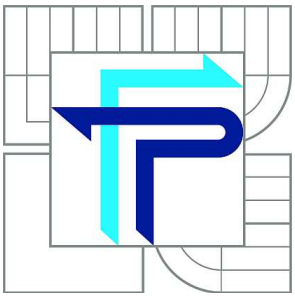
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

BEZPEČNOST ELEKTRONICKÉHO BANKOVNICTVÍ PRO FIRMU

SECURITY OF ELECTRONIC BANKING

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JIŘÍ RENNÉT
AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. JIŘÍ DVOŘÁK, DrSc.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/2010
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Rennét Jiří, Bc.

Řízení a ekonomika podniku (6208T097)

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

Bezpečnost elektronického bankovnictví pro firmu

v anglickém jazyce:

Security of Electronic Banking

Pokyny pro vypracování:

Úvod
Systémové vymezení problému
Cíl práce
Informační zdroje
Současný stav řešené problematiky
Analýza řešeného problému
Návrh řešení problému
Zhodnocení návrhu
Závěr
Seznam použitých informačních zdrojů
Seznam zkratek a pojmů
Přílohy

Seznam odborné literatury:

LANCE,James. Phishing bez záhad. 1.vyd. Praha : Grada 2007. 281 s. ISBN 978-80-247-1766-1.
MLNEK, Jaroslav. Zabezpečení obchodních informací. 1.vyd. Praha : Grada, 2007. 154 s. ISBN 978-80-251-1511-4.
PIPER,F. Kryptografie. 1.vyd. Praha : Computer Press, 2006. 157 s. ISBN 80-7363-074-5.
SEDLEK,J. E-komerce, internet a mobil marketing od A do Z. 1.vyd. Praha : Grada 2006. 351 s. ISBN 80-7300-195-0.
VADLENKA, Libor. Elektronické obchodování. 1.vyd. Praha : Computer Press, 2007. 163 s. ISBN 978-80-86530-40-6.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2009/2010.

L.S.

PhDr. Martina Rašticová, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA

V Brně, dne 16.05.2010

Abstrakt

Diplomová práce podrobně rozebírá a analyzuje zabezpečení elektronického bankovnictví vybraného bankovního sektoru v České Republice. Z těchto výsledků a poznatků definuje nejvhodnější elektronické bankovnictví z hlediska bezpečnosti a toto doporučuje firmě Profes Projekt s.r.o. Dále provádí analýzu současného používaného elektronického bankovnictví ve firmě a rozebírá teoretické poznatky z oboru elektronického obchodování.

Klíčová slova

Elektronické obchodování, platební karty, SSL, autentizace uživatele, autorizace, identifikace, šifrování, elektronický podpis, certifikační protokoly, certifikační autorita, certifikát.

Abstract

Master’s thesis analyzes in detail the security of electronic banking within the chosen banks in Czech republic. On the base of these knowledge it defines and recommendes the most secure electronic banking for Profes Project s.r.o. company. In the folowing it investigates a current electronic banking in the company and it carries out basic theoretical findings.

Keywords

Electronic banking, credit card, SSL, user’s authentication, authorization, identification, encryption, electronic signature, certificate protocols, CA, certificate.

Bibliografická citace VŠKP dle ČSN ISO 690

RENNÉT, Jiří. Bezpečnost elektronického bankovnictví pro firmu. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 74 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

Čestné prohlášení

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

V Pardubicích, dne 22. května 2010

Poděkování

Rád bych upřímně poděkoval prof. Ing. Jiřímu Dvořákovi, DrSc. za cenné náměty, připomínky, rady a čas, který mi věnoval při zpracování této diplomové práce.

1 ÚVOD 10

2 SYSTÉMOVÉ VYMEZENÍ PROBLÉMU 11

2.1 FIRMA PROFES PROJEKT 12

2.1.1 Předmět podnikání 12

2.1.2 Historie a současná činnost 12

2.1.3 Ekonomická situace 14

2.2 POHLED FIRMY 14

3 CÍL PRÁCE 15

4 INFORMAČNÍ ZDROJE 16

4.1 VIRTUÁLNÍ KNIHOVNY 16

4.2 ELEKTRONICKÉ DOKUMENTY 18

4.3 WEBOVÉ STRÁNKY 18

4.4 MONOGRAFIE 18

5 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY 19

5.1 HISTORIE ELEKTRONICKÉHO BANKOVNICTVÍ 19

5.2 SOUČASNÝ STAV V ČESKÉ REPUBLICE 20

5.3 SOUČASNÝ STAV VE SVĚTĚ 21

5.4 PLATEBNÍ KARTY 21

5.4.1 Podle typu provedení karty 21

5.4.2 Podle zabezpečení karty 22

5.4.3 Podle formy vyúčtování transakcí 22

5.5 TELEFONNÍ BANKOVNICTVÍ 23

5.6 GSM BANKING 23

5.7 HOMEBANKING 24

5.8 INTERNETBANKING 25

5.8.1 Komunikace s bankou 25

5.8.2 Možnosti internetbankingu 26

5.9 BEZPEČNOST ELEKTRONICKÉHO OBCHODOVÁNÍ 26

5.9.1 Základní pojmy 26

5.10 ZABEZPEČENÉ PROTOKOLY 29

5.11 SOUČASNÝ STAV VE FIRMĚ PROFES PROJEKT S.R.O. 29

6 ANALÝZA ŘEŠENÉHO PROBLÉMU 30

6.1 VÝBĚR BANKOVNÍHO SEGMENTU 30

6.1.1 Komerční banka (KB) 31

6.1.2 Raiffeisen bank 32

6.1.3 Citibank ... *33*
6.1.4 Česká spořitelna ... *34*
6.1.5 UniCredit Bank ... *35*
6.2 HROZBA PRVNÍ - UŽIVATEL ... 36
6.2.1 Phishing ... *36*
6.2.2 Pharming ... *39*
6.2.3 Další časté chyby ... *39*
6.2.4 Doporučení firmě ... *40*
6.3 HROZBA DRUHÁ - IDENTIFIKACE BANKY A ŠIFROVÁNÍ DAT ... 41
6.3.1 Důvěryhodnost a platnost certifikátů vybraných bank ... *41*
6.3.2 Podpora protokolů ... *44*
6.3.3 Šifrování ... *46*
6.3.4 Síla šifry ... *48*
6.4 HROZBA TŘETÍ – AUTENTIZACE KLIENTA A AUTORIZACE TRANSAKCE ... 49
6.4.1 Jméno a heslo, certifikát, kalkulátor ... *49*
6.4.2 Běžná SMS, SMS Tookit, Čipová karta ... *51*
7 NÁVRH ŘEŠENÍ PROBLÉMU ... 53
7.1 HODNOCENÍ BEZPEČNOSTI CERTIFIKÁTU ... 53
7.1.1 Hodnocení bezpečnosti protokolů ... *55*
7.1.2 Hodnocení úrovně šifrování ... *56*
7.1.3 Hodnocení úrovně autentizace a autorizace ... *58*
7.2 HODNOCENÍ CELKOVÉ BEZPEČNOSTI ... 60
7.3 DOPORUČENÉ ŘEŠENÍ PRO FIRMU ... 63
7.4 HARMONOGRAM ZMĚNY ... 63
8 ZHODNOCENÍ NÁVRHU ... 64
8.1 ZHODNOCENÍ Z POHLEDU BEZPEČNOSTI ... 64
8.2 EKONOMICKÉ ZHODNOCENÍ NÁVRHU ... 65
8.2.1 Soupis předpokládaných transakcí ... *65*
8.2.2 Další faktory ovlivňující náklady ... *65*
8.2.3 Výpočet bilance bankovního účtu ... *66*
9 ZÁVĚR ... 67
SEZNAM POUŽITÝCH INFORMAČNÍCH ZDROJŮ ... 68
SEZNAM ZKRATEK A POJMŮ ... 72
REJSTŘÍK ... 73
PŘÍLOHY ... 72

1 Úvod

Elektronické obchodování je fenomén, který zažívá největší boom až v posledních letech, kdy vývoj informačních technologií umožnil vznik nových produktů a služeb. Pro podnikatelské subjekty se tak otevřely nové možnosti platebních styků a pro ty, které toho dokázaly využít, vznikla nová konkurenční výhoda. V této době je již elektronické obchodování standardem, bez kterého lze jen stěží na trhu obstát.

Nakupování na internetu je na obrovském vzestupu. Velká výhoda a potenciál elektronického obchodování je v přístupu k zákazníkovi, který je rychlý, nezávislý na místě a za minimální náklady. Tyto výhody se samozřejmě nevztahují pouze k zákazníkovi, ale také k dodavatelům, odběratelům a nebo obchodním partnerům.

Využívání elektronického obchodování má však i stinné stránky. Tou dozajista nejdiskutovanější je bezpečnost prováděných transakcí. Často se také stává, že platební styk je realizován s druhou stranou, o které nemáme mnoho korektních informací. V této diplomové práci se proto budu věnovat analýze tohoto problému a výstupem práce bude doporučení nejbezpečnějšího internetového bankovnictví pro firmu Profes Projekt s.r.o.

2 Systémové vymezení problému

„Pojem elektronické bankovnictví se vžil pro označení elektronické formy komunikace mezi bankami a jejich klienty. Při vyřizování svých bankovních operací nepřichází klient do osobního kontaktu s pracovníky banky, ale provádí operace ze svého terminálu nebo jiného technického zařízení, které je veřejně dostupné. Jde o trend, který jde ruku v ruce s rozvojem informačních a telekomunikačních technologií, s vyšší výkonností výpočetní techniky a snižování ceny, za kterou je prodávána. Elektronické bankovnictví nemůže mít žádnou přesnou, taxativně vymezenou definici. Je to pojem, jehož aktuální obsah se vyvíjí spolu s informačními a komunikačními technologiemi. Nejlépe jej vystihuje pojem *vzdálené bankovnictví*.

Charakteristické rysy služeb zařazovaných do oblasti elektronického bankovnictví jsou následující:

- ☑ k poskytování služeb dochází prostřednictvím elektronického kanálu
- ☑ na jedné straně je klient s určitým technickým vybavením a na druhé straně je buď přímo automatický systém banky nebo pracovník obsluhující tento systém
- ☑ klient musí být při elektronické komunikaci vždy jednoznačně identifikovatelný a jeho právo vykonat požadovanou operaci je vždy ověřeno určitým autorizačním mechanismem
- ☑ nejčastějšími operacemi jsou zde tuzemský platební příkaz a stav peněz na účtu

Výhodou pro klienta je ušetřený čas a možnost komunikovat s bankou z různých míst. Banka rovněž ušetří a sice na transakčních nákladech.

Problémem je ale nutnost jednoznačné identifikace klienta bez osobního kontaktu a vysoké nároky na bezpečnost komunikace.“[1]

---

[1] *CEED* [online]. 2008 [cit. 2010-05-11]. Elektronické bankovnictví. Dostupné z WWW: <http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm>.

2.1 Firma Profes Projekt

Pro společnost Profes Projekt jsem již zpracovával návrh počítačové sítě jako moji bakalářskou práci. Vzhledem k tomu, že jsem se chtěl zajímat o téma bezpečnosti elektronického obchodování, tak jsem se znovu obrátil na vedení firmy s dotazem, zda mají zájem o analýzu stavu e-bankingu využívaného ve firmě a o návrhy na jeho zlepšení. Můj podnět byl přijat kladně.

V projekční kanceláři se drtivá většina všech transakcí provádí právě přes elektronické bankovnictví. S jednatelem společnosti jsem se domluvil, že vypracuji studii vhodnosti služeb jednotlivých bank v České republice právě pro firmu tohoto segmentu.

PROFES PROJEKT spol. s. r. o.
Vejrichova 272
511 01 Turnov
Česká republika
tel: +420 481 319 831
fax: +420 481 319 832
e-mail: profesprojekt@profesprojekt.cz
www: www.profesprojekt.cz
IČO: 46506942
zapsáno u OR u KS Hradec Králové, oddíl C, vložka 2071

2.1.1 Předmět podnikání

Projektová činnost ve výstavbě
Provádění staveb včetně jejich změn, udržovacích prací na nich a jejich odstraňování
Specializovaný maloobchod

2.1.2 Historie a současná činnost

Historie společnosti Profes projekt s.r.o. sahá do roku 1991. Její činnost se zpočátku orientovala téměř výhradně na provádění staveb, avšak postupně se rozšířila na další aktivity v oblasti stavebnictví a to především na projekční a inženýrskou činnost v různých oborech.

V oblasti projekčních činností se společnost zabývá občanskými a bytovými stavbami, průmyslovými stavbami a inženýrskými konstrukcemi. Vedle kompletních projektů zahrnujících zadání stavby, projektů pro veřejnoprávní projednání a podrobných realizačních projektů, nabízí klientům i zpracování studií a odbornou pomoc při práci na investičním záměru, při výběru nejvhodnějších variant a spolupráci při výběrovém řízení na dodavatele stavby. Ke všem projektovým stupňům jsou schopni dodat cenové kalkulace od předběžných propočtů ve fázi studie až po podrobné položkové rozpočty k realizační dokumentaci.

V oblasti nosných konstrukcí se zabývají návrhy ocelových, betonových i zděných konstrukcí občanských i bytových staveb. V oboru inženýrských konstrukcí zpracovávají projektovou a výrobní dokumentaci pro průmyslové a obchodní haly, technologické konstrukce, zásobníky, jeřábové dráhy a mostové jeřáby. Dále nabízí zpracování statických a dynamických výpočtů, odborné posudky stávajících konstrukcí a návrhy sanací staveb. Projektují rovněž vodovody, kanalizaci, plynovody a elektrorozvody včetně přípojek. Provádí také projekty nádrží, jímek, bazénů a čistíren odpadních vod. V oboru technického zařízení budov nabízejí projekty vnitřní kanalizace, vodovodu, domovního i průmyslového plynovodu, elektroinstalace a rozvodů technologických médií. Firma se rovněž specializuje na projekty zdrojů tepla, především plynových kotelen a zajišťuje jejich realizaci. Provádí posouzení energetické náročnosti budov a návrhy úspor energie.

Úroveň její činnosti je dána nejen tím, že veškeré práce jsou řízeny autorizovanými inženýry či techniky v příslušných oborech, ale i tím, že firma věnuje nemalé prostředky na vzdělávání a další odborný růst svých pracovníků. Maximální využití nejmodernější techniky společnosti dále umožňuje zrychlit, zefektivnit a zkvalitnit náročnou projekční a konstrukční práci. Svými výsledky se Profes projekt s.r.o. zařadil mezi přední projekční kanceláře v regionu. Tuto pozici získal dodržováním firemní strategie založené na kvalitě, serióznosti, flexibilitě a vysoké odborné úrovni práce.[2]

[2] Interní materiály firmy

2.1.3 Ekonomická situace

Zaměstnanci:

Společnost Profes Projekt čítá v současné době 10 zaměstnanců včetně 3 jednatelů (společníků), kteří společnost založili.

Celkový základní kapitál společnosti je 100 000 Kč.

Společnost s ručením omezeným byla založena společenskou smlouvou dne 27. 1. 1992.

Ukazatele podniku:

Tržby v roce 2009 dosáhly tržby společnosti 14 635 tisíc Kč.

ROA Podle ukazatele byla rentabilita celkových aktiv 49,65% v roce 2009.

ROE Podle ukazatele byla rentabilita vlastního kapitálu 71,44% v roce 2009.

Produktivita práce: Podle ukazatele který je podílem celkových tržeb a celkových mzdových nákladů byla produktivita práce 343% v roce 2009.

Veškerou činnost firmy tvoří poskytování služeb zákazníkům. [3]

2.2 Pohled firmy

Po prodiskutování požadavků firmy na elektronické bankovnictví jsem si utřídil několik kritérií na výběr produktu, které musím také zohlednit vedle samotné bezpečnosti služby. Jsou to:

- ☑ ***Otevřené řešení s možnostmi následujícího upgradu***
- ☑ ***Vysoký stupeň zabezpečení služby***
- ☑ ***Informace o účtech***
- ☑ ***Informace o bezhotovostních i hotovostních transakcích***
- ☑ ***Obecné informace (zprávy z banky, kurzovní lístek…)***
- ☑ ***Platební transakce***
- ☑ ***Možnost bezhotovostního styku v cizí měně***
- ☑ ***Šablony pro usnadnění transakcí***
- ☑ ***Přizpůsobení uživatelského profilu***
- ☑ ***Rozumné zhodnocení uložených finančních prostředků***
- ☑ ***Dostupnost pobočky banky***

[3] Interní materiály firmy

3 Cíl práce

Na základě podrobné analýzy vybraného segmentu bankovního sektoru ČR a identifikace používaných prostředků elektronického bankovnictví vytvořím odpovídající model bezpečného e-bankingu v rámci elektronického obchodování firmy.

Cíl práce v bodech:

- ☑ Výběr bankovního segmentu
- ☑ Analýza bezpečnosti internetového bankovnictví
- ☑ Hodnocení analýzy
- ☑ Návrh řešení

Cílem této diplomové práce je navrhnout optimální bankovní službu, která obsahuje kvalitní a bezpečné internetové bankovnictví, pro společnost Profes Projekt sídlící v Turnově. V této době firma využívá neefektivní a nekvalitně zabezpečený e-banking, který navíc nenabízí ani výhodné úročení. Firma má několik požadavků, které budou hlavním opěrným bodem celé diplomové práce a které chci splnit beze zbytku.

Hlavním úkolem je detailně analyzovat vybraný počet bank v České Republice z hlediska bezpečnosti jejich internetových bankovnictví a tyto údaje přehledně zpracovat. Dále vytvořit relevantní a efektivní kvalifikační systém, pomocí kterého z práce vznikne konkrétní výstup. Tento výstup bude dále prezentován firmě Profes Projekt a bude jí navrhnuto řešení zadaného problému.

Celková práce musí mít pro firmu přínos jak z hlediska bezpečnostního, tak z hlediska ekonomického a musí být natolik kvalitní, aby se jí firma mohla bez obav řídit.

4 Informační zdroje

V oblasti elektronického zabezpečení je kladen vysoký důraz na aktuálnost vybraných informací. Vývoj v této oblasti je neustále velice rychlý a proto je třeba sledovat nejnovější trendy a novinky. Informační zdroje využité v této diplomové práci lze dělit do několika kategorií:

4.1 Virtuální knihovny

Nejdostupnějším a zároveň odborným zdrojem jsou virtuální knihovny. Pomocí virtuálních knihoven se snadno dostaneme k obsáhlým zdrojům elektronických článků, dokumentů, periodik, popřípadě absolventských prací. Na internetu jsou snadno k nalezení i virtuální knihovny v cizích jazycích.

Příklady virtuálních zdrojů:

☑ *http://www.bibliothecaeconomica.cz/*

Tato virtuální knihovna nabízí široký výběr ekonomických publikací k volnému stažení. Jedná se především o publikace týkající se vývoje ekonomiky, bankovnictví, peněžnictví a podobně.

☑ *http://www.ndk.cz/*

Stránky *Národní digitální knihovny* jsou obsáhlým zdrojem volně dostupných knih, jak českých, tak zahraničních, článků a periodik. Vyhledávání požadovaného dokumentu lze uskutečnit snadno pomocí klíčových slov v dokumentu a požadovaného typu dokumentu.

☑ *http://info.jib.cz/*

Na portálu Jednotné informační brány nalezneme databázi e-časopisů roztříděnou dle dostupnosti. Databáze obsahuje taktéž volně přístupné časopisy, které jsou k dispozici všem. Ostatní databáze jsou přístupné pouze čtenářům té knihovny, která je spravuje.

☑ *http://library.muni.cz/ezdroje/*

Výbornou virtuální knihovnou je například knihovna Masarykovy Univerzity v Brně. Na webové adrese naleznete seznam celosvětových portálů pro vyhledávání článků a odborných textů.

Cizojazyčné digitální knihovny:

☑ *http://www.neha.nl/w3vl/*

Obsahem této virtuální knihovny jsou především soupisy uskutečněných a plánovaných konferencí, časopisy a odkazy na výzkumné instituce. Knihovna se primárně zabývá ekonomickou a obchodní historií.

☑ *http://www.docstoc.com/*

Tato stránka obsahuje veřejnou celosvětovou databázi absolventských prací a elektronických článků, a to vše přehledně rozčleněno do mnoha kategorií.

Vyhledávání českých absolventských prací:

☑ *http://is.muni.cz/*

Na portálu Masarykovy Univerzity je dostupná databáze většiny bakalářských a diplomových prací posledních let.

☑ *http://theses.cz/*

Slouží jako národní registr závěrečných prací a tím poskytuje i možnosti odhalení plagiátorství. Je to databáze závěrečných prací studentů vysokých škol, které jsou do programu zapojeny. Ne všechny práce jsou dostupné v plném textu, ale mnoho z nich ano.

4.2 Elektronické dokumenty

Jsou mnohem aktuálnější než knižní publikace, ale je třeba brát zřetel na relevantnost informací jednotlivých autorů. V ideálním případě vycházíme z elektronických dokumentů pouze od autora, který je nám známý. Často se jedná také o odborné studie.

4.3 Webové stránky

Nejrychleji se aktualizujícím informačním prostorem jsou články na webových stránkách specializovaných odborných serverů. Většinou se jedná o pohled na určitý problém očima odborníků, kteří spolupracují pro daný sever. Proto není důvod se obávat o věrohodnost podaných informací. Lze samozřejmě čerpat jak z českých, tak z cizojazyčných serverů.

4.4 Monografie

Knihy nejsou tou nejaktuálnější, ale jsou jistě nejobsáhlejší možností, jak porozumět problematice elektronického bankovnictví. Českých titulů (popř. titulů přeložených do češtiny) není mnoho, proto je vhodné poohlédnout se po anglických publikacích.

5 Současný stav řešené problematiky

V této kapitole bude popsána problematika internetového obchodování jako celku. Vyzdvižena ovšem bude část obsahující detailní seznámení s problematikou teorie internetového bankovnictví.

Za zmínku jistě stojí už začátky elektronického obchodování.

5.1 Historie elektronického bankovnictví

Typickou formou, pod kterou si většina lidí vybaví elektronické obchodování je poskytování bankovních služeb skrze internet.

Všeobecně se jako počátek vzniku elektronického bankovnictví považuje vznik debetních platebních karet. Dalším významným vývojovým stupněm bylo zahájení činnosti First Direct Bank v Leedsu, banky která obsluhuje své klienty pouze „na dálku" prostřednictvím telefonních linek. Jako první vydala firma Western Union Telegraph Company platební kartu v roce 1914. Pomocí této karty bylo možno zasílat telegramy bez hotovosti. Jako první universální karta je známa karta společnosti Diner Club International, která ji vydala pouze 200 vybraným klientům. V dalším roce vydala platební karty i první banka (The Franklin National Bank z New Yorku). V této době stačilo při požití kartu předložit a podepsat účet. Jediným bezpečnostním prvkem tedy bylo vizuální ověření shodnosti podpisu s podpisovým vzorem na kartě. O něco později se začalo ještě kontrolovat, zda karta není na seznamu odcizených nebo zablokovaných karet. Toto všechno probíhalo samozřejmě bez využití počítačů.

Banky ovšem sledovaly trendy ve vývoji výpočetní techniky a brzy se staly významnými zákazníky výrobců počítačů. Zprvu tyto počítače sloužili pouze pro užití uvnitř banky, postupem času ale banky začaly provozovat elektronické bankomaty, ve kterých si mohli klienti s platební kartou vyzvednout hotovost. V této době se již transakce zaznamenávali elektronicky a de facto se tím odstartovala etapa elektronického bankovnictví. [4]

---

[4] viz. MARVANOVÁ, M, SCHLOSSBERGER, O a kol.: *Platební styk*, 2. dopl. vyd.. Praha : Bankovní institute, 1998. 376 s.

První bankomat na světě byl spuštěn roku 1939 v New Yorku, ale po půl roce byl z důvodu malého zájmu opět zrušen. Poté až v roce 1967 banka Barclays Bank v Londýně zprovoznila automat, který již byl hojně využíván. Počátky provozu bankomatů ovšem také nebyly bez problémů. První bankomaty nevyužívaly ani bezpečnostního magnetického proužku, nýbrž děrného štítku, a ke komunikaci mezi bankomatem a zákazníkem sloužil otočný válec, který snímal díry ve štítku. Zanedlouho se však podařilo problémy vyřešit a bankomaty se staly běžnou součástí všedního života. [5]

5.2 Současný stav v České Republice

V České Republice je využívání platebních karet již velmi rozšířeno. Nejobvyklejšími platebními kartami jsou Eurocard/Mastercard a Visa. Již dvě třetiny lidí starších 15 let mají debetní kartu, a dalších 5 % má kartu kreditní. V ČR je zhruba 3000 bankomatů a na 50 000 místech se dá platební kartou platit.

Do popředí se dostávají platební karty s mezinárodní platností na úkor tuzemských platebních karet, jejichž počet rychle klesá. Zatímco mezinárodních platebních karet je kolem osmi miliónů, karty s platností pouze v České republice se dají počítat na statisíce.

„Vnímání zákazníků se i v České republice začíná vylepšovat. Důvodem je především mnohem více profesionální přístup některých on-line prodejců. Obecně se začíná zkracovat doba dodání zboží zákazníkům a silnější elektronické obchody začínají fungovat na smluvní bázi nad velkoobchody. Fakticky to znamená, že mají již relativně přesné informace o stavu prodávaného zboží ve velkoskladu, od kterého toto zboží odebírají – toto zboží začínají navíc uvádět jako skladové. Rozšiřuje se také využívání on-line plateb debetními i kreditními kartami.

[5] viz. MARVANOVÁ, M, SCHLOSSBERGER, O a kol.: *Platební styk*, 2. dopl. vyd.. Praha : Bankovní institute, 1998. 376 s.

Česká republika má navíc svůj vlastní fenomén – dobírku. Ještě dnes platí zákazníci za více než 60 % objednaného zboží hotově při jeho předání. V USA naopak dobírku v českém provedení neznají vůbec.“[6]

5.3 Současný stav ve světě

Momentální situaci ve světě odráží fakt, že na rozdíl od Američanů, Evropané vždy byli k internetovému obchodování více skeptičtí. Do toho se ještě negativně projevil rychlejší technologický vývoj a rozšíření platebních karet v USA. Z tohoto důvodu bude Evropa jistě ještě několik let pozadu.

Platební karty jsou první moderní metodou elektronického bankovnictví, proto jim je věnován následující odstavec.

5.4 Platební karty

Platební karty jsou nejznámější formou elektronického obchodování. Jejich využití je levné, efektivní, praktické a při dodržování určitých zásad i velice bezpečné.

5.4.1 Podle typu provedení karty

- ☑ **Embosované karty** – mají na sobě vyražené tzv. vroubkované písmo, embossing. Lze s nimi platit na mechanických snímačích nazývaných imprintery.

- ☑ **Elektronické karty** – zcela hladké karty určené pouze pro elektronicky provedené transakce v platebních terminálech a imprinterech.

---

[6] *Marketingové noviny* [online]. 2006 [cit. 2010-05-11]. Historie elektronických obchodů. Dostupné z WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4391>.

- ☑ **Virtuální karty** – platební karty určené k platbám na internetu nebo k transakcím bez přítomnosti karty. Nejčastěji dostanete pouze číslo platební karty, které může být vytištěno např. jen na papíře, přijde vám formou SMS zprávy nebo jej uvidíte pouze v náhledu internetové aplikace.

5.4.2 Podle zabezpečení karty

- ☑ ***Karty magnetické*** – platební karta je vybavena pouze magnetickým proužkem.
- ☑ ***Karty čipové*** – platební karta má pouze čip, magnetický proužek chybí.
- ☑ ***Karty hybrid***ní – platební karta obsahuje čip i magnetický proužek.
- ☑ ***Karty bezkontaktní*** – platební karta obsahuje bezkontaktní technologii umožňující na dálku přenášet transakční údaje.

5.4.3 Podle formy vyúčtování transakcí

- ☑ ***Debetní karty*** – transakce je zúčtována neprodleně po obdržení informace o její výši. V praxi jde v průměru o 3–5 dnů. Tyto karty jsou vydávány pouze k bankovním účtům.
- ☑ ***Kreditní karty*** – při platbě kartou je možné využívat bezúročné období. Po obdržení výpisu transakcí kartou máte dvě možnosti: buď vše plně uhradíte a nebudete platit úroky, nebo uhradíte alespoň povinnou minimální splátku. Jsou vydávány k úvěrovým účtům.
- ☑ ***Charge karty*** – jde o karty s odloženou splatností. Po obdržení výpisu transakcí kartou musíte své závazky bezpodmínečně uhradit v plné výši. Karta je obdobou faktury: využíváte služby, přijde výpis a do data splatnosti jej zaplatíte. Účet v bance až na výjimky není podmínkou.

- ☑ ***Předplacené karty*** – nejprve vložíte na platební kartu finanční prostředky a teprve poté s ní můžete platit. Není nutný účet v bance, platební karty mohou být i anonymní nebo sloužit jako dárky.[7]

Další formou v postupném vývoji elektronického obchodování je telefonní bankovnictví, které nabývá na intenzitě s nástupem mobilních telefonů. V případě mobilních telefonů se již můžeme zabývat GSM bankingem a s rozvojem internetu přichází služby homebanking a internetbanking. Těmto vývojovým stádiím bude věnována následující kapitola.

5.5 Telefonní bankovnictví

„Princip této služby je jednoduchý. Klient zavolá na linku telefonního bankovnictví. U většiny bank je toto číslo bezplatné a lze na ně volat i z mobilního telefonu. Klient se tam prokáže svým identifikačním číslem a číslem PIN. Tato služba se vyskytuje ve dvou verzích. U té první klient komunikuje s automatickým hlasovým systémem. Zde lze získávat informace o produktech, o aktuálním zůstatku, ale také zde lze zadávat příkazy k úhradě či inkasu, trvalé příkazy, provádět konverzi měn. U této služby je důležité mít telefon s tónovou volbou.

Ve druhé verzi klient komunikuje s telefonním bankéřem, který poskytuje stejné služby jako pracovník na přepážce od zadávání příkazů po zakládání termínovaných vkladů. Zde je nevýhodou, že mimo pracovní dobu budete komunikovat jen s hlasovým systémem.“[8]

5.6 GSM banking

„Také u této služby existují dva druhy. První je SIM Toolkit. Zde banka do vašeho mobilního telefonu (na SIM kartu) nahraje vlastní bankovní aplikaci, která se objeví v menu vašeho telefonu. Při nahrávání aplikace je SIM karta zašifrovaná a nelze

---

[7] Měšec [online]. 2008 [cit. 2010-03-09]. Platební karty. Dostupné z WWW: <http://www.mesec.cz/bankovni-ucty/platebni-karty/pruvodce/>.

[8] Finance [online]. 2009 [cit. 2010-03-09]. Přímé bankovnictví. Dostupné z WWW: <http://www.finance.cz/bankovnictvi/informace/bezne-ucty/prime-bankovnictvi/>.

z ní získat žádné údaje, ani když vám ukradnou telefon. Současně je přístup k této aplikaci chráněn zvláštním bankovním PIN, které se nazývá BPIN. Potom vám tedy stačí listovat v menu aplikace správnou položku a vybrat některou ze základních služeb (např. zjišťování zůstatku na účtu, přehled historie pohybů na účtu, přehled kursů, zadávání příkazů). Na konec obdržíte informaci o vámi vybrané službě a to buď formou textové zprávy na mobilní telefon, nebo formou e-mailu do e-mailové schránky, která je předem definovaná. U nás tuto službu poskytují zajím dva operátoři.

Dalším druhem služby je SMS banking, jehož výhodou je použitelnost u všech mobilních telefonů, bez ohledu na operátora. Komunikace probíhá pouze prostřednictvím SMS zpráv. Na první pohled to nevypadá příliš bezpečně, ale banka i k této aplikaci může vydávat tzv. autentizační kalkulátor, s jehož pomocí si vygenerujete speciální kód, který vložíte do struktury SMS zprávy. Nevýhodou je složitější manipulace, protože SMS zprávy musíte posílat přesně ve formátu daném bankou. Např. U částka účet_debet účet_kredit splatnost [Vvar_symbol] [Kkonst_symbol] [Sspec_symbol] [MAC]. Zadávání tedy vyžaduje velkou pozornost, abyste se nepřepsali.“[9]

5.7 Homebanking

„Produkt umožňuje obsluhovat účet pomocí počítače připojeného k internetu a softwaru, který je dodán bankou (obvykle na instalačním CD). Nainstalujete si software z CD, připojíte se na internet a můžete si zajišťovat základní služby jako např. příkazy k úhradě (i do zahraničí), trvalé příkazy, zůstatky na účtu, konverze měn. Výhodou je zde, že tyto produkty bývají kompatibilní s účetními a ekonomickými programy, ale nevýhodou je, že lze používat pouze počítač, kde je program nainstalován.“[10]

---

[9] Finance [online]. 2009 [cit. 2010-03-09]. Přímé bankovnictví. Dostupné z WWW: <http://www.finance.cz/bankovnictvi/informace/bezne-ucty/prime-bankovnictvi/>.

[10] tamtéž

5.8 Internetbanking

Internet je ideálním prostředníkem mezi bankou a klientem, ovšem zasílané informace jsou velice citlivé a nepřetržitě vystavované útokům hackerů. Internet je již několik let nejlevnějším a nejkomplexnějším komunikačním médiem. Náklady na transakci provedenou přes internet jsou několikrát levnější než jakoukoli jinou formou.

Existuje několik možností jak realizovat operace na účtu pomocí internetbankingu. Následujících několik odstavců bude věnováno podrobnějšímu popisu možností a omezení internetbankingu.

5.8.1 Komunikace s bankou

Na rozdíl od homebankingu, který potřebuje nainstalovat speciální software, internetbanking žádnou instalaci nevyžaduje. Je to pouze online program, který je spuštěn na webových stránkách banky. Klientovi tak postačí pouze počítač s připojením na internet a jakýkoliv současný internetový prohlížeč.

Prohlížeč musí obsahovat technologii 128 bitového šifrování, což je ovšem běžný standard všech nynějších prohlížečů.

Potřeba připojení k internetu může být vnímána jako omezující faktor, ale musíme si uvědomit, že internet je budoucnost, a kvalita pokrytí a přístupu k němu rok od roku stoupá. Jistou nevýhodou může být nepropojitelnost internetového bankovnictví s podnikovým systémem, jelikož internet banking je možné spustit odkudkoli, kde je připojení.

GSM banking se může zdát více operativní než internetové bankovnictví, jelikož mobilní telefon máme s sebou všude, což u internetu není zdaleka pravda. [11]

[11] PEKÁRKOVÁ, Lucie. MOŽNOSTI ROZVOJE PŘÍMÉHO BANKOVNICTVÍ. Brno, 2008. 54 s. Bakalářská práce. Masarykova Univerzita, Ekonomicko-správní fakulta.

5.8.2 Možnosti internetbankingu

- ☑ Přehled účtů
- ☑ Platební příkazy v české měně, v cizích měnách
- ☑ Mobilní služby (dobíjení, platba faktur)
- ☑ Historie transakcí
- ☑ Trvalé příkazy, příkazy k inkasu
- ☑ Výpisy z transakcí zdarma

Po představení elektronického bankovnictví a jeho možností přichází na řadu dle mého názoru jedna z nejdůležitějších věcí v celém oboru internetového obchodování, a tou je bezpečnost. V následujících řádkách bude popsána problematika tohoto fenoménu dnešní doby.

5.9 Bezpečnost elektronického obchodování

5.9.1 Základní pojmy

- ☑ ***Autentizace*** – proces ověření identity subjektu, využívá se několik způsobů a jejich kombinací. Autentizace tedy probíhá podle toho:
  - co uživatel zná (heslo, PIN…)
  - co uživatel má (platební karta, privátní klíč…)
  - čím uživatel je (biometrické vlastnosti – otisk prstu, snímek sítnice…)
  - co uživatel umí (odpovědi na vygenerované dotazy)

- ☑ ***Autorizace*** – nastává v případě, že správně proběhla autentizace. Uděluje uživateli práva přístupu a povoluje určité aktivity.

- ☑ ***Identifikace*** – provádí systém, který se snaží porovnávat určitou sadu vzorků se vzorkem uživatele (otisky prstů, identifikační kódy atd.).

Problémem elektronického obchodování je přenos citlivých dat přes komunikační cestu, která není zabezpečená. Většinou se jedná o internet. Existuje několik požadavků, které musí výměna informací splňovat tak, aby došlo k bezpečnému a transparentnímu přenosu.

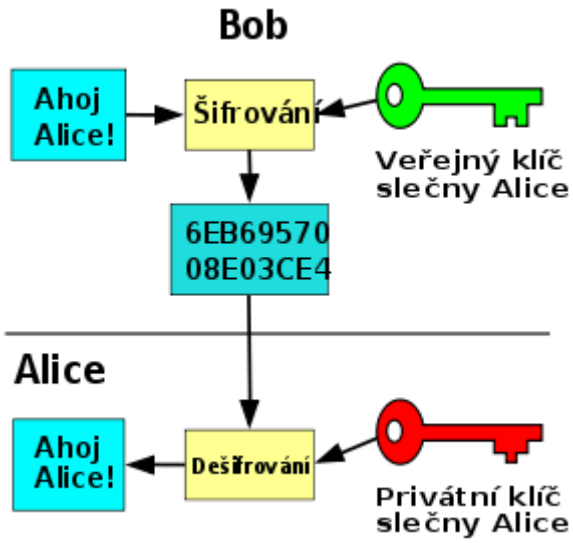
- ☑ ***Autentičnost dat*** – při přenosu lze ověřit a zjistit identitu uživatelů.

- ☑ ***Integrita dat*** – zajištění ověření, zda výměna informací proběhla vcelku beze změny obsahu.

- ☑ ***Důvěrnost dat*** – výměna dat je přístupná pouze dvěma stranám. Třetí strana nesmí být schopná obsah výměny identifikovat.

- ☑ ***Nepopiratelnost*** – odpovědnost osoby, která zprávu odeslala(přijala).

- ☑ ***Kryptografie*** – jinak také šifrování je základem bezpečného přenosu dat. Spočívá v převodu zprávy do podoby, která je čitelná pouze s určitou znalostí klíče. Data jsou nejdříve zakódována šifrou a po transferu dekódována klíčem. Algoritmus šifry bývá velice často známý, na druhé straně klíč je utajený a bez klíče se k zašifrované zprávě nedostaneme. Šifry se dělí dvěma způsoby:
  - symetrické – obě strany sdílejí stejný klíč (použije se k zakódování i dekódovaní zprávy)
  - asymetrické – každá strana má klíče dva (veřejný a soukromý), při posílání zprávu zašifrujeme veřejným klíčem příjemce a bez znalosti soukromého klíče ji nemůže nikdo jiný přečíst – viz Obr.1.



Obr. 1 - Asymetrické šifrování[12]

- ☑ ***Hašování*** – s jeho pomocí vytvoříme z celého textu pouze jeho otisk. Otisk může sloužit k jednoznačné identifikaci zašifrovaného textu, ale také kontroluje integritu dat. Slouží rovněž k rychlému vyhledávání, porovnávání atd. Vytvoření otisku je pouze jednosměrná funkce.

- ☑ ***Zaručený elektronický podpis*** – zaručuje autentizaci uživatele a integritu dat. Využívá asymetrického šifrování, kdy autor zakóduje dokument pomocí svého soukromého (tajného) klíče a tím je zajištěna autentičnost (je jediným vlastníkem tohoto klíče). Podpis je možno ověřit za použití autorova veřejného klíče.

Šifrováním neprochází celý dokument, ale jen jeho otisk (haš). Při ověření se tedy dešifruje otisk pomocí autorova veřejného klíče a porovná se s nezávislým výpočtem otisku dokumentu. Pokud jsou shodné, dokument je považován za důvěryhodný.
Samotný elektronický podpis nezaručuje důvěrnost zprávy. Vlastní dokument musí být ještě zašifrován veřejným klíčem příjemce.

---

[12] Zdroj: *Wikipedia* [online]. 2010 [cit. 2010-05-18]. Asymetrické šifrování. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Asymetrick%C3%A9_%C5%A1ifrov%C3%A1n%C3%AD>.

5.10 Zabezpečené protokoly

Protokol HTTP není sám osobě přizpůsobený pro využití v internetovém bankovnictví protože umožňuje pouze autentizaci uživatele na základě hesla a neumí například šifrovat data. Je proto třeba doplnit ho o SSL a tím vytvořit protokol HTTPS. Tento protokol lze využívat ve všech dostupných prohlížečích, které navíc využívají i dostačující 128-bitové šifrování.

Pro případného útočníka není problém získat přístup ke komunikaci mezi bankou a klientem, ale narazí na kvalitní šifrování dat, se kterým si neumí poradit.

Úroveň zabezpečení poskytována touto technologií je obecně považována za dostatečnou.

5.11 Současný stav ve firmě Profes Projekt s.r.o.

Již devátým rokem je firma Profes Projekt klientem UniCredit banky. Využívá podnikatelský účet Bussines konto exclusive s internetovým bankovnictvím BusinessNet.

Vzhledem ke stále častějším internetovým útokům na bankovní účty mě vedení firmy požádalo o analýzu bezpečnosti BusinessNet bankovnictví u UniCredit banky. Zároveň jsem firmě nabídnul, že analyzuji i další internetová bankovnictví a nabídnu alternativu, pokud by výše zmíněné internetové bankovnictví v analýze neuspělo.

V další kapitole bude následovat analýza prvků elektronického bankovnictví uvedených zejména v kapitole 5.9. Analýza se bude provádět vlastním průzkumem jednotlivých bankovních aplikací.

6 Analýza řešeného problému

V kapitole analýza řešeného problému se budu věnovat zevrubné analýze bezpečnosti elektronického bankovnictví v bankovním sektoru České republiky.

6.1 Výběr bankovního segmentu

Za úkol této diplomové práce jsem si zadal analýzu bankovního sektoru pouze v rámci bank působících na území České republiky. Do rozsáhlejší nabídky k diskuzi s firmou Profes Projekt jsem zařadil tyto banky, které nabízejí internetové bankovnictví a které mají dle požadavků firmy pobočku v maximální vzdálenosti do 20 km od města Turnov.

Jedná se o :

☑	Citibank	pobočka Liberec
☑	Česká spořitelna	pobočka Turnov
☑	Československá obchodní banka	pobočka Turnov
☑	GE money bank	pobočka Turnov
☑	ING bank	pobočka Liberec
☑	Komerční banka	pobočka Turnov
☑	mBank	pobočka Liberec
☑	Poštovní spořitelna	pobočka Liberec
☑	UniCredit bank	pobočka Liberec
☑	Volksbank	pobočka Liberec
☑	Raiffeisenbank	pobočka Liberec

Seznam výše uvedených bank jsem odeslal na konzultaci vedení firmy. Na základě jejich vlastních zkušeností a priorit jsem byl požádán o zpracování posudku bezpečnosti elektronického bankovnictví u pěti možných kandidátů na nového zprostředkovatele bankovních služeb. Následující odstavce obsahují seznam a představení jednotlivých bank a jejich přímého bankovnictví.

6.1.1 Komerční banka (KB)

Komerční banka

Kód banky:	0100
Adresa:	Na Příkopě 33,čp.969, 11407 Praha 1
Infolinka:	800 111 055
www:	www.kb.cz
email:	mojebanka@kb.cz

☑ ***Služba***

Z produktů Komerční banky jsem pro potřebu firmy vybral službu Excelent.

„Excelent je nadstandardní balíček bankovních produktů a služeb pro komplexní řízení Vašich firemních financí. Součástí balíčku je běžný korunový účet s možností čerpat povolený debet, běžný účet v cizí měně, dvě platební karty, telefonické bankovnictví a internetové nebo PC bankovnictví s 50 bezplatnými odchozími transakcemi měsíčně a současně 50 příchozích transakcí měsíčně zdarma.“[13]

☑ ***Přímé bankovnictví***

Komerční banka dále k bankovním službám nabízí e-banking pod názvem Profibanka.

„PC bankovnictví Profibanka je špičkový produkt přímého bankovnictví KB, který spojuje výhody internetového bankovnictví s výkonností lokálních aplikací. Splňuje všechny požadavky firem v oblasti platebního styku. Bezpečnostní řešení, které Profibanka využívá, je navrženo v souladu se standardy elektronického podpisu. Tak je zaručena špičková úroveň zabezpečení jak při komunikaci mezi bankou a uživatelem, tak při podepisování příkazů v rámci služby. Veškerá komunikace probíhá v protokolu SSL (Secure Socket Layer) a každou aktivní operaci uživatel podepisuje svým elektronickým podpisem.“ [14]

---

[13] *Komerční banka* [online]. 2006 [cit. 2010-03-16]. Excelent. Dostupné z WWW: <http://www.kb.cz/cs/seg/seg3/products/excelent_package.shtml>.

[14] *Komerční banka* [online]. 2006 [cit. 2010-02-25]. Profibanka. Dostupné z WWW: <http://www.kb.cz/cs/seg/seg4/products/profibanka.shtml>.

6.1.2 Raiffeisen bank

Raiffeisen bank

Kód banky:	5500
Adresa:	Hvězdova 1716/2b, 140 78 Praha 4
Infolinka:	800 900 900
www:	www.rb.cz
email:	info@rb.cz

☑ ***Služba***

Služeb pro firmy z nabídky banky Raiffeisen je několik. Jedná se o Profikonto, Pluskonto, Benefitkonto, Dualkonto a eKonto. Analýzou jednotlivých služeb jsem vybral službu eKonto ve verzi Premium.

„Podnikatelský účet eKonto a jeho služby Vám zajistí bezpečnou a pohodlnou správu Vašich financí. Zároveň získáte spořící účet Podnikatelské eKonto Plus s výhodnou úrokovou sazbou. Díky dvouprvkovému přístupu do internetového bankovnictví jsou Vaše finance stále v bezpečí.“[15]

☑ ***Přímé bankovnictví***

Internetové bankovnictví je automatickou součástí eKonta. V Raiffeisen Bank nemá přímé bankovnictví pojmenování. Na svých stránkách slibuje vysokou míru zabezpečení a výhodou nabídky této banky je nabídka tzv. eKomunikátoru, který dokáže propojit účetní systém firmy se systémem přímého bankovnictví.

---

[15] *Raiffeisen Bank* [online]. 2008 [cit. 2010-03-16]. Podnikatelské eKonto. Dostupné z WWW: <http://www.rb.cz/firemni-finance/podnikatele-a-male-firmy/podnikatelske-ucty/bezne-ucty/podnikatelske-ekonto/>.

6.1.3 Citibank

City Bank

Kód banky:	2600
Adresa:	Praha 6, Vokovice, Evropská 423/178, 166 40
Infolinka:	844 888 844
www:	www.citibank.cz
email:	info@rb.cz

☑ ***Služba***

Citibank má ve své nabídce služeb pro firmy dva balíčky. Jedná se o balíček Citibusiness a službu Citiprofession. V rámci přímého bankovnictví pokrývá potřeby a požadavky firmy. Pro naše potřeby vybírám službu Citibusiness.

„Citibusiness je bankovnictví pro malé a střední podniky a podnikatele a Vám přináší osobní přístup profesionálního bankéře, pohodlnou obsluhu Vašich financí v bezpečném internetovém bankovnictví, širokou nabídku produktů a služeb podle Vašich potřeb, individuální parametry úvěrových produktů a zázemí globální banky.“16

☑ ***Přímé bankovnictví***

Citibank Online je název přímého bankovnictví této banky. Jako většina bankovních domů, i tento anoncuje vysokou míru bezpečnosti elektronického bankovnictví.

---

16 *CitiBank* [online]. 2009 [cit. 2010-03-16]. CitiBusiness. Dostupné z WWW: <http://www.citi.com/czech/citibusiness/czech/docs/index.htm>.

6.1.4 Česká spořitelna

Česká spořitelna

Kód banky:	0800
Adresa:	Olbrachtova 1929/62 140 00 Praha 4
Infolinka:	800 207 207
www:	www.csas.cz
email:	csas@csas.cz

☑ ***Služba***

Mezi několika možnostmi jsem vybral program Profit, který je určen také malým firmám.

„Program PROFIT je společná nabídka produktů a služeb pro podnikatele a malé firmy s možností získat zvýhodněné produkty včetně např. zjednodušeného kontokorentu k běžnému účtu.“[17]

☑ ***Přímé bankovnictví***

Internetové bankovnictví jsem pro tuto službu zvolil SERVIS 24.

[17] *Česká spořitelna* [online]. 2008 [cit. 2010-03-16]. Program Profit. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/Profit_program_corp.xml?category=207>.

6.1.5 UniCredit Bank

UniCredit Bank

Kód banky: 2700

Adresa: Na Příkopě 20 111 21 Praha 1

Infolinka: 800 144 441

www: www.unicreditbank.cz

email: info@unicreditgroup.cz

☑ ***Služba***

Pro podnikatele a menší firmy banka nabízí program Business Konto v různých modifikacích. Firma Profes Projekt s.r.o. využívá Konto Exclusive.

„BUSINESS Konto se nabízí ve třech variantách, v závislosti na počtu transakcí zdarma, druhu přímého bankovnictví a typu platební karty. Záleží jen na Vašich potřebách, které BUSINESS Konto zvolíte. BUSINESS Konto Exklusive navíc od základu obsahuje všechny tuzemské příchozí i odchozí platby zadané elektronicky , Online Banking nebo BusinessNet Basic, 5 výběrů z bankomatů jiných bank, Visa Business nebo MasterCard (embosovaná debetní karta),vedení provozního úvěru a vedení druhého běžného účtu v Kč nebo v cizí měně„[18]

☑ ***Přímé bankovnictví***

UniCredit nabízí pro firmy ideální internetové bankovnictví pod názvem BusinessNet Basic.

„BusinessNet je službou internetového bankovnictví vytvořenou s cílem uspokojit náročné potřeby firemních klientů. K obsluze firemních účtů prostřednictvím služby BusinessNet postačí přístup na internet, internetový prohlížeč a na počítači nezávislý elektronický bezpečnostní klíč.“[19]

---

[18] *UniCredit Bank* [online]. 2009 [cit. 2010-03-16]. Business Konto. Dostupné z WWW: <http://www.unicreditbank.cz/cz/podnikatele/ucty/bussines-konto.html>.

[19] *UniCredit Bank* [online]. 2009 [cit. 2010-03-16]. Businessnet. Dostupné z WWW: <http://www.unicreditbank.cz/cz/podnikatele/prime-bankovnictvi/businessnet.html>.

6.2 Hrozba první - Uživatel

S novými útoky, či pokusy o útok na nějaký internetbanking se samozřejmě mění i ochrana proti nim.

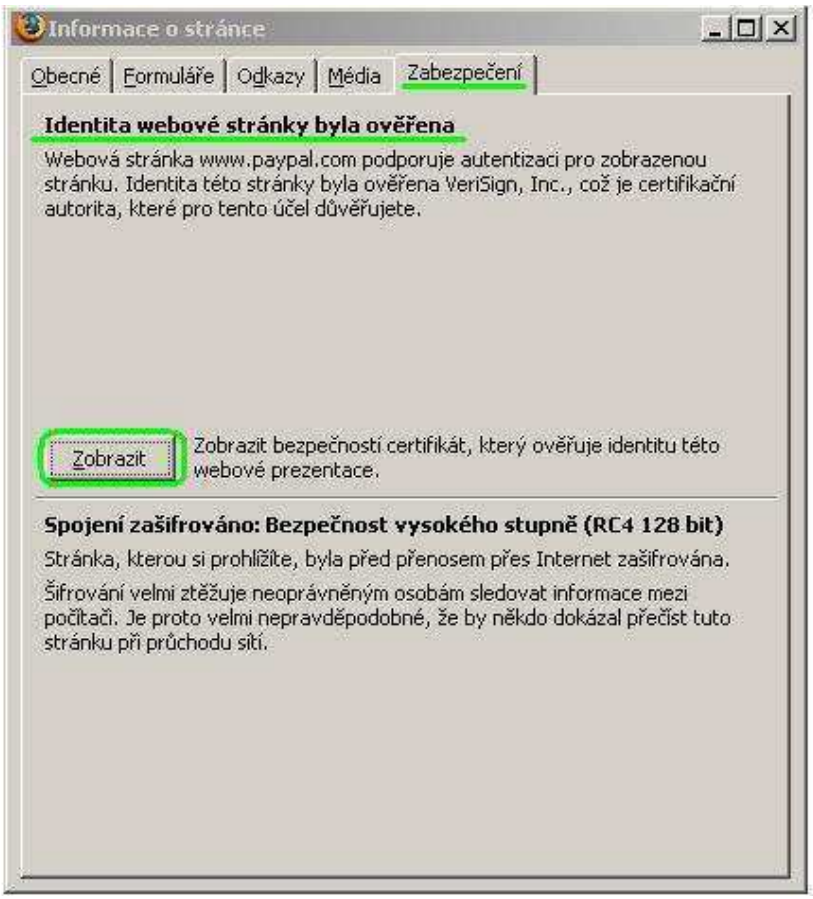
Běžný uživatel si pod pojmem zabezpečení představí pouze způsob přihlášení k aplikaci a možná ještě ověření odchozích transakcí. Požadavků na zabezpečení je samozřejmě více a jsou velice sofistikované. Často se jedná o velice protichůdná řešení a je těžké najít ideální stav, který by vyhovoval všem stranám, zejména tedy straně klientů a samotné bance.

Mnoho odborníků v oboru zajištění internetové bezpečnosti hovoří zcela jasně o tom, že největším problémem zabezpečení internetového bankovnictví je v dnešní době sám uživatel. V jednom případě je tím uživatelem nezkušený člověk, který nemá v počítači nainstalovány potřebné bezpečnostní prvky jako například antivirový program nebo firewall. Na druhé straně, a to je častější jev, jsou uživatelé relativně zběhlí v počítačové bezpečnosti, kteří ovšem nedbají instrukcí daného zabezpečovacího programu a často potvrdí chybová okna a hlášky, kterými jim program dává najevo, že něco není v pořádku, aniž by se seznámili s jejich obsahem. Dalším známým fenoménem počítačových pirátů je phishing.

6.2.1 Phishing

Tato počítačová kriminální aktivita není založena na krádeži dat jako ostatní, ale na dobrovolném prozrazení nezkušeným uživatelem. S phishingem se nejčastěji setkáme ve formě e-mailů. Uživateli přijde e-mail, který se zdánlivě podobá e-mailu od společnosti, se kterou uživatel pravidelně komunikuje, jedná se ale o podvrh. Tento podvrh většinou není těžké rozpoznat. Často se jedná o e-mail od uživatele, který má rozdílnou doménu než firma, za kterou se vydává. Phishing také poznáte podle toho, že odkaz, na který v e-mailu kliknete vás odkáže na stránku, která sice může vypadat povědomě, ale její hypertextový odkaz je určitě odlišný (např. http://www.paypal.com a http://www.paypa1.com).

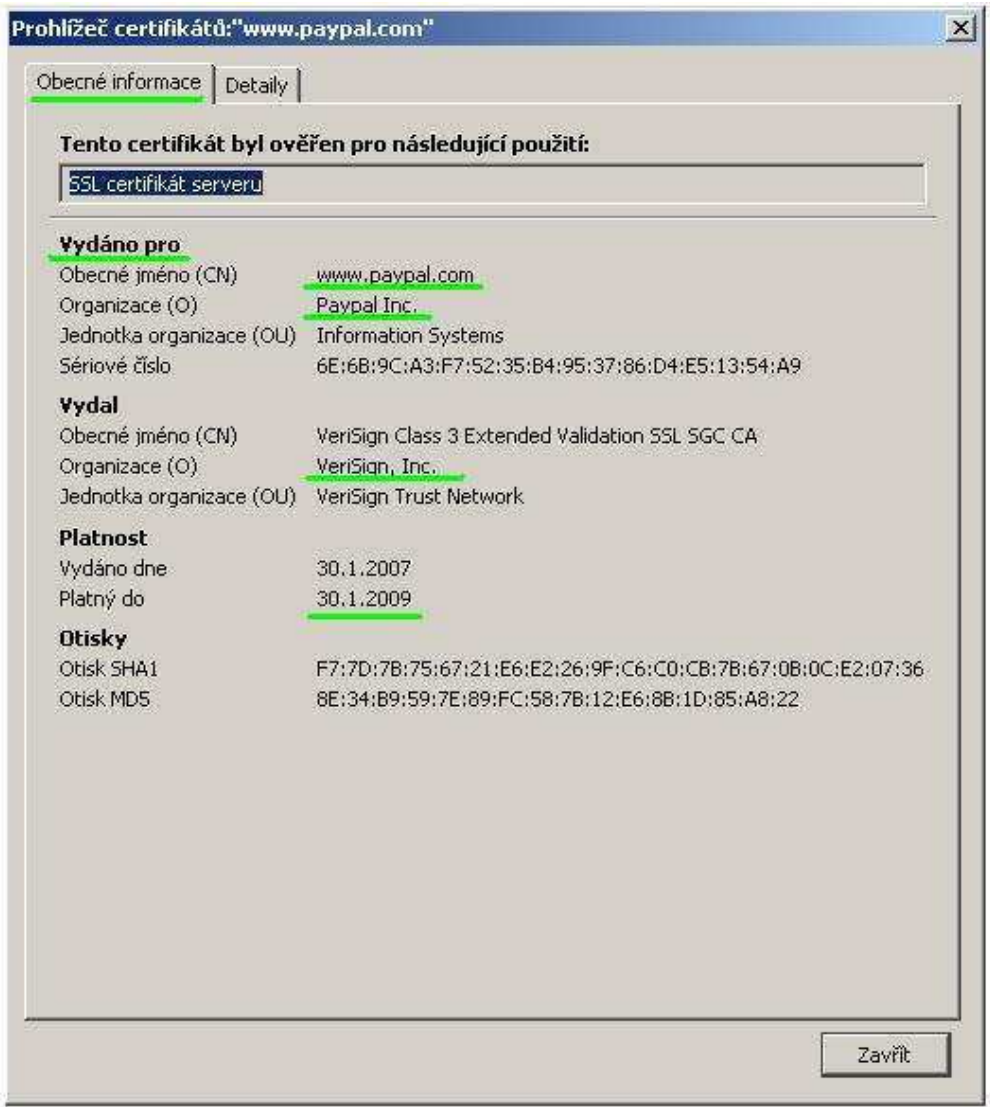
Pokud si chcete být opravdu jisti, že přijatý e-mail není škodlivý, pak je potřeba vyhledat v prohlížeči odkaz na zabezpečení stránky. V této záložce musí být uvedeno, že prohlížeč prověřil identitu stránky. Aby bylo toto možné, je nutné, aby prohlížeč měl v sobě importovaný kořenový certifikát certifikační autority, která stránku zabezpečuje. Ve většině případů se jedná o certifikační autoritu VeriSign, Inc.. Certifikát této autority je automaticky importován v každém prohlížeči již od jeho nainstalování.



Obr. 2 - Informace o stránce[20]

[20] *Hoax* [online]. 2010 [cit. 2010-05-18]. Phishing. Dostupné z WWW: <http://www.hoax.cz/phishing/>.

Dále je důležité ověřit si podrobnosti certifikátu, zda se majitel certifikátu shoduje s uvedenou společností, zda certifikát vydala důvěryhodná certifikační autorita a zda je časově platný. [21]



Obr. 3 - Prohlížeč certifikátů[22]

Pokud provedeme tuto vizuální kontrolu, můžeme mít v zabezpečené připojení důvěru.

---

[21] *Ibm.com* [online]. 2005 [cit. 2010-05-12]. Phishing and Internet Banking Security. Dostupné z WWW: <ftp://ftp..com/software/tivoli/whitepapers/Phishing_and_Internet_Banking_Security.pdf>.

[22] *Hoax* [online]. 2010 [cit. 2010-05-18]. Phishing. Dostupné z WWW: <http://www.hoax.cz/phishing/>.

6.2.2 Pharming

Pharming je novější a sofistikovanější forma phishingu. Neútočí přímo na uživatele, nýbrž na DNS[23] server, kterému zadá jiná kritéria překladu IP adres. Pokud tedy do vyhledávače zadáte hledanou stránku, pozměněný DNS server ji přeloží na jinou IP adresu a aniž by se dalo něčeho všimnout, ocitnete se na pirátské stránce.

Pharming lze provést i přímo v lokálních počítačích a to modifikací systémového souboru „hosts“, do kterého stačí přiřadit webové adrese IP adresu, na kterou má být uživatel přesměrován. Přístup do systémových souborů uživatele lze provést například infiltrací počítače trojským koněm.

Ochranou proti pharmingu je kvalitní a prověřený antivirový program, který se bude pravidelně aktualizovat. Překážkou může být i správně nastavený firewall.

Phishing i pharming jsou velkým problémem, se kterým toho bohužel kromě preventivních kroků v informovanosti klientů banky mnoho udělat nedokáží. Příkladem by mohlo být období, kdy klientům České spořitelny přišlo několik phishingových e-mailů. Spořitelna začala ihned rozesílat varovné zprávy, ovšem stejně zareagovali i piráti. Ti posílali podobné varovné zprávy, které opět obsahovaly odkazy na škodlivé stránky.

6.2.3 Další časté chyby

- Důvěra ve všechny certifikační autority

Uživatelé si často myslí, že jakýkoliv podepsaný certifikát jim zaručí korektnost dat. To je samozřejmě nesmysl, neboť certifikát může podepsat kdokoliv, kdo vlastní certifikační autoritu. Důležitá je kontrola toho, kdo certifikát vydal.

[23] DNS – Domain Name Server – hierarchický systém doménových jmen, překládá IP adresy na doménová jména

- Chyba při zadávání

Pokud uživatel vypisuje adresu ručně, může se stát, že v adresním řádku zapomene na písmeno „s“ při vypisování protokolu HTTPS. V tomto případě je možné, že se stránka otevře, ale SSL se nepoužije.

6.2.4 Doporučení firmě

Každá banka doporučuje sledovat a řídit se desaterem bezpečnosti přístupu k internetovému bankovnictví. I já doporučuji firmě řídit se tímto desaterem:

1)Ochrana souboru s osobním bezpečnostním certifikátem
2)používaní bezpečného (silného) PINu
3)ochrana hesla
4)sledování historie ochozích plateb a přihlašování
5)aktualizace softwarového vybavení počítače
6)používání svého počítače
7)používání anti-spyware programů a firewallů
8)nevstupování na neznámé stránky a nestahování neznámých souborů
9)otevírání pouze důvěryhodných
10) okamžité kontaktování při jakýchkoli pochybnostech [24]

[24] *Komerční banka* [online]. 2006 [cit. 2010-05-12]. Desatero bezpečnosti. Dostupné z WWW: <http://www.mojebanka.cz/cs/security.shtml>.

6.3 Hrozba druhá - Identifikace banky a šifrování dat

Každá nejen bankovní aplikace, která vyžaduje po uživatelích citlivé přístupové údaje musí být také vhodně zabezpečena. Každá banka v této době používá službu SSL, která vylepší standardní protokol pro přenos dat HTTP o bezpečnostní vrstvu a vznikne protokol HTTPS. Aby si mohl uživatel ověřit, zda se skutečně jedná o server, na který potřebuje zadat citlivé údaje a ne o jeho podvrh, používají banky certifikaci svých serverů pomocí komerčních certifikátů jednotlivých certifikačních autorit.

Certifikační autorita poté za provizi ověří na žádost uživatele stránku banky standardní procedurou, kterou ustanovuje ve své certifikační politice. V případě serverových certifikátů se ověřuje také samotné vlastnictví domény.

6.3.1 Důvěryhodnost a platnost certifikátů vybraných bank

Banka	Platnost certifikátu	Certifikační Autorita	Ověřování	Ochrana proti Clickjackingu
KB	18.3.2009 - 18.3.2011	VeriSign Class 3 Public Primary Certification Authority - G5	Extended Validation	Ano
Raiffeisen BANK	19.2.2010 - 19.2.2012	Class 3 Public Primary Certification Authority (OU)	Standartní	Ne
citibank	4.8.2009 - 4.8.2011	VeriSign Class 3 Public Primary Certification Authority - G5	Extended Validation	Ne
ČESKÁ SPOŘITELNA	11.7.2008 - 9.8.2010	Class 3 Public Primary Certification Authority (OU)	Standartní	Ne
UniCredit Bank	3.7.2009 - 3.7.2011	Class 3 Public Primary Certification Authority (OU)	Standartní	Ne

Tab. 1 - Důvěryhodnost a platnost certifikátů[25]

[25] zdroj vlastní z textu [2],[3],[9],[17],[20].

☑ ***Platnost certifikátu***

Každý certifikát se vydává na předem stanovenou dobu. Čím je tato doba kratší, tím častěji musí banka žádat o novou certifikaci a tím častěji se prověřuje a aktualizuje důvěryhodnost zabezpečení. Dá se tedy říci, že čím kratší je perioda obnovování certifikátu, tím zabezpečenější je i server. Běžné certifikáty se zpravidla vydávají na jeden rok. Všechny vybrané banky mají zajištěnu certifikaci na 2 roky, takže v tomto hledisku jsou si naprosto vyrovnané.

Dalo by se uvažovat o tom, že ta banka, která má nejčerstvěji obnovený certifikát, bude mít také nejaktuálnější a nejbezpečnější certifikát v tomto pohledu. Je to samozřejmě pravda, ovšem platnost certifikátů je v tomto případě srovnání celkem zanedbatelnou položkou.

☑ ***Certifikační autorita***

Certifikační autorita je subjekt, který zabezpečuje vydávání elektronicky podepsaných veřejných šifrovacích klíčů (digitálních certifikátů). Tímto způsobem, na základě principu přenosu důvěry, potvrzuje pravdivost údajů na zabezpečené stránce.
Přenosem důvěry se míní to, že se certifikační autorita svým podpisem zaručí za důvěryhodnost zabezpečené stránky a samotnému uživateli (popř.prohlížeči, softwaru…) k jistotě stačí, aby důvěřoval uvedené certifikační autoritě.

Všechny analyzované banky mají svůj certifikát provozovaný americkou společností VeriSign, Inc., která je špičkou v oboru a zajišťuje plnou důvěryhodnost certifikátu. Společnost VeriSign, Inc. dále provozuje dva ze třinácti kořenových serverů DNS, které jsou klíčové pro fungování celého internetu. Svoje certifikační služby dělí na několik tříd:

- Class 1 – třída určená jednotlivcům
- Class 2 – pro organizace
- Class 3 – třída určená pro větší servery s nutností digitálního podpisu, kde je zapotřebí nezávislé potvrzení certifikační autoritou
- Class 4 – transakce mezi společnostmi
- Class 5 – pro vládní bezpečnost, pro soukromé subjekty

Všechny banky využívají třídu Class 3.

☑ ***Ověřování***

Pouze Komerční banka a Citibank využívají modernějších metod dodatečného ověřování. Využívají tzv. EV SGC SSL certifikáty[26].

Rozšířené ověřování (EV) poskytuje vyšší úroveň zabezpečení a zajišťuje uživateli snadnější identifikaci tohoto lepšího zabezpečení tím, že při přístupu na stránku zabarví adresní řádek v prohlížeči na zeleno. Certifikát je vylepšený o principy ověřování žadatelů o certifikát. Tyto principy podléhají CA/Browser Forum, které zaštiťuje důležité certifikační autority a výrobce prohlížečů. Je to nejnovější druh certifikátů, který dokáží využít pouze moderní prohlížeče (Microsoft Internet Explorer 7, Mozilla Firefox 3.5, Safari 3.2., Opera 9.5 a Google Chrome).
Server Gated Cryptography (SGC) je pouze rozšířením protokolu, které umožňuje ve starších prohlížečích odemknout silnější způsoby šifrování. Do roku 2000 prohlížeče standardně využívali pouze slabé šifrování (40/56 bitů) kvůli omezením ze strany vlády USA. Některé certifikační autority proto byly oprávněny využít nástroje pro vylepšení šifrování v těchto prohlížečích.

[26] EV SGC SSL certifikáty – Extended Validation, Server Gared Crypthography, Secure sockets Layer

☑ ***Ochrana proti ClickJackingu***

ClickJacking je poměrně novou hrozbou pro bezpečí na internetu. Jedná se o způsob, kdy hacker zneužije funkci programovacího jazyka HTML, která slouží k vkládání obsahu z jiných webových stránek. Útočník potom prakticky donutí uživatele na toto tlačítko kliknout a tím může útočník dokonce přednastavit přehrávač tak, že mu umožní například uživatele odposlouchávat.

Ochrana proti ClickJackingu není jednoduchá a mnoho odborníků se domnívá, že zatím žádná stoprocentní ochrana neexistuje.

Mezi internetovými bankovnictvími zkoumaných bank obsahuje ochranu proti ClickJackingu pouze bankovnictví Komerční banky. Jediná další banka s touto ochranou na českém trhu je mBank.

6.3.2 Podpora protokolů

V této části analýzy budu zkoumat, které protokoly jsou podporovány SSL serverem banky. Server může podporovat i několik možných protokolů a každý z nich se liší svým zabezpečením.

Banka	TLS 1.2	TLS 1.1	TLS 1.0	SSL 3.0	SSL 2.0 +U.S.	SSL 2.0
KB	Ne	Ne	Ano	Ano	Ano	Ne
Raiffeisen BANK	Ne	Ne	Ano	Ano	Ano	Ne
citibank	Ne	Ne	Ne	Ano	Ano	Ne
ČESKÁ SPOŘITELNA	Ne	Ne	Ano	Ano	Ano	Ano
UniCredit Bank	Ne	Ne	Ano	Ano	Ano	Ano

Tab. 2 - Podpora protokolů[27]

[27] zdroj vlastní z textu [2],[3],[9],[17],[20].

Protokoly SSL a TLS poskytují zabezpečenou možnost komunikace na internetu, která znemožňuje odposlouchávání nebo falšování komunikace.

Protokoly SSL a TLS zahrnují mnoho bezpečnostních opatření:

- „Klient používá veřejný klíč certifikační autority (CA) k ověření jejího digitálního podpisu v serverovém certifikátu. Lze-li digitální podpis CA ověřit, klient přijme serverový certifikát jako platný certifikát vydaný důvěryhodnou CA.
- Klient ověřuje, zda je vydávající certifikační autorita na seznamu důvěryhodných CA.
- Klient kontroluje dobu životnosti serverového certifikátu. Autentizační proces se zastaví, pokud doba jeho platnosti vypršela.
- K ochraně před útoky typu Man-in-the-Middle porovnává klient aktuální DNS jméno serveru se jménem z certifikátu.
- Ochrana před několika známými útoky (včetně Man-in-the-Middle), jako je snaha o použití nižší (méně bezpečné) verze protokolu nebo slabšího šifrovacího algoritmu.
- Opatření všech aplikačních záznamů pořadovými čísly a používání těchto čísel v MAC.
- Používání ověřovacího kódu zprávy rozšířeného o klíč, takže jen vlastník klíče dokáže MAC ověřit. Jen v TLS.
- Zpráva ukončující inicializaci (Finished) obsahuje haš všech zpráv vyměněných v rámci inicializace oběma stranami.
- SSL 3.0 je proti SSL 2.0 vylepšeno přidáním šifer založených na SHA-1 a podporou autentizace certifikáty. Další vylepšení SSL 3.0 zahrnují lepší inicializační protokol a vyšší odolnost proti útokům typu man-in-the-middle.“[28]

[28] *Wikipedia* [online]. 2010 [cit. 2010-04-20]. Transport Layer Security. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Transport_Layer_Security>.

Výše uvedené protokoly jsou seřazeny sestupně od nejbezpečnějšího po nejméně bezpečný(tzn. TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0, SSL 2.0 + Upgrade support, SSL 2.0). Za celkovou bezpečnost serveru z hlediska protokolů je potřeba brát kombinaci všech využitých protokolů.

6.3.3 Šifrování

Banka	Klíč	Dékla klíče(bit)	Podpisový algoritmus
KB	RSA	2048	SHA1
Raiffeisen BANK	RSA	1024	SHA1
citibank	RSA	2048	SHA1
ČESKÁ SPOŘITELNA	RSA	1024	SHA1
UniCredit Bank	RSA	1024	SHA1

Tab. 3 - Šifrování[29]

☑ ***Klíč***

Při dešifrování šifrovacího systému RSA se naráží na dva problémy. Prvním je faktorizace (rozklad čísla na prvočíslo) a druhým RSA problém (získávání kořenu modulu množiny).

Všechny banky využívají standardní veřejné šifrování pomocí RSA.

[29] zdroj vlastní z textu [2],[3],[9],[17],[20].

☑ ***Délka klíče***

Typická délka klíčů se v dnešní době pohybuje mezi 1024 a 2048 bity. Čím větší délka klíče, tím se považuje šifra za bezpečnější a hůře prolomitelnou. Podle expertů se v blízké době podaří prolomit 1024 bitů dlouhý klíč. Toto tvrzení není jednotné, ale již v podvědomí se klíče 1024 bitů dlouhé nepovažují za extra bezpečné. Doporučenou délkou klíče je v dnešní době minimálně 2048 bitů.

☑ ***Podpisový algoritmus***

„SSH umožňuje bezpečnou komunikaci mezi dvěma počítači, která se využívá pro zprostředkování přístupu k příkazovému řádku, kopírování souborů a též jakýkoliv obecný přenos dat (s využitím síťového tunelování). Zabezpečuje autentizaci obou účastníků komunikace, transparentní šifrování přenášených dat, zajištění jejich integrity a volitelnou bezeztrátovou kompresi. Server standardně naslouchá na portu TCP/22.“[30]

Předpokládejme, že každý server(v našem případě banka) má vytvořený RSA veřejný klíč(v našem případě 1024 nebo 2048 bitů dlouhý) a ještě musí každou hodinu automaticky generovat ještě jeden RSA klíč, který se ovšem neukládá, ale slouží při komunikaci.

Spojení klienta a serveru pak vypadá následovně:

1. Klient naváže TCP spojení na portu 22
2. Server se představí – jmenuji se SSH-1 atd…
3. Klient se představí
4. Pokud se zjistí, že si nerozumí, spojení tím končí
5. Pokud si rozumí, pak server pošle svůj veřejný klíč RSA a klíč generovaný každou hodinu
6. Klient vygeneruje sessionkey a zašifruje jej oběma klíči serveru
7. Klient pošle zašifrovaný sessionkey
8. Obě strany začnou šifrovat [31]

---

[30] *Wikipedia* [online]. 2010 [cit. 2010-05-13]. Serure Shell. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Secure_Shell>.

[31] *Přírodovědecká fakulta, Univerzita Karlova* [online]. 2004 [cit. 2010-05-13]. Bezpečné vybírání elektronické pošty. Dostupné z WWW: <http://web.natur.cuni.cz/~kuda/howtos/ssh.html>.

6.3.4 Síla šifry

Banka	Šifra s nejkratší délkou (bitů)	Šifra s největší délkou (bitů)
KB	128	128
Raiffeisen BANK	128	168
citibank	128	256
ČESKÁ SPOŘITELNA	40	128
UniCredit Bank	40	256

Tab. 4 - Síla šifry[32]

Silnější šifra (více bitů) zaručuje silnější zakódování, které pro případného útočníka znamená, že musí vyvinou mnohem větší úsilí při případném pokusu o prolomení. Server může podporovat šifry s různou silou(délkou), proto je v tabulce kvůli následnému výpočtu uvedena vždy nejslabší a nejsilnější šifra.

[32] zdroj vlastní z textu [2],[3],[9],[17],[20].

6.4 Hrozba třetí – Autentizace klienta a autorizace transakce

6.4.1 Jméno a heslo, certifikát, kalkulátor

Banka	Jméno a heslo	Certifikát	Autentizační kalkulátor
KB	Ne	Ano	Ne
Raiffeisen BANK	Ano	Ano	Ano
citibank	Ano	Ne	Ano
ČESKÁ SPOŘITELNA	Ano	Ne	Ano
UniCredit Bank	Ano	Ne	Ano

Tab. 5 - Autentizace klienta a autorizace transakce 1[33]

☑ ***Jméno a heslo***

Autentizace jménem a heslem je pro uživatele nejznámější. Skrývá ale mnoho potencionálních rizik. Největším a nejsnadnějším je vizuální odhalení (průmyslová kamera) popřípadě škodlivý software v počítači, který údaje přečte a odešle.

Je také zapotřebí porovnat náročnost a délku hesel. Jako uživatelské jméno se občas používá i číslo smlouvy, ovšem jako heslo je potřeba nastavit silnou kombinaci a to nejlépe písmen, číslic ale také speciálních znaků. Pokud je heslo dostatečně dlouhé (standardně minimálně 8 znaků) a obsahuje výše zmíněné komponenty, můžeme ho považovat za bezpečné.

Jméno a heslo bude v internetovém bankovnictví vždy jen část autentizace. Například certifikát v souboru v kombinaci se jménem a heslem vytváří silnou autentizační strukturu.

---

[33] *Měšec* [online]. 2010 [cit. 2010-05-18]. Přímé bankovnictví. Dostupné z WWW: <http://www.mesec.cz/produkty/prime-bankovnictvi/>.

☑ ***Certifikát***

Osobní certifikát se vydává jako soubor na pobočce banky na přenosném médiu (disketa, CD, flash disk…). Platnost certifikátu je zpravidla 1 rok a každý rok se tedy generuje certifikát nový. Například v případě Komerční banky probíhá generování certifikátu pomocí náhodných pohybu uživatele kurzorem myši. Tím se zajistí naprostá náhodnost a jedinečnost vygenerovaného certifikátu.

Při přístupu do internetového bankovnictví musíte zadat cestu k souboru, kde je certifikát uložen a svojí autentizaci potvrdit heslem k certifikátu.

Tento typ autentizace se nazývá dvoufaktorová autentizace, tzn. využívá to, co vím a co mám.

☑ ***Autentizační kalkulátor***

Autentizační kalkulátor je mobilní zařízení, které si musíte většinou od banky nebo jiné společnosti zakoupit. Po zapnutí kalkulátoru zadáte PIN, který máte již nastavený, určíte částku o kterou v transakci půjde, zadáte číslo účtu, předčíslí i kód banky příjemce a potvrdíte. Autentizační kalkulátor vygeneruje na základě zadaných údajů standardně desetimístný autentizační kód, pomocí které autentizujete transakci odeslanou do banky.

Autentizační kalkulátory jsou bezpečnější formou, jsou ale velice nepohodlné. Je nutné s sebou mít při ruce autentizační kalkulátor a každá transakce se generováním autentizačního kódu nepříjemně prodlužuje.

6.4.2 Běžná SMS, SMS Tookit, Čipová karta

Banka	Běžná SMS	Šifrovaná SMS SIM Toolkit	Čipová karta
KB	Ano	Ne	Ano
Raiffeisen BANK	Ano	Ano	Ne
citibank	Ne	Ne	Ne
ČESKÁ SPOŘITELNA	Ano	Ne	Ano
UniCredit Bank	Ano	Ne	Ne

Tab. 6 - Autentizace klienta a autorizace transakce 2[34]

☑ ***Běžná SMS***

Autentizace běžnou SMS zprávou zaručuje, že autorizaci platby nelze provést bez mobilního telefonu resp. SIM karty, jejíž telefonní číslo uživatel uvedl při podpisu smlouvy s bankou. Pro autentizaci je po zadání údajů platebního styku odeslána SMS zpráva s autentizačním kódem na telefonní číslo, které si klient zvolil. Transakci nelze bez zadání tohoto čísla autorizovat.

☑ ***Šifrovaná SMS, SIM Toolkit***

Toto řešení se využívá především v GSM bankovnictví. Na SIM kartu mobilního telefonu se nahraje bankovní aplikace, pomocí které se automaticky sestaví zpráva a odešle do příslušné banky.

---

[34] *Měšec* [online]. 2010 [cit. 2010-05-18]. Přímé bankovnictví. Dostupné z WWW: <http://www.mesec.cz/produkty/prime-bankovnictvi/>.

Vzhledem k tomu, že o využívání GSM bankovnictví firma Profes Projekt neuvažuje, je tato položka v tabulce pouze informativní a nebude zahrnuta do celkového hodnocení bezpečnosti.

☑ ***Čipová karta***

Můžeme se setkat i s terminologií tzv. Tokenů. Kromě čipové karty uživatel potřebuje ještě čtečku čipových karet, která se standardně připojuje k počítači přes USB rozhraní nebo sériový port (zřídka čtečka integrovaná v PC Card).

Princip je takový, že aplikace odešle data připravená k autentizaci do čipové karty, procesor v čipové kartě data zpracuje a vrátí zpět do počítače. Obrovskou výhodou čipových karet je fakt, že soukromý klíč nikdy neopustí čipovou kartu a nelze žádným způsobem kopírovat.

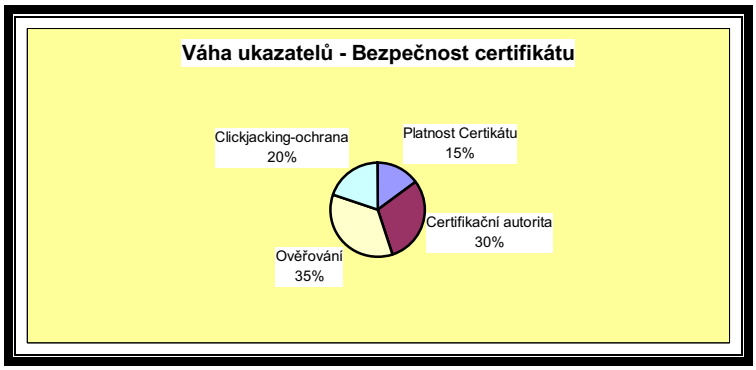
7 Návrh řešení problému

V dalších podkapitolách se budu věnovat hodnocení bezpečnosti jednotlivých internetových bankovnictví. V první řadě jsem si určil koeficienty (váhy) jednotlivých složek analyzovaných bankovnictví podle toho, jak velký mají na celkovou bezpečnost vliv. Čím nižší koeficient, tím menší vliv a naopak.

Výsledné s koeficientem přepočítané body jsem v rámci jedné banky sečetl a výsledkem je procentuální bezpečnost dílčího odvětví elektronického bankovnictví.

7.1 Hodnocení bezpečnosti certifikátu

Následující graf zobrazuje podíl jednotlivých položek v analýze důvěryhodnosti a platnosti certifikátů na celkovém hodnocení bezpečnosti certifikátu. Váhy jednotlivých ukazatelů jsou určeny dle osobních zkušeností autora.



Graf 1 - Váha ukazatelů - Bezpečnost certifikátu[35]

Tabulka níže obsahuje početní ohodnocení bezpečnosti certifikátů vybraných bank. Každá položka (Platnost certifikátu, Certifikační autorita atd.) má v levém sloupci popsány parametry hodnocení. Toto hodnocení je dále přepočítáno s koeficientem podílu z Grafu 1 a výsledkem je počet bodů, který se dále sečte s ostatními položkami a výsledkem je celkový počet procent bezpečnosti certifikátů jednotlivých bank.

[35] Zdroj vlastní

	Komerční banka	Raiffeisen bank	Citibank	Česká spořitelna	UniCredit bank
Platnost certifikátu					
100b.-více jak 20 měsíců		✓			
80b.-více jak 15 měsíců					
60b.-více jak 10 měsíců	✓		✓		✓
40b.-více jak 5 měsíců					
20b.-více jak 2 měsíce				✓	
Celkem bodů	60	100	60	20	60
Bodů s koeficientem 0,15	**9**	**15**	**9**	**3**	**9**
Certifikační autorita					
100b.-VeriSign Class3	✓		✓		
50b.-PCA Class3		✓		✓	✓
Celkem bodů	100	50	100	50	50
Bodů s koeficientem 0,3	**30**	**15**	**30**	**15**	**15**
Ověřování					
100b.-Extended Validation	✓		✓		
50b.-Standartní		✓		✓	✓
Celkem bodů	100	50	100	50	50
Bodů s koeficientem 0,35	**35**	**17,5**	**35**	**17,5**	**17,5**
Ochrana proti clickjackingu					
100b.-Ano	✓				
0b.-Ne		✓	✓	✓	✓
Celkem bodů	100	0	0	0	0
Bodů s koeficientem 0,2	**20**	**0**	**0**	**0**	**0**
Bezpečnost certifikátu	**94%**	**48%**	**74%**	**36%**	**42%**

Tab. 7 - Bezpečnost certifikátu[36]

Z analýzy bezpečnosti certifikátů jasně vyplývá, že nejbezpečnější parametry splňuje elektronické bankovnictví komerční banky s výbornými 94% ze 100% možných. Z velké míry je toto hodnocení ovlivněno tím, že banka jako jediná nabízí ochranu proti clickjackingu. Slušného výsledku dosáhla také Citibank se 74%. Na opačném konci tabulky vidíme elektronické bankovnictví České spořitelny s mizernými 36%. Do hodnocení je ale započítána i blížící se expirační doba certifikátu u kterého se

[36] zdroj vlastní

dá s jistotou předpokládat, že bude o další dva roky prodloužen. Z hlediska analýzy je ale zapotřebí zahrnout i toto kritérium.

7.1.1 Hodnocení bezpečnosti protokolů

Tabulka hodnocení bezpečnosti protokolů obsahuje soupis protokolů využívaných tou kterou bankou. V celkovém hodnocení se projevuje průměr vytvořený z nejlepšího a nejhoršího podporovaného protokolu.

	Komerční banka	Raiffeisen bank	Citibank	Česká spořitelna	UniCredit bank
Podpora protokolu					
100b.-TLS 1.2					
95b.-TLS 1.1					
90b.-TLS 1.0	✓	✓		✓	✓
80b.-SSL 3.0	✓	✓	✓	✓	✓
20b.-SSL 2.0				✓	✓
Celkem bodů (průměr amplitud)	**85**	**85**	**80**	**55**	**55**
Bezpečnost protokolů	**85%**	**85%**	**80%**	**55%**	**55%**

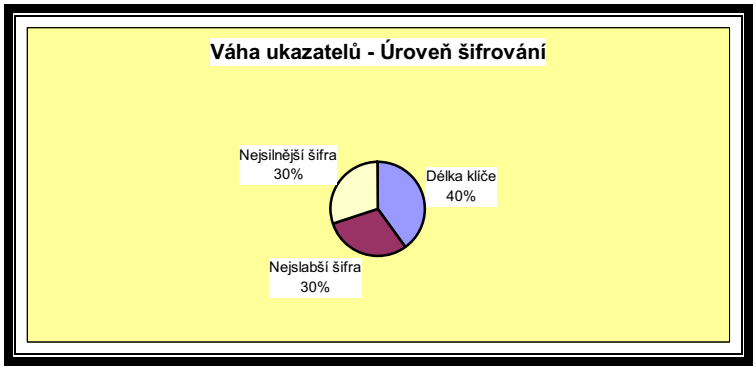
Tab. 8 - Hodnocení bezpečnosti protokolů[37]

Velice dobrého výsledku dosáhli hned tři analyzovaná elektronická bankovnictví. Jedná se o bankovnictví Komerční banky, Raiffeisen banky a Citibank, které všechny dosáhly hranice kolem 80%. Ostatní dvě banky v hodnocení doplatili na to, že stále využívají i zastaralý protokol SSL 2.0.

[37] zdroj vlastní

7.1.2 Hodnocení úrovně šifrování

Následující graf zobrazuje podíl jednotlivých položek v analýze úrovně šifrování na celkovém hodnocení šifrování. Váhy jednotlivých ukazatelů jsou určeny dle osobních zkušeností autora a poznatků získaných při psaní této diplomové práce.



Graf 2 - Váha ukazatelů - Úroveň šifrování[38]

V tabulce úrovně šifrování se hodnotí délka klíče podle kritérií uvedených v levém sloupci. Dále se hodnotí nejslabší a nejsilnější používaná šifra. Obě mají stejnou váhu a tedy i stejný koeficient na přepočítání bodů.

[38] zdroj vlastní

	Komerční banka	Raiffeisen bank	Citibank	Česká spořitelna	UniCredit bank
Délka klíče					
100b.-4096b					
80b.-2048b	✓		✓		
40b.-1024b		✓		✓	✓
0b.-méně než 1024b					
Celkem bodů	80	40	80	40	40
Bodů s koeficientem 0,4	**32**	**16**	**32**	**16**	**16**
Nejslabší šifra					
100b.-256b a více					
80b.-128b a více	✓	✓	✓		
20b.-64 až 127b					
0b.-méně než 64b				✓	✓
Celkem bodů	80	80	80	0	0
Bodů s koeficientem 0,3	**24**	**24**	**24**	**0**	**0**
Nejsilnější šifra					
100b.-256b a více			✓		✓
80b.-128b a více	✓	✓		✓	
20b.-64 až 127b					
0b.-méně než 64b					
Celkem bodů	80	80	100	80	100
Bodů s koeficientem 0,3	**24**	**24**	**30**	**24**	**30**
Úroveň šifrování	**80%**	**64%**	**86%**	**40%**	**46%**

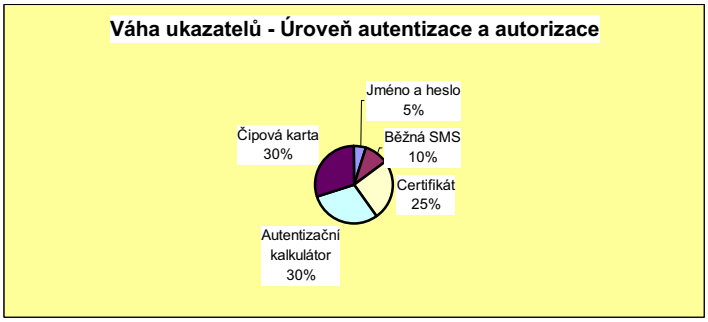
Tab. 9 - Úroveň šifrování[39]

Z hlediska šifrování se na prvním příčce umístila Citibank s výborným hodnocením 86%. S lehkým odstupem je na druhém místě komerční banka a s ještě relativně přijatelným hodnocením banka Raiffeisen na místě třetím. Poslední dvě banky získaly podprůměrné hodnocení a to hlavně kvůli nevyhovující nejslabší podporované šifře.

[39] zdroj vlastní

7.1.3 Hodnocení úrovně autentizace a autorizace

Následující graf zobrazuje podíl jednotlivých položek v analýze úrovně autentizace a autorizace na celkovém hodnocení této úrovně. Váhy jednotlivých ukazatelů jsou určeny dle osobních zkušeností autora a poznatků získaných při psaní této diplomové práce.



Graf 3 - Váha ukazatelů - Úroveň autentizace a autorizace[40]

V tabulce úrovně autentizace a autorizace porovnávám možnosti i kombinace prvků použitých při autentizaci uživatele i při následné autorizaci transakce.

[40] zdroj vlastní

	Komerční banka	Raiffeisen bank	Citibank	Česká spořitelna	UniCredit bank
Jméno a heslo					
100b.-Ano		✓	✓	✓	✓
0b.-Ne	✓				
Celkem bodů	0	100	100	100	100
Bodů s koeficientem 0,05	**0**	**5**	**5**	**5**	**5**
Certifikát					
100b.-Ano	✓	✓			
0b.-Ne			✓	✓	✓
Celkem bodů	100	100	0	0	0
Bodů s koeficientem 0,25	**25**	**25**	**0**	**0**	**0**
Autentizační kalkulátor					
100b.-Ano		✓	✓	✓	✓
0b.-Ne	✓				
Celkem bodů	0	100	100	100	100
Bodů s koeficientem 0,30	**0**	**30**	**30**	**30**	**30**
Běžná SMS					
100b.-Ano	✓	✓		✓	✓
0b.-Ne			✓		
Celkem bodů	100	100	0	100	100
Bodů s koeficientem 0,10	**10**	**10**	**0**	**10**	**10**
Čipová karta					
100b.-Ano	✓			✓	
0b.-Ne		✓	✓		✓
Celkem bodů	100	0	0	100	0
Bodů s koeficientem 0,3	**30**	**0**	**0**	**30**	**0**
Úroveň autentizace a autorizace	**65%**	**70%**	**35%**	**75%**	**45%**

Tab. 10 - Úroveň autentizace a autorizace[41]

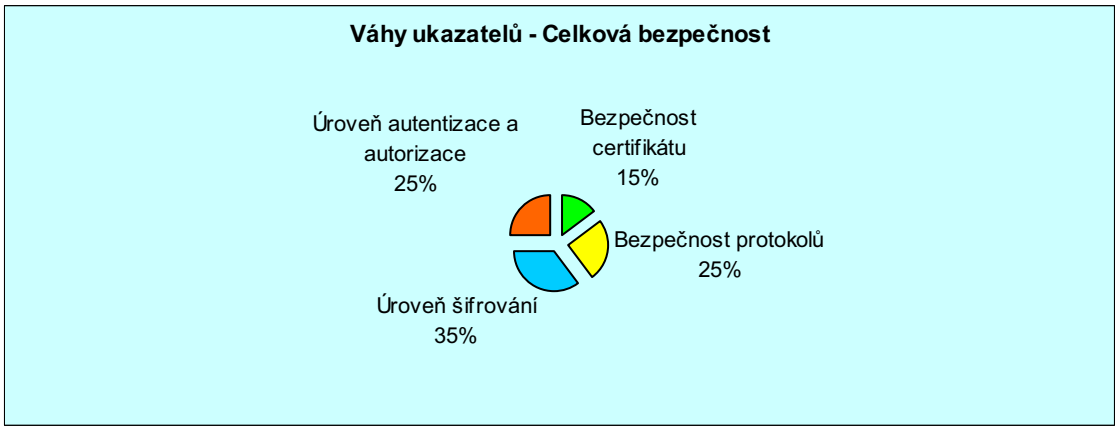
Autentizace a autorizace je silnou stránkou elektronického bankovnictví České spořitelny. Komerční a Raiffeisen banka také nemají špatné hodnocení. UniCredit bank a Citibank jsou pod průměrem a to zejména proto, že nepoužívají ani certifikát v souboru ani certifikát na čipové kartě.

[41] zdroj vlastní

7.2 Hodnocení celkové bezpečnosti

Následující graf zobrazuje podíl jednotlivých položek v analýze celkové bezpečnosti . Váhy jednotlivých ukazatelů jsou určeny dle osobních zkušeností autora a poznatků získaných při psaní této diplomové práce.

Nejvyšší váhu kladu na úroveň šifrování komunikace v rámci elektronického bankovnictví. Bezpečnost protokolů a autentizace s autorizací se shodně podílejí ne celku jednou čtvrtinou. Nejméně důležitou složkou je zabezpečení certifikátu, které se na hodnocení podílí 15-ti procenty.



Graf 4 - Váhy ukazatelů - Celková bezpečnost[42]

Dle výše uvedeného grafu vah ukazatelů celkové bezpečnosti jsem v následující tabulce přepočítána úroveň celkové bezpečnosti elektronických bankovnictví jednotlivých bank. Podíly jsou v rámci jedné banky sečteny a tvoří celkové hodnocení bezpečnosti elektronického bankovnictví banky.

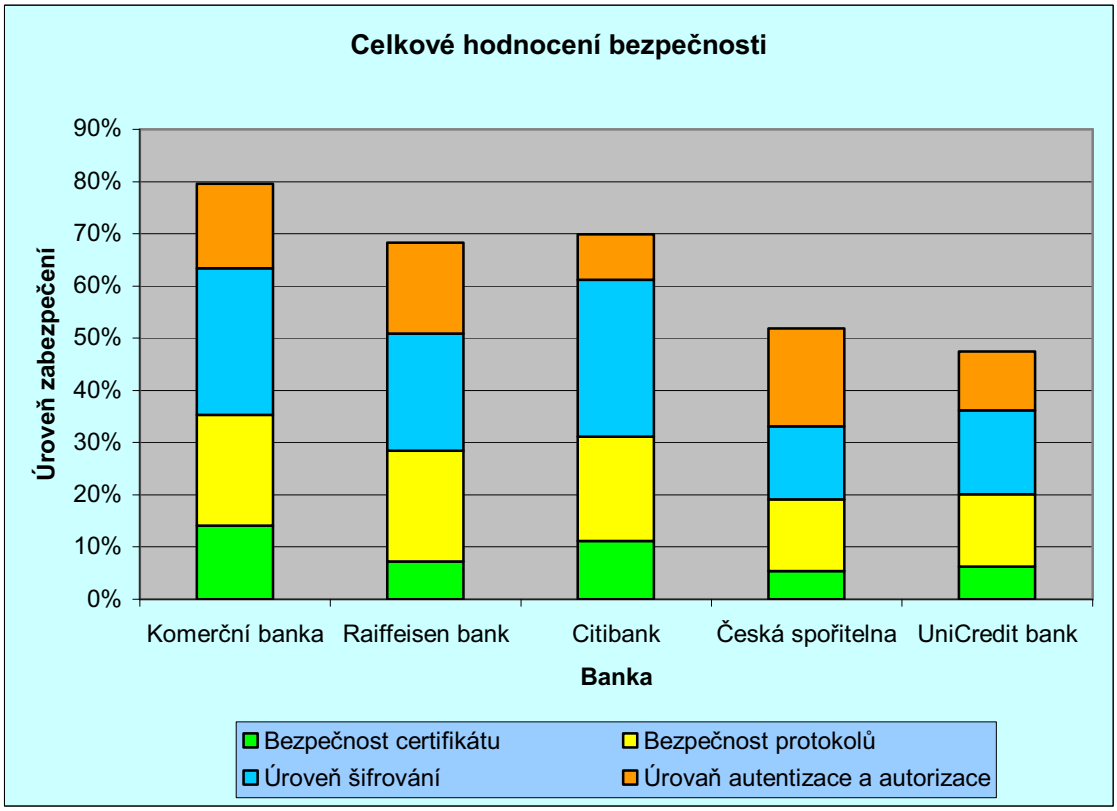
[42] zdroj vlastní

	Komerční banka	Raiffeisen bank	Citibank	Česká spořitelna	UniCredit bank
Bezpečnost certifikátu	94%	48%	74%	36%	42%
Podíl s váhou 0,15	**14%**	**7%**	**11%**	**5%**	**6%**
Bezpečnost protokolů	85%	85%	80%	55%	55%
Podíl s váhou 0,25	**21%**	**21%**	**20%**	**14%**	**14%**
Úroveň šifrování	80%	64%	86%	40%	46%
Podíl s váhou 0,35	**28%**	**22%**	**30%**	**14%**	**16%**
Úroveň autentizace a autorizace	65%	70%	35%	75%	45%
Podíl s Váhou 0,25	**16%**	**18%**	**9%**	**19%**	**11%**
Celková bezpečnost	**80%**	**68%**	**70%**	**52%**	**47%**

Tab. 11 - Celková bezpečnost[43]

Celkové hodnocení z tabulky (Tab.11) přeneseme do následujícího grafu (Graf 5).

[43] zdroj vlastní



Graf 5 - Celkové hodnocení bezpečnost[44]

Z analýzy provedené v této diplomové práci jsem došel tomuto pořadí a hodnocení bezpečnosti elektronického bankovnictví vybraných bank:

1) **Komerční banka 80%**
2) **Citibank 70%**
3) **Raiffeisen bank 68%**
4) **Česká spořitelna 52%**
5) **UniCredit bank 47%**

Komerční banka dosáhla výborného hodnocení především proto, že všechny analyzované částí bankovnictví dosáhly nadprůměrných výsledků. Mezi druhou Citibank a třetí Raiffeisen bank je zanedbatelný rozdíl pouhých dvou procent a obě tyto banky dosáhly uspokojivého výsledku. Česká spořitelna si drží slabý průměr na čtvrtém místě a o pět procent horší je na posledním místě UniCredit bank s podprůměrným výsledkem.

[44] zdroj vlastní

7.3 Doporučené řešení pro firmu

Z analýzy bezpečnosti pěti vybraných internetových bankovnictví jasně vyplynulo, že momentálně využívaná služba BusinessNet od Unicredit banky není v oblasti bezpečnosti vůbec uspokojivá.

Jako jediná nedosáhla ani hranice 50% a její služby proto rozhodně nemohu z hlediska bezpečnosti finančních prostředků firmě Profes Projekt s.r.o. doporučit.

I přes rozsáhlý průzkum všech bezpečnostních faktorů se internetové bankovnictví Komerční banky ukázalo jako opravdu dobře zabezpečené. Na českém trhu bychom těžko hledali lepšího kandidáta v této kategorii.

Vzhledem k této skutečnosti a výsledkům analýzy jsem se rozhodl, že firmě Profes Projekt doporučím změnu banky a tím i změnu internetového bankovnictví. Touto bankou bude tedy Komerční banka s internetovým bankovnictvím Profibanka.

7.4 Harmonogram změny

1. Červenec 2010 – schůzka s bankovním poradcem Komerční banky a domluvení podmínek
2. Červenec 2010 – Podání výpovědi UniCredit bance s výpovědní lhůtou 1 měsíc
3. Červenec 2010 – Zřízení služby Excelent s internetovým bankovnictvím Profibanka u Komerční banky
4. Srpen 2010 – Převod finančních prostředků z účtu UniCredit banky na nový účet Komerční banky přes internetové bankovnictví
5. Srpen 2010 – Definitivní zrušení účtu UniCredit banky

8 Zhodnocení návrhu

8.1 Zhodnocení z pohledu bezpečnosti

Internetové bankovnictví komerční banky vykazuje mnohem vyšší bezpečnost než dosud využívané internetové bankovnictví banky UniCredit. Prakticky ve všech dílčích parametrech analyzovaných v této práci je Profibanka o mnoho napřed než BusinessNet bankovnictví.

Obrovský rozdíl mezi původní a mnou doporučenou službou je již v bezpečnostním certifikátu. Někdo může oponovat tím, že mezi certifikáty běžně používanými nejsou znatelné bezpečnostní rozdíly. Dle mého názoru se celková bezpečnost odvíjí od dílčích složek a bankovnictví je zabezpečené jen tak, jak zabezpečený je jeho nejslabší článek. Rozdíl v úrovni certifikátů je především v rozšířeném ověřování a ochraně proti clickjackingu, které nabízí Komerční banka.

Z hlediska protokolů podporovaných jednotlivými bankami je na tom Komerční banka opět o poznání lépe, a to zejména z toho důvodu, že oba protokoly, které podporuje, jsou na dobré bezpečností úrovni. Na druhé straně UniCredit banka podporuje oba protokoly také, ale ještě navíc využívá protokolu SSL 2.0, který již v dnešní době rozhodně není bezpečný.

Jak jsem již shrnul výše, není překvapením, že Komerční banka dominuje i na poli šifrování komunikace. Využívá delší, a tedy bezpečnější veřejný klíč, a navíc je následná komunikace zašifrována vždy bezpečnou 128bitovou šifrou.

Z hlediska autentizace je dle mého názoru certifikát na čipové kartě tou nejlepší možností zabezpečení správné autentizace i autorizace. UniCredit banka ho na rozdíl od Komerční banky pro své služby nevyužívá. Bohužel nevyužívá ani certifikát v souboru, a tak jediný způsob, jak si opravdu zabezpečit vstup do elektronického bankovnictví, je pomocí nepohodlného autentizačního kalkulátoru.

Mnou doporučené internetové bankovnictví Profibanka Komerční banky je tedy mnohem lépe zabezpečené než bankovnictví BusinessNet UniCredit banky, a proto budu firmě Profes Projekt s.r.o. moje rozhodnutí bez obav prezentovat.

8.2 Ekonomické zhodnocení návrhu

Ekonomická stránka není stěžejní částí této diplomové práce, ale je nutné ověřit, zda se můj návrh na změnu internetového bankovnictví nějak výrazně nedotkne nákladů na tuto službu. Od vedení firmy jsem získal soupis přibližných měsíčních transakcí, dle kterých vypočítám celkové roční náklady a rozdíl oproti stávajícímu stavu. Tento výpočet se bude týkat jak správy internetového bankovnictví, tak i vedení samotného účtu.

8.2.1 Soupis předpokládaných transakcí

☑	Měsíční výpis z účtu	1/měsíc
☑	Vklad na přepážce	6/rok
☑	Výběr z vlastního bankomatu	1/měsíc
☑	Výběr z cizího bankomatu	4/rok
☑	Výběr v zahraničí	2/50000/rok/
☑	Platba do jiné banky	4/měsíc
☑	Odchozí platby SEPA(v EUR)	3/rok
☑	Příchozí platby SEPA(v EUR)	3/rok

8.2.2 Další faktory ovlivňující náklady

☑	Výše zůstatku účtu	cca 1500000Kč
☑	Měsíční vedení účtu	dle banky
☑	Měsíční vedení internetového bankovnictví	dle banky
☑	Výše úročení	dle banky

8.2.3 Výpočet bilance bankovního účtu

V tabulce, která následuje za textem je obsažen výpočet celkových nákladů, výnosů a celkové bilance bankovního účtu. Jednotlivé položky jsou podle soupisu předpokládaných transakcí(8.2.1) rozpočítány na celý rok provozu služby.

	Komerční banka		UniCredit bank	
	1 transakce	**ročně**	1 transakce	**ročně**
Měsíční výpis z účtu poštou	20 Kč	**240 Kč**	0 Kč	**0 Kč**
Vklad na přepážce	0 Kč	**0 Kč**	20 Kč	**120 Kč**
Výběr z vlastního bankomatu	0 Kč	**0 Kč**	0 Kč	**0 Kč**
Výběr z cizího bankomatu	35 Kč	**140 Kč**	30 Kč	**120 Kč**
Výběr v zahraničí	1% min.100Kč	**1 000 Kč**	0,5%+100Kč	**700 Kč**
Platba do jiné banky	6 Kč	**288 Kč**	0 Kč	**0 Kč**
Odchozí platby SEPA(v EUR)	195 Kč	**585 Kč**	250 Kč	**750 Kč**
Příchozí platby SEPA(v EUR)	145 Kč	**435 Kč**	200 Kč	**600 Kč**
Měsíční vedení účtu	812Kč (včetně IB)	**9 744 Kč**	1 199 Kč	**14 388 Kč**
Měsíční vedení IB	0Kč(v ceně účtu)	**0 Kč**	290 Kč	**3 480 Kč**
Náklady celkem za rok		**12 432 Kč**		**20 158 Kč**
Výše získaného úroku	0,02%	**300 Kč**	0,2%	**3 000 Kč**
Bilance bankovního účtu		**12 132 Kč**		**17 158 Kč**

Tab. 12 - Bilance bankovního účtu[45]

Dle výpočtu v tabulce(tab.12) vychází při využití doporučené služby Komerční banky **úspora ve výši 5026 Kč** a to zejména z důvodu jednotného poplatku za vedení účtu i internet bankingu na straně Komerční banky.

[45] Zdroj viz. [17] a [20]

9 Závěr

V první části diplomové práce nazvané Systémové vymezení problému jsem se zaprvé věnoval teoretickému základu elektronického obchodování v širším slova smyslu s krátkým výtahem historie. V další řadě jsem zahrnul odbornou teorii bezpečnosti elektronického obchodování, a to zejména elektronického podpisu, zabezpečeným protokolům a podobně. Dále tato část obsahuje výběr potenciálních bankovních domů, ze kterých jsem dále analyzoval ten nejvhodnější. K získání informací jsem využil knižní publikace a články vydané na internetu ale také virtuální knihovny.

V další části práce jsem rozebral současný stav řešené problematiky, představil zadavatele, firmu Profes Projekt, její historii a obchodní činnost. Dále jsem analyzoval všechny možné služby potenciálních bank, a to zejména z pohledu bezpečnosti, a provedl jejich detailní rozbor. V této části práce jsem se opíral hlavně o oficiální informace jednotlivých bank, ale také o zkušenosti a vědomosti, kterých jsem nabyl za necelých pět let studia na Fakultě podnikatelské VUT v Brně.

Ve třetí části práce jsem navrhnul řešení daného problému na základě již získaných analýz a dat. Vybral jsem jednu Komerční banku a její službu Excelent s internetovým bankovnictvím Profibanka určenou přímo pro firmu Profes Projekt a pro podobné firmy v tomto segmentu. Provedl jsem také ekonomické zhodnocení výběru produktu.

Věřím, že tato diplomová práce bude mít pro firmu Profes Projekt s.r.o. pouze kladný přínos, a že se vedení firmy již dále nebude strachovat o bezpečí svých finančních prostředků.

Seznam použitých informačních zdrojů

[1]CEED [online]. 2008 [cit. 2010-05-11]. Elektronické bankovnictví. Dostupné z WWW: <http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm>.

[2]Česká spořitelna [online]. 2008 [cit. 2010-03-16]. Program Profit. Dostupné z WWW:<http://www.csas.cz/banka/content/inet/internet/cs/Profit_program_corp.xml?category=207>.

[3]CitiBank [online]. 2009 [cit. 2010-03-16]. CitiBusiness. Dostupné z WWW: <http://www.citi.com/czech/citibusiness/czech/docs/index.htm>.

[4]Electronic Banking: The Ultimate Guide to Online Banking. SCN Education B.V. GWV-Vieweg, 2001. 400 s. ISBN 3528057548.

[5]Finance [online]. 2009 [cit. 2010-03-09]. Přímé bankovnictví. Dostupné z WWW: <http://www.finance.cz/bankovnictvi/informace/bezne-ucty/prime-bankovnictvi/>.

[6]GALDA, Marek. *PŘÍMÉ BANKOVNICTVÍ – SROVNÁNÍ VYBRANÝCH BANK* [online]. Brno, 2007. 56 s. Bakalářská práce. Masarykova Univerzita, Ekonomicko-správní fakulta. Dostupné z WWW: <http://is.muni.cz/th/100339/esf_b/BP_Galda__prime_bankovnictvi_-_porovnani_vybranych_bank.pdf>.

[7]Ibm.com [online]. 2005 [cit. 2010-05-12]. Phishing and Internet Banking Security. Dostupné z WWW: <ftp://ftp.software.ibm.com/software/tivoli/whitepapers/Phishing_and_Internet_Banking_Security.pdf>.

[8]JELÍNKOVÁ, Lenka. *Bibliografický popis elektronických online zdrojů v zahraniční a domácí katalogizační praxi*[online]. Praha, 2006. 103 s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta. Dostupné z WWW: <http://www.webarchiv.cz/files/dokumenty/ostatni/DPjelinkova2006.pdf>.

[9]Komerční banka [online]. 2006 [cit. 2010-05-12]. Desatero bezpečnosti. Dostupné z WWW: <http://www.mojebanka.cz/cs/security.shtml>.

[10]Komerční banka [online]. 2006 [cit. 2010-02-25]. Profibanka. Dostupné z WWW: <http://www.kb.cz/cs/seg/seg4/products/profibanka.shtml>.

[11]Komerční banka [online]. 2006 [cit. 2010-03-16]. Excelent. Dostupné z WWW: <http://www.kb.cz/cs/seg/seg3/products/excelent_package.shtml>.

[12]LANCE, James. Phishing bez záhad. 2007. 281 s. ISBN 978-80-247-1766-1.

[13]Marketingové noviny [online]. 2006 [cit. 2010-05-11]. Historie elektronických obchodů. Dostupné z WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4391>.

[14]MARVANOVÁ, M, SCHLOSSBERGER, O a kol.: Platební styk, 2. dopl. vyd.. Praha : Bankovní institute, 1998. 376 s.

[15]Měšec [online]. 2008 [cit. 2010-03-09]. Platební karty. Dostupné z WWW: <http://www.mesec.cz/bankovni-ucty/platebni-karty/pruvodce/>.

[16]MLÝNEK, Jaroslav. Zabezpečení obchodních informací. 2007. 154 s.
ISBN 978-80-251-1511-4.

[17]PEKÁRKOVÁ, Lucie. MOŽNOSTI ROZVOJE PŘÍMÉHO BANKOVNICTVÍ. Brno, 2008. 54 s. Bakalářská práce. Masarykova Univerzita, Ekonomicko-správní fakulta.

[18]PIPER, Frederic. Kryprografie. 2006. 157 s. ISBN 80-7363-074-5.

[19]Přírodovědecká fakulta, Univerzita Karlova [online]. 2004 [cit. 2010-05-13]. Bezpečné vybírání elektronické pošty. Dostupné z WWW: <http://web.natur.cuni.cz/~kuda/howtos/ssh.html>.

[20]Raiffeisen Bank [online]. 2008 [cit. 2010-03-16]. Podnikatelské eKonto. Dostupné z WWW: <http://www.rb.cz/firemni-finance/podnikatele-a-male-firmy/podnikatelske-ucty/bezne-ucty/podnikatelske-ekonto/>.

[21]RENNÉT, Jiří. Návrh univerzální počítačové sítě pro Profes Projekt spol. s.r.o.. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2008. 54 s. Vedoucí diplomové práce Ing. Viktor Ondrák Ph.D.

[22]RYLKOVÁ, Lucie. *POROVNÁNÍ PODMÍNEK PRO VEDENÍ A ZŘIZOVÁNÍ ÚČTŮ* [online]. Brno, 2009. 79 s. Diplomová práce. Masarykova Univerzita, Ekonomicko-správní fakulta. Dostupné z WWW: <http://is.muni.cz/th/62874/esf_m/Diplomova_prace.pdf>.

[23]SEDLEK, Ji. E-komerce, internet a mobil marketing od A do Z . 2006. 351 s. ISBN 80-7300-195-0.

[24]ŠVADLENKA, Libor. Elektronické obchodování. 2007. 163 s. ISBN 978-80-86530-40-6.

[25]UniCredit Bank [online]. 2009 [cit. 2010-03-16]. Business Konto. Dostupné z WWW: <http://www.unicreditbank.cz/cz/podnikatele/ucty/bussines-konto.html>.

[26]UniCredit Bank [online]. 2009 [cit. 2010-03-16]. Businessnet. Dostupné z WWW: <http://www.unicreditbank.cz/cz/podnikatele/prime-bankovnictvi/businessnet.html>.

[27]WELCH, Brian. Electronic Banking and Treasury Security. 2nd edition. CRC Press, 1999. 304 s. ISBN 0849305292.

[28]Wikipedia [online]. 2010 [cit. 2010-05-13]. Serure Shell. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Secure_Shell>.

[29]Wikipedia [online]. 2010 [cit. 2010-04-20]. Transport Layer Security. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Transport_Layer_Security>.

Seznam zkratek a pojmů

CD	- Compact Disk (optický disk k ukládání dat)
DNS	-Domain Name Server (převádí doménová jména na IP adresy)
EV	-Extended Validation (pokročilé ověřování bezpečnostních certifikátů)
SGC	-Server Gated Cryprography (umožňuje starším prohlížečům využít silnější způsoby šifrování)
GSM	-Groupe Spécial Mobile (standart pro mobilní telefonování)
HTML	-HyperText Markup Language (programovací jazyk webových stránek)
HTTP	-HyperText Transfer Protocol (internetový protokol určený pro výměnu hypertextových dokumentů)
HTTPS	- (viz. HTTP, ale přenášená data jsou šifrována pomocí SSL nebo TLS)
IP adresa	-Internet Protokol Adress (jednoznačně definuje síťové rozhraní)
MAC	-Media Access Kontrol (identifikátor síťového zařízení)
PIN	-Personal Identification Numer (identifikátor pro platby, mobilní tel. atd.)
RSA	-Rivest, Shamir, Aleman (šifra s veřejným klíčem)
SEPA	-Single Euro Payment Area (iniciativa sjednocující platby v rámci EU)
SHA1	-Secure Hash Algorythm (zajišťuje hašování v kryptografii)
SSH	-Secure Shell (zabezpečený protokol pro přenos dat)
SSL	-Secure Sockets Layer (zajišťuje komunikaci šifrováním i autentizací)
TLS	-Transport Layer Security (nástupce protokolu SSL)

Rejstřík

A

Autentičnost dat 27
Autentizace 9, 26, 49, 51, 58
Autentizační kalkulátor 24, 50, 58
Autorizace 26

B

Bankomat 20
Bankovnictví ... 8, 10, 11, 12, 14, 15, 16, 18, 19, 21, 23, 24, 25, 26, 29, 30, 31, 32, 33, 34, 35, 36, 40, 44, 49, 50, 51, 52, 53, 54, 55, 58, 59, 61, 62, 63, 64, 67
Bezpečnost 8, 11, 26, 53, 54, 55, 59, 60

C

Certifikační autorita ... 41, 42, 53
Certifikát 37, 43, 50, 58
ClickJacking 44

Č

Čipová karta 9, 51, 52, 58

D

Délka klíče 47, 56
DNS server 39
Důvěrnost dat 27

E

E-banking 12, 15, 31
Elektronické obchodování 10

G

GSM banking 8, 23, 25

H

Hacker 29, 44
Hašování 28
Heslo 9, 26, 49, 58
Hypertextový odkaz 36

I

Identifikace 9, 27, 41
Integrita dat 27
Internet ... 8, 10, 19, 24, 25, 26, 27, 34, 35, 36, 38, 65, 67, 70

K

Klíč 46
Klient 11, 23, 29, 45, 47, 51
Komunikace ... 11, 31, 45, 47, 59
Konto 35, 69
Kryptografie 27

N

Nepopiratelnost 27

O

Ověřování 43, 54

P

Phishing 9, 36, 37, 38, 39, 67
Platební karta 22, 26
Platební příkaz 11
Platnost certifikátu 42, 50, 53
Podpisový algoritmus 47
Protokoly 8, 29, 44, 46, 63

R

Rozšířené ověřování 43

S

Síla šifry 9, 48
SMS Tookit 9, 23, 51
SSL 29, 31, 40, 41, 43, 44, 45, 46, 55, 63, 70

Š

Šifrování 9, 25, 27, 28, 29, 41, 43, 46, 47, 55, 56, 57, 59, 60,

U

Útok 29, 36
Uživatel ... 26, 31, 36, 39, 40, 41, 51, 52

Z

Zabezpečení 8, 14, 16, 22, 29, 31, 32, 36, 37, 42, 43, 59, 63

Přílohy

Příloha č.1	WWW stránky Profes Projekt spol.s.r.o.
Příloha č.2	Sazebník přímého bankovnictví Komerční banky
Příloha č.3	Sazebník internetového bankovnictví UniCredit bank
Příloha č.4	Rozhraní internetového bankovnictví Komerční banky
Příloha č.5	Princip plateb SEPA
Příloha č.6	Přístup do internetového bankovnictví České spořitelny
Příloha č.7	Rozhraní internet bankingu Servis24 – Česká Spořitelna
Příloha č.8	Základní informace – Komerční banka

Příloha č.1 WWW stránky Profes Projekt spol.s.r.o.

2. Sazebník přímého bankovnictví Komerční banky

Přímé bankovnictví

Služby přímého bankovnictví

	Expresní linka	Expresní linka Plus	Mojebanka	Mojebanka + Přímý kanál	Profibanka	Mobilní banka
Měsíční vedení	170,–	zdarma	170,–	290,–	290,–	19,–
Oprávnění pro první zmocněnou osobu	zdarma					–
Oprávnění pro druhou a každou další zmocněnou osobu	75,–	zdarma	75,–	75,–	75,–	–

Odeslání vyžádaných oznámení

	Prostřednictvím e-mailové zprávy	Prostřednictvím SMS zprávy	SMS zprávy vyžádané prostřednictvím automatizovaného hlasového systému	Prostřednictvím faxové zprávy
Odeslání oznámení	zdarma	2,50	2,50[1)]	5,–

[1)] Cena za vyžádanou transakční historii je 0,50 Kč za jednu SMS.

Další služby k přímému bankovnictví

Expresní linka KB

EL KB v rámci balíčku MUNICIPALITY	1. rok zdarma vč. zmocněných osob a jednorázového poplatku za zmocnění
Zřízení zmocnění pro Expresní linku KB	200,–
Úprava ve stávajícím zmocnění na EL KB	30,–

Zaslání minivýpisu a ostatní korespondence na vyžádání klienta EL KB z telefonního centra KB

Elektronickou poštou nebo faxem	zdarma
Listovní zásilkou	35,–
Opětovné zaslání PIN	160,–

Expresní linka Plus

Zřízení zmocnění pro Expresní linku Plus[1)]	200,–

[1)] Pokud klient vlastní EL KB a zároveň EL Plus, poplatek za zřízení zmocnění není u EL Plus účtován.

>> Mojebanka

Internetové bankovnictví Mojebanka v rámci balíčku MUNICIPALITY Internetové bankovnictví Mojebanka se službou Přímý kanál v rámci balíčku MUNICIPALITY	1. rok zdarma včetně zmocněných osob
Zpracování příkazu k administraci předaného na papírovém nosiči	100,–
První příkaz k administraci po zřízení služby přímého bankovnictví není zpoplatněn.	
Zpracování příkazu k administraci prostřednictvím systémů přímého bankovnictví	zdarma

>> Profibanka

Zřízení PC bankovnictví Profibanka	3 000,–
PC bankovnictví Profibanka v rámci balíčku MUNICIPALITY	zřízení zdarma
Zřízení PC bankovnictví Profibanka v rámci Optimum Medicum	sleva 50 %
Zřízení PC bankovnictví Profibanka pro více subjektů se společným statutárním zástupcem či majitelem	5 000,–
PC bankovnictví Profibanka v rámci balíčku MUNICIPALITY	1. rok zdarma včetně zmocněných osob
PC bankovnictví Profibanka pro členy statutárního orgánu a majitele firem, které využívají Profibanku, vč. zřízení služby a oprávnění pro zmocněné osoby	zdarma

>> Zabezpeční služeb přímého bankovnictví

Vydání nebo opětovné vystavení osobního certifikátu pro služby přímého bankovnictví	zdarma
Vydání nebo opětovné vystavení firemního certifikátu (platí pro službu Přímý kanál)	zdarma
Vydání čipové karty Můjklíč	390,–
Vydání čtečky čipových karet	250,– + 20 % DPH
Vydání kompletu čtečka a čipová karta Můjklíč	640,–
Vydání karty optického klíče	1 000,–
Blokace nebo odblokování karty optického klíče	zdarma

>> eTrading

Zřízení služby eTrading	zdarma
Používání služby eTrading	zdarma

Servisní služby pro přímé bankovnictví[1)]

Provedení instalace a zprovoznění libovolné aplikace nebo kombinace aplikací přímého bankovnictví na jednom počítači klienta (včetně výjezdu) na území ČR	2 400,– + 20 % DPH
Provedení instalace a zprovoznění libovolné aplikace nebo kombinace aplikací přímého bankovnictví na druhém a dalším počítači klienta v rámci jednoho výjezdu (místa) na území ČR	1 900,– + 20 % DPH
Servisní zásah – expresní do 6 hodin od jeho objednání klientem (odstranění závady, reinstalace, zprovoznění aplikace) pro libovolné aplikace přímého bankovnictví na území ČR (pouze při objednání v požadovaný pracovní den do 12.00 hod.)	2 700,– + 20 % DPH
Servisní zásah do 24 hodin od jeho objednání klientem (odstranění závady, reinstalace, zprovoznění aplikace) pro libovolné aplikace přímého bankovnictví na území ČR (pouze v pracovní dny)	2 200,– + 20 % DPH

Ceny jsou platné pro případy, kdy uvedené servisní služby zajišťuje externí subdodavatel, se kterým má KB pro takové výkony uzavřen smluvní vztah.

V ceně instalace libovolné aplikace nebo kombinace aplikací přímého bankovnictví jsou zahrnuty cestovní náklady a částka za instalaci a zprovoznění aplikace nebo kombinace aplikací přímého bankovnictví na jedné stanici klienta.

Ceny za instalace aplikací přímého bankovnictví zahrnují rovněž případnou instalaci čtecího zařízení pro čipové karty, ale pouze v případě, pokud byla objednána současně s instalací této aplikace.

V případě výjezdu do zahraničí za účelem instalace, odstranění závady, reinstalace a poradenství je cena stanovena individuálně dle skutečných prokazatelných nákladů.

MojePlatba

Zřízení služby MojePlatba	zdarma
Měsíční vedení služby[1)]	zdarma
Měsíční poplatek z objemu transakcí	individuálně

[1)] Platí pro klienty s běžným účtem vedeným u KB, ostatní individuálně.

TF Online

Zřízení služby TF Online	zdarma
Používání služby TF Online	zdarma

Příloha č.3 Sazebník internetového bankovnictví UniCredit bank

7.1. Online Banking - internetové bankovnictví

Zřízení produktu	bez poplatku
Poplatek za užívání produktu	140 Kč měsíčně
Zrušení produktu	bez poplatku

7.2. BusinessNet Basic - internetové bankovnictví

Zřízení produktu	500 Kč
Definice strukturovaných podpisových oprávnění	1 500 Kč
Poplatek za užívání produktu	290 Kč měsíčně
Servisní zásah, školení, konzultace prováděné pracovníkem banky	1 000 Kč + 250 Kč za každých započatých 15 min. + 20 % DPH
Zrušení produktu	bez poplatku

7.3. BusinessNet Professional - internetové bankovnictví

Zřízení produktu včetně definice strukturovaných podpisových oprávnění	3 000 Kč
Poplatek za užívání produktu	600 Kč měsíčně
Servisní zásah, školení, konzultace prováděné pracovníkem banky	1 000 Kč + 250 Kč za každých započatých 15 min. + 20 % DPH
Zrušení produktu	bez poplatku

7.4. Business Linka - telefonické bankovnictví

Zřízení produktu	bez poplatku
Poplatek za užívání produktu	140 Kč měsíčně
Zrušení produktu	bez poplatku

7.5. GSM Banking - mobilní bankovnictví

Zřízení produktu	bez poplatku
Poplatek za užívání produktu	140 Kč měsíčně
Zasílání bankovních SMS zpráv	2,90 Kč
Zrušení produktu	bez poplatku

7.6. Smart Banking - mobilní bankovnictví vyšší generace

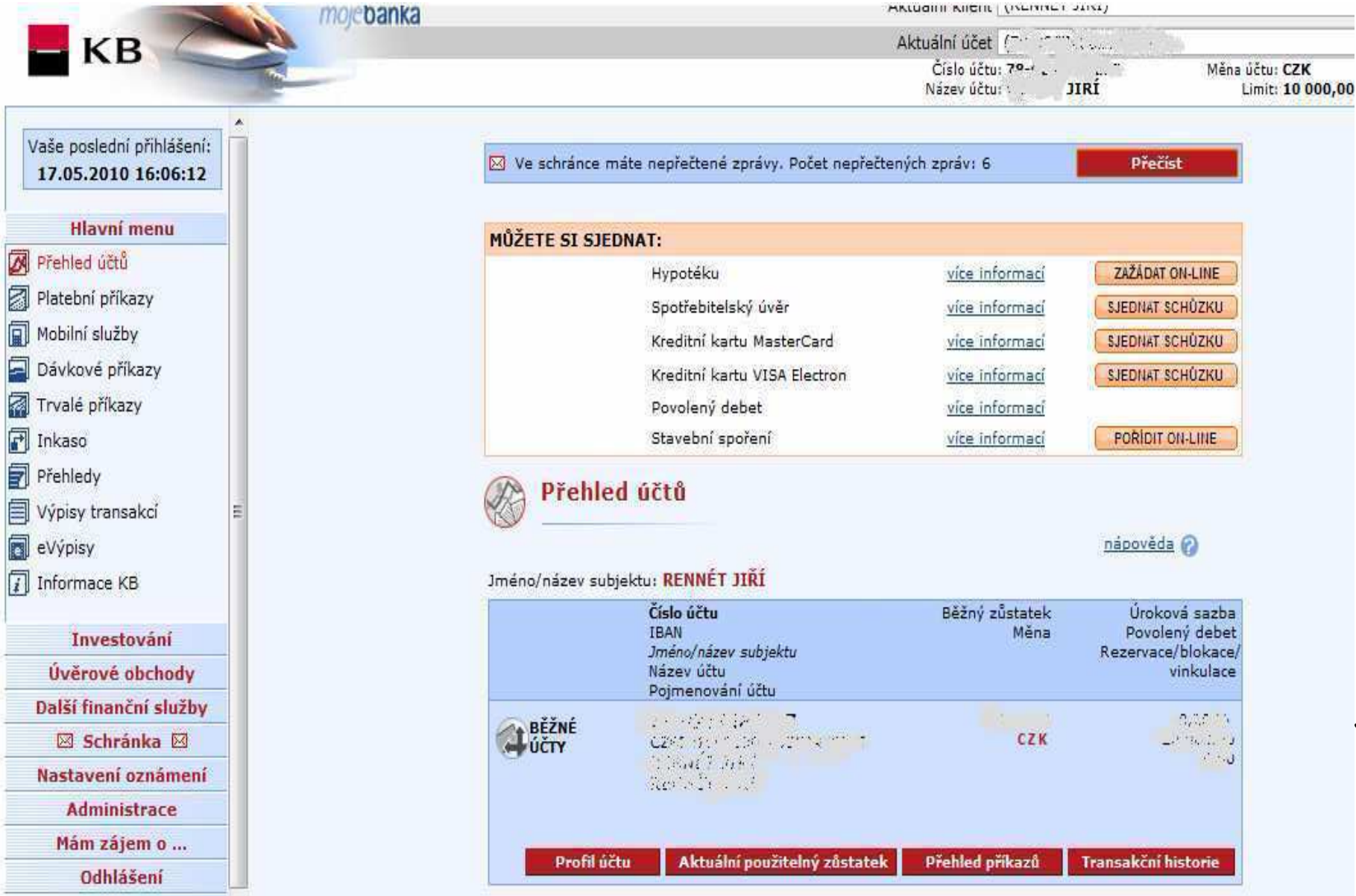
Zřízení produktu	bez poplatku
Poplatek za užívání produktu	140 Kč měsíčně
Zrušení produktu	bez poplatku

7.7. Zasílání informací

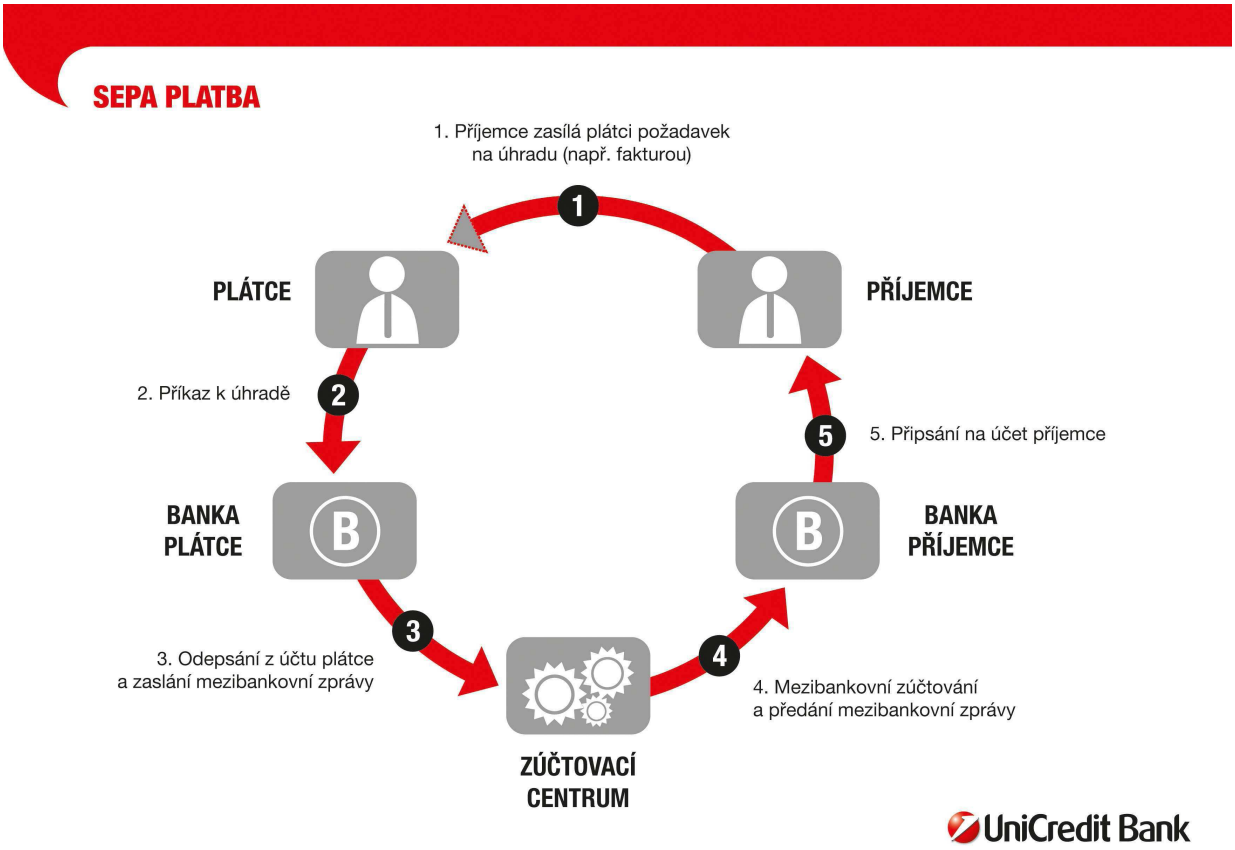
Zřízení produktu	bez poplatku
Poplatek za užívání produktu	bez poplatku
Zaslání SMS zprávy	2,90 Kč
Zaslání e-mailové zprávy	bez poplatku
Zrušení produktu	bez poplatku

Příloha č.4

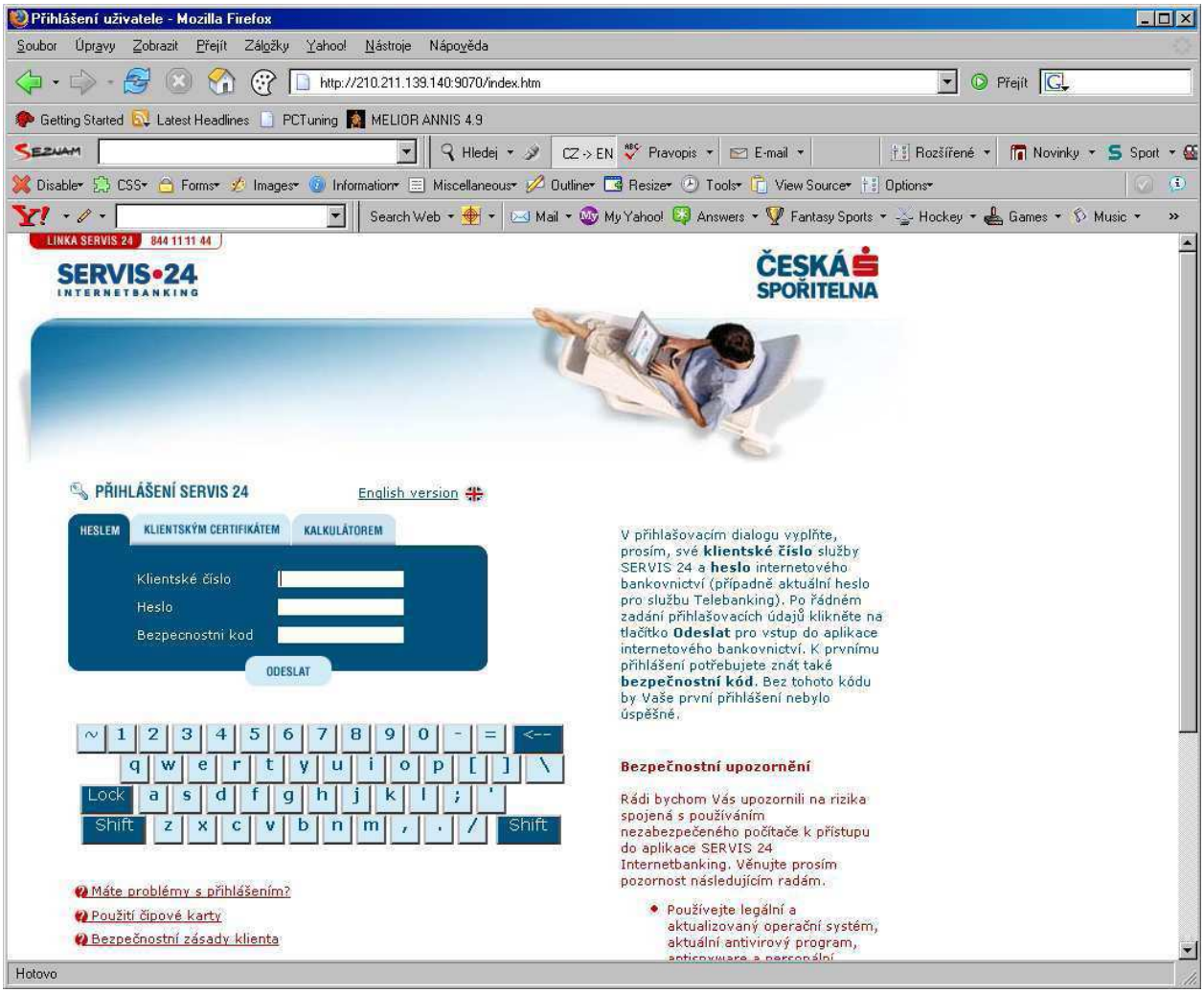
Rozhraní internetového bankovnictví Komerční banky



Příloha č.5 Princip plateb SEPA



Příloha č.6 Přístup do internetového bankovnictví České spořitelny



Příloha č.7 Rozhraní internet bankingu Servis24 – Česká Spořitelna

Profil

Profil - Základní informace

Komerční banka, a.s. (dále také "KB" nebo "Banka") je mateřská společnost Skupiny KB (dále také "Skupina"), která je tvořena devíti společnostmi. KB je také součástí mezinárodní skupiny Société Générale. Komerční banka patří mezi přední bankovní instituce v České republice a v regionu střední a východní Evropy. KB je univerzální bankou se širokou nabídkou služeb v oblasti retailového, podnikového a investičního bankovnictví. Společnosti finanční skupiny Komerční banky nabízejí další specializované služby, mezi které patří penzijní připojištění, stavební spoření, faktoring, spotřebitelské úvěry a pojištění, dostupné prostřednictvím sítě poboček KB, přímého bankovnictví a vlastní distribuční sítě.

Komerční banka a Skupina KB v roce 2009

Služby samotné Komerční banky využívalo téměř 1,62 milionu zákazníků prostřednictvím 398 poboček a 685 bankomatů po celé České republice a také telefonního, internetového a mobilního bankovnictví. V rámci pobočkové sítě Banka vybudovala 20 specializovaných business center pro střední podniky a municipality a 4 centra pro velké podniky.

Modrá pyramida stavební spořitelna, a.s. (dále "Modrá pyramida") obsluhovala 720 tisíc klientů a Penzijní fond KB registroval 498 tisíc účastníků penzijního připojištění. Počet aktivních klientů společnosti spotřebitelského financování ESSOX narostl na 312 tisíc. Na slovenském bankovním trhu působila Skupina prostřednictvím Komerční banky Bratislava.

Průměrný počet zaměstnanců Skupiny KB během roku 2009 činil 8 815.

Kreditní rating Komerční banky odráží kapitálovou sílu, výbornou likviditu a její zdravé hospodaření. Na konci roku 2009 měla Komerční banka dlouhodobý rating A1 v cizí i v domácí měně od Moody's Investors Service, A od Standard & Poor's a A od Fitch Ratings. Penzijní fond KB měl v národní ratingové stupnici od Moody's Investors Service stupeň Aa1.cz, což je nejvyšší možný rating pro penzijní fondy v České republice.

Historie

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

Skupina Société Générale

Komerční banka je součástí skupiny Societě Générale od října 2001. Skupina Societě Générale je jednou z největších finančních skupin v eurozóně. Skupina SG zaměstnává na celém světě 157 tisíc lidí ve třech klíčových oblastech:

- retailové bankovnictví, specializované financování a pojištění: Société Générale obsluhuje více než 32 milionů zákazníků na celém světě.
- privátní bankovnictví, globální investiční management a služby: Ke konci roku 2009 byla Société Générale jednou z největších bank v eurozóně podle aktiv v custody (3 073 miliardy EUR) a ve správě (344 miliardy EUR).
- Podnikové a investiční bankovnictví: Société Générale vytváří řešení pro své klienty ze všech sektorů s využitím celosvětových znalostí a zkušeností v investičním bankovnictví, globálních financích a globálních trzích.

Société Générale je součástí indexů společensky odpovědného investování: FTSE4Good a ASPI.

Komerční banka je důležitou součástí retailového bankovnictví skupiny Société Générale.