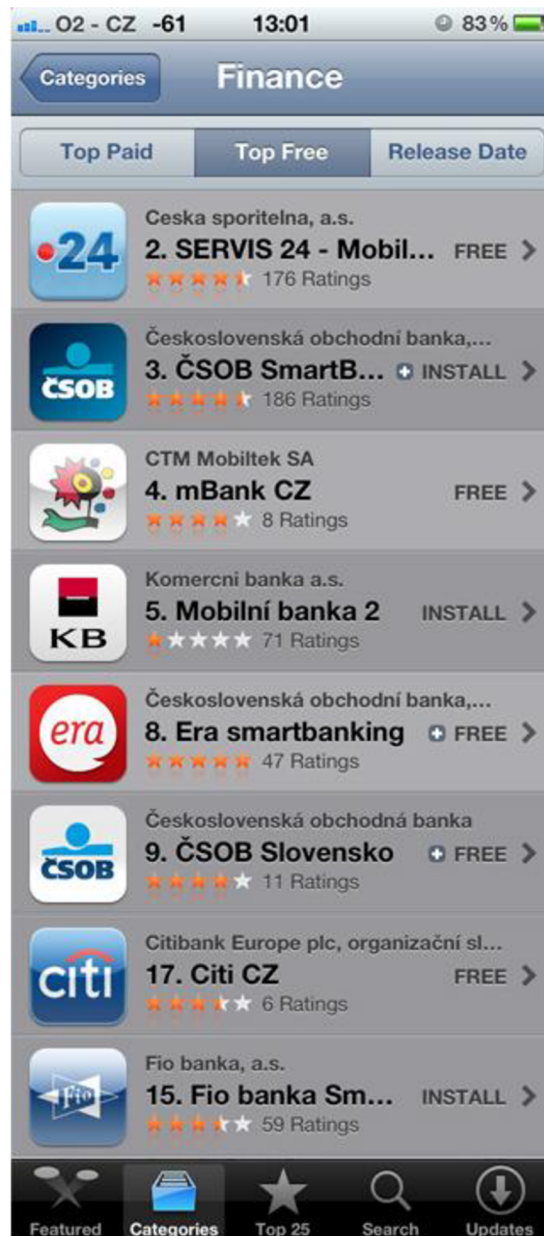
Z pohledu uživatelského je bezpečnější internetové bankovníctví a to hlavně z důvodu několika bezpečnostních prvků. Když uživatelská zodpovědnost selže na dvou stupních, stále existuje možnost odražení útoku, kdežto u mobilního bankovníctví stačí zadávat heslo v přítomnosti útočníka, který jej odposlouchá a pak pro něj v mnoha případech není problém zařízení odcizit a zneužít. Toto prozatím řeší White-list, ale pokud bude chtít banka tento, pro někoho mnohem nepříjemnější bezpečnostní prvek, než třeba Trading Key, odstranit, bude muset vymyslet jinou alternativu zabezpečení.

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. Vlastní návrh řešení, přínos návrhu řešení

4.1. Srovnání s konkurencí

Jak již bylo mnohokrát řečeno, smartbanking Komerční banky velmi zaostával za konkurencí. Ostatně následující obrázek pořízený z AppStore, před vydáním plnohodnotné, verze to jen dokazuje.



Obrázek 25: Seznam dostupných smartbankingových aplikací
Zdroj: vlastní

4.1.1. Fio banka

Fio banka byla první bankou, která na českém trhu nabídla nativní aplikaci pro smartbanking. Od jejího vydání z konce května 2011 byla aplikace 4x aktualizována. Aplikace prozatím eviduje cca 11 tisíc stažení a zhruba polovina uživatelů používá aktivní přístupy k účtu. Současná verze má dvě části. Otevřenou a uzavřenou. Podobně jako u aplikace Komerční banky, nabízí otevřená část informace o pobočkách a bankomatech (pod jedním odkazem), ale bohužel nemá integrovanou mapu a je nutno každou pobočku nebo bankomat zobrazovat zvlášť a neustále přepínat mezi aplikacemi Fio a Google maps. Dále pak obsahuje kalkulačku poplatků a důležité kontakty.

Pokud chce uživatel obsluhovat své účty, musí se nejprve přihlásit. Před prvním přihlášením je nutné smartbanking aktivovat v internetovém bankovníctví. Přístup do zabezpečené části aplikace je zajištěn loginem a heslem, které si uživatel zvolí ve svém internetbankingu. Pro jednoznačnou identifikaci telefonu, ze kterého bude k účtu přistupováno, se uvádí unikátní číslo telefonu UDID u iOS a IMEI u Androidu. Transakce se navíc potvrzuje PINem, který se volí tamtéž.

Po přihlášení do zabezpečené části, pak může uživatel aktivně nakládat se svými účty. Aplikace mu nabízí přehledy zůstatků na všech aktivních účtech, historii transakcí na vybraném účtu až 3 měsíce zpět nebo třeba detail transakce na účtu s možností opakování odchozí platby. Dále pak má uživatel možnost zadávat převody mezi vlastními účty, zadávat jednorázové platební příkazy v CZK v rámci ČR a v EUR na Slovensko na jakákoli čísla účtů. Může si také vypsát přehled čekajících nebo neuskutečněných plateb.

- + první na trhu
- neintegrovaná mapa
- nekompatibilní s iPhone 3G a iPad

Hodnocení: 70%

zablokuje. Odblokování lze provést v nastavení internetového bankovníctví. Aplikace umožňuje provádět platby na jakákoliv čísla účtů v ČR, které umí přijímat standardní bezhotovostní platby.

- + skenování složenek
- absence několika funkcí
- chudá nabídka veřejně dostupných informací
- fatální chyba aplikace - po 14 dnech používání se nelze připojit

Hodnocení: 60%

4.1.3. Československá obchodní banka

ČSOB vydala aplikaci pro smartbanking začátkem roku 2012 a v polovině dubna téhož roku, už aplikaci používalo přes 28 tisíc uživatelů a zaznamenáno bylo přes 45 tisíc stáhnutí. Design aplikace je na pohled příjemný. Na rozdíl od konkurenčních aplikací tohoto typu, se uživatel vždy vrací na úvodní obrazovku. Z tohoto důvodu, je zde zobrazeno 12 různých tlačítek pro obsluhu aplikace, což je, s porovnáním s konkurenčními aplikacemi, nejvíce. Zabezpečené části jsou od volně přístupných před přihlášením, rozlišeny malým symbolem zámku v rohu každé ikony. Zajímavou funkcí je možnost návrhu vzhledu platební karty přímo z fotoaparátu mobilního telefonu. Jinak aplikace nabízí velmi podobné funkce jako konkurenční klienti.



Obrázek 28: ČSOB smartbanking
Zdroj: vlastní

Aktivace je možná pouze pro klienty služby ČSOB InternetBanking 24 s SMS klíčem a lze ji provést přímo v aplikaci stisknutím tlačítka „Aktivovat“. Pro aktivaci je nezbytné zadat identifikační číslo, PIN a SMS klíč. K následným přihlášením postačí identifikační číslo a PIN, kterým se zároveň potvrzují všechny platby. Bez zadání PINu, nebude žádná transakce autorizována a následně zpracována.

- + příjemné ovládání
- absence několika funkcí

Hodnocení: 90%

4.1.4. ERA Poštovní spořitelna

Vzhledem k tomu, že Poštovní spořitelna patří do skupiny ČSOB je její aplikace, až na barevné schéma, naprosto totožná s aplikací Československé obchodní banky. V březnu roku 2012 aplikace evidovaly dohromady 45 tisíc stáhnutí a 28 tisíc aktivních uživatelů.

- + příjemné ovládání
- absence několika funkcí

Hodnocení: 90%

4.1.5. UniCredit Bank

Společnost s hrdostí na svých webových stránkách uvádí, že byla první na českém trhu, jež uvedla aplikaci pro smartbanking. Aplikaci vydala v říjnu 2011, ale společnost FIO, uvedla svou aplikaci o několik měsíců dříve. Pro neklienta UniCredit je ale aplikace naprosto nepoužitelná. V nezabezpečené části jsou pouze tři ikony, odkazující na webové stránky banky. UniCredit jako první a zatím jediná banka, nabízí aplikaci i pro jiné operační systémy, než iOS a Android a to konkrétně pro Symbian, Blackberry a nově také pro Windows Phone.

Pro první přihlášení je nezbytné zadat šestnáctimístný bezpečnostní kód, který uživatel obdržel v SMS a uživatelské číslo klienta totožné s číslem pro přihlášení do internetového bankovníctví. Poté si uživatel zvolí bezpečnostní šestimístný PIN, který je pro další používání aplikace jediným autentizačním prvkem.

Aplikace pro své klienty nabízí informace o:

- přehledu účtů a jejich zůstatků,
- historii pohybů na účtech (maximálně jen 60 dnů),
- tuzemské platby,
- zahraniční platby,
- konverzi cizí měny mezi vlastními účty (novinka),
- přehled karet
- historii pohybů na kartách,
- informace o aktuálních kurzech měn,
- mapu poboček a bankomatů

Nabídka služeb je vcelku štedrá, aplikace je přehledná a rychlá a jako jedna z mála dokáže zobrazit historii kreditních transakcí.

- + podpora různých operačních systémů
- nepřehledné ovládání

Hodnocení: 80%

4.1.6. GE Money Bank

Velkou chybou hned při startu aplikace, je žádost o povolení polohových služeb. V případě, že uživatel zjištění polohy zakáže, je mu funkce na zjištění polohy bankomatu či pobočky vcelku k ničemu. V opačném případě povolené polohové služby spotřebovávají energii baterie závratným způsobem.

Celkově aplikace působí, jako modifikované internetové bankovníctví, přeepsané do jiného programovacího jazyka. Stejně jako v mobilní verzi internetových stránek je i aplikace schopna:

- kontrolovat zůstatky na svém účtu,
 - odeslat platbu
 - aktivovat platby na internetu ke své kartě,
 - informace o nabídce produktů a služeb,
 - aktuální kurzy měn s jednoduchým převodníkem,
 - kalkulačky výše měsíční splátky hypotéky nebo Expres půjčky,
 - kontakty a telefonní čísla.
-
- špatné ovládání polohových služeb
 - méně přehledná

Hodnocení: 50%

4.1.7. mBank

V první verzi aplikace, byla velkým nedostatkem možnost provádět pouze pasivní operace, tzn. operace, při níž není vyžadována autorizace. Tyto informace samozřejmě poskytuje pouze přihlášeným uživatelům. V další verzi již aplikace podporovala zasílání plateb, ale pouze na předdefinované účty a v nejnovější verzi aplikace, bylo již i toto omezení odstraněno. Aplikace zobrazuje přehledy produktů, informace o aktuálním použitelném zůstatku nebo třeba transakční historii.

Přehled funkcí aplikace mBanka smartbanking:

Osobní a podnikatelské účty

- Přehled a detaily ke všem osobním, podnikatelským a spořicímu účtům
- Platební příkazy
- Detaily jednotlivých účtů
- Historie transakcí

- Nezaúčtované transakce
- Blokace plateb
- Plánované transakce
- Trvalé platební příkazy
- Inkaso / SIPO

Platební karty

- Přehled a detaily platebních karet
- Autorizační limity dle částky a počtu
- Transakční historie
- Nezaúčtované transakce na platebních kartách
- Blokace plateb
- Provedení on-line splátky na kreditní kartě a zobrazení detailů smlouvy
- Detaily úvěrových produktů
- Parametry úvěrového produktu
- Blokace přístupových kanálů
- Seznam a mapa obchodních míst, kontaktní údaje mBank
- Hotovostní úvěry, hypotéky

Mobilní aplikace je vytvořena speciálně pro mobilní zařízení firmy Apple (iPad nebo iPhone) a další značky telefonů nepodporuje. Aplikace je dostupná zdarma a v podstatě nabízí přístup k vybraným funkcím internetového bankovníctví. Je přehledná, intuitivní a příjemně ovladatelná.

- + přehledné ovládání
- absence několika funkcí
- vysoký počet „bugů“

Hodnocení: 50%

4.1.8. Citibank

Mobilní aplikace Citi Mobile zobrazuje stav a historii běžných a spořicíh účtů, termínovaných vkladů, investic, osobní půjčky a kreditních karet. Umožňuje převody mezi vlastními účty v české i cizí měně, platby v rámci Citibank ČR a tuzemské platby do ostatních bank. Uživatel si může založit termínovaný vklad, který nabízí oproti pobočce výhodnější sazbu. Ke standardní výbavě aplikace patří také vyhledání nejbližších bankomatů a poboček.

Přístup ke svému bankovnímu účtu mají klienti po přihlášení pomocí SMS klíče, doručeného na mobilní telefon, či pomocí tradičního osobního klíče. Po přihlášení se objeví hlavní menu aplikace v podobě pěti ikon:

- Účty
- Převody
- Termínované vklady
- Kurzy
- Nastavení

Pro někoho zajímavou funkcí je, že aplikace umí rozpoznat obchody v aktuálním okolí, ve kterých je možno uplatnit slevu k Citi kreditní kartě.

- + seznam obchodů s uplatnění slevy
- nepřehledné ovládání

Hodnocení: 60%

4.2. Výsledné hodnocení

Nejlépe hodnocená a tudíž největším konkurentem Mobilní Banky 2, je aplikace pro mobilní bankovníctví Československé obchodní banky. Aplikace nabízí široké portfolio služeb a přitom si zachovává přehlednost a uživatelskou přívětivost. I přesto ale obsahuje spoustu nedostatků, na kterých se dá stavět konkurenční strategie.

Tabulka 2: Výsledné hodnocení

Banka	Hodnocení
Fio	70%
Česká spořitelna	60%
ČSOB / ERA	90%
UniCredit	80%
GE Money Bank	50%
mBank	50%
Citibank	60%

Zdroj: vlastní

4.3. Zhodnocení nové verze Mobilní Banky 2

Komerční banka sice přichází na trh mobilních aplikací s plnohodnotným produktem jako jedna z posledních, ale o to víc si dává záležet na kvalitě zpracování, funkčnosti a použitelnosti aplikace. Tuto pozici nebere jako nevýhodu. Naopak se jí 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. 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.

4.4.1. Odstranění White-listu

Za nejvýznamnější považuji v co nejkratší možné době odstranění, resp. nahrazení bezpečnostního prvku White-list, jehož přítomnost výrazně snižuje použitelnost aplikace a posouvá ji do průměru.

4.4.2. Investiční portfolio

Mezi významné funkce patří sledování vývoje svého portfolia přímo v aplikaci mobilního telefonu. Základním kamenem je sledování vývoje investičního životního pojištění Vital Invest, které investuje prostředky do různě rizikových IKS fondů Komerční banky, ale samozřejmě i jiných, jako je třeba penzijní fond.

4.4.3. 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 zasláný, elektronicky podepsaný dokument, potvrzující odeslání platby na konkrétní účet, s možností okamžitého zaslání tohoto dokumentu protistraně.

Závěr

Mobilní bankovníctví 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.

Celá práce byla směřována do hodnocení hlavně technické stránky služeb banky. Bankovníctví 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 4.1 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 z osmi 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, druhá 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 šesti bank. Jedná se o maličkosti, ale právě tyto maličkosti dnes hrají významnou roli v konkurenčním boji o klienta.

Seznam použité literatury

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 bankovníctví 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. ISBN 80-247-1278-4.
- (14) PŘÁDKA M., KALA, J. *Elektronické bankovníctví*. 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.

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. *Účastníci 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 síti 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 bankovníctví 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 bankovníctví*. [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 bankovníctví*. [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 bankovníctví 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.

Seznam obrázků a tabulek

Seznam obrázků

Obrázek 1: Biometrické technologie	15
Obrázek 2: Šifrování a dešifrování pomocí jediného klíče.....	16
Obrázek 3: Asymetrické šifrování	17
Obrázek 4: GSM Banking: Jednorázový platební příkaz	29
Obrázek 5: Home banking	30
Obrázek 6: Phone banking: Nabídka hlasového stromu	31
Obrázek 7: Internet banking KB	32
Obrázek 8: Autentizační kalkulatory	34
Obrázek 9: Počet klientů smartbankingu podle bank k dubnu 2012	36
Obrázek 10: Schéma Expresní linky.....	40
Obrázek 11: Minimální požadavky na systém.....	41
Obrázek 12: Certifikát v souboru.....	42
Obrázek 13: Certifikát na číspové kartě	42
Obrázek 14: Hlavní obrazovka MojiBanky	43
Obrázek 15: Navigační menu	44
Obrázek 16: Přehled platebních karet.....	44
Obrázek 17: Plánování schůzky v bance	46
Obrázek 18: Připravovaná verze MojiBanky.....	47
Obrázek 19: Mobilní banka – přihlášení.....	50
Obrázek 20: Mobilní banka – přehled	50
Obrázek 21: Hlavní obrazovka	53
Obrázek 22: Pobočky	54
Obrázek 23: MB2 - hlavní obrazovka.....	56
Obrázek 24: MB2 – přihlášení.....	56
Obrázek 25: Seznam dostupných smartbankingových aplikací	63
Obrázek 26: Chybné skenování složenek	65
Obrázek 27: Správné skenování složenek	65
Obrázek 28: ČSOB smartbanking.....	66

Seznam tabulek

Tabulka 1: Minimální konfigurace telefonu	48
Tabulka 2: Výsledné hodnocení	72