Univerzita Pardubice
Fakulta ekonomicko-správní

Bezpečnost v elektronickém bankovnictví

Martin Flamík

Bakalářská práce
2010

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2009/2010**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin FLAMÍK**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Informační a bezpečnostní systémy**

Název tématu: **Bezpečnost v elektronickém bankovnictví**

Zásady pro vypracování:

Historie a vývoj e-bakovnictví.
Přehled služeb u vybraných bankovních institucí a jejich porovnání.
Druhy zabezpečení určitých operací a citlivých dat v e-bankovnictví.
Porovnání zabezpečení u vybraných bankovních institucí.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] **HEFFERNAN, Shelagh A.. Modern banking. 1st edition. Chichester : John Wiley & Sons, 2005. 716 s., tabulky, grafy. ISBN 0-470-09500-8.**

[2] **KALA, J., PŘÁDKA, M.. Elektronické bankovnictví : Rady a tipy. 1. vyd. Praha : Computer Press, a.s., 2000. 166 s. ISBN: 80-7226-328-5.**

[3] **DOUCEK, P., NOVÁK, L., SVATÁ, V.. Řízení bezpečnosti informací. 1. vyd. Praha : Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.**

[4] **DOSTÁLEK, L., et al. Velký průvodce protokoly TCP/IP : Bezpečnost. 2. vyd. Praha : Computer Press, a.s., 2003. 592 s. ISBN 80-7226-849-X.**

Vedoucí bakalářské práce: **Ing. Jana Filipová**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **5. října 2009**

Termín odevzdání bakalářské práce: **30. dubna 2010**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne: 20. 4. 2010

Martin Flamík

Poděkování:

Touto cestou bych rád poděkoval své vedoucí bakalářské práce paní Ing. Janě Filipové, za její cenné připomínky, rady a poznatky nejen k obsahu, ale i k formální stránce této práce. Bez těchto cenných informací by nemohla tato práce vzniknout.

ANOTACE

Tato práce se zabývá elektronickým bankovnictvím, nejen jeho historií, ale i postupným vývojem až do současnosti. Dále jsou zde popsány komunikační kanály mezi bankou a klientem, které jsou analyzovány z finančního hlediska u vybraných bankovních institucí. Převážná část práce je zaměřena na bezpečnost v elektronickém bankovnictví. Obsahuje také analýzu bezpečnosti elektronického bankovnictví u vybraných bankovních institucí.

KLÍČOVÁ SLOVA

elektronické bankovnictví, bezpečnost, šifrování, autorizace, autentizace

TITLE

Security in electronic banking

ANNOTATION

This work deals with the electronic banking, not only with history, but also with the gradual development up to the present. There are further described the communication channels between banks and customers which are analyzed from a financial point of view of the selected banking institutions. Most of the work is focused on security of electronic banking. It also includes a security analysis of electronic banking in the selected banking institutions.

KEYWORDS

electronic banking, security, encryption, authorization, authentication

OBSAH

ÚVOD

Již několik desítek let určuje vývoj elektroniky a komunikačních systémů směr nejen samotného obchodování, ale i bankovních systémů s tím spjatých. Dynamický rozvoj internetu, mobilních telefonů, osobních počítačů a mnoho dalších informačních technologií nutí všechny obchodníky bez ohledu na zaměření a druh produkce, vstoupit na elektronický trh, bez kterého není v dnešní době možné obstát v konkurenčním boji. Tím umožňují svým potencionálním zákazníkům rychlé, nízkonákladové objednání požadovaného produktu. Proto, aby mohlo dojít i k rychlému zaplacení, je zapotřebí i okamžitý přístup k bankovnímu účtu a transakčním operacím. To případnému zákazníkovi umožňuje elektronické bankovnictví.

Většina z nás již uvítala možnosti internetu a počítačů jako obchodní příležitosti, ať už z pohledu prodávajícího nebo kupujícího. V několika málo minutách vyhledat požadovaný produkt, dozvědět se o něm potřebné informace a ještě k tomu porovnat ceny u desítky dalších prodejců a to z pohodlí svého domova či kanceláře. Bylo by možné jmenovat další a další pozitiva tohoto poměrně nového a rychle se rozvíjejícího se tržního mechanismu. Nemalé procento lidí si však také uvědomuje a obává se možného zneužití tohoto komunikačního rozhraní a to hlavně při zadávání citlivých informací pro případnou bezhotovostní platbu. Proto je i jedním z cílů této práce seznámit tuto populaci se zabezpečením elektronického bankovnictví a elektronické komunikace všeobecně.

Jedním z hlavních důvodů, proč jsem si zvolil téma zabezpečení u elektronického bankovnictví, bylo nejen rozšířit si doposavad získané znalosti bezpečnostních prvků a forem zabezpečení, ale také analýza současně nabízených bezpečnostních opatření u vybraných bankovních institucí. Byla snaha vybrat takové instituce, které pokrývají převážnou většinu bankovního trhu v České republice. Od těch největších až po nedávno vzniklé či nízkonákladové.

V první části bakalářské práce jsou nejprve vysvětleny základní pojmy využívané ve spojení s elektronickým bankovnictvím. Je zde také popsán vývoj elektronického bankovnictví. A to od samotného počátku vzniku bezhotovostní platby pomocí karet, přes využití prvních bankomatů až po využívání nynějších bankovních technologiích.

Ve druhé kapitole analyzuji stávající možnosti komunikace s vybranými bankovními institucemi a vyhodnocuji jejich nákladovost z pohledu pořízení poskytované služby a z pohledu poplatků za vedení bankovní služby.

Ve třetí kapitole se zabývám již samotnými bezpečnostními prvky a aspekty elektronické komunikace mezi bankou a klientem. Jsou zde popsány základní principy šifrování dat, elektronického podpisu, principy autentizace a autorizace a také další bezpečnostní prvky využívané v elektronickém bankovnictví.
Poslední kapitola je tvořena praktickým srovnáním bankovních institucí v zabezpečení nejpoužívanějšího elektronického bankovnictví - internetového. V této kapitole jsem využil znalosti o více-kriteriálních rozhodovacích procesech získané studiem. Porovnány byly bezpečností prvky autentizace a autorizace na straně klienta, jelikož se jedná, oproti zabezpečení samotného bankovního systému v bance, o nejkritičtější část komunikačního kanálu a to z důvodu zásahu lidského faktoru.
Tato práce není úplným přehledem bezpečnostních prvků v oblasti elektronického bankovnictví, protože to ani není vzhledem ke stanovenému rozsahu bakalářské práce možné. Měla by sloužit hlavně klientům využívající elektronické bankovnictví jako zdroj aktuálních, teoretických i praktických znalostí spojených s bezpečností v elektronickém bankovnictví.

Cíle této bakalářské práce:

- historie a vývoj elektronického bankovnictví;
- přehled služeb u vybraných bankovních institucí a jejich porovnání;
- popsání druhů zabezpečení určitých operací a citlivých dat v elektronickém bankovnictví;
- porovnání zabezpečení u vybraných bankovních institucí.

1. HISTORIE A VÝVOJ ELEKTRONICKÉHO BANKOVNICTVÍ

Aby bylo možné používat v následující práci pojem elektronické bankovnictví, je zapotřebí si nejprve objasnit, co vlastně tento pojem znamená. V dnešním medializovaném světě je pojem elektronické bankovnictví často používaným termínem a to i v anglickém znění, čili e-banking. Navzdory tomu však bývá mylně zaměňován s anglickými výrazy e-commerce a e-business. Proto je důležité nejprve vysvětlit rozdíl mezi uvedenými výrazy a poté již bude následovat samotný vývoj elektronického bankovnictví nejen v zahraničí, ale i v ČR.

1.1. Vysvětlení základních pojmů

Z pohledu hierarchického členění by byl výraz **e-business** na prvním místě. E-business v překladu znamená elektronické podnikání, je hlavním představitelem tzv. „nové ekonomiky“, související především s rozvojem internetu a telekomunikací [11]. Většina lidí si pod pojmem e-business představí pouze internetové obchody a rezervační systémy u cestovních agentur či v kulturních zařízeních. Pod toto označení ovšem nespadá pouze elektronické obchodování, ale i mnoho dalších odvětví, jejichž cílem je podpora a zvýšení efektivity podnikových procesů. Pojem e-business tedy zahrnuje nespočet obchodních procesů jako: management zásobování, zpracovávání objednávek, elektronické nakupování, vztahy se zákazníky, zákaznický servis, využívání ERP[1] systémů, využití EDI[2] a EDIFACT[3] a mnoho dalších [16].

E-commerce (elektronická komerce, elektronický obchod) je podmnožinou e-businessu. Pokud by byl tento pojem brán z obecného hlediska, tak lze pod daný termín zahrnout jakékoliv webové stránky, které nabízejí výrobky, služby či jiné produkty a zároveň tyto stránky umožňují i jejich objednávku. E-commerce je také pojem používaný k označení veškerých obchodních operací, při kterých se využívá elektronických komunikačních kanálů. Hlavním charakteristickým prvkem jsou především internetové obchody i elektronické bankovnictví a s nimi související problematika. Patří sem i většina činností spadajících pod elektronický marketing (např. e-mail marketing, online reklama a všechny možné aktivity podporující internetové obchodování) [12].

[1] ERP systém (Enterprise Resource Planning) - informační systém, pomocí kterého se řeší plánování a řízení podnikových procesů a je prostředkem ke zvýšení efektivity podnikových procesů.
[2] EDI (Electronic Data Interchang) - jedná se o strukturovaný standard přenosu dat mezi organizacemi v elektronické podobě.
[3] EDIFACT (Electronic Data Interchange For Administration, Commerce, and Transport) - elektronická výměna dat pro správu, obchod a dopravu založený na EDI standardu. Byl vyvinutý v rámci Organizace spojených národů.

E-banking (elektronické bankovnictví) je podmnožinou e-commerce (B2C[4]) [6]. Pojem elektronické bankovnictví (označované také jako přímé) je výraz, jímž je označována elektronická komunikace mezi bankou a klientem. Klient banky provádí požadované finanční operace ze svého komunikačního zařízení nebo jiného technického zařízení a to prostřednictvím moderních komunikačních kanálů. To znamená, že klient nemusí navštěvovat pobočku banky kvůli každému bankovnímu požadavku, ale převážnou většinu úkonů si může uživatel obstarat a vyřídit z pohodlí domova, kanceláře či kdekoli jinde.

Druhů a typů elektronického bankovnictví je několik, je tedy možné přistupovat ke svým bankovním účtům a provádět platební operace mnoha způsoby. V současné době se pro tuto elektronickou komunikaci, mezi finančním sektorem a klientem, využívá především technologická rozhraní jako internet a to pomocí Internet-banking (internetové bankovnictví), dále bankovnictví přes specializovaný software na PC (Home-banking) a GSM[5]-banking (využití mobilního telefonu jako komunikačního rozhraní) či Phone-banking (komunikace přes telefon buď s automatickým telefonním systémem či telefonním bankéřem), v poslední době velmi oblíbený PDA-banking (komunikace prostřednictvím PDA[6]). V blízké budoucnosti se dá předpokládat rozšíření o další mobilní rozhraní a také rozšíření o interaktivní televize. Od tohoto nově zavedeného komunikačního rozhranní se očekává ještě větší zalíbení něž u stávajícího internetového bankovnictví. To by mělo zajistit ještě flexibilnější, otevřenější samoobslužné spojení s bankou, kterým klient může naplňovat své každodenní potřeby, ať už se jedná o bankovní služby či informace o jeho financích na účtu.

1.2. Vývoj elektronického bankovnictví

Z historického hlediska je elektronické bankovnictví poměrně novým typem bankovnictví. Navzdory tomu se však velmi rychle vyvíjí a to ruku v ruce s technickým vývojem počítačů, mobilních telefonů a elektroniky všeobecně.

Za samotný počátek elektronického bankovnictví lze považovat vznik debetních platebních karet. První platební karta byla vydána v roce 1914 firmou Western Union Telegraph Company. Byla vyrobená z plechu a umožňovala zákazníkům telefonovat a zasílat telegramy bez okamžitého placení. Zákazník poté ke konci měsíce obdržel výpis telefonátů a telegramů, jejich individuální ceny a celkový součet. Tuto „fakturu“ poté zaplatil šekem nebo příkazem z banky. Společnost se tímto krokem snažila udržet své nejlepší zákazníky a přimět je

[4] B2C - Business to Customers je jedna z forem E-commerce.
[5] GSM (Global System for Mobile Communications) - v původním francouzském znění „Groupe Spécial Mobile“. Jedná se o nejpoužívanější komunikační standard využívaný u mobilních telefonů.
[6] PDA (Personal Digital Assistant) - osobní digitální pomocník, bývá často v češtině překládán jako kapesní počítač.

k častějšímu využívání služeb s bezhotovostní platbou. Proto se tyto karty často nazývají věrnostní platební karty. [8, 30]

První „univerzální“ platební karta byla uvedena na trh v roce 1950, kdy společnost Diners Club International vydala platební kartu 200 vybraným klientům. Tyto úvěrové karty nazvané Charge Card umožňovaly majitelům karet bezhotovostní placení ve vybraných restauracích, hotelech a obchodech, které měly s klubem uzavřenou smlouvu. Avšak první bankovní platební karta se objevila o rok později a to roku 1951 u The Franklin National Bank of New Yorku. Tato karta byla vydávána zdarma nejdůvěryhodnějším klientům a obchodníci platili bance poplatky za uskutečněné transakce. Při použití této platební karty stačilo zákazníkovi předložit identifikační kartu a podepsat účet. Prodávající ověřil, zda se podpis kupujícího shoduje se vzorem na kartě. Později přibyla ještě kontrola, zda předložená karta není na seznamu zablokovaných karet. Ovšem jak zpracování faktury, tak kontrola se seznamem zablokovaných karet zprvu probíhala bez pomoci výpočetní techniky. Klienti poté museli došlé vyúčtování uhradit do 30, 60 nebo 90 dnů. Vydávání těchto karet však bylo dosti nákladné a nepřinášelo bance očekávaný zisk. Z toho důvodu bylo jejich vydávání pozastaveno. V roce 1958 se objevila další banka, jež začala vydávat platební karty a to Bank of America. Karty byly poprvé v historii vyrobeny z plastu, díky tomu bylo umožněno placení pomocí imprinterů[7]. V roce 1966 umožnila tato banka využívat tento patentový systém platby i ostatním americkým bankám a jedné z anglických bank, odkud se platební karty rozšířily dále po Evropě. [8, 30]

Banky se tím pádem staly jedním z nejvýznamnějších zákazníků u výrobců počítačů a elektronických komunikačních zařízení. Tato, v té době, drahá technika byla z počátku využita pouze pro vnitřní systémy bank. Následně se však objevily první bankomaty. První ATM[8] navrhl a postavil Luther George Simjian. Ten byl nainstalován již v roce 1939 v New Yorku a patřil City Bank of New York. Pro nezájem klientů byl ale po šesti měsících provozu odstraněn. To způsobilo, že se na následujících 25 let byl systém ATM zastaven. Až v roce 1967 ho opět uvedla do provozu banka Barclays Bank v Enfield Town v severním Londýně, ten již byl klienty využíván častěji a došlo i k jeho dalšímu rozšíření [34]. Počet vydávaných platebních karet se postupně zvyšoval a jimi uplatňované transakce narůstaly, což způsobovalo, že klasické papírové zpracování pomocí imprinterů nebylo příliš pohodlné. Proto se začátkem 80. let 20. století objevily první elektronické platební terminály umožňující

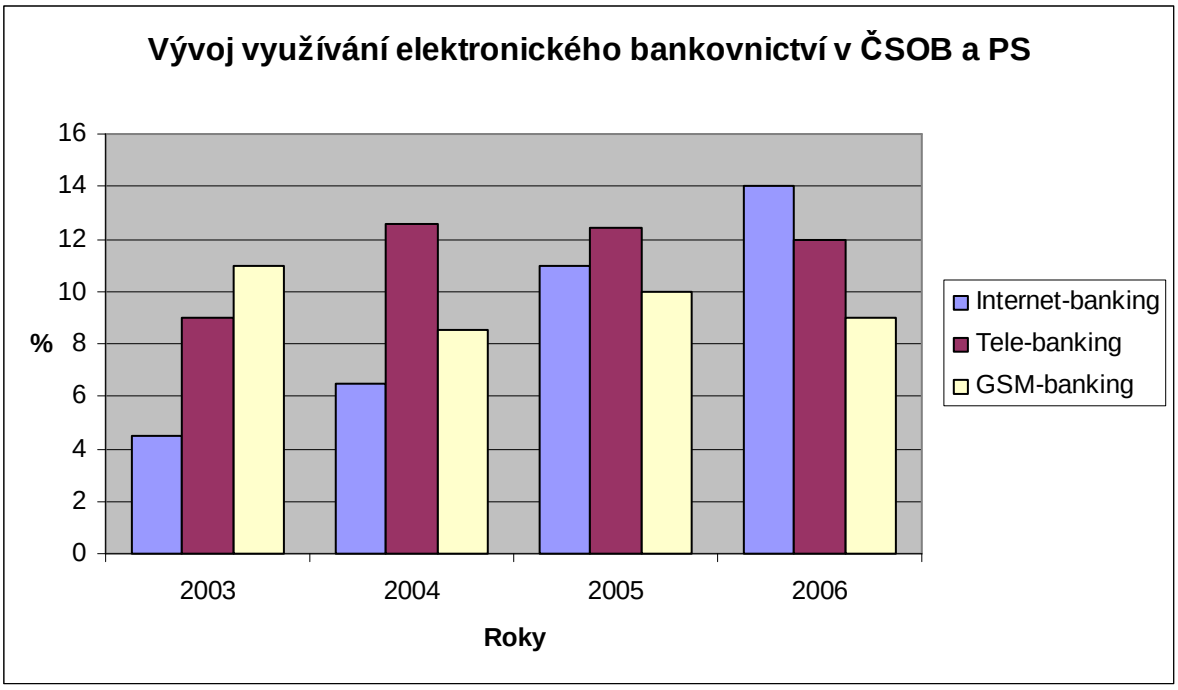
[7] Imprinter - mechanický snímač pro zkopírování embosovaných údajů na platební kartě, lidově je nazýván jako „žehlička“.

[8] ATM (Automatic Teller Machine) - počítačové tele-komunikační zařízení umožňující, klientům z bankovních institucí, zadávat a vyřizovat finanční transakce bez nutnosti osobní obsluhy bankéře či úředníka.

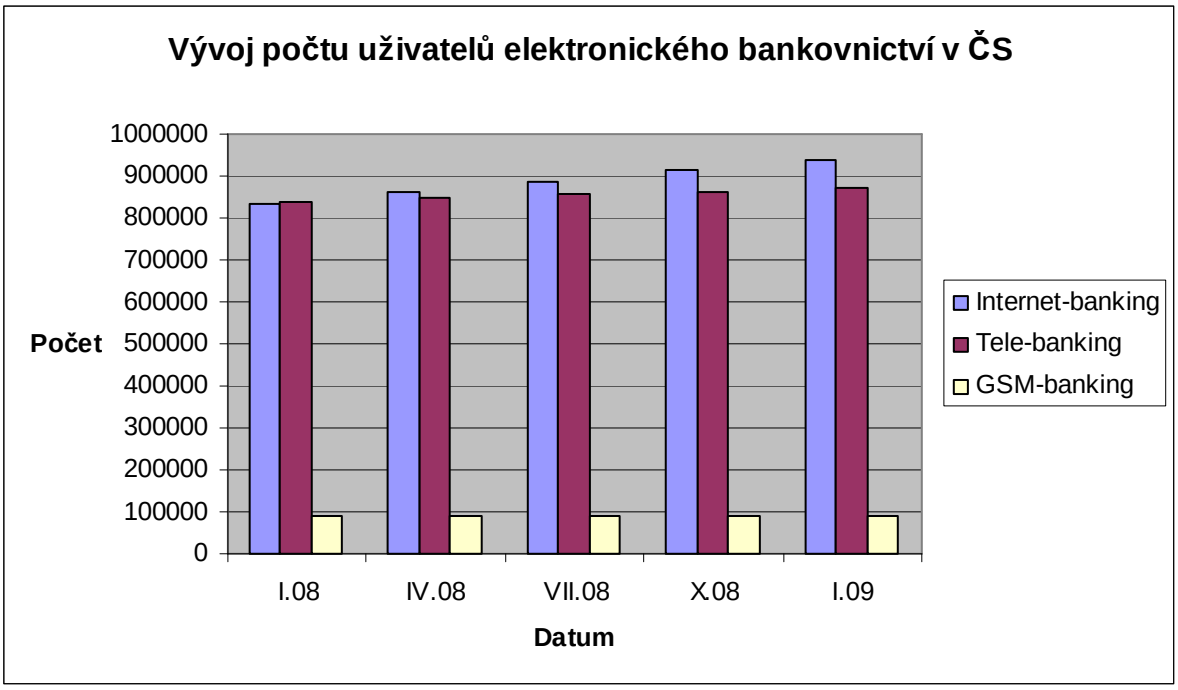
zpracovávat objednávky u obchodníků elektronicky. Zprvu se jednalo o off-line platební terminály, které potvrzovaly transakci samy bez připojení k centrálnímu systému. Následně se zavedly on-line platební terminály, které byly připojeny k autorizačnímu středisku.

Na českém trhu se však platební kreditní karty objevily mnohem déle a to roku 1988. První, kdo na našem území začal vydávat platební karty, byla Živnostenská banka. Přibližně za rok se přidala Česká státní spořitelna, která vydávala karty ke svým sporožirovým účtům. Ty umožňovaly i výběr z bankomatů. Od té doby rostl výdej platebních karet u všech bankovních institucí závratnou rychlostí. Nyní karty dominují v obchodních transakcích nejen ve světě, ale i ČR. V září roku 2009 bylo evidováno 8,9 milionu platebních karet při počtu 10,45 milionu obyvatel. Vyplývá to ze statistiky Sdružení pro bankovní karty (SBK) [29]. [8, 30]

Průlomovým rokem pro české bankovnictví byl rok 1989. Ten představoval počátek transformace české ekonomiky z centrálně plánované na tržní ekonomiku. Důležitým prvkem pro rozvoj elektronického bankovnictví byl také rozvoj komunikační a výpočetní techniky a to od pevných telefonů přes mobilní telefony až k internetu. Do této doby byla pro většinu obyvatel jediným běžně dostupným bankovním produktem pouze vkladní knížka. Avšak následující vývoj platebního styku a komunikační techniky jednoznačně a nekompromisně směřoval k elektronickému bankovnictví. Což dokazují i následující průzkumy bank (Obrázek 1, 2).



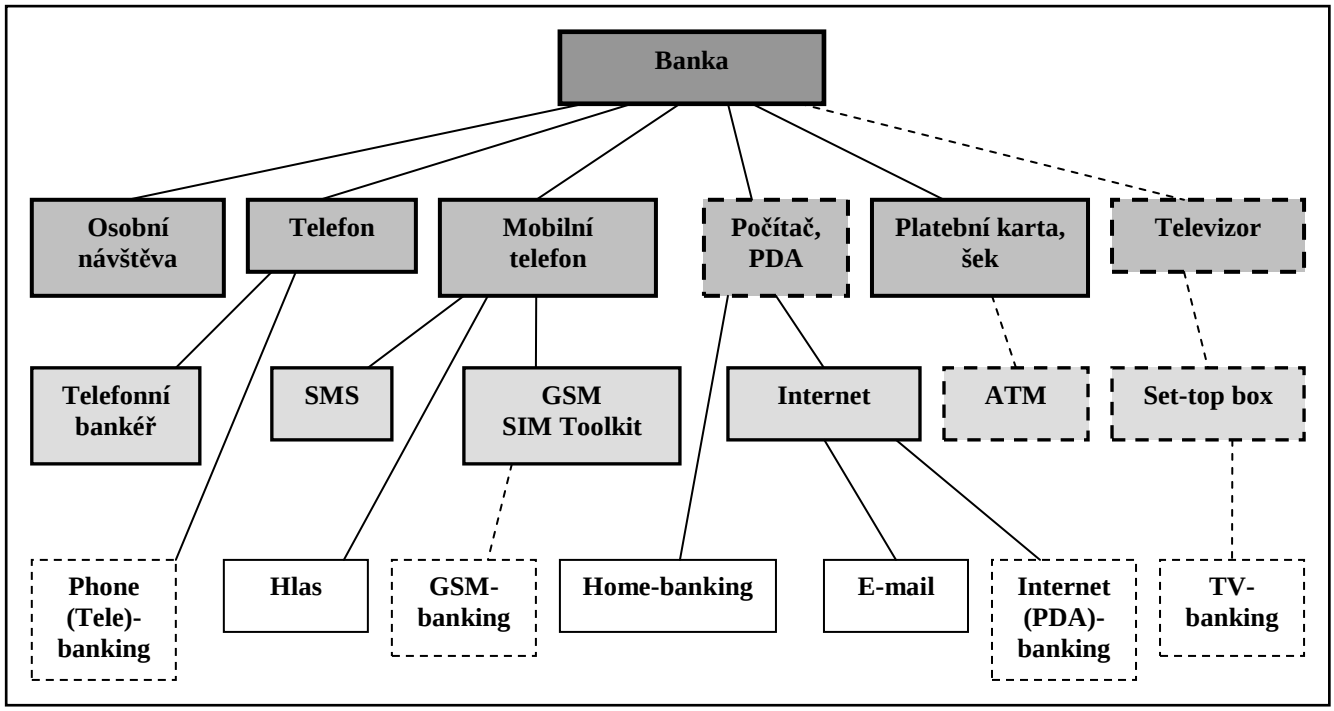
Obrázek 1 - Statistika využívání přímého bankovnictví [35]. Vlastní zpracování.



Obrázek 2 - Vývoj počtu uživatelů elektronického bankovnictví [32]. Vlastní zpracování.

1.3. Možnosti komunikace v elektronickém bankovnictví

S vývojem komunikačních technologií došlo i v bankovnictví k vývoji přístupu uživatelů ke svým bankovním účtům a i k možnosti jejich správy. Impulsem k tomuto elektronickému zpracování bankovních transakcí a komunikaci s bankou, bez nutnosti návštěvy samotné banky, je podstata člověka jako líného tvora a jeho snaha si vše zjednodušovat a zlehčovat a přitom zrychlit. V dnešní době má klient banky mnoho způsobů komunikace se svým účtem a nepřeberné množství operací a příkazů pro jeho případnou správu. Následující obrázek (Obrázek 3) graficky znázorňuje stromovou strukturu přístupu a komunikace klienta s bankou.



Obrázek 3 - Komunikační kanály. Upraveno podle: [8]

2. PŘEHLED SLUŽEB ELEKTRONICKÉHO BANKOVNICTVÍ U VYBRANÝCH INSTITUCÍ A JEJICH POROVNÁNÍ

Jak již bylo zmíněno, možností komunikací mezi bankou a klientem je celá řada. Následující kapitola je zaměřena hlavně na ty, které umožňují přímé bankovnictví. Díky kterým, dle statistik jednotlivých bank, nejen v ČR, jsou prováděny více jak polovina všech bankovních transakcí a nadále se tento poměr zvyšuje [4]. Rychlé elektronické zpracování požadavků totiž zvyšuje komfort nejen klientům, ale i samotným zaměstnancům bank.

Druhy přímého bankovnictví jsou následující:

- Tele-banking (Phone-banking);
- Internet-banking;
- GSM-banking;
- Home-banking;
- a jako novinky PDA-banking a TV-banking.

V následující tabulce (Tabulka 1) je znázorněn přehled elektronického bankovnictví u vybraných bankovních institucí v ČR.

Tabulka 1 - Druhy přímého bankovnictví u vybraných bankovních institucí

	Druhy přímého bankovnictví					
Bankovní instituce	**Tele-banking**	**Internet-banking**	**GSM-banking**	**Home-banking**	**PDA-banking**	**TV-banking**
Citibank	CitiPhone	CityBank Online	/	/	/	/
Česká spořitelna	Servis 24 Tele-banking	Servis (Bussines) 24 Internet-banking	Servis 24 GSM-banking	MultiCash	/	/
ČSOB	Linka 24	Internet-Banking 24	Mobil 24	Business-Banking 24 / Multi-Cash 24	/	/
GE Money Bank	Telefon Banka	Internet Banka	Mobil Banka	BankKlient	/	/
Komerční banka	Expresní linka	Moje banka	Mobilní banka	Přímý kanál / Profibanka / Multicash	/	/
LBBW	/	LBBW Direct	/	MultiCash	/	/
mBanka	mLinka	Internetové bankovnictví	/	/	/	/
Oberbank	/	eBanking	/	/	/	/
Poštovní spořitelna	Max Phone PS	MAX Internet-banking PS	Max mobil PS	MAX Home-banking	/	TV Bank PS
Raiffeisenbank+ eBanka	Telefonní bankovnictví	RB Internet banking/ eKonto	GSM bankovnictví	MultiCash / Gemini	PDA Banking	/
UniCredit Bank	Telebanking / Bussines linka	Online Banking / BussinesNet	GSM Banking / Smart Banking	Eltrans 2000 / MultiCash	Smart Banking	/
Volksbank	Phone banking	Internet Banking	/	Homebanking	/	/

Zdroj: [21, 23, 14, 15, 25, 18, 24, 17, 13, 19, 22, 26, 20]. Vlastní zpracování.

Z tabulky 1 lze vyčíst, že všechny banky poskytují internetové bankovnictví. Převážná většina bank také umožňuje správu klientských účtu prostřednictvím telefonu (tuto možnost nemají klienti LBBW a Oberbank). Nejširší spektrum služeb elektronického bankovnictví nabízejí banky Raiffeisenbank, UniCredit Bank a Poštovní spořitelna. Ty do svých komunikačních rozhraní nově zařadily PDA respektive TV.

Pro porovnání služeb u vybraných bankovních institucí, poskytujících elektronické bankovnictví, bylo jako hlavní kritérium zvoleno cena, neboli náklady na pořízení a vedení služby. Následující tabulka (Tabulka 2) zobrazuje dílčí i průměrnou nákladovost služeb u dané bankovní instituce a to za základní variantu dané služby.

Tabulka 2 - Cenová nákladovost služeb u vybraných bankovních institucí

	Poplatky za zřízení služby / vedení služby (měsíčně) v Kč						
Bankovní instituce	**Tele-banking**	**Internet-banking**	**GSM-banking**	**Home-banking**	**PDA-banking**	**TV-banking**	**Průměrná výše poplatků[9]**
Citibank	0/0	0/0	/	/	/	/	0/0
Česká spořitelna	0/25	0/25	0/25	5000/200	/	/	0/25
ČSOB	0/40	0/0	0/0	1400-5000/230-500	/	/	0/13,33
GE Money Bank	0/49	0/49	0/49	-/250	/	/	0/49
Komerční banka	0/39	0/39	0/19	3000-5000/-	/	/	0/32,33
LBBW	/	0/0	/	-	/	/	0/0
mBanka	0/0	0/0	/	/	/	/	0/0
Oberbank	/	0/0	/	/	/	/	0/0
Poštovní spořitelna	0/0	0/0	0/0	50/150	/	0/0	0/0
Raiffeisenbank+ eBanka	0/50	0/50	0/50	1785-9520/750-1000	-	/	0/50
UniCredit Bank	0/70	0/70	0/70	5000-10000/ 800-1000	0/70	/	0/70
Volksbank	0/39	0/30	/	3000-5000/199-1000	/	/	0/34,50

Zdroj: [21, 23, 14, 15, 25, 18, 24, 17, 13, 19, 22, 26, 20]. Vlastní zpracování

[9] Průměr všech poplatků kromě Home-bankingu, jelikož je tato služba přístupná pouze pro podnikatele a právnické osoby.

Jak je z tabulky 2 patrné, tak náklady na zřízení uvedených služeb, kromě služeb Home-bankingu, jsou nulové. Jediný poplatek, který při zřizování vzniká, je za pořízení bezpečnostního prvku (čipová karta+čtečka, USB klíč[10], kalkulátor). Cena těchto zařízení se pohybuje v rozmezí 200 - 500 Kč. Oproti tomu si banky za vedení elektronického bankovnictví inkasují desítky korun měsíčně. Nejméně klienti za své služby zaplatí u menších bank, jako jsou LBBW, mBanka, Oberbank atd. To se samozřejmě následně projevuje u poskytovaných služeb a to nejen z hlediska jejich správy, ale i na vzhledu, ovladatelnosti a samozřejmě i zabezpečení. V porovnání větších bank obstála nejlépe, z pohledu nákladovosti, ČSOB a Česká spořitelna, nejhůře pak UniCredit Bank a Raiffeisenbank.

3. BEZPEČNOST V ELEKTRONICKÉM BANKOVNICTVÍ

Zavedení elektronického bankovnictví přináší mnohá pozitiva, od rychlosti až po pohodlnost ovládaní z domova. Existují samozřejmě také jistá rizika, která vznikají při zadávání příkazů a transakcí tzv. na „dálku“. Nemálo lidí se právě této komunikace s bankou obává a nadále dávají přednost osobnímu kontaktu s bankéři, což jim připadá jako nejbezpečnější správa jejich financí. Je však zapotřebí brát v potaz, že stejně jako bylo a je důležité budování velkých, bezpečných sejfů proti fyzickému ohrožení, tak na stejné či ještě vyšší úrovni je zabezpečení elektronického bankovnictví proti elektronickému ohrožení. V následující kapitole budou popsány jak druhy zabezpečení určitých operací, tak i zabezpečení komunikace mezi bankou a klientem. Budou zdůrazněny hlavně bezpečnostní prvky, které jsou nyní používány anebo donedávna tvořily bezpečnostní standardy.

3.1. Základní bezpečnostní termíny

Předtím, než zde budou řešena samotná bezpečnostní opatření a zabezpečovací prvky v elektronickém bankovnictví, tak je zapotřebí vysvětlit základní pojmy a termíny, která jsou běžně využívána v bezpečnosti. Bez pochopení a rozlišení těchto výrazů by mohlo dojít k nesrovnalostem či jisté mystifikaci.

Jako první ze základních bezpečnostních termínů bude vysvětlen pojem **identifikace**. Ten označuje proces určení identity (totožnosti) příslušné osoby (uživatele). V tomto případě nastávají dvě možnosti a to, že uživatel buď předkládá údaje o své identitě (jméno, příjmení, rodné číslo, klientské číslo) nebo neudává žádné údaje, ale je držitelem určitého charakteristického (nezaměnitelného) identifikačního prvku (čipová karta, otisk prstu atd.)

[10] Jedná se o USB zařízení skládající se z procesoru, paměti, displeje a minimálně dvou tlačítek (OK, STORNO). Na této paměti je uložen certifikát uživatele, pomocí něhož se autentizuje a autorizuje transakce.

a systém se snaží zjistit jeho identitu prohledáváním databáze s uloženými identifikátory všech uživatelů.

Dalším termínem, velmi hojně využívaným, je **autentizace**. Jedná se o proces ověřování identity uživatele. Ten předkládá tvrzení o své identitě a po zadání těchto údajů systém ověřuje shodu s uloženými identifikátory v databázi. Následuje rozhodnutí, zda se jedná o oprávněného či neoprávněného uživatele.

Posledním ze základních výrazů je **autorizace**. To je proces, který navazuje na autentizaci a můžeme ho chápat jako přiřazení určitých práv (co uživatel může a co ne) pro práci a využívání příslušného systému. [7]

3.2. Druhy bezpečnostních opatření

Zabezpečení v elektronickém bankovnictví lze rozdělit na:

- **Bezpečné navázání komunikace** – jedná se o zabezpečení integrity mezi komunikovanými stranami (klient - banka). V internetovém bankovnictví se využívá implementovaných bezpečnostních protokolů ve webových prohlížečích: protokol S-HTTP, protokol SSL (nejpoužívanější). Do tohoto bloku lze zahrnout i bezpečnost webových prohlížečů, což je také velmi důležitý, ale také často opomíjený prvek u internetového bankovnictví.
- **Šifrování dat** – jedná se především o dva druhy šifrování, symetrické a asymetrické.
- **Bezpečná autentizace klienta** – zde se využívá několik druhů autentizačních prvků klienta a velmi často jejich vrstvení. Jedná se především o jméno a heslo, PIN[11], certifikát, čipová karta, jednorázový SMS kód, elektronický kalkulátor a další.
- **Bezpečná autorizace transakcí** – u autorizace transakcí se nejčastěji využívá certifikát, dále čipová karta, jednorázový SMS kód a elektronický kalkulátor.

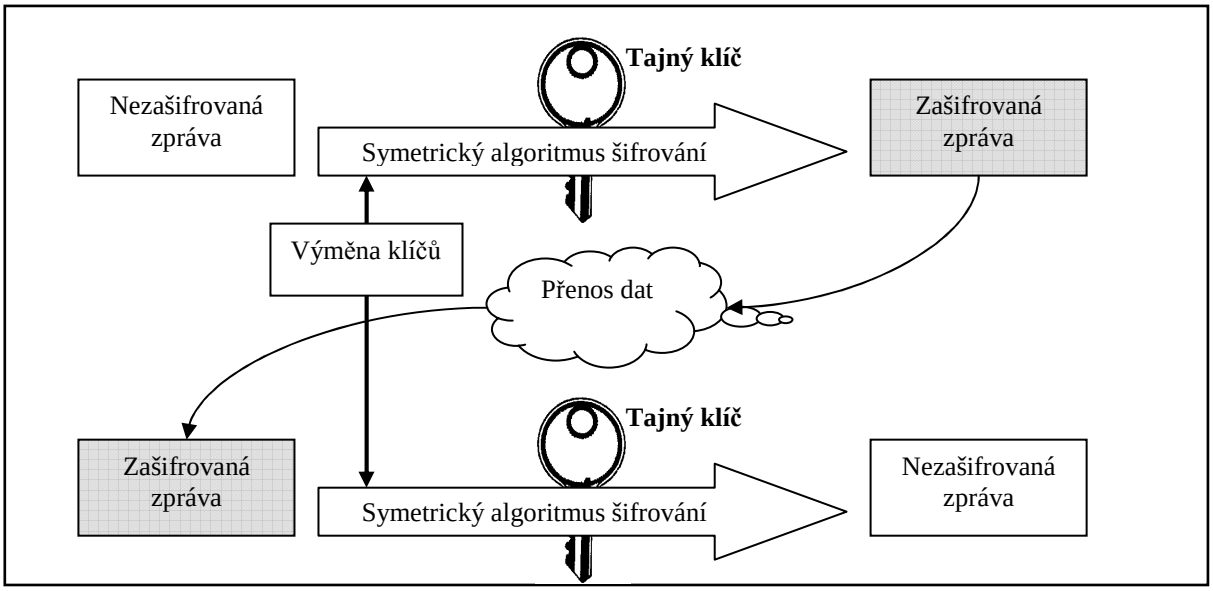
3.3. Šifrování dat

Šifrování nebo také kryptografie je nauka o způsobu utajování zpráv pomocí šifer. Po zašifrování zprávy se zašifrovaný blok dat přenáší po komunikačním kanálu a je tak chráněn před neoprávněným přístupem. Zpětná přeměna do srozumitelné podoby je možná pouze s využitím speciální znalosti a to dešifrovacího klíče. Využívají se, jak již bylo zmíněno, dva typy šifer a to symetrické a asymetrické, ty se liší použitím klíčů a typem použitého algoritmu.

[11] PIN (Personal Identification Number) - osobní identifikační číslo (číselné heslo), používané pro jednoznačnou identifikaci.

3.3.1. Symetrické šifrování

Symetrické šifrování je charakteristické tím, že využívá pouze jednoho klíče. Ten se použije k zašifrování zprávy na straně odesílatele a také pro dešifrování zprávy na straně příjemce. Tím však vzniká nutnost, ještě před začátkem komunikace, bezpečně dopravit jak informace o samotném šifrovacím algoritmu, tak samotný klíč, příjemci zprávy. Pro tuto výměnu se využívá asymetrická šifra, čímž je zajištěn bezpečný přenos klíče (viz Obrázek 4). Výhodou těchto šifer je aplikace šifrovacích algoritmů téměř v reálném čase a přitom s použitím dostatečně dlouhého klíče (128, 256 bitů). Dnes není v možnostech moderní výpočetní techniky, bez znalosti správného klíče, tyto šifry prolomit v reálném čase. Druhy používaných symetrických šifrovacích algoritmů: DES[12], AES[13], IDEA[14]. [9]



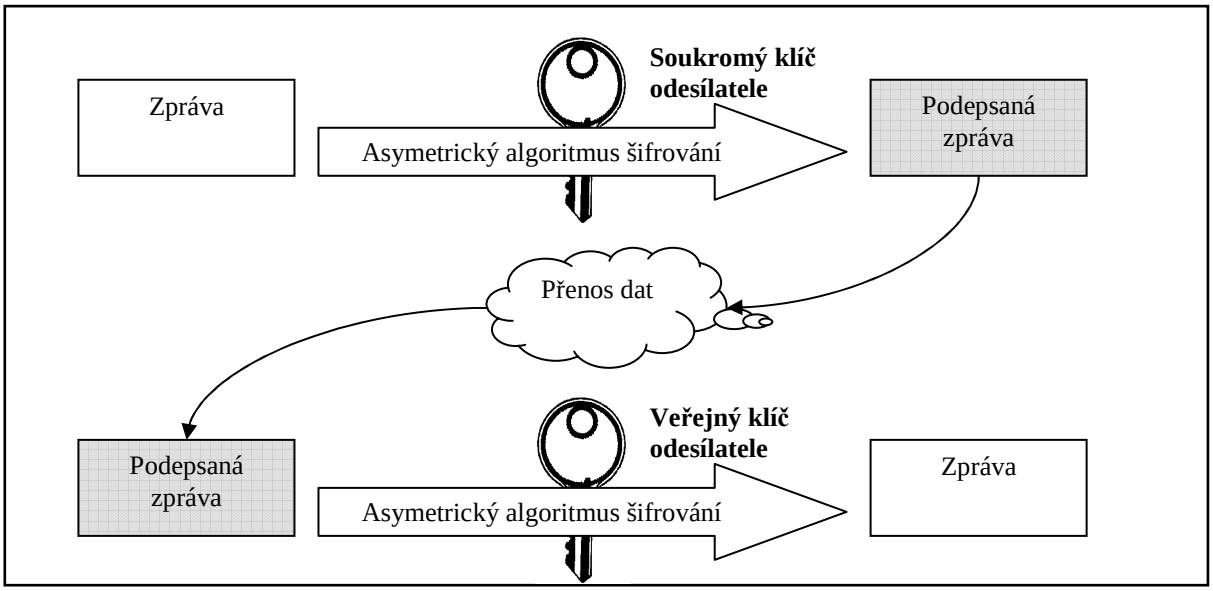
Obrázek 4 - Šifrování zpráv symetrickou šifrou [9]. Vlastní zpracování.

3.3.2. Asymetrické šifrování

Od symetrického šifrování se liší použitím dvou klíčů, jeden pro šifrování zprávy a druhý pro dešifrování. Tyto klíče si uživatel vygeneruje pomocí běžně dostupných programů (např.: webový prohlížeč) a stane se tak jejich jediným držitelem. Pokud není možné odvodit jeden klíč z druhého klíče, hovoříme o nich jako o soukromém klíči a veřejném klíči. Soukromý klíč by měl majitel maximálně střežit, jelikož je jediným vlastníkem, kdežto veřejný klíč by měl být volně dostupný. Tato dvojice klíčů se využívá ke dvěma základním účelům.

První z nich (Obrázek 5), je zajištění integrity dat a zaručení odpovědnosti odesílatele za zprávu. [9]

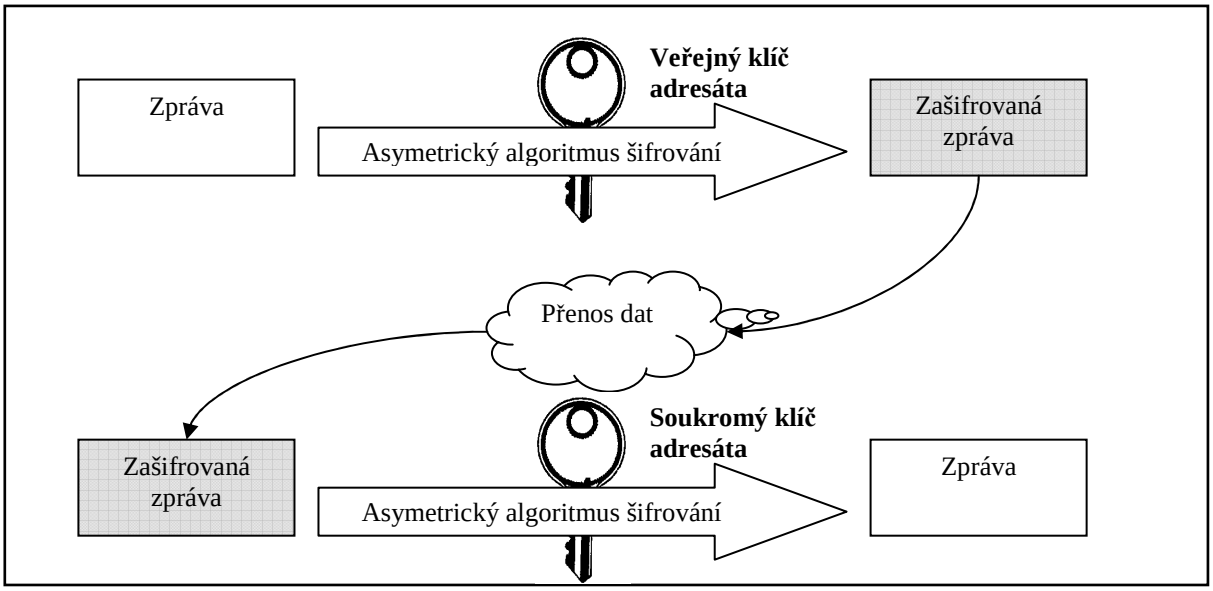
[12]DES (Data Encryption Standard) - symetrická šifra vyvinutá v 70. letech. V roce 1977 byla zvolena za standard (FIPS 46) pro šifrování dat. Nynější varianta je Triple DES - 3TDES pracuje s klíčem o celkové délce 168 bitů.
[13]AES (Advanced Encryption Standard) - nynější schválený standard. Nástupce šifrovacího standardu DES.
[14]IDEA (International Data Encryption Algorithm) - symetrická bloková šifra vyvinutá Švýcarským národním technologickým institutem (ETHZ) v Zürichu. Momentálně patentově chráněna.



Obrázek 5 - Přenos nešifrované, ale podepsané zprávy [9]. Vlastní zpracování.

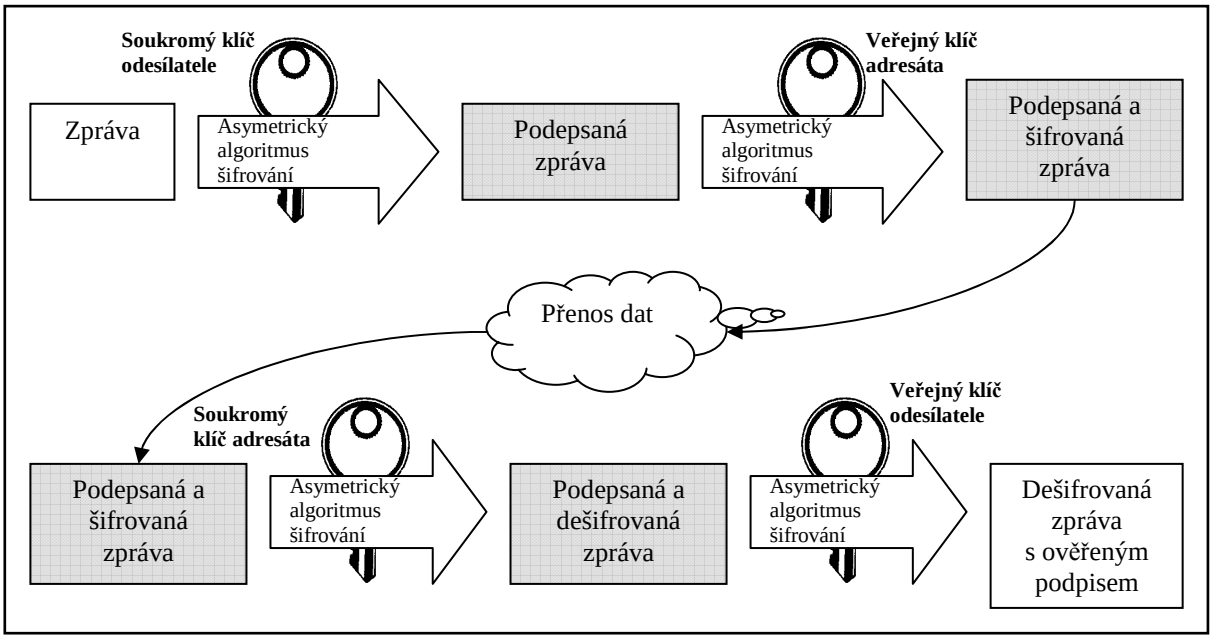
Jedná se o použití soukromého klíče odesílatele na odesílanou zprávu a využití veřejného klíče odesilatele k dešifrování. Tento způsob využití klíčů odesílatele není nazýván šifrování, ale podepsání zprávy, jelikož zde není řešena důvěrnost zprávy [9]. Tzn., že zprávu může přečíst kdokoli s použitím veřejného klíče. Tento problém řeší druhý způsob využití dvojice klíčů.

V druhém případě je řešena samotná důvěrnost zprávy. Tzn., že zprávu může přečíst pouze oprávněná osoba, v našem případě držitel soukromého klíče (viz Obrázek 6).



Obrázek 6 - Přenos šifrované, ale nepodepsané zprávy [9]. Vlastní zpracování.

Oba tyto způsoby lze zkombinovat (Obrázek 7), čímž je zaručena důvěrnost informací, autentizace odesílatele i zaručena jeho odpovědnost za odeslanou zprávu.



Obrázek 7 - Přenos šifrované a podepsané zprávy [9]. Vlastní zpracování.

Nynějším nejpoužívanějším asymetrickým algoritmem je algoritmus RSA[15]. Mezi bývalé standardní algoritmy můžeme zařadit DSA[16], ECDSA a další. Nevýhodou asymetrických šifer je, že jsou oproti symetrickým šifrám, asi 1000krát pomalejší [9]. Proto se v reálném světě kombinují oba šifrovací systémy, kde se využívá rychlost symetrického a flexibilita asymetrických systémů jako je toho u digitálních podpisů.

3.4. Elektronický podpis

Pojmem elektronický podpis, dle znění v zákoně[17], představuje údaje v elektronické podobě, které jsou připojeny nebo logicky spojeny s datovou zprávou a slouží ke zjištění totožnosti podepsané (oprávněné) osoby ve vztahu k datové zprávě.

Důležitým hlediskem je, aby tento podpis byl bezpečný (nepodvrhnutý) tzn., aby byl ověřen prokazatelně bezpečným způsobem. V praxi je dnes za bezpečný elektronický podpis považován digitální podpis, který využívá znalosti a principy šifrování s veřejným klíčem.

Další variantou elektronického podpisu je podepisování pomocí biometrických prvků. Ty se však v bankovnictví příliš nepoužívají, hlavní zastoupení mají v kriminalistice.

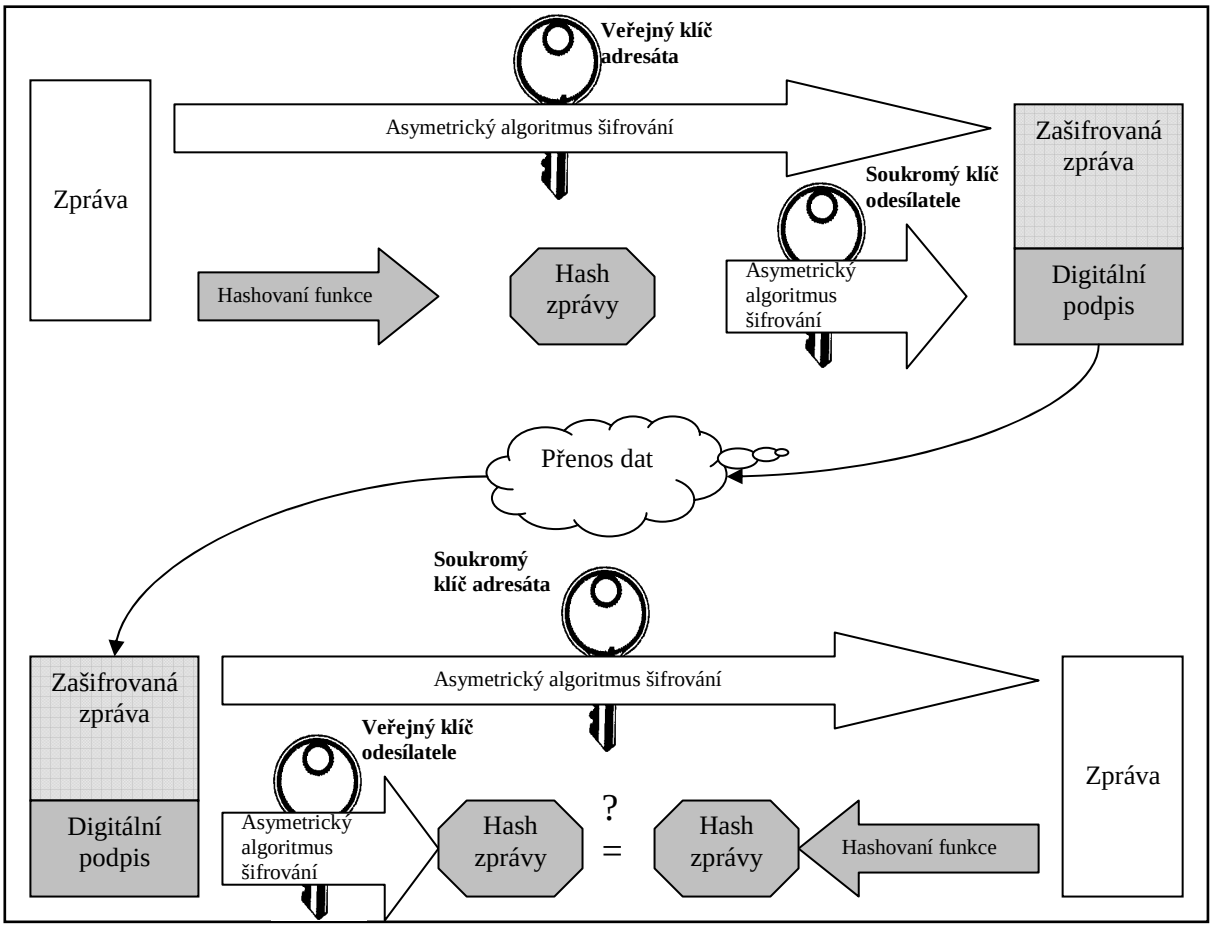
[15] RSA (Rivest-Shamir-Adelman) - asymetrická šifra vytvořená roku 1977 a pojmenovaná zkratkami autorů.
[16] DSA (Digital Signature Algorithm) - algoritmus, který byl v nedávné minulosti využíván ve standardu pro digitální podpis.
[17] Zákona o elektronickém podpisu č. 227/2000 Sb. a novelizován zákony 226/2002 Sb., 517/2002 Sb. a 440/2004 Sb.

3.4.1. Digitální podpis

Jak již bylo zmíněné, jedná se nejpoužívanější a nejbezpečnější elektronický podpis v elektronické komunikaci. Digitální podpis dokumentu zaručuje příjemci tři základní bezpečnostní aspekty a to autentizaci, integritu a nepopiratelnost (odpovědnost) autorství. Nezaručuje však důvěrnost dokumentu, ta se zajišťuje šifrováním samotné zprávy.

Digitální podpis využívá metodu šifrování s veřejným klíčem, přičemž nejčastěji algoritmus RSA, a dále využívá tzv. hash. Jedná se o otisk dokumentu. Ten je vytvořen jednocestnou funkcí, která z libovolně dlouhého dokumentu (textu), vygeneruje krátký text (řetězec znaků) s konstantní délkou. Dříve používanými algoritmy byly MD-5 (16B hash) a SHA-1 (20B hash) jsou nyní považovány za nedostačující z důvodu tvorby stejných otisků z různých textů, nyní je nejčastěji využíván SHA-2 s otiskem dlouhým 64B. [1]

Princip podepisování zprávy je znázorněn na následujícím obrázku (Obrázek 8).



Obrázek 8 - Bezpečná komunikace s ověřením digitálního podpisu [9]. Vlastní zpracování.

Z obrázku 8 je patrné, že je při tomto bezpečném podepisování postup následující. Nejprve se vypočítá hash ze zprávy a ten se pomocí soukromého klíče odesílatele podepíše. Tím se vytvoří digitální podpis. Následně se zašifruje i samotná zpráva pomocí veřejného klíče adresáta, aby byla zaručena integrita. Adresát takto obdrženou zprávu dešifruje pomocí svého

soukromého klíče a vypočte z ní, pomocí stejné hashovaní funkce jako u odesilatele, hash. Ten by se měl, pokud nedošlo k narušení integrity, shodovat s dešifrovaným hashem přijatým v digitálním podpisu.

Tímto jsou splněny všechny bezpečnostní cíle bezpečné komunikace, ale jelikož se v tomto případě používá asymetrické šifrování na celou zprávu, je tento proces poměrné zdlouhavý. Proto se v praxi častěji využívá pro šifrování celé zprávy symetrické šifrování, které je mnohem rychlejší a asymetrické šifrování se využívá pouze pro tvorbu digitálního podpisu a pro přenos (výměnu) klíče pro symetrické šifrování.

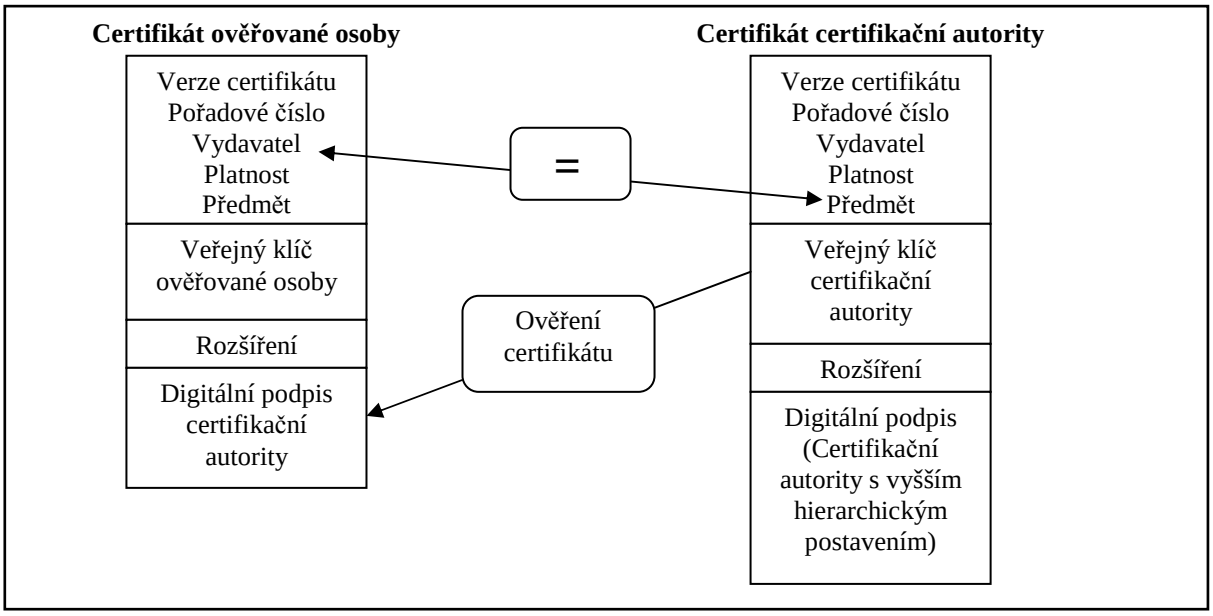
3.4.2. Certifikát

Proto, aby mohl být digitální podpis bezpečně využíván v běžné komunikaci. Je nezbytné, aby byl zajištěn přístup k veřejným klíčům a jejich bezpečné spravování. Samozřejmostí je také ověřené spojení veřejného klíče a jeho vlastníka z důvodu integrity dat. Všechny tyto aspekty by měl zajistit certifikát veřejného klíče vydaný příslušnou certifikační autoritou (CA)[18]. Ten nás chrání proti podvržení veřejného klíče.

Primární funkcí certifikátu je ověřené spojení mezi identitou osoby a jejím veřejným klíčem. Jedná se o datovou strukturu, která obsahuje verzi certifikátu, veřejný klíč dané osoby, její identifikační údaje, název vydavatele certifikátu, algoritmus podpisu, platnost certifikátu, pořadové číslo certifikátu a případné rozšíření. Všechny tyto údaje a jejich pravdivost, potvrzuje certifikační autorita svým digitálním podpisem. Takto vystavený certifikát se dá považovat za důvěryhodný identifikační prvek a často je přirovnáván k elektronickému občanskému průkazu. Aby mohl být certifikáty hromadně a celosvětově využívány, je jeho forma upravena dle standardizované normy X.509. Samozřejmě i certifikát prošel vývojem a nynější používaná verze certifikátu je verze 3. [1]

V systému ověřování digitálním podpisem se tedy pro bezpečnou výměnu veřejných klíčů využívá certifikát, který je přidán k samotnému dokumentu a jeho digitálnímu podpisu. Proto, aby mohl příjemce zprávy ověřit pravost certifikátu, musí ověřit pravost digitálního podpisu na certifikátu pomocí veřejného klíče certifikační autority. Ten nalezne na jejich oficiálních stránkách v certifikátu certifikační autority. Tato vazba je znázorněna na obrázku 9.

[18] CA - subjekt, který vydává certifikáty, potvrzuje jejich pravost a spravuje je. Mezi nejuznávanější v ČR patří VeriSign, První certifikační autorita (I.CA) a GlobalSign.



Obrázek 9 - Znázornění ověřování certifikátu [1]. Vlastní zpracování.

3.5. Webový prohlížeč a bezpečnostní protokoly

Samotné bezpečnostní protokoly zajišťují vzájemnou bezpečnou komunikace mezi klientem banky a bankou. Starají se o to, aby měl klient jistotu, že komunikuje přes webové rozhraní banky a ne přes podvrženou stránku. V dnešní době jsou implementovány ve většině webových prohlížečů jako Internet Explorer, Mozilla Firefox, Opera a další.

3.5.1. Protokol S-HTTP

Protokol S-HTTP (Secure Hypertext Transport Protokol) byl zaveden roku 1994 firmou Enterprise Integration Technologies a to pro potřebu bezpečnostního standardu na internetu. Jeho základními vlastnostmi jsou [9, 2]:

- rozšiřuje sadu instrukcí HTTP, aby mohl umožnit šifrování a jinak zabezpečit prováděné transakce;
- používá záhlaví ve stylu HTTP;
- používá metodu podpisů, šifrování, kontroluje autentičnost zpráv;
- podporuje certifikáty a podepisování pomocí klíčů.

3.5.2. Protokol SSL

Protokol SSL (Secure Sockets Layer) vytvořila firma Netscape, jedná se o dnešní nejpoužívanější bezpečnostní webový protokol. Je to v podstatě vrstva ISO/OSI modelu vložená mezi transportní a aplikační a používá architekturu klient/server. Mezi jeho základní vlastnosti patří [9, 2]:

- poskytuje šifrování dat, zabezpečení integrity a ověření autentičnosti, jak na straně serveru, tak na straně klienta;
- pro ověření identity odesílatele používá digitální podpis;
- zajišťuje bezpečný přechod dat mezi aplikační a transportní vrstvou;
- je kompatibilní s firewally.

Takto zabezpečené spojení mezi klientem a serverem je možné poznat podle URL adresy v používaném prohlížeči, jelikož zabezpečené komunikační protokoly připojí ke své zkratce písmeno „s“ (https, ftps atd.).

Komunikace na této zabezpečené úrovni probíhá jak na S-HTTP tak na SSL obdobně, pouze u SSL probíhá navázání spojení o něco déle z důvodu vzájemného ověřování obou komunikujících stran pomocí certifikátů. Dále se jedná o dohodnutí algoritmu s veřejným klíčem (ve většině případů algoritmu RSA), pomocí něhož dojde k výměně klíče pro symetrickou šifru a dohodnutí na samotné symetrické šifře, která se využije pro další komunikaci. Poté již následuje samotná zabezpečená komunikace pomocí symetrického šifrování. [9]

3.5.3. Bezpečnost webového prohlížeče

V neposlední řadě je také důležité, nejen při používání elektronického bankovnictví, využívat vhodný software a jeho aktualizace. V našem případě se jedná například o webové prohlížeče či softwary pro Home-banking. Aktualizace nám totiž mohou poskytnout opravné „balíčky“ nebezpečných chyb, které byly přehlédnuty při vývoji těchto aplikací. Tyto chyby dokáží zkušení útočníci využít k napadení daného systému a získat cenné informace, či narušit integritu dat a proto je potřeba se proti nim bránit bezpečnostními aktualizacemi. Pro názornost je v následující tabulce (Tabulka 3) znázorněn počet objevený chyb a jejich oprav u tří nejpoužívanějších webových prohlížečů v letech 2006, 2007, 2008 a 2009.

Tabulka 3 - Chyby ve webových prohlížečích za rok 2006 - 2009

Webový prohlížeč	Objevené chyby				Opravené chyby			
	2006	2007	2008	2009	2006	2007	2008	2009
Internet Explorer 6, 7	110	82	31	37	74	31	/	/
Mozilla Firefox	45	19	115	110	36	7	/	/
Opera	18	5	30	15	18	0	30	15

Zdroj: [33, 31, 36, 27]. Vlastní zpracování.

Z tabulky 3 je patrné, že počet chyb se neustále mění a není zrovna zanedbatelný u jakéhokoliv webového prohlížeče, proto je zapotřebí jejich aktualizace sledovat a nezanedbávat jejich správu.

3.6. Druhy autentizačních a autorizačních prvků v elektronickém bankovnictví

Autentizace klienta v bankovním systému a následná autorizace zadávaných transakcí je nejkritičtějším bodem ve využívání elektronického bankovnictví, jelikož zde velkou roli hraje lidský faktor. Proto je zapotřebí využívat kvalitní bezpečnostní prvky, které klienty ochrání nejen proti jim samotným (jejich bezpečnostním karambolům), ale hlavně proti případným útočníkům. V následující kapitole jsou popsány ty, které jsou aktuálně využívány nejen v českém bankovnictví.

3.6.1. Uživatelské jméno a heslo

Jedná se asi o nejpoužívanější, ale také nejméně bezpečný způsob autentizace. Stačí znát pouze tyto údaje, aby se útočník dostal na účet klienta. Získá je například odpozorováním, pomocí trojského koně či keyloggeru[19] nebo nějakou z metod phishingu[20]. Pokud není následně vyžadována autorizace samotných transakcí, může klient přijít o všechnu finanční hotovost na účtu a i mnohem víc. Proto by měl uživatel doplnit tento autentizační prvek o další bezpečnostní prvek, viz níže.

3.6.2. PIN

Bývá nejčastěji používán v kombinaci s uživatelským jménem a heslem. Jedná se o 4-6ti místné číslo, které obdrží klient od banky. V některých případech si ho může klient sám zvolit. Je využíván jak pro autentizace při vstupu do aplikací, tak pro autorizaci plateb (především v telefonním a GSM bankovnictví). V současnosti je nahrazován jednorázovým SMS kódem.

3.6.3. Jednorázový SMS kód

Tento autentizační a autorizační prvek je založen na předpokladu, že klient vlastní mobilní telefon. Dříve, kdy ještě nebyly mobilní telefony tolik rozšířené, se využívala sada

[19] Keylogger - software, který snímá stisky jednotlivých kláves. Využívá se také pro zjišťování zadávaných údajů a hesel pomocí klávesnice.
[20] Phishing - pochází z anglického slova fishing (rybaření). Jedná se způsob získání citlivých informací pomocí e-mailů od zdánlivě důvěrných institucí - např.: banky.

jednorázových hesel - TANů[21] [7]. Nyní se velmi často využívá jednorázový SMS kód ve spojení s předešlým druhem autentizace - jméno a heslo. Po zadání těchto přihlašovacích údajů je klientovi zaslána SMS zpráva s jednorázovým heslem, které následně zadá do systému. Ještě nedávno se využíval tento SMS kód pro vstup a klient měl přístup ke všem aktivním transakcím bez dalšího potvrzování. Nyní je však z bezpečnostních důvodů preferována metoda potvrzení každé aktivní operace (jak autentizace klienta, tak autorizace transakcí) pomocí jednorázového SMS kódu.

3.6.4. Certifikát

Využívá se jak pro autentizace klienta, tak pro autorizaci transakcí a bývá velmi často kombinován s jednorázovým SMS kódem. Proto, aby mohl klient tento prvek využívat, musí od banky obdržet osobní klientský certifikát, buď uložený v souboru (na disketě, CD, Flash paměti, jednorázově na webových stránkách banky atd.) nebo na čipové kartě. Klient následně používá certifikát dle požadavků v bankovním systému. Primárním pravidlem při využívání certifikátu je neukládat certifikát na pevný disk, zde je totiž lehce kopírovatelný [1]. Vždy by měl být uložený na externím médiu, které bude připojeno jen při přistupování k účtu. Po ukončení transakcí, by mělo být samozřejmostí médium z počítače opět vyjmout a bezpečně uschovat. Vyšší bezpečnost poskytuje klientský certifikát uložený na čipové kartě. V tomto případě je však nutné pořídit si čtečku čipových karet. Výhodou oproti souboru na CD či Flash paměti je obtížnost zkopírování.

3.6.5. Elektronický kalkulátor

Jedná se o jeden z nejbezpečnějších způsobů autentizace a autorizace. Jde o elektronické zařízení (připomíná kalkulačku) [10], které dokáže generovat jednorázová hesla pro přístup k bankovní aplikaci. Tato zařízení jsou buď připojena, nebo nejsou připojena k počítači a jsou synchronizována se systémy banky tak, aby obě strany generovaly shodné klíče. Po spuštění kalkulátoru je zapotřebí zadat vstupní PIN, který klient obdrží od příslušné banky a na základě zadávaných transakčních údajů (číslo účtu, částka, kód banky atd.) je vygenerováno jedinečné jednorázové heslo. Toto heslo poté klient zadává do bankovní aplikace a je ověřeno, že je majitelem příslušného kalkulátoru [28]. Pro útočníka je téměř nemožné bez vlastnictví daného kalkulátoru a transakčních údajů napadnout jakoukoliv operaci.

[21] TAN (Transaction Authentication Number) -.autorizační a autentizační kód. Klient banky obdržel sadu kódů (např. 100). Tyto kódy následně, dle požadavků autentizace a autorizace, jednorázově využíval a zadával do bankovního systému.

3.6.6. Dodatečné bezpečností prvky

Téměř každá bankovní instituce umožňuje rozšíření standardně poskytovaných bezpečnostních prvků. Do této kategorie lze zařadit:

- **Časový limit nečinnosti** - jedná se dobu, po které je klient automaticky odhlášen ze systému v případě své nečinnosti.
- **Časový transakční limit** - jde o maximální transakční částku, kterou může klient uskutečnit během určitého časového intervalu. Nejčastěji se jedná o denní, týdenní. Pokud chce klient uskutečnit větší platbu než je transakční limit, musí ve většině případů navštívit pobočku své banky.
- **Zaslání SMS zprávy při každé aktivní transakci** - velmi praktický pomocník při správě svého účtu, jelikož má klient neustálý dohled nad svým účtem a může zabránit případné nevyžádané transakci.

3.7. Bezpečnost jednotlivých elektronických bankovnictví

Stejně jako se liší druhy elektronického bankovnictví používanou komunikační technologií, tak je pochopitelné, že i bezpečnostní prvky budou odlišné. V této kapitole budou stručně popsány bezpečnostní prvky aplikované v jednotlivých elektronických bankovnictvích.

3.7.1. Tele-banking

Při vstupu do toho systému se nejčastěji využívá klientovo jméno (číslo) a heslo (PIN). Samotná autorizace transakcí je prováděna kontrolními otázkami na údaje vlastníka účtu. Například se jedná o jednorázová hesla obdržená v bance, čísla smluv, účtů atd.

3.7.2. GSM-banking

Přenos dat je chráněn nejen samotným šifrováním v GSM sítích - norma GSM 03.48 [2], ale využívá se i přídavných funkcí SIM karty - SIM Toolkit. Ta umožňuje symetrické šifrování, kde je využitý šifrovací klíč uložen na SIM kartě klienta a v systému banky. Tím je zajištěn bezpečný přenos dat mezi telefonem a bankou. Autorizace plateb je nejčastěji prováděna pomocí bankovního PINu. [5]

3.7.3. Internet a PDA-banking

Bezpečný přenos dat mezi webovým a bankovním systémem je zabezpečen bezpečnostními protokoly, převážně SSL, o kterém bylo psáno dříve. Pro autentizaci klienta a autorizaci transakcí je využívána řada bezpečnostních prvků, většina z nich již byla zmíněna (jméno a heslo, certifikát, SMS kód, čipové karty, kalkulátor atd.) [7].

3.7.4. Home-banking

Od internetového bankovnictví se liší tím, že je pevně svázán s počítačem, kde je využívaný software nainstalován. To bývá převážně doma či v práci. Už tím je zajištěna jistá bezpečnost. Bezpečná komunikace je zajištěna pomocí šifrování, podobně jako u internetového bankovnictví a to za využití certifikátů zúčastněných stran [2]. Pro autentizaci klienta a autorizaci transakcí se nejčastěji využívá jméno a heslo, certifikát, čipová karta a kalkulátor.

4. ZABEZPEČNÍ U VYBRANÝCH BANKOVNÍCH INSTITUCÍ A JEJICH POROVNÁNÍ

Pro porovnání zabezpečení u vybraných bankovních institucí byly vybrány autentizační a autorizační prvky a to u nejpoužívanějšího elektronického bankovnictví - internetového. Porovnání bylo prováděno pomocí více-kriteriálního rozhodování. Druhy rozhodovacích mechanismů byly vybrány tři - Bodové ohodnocení a Saatyho metoda pomocí programu MS Office Excel 2003 a metoda AHP[22] v programu CDP (Criterium DecisonPlus).

4.1. Porovnání autentizačních prvků

Pro porovnání zabezpečení bylo zvoleno dvanáct, již dříve zmiňovaných, bankovních institucí. Jako kritéria porovnání byly zvoleny autentizační prvky, které má klient možnost využívat, nebo jsou součástí standardního přihlašovacího postupu. Tato kritéria byla následně, u zvolených metod, ohodnocena dle úrovně jejich bezpečnosti. V následující tabulce 4 jsou znázorněny autentizační prvky, které dané banky poskytují.

Tabulka 4 - Poskytované autentizační prvky u vybraných bankovních institucí

	Poskytované autentizační prvky				
Bankovní isntituce	**Jméno a heslo**	**Certifikát**	**Čipová karta**	**SMS kód**	**Kalkulátor**
LBBW	ano		ano		ano
Citibank	ano				ano
Česká spořitelna	ano		ano		ano
ČSOB	ano		ano		
Raiffeisenbank+eBanka	ano	ano		ano	ano
GE Money Bank	ano	ano		ano	
UniCredit Bank	ano	ano		ano	ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano				
Volksbank	ano	ano			
mBank	ano				
Oberbank	ano				

Zdroj: [7, 21, 23, 14, 15, 25, 18, 24, 17, 13, 19, 22, 26, 20]. Vlastní zpracování

[22] AHP (Analytic Hierarchy Process) - analytický hierarchický proces, neboli strukturovaná technika pro řešení složitých rozhodovacích problémů.

4.1.1. Metoda bodového ohodnocení

Jako první metoda pro porovnání autentizačních prvků, byla zvolena metoda bodového ohodnocení. Jedná se totiž o početně jednodušší metodu a zároveň jsou její výsledky dosti vypovídající.

U této rozhodovací metody byly kritériím uděleny body (hodnoty vah) v rozmezí 1 - 9 podle úrovně zabezpečení (1 = nejnižší bezpečnost, 9 = nejvyšší bezpečnost). Následně pro jednodušší vyhodnocování výsledků bylo slovní ohodnocení převedeno na číselné. Poté byl jednotlivým bankám přidělen odpovídající počet bodů a posléze byly seřazeny dle jejich hodnot, což také znázorňuje tabulka 5.

Tabulka 5 - Bodové ohodnocení bankovních institucí - autentizace

Autentizační prvky	**Jméno a heslo**	**Certifikát**	**Čipová karta**	**SMS kód**	**Kalkulátor**	
Ohodnocení bezpečnostní úrovně	**1**	**3**	**5**	**7**	**9**	**Celkové bodové hodnocení**
Raiffeisenbank+eBanka	1	1		1	1	**20**
UniCredit Bank	1	1		1	1	**20**
LBBW	1		1		1	**15**
Česká spořitelna	1		1		1	**15**
Komerční banka		1	1	1		**15**
GE Money Bank	1	1		1		**11**
Citibank	1				1	**10**
ČSOB	1		1			**6**
Volksbank	1	1				**4**
Poštovní spořitelna	1					**1**
mBank	1					**1**
Oberbank	1					**1**

Zdroj: autor

Pro lepší porovnání s následujícími metodami pro podporu rozhodování byla přidělená skóre znormována pomocí vzorce (2) a bankám bylo přiřazeno pořadí dle výsledků (viz. Tabulka 6).

Tabulka 6 - Znormování bodového ohodnocení a určení pořadí - autentizace

Bankovní instituce	**Skóre**	**Pořadí**
Raiffeisenbank+eBanka	0,168	**1**
UniCredit Bank	0,168	**1**
LBBW	0,126	**2**
Česká spořitelna	0,126	**2**
Komerční banka	0,126	**2**
GE Money Bank	0,092	**3**
Citibank	0,084	**4**
ČSOB	0,050	**5**
Volksbank	0,034	**6**
Poštovní spořitelna	0,008	**7**
bank	0,008	**7**
Oberbank	0,008	**7**

Zdroj: autor

4.1.2. Saatyho metoda

Následující použitou metodou pro porovnání zabezpečení byla Saatyho metoda, která je v praxi velmi hojně využívána pro nejrůznější rozhodovací problémy.

Při určování vah kritérií (autentizačních prvků) a samotném výpočtu jsem se řídil znalostmi nabytými v předmětu Rozhodovací procesy ve 4. semestru roku 2008/2009. Určení normovaných vah je shrnuto v tabulce 7 a samotný výpočet je znázorněn v příloze 1.

Tabulka 7 - Určení vah kritérií - autentizace

	Jméno a heslo	**Certifikát**	**Čipová karta**	**SMS kód**	**Kalkulátor**	**b_i**	**Váhy**
Jméno a heslo	**1**	1/3	1/5	1/7	1/9	0,254	**0,033**
Certifikát	3	**1**	1/3	1/5	1/7	0,491	**0,064**
Čipová karta	5	3	**1**	1/3	1/5	1,000	**0,130**
SMS kód	7	5	3	**1**	1/3	2,036	**0,264**
Kalkulátor	9	7	5	3	**1**	3,936	**0,510**

Zdroj: autor

Pro ohodnocení kritérií bylo využito rozmezí hodnot 1 - 9 kde:

- 1 – rovnocenné kritérium;
- 3 – slabě preferované kritérium;
- 5 – silně preferované kritérium;
- 7 – velmi silně preferované kritérium;
- 9 – absolutně preferované kritérium.

Při sestavování matic Saatyho metodou bylo zapotřebí jejich správnost ověřit indexem konzistence (KI). Ten se vypočte pomocí vztahu :

$$KI = (\lambda_{\max} - m)/(m-1) \quad (1).$$

Kde λ_{max} je maximální vlastní číslo matice a m je počet variant, přičemž je za správně sestavenou matici považována matice s KI $\leq$ 0,1 [3]. Pro matici vah kritérií byl index konzistence stanoven na hodnotu **0,069**, což bez problému splňovalo vymezenou mez.

Po výpočtu samotných alternativ (bankovních institucí) a ohodnocení váhami kritérií byl výsledek vynesen do tabulky 8. I zde bylo zapotřebí normování vah a to pomocí vztahu:

$$v_i = \frac{b_i}{\sum_{i=1}^{n} b_i} \quad (2).$$

Kde b_i, v tomto případě, představuje geometrický průměr řádku Saatyho matice, respektive přidělené skóre.

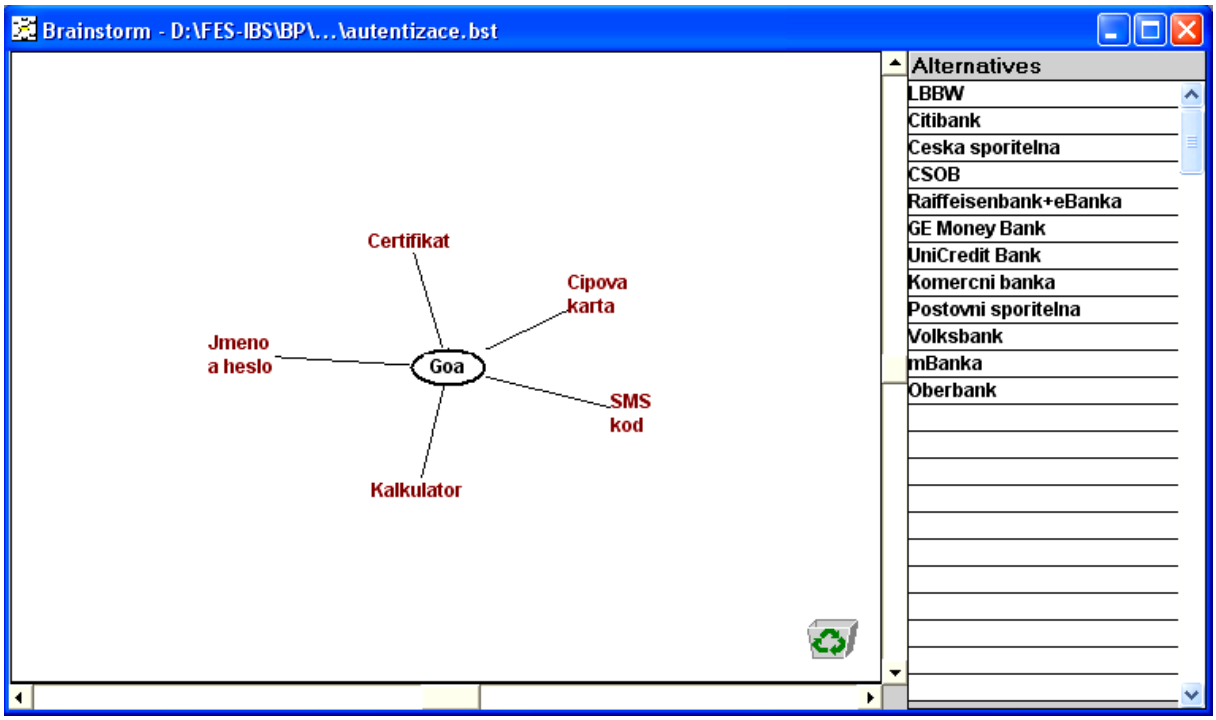
Tabulka 8 - Výsledné skóre Saatyho metody a určení pořadí - autentizace

Bankovní instituce	Skóre	Pořadí
Raiffeisenbank+eBanka	0,159	**1**
UniCredit Bank	0,159	**1**
Česká spořitelna	0,125	**2**
LBBW	0,125	**2**
Komerční banka	0,102	**3**
Citibank	0,101	**4**
GE Money Bank	0,081	**5**
ČSOB	0,046	**6**
Volksbank	0,033	**7**
Poštovní spořitelna	0,023	**8**
mBank	0,023	**8**
Oberbank	0,023	**8**

Zdroj: autor

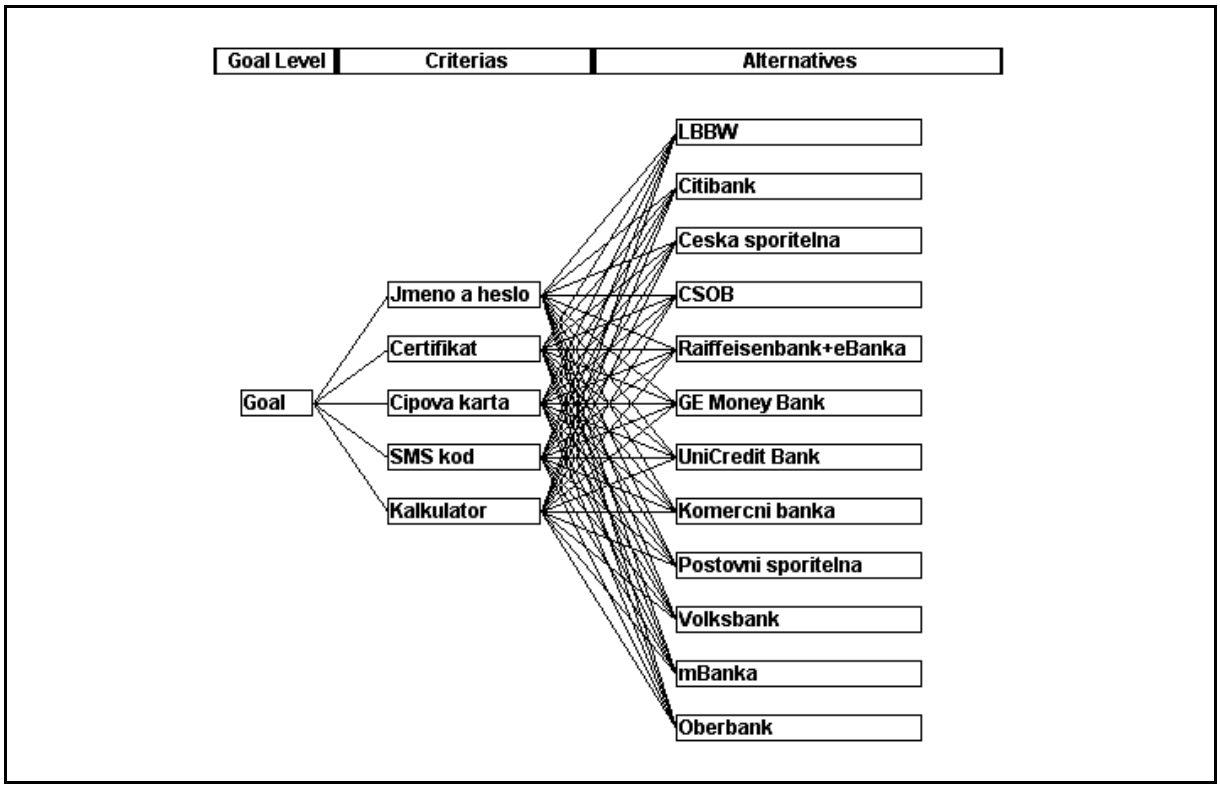
4.1.3. Metoda AHP v programu CDP

Jako poslední metoda byla zvolena metoda AHP v programu CDP verze 3.0.4/S. Zde bylo zapotřebí nejprve zapojit prvky (kritéria) do rozhodovacího systému v programovém okně Brainstorm a vyplnit alternativy pro rozhodování (viz Obrázek 10).



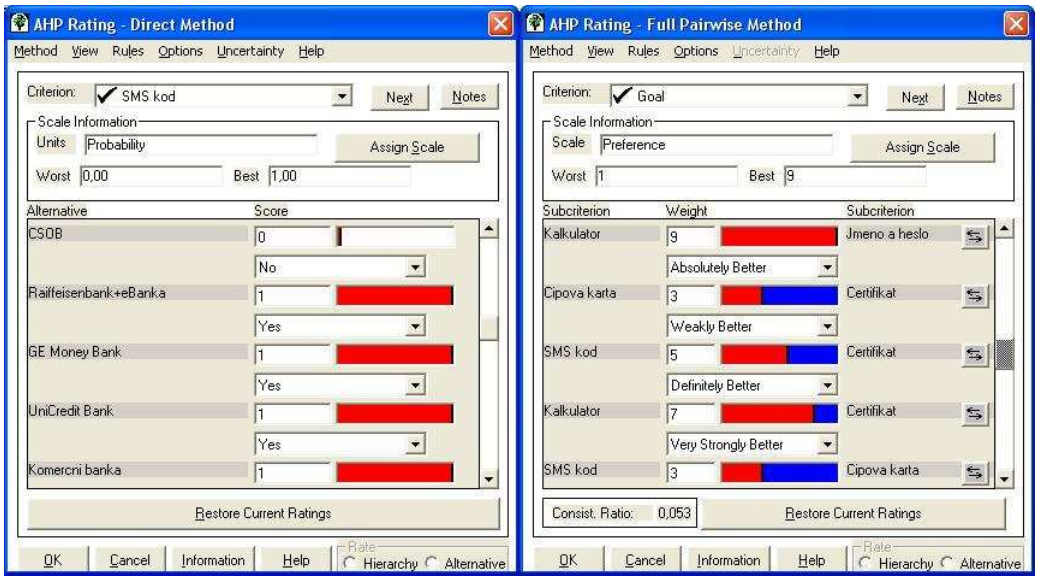
Obrázek 10 - Brainstorm - autentizace. Zdroj: autor

Poté následovalo vytvoření hierarchického modelu rozhodování - Hierarchy. Ten propojil samotná kritéria se všemi alternativami (Obrázek 11).



Obrázek 11 - Hierachický model - autentizace. Zdroj: autor

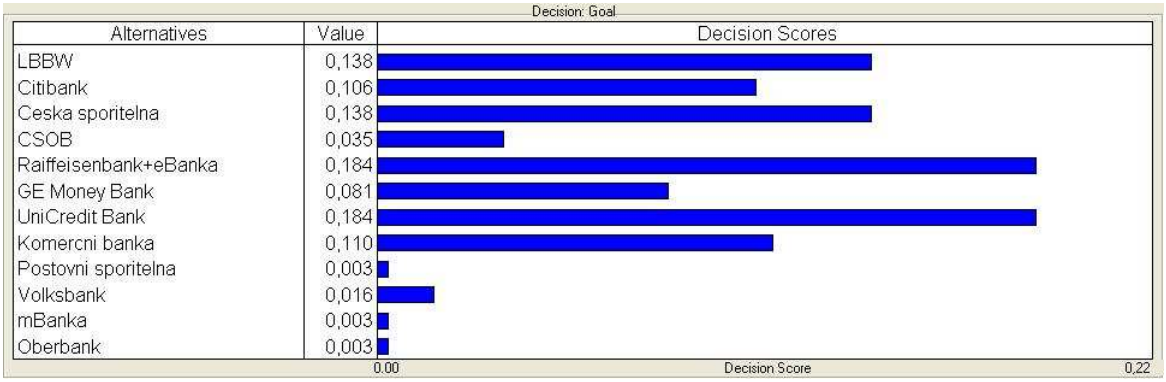
Poté bylo zapotřebí vyplnit hodnoty kritérií u jednotlivých alternativ dle zdrojové tabulky a obdobně jako u Saatyho metody doplnit váhy kritérií. V mém případě se jednalo opět o rozmezí 1 - 9 se stejnými parametry jako v předchozí metodě (Obrázek 12).



Obrázek 12 - Vyplnění hodnot kriterií u alternativ a určení vah kritérií - autentizace. Zdroj: autor

Program CDP také umožňuje výpočet a zobrazení hodnoty indexu konzistence (Consist. Ratio) v okně pro zadávání vah kritérií (Goal). Tato hodnota se, v mém případě, zastavila na

čísle **0,053**, což splňuje podmínku ≤ 0,1. Poté už jen stačilo zobrazit výsledné skóre, které je vidět na následujícím obrázku (Obrázek 13).



Obrázek 13 - Výsledné skóre v CDP - autentizace. Zdroj: autor

Podle výsledného skóre z programu CDP byly bankovní instituce seřazeny a bylo jim přiděleno pořadí, což je patrné z následující tabulky 9.

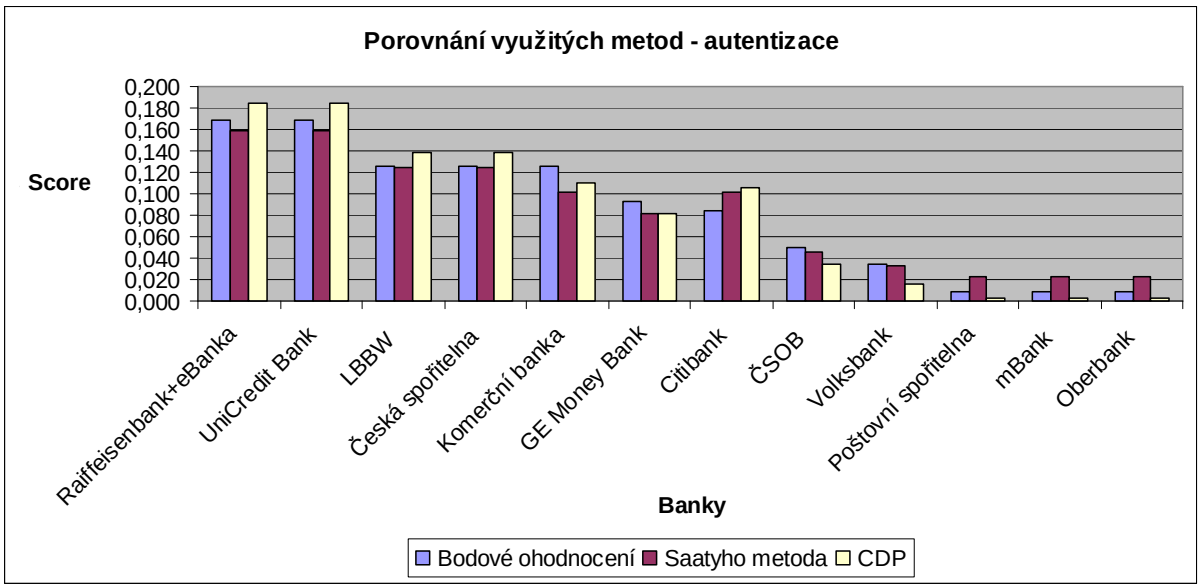
Tabulka 9 - Výsledná skóre metody AHP v CDP a určení pořadí - autentizace

Bankovní instituce	Skóre	Pořadí
Raiffeisenbank+eBanka	0,184	**1**
UniCredit Bank	0,184	**1**
LBBW	0,138	**2**
Česká spořitelna	0,138	**2**
Komerční banka	0,110	**3**
Citibank	0,106	**4**
GE Money Bank	0,081	**5**
ČSOB	0,035	**6**
Volksbank	0,016	**7**
Poštovní spořitelna	0,003	**8**
mBank	0,003	**8**
Oberbank	0,003	**8**

Zdroj: autor

4.1.4. Porovnání využitých metod

Pro přehlednost a shrnutí výsledků využitých metod byly výsledná skóre zobrazena v jednotném grafu (Obrázek 14). Z tohoto grafu je patrné, že pořadí jednotlivých bankovních institucí se na prvních dvou a na posledních třech místech neměnilo. Zato na ostatních místech, dle použité metody, docházelo k menším změnám pořadí.



Obrázek14 - Porovnání výsledných skóre u použitých metod - autentizace. Zdroj: autor

4.2. Porovnání autorizačních prvků

Porovnání autorizačních prvků probíhalo analogicky jako u porovnávání autentizačních prvků. Porovnány byly ty samé bankovní instituce a bylo využito taktéž tří metod pro podporu rozhodování. Zdrojová data (autorizační prvky u bankovních institucí) jsou znázorněna v tabulce 10.

Tabulka 10 - Poskytované autorizační prvky u vybraných bankovních institucí

	Poskytované autorizační prvky			
Bankovní instituce	**Certifikát**	**Čipová karta**	**SMS kód**	**Kalkulátor**
LBBW		ano		ano
Citibank				ano
Česká spořitelna		ano	ano	ano
ČSOB		ano	ano	
Raiffeisenbank+eBanka	ano		ano	ano
GE Money Bank	ano		ano	
UniCredit Bank				ano
Komerční banka	ano	ano	ano	
Poštovní spořitelna			ano	
Volksbank	ano	ano		
bank			ano	
Oberbank			ano	

Zdroj: [7, 21, 23, 14, 15, 25, 18, 24, 17, 13, 19, 22, 26, 20]. Vlastní zpracování

4.2.1. Metoda bodového ohodnocení

U této metody byly slovní hodnoty opět převedeny na číselné, obdobně jako v předchozím případě a kritéria (autorizační prvky) byla ohodnocena body v rozmezí 1 - 7. Následně bylo k jednotlivým bankovním institucím vypočítán odpovídající počet bodů a ty byly podle nich sestupně seřazeny, viz tabulka 11.

Tabulka 11 - Bodové ohodnocení bankovních institucí - autorizace

Autorizační prvky	Certifikát	Čipová karta	SMS kód	Kalkulátor	
Ohodnocení bezpečnostní úrovně	**1**	**3**	**5**	**7**	**Celkové bodové hodnocení**
Česká spořitelna		1	1	1	**15**
Raiffeisenbank+eBanka	1		1	1	**13**
LBBW		1		1	**10**
Komerční banka	1	1	1		**9**
ČSOB		1	1		**8**
Citibank				1	**7**
UniCredit Bank				1	**7**
GE Money Bank	1		1		**6**
Poštovní spořitelna			1		**5**
mBank			1		**5**
Oberbank			1		**5**
Volksbank	1	1			**4**

Zdroj: autor

Pro lepší porovnání této metody s následujícími bylo výsledné bodové ohodnocení také normalizováno.

Tabulka 12 - Znormování bodového ohodnocení a určení pořadí - autorizace

Bankovní instituce	Skóre	Pořadí
Česká spořitelna	0,160	**1**
Raiffeisenbank+eBanka	0,138	**2**
LBBW	0,106	**3**
Komerční banka	0,096	**4**
ČSOB	0,085	**5**
Citibank	0,074	**6**
UniCredit Bank	0,074	**6**
GE Money Bank	0,064	**7**
Poštovní spořitelna	0,053	**8**
mBank	0,053	**8**
Oberbank	0,053	**8**
Volksbank	0,043	**9**

Zdroj: autor

4.2.2. Saatyho metoda

Samozřejmě i pro autorizační prvky byla jako další metoda porovnání použita Saatyho metoda. Zde byla autorizační kritéria ohodnocena stejným rozsahem jako u bodového ohodnocení, tzn. 1 - 7 a se stejnými vlastnostmi jako u autentizačních prvků. Určení normovaných vah je znázorněno v následující tabulce 13. I v tomto případě bylo zapotřebí ověřit správnost sestavení matice pomocí indexu konzistence. Výsledný index konzistence pro matici normovaných vah vyšel **0,043**, takže byla splněna požadovaná podmínka.

Tabulka 13 - Určení vah kritérií - autorizace

	Certifikát	Čipová karta	SMS kód	Kalkulátor	b_i	Váhy
Certifikát	**1**	1/3	1/5	1/7	0,312	**0,055**
Čipová karta	3	**1**	1/3	1/5	0,669	**0,118**
SMS kód	5	3	**1**	1/3	1,495	**0,263**
Kalkulátor	7	5	3	**1**	3,201	**0,564**

Zdroj: autor

Po aplikaci Saatyho metody na zdrojová data autorizačních prvků a po využití znormovaných vah kritérií bylo vypočítáno skóre a určeno pořadí příslušných bankovních institucí (viz Tabulka 14). Celý výpočet a postup je znázorněn příloze 2.

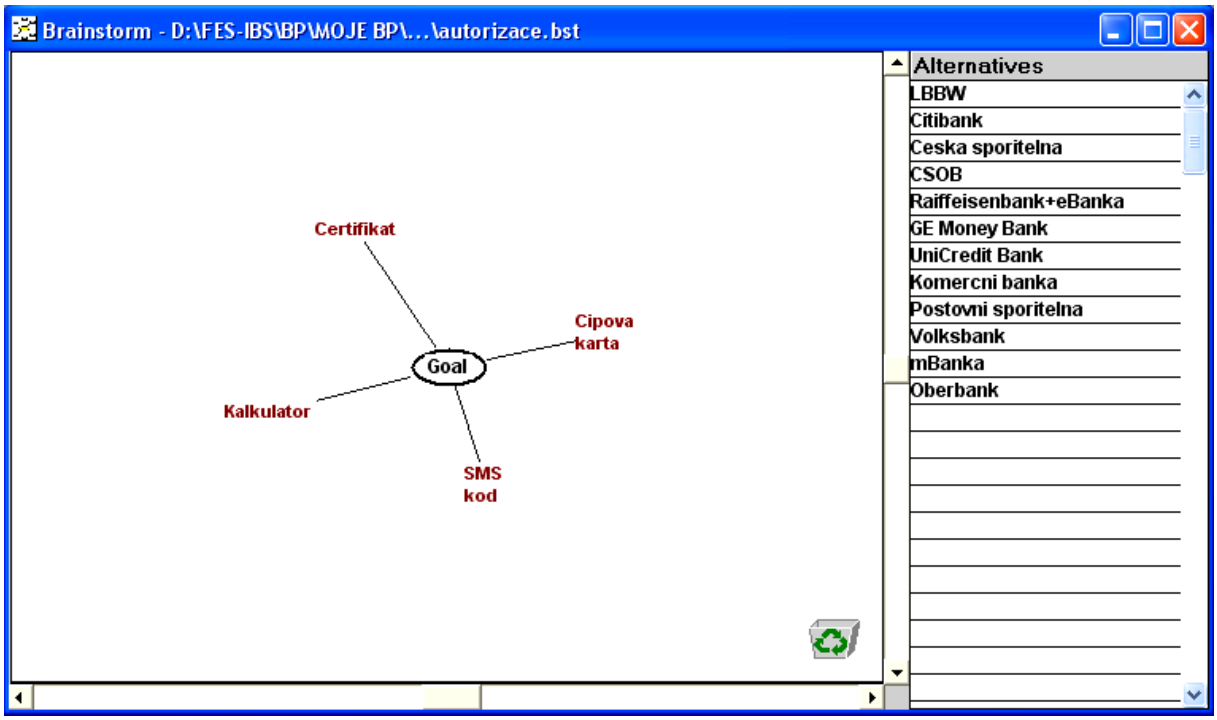
Tabulka 14 - Výsledné skóre Saatyho metody a určení pořadí - autorizace

Bankovní instituce	Skóre	Pořadí
Česká spořitelna	0,150	**1**
Raiffeisenbank+eBanka	0,142	**2**
LBBW	0,123	**3**
Citibank	0,105	**4**
UniCredit Bank	0,105	**4**
Komerční banka	0,074	**5**
ČSOB	0,064	**6**
GE Money Bank	0,056	**7**
Volksbank	0,046	**8**
Poštovní spořitelna	0,046	**8**
mBank	0,046	**8**
Oberbank	0,046	**8**

Zdroj: autor

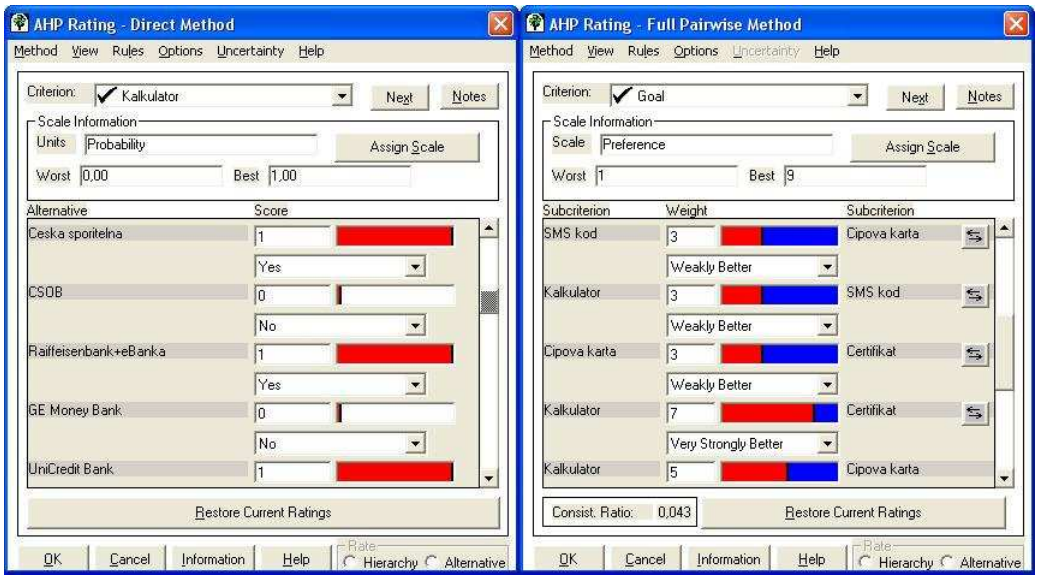
4.2.3. Metoda AHP v programu CDP

Jako poslední byla opět využita metoda AHP v programu CDP, postupovalo se stejně jako v předchozím případě autentizačních prvků. Jediný rozdíl byl ten, že vstupní kritéria (autorizační prvky) byly pouze čtyři, oproti předchozím pěti. Byl opět sestaven rozhodovací systém v okně Brainstorm (viz Obrázek 15).



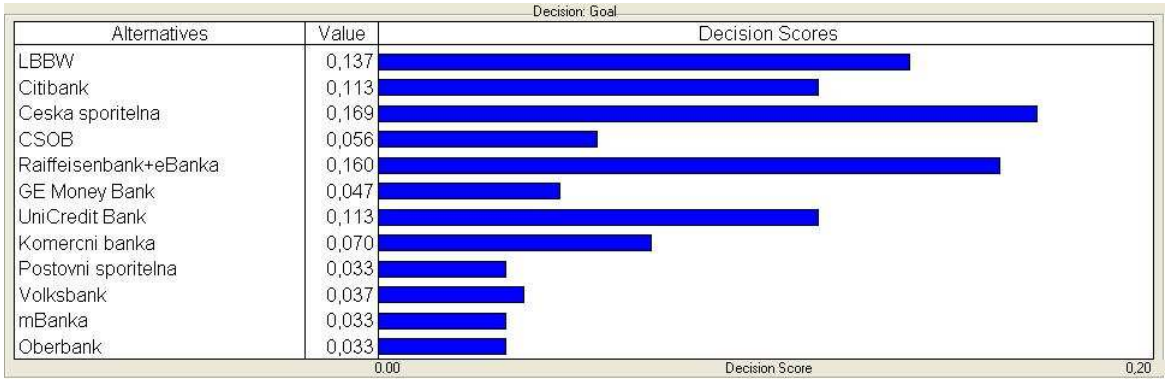
Obrázek 15 - Brainstorm - autorizace. Zdroj: autor

Následně byl vytvořen hierarchický rozhodovací model a poté již mohlo proběhnout samotné zadávání vstupních parametrů pro jednotlivé alternativy u daného kritéria, což je znázorněno na obrázku 16.



Obrázek 16 - Vyplnění hodnot kriterií u alternativ a určení vah kritérií - autorizace. Zdroj: autor

Bylo využito i výpočtu indexu konzistence u stanovení vah kritérií. Tato hodnota opět splňovala podmínku $\leq 0{,}1$ a zároveň se rovnala hodnotě v Saatyho metodě, tzn. **0,043**. Výsledné skóre z programu CDP je znázorněného na obrázku 17.



Obrázek 17 - Výsledné skóre v CDP - autorizace. Zdroj: autor

Pro možnost porovnání s předešlými metodami byly bankovní instituce znovu seřazeny podle výsledného skóre a bylo jim přiděleno příslušné pořadí, což znázorňuje tabulka 15.

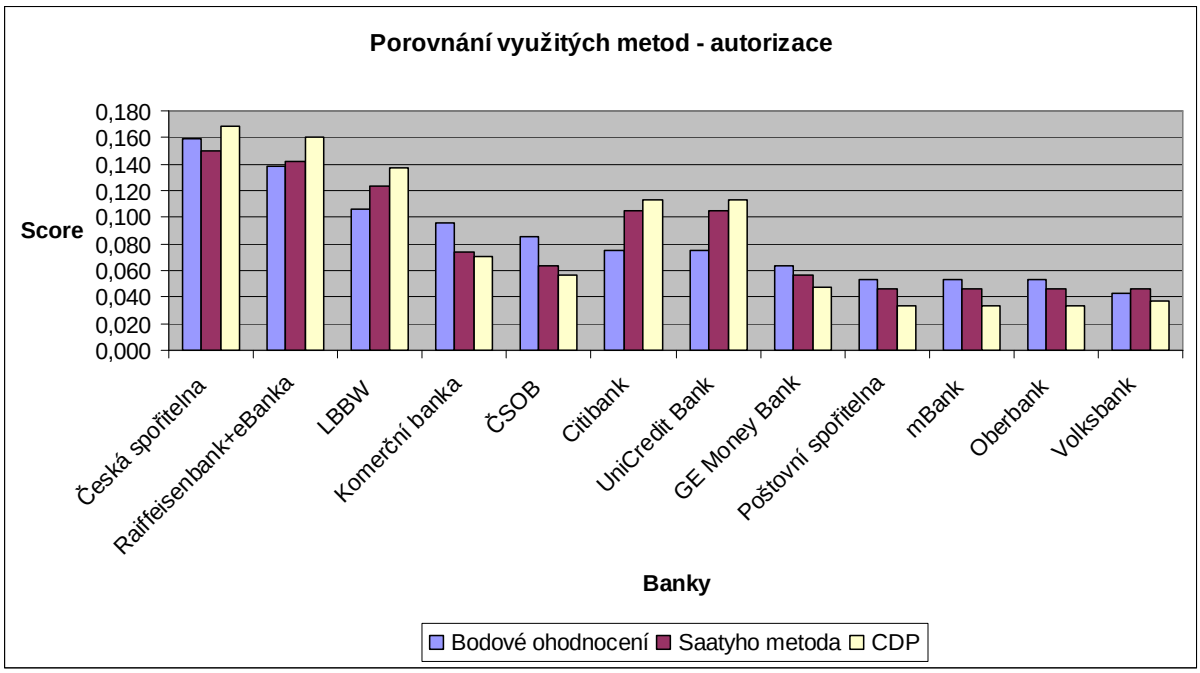
Tabulka 15 - Výsledná skóre metody AHP v CDP a určení pořadí - autorizace

Bankovní instituce	Skóre	Pořadí
Česká spořitelna	0,169	**1**
Raiffeisenbank+eBanka	0,160	**2**
LBBW	0,137	**3**
Citibank	0,113	**4**
UniCredit Bank	0,113	**4**
Komerční banka	0,070	**5**
ČSOB	0,056	**6**
GE Money Bank	0,047	**7**
Volksbank	0,037	**8**
mBank	0,033	**9**
Oberbank	0,033	**9**
Poštovní spořitelna	0,033	**9**

Zdroj: autor

4.2.4. Porovnání využitých metod

I v případě autorizačních prvků byla porovnána výsledná skóre použitých rozhodovacích metod. Zde je patrný obdobný vztah jako u výsledků autentizačních prvků. První tři místa zůstala ve všech metodách obsazena stejně, ovšem na ostatních docházelo k nemalým změnám jako například u Komerční banky či Volksbank. Poměrně dobře je to patrné na následujícím celkovém grafu - Obrázek 18.



Obrázek 18 - Porovnání výsledných skóre u použitých metod - autorizace. Zdroj: autor

4.3. Určení výsledného pořadí

Pro určení výsledného pořadí v zabezpečení internetového bankovnictví byla jednotlivá znormovaná skóre bankovních institucí, jak z autentizačních, tak autorizačních prvků, sečtena a opět znormována. Následně bylo určeno celkové výsledné pořadí. Výsledná skóre, s určením výsledného pořadí, jsou znázorněno v tabulce 16 a samotný postup výpočtu je prezentován v příloze 3.

Tabulka 16 - Celkové skóre zabezpečení a určení celkového pořadí

Bankovní instituce	Výsledné pořadí pro autentizaci	Výsledné pořadí pro autorizaci	Celkové skóre	Celkové pořadí
Raiffeisenbank+eBanka	1	2	0,159	**1**
Česká spořitelna	2	1	0,145	**2**
UniCredit Bank	1	4	0,134	**3**
LBBW	2	3	0,126	**4**
Citibank	4	4	0,097	**5**
Komerční banka	3	5	0,096	**6**
GE Money Bank	5	7	0,070	**7**
ČSOB	6	6	0,056	**8**
Volksbank	7	9	0,035	**9**
Poštovní spořitelna	8	8	0,028	**10**
bank	8	8	0,028	**10**
Oberbank	8	8	0,028	**10**

Zdroj: autor

5. ZÁVĚR

Tato bakalářské práce se zabývá elektronickým bankovnictvím se zaměřením na jeho bezpečnost. Elektronické bankovnictví patří mezi velmi rychle se rozvíjející formy správy financí a to nejen osobních, ale především firemních. Její nespornou výhodou je 24 hodinový přístup ke klientským účtům v bance a tím pádem poskytuje možnost kdykoli a kdekoli využít své finanční prostředky. Další nespornou výhodou těchto bankovních systémů je nízkonákladová správa. Poplatky jsou totiž, při využití elektronického bankovnictví, několikanásobně menší, než při využití služeb bankéře v bance. Tím, že se ale tyto finanční transakce a operace zadávají elektronicky a odesílají se pomocí různých elektronických kanálů, se sice snižuje jejich nákladovost, ale vzniká zde i jisté riziko napadení (získání, pozměnění citlivých informací). Proto jsem se chtěl touto prácí zaměřit na bezpečnostní prvky, které tyto rizika útoku minimalizují.

Jelikož se nacházíme v období krátce po finanční krizi, rozhodl jsem se do této bakalářské práce začlenit i finanční aspekty elektronického bankovnictví. U vybraných dvanácti bankovních institucí ČR byly porovnány poplatky za zřízení a vedení služeb. Stěžejní částí této práce je však bezpečnost, analyzoval jsem proto bezpečnostní prvky u nejvyužívanějšího elektronického bankovnictví, což je bezesporu internetové. I v tomto případě jsem porovnával dvanáct bankovních institucí, které pokrývají převážnou většinu bankovního trhu v ČR.

Při porovnání finanční nákladnosti elektronického bankovnictví u vybraných bankovních institucí byla u každé instituce zjištěna průměrná výše poplatků za dané poskytované služby. Nulové náklady byly zjištěny u těchto bankovních institucí: Citibank, LBBW, mBanka, Oberbank a Poštovní spořitelna. Nejvyšší měsíční poplatky, ve výši několika desítek korun, klienti zaplatí u UniCredit Bank a Raiffeisenbank+eBank. Podrobnější informace o poplatcích a výsledky zjištěných hodnot jsou zobrazeny v tabulce 2.

U porovnání zabezpečení bylo použito tří rozhodovacích metod (Bodové ohodnocení a Saatyho metoda s využitím programu MS Office Excel 2003 a metoda AHP v programu CDP). Z těchto výpočtů bylo vyvozeno, že nejbezpečnějšími bankovními institucemi jsou Raiffeisenbank+eBank, Česká spořitelna a UniCredit Bank. Nejhůře na tom, v oblasti bezpečnosti, obstály Poštovní spořitelna, mBanka a Oberbank. Z výsledků je patrná jistá závislost mezi výší poplatků a úrovní zabezpečení tzn., že čím jsou poplatky za služby vyšší, tím jsou i bezpečnostní prvky kvalitnější, což je podle mne pochopitelné. Postupy výpočtů a výsledky jsou popsány v kapitole 4, podrobnější výpočty byly umístěny do přílohy bakalářské práce (Příloha 1 - 3).

SEZNAM LITERATURY

Monografie

[1] DOSTÁLEK, Libor; VOHNOUTOVÁ, Marta. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. První. Praha: Computer Press, a.s., 2006. 534 s. ISBN 80-251-0828-7.

[2] DOSTÁLEK, Libor, et al. *Velký průvodce TCP/IP: Bezpečnost*. První. Praha : Computer Press, a.s., 2001. 565 s. ISBN 80-7226-513-X.

[3] FOTR, Jiří, et al. *Manažerské rozhodování : Postupy, metody, nástroje*. Vyd. 1. Praha : Ekopress, 2006. 409 s. ISBN 80-86929-15-9.

[4] HEFFERNAN, Shelagh. *Modern banking*. 1st edition. Chichester : John Wiley & Sons, 2005. 716 s. ISBN 0-470-09500-8.

[5] MÁČE, Miroslav. *Platební styk: Klasický a elektronický*. 1. vydání. Praha : Grada, 2006. 220 s. ISBN 80-247-1725-5.

[6] MACHKOVÁ, Hana, et al. *Mezinárodní obchodní operace*. První. Praha : Grada Publishing a.s., 2007. 244 s. ISBN 978-80-247-1590-2.

[7] MATYÁŠ, Vašek, et al. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. 1. vydání. Brno: Masarykova univerzita, 2008. 125 s. ISBN 978-80-210-4556-9.

[8] PŘÁDKA, Michal; KALA, Jan. *Elektronické bankovnictví*. První. Praha : Computer Press, a.s., 2000. 166 s. ISBN 80-7226-328-5.

[9] ZELENKA, Josef, ČAPEK, Jan, et al. *Ochrana dat: Kryptologie*. První. Hradec Králové: GAUDEAMUS, 2003. 198 s. ISBN 80-7041-737-4.

Webové stránky

[10] *A&&L Soft: Autentizační kalkulátory* [online].A&&L Soft, s.r.o., 2000-2010 [cit. 2010-02-12]. Bezpečnostní technologie. Dostupné z WWW: <http://www.alsoft.cz/cz/Products/Security/Security-Technology/Authentication-Tokens/>.

[11] *Adaptic* [online].Adaptic s.r.o., 2005-2009 [cit. 2009-11-07]. Co je to E-bussiness. Dostupné z WWW: <http://www.adaptic.cz/znalosti/slovnicek/e-business.htm>.

[12] *Adaptic* [online].Adaptic s.r.o., 2005-2009 [cit. 2010-03-06]. Co je to E-commerce?. Dostupné z WWW: <http://www.adaptic.cz/znalosti/slovnicek/e-commerce.htm>.

[13] *City Česká republika* [online].Citigroup Inc., 2009 [cit. 2010-01-27]. Internetové bankovnictví. Dostupné z WWW: <http://www.citibank.cz/czech/consumer-banking/czech/bankovnictvi/internetove.htm>.

[14] *Česká spořitelna: Přímé bankovnictví* [online]. Česká spořitelna, [2009] [cit. 2009-11-02]. Dostupný z WWW: <http://www.csas.cz/banka/menu/cs/lide/nav00000_lide_nds_13>.

[15] *ČSOB: Elektronické bankovnictví* [online]. ČSOB, 2009 [cit. 2009-11-02]. Dostupný z WWW: <http://www.csob.cz/cz/Lide/Elektronicke-bankovnictvi/Stranky/default.aspx>.

[16] *FastCentrik* [online].NetDirect s.r.o., 2009 [cit. 2009-11-07]. E-bussiness. Dostupné z WWW: <http://www.fastcentrik.cz/slovnik-pojmu/e-business.aspx>.

[17] *GE Money CZ* [online]. GE Money, 2001-2010 [cit. 2010-01-27]. Účty pro podnikatele a banky. Dostupné z WWW: <http://www.gemoney.cz/ge/cz/2/ucty>.

[18] *Komerční banka* [online]. Komerční banka, 2006 [cit. 2010-01-27]. Přímé bankovnictví. Dostupné z WWW: <http://www.mojebanka.cz/>.

[19]LBBW. *LBBW Bank CZ* [online]. 2007 [cit. 2010-03-10]. Elektronické bankovnictví. Dostupné z WWW: <http://www.lbbw.cz/cs/nasi-klienti/podnikatele-a-male-firmy/elektronicke-bankovnictvi/index.shtml>.

[20] *MBank* [online].Intercon, 1999-2007, 01-03-2010 [cit. 2010-03-10]. O službách. Dostupné z WWW: <http://www.mbank.cz/pruvodce/sluzby/#tabs=0>.

[21] *Měšec* [online]. 1998-2010, 13.3.2010 [cit. 2010-03-16]. Přímé bankovnictví - srovnání. Dostupné z WWW: <http://www.mesec.cz/produkty/prime-bankovnictvi/>. ISSN 1213-4414.

[22] Oberbank. *Oberbank AG* [online]. 2006 [cit. 2010-03-10]. Informace o produktu. Dostupné z WWW: <http://www.oberbank.cz/oberbank.asp?menue=/webNav.asp%3Fcode%3DeBanking%20CZ%26database=www&content=/obkhome/263.asp>.

[23] *Poštovní spořitelna: Elektronické bankovnictví* [online]. Poštovní spořitelna, 2009 [cit. 2009-11-02]. Dostupný z WWW: <http://www.postovnisporitelna.cz/Obcane/ucty-a-platby/elektronicke-bankovnictvi/Stranky/default.aspx>.

[24] *Raiffeisenbank* [online]. Raiffeisenbank, 2008 [cit. 2010-01-27]. O internetovém bankovnictví. Dostupné z WWW: <http://www.rb.cz/firemni-finance/podnikatele-a-male-firmy/prime-bankovnictvi/sluzby-pro-firemni-ucty/>.

[25] *UniCredit Bank* [online].UniCredit Bank Czech Republic, a.s., 2010 [cit. 2010-01-27]. Přímé bankovnictví. Dostupné z WWW: <http://www.unicreditbank.cz/cz/obcane/prime-bankovnictvi.html>.

[26] Volksbank CZ. *Volksbank* [online]. 2005 [cit. 2010-03-10]. Elektronické bankovnictví. Dostupné z WWW: <http://www.volksbank.cz/vb/jnp/cz/podnikatele/elektronicke_bankovnictvi/index.html>.

Elektronické články

[27] Cenzin. *Web Aplication Security Trends Report* [online]. Q1-Q2 2009, 1, [cit. 2010-02-14]. Dostupný z WWW: <http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q1-Q2-2009.pdf>.

[28] Česká spořitelna. Uživatelský manuál SERVIS 24 Internetbanking : Autorizace transakce pomocí autentizačního kalkulátoru. *Uživatelský manuál* [online]. 25.11.2009, 1, [cit. 2010-02-21]. Dostupný z WWW: <https://www.servis24.cz/stat/ebanking/s24/help/cs/ib_hlp_cic_autpakal.html>.

[29] ČTK. *Finanční Noviny: SBK: Počet platebních karet se přiblížil počtu obyvatel ČR* [online]. Neris, s.r.o., 2009, 21.12.2008 14:53 [cit. 2009-11-01]. Dostupný z WWW: <http://www.financninoviny.cz/zpravy/sbk-pocet-platebnich-karet-se-priblizil-poctu-obyvatel-cr/351208&id_seznam=5098>.

[30] *Historie platebních karet* [online]. AWD Česká republika s.r.o., 2000-2009 [cit. 2009-10-27]. Dostupný z WWW: <http://www.finance.cz/bankovnictvi/informace/platebni-karty/historie/>.

[31] HULÁN, Radek. Opera Software jako jediná opravuje 100% chyb. *MyEgo* [online]. 31.1.2007, 1, [cit. 2010-02-14]. Dostupný z WWW: <http://myego.cz/item/opera-software-jako-jedina-opravuje-100-chyb>.

[32] LORENC, David, PIKÁLEK, David. *Pohled banky na bezpečnost přímého bankovnictví* [online]. Česká spořitelna, 26.2.2009 [cit. 2009-10-25]. Dostupný z WWW: <http://i.iinfo.cz/urs-att/David_Pikalek_a_David_Lorenc_-_Moznosti_zabezpeceni_primeho_bankovnictvi-123572814286074.ppt>.

[33] [MINIBERGER, B. Elektronické bankovnictví. *Seminář pro studenty BIVŠ obor IT a EO* [online]. 2007, 1, [cit. 2010-02-24]. Dostupný z WWW: <http://is.bivs.cz/el/6110/zima2008/B107EBA/Elektronicke_bankovnictvi_2007.pdf>.]

[34] NEZBEDA, Ondřej. Bankomat svět: Už před sedmdesáti lety si lidé mohli vybírat peníze skrz zeď. *RESPEKT.CZ* [online]. 30.8.2009, 8, [cit. 2009-11-06]. Dostupný z WWW: <http://respekt.ihned.cz/c1-38170690-bankomat-svet>.

[35] NMS. *Trendy elektronického bankovnictví* [online]. Praha : ČSOB a.s., 26.červenec 2006 [cit. 2009-10-25]. Dostupný z WWW: <http://www.csob.cz/WebCsob/Csob/Servis-pro-media/PB_CSOB_ELB_vysledky_studie_NMS.pdf>.

[36] Report. *Secunia* [online]. 2008, 1, [cit. 2010-02-14]. Dostupný z WWW: <http://secunia.com/gfx/Secunia2008Report.pdf>.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

SEZNAM ZKRATEK

AES - Advanced Encryption Standard

AHP - Analytic Hierarchy Process

ATM - Automatic Teller Machine

B2C - Business to Customers

CD - Compact Disc

CDP - Criterium DecisionPlus

ČR - Česká republika

ČS - Česká spořitelna

ČSOB - Československá obchodní banka

DES - Data Encryption Standard

DSA - Digital Signature Algorithm

ECDSA - The Elliptic Curve Digital Signature Algorithm

EDI - Electronic Data Interchang

EDIFACT - Electronic Data Interchange For Administration, Commerce, and Transport

ERP - Enterprise Resource Planning

GSM - Global System for Mobile Communications

HTTP - Hypertext Transfer Protocol

IDEA - International Data Encryption Algorithm

LBBW - Landesbank Baden-Württemberg

MD-5 - Message Digest algorithm - 5

PC - Personal computer

PDA - Personal Digital Assistant

PIN - Personal Identification Number

PS - Poštovní spořitelna

RSA - Rivest-Shamir-Adelman

SBK - Sdružení pro bankovní karty

SHA - Secure Hash Algorithm

SIM - Subscriber Identity Module

SMS - Short Message Service

SSL - Secure Sockets Layer

TAN - Transaction Authentication Number

TV - Television

URL - Uniform Resource Locator

PŘÍLOHA

Příloha 1 - Výpočet Saatyho metodou - autentizace

		k1	k2	k3	k4	k5
		Jméno a heslo	**Certifikát**	**Čipová karta**	**SMS kód**	**Kalkulátor**
a1	**LBBW**	ano		ano		ano
a2	**Citibank**	ano				ano
a3	**Česká spořitelna**	ano		ano		ano
a4	**ČSOB**	ano		ano		
a5	**Raiffeisenbank+eBanka**	ano	ano		ano	ano
a6	**GE Money Bank**	ano	ano		ano	
a7	**UniCredit Bank**	ano	ano		ano	ano
a8	**Komerční banka**		ano	ano	ano	
a9	**Poštovní spořitelna**	ano				
a10	**Volksbank**	ano	ano			
a11	**mBank**	ano				
a12	**Oberbank**	ano				

													Geometrický průměr	**Znormovaná data**
k1	**a1**	**a2**	**a3**	**a4**	**a5**	**a6**	**a7**	**a8**	**a9**	**a10**	**a11**	**a12**	**bi**	**vi**
a1	**1**	1	1	1	1	1	1	9	1	1	1	1	1,201	0,090
a2	1	**1**	1	1	1	1	1	9	1	1	1	1	1,201	0,090
a3	1	1	**1**	1	1	1	1	9	1	1	1	1	1,201	0,090
a4	1	1	1	**1**	1	1	1	9	1	1	1	1	1,201	0,090
a5	1	1	1	1	**1**	1	1	9	1	1	1	1	1,201	0,090
a6	1	1	1	1	1	**1**	1	9	1	1	1	1	1,201	0,090
a7	1	1	1	1	1	1	**1**	9	1	1	1	1	1,201	0,090
a8	1/9	1/9	1/9	1/9	1/9	1/9	1/9	**1**	1/9	1/9	1/9	1/9	0,133	0,010
a9	1	1	1	1	1	1	1	9	**1**	1	1	1	1,201	0,090
a10	1	1	1	1	1	1	1	9	1	**1**	1	1	1,201	0,090
a11	1	1	1	1	1	1	1	9	1	1	**1**	1	1,201	0,090
a12	1	1	1	1	1	1	1	9	1	1	1	**1**	1,201	0,090
													13,344	1,000
			λ_{max}	12									KI	0,000

k2	**a1**	**a2**	**a3**	**a4**	**a5**	**a6**	**a7**	**a8**	**a9**	**a10**	**a11**	**a12**	**bi**	**vi**
a1	**1**	1	1	1	1/9	1/9	1/9	1/9	1	1/9	1	1	0,400	0,019
a2	1	**1**	1	1	1/9	1/9	1/9	1/9	1	1/9	1	1	0,400	0,019
a3	1	1	**1**	1	1/9	1/9	1/9	1/9	1	1/9	1	1	0,400	0,019
a4	1	1	1	**1**	1/9	1/9	1/9	1/9	1	1/9	1	1	0,400	0,019
a5	9	9	9	9	**1**	1	1	1	9	1	9	9	3,603	0,173
a6	9	9	9	9	1	**1**	1	1	9	1	9	9	3,603	0,173
a7	9	9	9	9	1	1	**1**	1	9	1	9	9	3,603	0,173
a8	9	9	9	9	1	1	1	**1**	9	1	9	9	3,603	0,173
a9	1	1	1	1	1/9	1/9	1/9	1/9	**1**	1/9	1	1	0,400	0,019
a10	9	9	9	9	1	1	1	1	9	**1**	9	9	3,603	0,173
a11	1	1	1	1	1/9	1/9	1/9	1/9	1	1/9	**1**	1	0,400	0,019
a12	1	1	1	1	1/9	1/9	1/9	1/9	1	1/9	1	**1**	0,400	0,019
													20,816	1,000
			λ_{max}	12									KI	0,000

k3	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	bi	vi
a1	**1**	9	1	1	9	9	9	1	9	9	9	9	4,327	0,205
a2	1/9	**1**	1/9	1/9	1	1	1	1/9	1	1	1	1	0,481	0,023
a3	1	9	**1**	1	9	9	9	1	9	9	9	9	4,327	0,205
a4	1	9	1	**1**	9	9	9	1	9	9	9	9	4,327	0,205
a5	1/9	1	1/9	1/9	**1**	1	1	1/9	1	1	1	1	0,481	0,023
a6	1/9	1	1/9	1/9	1	**1**	1	1/9	1	1	1	1	0,481	0,023
a7	1/9	1	1/9	1/9	1	1	**1**	1/9	1	1	1	1	0,481	0,023
a8	1	9	1	1	9	9	9	**1**	9	9	9	9	4,327	0,205
a9	1/9	1	1/9	1/9	1	1	1	1/9	**1**	1	1	1	0,481	0,023
a10	1/9	1	1/9	1/9	1	1	1	1/9	1	**1**	1	1	0,481	0,023
a11	1/9	1	1/9	1/9	1	1	1	1/9	1	1	**1**	1	0,481	0,023
a12	1/9	1	1/9	1/9	1	1	1	1/9	1	1	1	**1**	0,481	0,023
													21,153	1,000
			λ_{max}	12									KI	0,000

k4	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	bi	vi
a1	**1**	1	1	1	1/9	1/9	1/9	1/9	1	1	1	1	0,481	0,023
a2	1	**1**	1	1	1/9	1/9	1/9	1/9	1	1	1	1	0,481	0,023
a3	1	1	**1**	1	1/9	1/9	1/9	1/9	1	1	1	1	0,481	0,023
a4	1	1	1	**1**	1/9	1/9	1/9	1/9	1	1	1	1	0,481	0,023
a5	9	9	9	9	**1**	1	1	1	9	9	9	9	4,327	0,205
a6	9	9	9	9	1	**1**	1	1	9	9	9	9	4,327	0,205
a7	9	9	9	9	1	1	**1**	1	9	9	9	9	4,327	0,205
a8	9	9	9	9	1	1	1	**1**	9	9	9	9	4,327	0,205
a9	1	1	1	1	1/9	1/9	1/9	1/9	**1**	1	1	1	0,481	0,023
a10	1	1	1	1	1/9	1/9	1/9	1/9	1	**1**	1	1	0,481	0,023
a11	1	1	1	1	1/9	1/9	1/9	1/9	1	1	**1**	1	0,481	0,023
a12	1	1	1	1	1/9	1/9	1/9	1/9	1	1	1	**1**	0,481	0,023
													21,153	1,000
			λ_{max}	12									KI	0,000

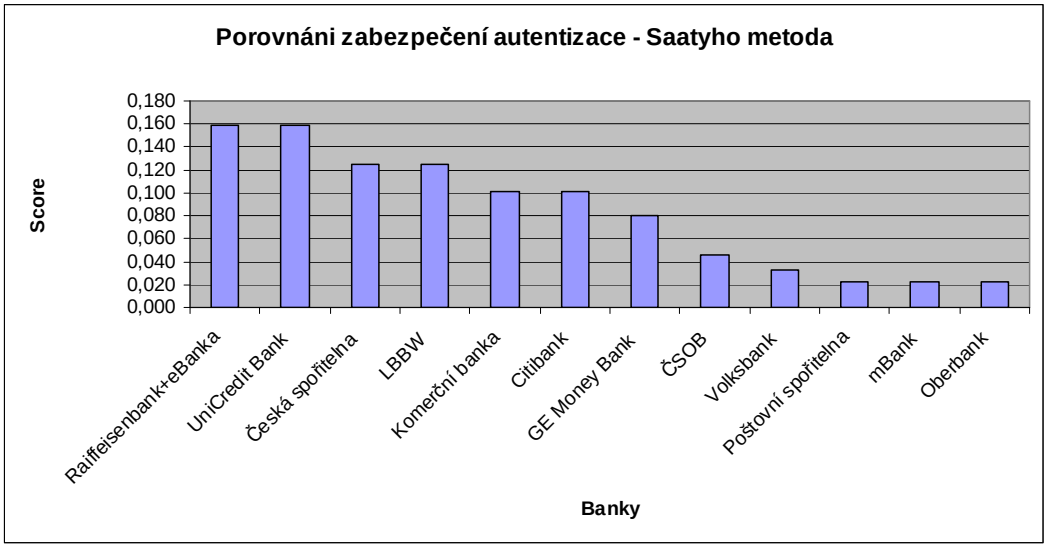
k5	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	bi	vi
a1	**1**	1	1	9	1	9	1	9	9	9	9	9	3,603	0,173
a2	1	**1**	1	9	1	9	1	9	9	9	9	9	3,603	0,173
a3	1	1	**1**	9	1	9	1	9	9	9	9	9	3,603	0,173
a4	1/9	1/9	1/9	**1**	1/9	1	1/9	1	1	1	1	1	0,400	0,019
a5	1	1	1	9	**1**	9	1	9	9	9	9	9	3,603	0,173
a6	1/9	1/9	1/9	1	1/9	**1**	1/9	1	1	1	1	1	0,400	0,019
a7	1	1	1	9	1	9	**1**	9	9	9	9	9	3,603	0,173
a8	1/9	1/9	1/9	1	1/9	1	1/9	**1**	1	1	1	1	0,400	0,019
a9	1/9	1/9	1/9	1	1/9	1	1/9	1	**1**	1	1	1	0,400	0,019
a10	1/9	1/9	1/9	1	1/9	1	1/9	1	1	**1**	1	1	0,400	0,019
a11	1/9	1/9	1/9	1	1/9	1	1/9	1	1	1	**1**	1	0,400	0,019
a12	1/9	1/9	1/9	1	1/9	1	1/9	1	1	1	1	**1**	0,400	0,019
													20,816	1,000
			λ_{max}	12									KI	0,000

Ohodnocení vah kritérií							
	k1	k2	k3	k4	k5	Geometrický průměr	Váhy
k1	1	1/3	1/5	1/7	1/9	0,254	0,033
k2	3	1	1/3	1/5	1/7	0,491	0,064
k3	5	3	1	1/3	1/5	1,000	0,130
k4	7	5	3	1	1/3	2,036	0,264
k5	9	7	5	3	1	3,936	0,510
						7,718	1,000

λ_{max}	5,276	KI	0,069

Kritérium	Váhy	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	
k1	0,033	0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,010	0,090	0,090	0,090	0,090	
k2	0,064	0,019	0,019	0,019	0,019	0,173	0,173	0,173	0,173	0,019	0,173	0,019	0,019	
k3	0,130	0,205	0,023	0,205	0,205	0,023	0,023	0,023	0,205	0,023	0,023	0,023	0,023	
k4	0,264	0,023	0,023	0,023	0,023	0,205	0,205	0,205	0,205	0,023	0,023	0,023	0,023	
k5	0,510	0,173	0,173	0,173	0,019	0,173	0,019	0,173	0,019	0,019	0,019	0,019	0,019	
														Kontrolní součet
Celkové ohodnocení		0,125	0,101	0,125	0,046	0,159	0,081	0,159	0,102	0,023	0,033	0,023	0,023	1,000

	Název	Score	Pořadí
a5	Raiffeisenbank+eBanka	0,159	1
a7	UniCredit Bank	0,159	1
a3	Česká spořitelna	0,125	2
a1	LBBW	0,125	2
a8	Komerční banka	0,102	3
a2	Citibank	0,101	4
a6	GE Money Bank	0,081	5
a4	ČSOB	0,046	6
a10	Volksbank	0,033	7
a9	Poštovní spořitelna	0,023	8
a11	mBank	0,023	8
a12	Oberbank	0,023	8



Příloha 2 - Výpočet Saatyho metodou - autorizace

		k1	k2	k3	k4
		Certifikát	**Čipová karta**	**SMS kód**	**Kalkulátor**
a1	**LBBW**		ano		ano
a2	**Citibank**				ano
a3	**Česká spořitelna**		ano	ano	ano
a4	**ČSOB**		ano	ano	
a5	**Raiffeisenbank+eBanka**	ano		ano	ano
a6	**GE Money Bank**	ano		ano	
a7	**UniCredit Bank**				ano
a8	**Komerční banka**	ano	ano	ano	
a9	**Poštovní spořitelna**			ano	
a10	**Volksbank**	ano	ano		
a11	**mBank**			ano	
a12	**Oberbank**			ano	

													Geometrický průměr	**Znormovaná data**
k1	**a1**	**a2**	**a3**	**a4**	**a5**	**a6**	**a7**	**a8**	**a9**	**a10**	**a11**	**a12**	**bi**	**vi**
a1	**1**	1	1	1	1/9	1/9	1	1/9	1	1/9	1	1	0,481	0,023
a2	1	**1**	1	1	1/9	1/9	1	1/9	1	1/9	1	1	0,481	0,023
a3	1	1	**1**	1	1/9	1/9	1	1/9	1	1/9	1	1	0,481	0,023
a4	1	1	1	**1**	1/9	1/9	1	1/9	1	1/9	1	1	0,481	0,023
a5	9	9	9	9	**1**	1	9	1	9	1	9	9	4,327	0,205
a6	9	9	9	9	1	**1**	9	1	9	1	9	9	4,327	0,205
a7	1	1	1	1	1/9	1/9	**1**	1/9	1	1/9	1	1	0,481	0,023
a8	9	9	9	9	1	1	9	**1**	9	1	9	9	4,327	0,205
a9	1	1	1	1	1/9	1/9	1	1/9	**1**	1/9	1	1	0,481	0,023
a10	9	9	9	9	1	1	9	1	9	**1**	9	9	4,327	0,205
a11	1	1	1	1	1/9	1/9	1	1/9	1	1/9	**1**	1	0,481	0,023
a12	1	1	1	1	1/9	1/9	1	1/9	1	1/9	1	**1**	0,481	0,023
													21,153	1,000
			λ_{max}	12									KI	0,000

k2	**a1**	**a2**	**a3**	**a4**	**a5**	**a6**	**a7**	**a8**	**a9**	**a10**	**a11**	**a12**	**bi**	**vi**
a1	**1**	9	1	1	9	9	9	1	9	1	9	9	3,603	0,173
a2	1/9	**1**	1/9	1/9	1	1	1	1/9	1	1/9	1	1	0,400	0,019
a3	1	9	**1**	1	9	9	9	1	9	1	9	9	3,603	0,173
a4	1	9	1	**1**	9	9	9	1	9	1	9	9	3,603	0,173
a5	1/9	1	1/9	1/9	**1**	1	1	1/9	1	1/9	1	1	0,400	0,019
a6	1/9	1	1/9	1/9	1	**1**	1	1/9	1	1/9	1	1	0,400	0,019
a7	1/9	1	1/9	1/9	1	1	**1**	1/9	1	1/9	1	1	0,400	0,019
a8	1	9	1	1	9	9	9	**1**	9	1	9	9	3,603	0,173
a9	1/9	1	1/9	1/9	1	1	1	1/9	**1**	1/9	1	1	0,400	0,019
a10	1	9	1	1	9	9	9	1	9	**1**	9	9	3,603	0,173
a11	1/9	1	1/9	1/9	1	1	1	1/9	1	1/9	**1**	1	0,400	0,019
a12	1/9	1	1/9	1/9	1	1	1	1/9	1	1/9	1	**1**	0,400	0,019
													20,816	1,000
			λ_{max}	12									KI	0,000

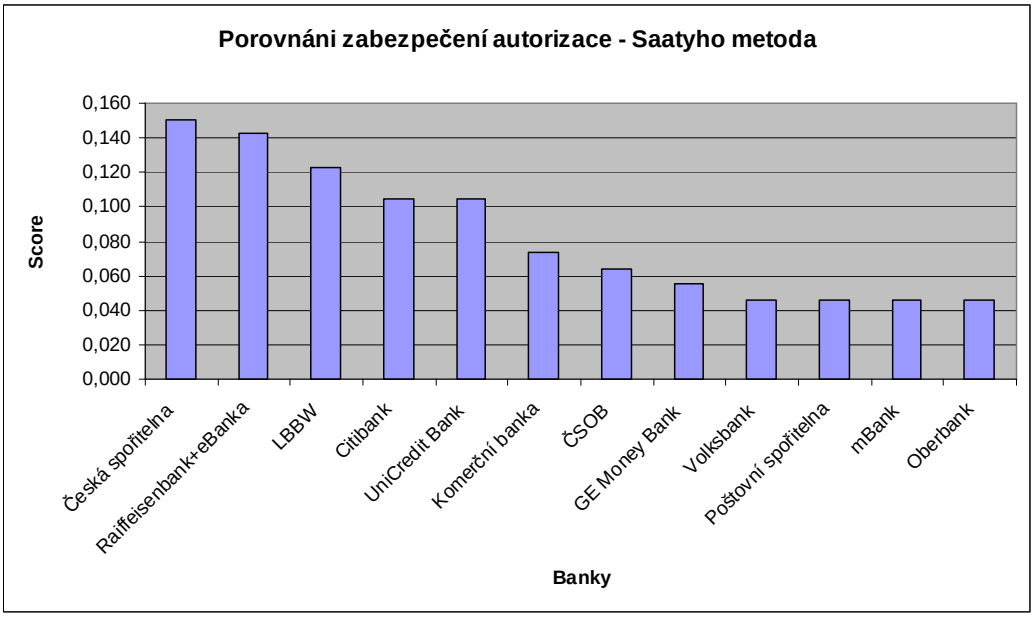
k3	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	bi	vi
a1	**1**	1	1/9	1/9	1/9	1/9	1	1/9	1/9	1	1/9	1/9	0,231	0,013
a2	1	**1**	1/9	1/9	1/9	1/9	1	1/9	1/9	1	1/9	1/9	0,231	0,013
a3	9	9	**1**	1	1	1	9	1	1	9	1	1	2,080	0,118
a4	9	9	1	**1**	1	1	9	1	1	9	1	1	2,080	0,118
a5	9	9	1	1	**1**	1	9	1	1	9	1	1	2,080	0,118
a6	9	9	1	1	1	**1**	9	1	1	9	1	1	2,080	0,118
a7	1	1	1/9	1/9	1/9	1/9	**1**	1/9	1/9	1	1/9	1/9	0,231	0,013
a8	9	9	1	1	1	1	9	**1**	1	9	1	1	2,080	0,118
a9	9	9	1	1	1	1	9	1	**1**	9	1	1	2,080	0,118
a10	1	1	1/9	1/9	1/9	1/9	1	1/9	1/9	**1**	1/9	1/9	0,231	0,013
a11	9	9	1	1	1	1	9	1	1	9	**1**	1	2,080	0,118
a12	9	9	1	1	1	1	9	1	1	9	1	**1**	2,080	0,118
													17,565	1,000
			λ_{max}	12									KI	0,000

k4	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	bi	vi
a1	**1**	1	1	9	1	9	1	9	9	9	9	9	3,603	0,173
a2	1	**1**	1	9	1	9	1	9	9	9	9	9	3,603	0,173
a3	1	1	**1**	9	1	9	1	9	9	9	9	9	3,603	0,173
a4	1/9	1/9	1/9	**1**	1/9	1	1/9	1	1	1	1	1	0,400	0,019
a5	1	1	1	9	**1**	9	1	9	9	9	9	9	3,603	0,173
a6	1/9	1/9	1/9	1	1/9	**1**	1/9	1	1	1	1	1	0,400	0,019
a7	1	1	1	9	1	9	**1**	9	9	9	9	9	3,603	0,173
a8	1/9	1/9	1/9	1	1/9	1	1/9	**1**	1	1	1	1	0,400	0,019
a9	1/9	1/9	1/9	1	1/9	1	1/9	1	**1**	1	1	1	0,400	0,019
a10	1/9	1/9	1/9	1	1/9	1	1/9	1	1	**1**	1	1	0,400	0,019
a11	1/9	1/9	1/9	1	1/9	1	1/9	1	1	1	**1**	1	0,400	0,019
a12	1/9	1/9	1/9	1	1/9	1	1/9	1	1	1	1	**1**	0,400	0,019
													20,816	1,000
			λ_{max}	12									KI	0,000

Ohodnocení vah kritérií						
	k1	**k2**	**k3**	**k4**	**Geometrický průměr**	**Váhy**
k1	**1**	1/3	1/5	1/7	0,312	0,055
k2	3	**1**	1/3	1/5	0,669	0,118
k3	5	3	**1**	1/3	1,495	0,263
k4	7	5	3	**1**	3,201	0,564
					5,678	1,000
			λ_{max}	4,129	KI	0,043

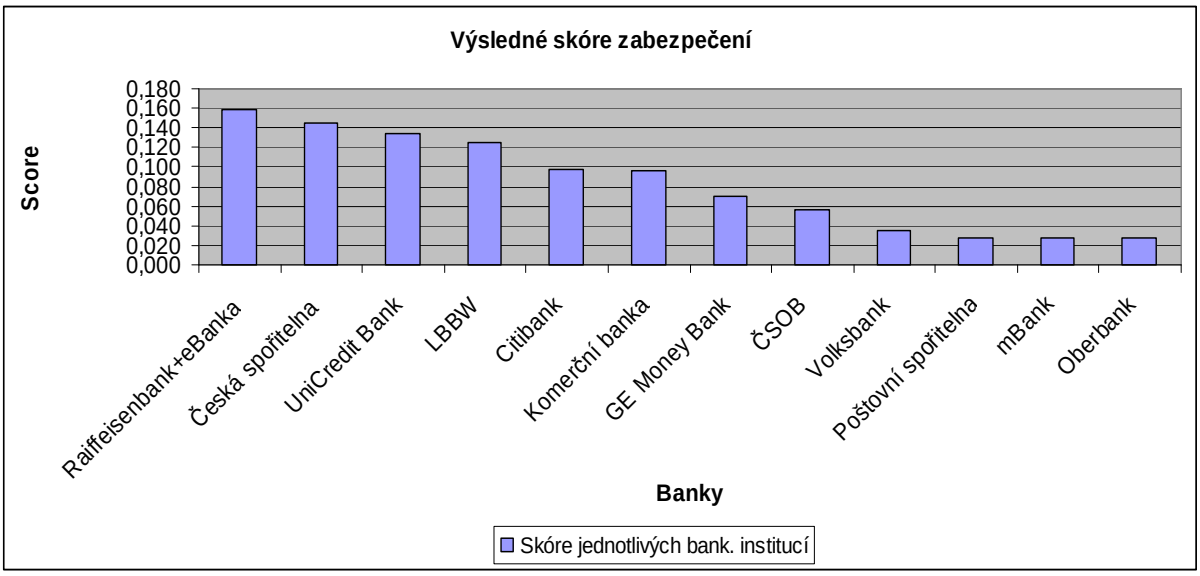
Kritérium	Váhy	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	
k1	0,055	0,023	0,023	0,023	0,023	0,205	0,205	0,023	0,205	0,023	0,205	0,023	0,023	
k2	0,118	0,173	0,019	0,173	0,173	0,019	0,019	0,019	0,173	0,019	0,173	0,019	0,019	
k3	0,263	0,013	0,013	0,118	0,118	0,118	0,118	0,013	0,118	0,118	0,013	0,118	0,118	
k4	0,564	0,173	0,173	0,173	0,019	0,173	0,019	0,173	0,019	0,019	0,019	0,019	0,019	
														Kontrolní součet
Celkové ohodnocení		0,123	0,105	0,150	0,064	0,142	0,056	0,105	0,074	0,046	0,046	0,046	0,046	1,000

	Název	Score	Pořadí
a3	Česká spořitelna	0,150	1
a5	Raiffeisenbank+eBanka	0,142	2
a1	LBBW	0,123	3
a2	Citibank	0,105	4
a7	UniCredit Bank	0,105	4
a8	Komerční banka	0,074	5
a4	ČSOB	0,064	6
a6	GE Money Bank	0,056	7
a10	Volksbank	0,046	8
a9	Poštovní spořitelna	0,046	8
a11	mBank	0,046	8
a12	Oberbank	0,046	8



Příloha 3 - Výpočet výsledného pořadí

	Celkové skóre pro autentizaci	Výsledné pořadí pro autentizaci	Celkové skóre pro autorizaci	Výsledné pořadí pro autorizaci	Celkové skóre	Výsledné skóre	Výsledné pořadí
Raiffeisenbank+eBanka	0,511	1	0,441	2	0,952	0,159	1
Česká spořitelna	0,389	2	0,479	1	0,868	0,145	2
UniCredit Bank	0,511	1	0,292	4	0,803	0,134	3
LBBW	0,389	2	0,366	3	0,755	0,126	4
Citibank	0,291	4	0,292	4	0,583	0,097	5
Komerční banka	0,338	3	0,239	5	0,577	0,096	6
GE Money Bank	0,254	5	0,166	7	0,421	0,070	7
ČSOB	0,132	6	0,205	6	0,337	0,056	8
Volksbank	0,082	7	0,125	9	0,207	0,035	9
Poštovní spořitelna	0,034	8	0,132	8	0,166	0,028	10
mBank	0,034	8	0,132	8	0,166	0,028	10
Oberbank	0,034	8	0,132	8	0,166	0,028	10
Kontrolní součty	3,001		3,001		6,002		



Příloha 4 - Bezpečnostní zásady internetového bankovnictví
Zdroj: Bezpečnostní zásady. Bezpečnost služby internetového bankovnictví *[online]. 2010, 1, [cit. 2010-03-20]. Dostupný z WWW: <https://ibs.rb.cz/IB/help/Bezpecnostni_zasady.html>*.

BEZPEČNOST SLUŽBY INTERNETOVÉHO BANKOVNICTVÍ

Níže jsou popsána konkrétní bezpečnostní doporučení pro bezpečné nastavení klientského počítače. Tato bezpečnostní doporučení byla převzata z nejbezpečnějšího internetového bankovnictví a to od bankovní instituce Raiffeisenbank+eBank.

Obecné bezpečnostní zásady

- Doporučujeme využít možnosti nastavení denního limitu pro tuzemské platební příkazy.
- Bezpečnostní jména, hesla a kódy ke službám uchovávejte na bezpečném místě.
- Smlouvu o zřízení služeb přímého bankovnictví, její přílohy a obálky s hesly pro Internetové bankovnictví, s jednorázovými transakčními hesly a s osobním číslem uchovávejte na bezpečném místě.
- V případě podezření na prozrazení Vašich bezpečnostních jmen, hesel nebo kódů kontaktujte banku na nonstop bezplatné telefonní lince 800 900 900 a požádejte o zablokování příslušných služeb.

Specifické bezpečnostní zásady pro používání služby Internetové bankovnictví

Zabezpečení systému Internetového bankovnictví je tak silné, jak silný je jeho nejslabší článek. Systém Internetového bankovnictví se skládá ze serverů banky, sítě internet, sítě GSM, uživatelova počítače a uživatelova mobilního telefonu.

Servery banky jsou zabezpečeny serverovými certifikáty, soustavou firewallů, ochranných zón, monitorovacích zařízení a dalších mechanismů, které v celém systému Internetového bankovnictví tvoří velmi silný článek.

Potenciálně nejnedůvěryhodnější článek - internet - je dostatečně silný díky šifrovanému spojení mezi serverem banky a uživatelským počítačem.

Síť GSM je využívána pouze pro přenos dílčích informací, které samy o sobě nemohou být zneužity k bezpečnostnímu prolomení Internetového bankovnictví.

Zbývající dva články – uživatelský počítač a mobilní telefon – jsou potenciálně nejzranitelnější místa celého systému, a to z toho důvodu, že za jejich zabezpečení nemůže odpovídat banka, ale pouze sám klient.

Ochrana mobilního telefonu je poměrně snadná, stačí mít telefon fyzicky neustále při sobě, chránit jej PINem a při nepoužívání jej vypínat.

Již obtížnější může být pro laického uživatele zajištění bezpečnosti počítače, aby na něj nikdo nemohl nainstalovat programy umožňující dálkovou správu včetně odečítání klávesnice (získání hesla), kopírování souborů (certifikátu), případně podvržení zobrazované informace. Je proto nezbytné věnovat zabezpečení uživatelského počítače náležitou pozornost a případně bezpečnostní nastavení také konzultovat s odborníkem.

Klientům, kteří se dobře neorientují v základech počítačové bezpečnosti, nemají nainstalovanou a pravidelně aktualizovanou antivirovou a antispyware ochranu, nedoporučujeme používat metodu podpisového certifikátu, ale spíše metodu SMS kódů. SMS kód totiž představuje vynikající ochranu před napadením klientova počítače přes síť a zavádí do autentizace fyzický předmět (SIM kartu). Použití této metody nicméně znamená nutnost postarat se o bezpečnost mobilního telefonu. Při používání SMS kódů současně doporučujeme měnit často přístupové heslo do Internetového bankovnictví.

Podepisování pomocí SMS kódů naopak nedoporučujeme klientům, kteří často ztrácejí mobilní telefony, nedůvěřují rodinným příslušníkům, nechrání si použití mobilního telefonu PINem nebo z jiných důvodů nemohou ochránit svůj mobilní telefon byť i před krátkodobým zcizením.

Doporučené postupy a nastavení

- Doporučujeme změnit heslo pro přihlášení alespoň jednou měsíčně.
- Při volbě hesla nepoužívejte snadno odhadnutelné informace, jako jsou jména, data narození, telefonní čísla apod.
- Vaše heslo pro přihlášení nikomu nesdělujte a zabraňte odpozorování hesla při jeho zadávání.
- Podpisový certifikát uchovávejte odděleně (např. na zálohované disketě, obě uložte na bezpečná místa) od počítače, na kterém používáte aplikaci Internetové bankovnictví.
- Ve veřejných prostorách (knihovny, internetové kavárny, školy…) nedoporučujeme používat podpisový certifikát, ale SMS kód. Použijete-li přesto certifikát, nekopírujte jej na disk počítače a neinstalujte jej. Před odchodem ukončete všechna spojení s bankovním serverem, ukončete prohlížeč (browser).
- Nezapomeňte si pravidelně alespoň jednou ročně obnovovat platnost podpisového certifikátu.
- V případě ztráty nebo zničení podpisového certifikátu a zejména při podezření, že si někdo mohl pořídit kopii Vašeho certifikátu, ihned žádejte o jeho zneplatnění a vydání certifikátu nového.

- V případě ztráty mobilního telefonu, na který si necháváte zasílat SMS kódy, ihned tuto metodu zablokujte nebo si změňte telefonní číslo pro zasílání SMS kódů.
- V případě podezření na zneužití Vašich přístupových práv žádejte o zablokování těchto práv.
- Ve Vašem prohlížeči používejte maximální možnou sílu šifrování (128 bit).
- Při komunikaci se serverem banky používejte protokol TLS, nebo alespoň SSL 3.0.
- Nainstalujte si antivirový software a pravidelně (nejméně jednou týdně) provádějte jeho aktualizaci.
- Nainstalujte si antispyware software a pravidelně (nejméně jednou týdně) provádějte jeho aktualizaci.
- Při použití antiviru věnujte pozornost případným změnám v systémových souborech, projeví se zde útoky typu trojan horse (vir importovaný např. souborem připojeným k mailu).
- Pro běžnou práci, zejména při práci s internetem, nepoužívejte uživatelský profil s administrátorskými právy.
- Před připojením k bance vždy uzavřete všechna okna internetového prohlížeče a pak znovu prohlížeč spusťte (zabráníte tak některým druhům útoků).
- Neumožňujte jiné osobě, aby se připojovala k síti prostřednictvím Vašeho uživatelského profilu. Před odchodem od počítače vždy uzamkněte obrazovku nebo ukončete všechna spojení mezi Vámi a serverem. Médium (disketu) s podpisovým certifikátem bezpečně uložte. Telefon pro zasílání SMS kódů mějte vždy při sobě.
- Nepovolujte ukládání hesel ve Vašem počítači; pokud jste tak již učinili, hesla smažte a ukládání zrušte (Tools/Internet Options/Content/Autocomplete/Clear passwords a NEzaškrtnout Usernames and passwords on forms). Toto je zvlášť důležité, pokud pracujete z veřejného terminálu, internetové kavárny, nebo jiného nedůvěryhodného počítače.
- Doporučujeme chránit počítač programy typu "Personal firewall', především při připojení k internetu pevnou linkou (přes kabelovou televizi a pod.).
- Nedoporučujeme instalovat software získaný z nedůvěryhodných zdrojů (veřejné knihovny SW, přílohy v mailu apod.). Zejména nelegálně získaný SW může obsahovat tzv. "trojské koně" a Vaše hesla, klíče i certifikáty odesílat autorovi těchto (nelegálně upravených) programů. Věnujte zvýšenou pozornost příjmu mailů s přílohami - viry šířené e-mailem často obsahují tzv. "zloděje hesel".
- Na počítači, ze kterého obsluhujete Internetové bankovnictví, nedoporučujeme používat takzvané "instant -messengery", tedy aplikace pro internetovou komunikaci v reálném čase, například ICQ, AOL, GoogleTalk, Microsoft MSN messenger, nebo VoIP službu Skype. Tyto systémy obsahují řadu bezpečnostních nedostatků a chyb, většina z nich se obtížně aktualizuje a je zde vysoké riziko instalace verze s podvodně vloženým škodlivým programovým kódem. Tyto systémy lze snadno zneužít ke zjišťování zadávaných hesel i ke stažení libovolného souboru z napadeného PC.
- Pokud z nějakého důvodu musíte programy typu instant messaging používat, jako minimum doporučujeme tyto služby nespouštět se systémem, před použitím Internetového bankovnictví restartovat PC a tyto programy nespouštět, dokud neskončíte práci v Internetovém bankovnictví. Pokud v rámci těchto systémů obdržíte jakoukoli zprávu obsahující odkaz, je vždy nutné se před kliknutím na odkaz přesvědčit, kdo zprávu poslal a zda jde o důvěryhodný zdroj.
- Instalujte důležité servicepacky
  (pro Microsoft: **http://windowsupdate.microsoft.com**).
- Přiřaďte si server internetového bankovnictví Raiffeisenbank a.s. do zóny důvěryhodných serverů. Do zóny důvěryhodných serverů doporučujeme přiřazovat

pouze servery internetových bankovnictví bank a certifikačních autorit, s nimiž jste v obchodním vztahu.

- V nastavení webového prohlížeče pro zónu obecného internetu nastavte:
  - zákaz stahování ActiveX objektů (nepodepsaných i podepsaných)
  - zákaz inicializace a skriptování prvků neoznačených jako bezpečné
  - zákaz skriptovaných activeXobjektů označených jako bezpečné
  - u MS VM - Povolení pro jazyk JAVA: vysoké zabezpečení
  - zákaz přístupu k datům v různých doménách
  - zákaz instalace součástí desktopu
  - zákaz spouštění souborů a programů v IFRAME
  - zákaz používání sub-framů v rámci různých domén
  - vysoké zabezpečení u Software channel permissions
  - zákaz vkládání do schránky pomocí skriptů
  - zákaz skriptování pomocí java appletů
- **Dále doporučujeme**
  - nepoužívat nástroje rozšiřující služby prohlížeče (jako například MyIE, Maxthon)
  - pravidelně promazávat dočasné internetové soubory
  - ověřovat platnost serverových certifikátů
  - umožnit upozorňování na neplatné serverové certifikáty
  - umožnit upozorňování na přesměrování při odesílání formulářů
  - umožnit upozorňování na přechod mezi zabezpečeným a nezabezpečeným spojením

Pamatujte: umožníte-li někomu přístup ke svým bezpečnostním prostředkům, nebo ke svému počítači, dáváte mu možnost toto zneužít.