Technická univerzita v Liberci
Hospodářská fakulta

DIPLOMOVÁ PRÁCE

2008 Denisa Zavadilová

Technická univerzita v Liberci
Hospodářská fakulta

Studijní program: 6208 - Ekonomika a management
Studijní obor: Podniková ekonomika

Internetové bankovnictví; Porovnání produktů Komerční banky a Československé obchodní banky

Internetbanking; A Comparison between Products of Komerčni banka and Československá obchodní banka

Číslo závěrečné práce

DP – PE – KFÚ – 2008 60

DENISA ZAVADILOVÁ

Vedoucí práce: prof. Ing. Anděla Landorová, CSc., Katedra financí a účetnictví
Konzultant : Lukáš Bér, Komerční banka

Počet stran: 86 Počet příloh: 6

Datum odevzdání 9. května 2008

Prohlášení

Byla jsem seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 - školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracovala samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

V Liberci dne 1. května 2008

……
podpis

Poděkování

Děkuji vedoucí mé diplomové práce prof. Ing. Anděle Landorové, CSc. za trpělivou spolupráci a odborné vedení.

Resumé

Diplomová práce se zabývá srovnáním internetového bankovnictví KB a ČSOB. V první části je popsán vznik a postupný vývoj Internetu jako nové technologie ve světě a v České republice. Druhá kapitola je zaměřena na využití Internetu v bankovnictví jako jednoho z přímých kanálů v komunikaci mezi klientem a bankou. Třetí kapitola zkoumá internetové bankovnictví z hlediska zabezpečení, jak z pohledu klienta jako běžného uživatele počítače, tak z pohledu banky a jejího přístupu k možném zneužití internetové aplikace. V následující kapitole je v krátkosti nastíněn vývoj internetového bankovnictví v České republice a jeho obliba a využívání českými klienty.

V úvodu praktické části jsou představeny dvě z největších bank působících na českém trhu – Komerční banka a Československá obchodní banka – a jejich produkty v oblasti internetového bankovnictví. Tyto produkty jsou v následující části porovnány z hlediska nákladů a možných způsobů zabezpečení.

Summary

The thesis deals with the comparison of Internet banking products the Komerční banka and the Československá obchodní banka. The first part describes the origin and development of Internet as a new technology both abroad and in the Czech Republic. The second chapter includes the types of Internet utilization in the banking industry as one form of the direct banking and communication channel used between the bank and the client. The third chapter investigates Internet banking in the area of security methods in the client's view – as a common user of computer – as well as in the view of bank and its approach to potential trespass of Internet application. In the following chapter there is the development of Internet banking in the Czech Republic, its popularity, and usage by Czech clients briefly drawn out.

In the introduction of practical project there are two of the biggest banks occurring in the Czech bank marketplace introduced – Komerční banka a Československá obchodní banka – and there are presented products of internet banking provided by these banks, too. These products are compared in the next chapter especially in light of costs and forms of security.

Klíčová slova

Internet	Internet
internetové bankovnictví	internet banking
homebanking	homebanking
komunikační kanál	communication channel
banka	bank
bezpečnost	security
elektronický klíč	electronic key
šifrování	cryptoghraphy
elektronický podpis	electronic signature
osobní certifikát	identity certificate

Obsah

Seznam použitých zkratek a symbolů

apod.	a podobně
ARPA	Advanced Research Project Agency
a. s.	akciová společnost
atd.	a tak dále
BBS	Bulletin Board System
CD	Compact Disc
č.	číslo
ČR	Česká republika
ČSFR	Československá federativní republika
ČSOB	Československá obchodní banka
ČVUT	České vysoké učení technické
DES	Data Encryption Standard
DNS	Domain Name Systém
EARN	European Academic and Research Network
EDI	Electronic Data Interchange
FA2	dvoufázová autentizace
FERNET	Federal and Research Network
FESNET	Federal and Research Network
FFIEC	Federal Financial Institutions Examination Council
GfK	Gesellschaft für Konsumforschung
GSM	Global System for Mobile communications
http	Hyper-Text Transfer Protocol
https	Hypertext Transfer Protocol over Secure Socket Layer
HTML	HyperText Markup Language
IBM	International Business Machines
KB	Komerční banka
kbit/s	kilo bit per sekund
MILNET	Military Network
MIT	Massachusetts Institute of Technology
MSN	Microsoft Network

např.	například
NASA	National Aeronautics and Space Administration
NCP	Network Control Protocol
NSFNET	National Science Foundantion Network
OTP	One Time Password
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIN	Personal Identification Numer
RAND	Research And Development
SMS	Short Message Service
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/ Internet Protocol
tj.	to je
UCLA	University of California Los Angeles
UN/EDIFACT	United Nations/Electronic Data Interchange For Administration, Commerce and Transport
USA	United States of America
USB	Universal Serial Bus
USENET	User's Network
WWW	World Wide Web
%	procenta

Úvod

K volbě tématu mé diplomové práce mě vedl zejména zájem o využití moderních technologií v oblasti bankovnictví, stejně jako možnost dozvědět se z pozice běžného uživatele internetového bankovnictví více o jeho principech a alternativních způsobech zabezpečení.

Ve své diplomové práci jsem si kladla za cíl zkoumat využití Internetu v bankovnictví a přínosy moderní technologie v této oblasti společně s možnými hrozbami, které nutí vážně se zamýšlet nad zabezpečením celého systému – nejen v rovině technické – ale i organizační. V kapitole věnované otázce bezpečnosti je ve shodě s teoretickými předpoklady rozebrán jak pohled banky, tak přístup klienta k této problematice a na základě syntézy těchto faktů nastíněn možný způsob řešení organizačního i technologického zabezpečení internetového bankovnictví.

V praktické části jsou představeny služby internetového bankovnictví dvou předních peněžních ústavů působících v České republice – Komerční banky a Československé obchodní banky. Tyto produkty jsou následně porovnávány v oblasti nákladů vynaložených nepodnikající fyzickou osobou (občanem) a z hlediska rozdílnosti v možných způsobech zabezpečení proti neoprávněnému získání bezpečnostních prvků a jejich následnému zneužití v systému internetového bankovnictví.

1 Historie a rozvoj Internetu

Tato kapitola je věnována problematice vzniku a rozvoje Internetu jak z pohledu světového, tak lokálního.

Vývoj Internetu ve světě

Dříve než se začneme zabývat Internetem jako základním kamenem internetového bankovnictví, bylo by vhodné nastínit jeho historii, abychom tak lépe pochopili i samotnou podstatu jeho existence.

První myšlenka, která předznamenávala vznik Internetu, přišla v 60. letech. Spojené státy nejdříve založily Agenturu pro pokročilé výzkumné projekty (ARPA - Advanced Research Project Agency) v rámci Ministerstva obrany. Tento počin byl reakcí na úspěšné vypuštění první umělé družice Sputnik v roce 1957. Úspěch Sovětského svazu byl v období studené války pro Spojené státy nežádoucí, a tak vzniklá agentura dostala za úkol převzetí vedoucí pozice v oblasti vědy a technologie použitelné ve vojenství. [8]

Vše začalo strategickou zakázkou týkající se zajištění spolehlivého a bezpečného způsobu komunikace pro případ tehdy pravděpodobné atomové války. Tuto zakázku dostala v šedesátých letech společnost RAND, což bylo přední americké mozkové centrum v období studené války. Zakázka zněla: „Sestavte nám velitelskou a komunikační síť, která by nás po atomové válce dokázala spojit jak s vojenskými základnami, tak s jednotlivými městy.“ Problém byl zřejmý, kdyby existovalo centrální velitelské a komunikační stanoviště, pak by bylo jasným a nevyhnutelným terčem nepřátelského útoku. RAND řešil tuto složitou zakázku za hlubokého vojenského utajení a dospěl k odvážnému, ovšem zcela prostému řešení zveřejněnému v roce 1964. Jeho základním principem byl fakt, že plánovaná komunikační síť nebude mít centrální zařízení a bude sestavena tak, aby jednotlivé součásti sítě mohly spolu nezávisle na ostatních komunikovat. Jinými slovy síť, kde jednotlivé uzly jsou rovnocenné a která je odolná proti výpadkům některých počítačů do ní zapojených. Tento základní princip tehdy – za časů centrálních počítačů – znamenal senzaci a průlom ve světě počítačových technologií. [6]

Několik univerzit v USA se dozvědělo o této bezpečné koncepci a snažilo se ji realizovat. Především se jednalo o školy MIT neboli Massachusetts Institute of Technology a UCLA (University of California Los Angeles). Už v roce 1968 testovala National Physical Laboratory ve Velké Británii koncept globální sítě. [6]

Na základě těchto zkušeností byl na ministerstvu obrany USA, přesně v oddělení s názvem ARPA – Advanced Research Project Agency, odstartován projekt, při němž byla skutečně vyvinuta a spravována síť skládající se ze superpočítačů šedesátých let jako uzlů této sítě. Tyto tehdy drahé a výkonné počítače, dobře použitelné v síti, by dnešním požadavkům na rychlý počítač už zdaleka nevyhovovaly. V prosinci roku 1969 už byly na tuto síť připojeny čtyři uzly, tedy vznikla malá síť, které dal Pentagon název ARPANET (dle jejího tvůrce) a která je dnes považována za „matku Internetu“. [6]

Opravdový počátkem Internetu bychom mohli označit rok 1967, kdy byl poprvé prezentován návrh designu sítě ARPANET. Síť samotná byla založena v roce 1969 a jejím domovem se staly čtyři vědecké instituce, kterým zajistila přístup k nejvýkonnějším počítačům. Tyto čtyři počítače transportovaly data po několika telefonních linkách. Takzvaný uzlový počítač mohl být řízen jiným počítačem cestou Repote-Control (dálková kontrola). Díky ARPANETu mohli vědci a technici využívat možnosti počítače i na delší vzdálenosti. Kvůli spolehlivosti se přenášená data rozdělila na přiměřeně velké části - tzv. pakety, které se přenáší samostatně. Všechny pakety nesou informaci o svém příjemci a cesta každého paketu je určena samostatně, tedy nezávisle na ostatních paketech. V případě, že je zničena jedna z cest, paket může dojít k adresátovi cestou jinou. Data byla předávána od uzlu k uzlu, až dospěla k cíli. I když velké části sítě vypadly, nevadilo to, balíčky pokračovaly dál po zbylých uzlech. Na první pohled vypadal takový způsob zprostředkování informací velmi nehospodárně, ale na druhou stranu je nutno si uvědomit, že byl daleko méně napadnutelný. [6]

Ministerstvo obrany USA omezilo přístup k ARPANETu ze začátku jen vojákům a dalším osobám, které se zabývaly výzkumem ve vojenství. V roce 1971 bylo připojeno už patnáct uzlů.

Po ověření spolehlivosti byla síť ARPANET v roce 1972 poprvé představena veřejnosti, což mělo ještě téhož roku za následek její další rozšíření na celkem sedmatřicet uzlů. Rok poté se k síti připojily i první neamerické instituce. Po dalších dvou letech byl učiněn překvapující objev. Namísto očekávaného hlavního využití této sítě prostřednictvím Remote-Computingu byla síť využívána především k přenosu zpráv a osobních sdělení, tedy ke vzájemné komunikaci. Důvod je jasný: rozrůstající se počítačová síť umožňovala vědcům možnost spolupráce na projektech, výměnu zpráv a zkušeností z jejich práce. Každý uživatel byl vybaven svým vlastním číslem a e-mailovou adresou umožňující elektronickou poštu mezi uživateli počítačů v síti. Nic tudíž nebránilo v tomu, aby byla komunikace mezi osobami bez obav využívána. Síť tedy nakonec skutečně odpovídala původnímu požadavku elektronické komunikace, změnilo se pouze její zaměření z vojenského na univerzitní pole působnosti. [8]

Během sedmdesátých let se k ARPANETu začaly připojovat další sítě. Jeho decentralizovaná struktura ulehčovala další rozrůstání. Podstatný rozdíl tkvěl v tom, že tato síť, na rozdíl od sítí závislých na výrobci, dokázala rozpoznat různé počítačové systémy, pokud tyto systémy jako společnou řeč používaly protokoly, přenášející pakety dat. Komunikační standard byl pojmenován NCP (Network Control Protocol), brzy byl ovšem nahrazen díky dále se vyvíjející technice dodnes používaným standardem TCP/IP (Transmission Control Protocol/ Internet Protocol), který používá k identifikaci čtveřici čísel z intervalu 0-255. TCP navádí pakety dat podle jejich adres mnoha různými uzly a sítěmi i s jejich rozdílnými standardy k cíli. [6, 9]

Dalším milníkem historie internetu byl rok 1983, kdy se od ARPANETu oddělila vojenská část sítě tzv. MILNET (Military Network) a stala se z ní samostatná síť. Spojení mezi oběma sítěmi však přetrvalo a umožňovalo tak další komunikaci. Tento způsob spojení byl nazván DARPA Internet (Defense Net + ARPANET= DARPA). To mělo zásadní význam, protože tím síť ARPANET prošla „zcivilněním“ a to umožnilo jeho další významný rozvoj. [6]

Postupně docházelo k dalšímu připojování decentralizovaných veřejných sítí, jako například celosvětové sítě Unix nebo USENET (User’s Network). K DRAPA Internetu

bylo připojeno mnoho dalších univerzitních sítí a několik podnikových sítí. Všechny tyto sítě se nestaly součástí Internetu, byly jen speciálně napojeny tak, aby si navzájem poskytovaly ničím nerušenou výměnu informací a dat. Název DARPA Internet bylo brzy zkráceno na pouhé INTERNET. V roce 1984 byla překročena v té době senzační hranice 1 000 zasíťovaných počítačů.

Rok 1986 znamenal zásadní průlom. Vznikl totiž NSFNET (National Science Foundantion Network) na popud vládní agentury National Science Foundation a rozvoj této sítě byl silně podporován především z akademické obce. Tato nově vzniklá síť umožňovala přenosovou rychlost celých 56 kbps. Toto sjednocení propojovalo prostřednictvím pěti výkonných počítačových center sítě celých Spojených států amerických. Za podpory NFS byly do sítě připojovány další a další univerzity a výzkumná střediska, mezi jinými také NASA a National Institute of Health. Počet uzlů se do konce osmdesátých let zvýšil mnohonásobně - na více jak sto tisíc uzlů. [9]

ARPANET postupně přešel na NSFNET, který se brzy projevil jako nositel pokroku. Úspěšný ARPANET oficiálně přestal existovat v roce 1989, ale jeho vliv je znát ještě dnes. Dnešní uživatel Internetu užívá i nadále protokolu TCP/IP ARPANETu, který je dnes celosvětovým standardem. [4]

V osmdesátých letech zaznamenala také Evropa vznik prvních větších sítí. V roce 1983 spatřila světlo světa EARN (European Academic and Research Network), která se za krátko připojila k americkému ARPANETu, resp. NFSNETu. [9]

V roce 1989 vymyslel Tim Berners-Lee nový způsob komunikace pro vnitřní potřebu laboratoří CERN ve švýcarské Ženevě. Tzv. protokol HTTP (Hyper-Text Transfer Protocol). Tento způsob umožňoval tvořit hypertextové dokumenty (texty, které obsahují odkazy na další dokumenty, které mohou být umístěny na jiném počítači, třeba na druhém konci světa), ty pak vystavovat na serverech a poskytovat je ostatním uživatelům sítě. K tomu, aby se daly tyto dokumenty prohlédnout, však byla zapotřebí znalost IP adresy serveru. To bylo dosti nepohodlné a vedlo to k zavedení DNS (Domain Name System), který umožňoval ke každé adrese přiřadit určité jméno. Díky jednoduchému a intuitivnímu

ovládání se tato služba rozšířila i za brány firmy CERN a dnes jí známe pod jménem World Wide Web.

Zanedlouho byly k dokumentům připojeny i obrázky. Vzhled dokumentů byl přirozenější a umožnil ještě lepší komunikaci. Právě existence WWW spolu s masovým rozšířením osobních počítačů přilákala na Internet milióny nových uživatelů, a tím začal být Internet zajímavý i pro podnikatele, kteří mají připojení umožněno již roku 1992. Téhož roku počet uzlů dosáhl 1,4 milionu a růst Internetu neustále zrychloval. V roce 1993 byl představen první WWW prohlížeč - Mosaic. Od tohoto roku prožívá Internet v USA veliký rozmach. WWW služba se postupně zpřístupňuje široké veřejnosti a získává větší a větší podíl na počtu přenesených dat.. O dva roky později, v roce 1995, byl na Internet připojen dvojnásobek počítačů s porovnáním s rokem 1993. Šlo již již celkem o dva miliony počítačů. [9]

Rozvoj Internetu od počátku devadesátých let je bezpříkladný. Rozšířil se rychleji než telefon nebo fax. Přidávaly se k němu školy, knihovny, komerční sektory i soukromé osoby - jednotlivci. Mimořádné oblibě se Internet těšil u vědců a studentů na univerzitách a ve výzkumných ústavech. Mnohostrannost a jednoduchý přístup ke stovkám miliónů dat a databází enormně urychluje vědecký pokrok. Takto se na celém světě objevil nový druh publikační činnosti, při které uživatel obdrží elektronickou kopii textu nebo obrázku. Americký Internet se z počátku netěšil přílišnému zájmu klasických počítačových firem; do jeho vlny nastoupily neznámé firmy jako Cisco, Netscape, AOL a Yahoo. V té době suverénně kralující IBM se postupně budovaly vlastní celosvětové páteřní sítě, ale například Bill Gates, šéf firmy Microsoft, byl v ranných počátcích k Internetu kritický a označoval jej za slepou vývojovou větev.

Ovšem historie nedala Billu Gatesovi za pravdu. Slepou vývojovou větví se stala spíše síť MSN (Microsoft Network), která se měla stát alternativou Internetu. I přes její implicitní umístění do Windows velkého rozšíření nedoznala a postupem času se proměnila v součást Internetu.

Jak je z textu parné, při procesu vzniku a rozšiřování Internetu vznikalo velké množství sítí, jejichž jména označovala jednotlivé rozpočtové a investiční celky. Šlo o samostatné sítě, které ovšem byly propojeny s jinými sítěmi. Právě toto propojení všech sítí dalo vzniknout dnešnímu Internetu. Jednotlivé sítě jsou pak jeho podčásti. Své názvy mají dnes již nejenom akademické a vládní sítě, ale například i firemní sítě a sítě jednotlivých internetových poskytovatelů. V rámci těchto sítí mohou platit pravidla a omezení definovaná provozovatelem sítě, ovšem pokud má takováto síť propojení s ostatními sítěmi na bázi protokolů předepsaných pro Internet (zejména již výše zmíněný protokol TCP/IP), můžeme o této síti hovořit jako o Internetu. Ne nadarmo se Internetu říká „Síť sítí“ - metafyzicky je opravdu Internet propojením, branou mezi jednotlivými sítěmi.

Fenomén Internetu roste z hodiny na hodinu. Internet se už dávno rozšířil ze své původní zamýšlené šíře a oblasti působnosti, pro niž byla zkonstruována síť ARPANET. Dnes je to celosvětová komunikační síť, otevřená pro kohokoliv a kdykoliv.

Historie českého Internetu

Devadesátá léta znamenala vstup Internetu i do tehdejšího Československa. První sítí, která se zde objevila, byla v roce 1989 amatérská síť FidoNET, nekomerční a vládou nepodporovaný projekt. Největší boom prožíval FidoNET v letech 1993 až 1996. Pro připojení do FidoNETu stačila klasická telefonní linka, stejně jako pro síť EUNet, která se do Prahy dostala v květnu roku 1990. [7, 8]

Dalším krokem v budování počítačových sítí byl první český uzel sítě EARN (European Academic and Research Network) – evropské odnože BITNETu, který na ČVUT v Praze začal pracovat v říjnu 1990. Právě přes tuto síť se o rok později uskutečnilo první připojení do sítě Internet. Datem připojení tehdejší ČSFR k Internetu se uvádí listopad 1991, ale za oficiální datum připojení lze považovat 13. únor roku 1992, kdy proběhlo na půdě pražského ČVUT slavnostní připojení. Do té doby byl Internet v České republice výsadou jen několika málo jedinců. [8]

Po připojení volaly i ostatní vysoké školy z celé ČSFR a tak v prosinci 1991 schválilo české ministerstvo školství projekt předložený akademickou obcí a v červnu 1992 uvolnilo

20 miliónů korun pro vybudování páteřní sítě spojující univerzitní města. Na slovenskou část projektu podobně přispělo slovenské ministerstvo školství. [7]

Největším problémem v rozvoji českého Internetu byly komunikační struktury. Napřed tu byly dílčí problémy, například: jak rozdělit původně plánovanou federální síť FESNET. Mimochodem, tato síť se původně měla jmenovat FERNET (Federal and Research Network), nakonec ale zvítězil méně humorný název FESNET. [7]

Po rozpadu ČSFR se FESNET rozdělil na ČESNET a slovenskou část SANET. CESNET měl hvězdicovitou strukturu, jejíž středy byly v Praze a Brně. V listopadu 1992 tato města spojovala pevná linka o kapacitě 64kbps. Paprskovitě z těchto měst vedly linky do dalších středisek: Liberce, Olomouce, Českých Budějovic, Pardubic, Plzně a dalších. Všechna další spojení už byla realizována po telefonních linkách. [8]

Na sklonku roku 1993 zaznamenal CESNET, do té doby nekomerční poskytovatel Internetu, určitou míru poptávky po komerčním využití Internetu. Začátkem roku 1994 pak začal budovat plány, jak nabídnout Internet i komerčním firmám. Veletrh informačních a komunikačních technologií Invex roku 1994 byl prvním velkým krokem komercionalizace Internet. COnet, čistě komerční subjekt, který vznikl v dubnu 1994, a CESNET vytáhly do boje za získání zájemců o připojení k Internetu, avšak zájem mezi firmami o připojení k Internetu nebyl nijak značný a v podstatě kopíroval slova tehdejšího šéfa COnetu Jiřího Orsága: „Přinášíme Internet každému, kdo na něj má prostředky.“ [8]

Byl to až rok 1995, kdy se začal důrazněji prosazovat trend využívání Internetu firmami k sebeprezentaci a komerční činnosti. A byl to opět CESNET, který propojoval akademická pracoviště a zároveň poskytoval komunikační pásmo. Toho mohli využít nově vznikající poskytovatelé Internetu. A jejich prostřednictvím se na Internet připojili koncoví uživatelé – buď pevnou linkou, nebo klasickým telefonním připojením. Analogová linka a modem.
Přestože na českém Internetu skončilo období, kdy přístup měla výhradně akademická sféra, trvalo ještě pár let, než se na vizitkách začaly hromadně objevovat e-mailové adresy. Ještě v roce 1997 nebyla e-mailová adresa pravidlem ani u zaměstnanců firem, které se zabývaly počítačovým průmyslem. [7]

V letech 1995 a 1996 nastal společně s rozvíjející se komercionalizací Internetu v Čechách i bouřlivý rozvoj. V roce 1995 na Invexu byla připojena celá veletržní síť InvexNet linkou 64 kbit/s a je umožněno připojení každého stánku k Internetu. Ivo Lukačovič v roce 1996 spouští Seznam jako první katalogový vyhledávací server v ČR a v roce 1997 založil slovenský Zoznam jako první velký portál na Slovensku. [8]

Významnou překážkou na cestě k většímu rozšíření Internetu mezi domácí uživatele byla vysoká cena připojení a počítačů, která však časem začala klesat na přijatelnou úroveň. Byla to však především politika SPT Telecom, která vedla v roce 1998 ke vzniku zřejmě nejznámější protestní akce internetové komunity u nás, iniciativy Internetem proti monopolu. Ta reagovala na ohlášené zvýšení cen za vytáčené připojení k síti, plánované od ledna 1999. Nakonec se jí podařilo na Telecomu vymoci zvláštní tarif. Spory o délku a cenu impulzu vzaly nakonec za své s tím, jak poskytovatelé přešli na nabídku připojení za měsíční paušál. [7, 8]

Postupně začali služby Internetu poskytovat i alternativní telefonní operátoři, kabelové televize i provozovatelé mobilních sítí. Možností jak se připojit k síti je tak v současnosti celá řada, čemuž odpovídá i stále rostoucí obec uživatelů. Zároveň díky zostřující se konkurenci dochází k postupnému snižování nákladů na připojení a díky neustálému technickému pokroku ke zlepšování kvality a zvyšování rychlosti připojení.

Podle průzkumu Českého statistického úřadu, který proběhl ve druhém čtvrtletí loňského roku, má přístup k internetu 27 procent českých domácností, z nichž 57 procent využívá některou z technologií rychlého připojení. [7]

Dnes se již dá již říci, že Web se stal běžnou součástí života Čechů. Stále více činností lze částečně, nebo úplně přesunout do virtuálního světa. Možnosti komunikace tak pomáhají otevření České republiky světu.

Příčiny úspěchu Internetu

1) **Internet je síť pokrývající celou zeměkouli.** Tato skutečnost není sama o sobě výjimečnou – např. telefonní síť je také vybudována na celé zeměkouli. Rozdíl je v tom, že internetová síť je zcela variabilní – tedy libovolně modifikovatelná a nezávislá na velkých „monopolních“ provozovatelích.

2) **V Internetu jsou všichni právě připojení uživatelé on-line.** To znamená, že v reálném čase běží i ostatní počítače. Internet nemá žádné časové omezení – běží nepřetržitě – 24 h denně 365 dní v roce - na celé Zemi a v kterémkoli čase je přístupný různým lidem v různých částech světa.

3) **Přenášení dat v digitální podobě**. Pod pojmem „data“ si lze představit vše, co lze digitalizovat. Tedy nejen textové informace, ale i obrázky, zvuk, video, telefonní hovory a jakékoliv soubory informací.

4) **Komunikace po Internetu je levná.** Pokud se uživatel připojí k Internetu přes telefonní linku, připojuje se vždy k nejbližšímu uzlu a pak můžete využívat celé sítě. Přitom nenese náklady (většinou pouze za telefon) jen pro připojení právě k tomuto uzlu. Jestliže tento postup zvolí druhý uživatel na opačné straně planety, pak oba účastníci mohou společně komunikovat pouze za cenu lokálních telefonních poplatků přes celou zeměkouli.

5) **Snadné ovládání.** Bylo to právě stanovení standardu WWW, které zásadně ovlivnilo rozšíření Internetu mezi širokou veřejnost. Výrazným zjednodušením, které s sebou tento standard přinesl, se používání Internetu s pomocí internetových prohlížečů stalo velice snadným a zpřístupnilo Internet desetitisícům nových uživatelů.. K základní práci s Internetem stačí uživateli znát alespoň trochu klasické grafické prostředí (např. Windows) a ovládat několik málo funkcí internetového prohlížeče – napsat WWW adresu, umět používat hypertextové odkazy, klikat myší na odkazy a číst.

6) **Velké množství uživatelů.** Díky všem výše uvedeným skutečnostem se o Internet zajímá stále více lidí, firem a institucí. Ti se pak na Internetu prezentují svými

stránkami, čímž se Internet stává stále zajímavějším a láká větší a větší množství lidí. Dalo by se říci, že je to zacyklený proces tzv. automatického obnovování a rozšiřování Internetu jako takového.

7) **Svoboda publikování.** Na Internetu může publikovat kdokoliv téměr cokoliv. Z technického hlediska nemůže nikdo konkrétní jedinci zabránit, aby umístil své stránky nebo soubory na Internet. V současné době existuje velké množství firem, které tuto službu poskytují i zdarma. Po právní a etické stránce však zveřejňovaná data nesmí porušovat platné zákony.

8) **Pružnost, rychlost a neomezenost.** Veškerý tok dat na Internetu probíhá v elektronické formě. Není k tomu třeba žádných fyzických nosičů jako jsou papíry, přepravní služby či jiné technické prostředky (pochopitelně kromě samotných počítačů a sítí). Tok dat a jejich aktualizace je neobyčejně rychlá a pružná. Pokud například bude chtít uživatel změnit určitou informaci na internetové stránce, stačí provést několik jednoduchých úkonů v kanceláři a není třeba nechávat přetiskout všechny propagační materiály. Stejně tak přenášení fotek, které uživatel pořídí, může ihned v digitální podobě umístit na internetové stránky a již několik minut po vyfotografování je může zhlédnout téměř celý svět. Pružnost a rychlost aktualizace je jedna z obrovských výhod Internetu. [4]

2 Vliv nových technologií na oblast bankovnictví

Banky byly po staletí omezeny při komunikaci s klientem na osobní styk prostřednictvím svých poboček. Takovýto styk klienta s bankou se nazývá pobočkové bankovnictví. Znamená to, že banka je pro svého klienta k dispozici pouze v místě, kde má umístěnu pobočku a pouze během otvírací doby.

V druhé polovině dvacátého století se však díky prudkému technologickému vývoji tato situace velmi výrazně změnila. Výrazný technologický posun dává finančním institucím k dispozici širokou škálu prostředků pro komunikaci s klientem. Je to především pevná telefonní linka, Internet, mobilní telefon. Tyto nové komunikační kanály dávají vzniknout novému způsobu takzvaně „přímé“ neboli bezbariérové komunikaci klienta s bankou, nazývané dle její největší výhody „přímé bankovnictví“. Mezi místa, kde je možné s bankou komunikovat, vedle pobočky přibyly např. bankomaty, samoobslužné terminály, webové stránky atd. [4]

Díky rychle se vyvíjejícímu vnějšímu prostředí a globalizaci trhů, s níž jde ruku v ruce nárůst konkurence, dochází k výraznému růstu důležitosti inovací ve finančním sektoru. To je zásadní změna v tradičním, historicky zakořeněném, chápání banky jako konzervativní finanční instituce odolávající většině vnějších vlivů.

Příčiny těchto zásadních změn v chování bank jsou především:

- úspora nákladů a
- zatraktivnění služeb pro klienta. [5]

Úspora nákladů je dána snížením variabilních nákladů na jednu transakci. Na druhou stranu je třeba jednorázově investovat větší objem prostředků pro zavedení moderních komunikačních prostředků, které krátkodobě zvyšují fixní náklady. Banky nejsou schopny po uvedení nových technologií do praxe zajistit okamžitou návratnost těchto investic pomocí radikálních úspor, jako je například propuštění personálu nebo uzavření části svých poboček., Pokud banka nechce riskovat ztrátu podstatné části svých klientů, taková úsporná opatření mohou následovat až po relativně dlouhé době. [5]

Úspora nákladů se projevuje až po určité době – a to především při vyšších objemech transakcí zejména u těch bank, které operují na velkých trzích, nebo globálně.

Dalším podnětem těchto inovací je zatraktivnění služeb pro klienta neboli zvýšení přidané hodnoty pro klienta. Pro banky je důležité si uvědomit, že určitá část populace vnímá rychlost služeb, jejich kvalitu a úsporu času jako důležité měřítko při rozhodování. A právě používání moderních prostředků může klientovi jeho kritéria bezpodmínečně splnit. Velikost této skupiny osob je v jednotlivých zemích různá a je závislá jak na vyspělosti dané země, tak na kulturních a sociálních tradicích a na politických podmínkách. [5]

Pokud banka považuje za svůj hlavní cíl při přechodu na přímé bankovní služby zatraktivnění svých služeb, dojde nakonec k závěru, že přímé bankovnictví vyžaduje v mnoha ohledech jiný přístup a jinou filozofii než klasické „pobočkové“ bankovnictví.

Jedná se zejména o:

- speciální klientskou segmentaci,
- odlišné fungování pobočkové sítě,
- jinou filozofii marketingu služeb. [5]

Nejnižší variabilní náklady pro banky v sobě skrývá komunikace prostřednictvím počítače, ať už se jedná o Internet či klasické modemové spojení. Internet však vzhledem ke své dostupnosti postupně klasické modemové spojení již zastínil.

Internet má své výhody i nevýhody. Výhody jsou více než jasné. Tkví především v nízkých variabilních nákladech a v možnosti vysokého klientského komfortu, jenž je dán zejména přehledností, kterou nelze získat prostřednictvím telefonu ani pomocí klasických poštovních výpisů či bankovních přepážek. Klasické webové stránky jsou naopak nevhodné pro vyřizování nestandardních záležitostí, jako jsou například reklamace, nebo speciální požadavky a dotazy klientů. Zde může být částečným řešením předcházení těmto dotazům formou FAQ (frequent asked questions) vystavených na webové stránce nebo formou internetových diskusí za účasti banky. Mnoha dotazům se dá také předejít správnou – především přehlednou a jasnou - strukturou internetových stránek a informačních materiálů banky. Proto je důležité, aby banka měla vytvořený proces, který

vyhodnocuje dotazy klientů a zajišťuje tak zpětnou vazbu pro tvůrce informačních materiálů. [3,5]

Část komunikace může být nabídnuta také prostřednictvím elektronické pošty. Email může být vhodný pro vyřizování reklamací a méně standardních dotazů, přičemž určité segmenty klientů tento způsob komunikace vyžadují či upřednostňují email například před telefonem. [5]

Velký rozmach přímého bankovnictví ovšem neznamená úplný zánik bankovních poboček. K transformaci od osobního jednání k neosobním komunikačním kanálům (Internetu, mobilním telefonům) dochází postupně a stále ještě přetrvává segment populace, který nebude ochotný přijmout moderní technologie. Do budoucna lze ovšem u moderních bank očekávat postupné přetváření poboček spíše na jakási konzultačně-prodejní místa, kam klient bude chodit pouze s určitou speciální záležitostí a bude očekávat získání přidané hodnoty ve formě rady. Běžné operace bude klient provádět sám pomocí pro něj nejdostupnějších technologií. [5]

Toto vytváří tlak na změnu způsobu myšlení v bankách. Rozhodně se nejedná o lehkou změnu, naopak tato změna bude trvat v mnoha bankách ještě relativně dlouhou dobu. Pokud by například velká banka měla změnit své pobočky na konzultační místa, zvláště pak ve prospěch služeb poskytovaných moderními komunikačními prostředky, znamenalo by to v mnohých případech i výměnu personálu, který v současné době sice stačí na vyřizování běžných bankovních operací, ale pokud by měl sloužit jako skutečný finanční poradce ve světě moderních finančních služeb, bude jeho kvalifikace v mnoha případech nedostatečná.

Bankovnictví prochází velkými změnami, a to zejména díky dvěma významným trendům: informační a komunikační revoluci a globalizaci. Banky jsou nuceny se pod vlivem těchto změn přizpůsobovat okolním změnám především investicemi do inovací, které se pro ně stávají stále důležitější. Důsledkem těchto tlaků jsou nejenom změny v chování bank vůči svým klientům a nabízení pestřejších možností komunikace a produktů, ale i změny ve vnitřním chování bank, kdy prostředí nutí banky k daleko dynamičtějšímu chování a

uspořádání. Roste význam fixních nákladů a klesá význam variabilních nákladů, což má za následek vlnu fůzí a akvizic, které můžeme ve světě pozorovat.

Homebanking jako první krok k internetovému bankovnictví

Banky v době, kdy to rozvoj informačních technologií umožnil, nabídly speciální možnosti komunikace, určené zejména firmám, souhrnně označované jako "homebanking". Ve světě to bylo v osmdesátých letech 20. století, v České republice až o něco později, počátkem let devadesátých. Jednalo se o způsob komunikace klienta a banky za pomoci osobního počítače vybaveného speciálním softwarem, přičemž samotný přenos dat probíhá většinou prostřednictvím modemu a telefonní linky. Protože jednu z hlavních rolí při této komunikaci hraje počítač, používají některé banky namísto termínu "homebanking" výraz „PC bankovnictví“. I přesto, že se tak přímé bankovnictví přiblížilo i běžným spotřebitelům, stále existovalo veliké omezení spočívající právě v nutnosti přímého spojení s bankovním systémem přes telefonní linku, jakož i v nákladech na aktualizaci a údržbu specifického softwaru. [3,5]

Homegankingové systémy nepřinášely svým uživatelům pouze výhody v tom, že nebylo třeba každodenní osobní návštěvy banky. Podnikatelské subjekty jsou ze zákona povinny vést dokonalou účetní evidenci a nacházejí-li se jednou data v elektronické podobě, lze je importovat do účetnictví, což přináší další výraznou úsporu jak času, tak drahé pracovní síly. Tento proces ovšem funguje také v opačném směru – účetní příkazy lze také zadávat přímo z účetního systému. [5]

2.1.1 Komunikace pomocí přenosových médií a BBS

V době, kdy se Internet teprve rozvíjel a výměna dat prostřednictvím modemu a telefonní linky byla ještě v zárodku, začaly banky nabízet firemním klientům první možnost elektronické komunikace, při níž byla využívána tzv. přenosová média – především diskety, které svou datovou kapacitou a univerzálností vyhovovaly pro tento účel nejvíce.[5]

Tato média sice umožňovala elektronickou formu komunikace, stále ovšem bylo nutné přinášet data do banky osobně. Z toho důvodu začaly banky nabízet přednost dat do banky pomocí modemu a standardu BBS (Bulletin Board System). Klient tak nemusel chodit do banky s disketou, ale data byla posílána přímo z počítače klienta. [5]

Prostřednictvím přenosných médií, příp. BBS, se uskutečňovaly dva základní typy operací:

- zadávání platebních příkazů,
- přijímání výpisů z účtu. [5]

Důležitá byla i volba datového formátu, ve kterém si klient a bankou informace vyměňoval. Banka klienta vybavila speciálním softwarem, který uměl vkládaná data (tj. platební příkazy) uložit do požadovaného formátu a obdržená data (tj. výpisy z účtu) zobrazit. K tomuto účelu obvykle soužil speciální software banky. [5]

Je třeba poznamenat, že používání přenosných médií, příp. BBS, je dnes již velmi zastaralý způsob, který byl ve své době používán poměrně malým množstvím klientů.

Oproti tomu moderní homebankingové systémy umožňují komfortní komunikaci s bankou a nabízejí uživatelům mnohem větší možnosti využití, než tomu bylo u elektronické komunikace prostřednictvím přenosných médií a BBS. Zásadní rozdíl tkví v tom, že se klient napojuje přímo na bankovní systém, může tak získávat on-line informace o svém účtu, například položit dotaz na aktuální disponibilní zůstatek. [5]

Spojení homebankingu a internetového bankovnictví

Na homebankingových systémech firemní klienti oceňují zejména urychlení práce a napojení na účetnictví. V případě, že klient využívá internetového bankovnictví, je to opět řešeno přes speciální software, který si klient nainstaluje na svém počítači. Tento software může buď sloužit jako prostý filtr mezi účetním systémem klienta a internetovým systémem banky, nebo může navíc umožňovat provádění bankovních operací. Stejně jako v předchozích případech je nezbytné vyřešit otázku bezpečnosti. [3,5]
Spojení homebankingu a internetového bankovnictví je výhodné zejména v případech, kdy ve firmě je pouze jeden člověk (např. finanční ředitel), který má právo provádět transakce

s firemním účtem. Zadávání platebních příkazů je potom prosté. Příkazy v účetním systému připraví například účetní a rovnou je odešle do banky. Banka však příkazy neprovede do té doby, než je svým elektronickým podpisem potvrdí osoba disponující potřebným oprávněním, v našem případě finanční ředitel. Ten se přitom může nacházet na druhém konci světa – stačí, aby měl přístup k jakémukoli počítači připojenému k Internetu, pomocí kterého může vstoupit do bankovního systému. [5]

Řada z funkcí homebankingu již byla postupně nahrazena Internetem – tedy přímým přístupem do centrálního systému banky s aktuálními informacemi. Funkce internetového bankovnictví a homebankingu se postupně prolnuly a navzájem doplnily. Dnes již tyto oblasti splynuly a jen těžko je lze jasně oddělit. Firmy i nadále provozují své účetní systémy s bankovními aplikacemi, a právě k tomuto provázání slouží hromadný přenos dat, k jehož předávání slouží právě Internet.

Internetové bankovnictví

Internet je v současné době pro banky i pro jejich klienty nejlevnějším komunikačním médiem. Transakce provedená jeho prostřednictvím je několikanásobně levnější než transakce provedená pomocí telefonu. Ve srovnání s klasickým způsobem na pobočce je úspora až stonásobná. Na druhou stranu náklady na implementaci internetového bankovnictví jsou značně vysoké, banky tudíž do svého portfolia služeb internetového bankovnictví zařazují nejen pasivní operace (např. zjištění zůstatku a transakcí na účtu), ale také operace aktivní tzv. transakční.

Internetové bankovnictví může být tzv.:

- neplnohodnotné - vázáno na konkrétní počítač,
- plnohodnotné – přístupné z jakéhokoli počítače připojeného k Internetu. [5]

Pro používání internetového bankovnictví prvního typu si klient musí na svůj počítač nainstalovat speciální (bezpečnostní) software poskytovaný bankou. Pro zajištění bezpečnosti jsou využívány digitální certifikáty a digitální podpisy, které tento speciální software generuje při komunikaci klienta a banky. Internetové bankovnictví tohoto typu tedy nelze využít z jiného než předem nakonfigurovaného počítače.

Druhý typ pro zajištění bezpečnosti vyžaduje, aby klient a banka měli k dispozici zařízení schopné zajistit vzájemnou autentizaci obou komunikujících stran. Toto zařízení není nijak spojeno s počítačem, klient a banka si mezi sebou vyměňují vygenerované kódy. Na počítač klienta není instalován žádný speciální software, internetové bankovnictví lze tedy bez problémů používat například jednou z domova a podruhé ze zaměstnání.

Elektronická pošta v bankovnictví

Elektronickou poštu považujeme v bankovnictví spíše za doplněk internetového bankovnictví. Rozhodně není vhodná pro provádění běžných transakcí, neboť každou operaci by bylo v bance potřeba manuálně zpracovat. Klient, který je běžným uživatelem služeb elektronické pošty, je také uživatelem Internetu obecně a může veškeré požadavky zadat komfortněji prostřednictvím internetového bankovnictví.

Elektronická pošta je pro oblast přímého bankovnictví také využitelná. Existují určité oblasti, kde je její použití velice výhodné.

Je to v případě:

- řešení problémů a reklamací,
- hromadná komunikace generovaná bankou. [5]

2.1.2 Řešení problémů a reklamací

Banka nabízející služby přímého bankovnictví musí být připravena nabídnout svým klientům komplexní a rychlý servis i tehdy, pokud nefunguje vše tak jak má. A není přitom důležité, zda se jedná o selhání lidského faktoru, techniky banky, či zda problém způsobil sám klient svou neznalostí. Elektronická pošta pak slouží jako individuální komunikační kanál, který umožňuje vyřizování dotazů, reklamací a dalších problémů.
Elektronická pošta společně s nepřetržitou telefonickou podporou vytváří užší vztah mezi klientem a bankou a buduje vzájemnou důvěru.

2.1.3 Hromadná komunikace generovaná bankou

Elektronická pošta je ideální i pro hromadnou komunikaci generovanou bankou (výpisy z účtu, informace o došlých platbách, atd.). Náklady na takovýto způsob informování klientů jsou několikanásobně nižší a používání tohoto média je několikanásobně rychlejší než klasická pošta. V některých případech lze již dnes díky technologické vyspělosti použít ještě rychlejší kanál, kterým jsou krátké textové zprávy.

Význam Internetu pro bankovnictví

Internet neuvěřitelným tempem mění nejenom bankovnictví samotné, ale i ekonomické a sociální prostředí, ve kterém banky operují. Jen těžko bychom hledali oblast, do které Internet vůbec nezasahuje.

Banky velmi rychlým tempem směřují do prostředí, které se výrazně odlišuje od toho, na něž byly zvyklé. Velké světové banky si uvědomují, že pokud velmi rychle nezaujmou svoji novou pozici na trhu v nově formulovaném prostředí, brzy zaniknou nehledě na jejich současnou velikost. Proto jsou nuceny uskutečňovat významné investice a poskytnout značnou část ze své intelektuální kapacity právě na rozvoj internetových aplikací ve finančním sféře.

Bylo by chybné chápat Internet jen jako další způsob komunikace s klientem. Na základě jeho vývoje lze pozorovat změny ve všech bankovních oblastech, od způsobu komunikace s klientem počínaje, přes marketing, prodej, či řízení lidských zdrojů.

3 Bezpečnost internetového bankovnictví

Internet se obecně považuje za velice snadno zneužitelný a napadnutelný kanál. Jakákoliv citlivá data v elektronické podobě je nutné chránit před zneužitím a v oblasti bankovnictví, kde se tato data týkají operací s penězi, platí toto pravidlo o to více. V dnešním neustále se měnícím vnějším prostředí, které se velmi výrazně projevuje právě v oblasti ochrany elektronických dat, jsou banky nuceny zavádět stále dokonalejší a důmyslnější bezpečnostní systémy. [4]

Teoretické předpoklady

Bezpečnost systému obecně závisí jednak na zajištění bezpečnosti aplikací, jednak na zabezpečení fyzické bezpečnosti systému. Zabezpečení aplikace spočívá v provádění autentizace klienta, certifikace dat, a v jejich ověření v případě přístupu klienta po Internetu navíc nastupuje ochrana dat šifrováním. [2, 5]

3.1.1 Zásady bezpečnosti na straně banky

1. Bezpečná komunikace s klientem

- Důvěryhodnost zpráv – zpráva je důvěrná informace určená výhradně pro příjemce – klienta, tato problematika se řeší pomocí šifrování zpráv.
- Autentizace protistrany – odpověď na otázku: „komunikuji opravdu s tím, s kým si myslím?“ pomáhá řešit princip šifrování a elektronický klíč.
- Prokazatelnost původu zprávy – schopnost prokázat klientovi či bance, že poslala určitou zprávu, řeší se pomocí digitálního podpisu a certifikace dat elektronickým klíčem.

2. Zabránění průnikům dovnitř banky po Internetu

- Soustava firewallů, která je velmi pečlivě nastavena.
- Oddělené role správců jednotlivých systémů.

3. Na zabezpečení zneužití zevnitř banky

- Zajištění principu „co není dovoleno, je zakázáno“.
- Použití systému čtyř očí – u každé operace jsou nejméně dva zaměstnanci.
- Precizní systém přístupových práv pro interní uživatele bankovního systému.

- Další technologická ochrana, spočívající v použití nezávislého softwaru, který vyhledává anomálie (např. mnoho malých převodů na jednom účtu).[1]

3.1.2 Elektronický klíč

Autentizace klienta a banky, certifikace dat posílaných klientem do banky a ověřování mohou být prováděny elektronickým klíčem. Elektronický klíč využívá principu symetrického šifrování. Obsahuje naprogramovaný šifrovací algoritmus a šifrovací klíč DES (Data Encryption Standard) délky 56 bitů. Autentizace probíhá na principu symetrického zašifrování zprávy na základě klienta i banky a porovnání výsledků. Certifikace probíhá obdobně s tím, že součástí zprávy jsou jednotlivé údaje v příkazu klienta. Banka kontroluje, zda certifikační kód zadaný klientem je pro rozšifrování totožný s došlými údaji klienta, a teprve poté příkaz provede. [5]

3.1.3 Šifrování

Proto, aby se zpráva stala nečitelnou pro neoprávněnou osobu, se používá šifrování. Šifrování znamená převedení vnímatelných a srozumitelných slov a číslic do kódované podoby nedávající smysl.

První metody šifrování byly použity již před 4 000 lety za vlády faraónů ve starém Egyptě. Díky převratnému rozvoji výpočetní techniky a nárůstu výpočetních výkonů byly šifrovací algoritmy zdokonaleny na takovou úroveň, že jsou současnými technickými prostředky nerozluštitelné.

Šifrování si lze v podstatě představit jako mechanismus zámků na dveřích vedoucích ke klientovým informacím v bance. Pro klienta a server banky je velice snadné převést nesrozumitelnou podobu zprávy do srozumitelné formy, ale pro případného útočníka je to problém, protože k takovému zámku existují miliardy možných klíčů. Při každém novém navázání spojení klienta a banky dojde k vygenerování a výměně náhodného klíče, následně použitého na kódování probíhající komunikace. Počet potenciálních klíčů k zámku je závislý na síle šifrování, tj. na délce šifrovacího klíče. Při každém novém

[1] PŘIHRÁDKA, M. a KALA, J. *Elektronické bankovnictví : [rady a tipy]*. Vyd. 1. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5. str. 75, 76.

navázání komunikace se generuje nový klíč, pro rozluštění je potřeba začínat opět zcela od začátku.

a) Délka šifrovacího klíče

Za minimální délku klíče pro symetrické šifrování je považováno 80 bitů. To znamená , že k určitému zámku existuje 2^{80} možných klíčů. Běžně se užívají až 128-bitové klíč. Tuto délku šifrovacího klíče užívá například Expandia banka (SSL3) – to znamená, že existuje 2^{128} možných klíčů. Počítač proto potřebuje exponenciálně více výkonu k nalezení správného klíče než u 80-bitového šifrování.

Do jaké míry je v současné době možné prolomit šifrovací klíče různé délky?

- Šifrování pomocí 60 bitů je rozluštitelné (technologicky i finančně či organizačně).
- Šifrování pomocí 80 bitů je rozluštitelné (technologicky, nikoliv finančně či organizačně – nelze soustředit dostatečný počet počítačů dohromady).
- Šifrování pomocí 128 bitů je nerozluštitelné technologicky.
- Šifrování pomocí 180 bitů je nerozluštitelné, protože na Zemi nemáme momentálně k dispozici dostatek energie.[2]

b) Princip fungování šifrování

Symetrické šifry

Symetrické šifry jsou takové, u nichž se stejný šifrovací klíč používá jak pro zašifrování, tak i pro zpětnou rekonstrukci dat, k zašifrování i rozšifrování je použito jediného klíče. Nevýhoda tohoto typu šifrování spočívá v možnosti nedostatečné bezpečnosti kanálu, kterým mezi odesílatelem a příjemcem dojde k předání klíče. Potom je otázkou, jak bezpečným kanálem byl klíč předán a do jaké míry je osoba příjemce zprávy důvěryhodná. Tento typ šifer je používán spíše k přímému šifrování dat na disku nebo před jejich přenosem. [2, 5]

[2] PŘIHRÁDKA, M. a KALA, J. *Elektronické bankovnictví : [rady a tipy]*. Vyd. 1. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5. str. 79.

Asymetrické šifry

U asymetrických šifer je k zašifrování dat použito jiného klíče než k rozšifrování těchto dat. Díky matematickým algoritmům je možné vygenerovat dvojici šifrovacích klíčů, které se nazývají „soukromý“ a „veřejný“ klíč. Zprávu zašifrovanou jedním z nich lze rozšifrovat pouze druhým z dvojice těchto klíčů. Soukromý klíč je ve vlastnictví majitele, který jej používá k rozšifrování zpráv. Veřejný klíč je dostupný k šifrování komukoliv, kdo si přeje komunikovat s vlastníkem soukromého klíče. Oba tyto klíče jsou natolik rozdílné, že znalost jednoho v žádném případě neumožňuje určit podobu druhého klíče. Soukromý klíč nutný k rozšifrování zprávy není třeba posílat žádným komunikačním kanálem, tudíž nehrozí nebezpečí jeho vyzrazení či zneužití. Tento způsob šifrování je oproti symetrickému šifrování daleko bezpečnější. Jako u jakéhokoliv jiného klíče, i bezpečnost algoritmů asymetrického šifrování je přímo úměrně závislá na délce použitého šifrovacího klíče. [2, 5]

V praxi se využívá kombinace obou metod šifrování. Jedna strana stanoví symetrický klíč, zašifruje jej pomocí asymetrické šifry a pošle jej partnerovi. Ten jej rozšifruje a v tu chvíli oba znají symetrický klíč. Tímto způsobem probíhá například šifrování pomocí protokolu SSL (Secure Sockets Layer). Protokol SSL se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP (Hyper Text Transfer Protocol). [10]

Ustavení SSL spojení funguje na principu asymetrické šifry, kdy každá z komunikujících stran má dvojici šifrovacích klíčů - veřejný a soukromý. Veřejný klíč je možné zveřejnit a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

Ustavení SSL spojení (tzv. SSL handshake neboli potřásání rukou) pak probíhá následovně:

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.

3. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
4. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu jej.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od tohoto okamžiku bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
7. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od této doby komunikují přes šifrované spojení.[3]

c) Prokazatelnost původu zprávy

Banka každý vydaný dokument, u kterého to má smysl, na vyžádání digitálně podepíše. Klient má potom jistotu, že zpráva pochází opravdu z banky. Tento vztah platí i opačně, klient všechny důležité dokumenty digitálně podepisuje, banka si je proto jistá jejich původem a může s klidným svědomím provést požadované operace. [4]

d) Princip fungování digitálního podepisování

Tento princip je obdobný jako výše popsaný princip asymetrického šifrování. Pouze se zde role veřejného a privátního klíče obrací. Digitální podpis je soubor znaků, jedinečný pro podepisovanou zprávu a daný privátní klíč. Digitální podpis jiné zprávy (byť podepsané stejným privátním klíčem) bude jiný a digitální podpis stejné zprávy za použití jiného privátního klíče bude také odlišný. [5]

Nejprve byl vytvořen elektronický podpis, což je informace, která se připojuje k elektronickým datům, aby identifikovala odesílatele příjemci. Podepsáno může být v podstatě cokoliv a to i bez nutného vytištění na papír, například obsah diskety, fotografie, přístupy k www serverům, emailová zpráva, přístupy do databáze apod.

[3] *Secure Socker Layer* [online]. [cit. 18. 1. 2008]. Dostupné z: < http://cs.wikipedia.org/wiki/SSL >

Největším problémem byla ověřitelnost elektronického podpisu. Proto byl vytvořen tzv. digitální podpis, který umožňuje jednoznačnou identifikaci osoby. Digitální podpis je v podstatě spojením klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka. Tak je zajištěno svázání podpisu s určitou osobou. K tomu, aby byl digitální podpis skutečně důvěryhodný, je dobré, aby byl certifikát ověřen třetí nezávislou osobou, která tak ručí za jeho pravost. Takovou instancí je právě certifikační autorita. [5]

Do roku 2000 neexistoval v českém právním řádu předpis, který by umožňoval všeobecné využití elektronického podpisu a veškeré závažné záležitosti bylo nutné podepisovat klasickým způsobem. I přesto se elektronický podpis používal, bylo však nutné každý takový vztah uzavřít smluvně. Revoluci přineslo přijetí zákona č. 227/2000 Sb. o elektronickém podpisu, který zařadil elektronický podpis mezi možné varianty podpisů veškerých dokumentů.

e) Certifikáty a způsob jejich využití

Certifikáty je možné obecně rozdělit na dvě základní skupiny, osobní a serverové. Osobní certifikáty jsou určeny k ověření totožnosti jednotlivých osob. Serverové certifikáty jsou určeny pouze pro servery a ty vždy zastupuje vlastník serveru.

Využití osobních certifikátů je v praxi velmi obsáhlé. V současné době stále více uzavírají smlouvy jen pomocí elektronického styku. Pomocí elektronického podpisu s certifikátem bude brzy možné podávat například daňová přiznání, žádosti atd. Velké využití budou mít certifikáty i v e-komerci. Zejména v internetových obchodech bude vyžadováno podepisování objednávek elektronickým podpisem, aby nemohla být objednávka zpochybněna. Největší již funkční využití digitálního podpisu je v bankovní sféře. Certifikát je zejména využíván pro přístup klientů bank k službě internetového bankovnictví. V rámci této služby certifikát slouží k přihlašování do internetových aplikací a k potvrzování operací prováděných klientem.[11]

Odesílatelův osobní certifikát může také využít adresát. Použitím veřejného klíče odesílatele zašifruje zprávu či dokument, který bude moci být rozšifrován pouze za pomoci

soukromého klíče původního odesílatele. Je tak zajištěno, že zaslaná zpráva bude k přečtení pouze určené osobě. Osobní certifikát může také sloužit pro přístup k serverům. Na server tak může přistoupit pouze osoba s ověřeným certifikátem, jehož identifikační číslo je uvedeno v databázi serveru, tzn. konkrétní osoba. [11]

U serverových certifikátů již není využití tak rozsáhlé. Tento typ certifikátu je převážně využíván v kombinaci s SSL. Serverové certifikáty jsou určené pro bezpečnou komunikaci uživatelů se serverem, kde se pomocí certifikátu a SSL chrání důležitá data návštěvníků serveru. [11]

3.1.4 Zabránění průnikům dovnitř banky po Internetu

Pro zabránění přístupu jakéhokoliv neautorizovaného subjektu do prostředí banky je vnitřní prostor chráněn systémem hardwarových a softwarových ochranných zdí. Ochranné zdi tzv. firewally slouží pro zastavení případných útočníků. Firewally jsou umístěny před všechny systémy používané v bance. Umožní tedy přístup pouze těm klientům, kteří splňují nadefinované pravidlo. Například nutným pravidlem je „Umožni komunikaci komukoliv z Internetu, který využívá webovou službu a chce se připojit na server, který se jmenuje bank.expandia.cz“. Pokud se objeví jiný požadavek nesplňující zadanou podmínku, firewall přístup odmítne. [5]

Centrální systém bank není chráněn pouze jedním firewallem, ale je aplikována řada po sobě jdoucích ochran. V této řadě serverů jsou použité i jiné platformy operačních systémů, které mají vzájemně odlišné vlastnosti. V rámci přístupové větve také dochází ke změně komunikačního protokolu TCP/IP (viz kapitola 1.1 Vývoj Internetu ve světě) na docela odlišný komunikační protokol, což technicky znemožňuje použití přímého napojení na klientský systém. Každý ze systémů je on-line monitorován a každá neobvyklá operace je zaznamenána pro další analýzu. [5]

3.1.5 Bezpečnosti organizační a technologická

Mezi základní bezpečnostní zásady patří tzv. „princip čtyř očí“, kdy pro provedení všech důležitých operací je nutná přítomnost minimálně dvou oprávněných osob. Další zásadou je dodržování oddělených rolí operátorů a správců systému, stejně jako oddělení správců jednotlivých prvků ochranné zdi (tj. správce firewallů je oddělený od správce proxy serveru či klientského systému). Výsledkem je, že každý zaměstnanec má přístup jen k části systému. [5]

Celý informační systém je navržen tak, že používá technologie digitálních podpisů i při operátorském provozu (jsou podepisována data), takže není možno mu podvrhnout data špatná. Systém si tak například před provedením úročení zkontroluje, jestli jsou úrokové sazby podepsány oprávněným operátorem. Vzhledem k tomu, že digitální podpis zaručuje i integritu dat, tj. neměnnost a úplnost, je možné s jistotou tvrdit, že data nebyla podvržena neoprávněnou osobou. [5]

Informační systém běží v geograficky vzdáleném klastru. To znamená, že pokud vypadne jakýkoli počítač, je okamžitě nahrazen jiným. Geografickou vzdáleností je zajištěn běh i v případě, že dojde k požáru v jedné z lokalit. Pracoviště jsou umístěna ve dvou lokalitách a obě jsou plnohodnotná. Při běžném provozu si rozdělují práci, při výpadku jednoho z nich přebírá celou práci druhé lokality. Lokality jsou vybírány tak, aby byla rozložena rizika (například rizika živelných pohrom). [5]

Jedním z nejvíce střežených tajemství je bankovní šifrovací soukromý klíč. Klíč je uložen v takzvaném šifrátoru, což je počítač ve speciálním plášti. Šifrátor je ochotný vykonat pouze kryptografické operace, nikdy však nevydá tajemství v podobě soukromého klíče, a to ani při fyzickém napadení šifrátoru. Existuje jediná výjimka, a tou je zálohování klíče. Toto zálohování probíhá tak, že klíč je rozložen na dvě čipové karty. Každou tuto kartu dostane jedna osoba. Třetí osoba ví heslo k soukromému klíči. Pro zneužití klíče by tedy byla nutná spolupráce tří osob. Ze zálohy je však možná obnova v případě technologické ztráty soukromého klíče. [5]

Otázka bezpečnosti v praxi

V současném počítačovém a digitalizovaném světě je bezpečnost stále náročnější a žádanějším artiklem. Útoky a napadení jsou společně s růstem možností Internetu rozmanitější a sofistikovanější. V bankovním sektoru se na problematiku bezpečnosti tradičně klade mimořádný důraz, tudíž internetové bankovnictví a jeho zabezpečení je v poslední době jedním z významných fenoménů a zároveň značně kontroverzním tématem nejen ve světě informačních technologií.

3.1.6 Zabezpečení z pohledu banky

V České republice neexistuje banka, jejíž produkt by byl zcela nezabezpečený. Jsou však banky bezpečné a bezpečnější. Banka jako každý běžný obchodní subjekt musí dodržovat různé regulace, zákony a normy, a to vše i v oblasti bezpečnosti informačních technologií. Ovšem internetové bankovnictví se jako nabízený produkt snadno vejde do relativně volných nařízení, což skýtá řadu problémů. Samostatný standard pro internetové bankovnictví dosud neexistuje a tento fakt sám o sobě skýtá řadu problémů. Tuto úlohu prozatím supluje „Open Web Application Security Project“ (OWASP), což jsou všeobecně odborníky uznávané a prosazované materiály. [4]

Mnoho doporučení OWASP ovšem banky často ignorují z následujících důvodů:

- zlehčování rizika možného dopadu,
- zveličování možných útoků,
- český Internet = malý Internet,
- přenos odpovědnosti ze strany banky na klienta,
- pro uživatele je vydáno tzv. „desatero bezpečnosti“ – jestliže je dodržují, není se čeho bát,
- „nadstandardní“ bezpečnost je drahá a vyžaduje ji minimum uživatelů. [5]

Z výše zmíněného vyplývá, že banky jsou motivovány dělat minimum v oblasti bezpečnosti internetového bankovnictví.

[4; 5] Bankovnictví. Č. 5. Praha: Economia. 2006. ISSN 1213-7693.

3.1.7 Zabezpečení z pohledu klienta

Běžný uživatel je z pohledu bezpečnosti nenáročný a to především proto, že nerozumí této problematice natolik, aby byl schopen definovat své požadavky na zvýšení bezpečnosti užívaného internetového bankovnictví. V důsledku potom dochází k tomu, že v oblasti zlehčování hrozeb s bankou často souhlasí.

Obvyklý přístup uživatele k bezpečnosti internetového bankovnictví může být popsán následovně:

- zůstatek na běžném účtu nemívá vysoký, takže heslo a PIN mu jako bezpečnostní prvky stačí,
- ví, že banka používá zabezpečený způsob komunikace (například SSL),
- varování expertů považuje za strašení,
- nadstandardní bezpečnost je pro něho moc drahá a obvykle se v bance nesetká s dostatečným objasněním možných rizik „standardní“ bezpečnosti. [6]

Z těchto postojů běžného uživatele je patrné, že uživatelé jsou ve většině případů neznalí a bezpečnost příliš nevyžadují a nevytváří žádný tlak na bezpečnější služby. Uživatelé často podceňují rizika a věří informacím, které jim poskytne banka.

3.1.8 Rozumná míra zabezpečení

Jak z postojů banky, tak klienta, je patrné společné přesvědčení, že bezpečnost je drahá. Následkem toho je fakt, že většina aplikací vytvořených pro služby internetového bankovnictví obsahuje bezpečnostní chyby. Jen málokdy je možné v praxi se setkat s aplikacemi, které jsou navrhovány od začátku s důrazem na bezpečnosti, kdy je provozovatel natolik prozíravý, že jejich zabezpečení důkladně prověřuje a uživatelé jsou kvalifikovaně informování o rozdílech, které jim různé způsoby zabezpečení poskytují.

Dle tvrzení mnoha bezpečnostních expertů je PIN společně s heslem jednou z největších slabin. Správnou obranou proti ní nejsou dostatečně dlouhá hesla ani jejich častá změna, či

[6] Bankovnictví. Č. 5. Praha: Economia. 2006. ISSN 1213-7693.

uzamykání účtu po několika nezdařených pokusech. Řešením je tzv. „FA2“, neboli dvoufázová autentizace, nejlépe ve formě OTP (One Time Password). [7]

Pro takové řešení musí být splněny nutné předpoklady:

- řešení musí být dostupné, jednoduché a levné (nemusí se jednat o bankovní kalkulátory, zasílání hesel pomocí bankovních SMS je dostatečně efektivní),
- banky takové řešení musí doporučovat na prvním místě, možnost používat hesla by měla být výrazně omezena, nebo zrušena,
- větší důraz kladený na vzdělávání uživatelů je prvopočátečním krokem a nezbytným předpokladem. Mnohý běžný bankovní úředník není schopen klientovi řádně osvětlit tuto problematiku ani nastínit možná rizika. Je třeba uživatele dlouhodobě vzdělávat, vysvětlovat jim, v jakých případech je nutná obezřetnost a seznámit je s „bezpečnostními návyky“. [8]

3.1.9 Bezpečnost obsahu

Jakékoli podnikové prostředí s rozšířenou sítí počítačů připojených na Internet se může stát předmětem napadení, pokud není dostatečně chráněno. Taková napadení mohou vést až k narušení dostupnosti informačních systémů a snížení kvality nabízených služeb dané společnosti.

Koncepty zabezpečení musí počítat s řadou obranných prostředků, mezi něž patří hlavně nástroje pro Content Security, tj. bezpečnost obsahu. Jedná se o systémy pro monitorování a řízení přístupu webové a e-mailové komunikace, které v dnešní době představují klíčový stupeň nezbytné kontroly. Content Security se zabývá obranou před problematickým obsahem, který se může do podnikových sítí dostat ve formě SPAMu, virů, spywaru (program odesílající data z počítače bez vědomí jeho uživatele) či phishingu. [9]

a) Webová komunikace

[7; 8; 9] Bankovnictví. Č. 5. Praha: Economia. 2006. ISSN 1213-7693.

Spywary a viry se dostávají do počítačů především z tzv. „závadných“ webových stránek či softwaru a také prostřednictvím emailů. V takovém případě je třeba implementovat nástroj, který zamezí uživatelům Internetu v organizaci přistupovat na takové stránky. Nejlepším způsobem je aplikovat pravidla na základě kategorií stránek rozdělených podle obsahu. Následním krokem po zamezení přístupu na nežádoucí stránky je antivirová kontrola všech ostatních navštívených stránek, neboť i na seriózních stránkách se nedopatřením může objevit vir.

Slabým místem může být i využívání web-mailových či free-mailových služeb. Potom je nutné zajistit antivirovou ochranu nejen stránek, ale také všech příloh, které se objevují v emailech a jsou prostřednictvím Internetu stahovány a otvírány. [10]

b) Emailová komunikace

Druhou skupinou nástrojů jsou nástroje bojující s nežádoucím obsahem šířícím se emailem, jako je například SPAM, v dnešní době často diskutované téma. Detekce SPAMu probíhá několika různými způsoby, mimo jiné i pomocí tzv. „black-listů, které identifikují emailovou adresu, z níž byl SPAM odeslán. Dalšími způsoby pro rozpoznání SPAMu jsou analýza textu obsaženého v hlavičce a těle emailu a dále metoda rozpoznání škodlivého obsahu, v rámci níž jsou kontrolovány a vyhodnocovány obsahy všech internetových stránek, na něž odkazy uvedené v emailu směřují. [11]

Tato metoda se používá i pro účinný boj s „phishingem“, který lze ve stručnosti popsat jako email, jehož odesílatelem je důvěryhodná organizace (převážně banka) a který vyzývá uživatele k ověření jeho přihlašovacích údajů (jména a hesla). Následně může dojít ke zneužití poskytnutých údajů.

Všechny výše popsané metody mohou sloužit jak pro kontrolu a rozpoznání emailů adresovaných organizaci či bance, tak pro rozpoznávání dokumentů směřujících ven. Je tedy možné identifikovat, zda dokument, který se snaží některý ze zaměstnanců odeslat,

[10; 11] Bankovnictví. Č. 5. Praha: Economia. 2006. ISSN 1213-7693.

není interního charakteru a zda-li má adresát oprávnění takové dokumenty odesílat. V případě virů je problematická aktuálnost a použitelnost antivirového programu. U virů šířících se emailem (typicky označované jako „wormy“) je nejefektivnější způsob obrany vůbec jim neumožnit vstup do firemní sítě. Je poměrně jednoduché nastavit kritérium pro konkrétní typy příloh, které se nesmí dostat do organizace.

Podcenění problematiky Content Security může být ve svém důsledku příčinou nepříjemných obtíží uvnitř organizace a v některých případech – především v bankovním sektoru – může vést i ke snížení kredibility. Proto je třeba věnovat i této oblasti neustále vysokou pozornost. Důsledkem nasazení nástrojů pro bezpečnost obsahu je jednak významné omezení rizik, vyplývajících z kontaktu s podezřelým obsahem. Tyto nástroje ovšem také přispívají k zvyšování efektivity počítačových systémů v organizaci právě eliminací případných škod, což redukuje čas nutný na jejich případné odstranění.

Vymezení zodpovědnosti v oblasti zabezpečení

Internet a problémy s internetovým bankovnictvím mohou někdy vzbuzovat dojem, že se jedná o úkol pro informatiky a experty, kteří ovládají informační technologie na profesionální úrovni. Ovšem internetové, GSM a telefonické bankovnictví jsou především komunikační kanály mezi bankou a klienty a tak je třeba se na ně dívat.

Obecně platí, že zástupci bank, zodpovědní za přímé bankovní kanály, jsou s dostatečným předstihem informováni na možná nebezpečí, která s sebou tyto kanály přinášejí. Na přelomu července a srpna roku 2006 byli přesto nepřipraveni a jejich systémy nedokázaly odlišit transakci zadanou klientem od té, kterou zadává jménem klienta podvodník. Došlo tak k vykradení téměř dvou desítek bankovních účtů přes internetové bankovnictví. [12]

Případy vykradených účtů otevírají několik závažných otázek spojených s internetovým bankovnictvím - bez ohledu na to, jaký typ zabezpečení je klientovi nabízen. Jedná se mimo jiné o následující otázky:

- Kdo je zodpovědný za internetové bankovnictví a problémy s ním spojené?

- Je klient schopen dostatečně zabezpečit svůj počítač?
- Jaký bude postup, když bude mít klient svůj počítač dobře zabezpečený a někdo zneužije do té doby neznámou a tudíž neošetřenou slabinu? [13]

3.1.10 Zabezpečení klientova počítače

Jak je již poukazováno v předchozí kapitole 3.2.3, je nezbytná náležitá osvěta a vzdělávání uživatelů v oblasti rizik spojených s internetovým bankovnictvím. I přesto byl, stále je a také v budoucnosti bude značný rozdíl mezi znalostmi odborníků a znalostmi běžných uživatelů.

Dalším důležitým faktem je skutečnost, že současné bezpečnostní programy (například antivirové programy, personální firewally a podobně) ochrání svého uživatele pouze před počítačovým nebezpečím, které již někdo identifikoval, popsal, a výrobci bezpečnostních programů tyto popisy zahrnuli do databáze svých programů. Může se ovšem stát, že i v těchto programech se objeví technická chyba, která umožňuje útočníkům v podobě virů dostat se do klientova počítače. V technologickém vývoji se za posledních několik let bezpečnostní programy posunuly o značný kus kupředu, ale zároveň se minimálně o stejný kus posunuly i škodlivé programy. Pokud má být Internet bezpečně využíván pro přenos bankovních operací, je třeba s těmito riziky umět pracovat. [14]

Je zásadní si zároveň uvědomit fakt, že stejně tak jako v běžném životě nelze žádnou hmotnou věc na sto procent zabezpečit, podobně nelze klientům nařizovat, aby si své počítače zabezpečili na sto procent. Klient většinou není schopen v prostředí počítačové sítě rozpoznat náznaky nekalých praktik podvodníků. Například v situaci, když hacker ukradne uživateli jméno a heslo, jedná se o zkopírování dat, takže uživatel si téměř nemá šanci všimnout nějaké změny.

3.1.11 Zabezpečení po technické stránce

Internetové bankovnictví je především služba banky, omezování okruhu osob zodpovědných za jeho provoz pouze na techniky a informatiky je krátkozraké. Podobně

[12,;13] Bankovnictví. Č. 11. Praha: Economia. 2006. ISSN 1213-7693.
[14] Bankovnictví. Č. 11. Praha: Economia. 2006. ISSN 1213-7693.

málo prozíravé je snažit se vyřešit zabezpečení pouze v rovině technologické. Před několika lety bylo pro odborníky těžko představitelné, že je možné vniknout do cizího počítače, ukrást uživatelovo heslo a osobní certifikát a ty zneužít k vykradení účtu. To je po případech z léta roku 2006 veřejně známý způsob. Některé banky v současné době nabízejí jako dokonalejší způsob pro ověření klienta uložení jeho osobního certifikátu na čipovou kartu. Již nyní jsou ale v odborných kruzích známé a popsané způsoby, jak je možné zneužít i takto „zabezpečený" osobní certifikát. [15]

Snažit se vyřešit bezpečnost pouze v prostředí počítačových technologií je na první pohled zajímavá cesta, která může skýtat celou řadu nových zkušeností a objevů. Na druhou stranu je třeba si uvědomit, že technologie, které člověk vytvoří, dokáže jiný člověk dříve či později překonat. Zabezpečení pouze na úrovni technologické by tudíž představovalo stále bdělý a nikdy nekončící proces nepřetržitého zdokonalování a předbíhání možnostem zneužití právě vzniklých technologických možností.

3.1.12 Přijetí zodpovědnosti

Internetové bankovnictví je především služba banky. Jedná se o aplikaci, kterou si banka nechala vytvořit, provozuje ji a svým klientům nabízí její služby za úplatu. Při úvaze o vymezení zodpovědnosti na straně banky a na straně klienta je nutné brát zřetel na schopnosti a možnosti obou zúčastněných stran. Možnosti banky a jejích odborníků na informační systémy jsou značně rozsáhlé. Banka má dostatek prostředků pro zabezpečení informačních systémů, které má přímo pod kontrolou. totéž rozhodně nelze říci o klientech. Mezi desítkami nebo stovkami tisíc klientů se vždy najde někdo, kdo nebude mít bezchybný operační systém spolu se všemi používanými programy, nebo do jehož počítače se nějakým způsobem dostane škodlivý program.

Přijetí zodpovědnosti za provozovanou službu není snadný úkol. Banka musí být na takový postoj připravena - jak po stránce technické, tak především po stránce organizační. Touto cestou jde mnoho bank ve Spojených státech i v Kanadě, například Wells Fargo, Citibank, Fifth Third Bank. Tyto banky svým klientům v základní verzi internetového bankovnictví nabízejí přístup a zadávání transakcí pouze s použitím jména a hesla. Další „nadstavbové"

[15; 16] Bankovnictví. Č. 11. Praha: Economia. 2006. ISSN 1213-7693.

prostředky pro zabezpečení účtů se klientům nenabízejí jako nadstandard, ale jako samozřejmost v případech, kdy mají na účtech větší zůstatky než několik tisíc dolarů. [16]

Jak může fungovat internetové bankovnictví, když počítačové viry a další škodlivé kódy se snaží škodit v USA rozhodně častěji než v České republice? Tamní banky si již dávno uvědomily svoji odpovědnost za službu, kterou poskytují klientům, a ve vlastním zájmu garantují schopnost rozeznat transakci, kterou zadal klient, od transakce, kterou jeho jménem zadává podvodník. I v případě přístupu k řešení mimořádných událostí najdeme obrovský rozdíl mezi Severní Amerikou a Českou republikou. V USA i v Kanadě je klient na prvním místě, a pokud má nějaké problémy, banka se mu snaží pomoci. [17]

Případy, které se staly v ČR ukázaly, že banky, jejichž klientům byly vykradeny účty prostřednictvím internetového bankovnictví, nebyly na tyto mimořádné události připraveny. Odmítaly připustit, že by mohl být problém v systému banky. Tomu odpovídal i přístup kompetentních pracovníků na centrálách příslušných bank. Jelikož neměli zpracovaný manuál na takový typ mimořádné události a protože se jednalo o běžné klienty retailingového bankovnictví, reklamace klientů byly bez dalšího zkoumání zamítnuty.

Nejdůležitější je si uvědomit, že internetové bankovnictví není službou oddělení IT, resp. přímých kanálů, ale celé banky. Internetové bankovnictví a další přímé kanály jsou správnou cestou, ovšem počítače, internet a obecně moderní technologie mají stále velký náskok před okolním světem a běžní uživatelé, kteří nejsou z oboru informačních technologií, nemají vždy dostatek možností znát nové objevy v tomto oboru. Informace o stále nově objevovaných chybách v počítačových programech, nových škodlivých programech a případy vykradených účtů ukázaly, že běžní klienti se mohou stát obětí, i když mají počítač zabezpečený na průměrně dobré úrovni. Tuto skutečnost je třeba přijmout a hledat řešení v dalších oblastech spojených s provozem internetového bankovnictví, ale i jiných služeb založených na moderních technologiích.

[17] Bankovnictví. Č. 11. Praha: Economia. 2006. ISSN 1213-7693.

Spotřebitelský výzkum vnímání bezpečnosti on-line bankovnictví

Bezpečnostní divize společnosti Elisa-Madison-Communications vydala počátkem roku 2007 výsledky svého čtvrtého každoročního výzkumu online podvodů na zákaznících finančních institucí. Tento výzkum byl prováděn v prosinci roku 2006 a zúčastnilo se jej 1678 dospělých osob z osmi zemí po celém světě. Respondenti byli dotazováni na rostoucí hrozby podvodů, jako je phishing, vishing (obdoba phishingu využívající k podvodům telefonní) a snahy jejich finančních institucí o posílení autentifikace vzdálených bankovních transakcí. [18]

3.1.13 Důvěra v Internet jako komunikační kanál

Asi 82 % vlastníků účtů spíše neodpovídá na e-mail od banky, protože se obávají podvodu pomocí phishingu. Toto číslo se zvýšilo ze 79 % v roce 2005 a 70 % v roce 2004. Více než polovina respondentů uvedla, že by si nepořídila internetové bankovnictví. Až 44% vlastníků účtů uvedlo, že jsou v posledním půlroce znepokojeni dalšími typy útoků typu phishingu. Tento výzkum potvrzuje, že trh se pohybuje správným směrem - více než 90 % zákazníků je ochotno používat silnějšího zabezpečení než je standardní uživatelské jméno a heslo, pokud se jejich banka rozhodne nabídnout vyšší stupeň zabezpečení. Banky by na tento fakt rozhodně neměly zapomínat, pokud chtějí posílit svoji pozici v oblasti internetového bankovnictví. [19]

Dále 82% vlastníků účtů by uvítalo, kdyby jejich banka sledovala práci s online a telefonním účtem a pátrala po podivných aktivitách nebo chování; 51% respondentů se domnívá, že by je banka měla kontaktovat, když zjistí jakoukoli podezřelou aktivitu. Britští vlastníci účtů jsou v tomto ohledu nejvyhraněnější; až 93% respondentů by chtělo monitorování online bankovnictví, zatímco ve Francii se toto číslo pohybuje kolem 70%.[20]

[18; 19; 20] Bankovnictví. Č. 3. Praha: Economia. 2007. ISSN 1213-7693.

69 % vlastníků účtů se domnívá, že by finanční instituce měly nahradit přihlašování pomocí uživatelského jména a hesla silnější autentifikací pro internetové bankovnictví. Přestože uživatelé volají po větší bezpečnosti a chtějí ji používat, pouze 39 % vlastníků účtů odpovědělo, že vědí o tom, že jejich banka nabízí nějakou podobu dodatečné bezpečnosti (personalizované stránky, autentifikace založená na rizicích, jednorázově generovaná hesla).

Faktem zůstává, že v roce 2006 byl poslední termín pro americké finanční instituce, aby posílily bezpečnost svých online služeb, jak to nařídil finanční regulátor Federal Financial Institutions Examination Council (FFIEC). Podle studie Gartner, která byla provedena mezi 50 americkými bankami v říjnu a listopadu roku 2006, dvě třetiny amerických bank již splňují doporučení FFIEC o silnější autentifikaci v prostředí internetového bankovnictví. [21]

3.1.14 Preferované metody autentifikace

Respondenti dostali na výběr z různých metod autentifikace, včetně hardwarových způsobů, personalizovaných obrázků a autentifikace založené na rizicích. Většina (73 %) se vyjádřila v tom smyslu, že by uvítali, kdyby jejich banka používala autentifikaci založenou na ověřování výše rizika. Tento typ autentifikace zahrnuje interní vyhodnocení identity uživatele, které je založeno na faktorech jako je místo přihlášení, IP adresa počítače a chování během transakce. Tyto faktory mohou být doplněny telefonním ověřením nebo tajnými otázkami, které kontrolují vysoce rizikové operace. Autentifikace založená na rizicích je utvořena tak, aby nabízela silnou bezpečnost s minimálním dopadem na uživatele.

V globálním měřítku chce 40 % respondentů používat hardwarové přístroje pro autentifikaci. Pokud by se jejich banka rozhodla využívat takové přístroje pro autentifikaci, pak přibližně polovina všech respondentů (49 %) souhlasila, že by uvítali, když by se pomocí stejného přístroje mohli přihlašovat i na další stránky vyžadující autentifikaci kromě stránek své banky. Více než polovina klientů (56 %) odpověděla, že by rádi

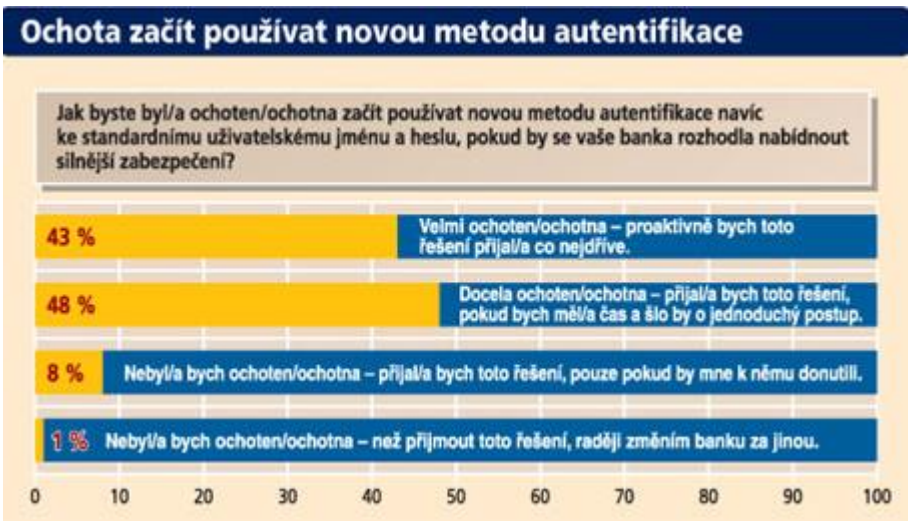
[21; 22] Bankovnictví. Č. 3. Praha: Economia. 2007. ISSN 1213-7693.

využívali personalizovaný obrázek k autentifikaci uživatele bankovních aplikací; 53 % mělo pocit, že by jim personalizované obrázky nabídly vyšší pocit bezpečnosti. Tento obrázek si zvolí sám uživatel a pomocí něho si ověří, že je na skutečném webu banky a ne na podvodné stránce. [22]

Graf č. 1:

Zdroj: Bankovnictví. Č. 3. Praha: Economia. 2007. ISSN 1213-7693.

Graf č. 2:



Zdroj: Bankovnictví. Č. 3. Praha: Economia. 2007. ISSN 1213-7693.

4 Internetové bankovnictví v České republice

Rozvoj výpočetní techniky v osmdesátých a především v devadesátých letech 20. století přinesl dříve nemyslitelné rozšíření bankovních služeb. Pohodlí komunikace s bankou pomocí počítače mohli v druhé polovině devadesátých let s postupným rozšiřováním Internetu okusit i uživatelé v České republice.

Historie internetového bankovnictví v ČR

V České republice se úloha Internetu v bankovnictví začala významně prosazovat v druhé polovině devadesátých let.

4.1.1 ČSOB a standard UN/EDIFACT

Mezi první průkopníky tohoto typu komunikačního kanálu mezi bankou a klientem byla i ČSOB, která v květnu roku 1995 zahájila novou vysoce progresivní formu elektronické komunikace se svými klienty při tuzemském platebním styku, při níž byla využívána národní podmnožina zpráv standardu UN/EDIFACT (United Nations/Electronic Data Interchange For Administration, Commerce and Transport), vytvořená ve spolupráci s Hospodářskou komorou ČR. [23]

Norma UN/EDIFACT předepisuje syntaxi a sémantiku zpráv, jejichž obsahem jsou běžné dokumenty vyměňované mezi dvěma stranami. Komunikace na bázi EDI je způsob výměny dat mezi dvěma nezávislými subjekty elektronickou formou s využitím definovaných formátů přenášených zpráv dle doporučeného mezinárodního standardu UN/EDIFACT. Celý projekt čítal několik etap, přičemž v první etapě projektu ČSOB přijímala zprávy umožňující bance zadat platební příkaz a výzvu k inkasu. Banka klientům předávala kreditní a debetní avízo a výpis z účtu pro tuzemský platební styk. [24]

Ve své době se jednalo o první realizovaný projekt z řady připravených odborných projektů k zavedení tohoto standardu v České republice. Jedna z mnohých výhod tohoto systému spočívá ve využití systému založeného na mezinárodních standardech v oblasti vlastní komunikace a strukturách přenášených dat. Tím vznikl produkt, který lze využít

[23; 24; 25] BLAŽEK, J. a UKLEIN, J. *Bankovnictví.* Vyd. 1. Brno: Doplněk, 1997. 179 s. Edice učebnic Právnické fakulty Masarykovy univerzity v Brně. ISBN 80-85765-91-8, str. 98.

nejen k výměně bankovních zpráv, ale i pro výměnu dat obecně, například objednávek, faktur a dodacích listů. Další nespornou výhodou byl fakt, že díky nezávislosti UN/EDIFACT na výrobcích operačních systémů či komunikačních protokolů lze tento systém vytvářet podle potřeba možností jednotlivých uživatelů, takže nebylo třeba zavádět jednotný komunikační systém či jednotná technická nebo softwarová vybavení. [25]

Tento projekt byl velice úspěšný. Všechny teoretické předpoklady se osvědčily v praxi, o čemž svědčí hojné využívání toho standardu pro služby internetového bankovnictví pro korporátní klientelu v řadě peněžních ústavů v České republice.

4.1.2 Expandia banka

Dalším významným milníkem v rozšiřování služeb internetového bankovnictví v ČR byl projekt první české banky orientované na přímé bankovnictví. Podnikatelský projekt připravovaný skupinou Expandia od poloviny roku 1997 vyvrcholil zahájením provozu v květnu 1998.

Expandia banka nabízela celou řadu moderních průlomových komunikačních kanálů jako Internet, fax, telefon, samoobslužné zóny, systém krátkých textových zpráv a síť mobilních telefonů GSM. Pojem přímé bankovnictví se brzy stal pevnou součástí českého bankovnictví. Začaly se jím označovat špičkové peněžní služby, které má klient k dispozici nepřetržitě, v kteroukoliv denní či noční hodinu a navíc z kteréhokoliv místa na světě. Průkopníkem tohoto pojetí bankovnictví byla v České republice Expandia banka.

Úspěšný projekt přímého bankovnictví přilákal v roce 1999 do Expandia banky již více než 20 tisíc klientů. V roce 2001 změnila banka svůj název na eBanka a zařadila se mezi uznávané finanční instituce na českém trhu. eBanka vykazuje dynamický růst v klíčových finančních ukazatelích i v počtu klientů. V různých soutěžích a anketách sklízí úspěchy za image, za přístup ke klientům i za kvalitní produkty a služby. [26]

[26] *Historie* [online]. [cit. 18. 1. 2008]. Dostupné z: < http://www.ebanka.cz/Informace-o-bance/Zakladni-udaje/Historie.html >

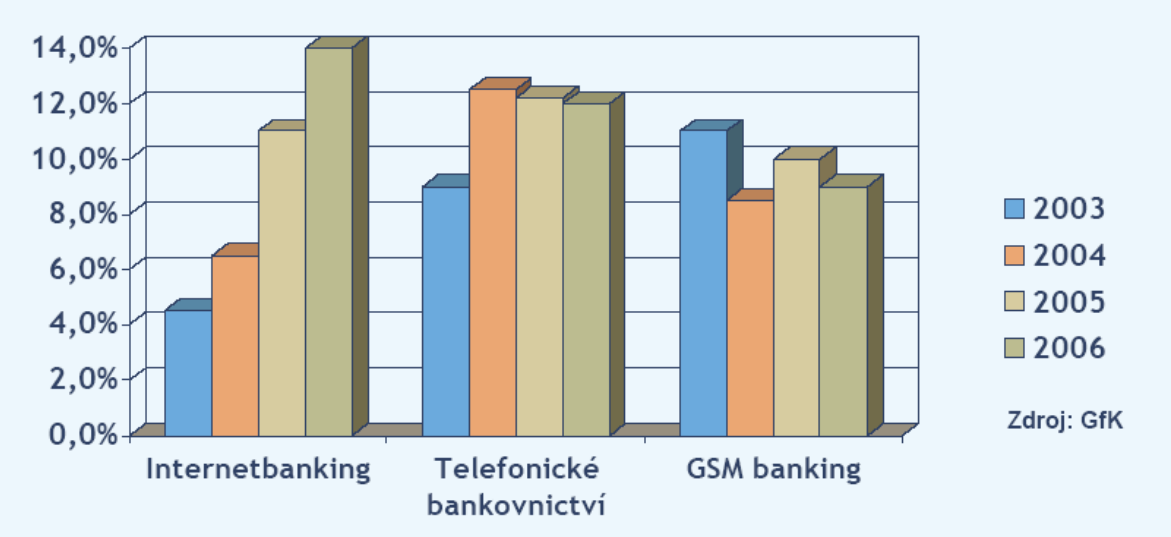
Obliba internetového bankovnictví v České republice

Internet jako přímý kanál pro vstup do banky stále nabývá v komunikaci mezi klientem a bankou na významu - je pohodlný pro klienta, výhodný a výnosný i pro banku, zrychluje a zlepšuje mnohé parametry komunikace, dává prostor pro nové služby a jeho vzrůstající obliba jako jednoho z nejpoužívanější přímých kanálů v České republice tyto přednosti jen potvrzuje.

4.1.3 Internet jako nejužívanější přímý kanál

Internet se teprve v roce 2006 stal nejužívanějším kanálem přímého bankovnictví. Ještě v předchozích letech vévodilo přímým kanálům telefonické ovládání účtu. Tento fakt ukázala i poziční analýza pro ČSOB, kterou vypracovala agentura Network Media Service. Výzkumu se zúčastnilo 2438 respondentů, kteří jsou aktivními uživateli českého internetu. ČSOB chce být podle svých ředitelů v oblasti přímého a elektronického bankovnictví lídrem trhu, udávat směr a stát se v oblasti přímého bankovnictví jedním z novátorů. [27]

Graf č. 3: Vývoj přímých kanálů v ČR v letech 2003 – 2006



Zdroj: Bankovnictví. Č. 10. Praha: Economia. 2007. ISSN 1213-7693.

Procento klientů, kteří vyřizují bankovní záležitosti pomocí Internetu více než jednou měsíčně, sice v průběhu let postupně narůstá, avšak teprve v roce 2005 těsně překročilo hranici 10 % všech klientů.

[27; 28] Bankovnictví. Č. 10. Praha: Economia. 2006. ISSN 1213-7693.

V průzkumu klienti kromě jiného také známkovali své banky - nejlepší známku za internetové bankovnictví ze škály od 1 do 5 dostala eBanka (1,19), za ní se umístila ČSOB (1,79). Na dalších pozicích stojí Česká spořitelna (2,01), Komerční banka (2,18) a GE Money Bank (2,41). [28]

Jednou měsíčně nebo častěji chodí na pobočky vyřizovat své finanční záležitosti stále ještě zhruba polovina českých bankovních klientů. Tato část se jen velmi nepatrně snížila mezi lety 2004 a 2006. Pětina klientů navštěvuje pobočky i vícekrát měsíčně. Zatímco v roce 2004 jich bylo těsně přes 20 %, v roce 2006 je to těsně pod 20 %. [29]

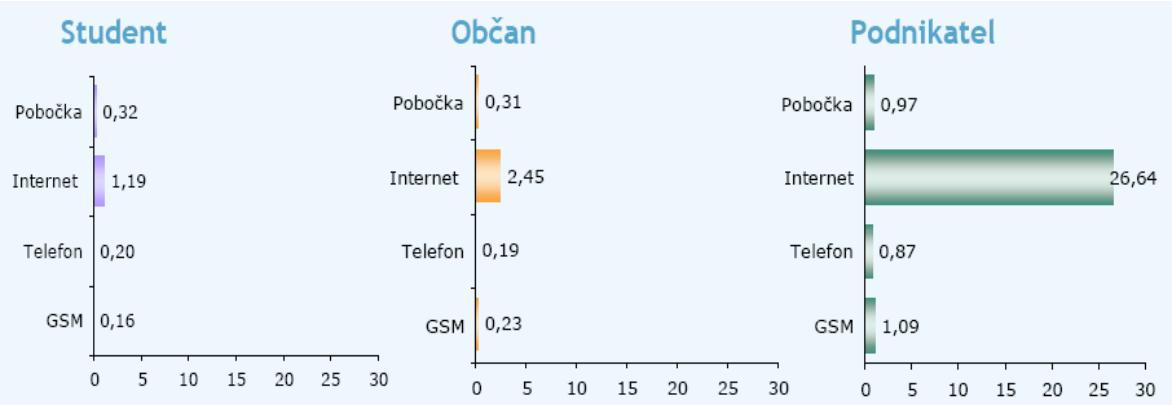
4.1.4 Pět skupin klientů

Z analýzy rovněž vyplývá, že můžeme rozlišovat zhruba pět skupin klientů. Nejpočetnější je aktivní klient s kombinací internetového a telefonického či GSM bankovnictví. Tato skupina čítá 43 % všech klientů. Druhá nejpočetnější skupina, skládající se z 19 % klientů, je sporadickým uživatelem přímých kanálů, zejména internetového bankovnictví. Třetí nejpočetnější skupina vůbec nepoužívá žádné přímé kanály, klientů s tímto přístupem je 17 %. Naopak 13 % patří k extrémním uživatelům přímého bankovnictví. A konečně zbylých 8 % klientů používá přístup pouze prostřednictvím telefonu nebo mobilního telefonu, ale nikoliv pomocí Internet. Nejaktivnějšími uživateli účtů i přímých kanálů jsou spíše muži s vyššími příjmy a podnikatelé s kladným vztahem k přímým kanálům. [30]

Pokud bychom zkoumali pouze jednorázové příkazy k úhradě do téže banky, vyhrál by internetový kanál u všech zkoumaných skupin klientů. Největší oblibě se Internet těší u podnikatelů. Průměrný klient z tomto segmentu zadá měsíčně takových příkazů 26,64, zatímco na pobočce pouze 0,97 příkazu. U studentů rovněž vede Internet s 1,19 příkazy za měsíc, při návštěvě pobočky s 0,32 příkazy. Ostatní občané zadají takových příkazů 2,45 přes Internet a 0,31 na pobočce. [31]

[29; 30; 31] Bankovnictví. Č. 10. Praha: Economia. 2006. ISSN 1213-7693.

Graf č. 4: Využívání jednotlivých kanálů pro zadání jednorázového příkazu k úhradě do téže banky (měsíčně)



Zdroj: Bankovnictví. Č. 10. Praha: Economia. 2006. ISSN 1213-7693.

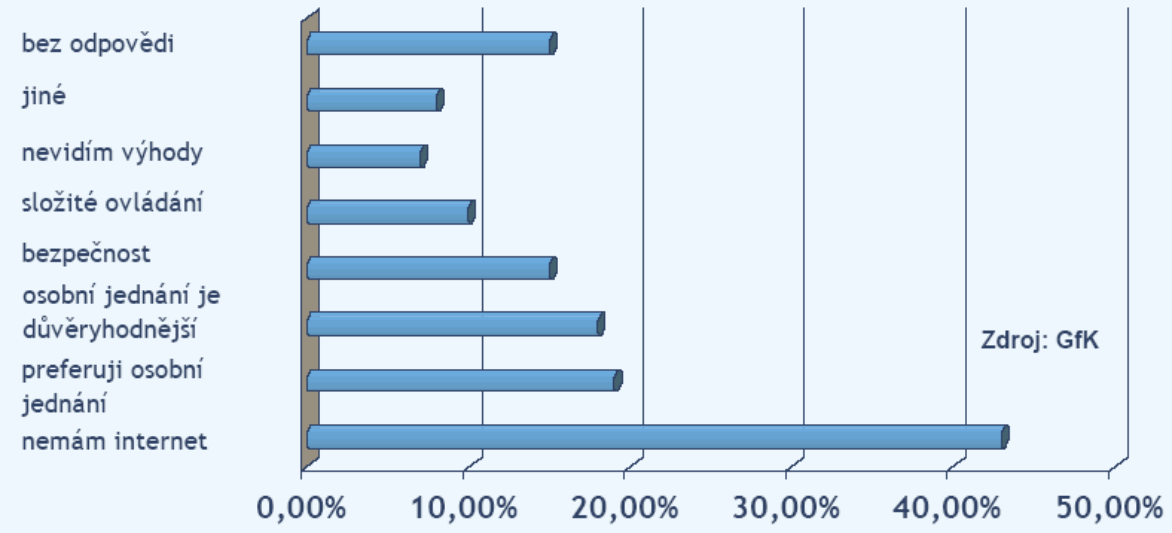
4.1.5 Problémy v rozvoji internetového bankovnictví

Rozvoj internetového bankovnictví dosud brzdí především penetrace internetu mezi obyvatelstvem. Jako nejčastější důvod nevyužívání internetového bankovnictví uvádějí respondenti výzkumu GfK, největšího německého institutu pro marketingový výzkum, nedostatečný přístup k Internetu.

Mezi důvody, proč nevyužívají internetové bankovnictví, uváděli respondenti výzkumu GfK nejčastěji nemožnost přístupu k Internetu. Přístup k Internetu nemá až 42 % klientů nevyužívajících internetové bankovnictví. Dalších 19% preferuje osobní jednání. Faktem, že osobní jednání je pro ně důvěryhodnější, obhajuje nevyužívání Internetu 18% těchto klientů. Pro 14% z nich je důvodem nedostatečná bezpečnost. Problém ve složitosti ovládání vidí 9% těchto klientů, 7% nevidí v Internetu žádné výhody, které by je přiměly k jeho užívání. [32]

Graf č. 5: Důvody nevyužívání internetového bankovnictví

[32; 33] Bankovnictví. Č. 10. Praha: Economia. 2006. ISSN 1213-7693.



Zdroj: Bankovnictví. Č. 10. Praha: Economia. 2006. ISSN 1213-7693.

Na otázku *"Setkal jste se při využívání přímého bankovnictví s problémy?"* odpovědělo kladně 12 % uživatelů internetového bankovnictví, přičemž 34 % z takto odpovídajících klientů uvedlo "nedostupnost služby", 17 % "komplikovanost" a 15 % "alternativní prohlížeče". [33]

5 Internetové bankovnictví Komerční banky

Profil banky

Komerční banka (KB) patří k nejvýznamnějším bankovním institucím v České republice a v regionu střední a východní Evropy. Je součástí mezinárodní skupiny Société Générale. Poskytuje komplexní služby drobného, podnikového a investičního bankovnictví. Široká nabídka služeb zahrnuje hypoteční úvěry, spotřebitelské půjčky a kreditní karty, stavební spoření a úvěry, životní a neživotní pojištění, penzijní připojištění, investice do podílových fondů, leasingové a factoringové služby, správu aktiv, správu cenných papírů, finanční poradenství a mnoho dalších. [12]

Komerční banka vznikla v lednu roku 1990 vyčleněním z bývalé Státní banky československé. V lednu 1992 změnila banka formu ze státního peněžního ústavu na akciovou společnost. V listopadu 1994 banka navýšila základní jmění na 9,502 miliardy

korun a to ji na dlouhou dobu umožnilo zastávat postavení nejsilněji kapitálově vybavené banky na českém trhu. [12]

V říjnu 2001 se Komerční banka stala součástí skupiny Société Générale v oblasti retailového bankovnictví. Mezi hlavní činnosti skupiny Société Générale patří poskytování služeb v oblastech retailového bankovnictví a finančních služeb, globálního investičního managementu a služeb v podnikovém a investičním bankovnictví. V oblasti retailového bankovnictví a finančních služeb obsluhuje ve Francii i po celém světě 22,5 milionu zákazníků. V 77 zemích světa skupina Société Générale zaměstnává celkem 120 tisíc lidí. Finanční skupina KB byla k 31. prosinci 2006 tvořena devíti společnostmi, na jejichž kontrole se podílela také KB. V sedmi společnostech drží KB nadpoloviční podíl a dvě jsou přidružené společnosti s podstatným vlivem KB. Průměrný počet zaměstnanců skupiny KB v roce 2006 činil 8 266. [12]

Služby Komerční banky využívá více než 1,5 milionu zákazníků prostřednictvím telefonního, internetového a mobilního bankovnictví. Banka obsluhuje síť 379 poboček a 649 bankomatů po celé České republice. V rámci pobočkové sítě banka vybudovala 35 specializovaných obchodních míst tzv. business center, pro střední podniky a municipality a 8 center pro velké podniky. Tato centra byla od 1. ledna 2007 sloučena do 4 korporátních divizí. [12]

Po závazku garantované úrovně služeb, který Komerční banka přijala jako první na českém trhu, se banka přihlásila rovněž ke Kodexu vztahů mezi bankami a klienty, vypracovanému v rámci České bankovní asociace. Úsilí o neustálé zlepšování služeb bylo v roce 2006 odměněno několika oceněními, jako "MasterCard Firemní banka roku 2006" nebo "Nejlepší transakce roku 2006" udělená časopisem Global Trade Review. [12]

Produkty internetového bankovnictví

Počátky elektronického bankovnictví v Komerční bance byly založeny na technologii BBS (viz kapitola 2.1.1). KB nabízela tuto služby právnickým a fyzickým osobám –

podnikatelům i občanům. Prostřednictvím poboček a expozitur může klient disponovat se svými účty a získávat informace o jejich zůstatcích dvěma způsoby:

- předáváním a přejímáním přenosových kompatibilních médií (především disket),
- přenosem dat přes modem systémem BBS s využitím telefonních linek. [34]

Oba způsoby vycházely ze stejného základu. Podmínkou využívání služeb bylo vedení běžného účtů u KB, příslušné technické vybavení a písemné uzavření smlouvy o poskytování elektronických bankovních služeb. K pořizování dat mohl klient používat vlastní programové vybavení nebo mu banka zapůjčila program KB DATA. [35]

Pro zabezpečení autenticity a pro utajení elektronicky přenášených dat prostřednictvím BBS nebo na disketách byla používána metoda asymetrického šifrováníÍ. Použitá metoda umožňovala kompresi, šifrování a digitální podpis přenášených dat. [36]

Tabulka č. 1: Ceník BBS

Operace	Sazba v Kč
Připojení přímého klienta na elektronický přenos dat systémem BBS	3 000,-
Používání systému BBS přímým klientem	350,- měsíčně
Používání systému BBS každým dalším klientem napojeným na přímého klienta	350,- měsíčně
Osobní návštěva klienta na jeho požádání (odstranění závady způsobené klientem, poradenství)	500,- + 5% DPH

Zpracování: vlastní na základě údajů zjištěných ze sazebníku KB z roku 2000

Dnes již je tento způsob elektronické komunikace banky a klienta značně zastaralý, následně byl nahrazen vyspělejšími technologiemi. Stojí za zmínku, že systém založený na BBS byl i ve své době pro klienty dosti nákladným (viz Tabulka č.1) a nebyl tudíž využíván velkým množstvím klientů.

[34; 35; 36] PŘIHRÁDKA, M., KALA, J. *Elektronické bankovnictví : [rady a tipy]*. Vyd. 1. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5.

5.1.1 Moje banka

Internetové bankovnictví s názvem „Mojebanka“ je určeno občanům, podnikatelům a firmám. Tato služba umožňuje provádět vybrané bankovní operace prostřednictvím Internetu a nabízí tak nepřetržitý přístup do banky. Pomocí služby Mojebanka může klient obsluhovat všechny své účty, které lze určením rozsahu přístupových práv zpřístupnit i více uživatelům. [13]

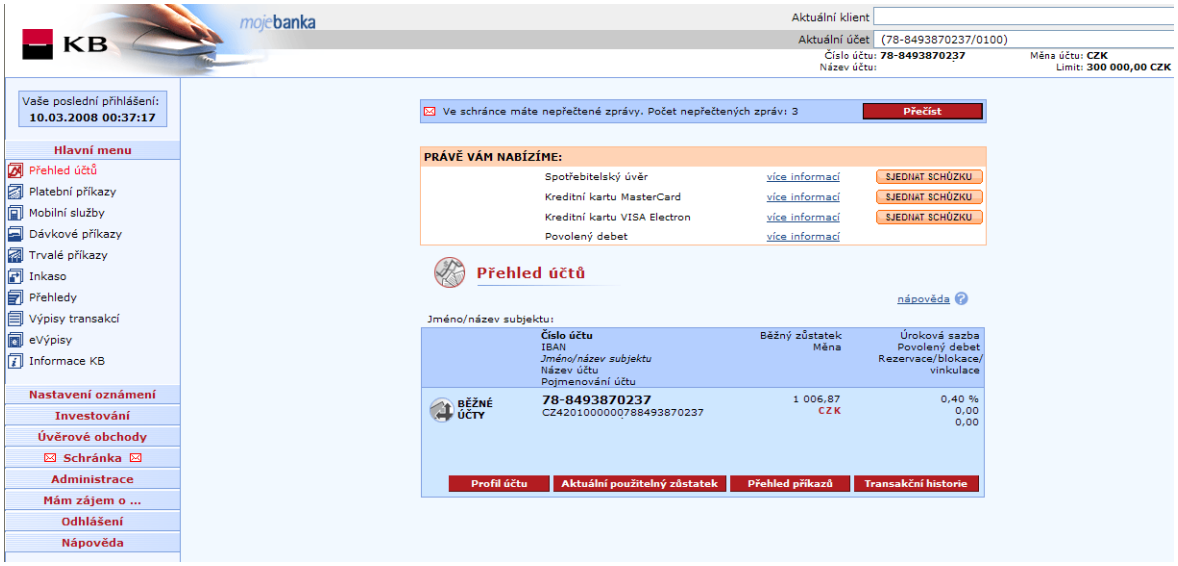
a) Možnosti služby Mojebanka

Služba Mojebanka klientovi umožňuje:

- získávat aktuální informace o účtech a transakcích (použitelný zůstatek, informace o výběrech z bankomatu a platbách provedených platební kartou, historie pohybů na účtu, apod.),
- zasílání SMS zpráv, e-mailů nebo faxů o nejrůznějších událostech na účtech (např. informace o zůstatku, o přijatých platbách, oznámení o operacích platební kartou atd.),
- stahování elektronických výpisů k účtům a platebním kartám s možností úplného zrušení zasílání papírových výpisů,
- zadávat příkazy k úhradě a inkasu, trvalé příkazy, povolit inkaso, nebo dobíjet kredit mobilního telefonu,
- propojit účetní systém s aplikací internetového bankovnictví (možnost zasílání platebních příkazů z účetního systému a stahování transakční historie do systému) a také
- on-line uzavřít smlouvu o investování do podílových fondů (aplikace nabízí neustálý přehled o investicích společně s aktuálními kurzy podílových fondů). [37]

Obr. č. 1: Prostředí aplikace Mojebanka

[37] *Mojebanka*[online]. [cit. 24. 2. 2008]. Dostupné z: <http://www.kb.cz/cs/seg/seg1/products/mojebanka.shtml>



Pramen: https://www.mojebanka.cz/InternetBanking/JSPLogin.jsp?L=CS

b) Bezpečnost

Bezpečnostní řešení, které aplikace Mojebanka využívá, je navrženo v souladu se standardy elektronického podpisu. Tak je zaručena vysoká úroveň zabezpečení jak při komunikaci mezi bankou a uživatelem, tak při podepisování příkazů v rámci služby. Veškerá komunikace probíhá v protokolu SSL (viz kapitola 3.1.3) a každou aktivní operaci uživatel podepisuje svým elektronickým podpisem, v případě užívání certifikátu v souboru navíc s doplňujícím autorizačním SMS kódem. [13]

Prvním nezbytným krokem pro založení služby Mojebanka je vytvoření osobního certifikátu v souboru nebo na čipové kartě. Osobní certifikát je obdobou průkazu totožnosti, kterým se klient prokazuje při elektronické komunikaci. Každý klient KB, který si přeje přistupovat ke svým účtům prostřednictvím Internetu, obdrží svůj osobní certifikát. Tento certifikát slouží pro zabezpečení komunikace mezi klientem a bankou. Osobní certifikát má podobu souboru a může být uložen na přenosném médiu (na disketě, USB flash disku, CD) nebo na čipové kartě. Osobní certifikát v souboru je platný jeden rok, osobní certifikát na čipové kartě je platný dva roky. Vydání a prodloužení osobního certifikátu poskytuje KB zdarma. [13]

V případě používání osobního certifikátu v souboru je nezbytné mít pro aktivní operace registrované mobilní telefonní číslo pro zasílání autorizačních SMS zpráv. Komerční

banka toto dodatečné bezpečnostní opatření zavedla v srpnu 2006 jako reakci na 10 zaznamenaných případů klientů, u nichž se objevily pokusy o zneužití jejich počítačů. Přechod na nový bezpečnostní systém probíhal v druhé polovině srpna 2006 a od 1. září 2006 již nebylo možné zadávat aktivní operace bez zadání autorizačního SMS kódu, který banka zasílá klientovi na předem registrované číslo mobilního telefonu. Jedná se o jednorázové heslo složené z různých kombinací čísel a písmen, které klient zadá do internetové aplikace, například při odesílání příkazu k úhradě (viz šipka 8. na Obr. č. 2) Pasivní operace (např. transakční historie, dotaz na zůstatek apod.) jsou od 1. září 2006 dostupné se stávajícím certifikátem bez nutnosti zadávání autorizačního SMS kódu. [13]

Obr. č. 2: Autorizace příkazu k úhradě pomocí autorizačního SMS kódu a certifikátu

Pramen: https://www.mojebanka.cz/InternetBanking/JSPLogin.jsp?L=CS

Osobní certifikát uložený na čipové kartě je určen pro klienty, kteří požadují vyšší zabezpečení uložení certifikátu. Hlavní výhodou a vlastností čipové karty je fakt, že certifikát z ní nelze žádným způsobem zkopírovat. Pokud tedy nedojde k fyzické ztrátě čipové karty, je zneužití certifikátu prakticky vyloučeno. Práce s certifikátem na čipové kartě je také mnohem snazší a rychlejší, neboť při využívání certifikátu na čipové kartě zadává klient pouze čtyřmístný PIN.

5.1.2 Profibanka

Profibanka je určena právnickým i fyzickým osobám podnikatelům s průměrným počtem plateb v rozmezí 101 až 3500 měsíčně. Statutární zástupce, popřípadě fyzická osoba podnikatel si může připojit i své soukromé účty. Elektronické bankovnictví Profibanka je špičkový produkt přímého bankovnictví KB, který spojuje výhody internetového bankovnictví s výkonností lokálních aplikací splňující všechny požadavky firem v oblasti platebního styku. Produkt Profibanka byl nasazen do plného produkčního provozu k 15. září 2001. [14]

a) Možnosti služby Profibanka

Aplikace Profibanka klientovi umožňuje:

- komplexní řešení firemního platebního styku a komunikace s bankou,
- nepřetržitý přehled o pohybech na účtech, efektivní řízení firemního cash flow,
- podstatnou časovou a finanční úspora oproti platebnímu styku na pobočkách,
- pohodlné zpracování velkého objemu plateb,
- časově neomezenou transakční historii, která zajistí přehled o všech obchodních aktivitách,
- velmi jednoduché a srozumitelné ovládání a
- špičkové zabezpečení založené na standardech elektronického podpisu.[38]

Nespornou výhodou aplikace Profibanka je schopnost spolupracovat s účetním systémem při zasílání platebních příkazů a stahování transakční historie. Používané formáty dat jsou BEST KB a Kompatibilní média (KM). Do těchto formátů nebo do vlastního formátu můžete také exportovat výpisy. Zobrazované informace pak lze uložit do souborů HTML. Služba je k dispozici ve dvou jazykových variantách – české a anglické. Stejně tak i tiskové výstupy a sestavy lze tisknout jak česky, tak anglicky. [14]

b) Bezpečnost

Bezpečnostní řešení, které Profibanka využívá, je navrženo v souladu se standardy elektronického podpisu. Tak je zaručena vysoká úroveň zabezpečení jak při komunikaci mezi bankou a uživatelem, tak při podepisování příkazů v rámci služby. Veškerá

[38] *Profibanka* [online]. [cit. 24. 2. 2008]. Dostupné z: < http://www.kb.cz/cs/seg/seg4/products/profibanka.shtml >

komunikace probíhá v protokolu SSL a každou aktivní operaci uživatel podepisuje svým elektronickým podpisem. [14]

Profibanka umožňuje zavést vícenásobnou kontrolu platebních příkazů zasílaných do banky. Integrovaná funkce vícenásobné autorizace dovoluje klientovi nechat každý příkaz či dávku příkazů podepsat až pěti podpisy. V praxi tento systém funguje například tak, že účetní připraví platební příkaz, který je pak podepsán manažerem a členem statutárního orgánu firmy. Dokud nemá platební příkaz požadovaný počet podpisů, banka ho nezpracuje. [13]

Zvláště výhodné je spojení lokální aplikace Profibanka s možnostmi internetového bankovnictví Mojebanka. Tak klient získá kompletní informace o všech svých účtech odkudkoliv na světě. Jedinečný systém Přímého bankovnictví KB klientům umožňuje používat produkty Mojebanka a Profibanka současně. Toto řešení je vhodné pro manažery, kteří potřebují mít přístup k bankovním účtům i mimo kancelář (např. z domova nebo na služební cestě). V praxi to může fungovat tak, že účetní připraví v sídle firmy platební příkazy prostřednictvím služby Profibanka a manažer je autorizuje na služební cestě pomocí služby Mojebanka.

5.1.3 Přímý kanál

Služba Přímý kanál je určen podnikatelům a firmám využívajícím účetní systémy. Přímý kanál je velmi jednoduchou a přitom efektivní nadstavbou služby Mojebanka. Nabízí možnost velmi jednoduše a rychle odesílat platební příkazy a stahovat výpisy přímo z prostředí účetního systému. Tím šetří čas, usnadňuje obsluhu a snižuje chybovost. Produkt přímý kanál byl nasazen do plného produkčního provozu k 1.červnu. 2002. [15]

a) Přednosti aplikace Přímý kanál

Aplikace Přímý kanál klientům umožňuje:

- pracovat pohodlně přímo ve známém prostředí klientova účetního systému,
- odesílat velké množství platebních příkazů a stahovat velké množství transakcí najednou,
- hromadně odesílat tuzemské i zahraniční platby,
- stahovat transakční historii a avíza z KB,

- stahovat výpisy z platebních karet (ve formátu PDF nebo strukturovaném formátu) a
- automatické stahování dat. [39]

Přímý kanál Vám nabízí klientům ještě další možnost, která výrazně urychluje komunikaci s bankou. Jde o automatické stahování dat pomocí firemního certifikátu. Tento způsob klientovi umožňuje mít každé ráno ve svém účetním a ekonomickém programu připraven aktuální zůstatek na účtech spolu s aktuálním přehledem o všech pohybech. Navíc je možné nastavit si libovolný interval stahování těchto dat (např. 10 sekund), takže klient může mít neustále perfektní přehled o stavu svých financí. Pro kontrolu informací již není třeba spouštět speciální bankovní aplikaci a je možné nerušeně dále pracovat v prostředí klientova účetního a ekonomického systému. [15]

b) Bezpečnost

Předpokladem pro založení služby Přímý kanál je vytvoření osobního certifikátu na čipové kartě. Tento certifikát slouží pro zabezpečení komunikace mezi klientem a bankou. Klient jej může používat při přihlašování a při podepisování jednotlivých transakcí. Veškerá komunikace probíhá v protokolu SSL a každou aktivní operaci uživatel podepisuje svým elektronickým podpisem zakódovaným v osobním certifikátu na čipové kartě. [15]

Stahování je navíc plně automatické a nevyžaduje zadávání hesla. To je nastaveno při zavedení služby a pak bezpečně uloženo v zašifrované podobě. Stahování si také může klient snadno načasovat pomocí externích programů, jako je MS Schedule. Automatické stahování dat umožňuje firemní certifikát, což je soubor, který lze uchovávat na disketě nebo na pevném disku klientova počítače (stejně jako osobní certifikát). Firemní certifikát je určen pouze pro pasivní přístup k informacím. Není s ním možné podepisovat a odesílat platby do banky. Platí dva roky od data vydání (s možností bezplatného prodloužení platnosti). [15]

[39] *Přímý kanál* [online]. [cit. 24.2.2008].
Dostupné z: <http://www.kb.cz/cs/seg/seg4/products/direct_channel.shtml>

5.1.4 EDI (Electronic Data Interchange)

Služba EDI KB je určena velkým podnikovým klientům – právnickým osobám, kteří přenášejí velké objemy dat, zpracovávají data automatizovaným způsobem, případně již používají systém EDI v jiných bankách (například ČSOB). [16]

Výměna dat mezi klientem a bankou probíhá na úrovni komunikace dvou EDI serverů (EDI server banky a EDI server klienta). Data jsou generována aplikací, konvertována, zabezpečena a odeslána klientem bance, nebo naopak. Tento způsob komunikace je vhodný pro dávkový režim platebních příkazů, protože předávání zpráv probíhá prostřednictvím schránek sítě X.400, což je veřejná datová síť provozovaná třetí stranou, specializovaná na výměnu dat ve formátu UN/EDIFACT. Banka nicméně zpracovává dávky příkazů převážně v režimu online (podle svých provozních možností), aby klientovi umožnila zrychlit cash flow. O této skutečnosti banka klienta informuje prostřednictvím avíza, které klient obdrží na základě sjednaných smluvních podmínek. Server klienta komunikuje přímo s centrálním systémem KB po celých 24 hodin. [40]

a) Výhody služby EDI KB

Produkt EDI KB přináší svým klientům následující výhody:

- přímé propojení systémů banky a klienta,
- bezproblémový přenos velkých objemů dat,
- zpracování plateb v režimu online
- aktuální informace o platbách zúčtovaných online prostřednictvím nástrojů přímého bankovnictví a v neposlední řadě
- vysoká úroveň zabezpečení předávaných dat. [41]

Klient je informován o provedených platbách prostřednictvím kreditních a debetních avíz zasílaných z banky podle smluvně sjednaného režimu. Kreditní avízo informuje o zaúčtované došlé platbě ze zahraničí či o tuzemské platbě zaúčtované v bance v režimu online. Avízo je generováno k platbám realizovaným v bance prostředky přímého bankovnictví KB (Mojebanka, Profibanka, Přímý kanál, EDI KB) s podmínkou, že druhý

[40; 41] *EDI* [online]. [cit. 24.2.2008].Dostupné z: < http://www.kb.cz/cs/seg/seg4/products/edi.shtml >

subjekt je též klientem Komerční banky. Debetní avízo informuje o zaúčtované vyšlé platbě do zahraničí či o tuzemské platbě zaúčtované v bance v režimu online. I v tomto případě je avízo generováno k platbám realizovaným v bance prostředky přímého bankovnictví KB. Klient může též získat informace o aktuálním stavu jím odeslaných plateb nebo o platbách přicházejících v průběhu dne na jeho účet prostřednictvím aplikací přímého bankovnictví Mojebanka nebo Profibanka. To se týká plateb zpracovávaných v rámci KB, nikoliv plateb z jiných bank. [16]

b) Bezpečnost

Systém EDIFACT zajišťuje jeden z nejdokonalejších způsobů ochrany dat, jaké se dnes ve světě používají. Zabezpečení elektronické výměny dat zahrnuje:

- digitální podpis pro zajištění integrity a neodmítnutelnosti předávaných dat,
- šifrování zpráv pomocí algoritmů DES/RSA,
- automaticky generovanou bezpečnostní zprávu AUTACK, která informuje odesílatele o tom, že protistrana zásilku přijala a odstranila její zabezpečení. [42]

Komerční banka pro klienty služby EDI KB zajišťuje také certifikaci veřejných klíčů prostřednictvím vlastní certifikační autority. [16]

6 Internetové bankovnictví Československé obchodní banky

Profil banky

[42] *EDI* [online]. [cit. 24.2.2008]. Dostupné z: < http://www.kb.cz/cs/seg/seg4/products/edi.shtml >

Skupina ČSOB je vedoucím hráčem na trhu finančních služeb v České republice. Skupina ČSOB je součástí mezinárodní bankopojišťovací Skupiny KBC, která aktivně působí v Belgii a v regionu střední a východní Evropy s tržní kapitalizací přes 30 mld. euro. [18]

Československá obchodní banka, a. s. (ČSOB) působí jako univerzální banka v České republice. ČSOB byla založena státem v roce 1964 jako banka pro poskytování služeb v oblasti financování zahraničního obchodu a volnoměnových operací. V červnu 1999 byla privatizována – jejím majoritním vlastníkem se stala belgická KBC Bank, která je součástí finanční skupiny KBC Banking and Insurance Group. Tato finanční skupina patří mezi nevětší a nejsilnější skupiny svého druhu v Evropě. Dalšími akcionáři se staly Evropská banka pro obnovu a rozvoj a Mezinárodní finanční korporace ze skupiny Světové banky. V červnu 2000 ČSOB převzala Investiční a poštovní banku. Tímto strategickým spojením vznikla nejsilnější banka v České republice. Do konce roku 2007 působila ČSOB na českém i slovenském trhu; slovenská pobočka ČSOB byla oddělena k 1.1.2008. [17]

Obchodní profil ČSOB zahrnuje následující segmenty: fyzické osoby (retailová klientela), malé a středně velké podniky, korporátní klientela a nebankovní finanční instituce, finanční trhy a privátní bankovnictví. V retailovém bankovnictví v ČR působí společnost pod dvěma obchodními značkami – ČSOB a Poštovní spořitelna, která využívá pro svou činnost rozsáhlé sítě České pošty. Klienti ČSOB jsou obsluhováni na 221 pobočkách v ČR, klienti Poštovní spořitelny jsou obsluhováni prostřednictvím 27 finančních center Poštovní spořitelny a zhruba na 3 340 obchodních místech České pošty (stav k 30. 9. 2007). ČSOB i Poštovní spořitelna dále poskytují své služby prostřednictvím různých kanálů přímého bankovnictví. [17]

Pobočková síť ČSOB nabízí současně se svými produkty a službami i produkty a služby celé Skupiny ČSOB. Ucelená nabídka služeb tak kromě bankovních služeb zahrnuje i pojistné a penzijní produkty (ČSOB Pojišťovna a penzijní fondy Stabilita a Progres), financování bydlení (Hypoteční banka a Českomoravská stavební spořitelna), kolektivní investování a správu majetku (investiční fondy ČSOB Investiční společnosti a ČSOB Asset Management) a specializovaných služeb (ČSOB Leasing a ČSOB Factoring). Služby

spojené s obchodováním na finančních trzích poskytuje Patria, sesterská společnost ČSOB. [17]

Kombinace síly značek ČSOB (pro bankovnictví, pojištění, správu aktiv, penzijní fondy, leasing a factoring), Poštovní spořitelna (bankovnictví v síti pošt), Hypoteční banka (hypotéky) a Českomoravská stavební spořitelna (financování bydlení) umožňuje Skupině ČSOB zaujímat silné pozice ve všech segmentech českého finančního trhu. [18]

Produkty internetového bankovnictví

6.1.1 ČSOB Internetbanking 24

ČSOB Internetbanking 24 je služba internetového bankovnictví určená všem klientům z řad fyzických osob, fyzických osob – podnikatelů i právnických osob. Nespornou předností této služby je přístup z jakéhokoliv počítače (splňujícího minimální hardwarové a softwarové požadavky) připojeného na síť Internet a vybaveného internetovým prohlížečem. To vše při zachování bezpečnosti a důvěrnosti přenášených dat. [19]

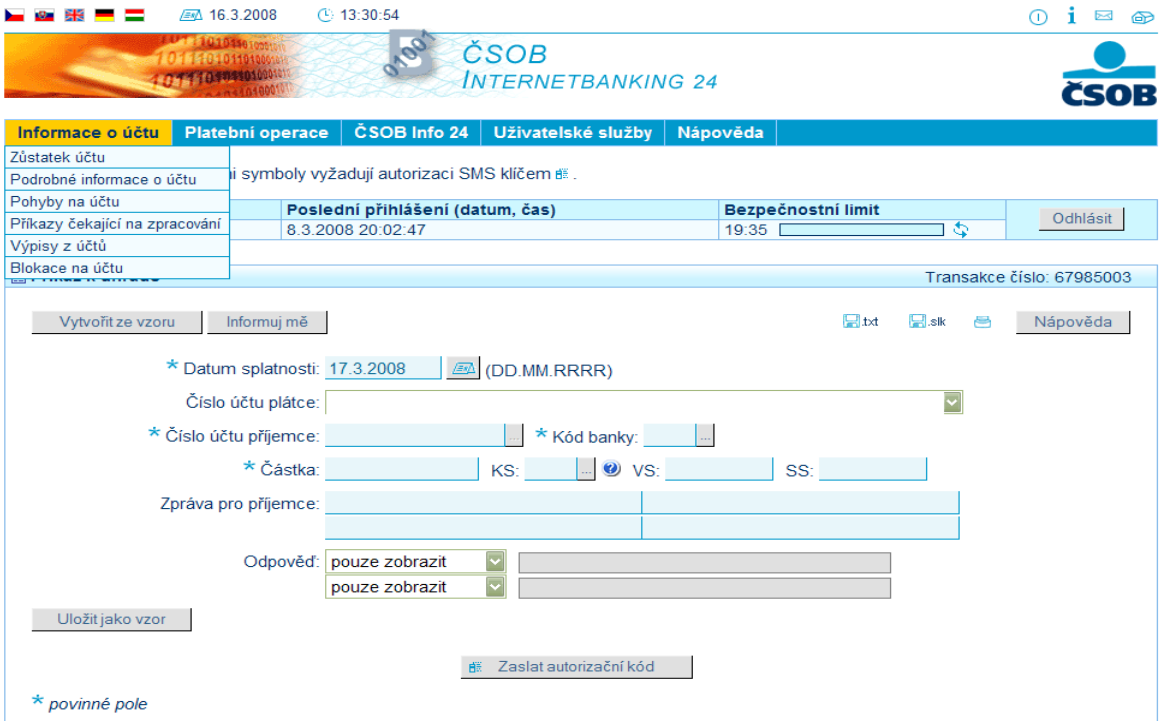
a) Možnosti služby ČSOB Internetbanking 24

ČSOB Internetbanking24 klientům umožňuje:

- zjišťování informací o účtu (zůstatek, pohyby na účtu, příkazy čekající na zpracování apod.),
- zadávání platebních operací prostřednictvím internetové aplikace (jednorázový či trvalý příkaz k úhradě, příkazy k inkasu, bankovní převody do zahraničí atd.),
- nastavení zasílání SMS zpráv nebo e-mailů o pohybech a zůstatku na účtu, transakcích platební kartou, kurzovním lístku a dalších aktualitách. [43]

Obr. č. 3: Prostředí aplikace ČSOB Internetbanking 24

[43] *ČSOB Internetbaking 24* [online]. [cit. 24. 2. 2008]. Dostupné z: < http://www.csob.cz/bankcz/cz/Produktovy-katalog/Elektronicke-bankovnictvi/CSOB-Internetbanking-24/CSOB-Internetbanking-24.htm >



Pramen: https://ib24.csob.cz/

b) Způsoby autorizace

Při zřízení služby si klient může vybrat ze dvou způsobů autorizace:

- elektronickým podpisem,
- SMS klíčem. [44]

Elektronický podpis

Elektronický podpis se generuje se na základě údajů (privátního klíče, veřejného klíče, certifikátu), které jsou uloženy z důvodu maximálního zabezpečení na kryptografické čipové kartě. Čipovou kartu získá klient při zřízení služby ČSOB Internetbanking 24. Je chráněna před zneužitím PINem a vysoká míra zabezpečení je dána skutečností, že klientovy údaje nikdy čipovou kartu neopustí (není je možné z karty přehrát jinam). Samotný elektronický podpis je také generován přímo v čipu karty a jeho generování nelze spustit bez znalosti PINu ke kartě. Pro komunikaci PC s čipovou kartou slouží čtečka čipových karet, kterou banka nabízí klientům při zřízení služby přímého bankovnictví. Nutnou podmínkou pro komunikaci s použitím elektronického podpisu je certifikát, který

[44] *ČSOB Internetbaking 24* [online]. [cit. 24. 2. 2008]. Dostupné z: < http://www.csob.cz/bankcz/cz/Produktovy-katalog/Elektronicke-bankovnictvi/CSOB-Internetbanking-24/CSOB-Internetbanking-24.htm >

je klientovi zaregistrován na pobočce banky při zřízení služby. ČSOB nabízí ke službě ČSOB Internetbanking 24 dva typy certifikátů – komerční a kvalifikovaný. [19]

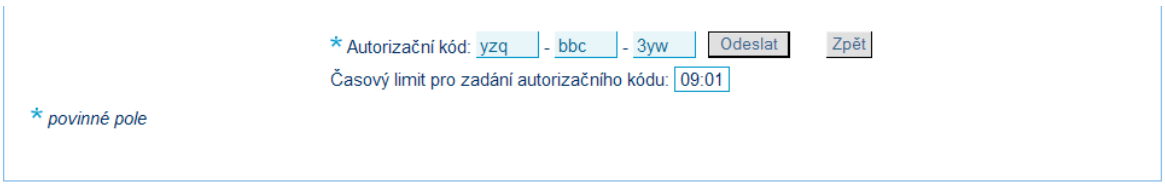
Komerční certifikát je určený pro běžné použití v rámci služby ČSOB Internetbanking 24. Kvalifikovaný certifikát je možné používat i pro komunikaci mimo službu ČSOB Internetbanking 24 a je ze zákona akceptován stejně jako občanský průkaz (např. pro komunikaci se státní správou, zdravotními pojišťovnami apod.). [19]

SMS klíč

SMS klíč je další ze způsobů autorizace aktivních operací služby ČSOB Internetbanking 24. Pokud si klient nechá aktivovat tento způsob autorizace, při zadávání aktivní operace mu bude při zadávání bankovních převodů zaslán SMS zprávou na mobilní telefon jednorázový autorizační kód pro danou operaci, vygenerovaný na základě klientova požadavku. [19]

Autorizační kód má podobu devítimístného alfanumerického řetězce složeného z malých písmen a číslic, který je pro lepší přehlednost rozdělen na trojice znaků oddělených pomlčkami (např. asd-v1b-gh7). Tento kód poté klient vepíše do určeného pole na formuláři. Pro jeho zadání má klient vyměřen časový limit 10 minut. Stiskem tlačítka „Odeslat“ proběhne autorizace a příkaz bude odeslán ke zpracování do banky. V případě chybného zadání autorizačního kódu do určených polí na formuláři dojde po pátém chybně zadaném autorizačním kódu k zablokování služby. Odblokování je možné pouze na pobočce ČSOB. [19]

Obr. č. 4: Zadání autorizačního SMS kódu



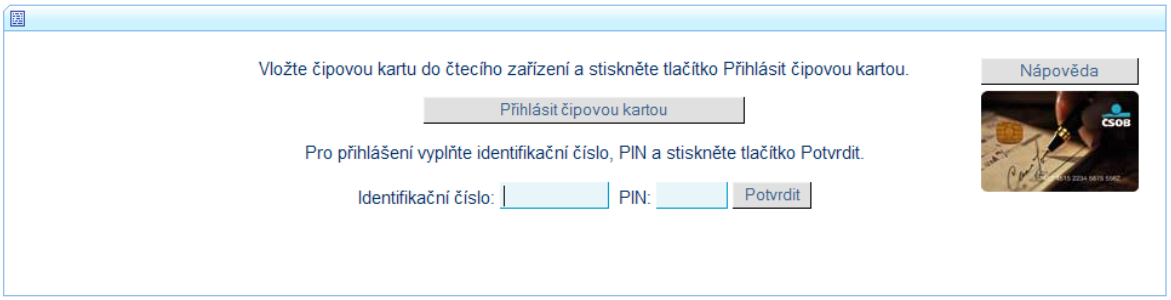
Pramen: https://ib24.csob.cz/

c) Způsoby přihlášení do internetové aplikace

ČSOB nabízí následující tři způsoby přihlášení do aplikace:

- identifikačním číslem a PINem,
- identifikačním číslem, PINem a SMS klíčem,
- certifikátem k elektronickému podpisu (na čipové kartě). [45]

Obr. č. 5: Přihlášení do internetové aplikace



Pramen: https://ib24.csob.cz/

Přihlášení ke službě je možné prostřednictvím identifikačního čísla a PINu, pro zvýšení bezpečnosti lze tento způsob přihlášení rozšířit o přihlášení pomocí SMS klíče (devítimístný alfanumerický řetězec malých písmen a číslic, který je klientovi automaticky zaslán SMS zprávou na mobilní telefon). Pokud pro autorizaci transakcí klient využívá certifikát k elektronickému podpisu, může jej využít i pro přihlášení. V průběhu přihlášení je nutné zadat PIN k čipové kartě, na níž je certifikát uložen. Po zadání správného PINu k čipové kartě je vygenerován elektronický podpis a odeslán na autentizační server k ověření identifikace. [19]

6.1.2 ČSOB Businessbanking 24

Služba určená podnikatelům a firmám k obsluze podnikových financí prostřednictvím osobního počítače s připojením k Internetu. Kromě informací o stavu a pohybech na účtu nabízí i možnost provádět vybrané bankovní operace. Své finance klient obsluhuje z počítače připojeného k Internetu (on-line režim) nebo z prostředí aplikace bez nutnosti připojení k Internetu (off-line režim). [20]

[45] *ČSOB Internetbaking 24* [online]. [cit. 24. 2. 2008]. Dostupné z: < http://www.csob.cz/bankcz/cz/Produktovy- katalog/Elektronicke-bankovnictvi/CSOB-Internetbanking-24/CSOB-Internetbanking-24.htm >

V off-line režimu lze:

- zadávat tuzemské příkazy k úhradě/inkasu i příkazy do zahraničí,
- vytvářet hromadná zadání příkazů k úhradě/inkasu,
- zobrazit kreditní i debetní avíza, výpisy z účtů a kurzovní lístky,
- zadávat tuzemské prioritní platby,
- exportovat/importovat data do/z účetních systémů. [46]

V on-line režimu je možné:

- zadávat všechny typy plateb jako v on-line režimu a dále
- zadávat trvalé příkazy k úhradě/inkasu,
- zadávat svolení k inkasu (zřízení, změna, zrušení),
- dobíjet kredit SIM karet mobilních operátorů ,
- získávat informace o aktuálním zůstatku a historii účtu,
- nastavit automatické zasílání vybraných informací prostřednictvím SMS zpráv nebo e-mailem (ČSOB Info 24). [47]

6.1.3 ČSOB Businessbanking 24 Online

Businessbanking 24 Online je služba určená podnikatelům a firmám k obsluze podnikových financí prostřednictvím osobního počítače s připojením k Internetu. Kromě provádění bankovních operací nabízí možnost získávat informace o stavu a pohybech na účtu a podporuje i výměnu dat s účetními systémy. [20]

a) Výhody služby ČSOB Businessbanking 24 Online

Mezi přednosti aplikace Businessbanking 24 Online patří:

- možnost importu platebních příkazů a
- export datových souborů – výpisů do účetních programů,
- finanční zvýhodnění elektronického platebního styku,

[46; 47] *ČSOB BusinessBanking 24* [online]. [cit. 24. 2. 2008]. Dostupné z:
< http://www.csob.cz/bankcz/cz/Firmy/Podnikatele/Elektronicke-bankovnictvi/CSOB-BusinessBanking-24.htm >

- uživatelská podpora na lince technické podpory,
- instalační a servisní služby specializované firmy,
- praktičnost práce v on-line (internetový prohlížeč) režimu,
- kompatibilita s většinou užívaných účetních systémů s podporou vzájemné výměny dat a také
- jazykové mutace - čeština, angličtina, němčina, maďarština a slovenština. [48]

Oproti off-line aplikaci má klient k dispozici všechny funkce systému při větším komfortu, bez nutnosti instalace aplikace. Zároveň se zrychluje práce s aplikací a přístup k datům.

b) Zabezpečení

Mimořádně kvalitní zabezpečení služby je založené na nejvyšších standardech. Transakce jsou opatřeny digitálními podpisy oprávněných osob, jejichž certifikáty jsou uloženy na čipových kartách. Služba umožňuje využívat kvalifikovaný certifikát vydaný podle zákona o elektronickém podpisu. [20]

6.1.4 ČSOB Homebanking 24

Služba ČSOB Homebanking 24 umožňovala přístup k účtu prostřednictvím klientova počítače a sítě Internet. Uživatel byl nucen pracovat ve dvou prostředích - v aplikaci nainstalované na pevném disku svého počítače a v prostředí internetového prohlížeče. [20]

V případě tohoto produktu můžeme pozorovat rychlý vývoj v oblasti internetové komunikace mezi bankou a klientem. Tato služba elektronického bankovnictví se již nezřizuje novým, ani stávajícím klientům, jelikož byla nahrazena technologicky dokonalejšími produkty BusinessBanking 24 a BusinessBanking 24 online a byla tudíž vyřazena z prodeje. [21]

[48] *ČSOB Businessbanking 24* [online]. [cit. 24. 2. 2008].
Dostupné z: < http://www.csob.cz/bankcz/cz/Firmy/Podnikatele/Elektronicke-bankovnictvi/CSOB-BusinessBanking-24.htm >

7 Komparace nákladů internetového bankovnictví KB a ČSOB

V této části se pokusím zjistit a na konkrétním příkladu ukázat, jak velkou úsporu na poplatcích přinese klientovi implementace internetového bankovnictví, a zároveň porovnám produkty KB a ČSOB z hlediska nabízených způsobů zabezpečení.

Porovnání nákladů na služby internetového bankovnictví

Komparace nákladů bude zahrnovat porovnání výše poplatků klienta nevyužívajícího služeb internetového bankovnictví (a ani jiného přímého kanálu) s celkovou sumou poplatků klienta využívajícího služeb internetového bankovnictví. K výpočtu celkových nákladů použiji předpokladu, že oba typoví klienti provádějí hotovostní operace a platby pomocí platební karty, která je již v České republice rozšířená i mezi klienty nevyužívajícími přímé bankovnictví.

Typovým klientem bude nepodnikající fyzická osoba neboli občan, který má založen klasický typ běžného účtu, na němž provádí obvyklé bankovní operace. Struktura a množství bankovních operací modelového klienta je složena takovým způsobem, aby byla rozmanitá a zároveň v praxi použitelná. Jsou v ní zastoupeny diferencované typy transakcí v různé četnosti dle typických požadavků dnešních bankovních klientů.

7.1.1 Výše poplatků klienta nevyužívajícího internetové bankovnictví

Skladba bankovních operací u klienta nevyužívajícího internetové bankovnictví je následující:

- vedení účtu,
- výpis z účtu zasílaný poštou 1×,
- došlé platby ze stejné banky 2 ×,
- došlé platby z jiného peněžního ústavu 2×,
- založení povoleného inkasa 1×,
- založení trvalého příkazu 1×,
- zrušení trvalého příkazu 1×,
- platba na základě trvalého příkazu do stejné banky 2×,
- platba na základě trvalého příkazu do jiného peněžního ústavu 2×,
- platba na základě povoleného inkasa do stejné banky 2×,
- platba na základě povoleného inkasa do jiného peněžního ústavu 2×,
- jednorázový příkaz k úhradě do stejné banky 2×,
- jednorázový příkaz k úhradě do jiného peněžního ústavu 1×.

Oba klienti využívají platební kartu pro tyto typy transakcí:

- výběr z bankomatu vlastní banky 5×,
- výběr z bankomatu cizí banky 2×,
- platba u obchodníka 8×,
- poplatek za platební kartu.

Klient ČSOB bude mít pro platební styk zřízen ČSOB běžný účet v českých korunách a klient KB účet nazvaný Ideal konto. Oba tyto účty jsou klasické typy běžných bankovních účtu, které v sobě zahrnují základní nabídku bankovních služeb na zhruba stejné a tudíž vzájemně dobře porovnatelné úrovni.

Ke každému z účtů je poskytována platební karta Visa Electron za stejný poplatek 200 Kč ročně. Komerční banka v rámci Ideal konta nabízí jeden výběr platební kartou z bankomatu vlastní banky zdarma.

Tabulka č. 2: Souhrn měsíčních poplatků klienta nevyužívajícího internetové bankovnictví

Operace	KB Ideal konto		ČSOB BÚ	
	za položku	měsíčně	za položku	měsíčně
Vedení účtu	22,-	22,-	20,-	20,-
Výpis z účtu zaslaný poštou	20,-	20,-	10,-	10,-
Došlé platby			6,-	24,-
- v rámci banky	5,-	10,-		
- do jiné banky v ČR	7,-	14,-		
Povolení k inkasu na pobočce	39,-	39,-	-	-
Založení trvalého příkazu k úhradě	39,-	39,-	-	-
Zrušení trvalého příkazu k úhradě	-	-	40,-	40,-
Platba vzniklá na základě trvalého příkazu k úhradě				
- v rámci banky	4,50	9,-	6,-	12,-
- do jiné banky v ČR	6,50	13,-	6,-	12,-
Odepsané inkaso				
- v rámci banky	5,-	10,-	6,-	12,-
- do jiné banky v ČR	7,-	14,-	6,-	12,-
Platba vzniklá z jednorázového příkazu k úhradě zadaného na pobočce				
- v rámci banky	20,-	40,-	30,-	60,-
- do jiné banky v ČR	22,-	22,-	30,-	30,-
Poplatek za platební kartu [1)]	16,70	16,70	16,70	16,7
Výběr z bankomatu v ČR				
- vlastní banky	5,- [2)]	20,- [2)]	6,-	30,-
- jiné banky	35,-	70,-	30,-	60,-
Platba u obchodníka	-	-	-	-
Celkem	**253,70 Kč**	**358,70 Kč**	**212,70 Kč**	**338,70 Kč**

[1)] roční poplatek za kartu u obou bank 200 Kč (200/12 =16,70);
[2)] 1 výběr z bankomatu vlastní banky měsíčně zdarma

Zpracování: vlastní na základě údajů ze sazebníků bank

Jak ukazuje tabulka č. 2, celkový souhrn poplatků za vedení běžného účtu a bankovní operace jsou u obou zmiňovaných bank poměrně vysoké. U ČSOB se celková výše pohybuje těsně pod 340 korunami a u Komerční banky je to o přesně o 20 korun více.

7.1.2 Výše poplatků klienta využívajícího internetové bankovnictví

U klienta využívajícího služeb internetového bankovnictví je struktura bankovních operací následující:

- vedení účtu,
- výpis z účtu zasílaný elektronicky 1× za měsíc,
- založení internetového bankovnictví,
- vedení internetového bankovnictví,
- došlé platby ze stejné banky 2×,
- došlé platby z jiného peněžního ústavu 2×,
- založení povoleného inkasa 1×,
- založení trvalého příkazu 1×,
- zrušení trvalého příkazu 1×,
- platba na základě trvalého příkazu do stejné banky 2×,
- platba na základě trvalého příkazu do jiného peněžního ústavu 2×,
- platba na základě povoleného inkasa do stejné banky 2×,
- platba na základě povoleného inkasa do jiného peněžního ústavu 2×,
- jednorázový příkaz k úhradě do stejné banky 2×,
- jednorázový příkaz k úhradě do jiného peněžního ústavu 1×.

V následující tabulce č. 3 je zachycen souhrn poplatků u obou bank při implementaci internetového bankovnictví. Předpokládejme, že klient Komerční banky si jako bezpečnostní prvky pro přístup do internetové aplikace a pro provádění aktivních operací zvolil certifikát uložený v souboru a autorizační SMS zprávy, klient ČSOB kombinaci identifikačního čísla, PINu a autorizačních SMS zpráv. V těchto případech je u obou bank zřízení služeb internetového bankovnictví zdarma.

Jak je na první pohled z tabulek č. 2 a 3 patrné, celková výše poplatků u klientů obou bank výrazně klesla. U Komerční banky celková úspora přesáhla 100 Kč a u ČSOB je to téměř 140 korun.

Tabulka č. 3: Souhrn měsíčních poplatků klienta využívajícího internetové bankovnictví

Operace	KB Ideal konto		ČSOB BÚ	
	za položku	měsíčně	za položku	měsíčně
Vedení účtu	22,-	22,-	20,-	20,-
Výpis z účtu zaslaný emailem	-	-	-	-
Zřízení internetového bankovnictví	-	-	-	
Vedení internetového bankovnictví	39,-	39,-	-	
Došlé platby			6,-	24,-
- v rámci banky	5,-	10,-		
- do jiné banky v ČR	7,-	14,-		
Povolení k inkasu - elektronicky	-	-	-	-
Založení trvalého příkazu k úhradě	-	-	-	-
Zrušení trvalého příkazu k úhradě	-	-	6,-	6,-
Platba vzniklá na základě trvalého příkazu k úhradě				
- v rámci banky	4,50	9,-	3,-	6,-
- do jiné banky v ČR	6,50	13,-	3,-	6,-
Odepsané inkaso				
- v rámci banky	5,-	10,-	6,-	12,-
- do jiné banky v ČR	7,-	14,-	6,-	12,-
Platba vzniklá z jednorázového příkazu k úhradě zadaného elektronicky				
- v rámci banky	4,-	8,-	3,-	6,-
- do jiné banky v ČR	6,-	6,-	3,-	3,-
Poplatek za platební kartu [1)]	16,70	16,70	16,70	16,7
Výběr z bankomatu v ČR				
- vlastní banky [2)]	5,-	20,-	6,-	30,-
- jiné banky	35,-	70,-	30,-	60,-
Platba u obchodníka	-	-	-	-
Celkem	**162,70 Kč**	**251,70 Kč**	**108,70 Kč**	**201,70 Kč**

[1)] roční poplatek za kartu u obou bank 200 Kč (200/12 =16,70);
[2)] 1 výběr z bankomatu vlastní banky měsíčně zdarma

Zpracování: vlastní na základě údajů ze sazebníků bank

7.1.3 Výše úspory při využití služeb internetového bankovnictví

Jaké položky se na úspoře podílely nejvíce, zobrazují následující tabulky. U Komerční banky (viz tabulka č. 4) platí klient za využívání služeb internetového bankovnictví měsíční poplatek 39 Kč, který je ovšem několikanásobně kompenzován snížením sazeb u většiny operací. Největší úsporu klient získá využitím elektronického zasílání výpisu z účtu, které je zcela zdarma, a při zadávání trvalého příkazu k úhradě či povolení k inkasu, které lze realizovat pomocí aplikace Mojebanka také zcela zdarma. Další redukci nákladů přestavuje elektronické zadávání jednorázového příkazu k úhradě, jehož sazba klesla až

pětinásobně; z původních 20,- korun v rámci KB, na pouhé 4 koruny. Poplatky za transakce provedené platební kartou jsou u klientů obou bank shodné.

Tabulka č. 4: Měsíční úspora na poplatcích u klienta KB

Operace	Poplatky klienta bez internet. bankovnictví	Poplatky klienta s internet. bankovnictvím
Vedení účtu	22,-	22,-
Výpis z účtu	20,-	-
Zřízení internetového bankovnictví	-	-
Vedení internetového bankovnictví	-	39,-
Došlé platby	24,-	24,-
Povolení k inkasu na pobočce	39,-	-
Založení trvalého příkazu k úhradě	39,-	-
Zrušení trvalého příkazu k úhradě	-	-
Platba vzniklá na základě trvalého příkazu k úhradě		
- v rámci banky	9,-	9,-
- do jiné banky v ČR	13,-	13,-
Odepsané inkaso		
- v rámci banky	10,-	10,-
- do jiné banky v ČR	14,-	14,-
Platba vzniklá z jednorázového příkazu k úhradě		
- v rámci banky	40,-	8,-
- do jiné banky v ČR	22,-	6,-
Poplatek za platební kartu [1)]	16,70	16,70
Výběr z bankomatu v ČR		
- vlastní banky [2)]	20,-	20,-
- jiné banky	70,-	70,-
Platba u obchodníka	-	-
Celkem	**358,70 Kč**	**251,70 Kč**

[1)] roční poplatek za kartu u obou bank 200 Kč (200/12 =16,70);
[2)] 1 výběr z bankomatu vlastní banky měsíčně zdarma

Zpracování: vlastní na základě údajů ze sazebníků bank

V případě klienta ČSOB (viz tabulka č. 5) je měsíční úspora při zavedení internetového bankovnictví ještě vyšší než u KB. To je způsobeno především absencí měsíčního poplatku za využívání služeb internetového bankovnictví ČSOB a také výrazným snížením poplatků při elektronickém zadání jednorázového příkazu k úhradě, kde se poplatek snížil až desetinásobně (z původních 30 Kč při zadání na pobočce na 3 Kč při zadání pomocí internetové aplikace). Další výraznou úsporu představuje bezplatné zasílání výpisu z účtu elektronickou formou a snížení poplatku za zrušení trvalého příkazu k úhradě z původních 40 Kč na 6 Kč.

Tabulka č. 5: Měsíční úspora na poplatcích u klienta ČSOB

Operace	Poplatky klienta bez internet. bankovnictví	Poplatky klienta s internet. bankovnictvím
Vedení účtu	20,-	20,-
Výpis z účtu	10,-	-
Zřízení internetového bankovnictví	-	-
Vedení internetového bankovnictví	-	-
Došlé platby	24,-	24,-
Povolení k inkasu na pobočce	-	-
Založení trvalého příkazu k úhradě	-	-
Zrušení trvalého příkazu k úhradě	40,-	6,-
Platba vzniklá na základě trvalého příkazu k úhradě		
- v rámci banky	12,-	6,-
- do jiné banky v ČR	12,-	6,-
Odepsané inkaso		
- v rámci banky	12,-	12,-
- do jiné banky v ČR	12,-	12,-
Platba vzniklá z jednorázového příkazu k úhradě		
- v rámci banky	60,-	6,-
- do jiné banky v ČR	30,-	3,-
Poplatek za platební kartu [1)]	16,7	16,7
Výběr z bankomatu v ČR		
- vlastní banky [2)]	30,-	30,-
- jiné banky	60,-	60,-
Platba u obchodníka	-	-
Celkem	**338,70 Kč**	**201,70 Kč**

[1)] roční poplatek za kartu u obou bank 200 Kč (200/12 =16,70);
[2)] 1 výběr z bankomatu vlastní banky měsíčně zdarma

Zpracování: vlastní na základě údajů ze sazebníků bank

Poplatky za transakce provedené platební kartou jsou opět u obou typů klientů stejné, přičemž jak u KB, tak u ČSOB platí, že banka výrazně zvýhodňuje výběry z bankomatů vlastní banky, za které se platí u KB 5 korun a u ČSOB 6 Kč, oproti výběrům z bankomatů jiných bank, kde činí poplatek 35 korun.

Na základě zjištěných údajů spočítám procentuelní úsporu na poplatcích při využívání internetového bankovnictví. Rozdíl celkového úhrnu poplatků při nevyužití internetového bankovnictví a součtu poplatků při jeho využití vydělím celkovou výší poplatků klienta nevyužívajícího internetové bankovnictví. Tento výpočet ukazuje procentní úsporu na poplatních při využití internetového bankovnictví.

Procentní úspora na poplatcích u klienta KB

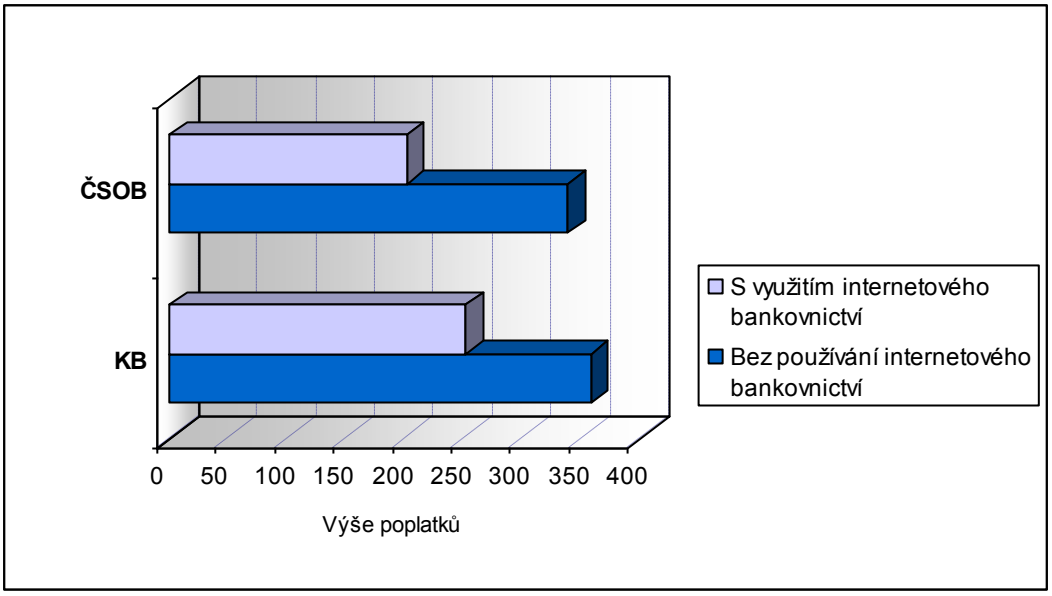
$\frac{358{,}70 - 251{,}70}{358{,}70} = 0{,}298$ -> **29,8%**

Procentní úspora na poplatcích u klienta ČSOB

$\frac{338{,}70 - 201{,}70}{338{,}70} = 0{,}4045$ -> **40,5 %**

Z provedených výpočtů vyplývá, že implementace internetového bankovnictví u klienta Komerční banky mu může přinést téměř třicetiprocentní úsporu na celkových poplatcích za vedení a bankovní transakce provedené na jeho běžném účtu. V případě ČSOB je tato úspora ještě vyšší, dosahuje až přes 40% celkové výše poplatků klienta nevyužívajícího služeb internetového bankovnictví. Tyto závěry jsou jasně patrné i v grafickém vyjádření.

Graf č. 6: Celkový souhrn měsíčních poplatků klienta u KB a ČSOB



Zpracování: vlastní na základě údajů z tabulek č. 4, 5

7.1.4 Způsoby přihlášení do internetových aplikací

a) KB

Prvním nezbytným krokem pro založení internetového bankovnictví KB je vytvoření osobního certifikátu v souboru nebo na čipové kartě. KB nabízí pro přihlášení do aplikace Mojebanka dva způsoby, které záleží na tom, jaký typ certifikátu si klient zvolí.

KB nabízí dva typy certifikátů:

- certifikát v souboru nebo
- certifikát na čipové kartě.

Osobní certifikát má podobu souboru a může být uložen na přenosném médiu nebo na čipové kartě. Pro využívání služby Přímý kanál je nutné založení osobního certifikátu na čipové kartě. Platnost osobního certifikátu v souboru je jeden rok, osobní certifikát na čipové kartě je platný dva roky. Vydání a prodloužení osobního certifikátu poskytuje KB zdarma.

V případě využívání osobního certifikátu v souboru, zadává klient při přihlášení do aplikace cestu k danému souboru, kde je certifikát uložen, a heslo, které si zvolí při aktivaci certifikátu. Osobní certifikát uložený na čipové kartě představuje vyšší stupeň zabezpečení díky svému uložení a nemožnosti dalšího zkopírování na jiné přenosné médium. Při využívání certifikátu na čipové kartě zadává klient čtyřmístný PIN.

b) ČSOB

ČSOB nabízí tři způsoby přihlášení klienta do aplikace:

- identifikačním číslem a PINem,
- identifikačním číslem, PINem a SMS klíčem,
- certifikátem k elektronickému podpisu (na čipové kartě).

Základním a nejjednodušším a také nejsnáze napadnutelným způsobem je přihlášení se prostřednictvím identifikačního čísla a PINu. Pro zvýšení bezpečnosti pro klienty, kteří nemají vydaný certifikát, rozšířila ČSOB tento způsob o další bezpečnostní prvek, tzv. SMS klíč (devítimístný alfanumerický řetězec malých písmen a číslic, který je klientovi automaticky při vstupu do aplikace zaslán SMS zprávou na mobilní telefon).

Pokud si klient přeje vyšší stupeň zabezpečení, banka mu vydá certifikát k elektronickému podpisu na čipové kartě. Pro přihlášení pomocí certifikátu klient zadává PIN k čipové kartě, na níž je certifikát uložen. Poté je vygenerován elektronický podpis a ten je odeslán na autentizační server k ověření identifikace klienta.

7.1.5 Autorizace aktivních operací v rámci internetového bankovnictví

a) KB

U internetového bankovnictví KB je autorizace aktivních operací rozdílná u klienta využívajícího osobního certifikátu v souboru a u klienta, který má uložen certifikát na čipové kartě.

V případě používání osobního certifikátu v souboru je nezbytné mít pro aktivní operace registrované číslo mobilního telefonu pro zasílání autorizačních SMS zpráv. Komerční banka toto dodatečné bezpečnostní opatření zavedla v srpnu roku 2006. SMS kód banka zasílá klientovi na předem registrované číslo mobilního telefonu. Jedná se o jednorázové heslo složené z různé kombinace čísel a písmen, které klient zadává do internetové aplikace při rekapitulaci aktivní operace na autorizační obrazovce spolu s heslem k osobnímu certifikátu v souboru. Na zdání správného autorizačního kódu má klient tři pokusy. Po třetím chybném zadání kódu je vygenerován a zaslán nový kód, na jehož zadání má klient opět tři pokusy. Přičemž SMS kód klient zadává v průběhu jednoho přihlášení pouze při první aktivní operaci, při dalších operacích již kód vyžadován není. Pasivní operace (např. transakční historie, dotaz na zůstatek apod.) jsou dostupné se stávajícím certifikátem bez nutnosti zadávání SMS kódu.

V případě využití certifikátu na čipové kartě, veškerá komunikace mezi klientem a bankou probíhá v protokolu SSL. Uživatel nemusí mít zaregistrováno číslo mobilního telefonu pro zasílání autorizačních SMS zpráv a každou aktivní operaci podepisuje „pouze“ svým elektronickým podpisem zakódovaným v osobním certifikátu na čipové kartě.

b) ČSOB

Služba ČSOB Internetbanking nabízí dva možné způsoby autorizace:

- elektronickým podpisem, generovaným na základě údajů uložených na čipové kartě,
- SMS klíčem.

Autorizaci na základě elektronického podpisu může využívat klient, který má vydán certifikát na čipové kartě. Tento certifikát je klientovi zaregistrován na pobočce banky při zřízení služby a klient ho zároveň využívá při přihlašování do internetové aplikace.

SMS klíč neboli autorizační kód je devítimístný alfanumerický řetězec složený z malých písmen a číslic, který je klientovi jednorázově zaslán na mobilní telefon při zadávání každé aktivní operace. Tento kód klient zadá do určeného pole na formuláři. Pro jeho vepsání je vyměřen časový limit 10 minut. Stiskem tlačítka „Odeslat“ proběhne autorizace a v případě bezchybně zadaného autorizačního kódu je příkaz odeslán ke zpracování do banky. V případě chybného zadání dojde po pátém chybně zadaném kódu k zablokování internetového bankovnictví. Odblokování je možné pouze na pobočce ČSOB.

7.1.6 Shrnutí

Hlavním rozdílem v zabezpečení internetových aplikací KB a ČSOB nabízené fyzickým osobám (občanům) je způsob uložení certifikátu. Komerční banka nabízí jak certifikát uložený na čipové kartě, tak certifikát v souboru. Oproti tomu ČSOB nabízí jen první ze zmiňovaných certifikátů a pro klienty, kteří si tento typ certifikátu nemají zájem pořídit (například kvůli nutnosti vlastnit k čipově kartě také čtecí zařízení), nabízí možnost zabezpečení na základě identifikačního čísla, PINu a autorizačního SMS kódu. Tento vícestupňový systém se v praxi ukázal jako odolnější proti útokům v porovnání se způsobem, který KB nabízela a jehož zabezpečení bylo zajištěno pouze prostřednictvím certifikátu v souboru bez nutnosti zdávat SMS kódy při provádění aktivních transakcí.

Komerční banka na základě ohrožení bezpečnosti klientů využívajících tento systém zabezpečení byla nucena v létě roku 2006 také přistoupit k zavedení autorizačních kódu, které klienti vlastnící certifikát v souboru zadávají při potvrzování aktivních operací.

Rozdílnost lze pozorovat také v četnosti zadávání autorizačních kódů. V případě internetové aplikace Komerční banky stačí zadat SMS kód při provádění transakcí v průběhu jednoho přihlášení pouze jednou – při první operaci, při dalších transakcích již kód není nutné zadávat. Oproti tomu v případě aplikace ČSOB je vyžadováno zadání autorizačního SMS kódu při potvrzování každé aktivní operace, což může být pro klienta v případě většího množství transakcí dosti zdlouhavé, přičemž oba způsoby zadávání autorizačních kódu poskytují stejnou úroveň zabezpečení. U internetových aplikací obou bank totiž platí, že pokud uživatel neprovede po dobu 20 minut žádnou akci, která by požadovala přijetí dat z banky nebo jejich odeslání, je relace z důvodu bezpečnosti ukončena, klient je automaticky odhlášen a pro pokračování je třeba se do aplikace přihlásit znovu.

Pokud klient využívá certifikát na čipové kartě, je způsob provádění transakcí pomocí internetové aplikace i úroveň zabezpečení u obou zmiňovaných bank stejná, odlišná je pouze cena za služby spojené s využívání certifikátu na čipové kartě. Ceny za tyto služby jsou uvedeny v následující tabulce.

Tabulka č. 6: Porovnání poplatků za služby internetového bankovnictví u KB a ČSOB

Banka	KB	ČSOB
Název produktu	*Moje banka Přímý kanál*	*Internetbanking 24*
Poplatek za zřízení služby	zdarma	zdarma
Poplatek za vedení služby měsíčně	39,-	zdarma
Poplatek za vydání čipové karty s bezpečnostním certifikátem	390,-	100,-
Obnova bezpečnostního certifikátu	zdarma	100,-
Vydání čtecího zařízení čipových karet	250,- [1)]	500,- / 650,- / 1 950,- [2)]

[1)] cena základního typu čtecího zařízení; [2)] rozdílné ceny pro různé typy čtecích zařízení – viz Příloha č. 4

Zpracování: vlastní na základě údajů ze sazebníků bank

Závěr

Cílem této práce bylo představit internetové bankovnictví, principy jeho fungování a zabezpečení a následně v této oblasti porovnat dva významné peněžní ústavy Komerční banku, a. s. a Československou obchodní banku, a. s.

V teoretické části jsou nastíněny hlavní milníky ve vývoji Internetu a je rozebírán jeho význam pro oblast bankovnictví společně s nutností dostatečného zabezpečení internetových aplikací jak ze strany banky, tak i na straně klienta. V praktické části jsou představeny produkty internetového bankovnictví KB a ČSOB, které jsou dále porovnány z hlediska úspory na poplatcích při jejich využívání a také v oblasti nabízených způsobů zabezpečení.

Z uvedených zkoumání jsem dospěla k poznání, že z hlediska nabídky služeb internetového bankovnictví obě banky poskytují svým klientům produkty na stejně vysoké technologické úrovni s obdobnými možnostmi zabezpečení, které se dnes běžně v oblasti výpočetní techniky užívají. Na základě porovnání možných způsobů zabezpečení vyplývá, že ČSOB byla po dlouhou dobu „o krok napřed“ ve využívání jednorázových autorizačních SMS zpráv jako druhého stupně tzv. dvoufázového zabezpečení aktivních bankovních operací. ČSOB plánuje vůdcovství v oblasti zabezpečení internetových aplikací udržovat i do budoucna a stát se tak předním inovátorem ve službách a možnostech internetového bankovnictví.

I v oblasti nákladů a celkové úspory při využívání Internetu nepodnikající fyzickou osobou se ČSOB umístila před Komerční bankou. Její poplatky za elektronické spravování účtu a bankovní transakce jsou oproti KB celkově nižší a úspora v nákladech klientů tudíž výrazně vyšší.

Na základě výsledků výzkumu byl prokázán značný přínos internetového bankovnictví z hlediska úspory na poplatcích za vedení účtu a běžné bankovní operace. Výše této úspory je pro přehlednost vyjádřena procentuelně a graficky. Při výpočtu jsem abstrahovala od počátečních tzv. fixních nákladů spojených s užíváním internetového bankovnictví, jako jsou výdaje spojené s koupí a provozem počítače, jelikož počítač připojený k Internetu je

dnes běžnou součástí téměř každé domácnosti a ve většině případů jej klient při zřizování internetového bankovnictví již vlastní a využívá i pro jiné účely. Nehledě na skutečnost, že ovládání účtu zadáváním operací přímo na pobočce s sebou přináší kromě vyšších poplatků také dodatečné náklady v podobě výdajů na dopravu, ušlý čas strávený čekáním na pobočce apod. V tomto případě lze považovat počáteční náklady na internetové bankovnictví a dodatečné náklady za pobočkové bankovnictví za vzájemně vykompenzované.

Z výše zmíněných faktů jsem dospěla k názoru, že význam internetového bankovnictví v České republice stále roste především díky komfortu, efektivitě a úspoře, kterou přináší jak klientům, tak i bankám. Klienti si možnosti a výhody internetového bankovnictví uvědomují a stále více jich využívají. Zatímco dříve bylo poskytnutí základních způsobů elektronického ovládání účtu pro banku konkurenční výhodou, dnes se poskytnutí komplexní škály funkcí a dalších vlastností stává v bankovním sektoru existenčním minimem.

Použitá literatura

[1] BLAŽEK, J. a UKLEIN,J. *Bankovnictví.* Vyd. 1. Brno: Doplněk, 1997. Edice učebnic Právnické fakulty Masarykovy univerzity v Brně. ISBN 80-85765-91-8.

[2] KOSIUR,D. a kol.: *Elektronická komerce*. Vyd 1. Brno:Computer Press, 1998. ISBN 80-7226-097-9.

[3] MILLER, R.LeRoy, PULSINELLI, R.W. *Modern Money and Banking*. 2nd Ed. New York : McGraw-Hill Book Company, cop. 1989. xii, 633 s. ISBN 0-07-042212-5.

[4] NAVRÁTIL, P. *Internet pro školy*. Vyd. 1. Bedihošť : Computer Media, 2001. ISBN 80-902815-3-2.

[5] PŘIHRÁDKA, M. a KALA, J. *Elektronické bankovnictví : [rady a tipy]*. Vyd. 1. Praha: Computer Press, 2000. Praxe manažera. ISBN 80-7226-328-5.

[6] WITTMANN, M. a BUKOVANSKÝ, S. *Co je to vlastně Internet?* Ostrava: Blesk, 1998. ISBN 80-86060-21-7.

[7] http://www.czechindustry.cz/revue/cz/view.php?cisloclanku=2007020062-Cesky-internet-slavi-patnacte-narozeniny

[8] http://www.webdesign.paysoft.cz/clanky/2006/historie-ceskeho-internetu/

[9] http://i-extra.net/internet-a-site/historie-internetu/

[10] http://www.wikipedia.cz

[11] http://www.caczechia.cz/start.asp?file=vyuziticertifikatu

[12] http://www.kb.cz/cs/com/profile/index.shtml

[13] http://www.kb.cz/cs/seg/seg1/products/mojebanka.shtml

[14] http://www.kb.cz/cs/seg/seg4/products/profibanka.shtml

[15] http://www.kb.cz/cs/seg/seg4/products/direct_channel.shtml

[16] http://www.kb.cz/cs/seg/seg4/products/edi.shtml

[17] http://www.csob.cz/bankcz/cz/Csob/O-CSOB/Profil-CSOB/

[18] http://www.csob.cz/bankcz/cz/Csob/O-CSOB/Skupina-CSOB/

[19] http://www.csob.cz/bankcz/cz/Lide/Elektronicke-bankovnictvi/CSOB-Internetbanking-24.htm

[20] http://www.csob.cz/bankcz/cz/Firmy/Podnikatele/Elektronicke-bankovnictvi/CSOB-BusinessBanking-24.htm

[21] http://www.csob.cz/bankcz/cz/Firmy/Podnikatele/Elektronicke-bankovnictvi/CSOB-Homebanking-24.htm

[22] http://www.bankovnictvi.ihned.cz

Seznam tabulek

Seznam grafů

Seznam obrázků

Seznam příloh