Analýza bezpečnosti platebních karet

Bc. Tomáš Šupa

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš Šupa**
Osobní číslo:	**A11507**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Analýza bezpečnosti platebních karet**

Zásady pro vypracování:

1. **Zjistěte současné bezpečnostní prvky a možnosti zabezpečení u platebních karet.**
2. **Vytvořte komplexní analýzu zabezpečení platebních karet u bank v ČR.**
3. **Zjistěte zabezpečení platebních metod používaných v zahraničí.**
4. **Definujte možnosti a způsoby zneužití platebních karet.**
5. **Srovnejte metodiky zabezpečení používané v ČR s metodikou používanou ve světě.**
6. **Navrhněte kroky pro úpravu zabezpečení platebních karet.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PŘÁDKA, Michal; KALA, Jan. Elektronické bankovnictví : rady a tipy. 1.vyd. Praha : Computer Press, a.s., 2000. 166 s. ISBN 80-722-6328-5.**
2. **MÁČE, Miroslav. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.**
3. **JUŘÍK, Pavel. Platební karty: 1870-2006 : velká encyklopedie. 1. vyd. Praha: Grada, 2006, 296 s. ISBN 80-247-1381-0.**
4. **NEHYBOVÁ, Marta. Bankovní služby nejen pro podnikatele: 1870-2006 : velká encyklopedie. . Brno: Miroslav Nehyba, 1999, 140 s. ISBN 80-902-6454-9.**
5. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy. Vyd. 1. Praha: Computer Press, 2000, xii, 166 s. Praxe manažera. ISBN 80-722-6328-5.**
6. **JUŘÍK, Pavel a Jan KALA. Platební karty: ilustrovaná historie placení. 1. vyd. Praha: Libri, 2000, xii, 166 s. Praxe manažera. ISBN 9788072774982.**
7. **JAMES, Lance. Phishing bez záhad. 1. vyd. Praha: Grada, 2007. 281 s. ISBN 978-80-247-1766-1.**
8. **MÁČE, Miroslav a Ladislav HOZÁK. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.**
9. **SCHLOSSBERGER, Otakar a Ladislav HOZÁK. Phishing bez záhad. 1. vyd. Praha: Grada, 2007. 281 s. ISBN 80-726-5073-4.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **22. února 2013**

Termín odevzdání diplomové práce: **22. května 2013**

Ve Zlíně dne 22. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Hlavním tématem práce je zabezpečení platebních karet. Práce dále popisuje a navzájem srovnává jednotlivé bezpečností prvky a využívané postupy v bankách českých i zahraničních, definuje základní pojmy z oblasti bezhotovostních plateb a elektronického bankovnictví, poukazuje na možná rizika, která při těchto moderních metodách hrozí a navrhuje, jak možným nebezpečí předcházet.

Klíčová slova: platební karty, zabezpečení, platební systémy, bezpečnostní prvky karet, internetové bankovnictví.

ABSTRACT

The main topic of this work is to provide credit cards. The work describes and compares each individual security features and procedures used in Czech and foreign banks, defines the basic concepts of non-cash payments and e-banking, highlighting possible risks in these modern methods of risk and suggests how to avoid potential danger.

Keywords: payment cards, security, payment systems, safety features cards, internet banking.

Na tomto místě bych rád poděkoval vedoucímu mé diplomové práce, kterým je pan Ing. David Malaník Ph.D., za pomoc při vypracování této práce, za odborné vedení a čas, který mi věnoval.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Žijeme v době neuvěřitelného technologického rozvoje, který nám denně a téměř na každém kroku ulehčuje naše životy. Nové technologie a s nimi i nové nápady, obzvláště pak v oboru informatiky či bankovnictví, s sebou ale přinášejí i nová rizika. S každým novým systémem pro snadnější a rychlejší platby přichází také myšlenka, jak tento systém porazit nebo jej zneužít. V oblasti elektronického bankovnictví a bezhotovostních služeb hovoříme nejčastěji o nebezpečí zvaném phishing, pharming a skimming, ale i nadále jsou pro platební karty největším nebezpečím sami uživatelé. Na základě těchto faktorů jsem se rozhodl věnovat svoji diplomovou práci právě této problematice, a to konkrétně problematice zabezpečení platebních karet. V této moderní době máme tendenci mít každou situaci vždy pod kontrolou. Chceme mít cokoliv a kdykoliv, a přesně to je dnes s platební kartou, máme-li na ní dostatečné finanční prostředky, možné.

V první části mé práce definuji základní teoretické termíny, týkající se platebních karet, jejich ochranných prvků a rozdělení dle způsobu provedení či podle použitých technologií, poté nastíním historickou linii vývoje platebních karet a jejich zabezpečení. V samostatné kratší kapitole se pak zabývám vznikem bankomatů a jejich jednoduchým popisem. Nezbytnou součást teoretické části tvoří platební systémy na internetu a internetové bankovnictví, výčet nejoblíbenějších platebních systémů u nás i v zahraničí, a především systémová ochrana těchto elektronických platebních systému.

Hlavním cílem práce je vymezit způsoby současného zabezpečování platebních karet, porovnat jednotlivé bezpečnosti prvky na základě jejich využití českými i zahraničními bankami a jejich zkušeností, a srovnat výhody a nevýhody všech způsobů zabezpečení. Zároveň bych se rád soustředil na již zmíněné možnosti zneužití platebních karet a platebních systému, a navrhl vhodná bezpečnostní opatření, která by mohla těmto rizikům předcházet.

I. TEORETICKÁ ČÁST

1 PLATEBNÍ KARTY

Platební karta nám umožňuje takzvanou bezhotovostní platbu nebo snadný a rychlý přístup k hotovosti pomocí bankomatu. Další možnosti jejího užití, různé funkce i zpoplatnění jednotlivých služeb se vždy liší v závislosti na bance, která kartu vystavila. V minulosti byly karty vyráběny z papíru, avšak z důvodu jejich snadného padělání se dnes již vyrábí pouze v plastové podobě, která zaručuje také delší životnost a umístění řady bezpečnostních prvků. Rozměr karty je dán mezinárodní normou ISO 3554 a stanoven na 85,6 x 54 mm [13]. Držitelem karty může být jak fyzická, tak i právnická osoba, která na žádost dala souhlas k vystavení a používání platební karty. Každému držiteli je k zúčtování transakcí prováděných platební kartou přiřazeno identifikační číslo karty, jež je shodné s číslem kartového účtu, který je taktéž vytvořen bankou vydávající platební kartu. Každá z těchto karet je opatřena identifikačními údaji držitele, přičemž ochranu těchto údajů i ochranu před jejím zneužitím zajišťují bezpečnostní prvky platební karty (viz. kapitola 1.4 Bezpečnostní prvky platební karty) [9]. V dnešní době umožňuje platbu kartou většina prodejců na celém světě, ať už v kamenných nebo internetových obchodech. Platební proces je rychlý, přesný a bezpečný. Kreditní karta je především symbolem dostupnosti, jelikož ji můžeme mít kdykoliv u sebe. Jednou z jejích nevýhod může být kreditní limit, který stanovuje maximální limit čili nejvyšší možná výše čerpání útraty, tento limit si většinou určuje sám držitel karty po dohodě s vydávající bankou na základě jeho platební historie. Většina platebních karet nabízí i různé formy odměn a bonusů za jejich užívání.

Bezhotovostní platební styk

Bezhotovostní platební styk je platba mezi dvěma subjekty, při níž nepoužíváme hotovost. Kromě platby kartou je možné jej uskutečnit bankovním převodem z účtu plátce na účet příjemce. Dnes nám navíc banky umožňují také platbu v jiných zahraničních měnách, která je automaticky převedena ve stejné hodnotě dle jejich vlastního kurzovního lístku.

1.1 Historie platebních karet

- **1914** – Americká telefonní a telegrafní společnost Western Union Telegraph Company zhotovuje první platební kartu na světě, která sloužila k zasílání telegrafů, telefonování a díky možnosti uhradit platbu na konci měsíce také využití bankovního úvěru. Výrobním materiálem byl plech.
- **1924** – Společnost General Petroleum Corporation of California (dnes Mobil Oil) přichází s kreditní kartou umožňující bezhotovostní platby za čerpání pohonných hmot a dalších služeb v rámci její společnosti v USA.
- **1929** – důsledkem vysokého konkurenčního boje začalo vznikat velké množství platebních karet, zejména věrnostních, kvůli americké hospodářské krize bylo však další vydávání karet pozastaveno.
- **1938** – Americká společnost AT&T zavádí pro své zákazníky karty Bell Systém Credit Card .
- **1950** – Společnost Diners Club International přichází s univerzálně použitelnými platebními kartami.
- **1951** – Platební karty společnosti Diners se jako první na světě stávají mezinárodními.

  Americká banka v New Yorku The Franklin National jako první přichází s kreditními kartami.
- **1958** – Platební karty vydává další americká finanční společnost a cestovní kancelář American Express.

  Americká společnost Bank of America vydává velmi úspěšní platební karty s názvem Bank Americard jako rodinnou kreditní kartu.
- **1965** – Čtyři americké banky v Chicagu přichází z vlastními platebními kartami a zakládají Midwest Bank Card Association.
- **1966** – Dalších sedmnáct amerických bank zakládá California Bank Card Association a přichází s vlastní licencí k vydávání platebních karet.
- **1968** – Čtyři banky v americké Kalifornii zakládají Western States Bancard Association (WSBA) a vlastní název pro platební karty Master Charge.

  První možnost platby platebními kartami v Československu, akceptuje je společnost Diners Club ve spolupráci s cestovní kanceláří Čedok. Postupně společnost Čedok spolupracuje i s kartami American Express, BankAmericard, Master Charge a JCB.

- **1980** – VISA představuje jednoho ze sponzorů olympijských her v Moskvě a při této příležitosti vydává první platební karty v zemích Sovětského svazu.
- **1988** – Maďarská banka, specializující se na zahraniční obchod, KHB vydává první platební karty VISA Classic.

  V tehdejším Československu vydává Živnostenská banka první platební kartu pro československé občany. Karta sloužila jako dispoziční k účtům společnosti Tuzex, jejíž poukazy bylo možné vybírat v bankách SBČS a ČSOB.
- **1990** – American Express otevírá v Praze první českou pobočku

  Česká Živnostenská banka vydává karty VISA Classic.

  Česká Komerční banka začíná od základů znovu budovat celý platební systém, přičemž čerpá ze znalostí a zkušeností z německých, rakouských a švýcarských bank, a zároveň pobízí ke spolupráci české i slovenské peněžní ústavy.
- **1991** – V České republice vzniká Mezinárodní sdružení pro platební karty (MSPK). Členy sdružení jsou Agrobanka Praha, Investiční banka, Komerční banka, Poštovní banka, Tatra banka, Všeobecná úvěrová banka a I.S.C. MUZO. Tyto banky v roce 1991 také budují jednotný bankový kartový systém, nejprve pro Eurocard a MasterCard, Cirus, eurošek, později i pro karty VISA.

  Česká Živnostenská banka vydává karty VISA Business.
- **1992** - Česká Živnostenská banka přebírá příjem karet JCB a Diners Club od společnosti Čedok, která v tentýž roce ukončila svoji činnost.
- **1998** – Společnost Diners Club začíná v České republice poprvé nabízet charge karty. Současně zahajuje Česká spořitelna propagaci kreditních karet svým vybraným klientům.
- **2000** – Bank Austria Creditanstalt (HBV Bank) vydává kreditní kartu Maxim.
- **2001** – Opravdový start kreditních a charge karet v České republice.
- **2005** – Všechny vyráběné elektronické platební karty začínají používat pouze čipovou technologii [1,2].

1.2 Vývoj platebních karet

V České republice dochází k největšímu vývoji platebních karet i celého systému po roce 1991, kdy bylo 4. února založeno Mezinárodní sdružení pro platební karty a na jeho základě také vytvořen jednotný kartový systém pro banky u nás. Celý projekt dostala na starosti společnost I. S. C. MUZO, která měla v první řadě za úkol vybudovat modernější

systém bank, který spočíval zejména ve spravování databází platebních karet, autorizací transakcí v bankomatech a obchodech, kladl důraz na personalizace platebních karet a vytváření a rozdělování PIN kódů. Úkolem I. S. C. MUZO bylo taktéž vybrat dodavatele, kteří by kromě dodání provozovali a spravovali bankomaty a platební terminály.

Přestože použití prvních platebních karet bylo založeno na jednoduchosti, základní princip se zachoval až do současnosti. Dříve stačilo pouze kartu předložit pověřené osobě, ta poté ověřila její platnost, totožnost majitele karty a jeho podpis podle podpisového vzoru. Klientův účet byl vždy připočten k celkové měsíční faktuře. První karty byly vyráběny z kovu a podobaly se vojenským identifikačním štítkům. Kov byl později nahrazen papírem. Oba materiály však byly nevyhovující a lehce padělatelné, jelikož neumožňovaly umístění dostatečných a účinných bezpečnostních prvků. Nyní se karty vyrábějí pouze v plastovém provedení [10].

1.3 Rozdělení platebních karet

V současnosti nám banky nabízí široký výběr platebních karet a s nimi i nejrůznějšími možnosti jejich využití. Mezi platební karty patří například karty kreditní, debetní či Charge, novinkou na trhu je mezi kartami elektronická peněženka [14].

Debetní karta

Debetní karta je základní a nejběžněji užívanou platební kartou u nás. Je propojena s bankovním účtem majitele, veškeré prováděné platby a platební převody jsou tudíž závislé na finančním zůstatku na tomto účtu. Pokud není stav účtu dostatečný, bezhotovostní platbu ani výběr z bankomatu není možné uskutečnit. Některé banky nabízejí možnost vyřízení kontokorentu, se kterým je možno provádět finanční operace i přesto, že zůstatek na účtu není dostatečný. Kontokorentní úvěr je bankovní služba omezená úvěrovým limitem, tedy se stanoveným maximem částky, kterou banka majiteli účtu půjčí. S využitím kontokorentní služby se tedy debetní karta stává jednodušší obdobou kreditní karty [14].

Kreditní karta

Kreditní karta se může na první pohled zdát totožná s kartou debetní, můžeme s ní však hradit naše platby a nákupy dle úvěrového rámce, na který banka přesně stanoví podmínky jeho splácení. Můžeme ji tedy používat i přes to, že náš bankovní účet nedisponuje dostatečnými finančními prostředky. Kreditní karta nám též umožňuje využít takzvaného bezúročného období, tedy platby bez využití úvěru a placení úroků z využité sumy, a tak splatit čerpanou částku do daného data v měsíci [34]. Hlavní výhodou kreditní karty je bezesporu rychlá možnost úvěru a čerpání spotřebitelských půjček. Nevýhodou může být pak omezený limit půjčky, který stanovuje banka po dohodě s držitelem karty, a nejčastěji se odvíjí od finančních možností držitele, jeho schopností splácet a historie jeho účtu a plateb.

Charge karta

Charge platební karty jsou nejčastěji využívány zaměstnavateli pro jejich zaměstnance jako finanční dotace na pokrytí jejich výdajů na služebních cestách [5]. Charge karta je stejně jako karta kreditní vázána úvěrem, který poskytuje vydávající banka v podobě finanční půjčky. Na rozdíl od kreditní karty není možné s kartou charge tyto půjčky splácet, čili rozdělit do delšího časového období a částku rozdělit, ale je nezbytné tento dluh vrátit najednou do konce sjednaného období, které obvykle činí jeden měsíc. Pokud majitel karty nesplatí částku ve stanovené lhůtě, je mu účtován poplatek za nedodržení této lhůty [14].

Elektronická peněženka

Elektronická peněženka neboli e-wallet slouží jako víceúčelová předplacená karta a lze pomocí ní čerpat pouze předem vloženou sumu, kterou lze opakovaně dobíjet. Je vhodná pro placení menších částek, jelikož na rozdíl od ostatních platebních karet je nákup s ní mnohem rychlejší a pro obchodníky i mnohem levnější. Tato karta je opatřena čipem, který nese údaj o množství vložených peněz. V některých státech karta uvádí i jméno a věk jejího držitele, a znemožňuje tak například nákup alkoholu či cigaret mladistvým a nezletilým. Elektronické peněženky mohou u nás vydávat banky s odpovídající bankovní licencí a společnosti, které získají povolení k jejich vydání od České národní banky. V České republice jsou elektronické peněženky využívány především dopravci, další známou formou u nás jsou platby PaySec a PayPal, určené pro bezpečnou internetovou platbu menších částek. Při platbě pomocí těchto služeb se nezadávají žádná citlivá data,

pouze uživatelské jméno a heslo. Je též možné nastavení maximálního platebního limitu, a zabezpečit platbu navíc také autorizací pomocí mobilního telefonu [15,17].

1.3.1 Rozdělení platebních karet podle způsobu provedení

Rozlišujeme dva typy platebních karet podle jejich provedení:

a) Elektronická platební karta

Elektronická platební karta je u nás stále velmi používanou kartou, je výrazně levnější než karta embosovaná a zároveň bezpečnější. Karty je možno použít pouze pro transakce, které online ověřuje klientské centrum, tedy výběr z bankomatu nebo platba u prodejců prostřednictvím elektronického platebního terminálu. Při ztrátě karty nebo jejího odcizení je téměř nulová šance jejího zneužití, neboť na kartě nejsou vytištěny žádné citlivé údaje. Mezi elektronické platební karty patří například MasterCard Cirrus a Maestro či VISA Electron [14].

b) Embosovaná platební karta

Embosovaná platební karta obsahuje veškeré důležité a citlivé údaje jako je číslo karty, jméno majitele, datum platnosti a CVV kód. Je možné s nimi platit jak pomocí elektronického terminálu, tak i prostřednictvím imprinteru, jehož platba je následně ověřena podpisem držitele karty pomocí podpisového vzoru. Nevýhodou této karty je vysoký stupeň nebezpečí zneužití při ztrátě či odcizení karty. Mezi nejznámější embosované platební karty patří MasterCard Standard, Gold nebo World Siginum. Ze série VISA karet jsou to pak VISA Classic, Silver, Gold a Platinum.

Obr. 1 Imprinter

1.3.2 Rozdělení platebních karet podle použité technologie

Platební karty využívají pro elektronické platby více druhů technologií:

a) Magnetický kroužek

Magnetický kroužek, umístěný na zadní straně platební karty, obsahuje menší množství uložených dat než čip, a to pouze nejnutnější informace o kartě a jejím majiteli, nezbytné pro výběr hotovosti z bankomatu či danou platbu. Díky snadné výrobě se využití zabezpečení magnetickým proužkem rozšířilo i mimo oblast bankovnictví. Magnetický proužek je podle normy ISO 7811 složen z následujících tří záznamových stop:

1) **První stopa:** Tato první stopa, která má 79 znaků a v bankovnictví obsahuje číslo karty a jméno klienta, byla původně definována v roce 1969 asociacemi leteckých dopravců pro usnadnění odbavení cestujících.
2) **Druhá stopa:** Tato stopa je vyvinuta pro online finanční transakce asociací ABA (American Bankers Accociation) a obsahuje celkem 40 numerických znaků, ve kterých je spolu s číslem zahrnuta i platnost karty.
3) **Třetí stopa:** Tato stopa je na rozdíl od první stopy vytvořena bankami a obsahuje 107 numerických znaků včetně záznamu, díky kterému se ověřuje správnost PIN kódu platební karty. Tato stopa jako jediná ze všech tří stop umožňuje přepis záznamu. Dříve se využívala u offline bankomatů.

b) Čipová technologie

Čipová technologie představuje vyšší míru zabezpečení a umožňuje uložení PIN kódu k ověření totožnosti klienta a identifikaci údajů na kartě [14]. Karta obsahuje počítačové čipy nebo čipy s integrovaným obvodem. Platební transakce již není nutné ověřovat online klientským centrem, ale platba lze uskutečnit také bez ověření v režimu offline. Platební karty jsou kompatibilní po celém světě - standard EMV. Mezi hlavní výhody čipové technologie patří větší bezpečnost, vyšší rychlost a daleko více možností, protože čip dokáže pojmout více informací než magnetický proužek.

c) Hybridní karty

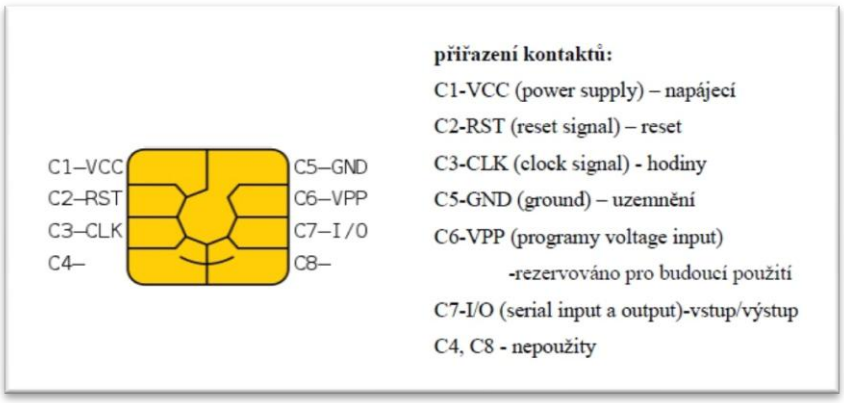
Hybridní karty jsou vybaveny magnetickým proužek i čipem.

1.4 Bezpečnostní prvky platební karty

Každá platební karta obsahuje kombinaci těchto ochranných prvků, které mají zvýšit zabezpečení proti jejich padělání:

Přední strana karty

1. **Logo banky** – Obrazové logo banky, u které má klient vytvořený bankovní učet a která platební kartu vydala (např. Komerční banka, Airbank, atd.).
2. **EMV čip** – Tento ochranný prvek je na všech platebních kartách povinně umístěn od roku 2005. Obsahuje veškeré zakódované informace a údaje o platební kartě a držiteli karty. Tento ochranný prvek je využíván pro výběr hotovosti z bankomatu. Díky tomuto čipu společně s použitím PIN kódu "Chip and PIN" se v počátcích jeho zavedení podařilo snížit počet skimming podvodů více než desetkrát. Čip, využívaný v bankovnictví na platebních kartách, se skládá z elektrický kontaktů, které se definují standardy ISO/IEC 7816-2, CPU mikroprocesorem, který využívá istrukční sadu Intel 8051 nebo Motorola 6805, kryptografickým koprocesorem a paměťmi typu RAM, ROM a EEPROM [31].



Obr. 2 Kontakty na čipové kartě

Více o čipové technologii a standardu EMV viz kapitola 2.2 Mezinárodní standard EMV.

3. **Hologram** – Samolepící etiketa se strukturou dvou či trojrozměrného zobrazení, která může obsahovat prvky, jako jsou kinetické efekty, barevné kódování, moarové efekty, mikrotexty, laserovou demetalizaci, číselná či další skrytá zobrazení. Při tvorbě hologramu se využívá metody Hot Stamping - hologram je zalisován do platební karty. První společností, která hologram začala využívat, byla společnost MasterCard, a to v

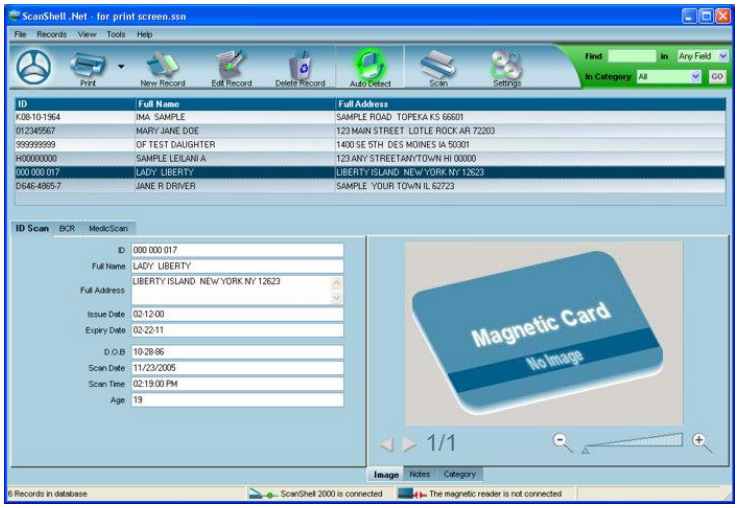
roce 1983. Tento ochranný prvek slouží ke zvýšení zabezpečení proti fyzickému okopírování platební karty a není tak snadné jej padělat.

4. **Číslo platební karty** - Základní identifikační údaj, který propojuje danou platební kartu s finančním účtem. Tento údaj je generován podle standardizace a podléhá normě ISO/IEC 7812. Tento způsob vytvoření čísla karty respektují všichni vydavatelé platebních karet. Údaj je možné si ověřit na internetu pomocí Luhnova algoritmu. První část tohoto čísla udává Major Industry number, následující čísla pak slouží k identifikaci účtu klienta u banky. Číslo platební karty můžeme rozdělit na dva druhy, a to podle způsobu provedení tohoto čísla.
    a. **Embosované** - Číslo je na platební kartě vyraženo a na pohled z karty vystupuje. Je to díky dřívějšímu použití pomocí Imprinteru, který číslo pomocí této metody vyražení čísla karty obtiskl na platební doklad.
    b. **Neembosované** - U tohoto druhu provedení je číslo karty pouze natisknuto na kartě a není z povrchu nijak vystouplé. Při platbě těmito kartami není možné použít imprinter.
5. **Logo vydavatele** – např. VISA, MasterCard. Každá z těchto platebních společností tiskne na platební karty logo pouze v jedné velikosti. Nemůže se tedy stát, že na jedné platební kartě má logo jiné rozměry než u platební karty vydané u jiné banky a stejné platební společnosti. Díky tomu se zvyšuje ochrana proti kopírování platební karty.
6. **Datum platnosti** – Datum vydání a datum expirace platební karty (měsíc/rok).
7. **Jméno a příjmení majitele** – Údaje o držiteli karty. Tento údaj je na kartě proveden stejnou metodou jako číslo karty (vyražen, nebo vytištěn).

Zadní strana karty

1. **Magnetický proužek** – Tento ochranný prvek, definovaný normou ISO 7811, obsahuje pouze důležité informace nutné pro výběr z bankomatu. Díky technologiím v bankomatu mohou být tyto informace nejen přečteny, ale v některých případech dokonce i změněny. V prvních fázích zavedení magnetických proužků byl kromě základních informací o majiteli účtu zapsán také údaj o maximálním hotovostním výběru z bankomatu. Tento záznam se přestal využívat kvůli jeho snadnému zneužití podvodníky. U platby kartou za použití magnetického proužku byla identifikace osoby ověřována pomocí shody podpisu s podpisovým vzorem na podpisovém proužku,

důsledkem toho vznikalo velké množství podvodů a časem vydavatelé přešli na čipové technologie, které jsou daleko lépe zabezpečeny díky použití společně s PIN kódem.
V dnešní době se pro platby kartou využívá právě čipové technologie. Další informace o magnetickém proužku viz. kapitola 1.3.2a Rozdělení platebních karet podle použité technologie.



Obr. 3 Software ScanShell ID Magnetic Reader

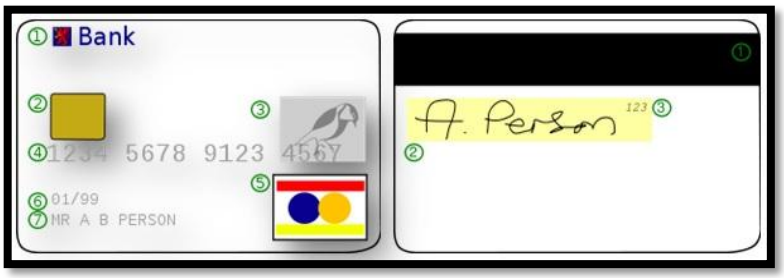
2. **Podpisový vzor (proužek)** – Podpisový proužek, určený pro podpis majitele účtu, nalezneme na všech platebních kartách. Pro zvýšení bezpečnosti tohoto ochranného prvku je na pozadí proužku vytištěn i vzor platební společnosti, který se může jednotlivým rokem vydání platební karty lišit. Díky vzoru společnosti se snižuje také možnost smazání a změny podpisu karty, a tím se zároveň i snižuje riziko padělání karet. Banky doporučují platební kartu podepsat ihned na místě při obdržení platební karty, některé banky dokonce informují své klienty, že bez správně podepsané platební karty na podpisovém proužku nebudou platby akceptovány. Rozeznat změněný podpis je možné na základě porušeného vzoru na podpisovém proužku. Pro zvýšení ochrany jsou na tomto proužku vytištěny i čtyři poslední čísla platební karty, díky kterým je tento ochranný prvek velmi těžce padělatelný.
3. **Kód karty** – Ochranný kód karty, který je zapsán také v magnetickém proužku karty, slouží jako ochranný mechanismus zabraňující padělání platebních karet. Jedná se zároveň o údaj, který je nezbytný pro ověření plateb na internetu.

Kód zapsaný na magnetickém proužku platební karty:

- CAV - JCB karty
- CVC - platební karty společnosti MasterCard
- CVV - platební karty společností Visa a Discover
- CSC - American Express

Kód na zadní straně platební karty:

- CID - platební karty American Express a Discover
- CAV2 - platební karty JCB
- CVC2 - platební karty MasterCard
- CVV2 - platební karty Visa



Obr. 4 Přední a zadní strana platební karty

1.5 Bankomaty

Bankomaty jsou samoobslužná zařízení, která byla jednou z prvních služeb, kterou mohli zákazníci využívat nonstop bez ohledu na otevírací dobu banky. Jen díky tomu se zařadily na seznam 100 nejvýznamnější vynálezů 20. století. První bankomat, který vydával hotovost, byl uveden do provozu 27. června 1967 v bance Barclays v Enfieldu (Velká Británie). Na tomto vynálezu a jeho vývoji se zasloužili Američané a Angličané. Před prvním velkým rozšířením bankomatů byl možný výběr hotovosti pouze na pobočkách bank, u kterých měl klient vedený účet. První bankomaty využívaly systém DACS (De La Rue Automatic Cash System) založený na přijímání jednorázových poukázek, které klient banky získal poštou s výpisem z účtu a za jejich výměnu vydával obálky s deseti librami. Tyto bankomaty se řadí do tzv. první generace. Druhá generace bankomatů, která nastoupila koncem 70. let, se vyznačovala vyšší úrovní zabezpečení. Byly zavedeny magnetické proužky na platebních kartách a k ověření totožnosti klienta se pro zvýšení bezpečnosti zavedly PIN kódy.

Obr. 5 První bankomat od společnosti Barclays

Třetí generace bankomatů nastoupila v polovině a čtvrtá koncem 80. let, kdy se začaly využívat hlavní výhody osobních počítačů. V současnosti je zavedena pátá generace bankomatů, která plně využívá internetových technologií.

Na první pohled je bankomat velmi jednoduché zařízení na obsluhu, ale jedná se o velmi složité zařízení, které se skládá ze tří hlavních částí:

- *Provozní část* (klávesnice, tiskárna, obrazovka, snímač platebních karet, transportní a počítačový systém)
- *Operátorská část* (operátorská klávesnice, tiskárna a počítač)
- *Trezor* (ochranná schránka pro bankovky)

Rozdělení bankomatů do skupin:

- určení pouze k vyplácení hotovosti (Cash Dispending Machine)
- vícefunkční bankomaty, které jsou schopné i peníze ukládat (ATM)

V počátcích nasazení bankomatů byly používané dříve offline bankomaty, které jsou dnes nahrazeny online bankomaty. Ty jsou od svých předchůdců připojeny přímo na autorizační centrum a ověření transakce probíhá v reálném čase u poskytovatele platební karty. Ověření transakce netrvá více než pár sekund, a na rozdíl od offline bankomatů nemusí být PIN zaznamenán na magnetickém proužku. První online bankomat na území Československa byl umístěn v Komerční bance v Praze na náměstí Republiky 19. února 1992 (Na Příkopě 28, dnes Česká národní banka).

Z důvodů zvýšení spolehlivosti a zabezpečení probíhá veškerá komunikace přes pronajaté linky. Tato síť je redundantní s více poskytovateli a s více centrálami. V případě výpadku některé cesty nastane vždy propojení přes jinou větev. PIN je šifrován přímo na klávesnici bankomatu a ve většině případů je celá komunikace šifrována 3DES klíčem, který je vždy unikátní pro každou transakci.

2 PLATEBNÍ SYSTÉMY A SYSTÉMOVÁ OCHRANA PLATEBNÍCH KARET NA INTERNETU

S příchodem prvního internetového obchodu se začala objevovat otázka ohledně realizace plateb na internetu. Tento obchod byl zaměřený na prodej hudebních CD (amazon.com) a vznikl v roce 1992 v USA. Do České republiky se tento boom internetových obchodů dostal až na přelomu tisíciletí, v té době čeští uživatelé internetu vnímali nákup na internetu za bezpečný a velmi často i daleko více cenově přijatelnější, na rozdíl od nákupu v kamenných obchodech. Hlavními důvody pomalejšího vývoje v obchodování na internetu v České republice jsou špatné zkušenosti uživatelů, kteří se stali oběťmi podvodů už v počátcích využívání internetu. Dalším důvodem pomalejšího vývoje internetových obchodů byla absence zákona, který by zcela jasně definoval a specifikoval povinnosti a vztahy obchodníků ke svým zákazníkům na internetu. Tento zákon č.480/2004 Sb. o službách informační společnosti nabyl platnosti v ČR až v roce 2004. V prvních počátcích online plateb byli čeští uživatelé nuceni žádat o povolení k provedení online platby u své banky, to však mělo za následek, že se v České republice stala nejrozšířenější metodou platby za zboží na internetu dobírka, která byla i v loňském roce 2012 v čele žebříčku nejpoužívanějších způsobů platby v internetových obchodech. Postupem času, kdy se internet stal nedílnou součástí každé domácnosti a nákup zboží na internetu už není pro žádnou domácnost novinkou, se setkáváme i s rozvojem systémů pro možnosti platby za námi vybrané zboží. Tyto systémy nazýváme "Platební systémy".

Platební systémy rozdělujeme:

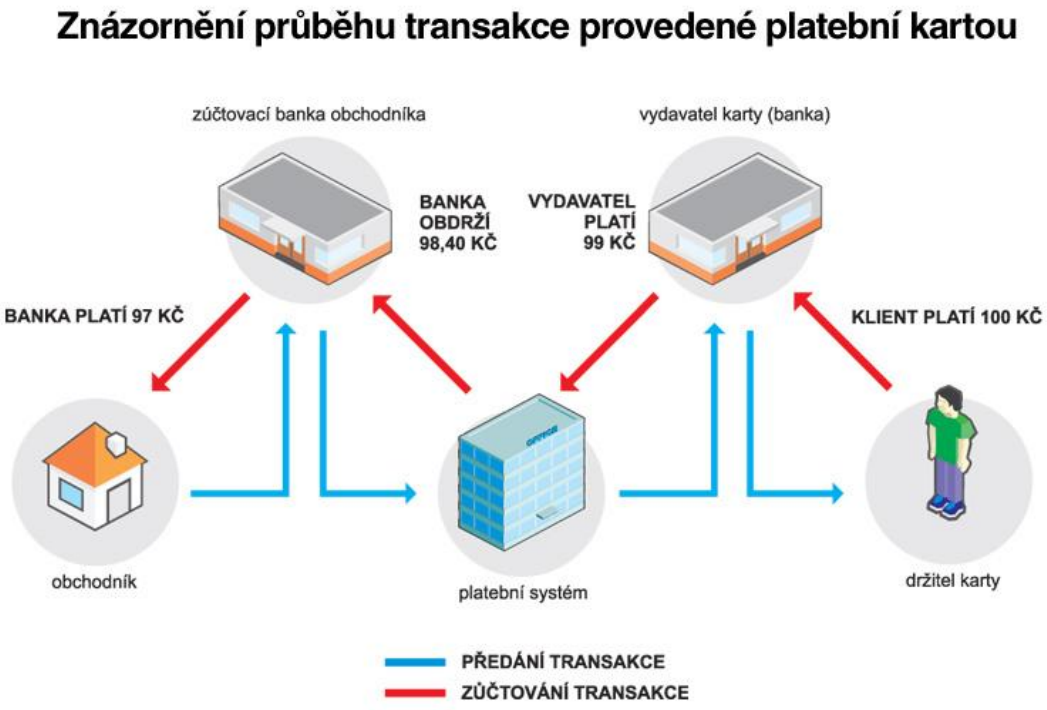
- **Elektronické platební systémy**
  Platební systémy, u kterých jsou během platby využívány informační technologie. Tyto systémy mají oproti klasickým platebním systémům velkou výhodu v zabezpečení citlivých informací. EPS vytvářejí prostředníka mezi odesílatelem a příjemcem platby a díky tomu se příjemce žádné citlivé informace nedozví. Mezi hlavní výhody a faktory těchto systémů patří:
  - Rychlost převodu peněz
  - Snadná uživatelská obsluha
  - Nízké poplatky za platbu na internetu
  - Zabezpečení informací

- **Klasické platební systémy**
  Systémy, u kterých nejsou využívány informační technologie. Mezi typické způsoby klasických platebních systémů patří:
  - platba dobírkou
  - platba hotově
  - platba při převzetí zboží
  - platba poštovní poukázkou
  - předplatným

2.1 Zpracování transakcí

Průběh platby kartou u EPS můžeme rozdělit na tři základní kroky:

- autorizace transakce (ověření)
- přenos transakce do clearingového systému (centrum platebního systému)
- vypořádání všech transakcí



Obr. 6 Průběh transakce platební kartou

Autorizace transakce (ověření)

Prvním krokem u zpracování převodu při platbách kartou je autorizace transakce, která spočívá v ověření a kontrole údajů na kartě (platnost karty, kontrola ochranných prvků karty a kontrola čísla karty, zdali není karta uvedena na seznamu zakázaných karet), ale zároveň dochází i k ověření finančního krytí celé transakce s kontrolou zůstatku na účtu majitele karty. Pokud autorizace karty proběhne v pořádku, systém odešle zpět autorizační kód, ale pokud je karta uvedena na seznamu kradených karet a ohlášena jako ztracená, tak systém předá příkaz pro zadržení karty (Pick-up) a celá transakce je zablokována. Celý tento proces trvá pouze pár vteřin.

Přenos transakce (clearing)

Přenos transakce probíhá prostřednictvím počítačové sítě, na které jsou připojeny jednotlivé banky v daném kartovém systému z celého světa. Tento systém provede clearing všech plateb, které se uskuteční danou kartou za celý den. Následně jednotlivé banky získají seznam plateb (ve prospěch, nebo vrub účtu) jednotlivých klientů.

Vypořádání všech transakcí

Vypořádání transakcí se provádí na základě výstupu z clearingového systému v podobě kreditních nebo debetních sald u jednotlivých bank. Vypořádání plateb má na starosti k tomu určená zúčtovací banka. Tato salda je následně vyúčtována za pomoci nostro účtů u zúčtovací banky. Následně jednotlivé banky zatíží nebo kreditují příslušné účty u svých klientů.

Jednotlivé banky si mohou zvolit v zúčtovacím systému jedno, nebo i více měn na zúčtování. V zemích Evropské unie se pro transakce banka může rozhodnout používat EURO jako zúčtovací měnu a v ostatních státech světa např. USD.

2.2 Mezinárodní standard EMV

Standard EMV byl vytvořen společnostmi MasterCard, Visa a Europay v roce 1994, kdy se tyto karetní společnosti společně dohodly na generaci platebních karet, které budou postaveny na čipové technologii. U této čipové technologie je kladen velký důraz na zabezpečení technologie, minimální možnost zneužití a zároveň garance vzájemné kompatibility karet na celém světě. Standard EMV rozdělujeme na čtyři dokumenty. První dokument stanovuje elektrické parametry, mechanické vlastnosti, přenosové protokoly, souborovou strukturu platebních terminálů a čipových karet. Druhý dokument se zabývá

bezpečnostními požadavky na platební systém (generování kryptografických klíčů a šifrování). Třetí dokument specifikuje a definuje požadavky na aplikace a strukturu APDU příkazů a poslední dokument stanovuje povinné a požadavky na platební terminály.

Hlavní výhody čipových technologií jsou:

- *Vyšší bezpečnost* - výrazně klesl počet podvodů
- *Rychlost*
- *Více možností* - na čip můžeme uložit více informací než na magnetický proužek

2.3 Zabezpečení elektronických platebních systémů

S rostoucím počtem uživatelů využívajících internetové bankovnictví roste stejně rychle i otázka zabezpečení. Pro další vývoj a rozšiřování elektronických platebních systémů o nové funkce se zabezpečení těchto systémů stává důležitějším. Existují standardy, kterých by se měl uživatel řídit a tím tak zmenšit možnost útoku a ztráty jeho osobních dat, které následně mohou vést k finanční ztrátě na bankovním účtu. Základ, bez kterého by se neměl počítač připojovat k žádnému internetovému bankovnictví a ani k žádnému online platebnímu systému, je kvalitní a aktualizovaný antivirový software. Dalším mechanismem k zabránění útoků je šifrování přenášených dat, využívání elektronických podpisů a samozřejmostí je i využívání bezpečnostních protokolů, mezi které se v dnešní řadí protokol SSL.

2.3.1 Zabezpečení přihlášení do internetového bankovnictví

První zabezpečovací proces se nazývá „autentizace klienta“. Tento krok slouží bance k ověření a identifikaci klienta, který vstupuje do internetového bankovnictví. Jednotlivé banky se v tomto kroku liší. Některé banky nabízejí v základní nabídce pouze starší a ne zrovna kvalitní zabezpečení, kdy je klient identifikován a ověřen pouze pomocí přihlašovacího jména a hesla (např. Airbank, mBank). Jiné banky nabízejí na výběr svým klientům z několika možných typů ověření autentizace pro vstup do internetového bankovnictví.

2.3.1.1 Autentizace pomocí přihlašovacího jména/čísla a hesla

Tato autentizace patří mezi nejstarší a nejméně bezpečné. Tento způsob zabezpečení vstupu do internetového bankovnictví je velmi nebezpečný. Hlavní výhoda a silná stránka této autentizace je, že klient se může v rychlosti přihlásit do internetového bankovnictví i

ze svého mobilního telefonu. Na druhou stranu existuje několik způsobů, jak tyto údaje nutné k přihlášení snadno získat, a proto se tato metoda neřadí mezi příliš vhodné a bezpečné. Nejméně náročným způsobem, jak získat přihlašovací jméno a heslo je metoda "přes rameno klienta", kdy útočník pozoruje klienta banky při neopatrném zadávání citlivých přihlašovacích údajů na klávesnici počítače, mobilu apod. Dalším způsobem je použití softwarových nebo hardwarových keyloggerů, které jsou schopné zaznamenávat všechna stisknutá tlačítka klávesnice, a ty následně ukládat v textové podobě do vnitřní paměti (hardwarové keyloggery) nebo paměti počítače, a ty následně odeslat kamkoliv prostřednictvím internetu. Díky tomu, že je pro přihlášení potřeba pouze těchto dvou údajů, vznikly různé techniky jak tyto údaje z uživatelů získat. Mezi oblíbené techniky patří phishing, kterému je věnována větší pozornost na následujících stránkách v kapitole 3.3.2. Phishing.

2.3.1.2 Autentizace pomocí certifikátu

Ověření přístupu pomocí certifikátu je daleko bezpečnějším způsobem k přihlášení klienta do internetového bankovnictví (např. Komerční banka). Tento certifikát je časově omezen a slouží jako vstupní klíč vydávaný bankou klienta spolu s internetovým bankovnictvím. Klient si certifikát uloží na externí disk či vypálí na CD a při přihlášení do internetového bankovnictví namísto uživatelského jména na vstupní bráně nastaví cestu k certifikátu. Nevýhoda této vstupní ochrany je, že klíč může být snadno zkopírován, a tudíž je lepší jej uchovávat na externím disku, nikoli však přímo v PC klienta. Klient se bez certifikátu nemohou do banky přihlásit, což se může jevit jako problém při pokusu o přihlášení z mobilního telefonu nebo z jiného počítače, kdy vstupní klíč nemá zrovna u sebe.

Obr. 7 Přihlášení do IB u Komerční banky

2.3.1.3 Zabezpečení přihlášení pomocí čipové karty

Další možností, která má na rozdíl od certifikátu uloženého na externím úložišti vyšší stupeň zabezpečení, je využívání čipové karty. Princip tohoto ověření a identifikace klienta je stejný jako u využívání certifikátu, ale s tím rozdílem, že jsou údaje pevně uloženy na kartě a nemohou být zkopírovány. Jediná možnost zneužití nastává pouze při odcizení čipové karty. Pro přístup do internetového bankovnictví za pomoci čipové karty je samozřejmě potřeba znát i heslo k čipové kartě, nebo v některých bankách PIN kód přidělený ke kartě. K této kartě je navíc i nutnost mít nainstalovanou čtečku karet, jejíž cena se v dnešní době pohybuje okolo 500kč.

2.3.1.4 Autentizace pomocí SMS a PIN kalkulátoru

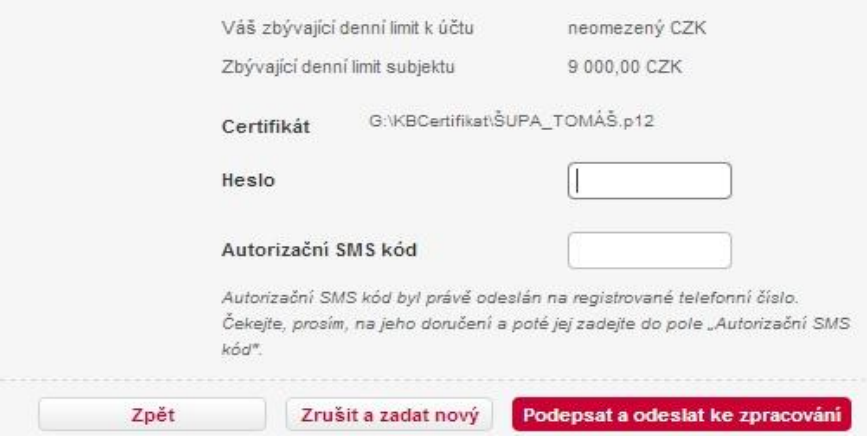
Následují dva další možné způsoby zabezpečení vstupu do IB banky. Prvním z těchto dvou způsobů je ověření klienta pomocí mobilního telefonu, kdy klient v internetové aplikaci zadává své klientské číslo. Na základě tohoto identifikačního čísla server vyhledá telefonní číslo, které je přiřazené k tomuto klientskému číslu a odešle na něj speciální přístupový kód, pomocí kterého se klient může přihlásit. Posledním způsobem a dá se říct, že i nejbezpečnějším typem přihlášení je ověření klienta pomocí PIN kalkulátoru. Klient do tohoto kalkulátoru, který je podobný klasické kalkulačce vyťuká své klientské číslo PIN kód a kalkulátor vygeneruje speciální autentizační kód, který klient vkládá při vstupu do internetové aplikace své banky. Tento kód je při každém pokusu o jeho získání jiný. Hlavní výhodou a kladnou stránkou tohoto zabezpečení je, že tento způsob patří momentálně k těm nejvíce bezpečným způsobům autentizace. Jediný způsob útočníka získat přístup do internetového bankovnictví klienta je získat přímo tento kalkulátor, bez kterého je přihlášení nemožné.

Obr. 8 PIN kalkulátor značky SEB

2.3.2 Zabezpečení aktivních a pasivních operací

Aktivní operace jsou takové operace, u kterých dochází k pohybu finančních prostředků na účtu. Mezi nejčastější typy zabezpečení aktivních operací, které banky nabízejí, patří zabezpečení:

- *pomocí SMS kódu*
- *certifikátu*
- *PIN kalkulátoru*



Obr. 9 Ověření aktivní operace u Komerční banky

V dnešní době převládá v České republice zabezpečení transakce (aktivní operace) pomocí SMS kódu. Tento způsob zabezpečení funguje na stejném principu jako u ověření klienta při přihlášení do platebního systému pomocí SMS kódu. Jakmile klient vyplní všechny informace potřebné pro provedení platby (číslo účtu, částka, v.s. atd.), systém ověří klienta vygenerováním číselného kódu, který odešle vlastníkovi účtu na jeho mobilní telefon. Tento kód je platný pouze pro aktuální operace a má časové omezení platnosti, které se u jednotlivých bank mohou lišit. Klient tento kód zadá do internetové aplikace a po jeho správné identifikaci přichází na řadu zpracování transakce, u které je potřeba ze strany klienta mít pouze potřebný zůstatek finančních prostředků k uskutečnění platby. V opačném případě, kdy není vyplněno pole pro zadání SMS kódu a autorizace platby není klientem ověřena tak zabezpečený systém platbu nedovolí a platba není provedena.

Pasivní operace jsou takové, u kterých nedochází k pohybu finančních prostředků. Tyto operace jsou zabezpečeny pouze vstupními bezpečnostními prvky, které zabezpečují vstup do internetového bankovnictví. V tomto případě nemá velký smysl se dál pokoušet např. zobrazení aktuálního zůstatku na účtu.

Mezi pasivní operace můžeme zařadit:

- *aktuální zůstatek finančních prostředků na účtu*
- *výpis a historie bankovních operací*
- *sledování transakcí a změn na účtu*

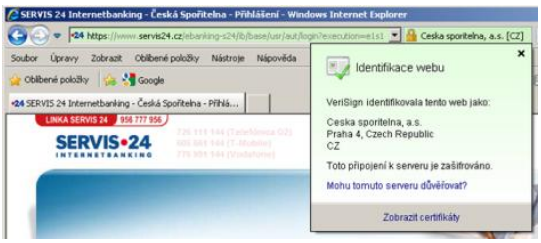
2.3.3 Zabezpečení elektronických platebních systémů - SSL/HTTPS a 3D Secure

Dnes, kdy je v nabídce velké množství různých softwarových a hardwarových platforem, vzniká potřeba a nutnost umožnit, aby všechny tyto prostředky mohli společně komunikovat, a to bez omezení a bez závislosti na svém softwarovém a hardwarovém vybavení. Tohoto cíle se nám daří dosáhnout pomocí standardizovaných protokolů. Dříve byl využíván protokol SET, vyvinutý společností VISA, ale v dnešní době ho nahradila technologie 3D SECURE, která využívá protokoly SSL/TLS. Technologie 3D SECURE je bankami označována jako nejvyšší možné zabezpečení, které se může klientovi nabídnout pro bezpečné platby na internetu.

Technologie zabezpečení SSL/HTTPS

SSL z anglického Secure Socket Layer doslova znamená "vrstva bezpečných socketů". Tento protokol je založen na použití asymetrické šifry, která zajišťuje pomocí šifrování a autentizací zabezpečení mezi oběma stranami komunikace. Jedná se v podstatě o vrstvu vloženou mezi transportní a aplikační. Nejčastěji se tento protokol u zabezpečení platebních systémů využívá ve spojení s https protokolem (zabezpečený HTTP protokol).

Hlavním cílem protokolu je chránit data před odposloucháváním, zfalšováním a paděláním. Zajišťuje spolehlivost a soukromí pro aplikace, které mezi sebou komunikují [23].



Obr. 10 Zabezpečený protokol https

SSL dělíme na dvě hlavní vrstvy:

- *SSL record Protocol* - tento protokol zodpovídá za enkapsulaci (zabalení) dat protokolů vyšší vrstvy (HTTP, FTP, Telnet)
- *SSL Handshake* - tento protokol zodpovídá za vytvoření zabezpečené komunikace mezi serverem a klientem. Toto zabezpečení je na založeno na ověření a odsouhlasení klíčů a šifrovacího algoritmu

Hlavní přínosy SSL

- Bezpečnost šifrování
- Spolehlivost (MAC - Message Authentication Code)
- Rozšiřitelnost o nové metody šifrování
- Interoperabilita a relativní efektivita

Využití SSL certifikátů

- online obchody (platební systémy)
- zpracovávání citlivých údajů
- výměna důvěrných informací
- projekty s administrací
- z legislativy - regulační ustanovení, které vyžadují zabezpečení přenosu

Obr. 11 Ceny SSL certifikátů na www.sslmarket.cz

3D SECURE

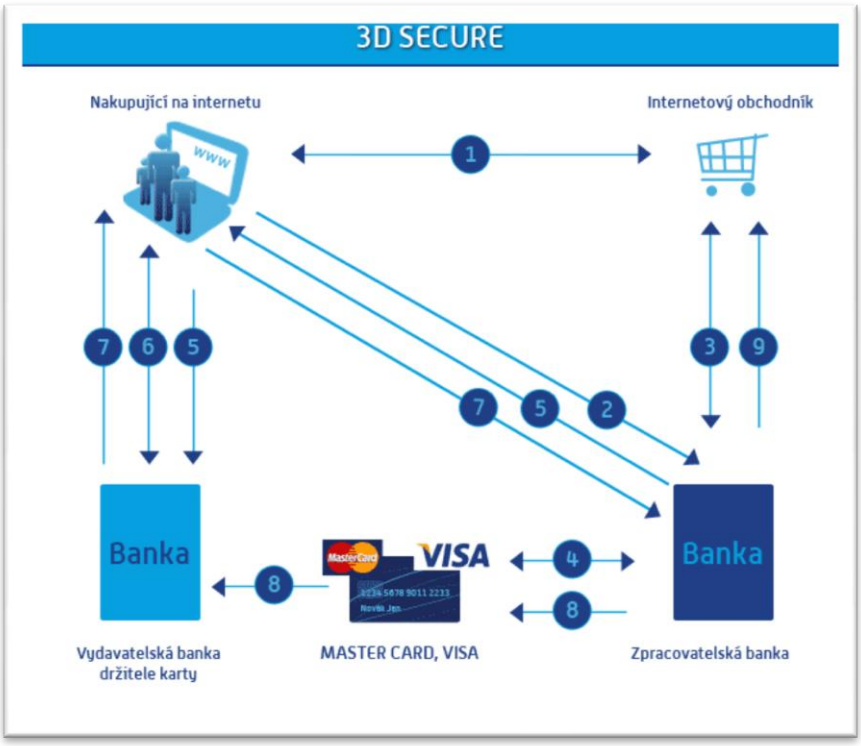
Aktuálně využívanou metodou pro bezpečnější platby na internetu je platba pomocí systému 3D Secure, který zabezpečuje ochranu tak, že veškeré údaje nutné ke zneužití platební karty neposkytuje obchodníkovi, ale přímo bance. Tento systém banky rády doporučují a označují za nejbezpečnější systém současnosti pro platby na internetu. Dříve (začátkem roku 2011) byla tato metoda využívaná pouze u internetových obchodů, které nabízeli svým zákazníkům rychlé platby pomocí platební karty. Postupem k této metodě zabezpečení přistoupila většina bank nejen v České republice, které využívají platební

karty MasterCard a Visa. Platba na internetu probíhá tak, že zákazník internetového obchodu při volbě platby kartou vyplní na zabezpečené stránce platebního systému číslo karty, datum expirace a validační CVV/CVC kód. Následně obdrží jednorázové heslo v podobě SMS zprávy na telefonní číslo registrované u banky klienta. Tento SMS kód má obvykle platnost pár minut a lze použít jen jednou. U každé další platby je generován nový kód. Tato technologie má mnoho výhod a je určitě velkým krokem kupředu v oblasti zabezpečení pro platby na internetu.

Obr. 12 Označení 3D Secure společností MasterCard a VISA

Průběh platby:

1) Zákazník si vybere zboží v internetovém obchodě.
2) Při potvrzení vybraného zboží a vybráni způsobu platby je zákazník přesměrován na stránku zpracovatelské banky, kde zadá platební údaje.
3) Odsouhlasení objednávky mezi Zpracovatelskou bankou a Obchodníkem.
4) Zpracovatelská banky vyšle dotaz na kartovou asociaci (MasterCard, VISA) a ta potvrdí zařazení/nezařazení vlastníka karty do 3D Secure systému a posílá odpověď zpátky do Zpracovatelské banky.
5) Je odeslána žádost o autentizaci ze strany zpracovatelské banky do vydavatelské banky držitele karty přes prohlížeč držitele karty.
6) Vydavatelská banka držitele karty požádá vlastníka karty o heslo. Vlastník heslo vyplní a banka ho následně potvrdí.
7) Vydavatelská banky odesílá odpověď zpátky do zpracovatelské banky přes prohlížeč nakupujícího na internetu (držitele karty).
8) Jestli tato autentizace proběhla v pořádku, je tato platba zpracována jako klasická platební transakce.
9) Zpracovatelská banka odesílá informaci internetovému obchodníkovi o výsledku celé transakce.



Obr. 13 Průběh platby 3D secure

2.4 Systémy pro platby na internetu

Jedná se o platební systémy, u kterých jsou během platby využívány informační technologie. Tyto systémy mají oproti klasickým platebním systémům velkou výhodu v zabezpečení citlivých informací. EPS vytvářejí prostředníka mezi odesílatelem a příjemcem platby, a díky tomu se příjemce žádné citlivé informace nedozví. Mezi hlavní výhody a faktory těchto systémů patří:

- Rychlost převodu peněz
- Snadná uživatelská obsluha
- Nízké poplatky za platbu na internetu
- Zabezpečení informací

2.4.1 PaySec

Platební systém PaySec, vytvořený bankou ČSOB ve spolupráci s Poštovní spořitelnou, slouží k rychlému a snadnému placení po internetu, a je tak českou moderní alternativou celosvětového platebního systému PayPal. K platbě pomocí PaySec však nepotřebujete platební kartu, jako je tomu u plateb prostřednictvím PayPal. Nakupování s PaySec je

bezpečnější, jelikož při platbě neuvádíte žádné citlivé údaje. Každá platba je také ověřena zasláním SMS s autorizačním kódem a to je hlavní silná stránka tohoto platebního systému. Pro užívání tohoto platebního systému se stačí jen zaregistrovat vyplněním on-line formuláře na stránkách www.paysec.cz, PaySec je zároveň přístupný pro klienty všech českých bank. Nezáleží na státní příslušnosti uživatele, avšak účet vedený u české banky je podmínkou k založení PaySec konta. Konto je nutné pravidelně dobíjet prostřednictvím bankovního převodu anebo za poplatek platební kartou. PaySec je univerzální, umožňuji internetové platby i převod peněz na jiný účet, je navíc rychlejší než běžný bankovní účet a jeho vedení i platby jsou zcela zdarma. Systém PaySec je podporován stovkami českých e-shopů, dále například společnostmi, jako jsou Aukro.cz či České dráhy [15].

- **Zabezpečení platebního systému PaySec**
  - Dobíjení a ochrany platby systémem 3D Secure
  - Platby provádí samotná banka bez přítomnosti obchodníka
  - Platby jsou autorizovány SMS kódem
  - Systém je šifrován 128bit SSL protokolem (Secure Sockets Layer)

- **Platební metody**
  - Platební karty: VISA, MasterCard, Diners Club
  - Internetové bankovnictví: ČSOB, Poštovní spořitelna (Era)
  - Další on-line platby: elektronická peněženka PaySec, mobilní platba přes aplikaci MasterCard Mobile pro platební karty VISA a MasterCard (podporováno operačním systémem Android a iOS)

2.4.2 PayU

PayU je mezinárodní internetový platební systém, pocházející z dílny společnosti Naspers, která působí již od roku 1915 a zabývá se on-line médii a e-commerce systémy. Pomocí PayU je možné platit v Maďarsku, Polsku, Rusku, Rumunsku, Turecku, Ukrajině, a od roku 2011 také v České republice. V Evropě byl zaveden už v roce 2005. Platební systém PayU je podobný jako u ostatních platebních systému, na rozdíl od českého PaySec však PayU umožňuje platit platební kartou. Pro pasivní uživatele je PayU zcela zdarma, přičemž poplatky za on-line platby jsou určovány individuálně podle průměrného obratu a výše transakce, a není nutná žádná registrace. Pro aktivní uživatele, tedy majitele či provozovatele e-shopů, tak činí výhodný (nejvýhodnější u nás) implementační poplatek

3900,- Kč, k registraci e-shopu stačí vyplnit registrační formulář na stránkách www.payu.cz a uzavřít klasickou či elektronickou smlouvu pro užívání PayU konta.

Platební bránu PayU u nás kromě cca 700 e-shopů podporují například Aukro.cz, Heureka.cz, Škoda Auto, Economia, Česká pošta, Tipsport nebo parfumerie Marionnaud [16].

- **Zabezpečení platebního systému PayU**
  - Platební transakce jsou chráněny 3D Secure systémem
  - Platby jsou na základě vydané licence kontrolovány ČNB
  - Platby provádí samotná banka bez přítomnosti obchodníka jako prostředníka
  - Systém je zabezpečen pomocí PCI DSS certifikátu
  - Systém je šifrován 128bit SSL protokolem
  - Bankovní převody jsou dále chráněny vlastními systémy jednotlivých bank

- **Platební metody**
  - Platební karty: VISA, MasterCard, Diners Club
  - Internetové bankovnictví: Česká spořitelna, Komerční banka, GE Money Bank, mBank, Raiffeisenbank, Sberbank, Fio banka
  - Další online platby: elektronická peněženka, mobilní platba přes MOBITO (od společnosti Mopet CZ), mobilní platba přes aplikaci MasterCard Mobile pro platební karty VISA a MasterCard (podporováno operačním systémem Android a iOS)
  - Offline platby: hotovostní platba SuperCASH (na terminálech Sazka a na přepážkách České pošty), platba složenkou

2.4.3 PayPal

Systém PayPal vznikl v roce 1998 a představuje nejznámější platební systém, rozšířený na celém světě. V Americe se úspěšně rozšířil díky masivní kampani, kdy každému novému uživateli připsal na jeho PayPal konto 10 dolarů. V roce 2000 pak PayPal koupila společnost eBay, největší internetový aukční portál na světě. Na rozdíl od ostatních platebních systému se PayPal konto nemusí dobíjet, ale platby jsou odesílány přímo prostřednictvím platební karty. Princip je tedy podobný jako samotná platba kartou, navíc je rychlejší, jelikož platební údaje a údaje o platební kartě se zadávají pouze jednou při

založení PayPal účtu. Přestože systém vyzívá k registraci, kterou lze uskutečnit na stránkách www.paypal.com, poněkud nevýraznou formou nabízí také platbu kartou bez registrace. Tato možnost je však méně bezpečná, a to z důvodu opakovaného zadávání citlivých údajů [17]. Při zakládání PayPal účtu si uživatel může vybrat z následujících možností:

- *Personal* - účet pro ty, kteří nakupují online
- *Premier* - účet pro ty, kteří nakupují a prodávají online
- *Business* - účet pro obchodníky

Výhodou je možnost automatického převedení transakcí na českou měnu, nicméně systém PayPal stále není možné zobrazit v češtině, výchozími jazyky jsou tak stále pouze angličtina, španělština, francouzština a čínština. S touto službou také není možné převádět peníze na cizí účty. Platební operace jsou zdarma, při převodu měny je účtován poplatek 2,5 % z platby, další poplatky jsou pak účtovány na základě výše nebo druhu jednotlivých transakcí.
Platby PayPal jsou podporovány řadou českých e-shopů a tisíci prodejci na celém světě, tím hlavním je bezesporu právě eBay.com.

- **Zabezpečení platebního systému PayPal**
    - Údaje o platební kartě se zadávají pouze jednou, a to při registraci účtu – platbu provází pouze sám PayPal bez přítomnosti obchodníka
    - Systém je šifrován 168bit SSL protokolem
    - Autorizace uživatele e-mailem
    - Verifikace karty - pro transakce vyšší než 2500,- Kč je nutné ověření registrované platební karty
    - Nastavení pomocí rozhraní HTTPS
- **Platební metody**
    - Platební karty: VISA, MasterCard, American Express, PayPal, Discover
    - Ostatní platby v jednotlivých zemích se liší

2.4.4 Moneybookers - Skrill

MoneyBookers je mezinárodní platební systém, podporovaný prodejci ve více než 30zemích světa. V roce 2007 byl systém MoneyBookers odkoupen společností Investcorp Technology Partners a začal nově vystupovat pod názvem Skills. Systém Skills představuje

budoucnost systému MoneyBookers a umožňuje dnes platbu v téměř 200 zemích po celém světě [18].

Registrace

Uživatel má taktéž při vytváření účtu možnost volby:

a) Osobní účet – online platby, Skrill (MoneyBookers) platby, převod peněz na bankovní účet
b) Podnikatelský účet – navíc příjem online plateb, využití Skrill (MoneyBookers) k platbám pro zaměstnance, příjem platby za vlastní služby, platby pro dodavatele.

U osobních účtů si Skrill (MoneyBookers) účtuje poplatek ve výši minimálně 1,- EUR měsíčně, při převodu měny (převod ve více než 40měnách) se pak hradí 2,49 % z platby. Příchozí transakce i vklad peněz je zcela zdarma. Umožňuje tedy přijímání a odesílání peněz, a to i na zahraniční účty.

- **Zabezpečení platebního systému Skrill (MoneyBookers)**
  - Autorizace uživatele e-mailem
  - Verifikační systém – ověření totožnosti uživatele, platební karty i bankovního účtu
  - Systém je šifrován 256bit SSL protokolem
  - Systém je zabezpečen pomocí PCI DSS certifikátu
- **Platební metody**
  - Platební karty: VISA, MasterCard, American Express, Diners Club, JBC
  - Internetové bankovnictví: banky podporující MoneyBookers (Skrill) platby se v jednotlivých zemích liší
  - Další online platby: elektronická peněženka Skrill, předplacená karta Moneybookers MasterCard (on-line i off-line platby)
  - Ostatní platby: více než 100 platebních metod (v jednotlivých zemích se liší), platba na splátky, platba na fakturu, platba složenkou
  - V ČR pouze platba platební kartou (viz výše) a bankovním převodem.

Obr. 14 Moneybookers Skrill

II. PRAKTICKÁ ČÁST

3 ZABEZPEČENÍ PLATEBNÍCH KARET U BANK V ČR

Není žádnou novinkou, že počet platebních karet v České republice prudce stoupá každým rokem. Za rok 2012 bylo v České republice podle Sdružení pro bankovní karty (BNK) vydáno přes 10 172 883 platebních karet, celkem se objem výběrů z bankomatů vyšplhal na 629 510 831 000 Kč. Meziročně se dokonce zvýšil počet transakcí v obchodních místech o více než 14%, naproti tomu se výběr z bankomatu zvýšil pouze o 2,7% - klienti bank začínají dávat více přednost platbě kartou než výběrem z bankomatu, kdy průměrná částka uhrazená přímo kartou je za minulý rok 921 Kč. Zabezpečení platebních karet a internetového bankovnictví udělal v České republice krok dopředu. Není už žádná banka, která by nepoužívala minimálně 128 bitové šifrování pomocí technologie SSL, ale stále je co vylepšovat a nic není nikdy dlouho dokonalé a bezpečné. Většina bank se snaží na svých internetových stránkách varovat o možných nástrahách a nebezpečí, které mohou vzniknout s nezodpovědným používáním platební karty, ale pořád existují i takové banky, které si s upozorněním klientů na možné nebezpečí příliš hlavu nelámou a spíše se snaží informovat klienty o svých nabídkách a službách než o možných nástrahách a podvodech s platebními kartami, které mohou uživatele karet potkat.

Bezpečnostní prvky a možností zabezpečení platebních karet

V dnešní době využívají všechny banky na území České republiky šifrování internetového bankovnictví pomocí minimálně 128 bitového kódu a technologií SSL. Banky se tedy v České republice mezi sebou liší pouze v možnostech zabezpečení autentizace klienta, zabezpečení aktivních operací (provedení transakce) a dalších služeb, díky kterým se snaží zvýšit zabezpečení svých služeb. Jsou banky, které se snaží své klienty informovat, ale drtivou většinu jenom zajímá počet klientů. Zabezpečení platebních karet v České republice se dá určit pouze podle služeb, které daná banka nabízí. Mezi tyto služby patří ochranné prvky při vstupu do internetového bankovnictví, nebo i nabízené pojištění platebních karet. Veškeré další bezpečnostní prvky týkající se platebních karet, mezi které patří technologie čipu, nebo i podpisové proužky nespadají pod banky, ale přímo pod vydavatele karet. Mezi největší světové vydavatele řadíme společnosti MasterCard a Visa jejichž karty nalezneme po celém světě.

3.1 Banky ČR

3.1.1 Česká spořitelna

Tato banka nejlépe ze všech bank působících na území České republiky informuje své klienty o možných hrozbách a možnostech zabezpečení platebních karet. Pravidelně varuje své klienty na svých internetových stránkách o aktuálních pokusech o phishing, virech zvyšující nebezpečí útoku a ohrožení účtů. Pro přístup do internetového bankovnictví je využíváno 128bitové šifrování pomocí SSL technologie. V nabídce banky je i GSM banking, zabezpečený díky šifrovaným SMS zprávám za použití 3DES šifry. Banka nabízí možnost autentizace klienta pomocí klientského čísla a hesla, ale i pomocí certifikátu. Banka vydává platební karty společnosti Visa [24].

Zabezpečení autentizace klienta:

- možnost přihlášení do internetového bankovnictví i pomocí certifikátu

Výhody

- Pojištění platební karty, které se vztahuje i na použití transakce s použitím PIN kódu
- Pojištění karty v případě násilného odcizení karty a následného vybrání hotovosti z bankomatu
- Banka na svých internetových stránkách informuje své klienty o útocích a podvodech platební kartou
- Autentizace klienta i pomocí certifikátu
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Banka nabízí pojištění platební transakce s, nebo bez použití PIN kódu
- Nabízí možnost nastavení limitu (i časového limitu výšky platby) v internetovém bankovnictví
- Podpora 24 hodin denně

Nevýhody

- Pouze jeden způsob zabezpečení autorizace platby
- Pojištěné platby na internetu pouze v případě ztráty, nebo odcizení karty
- Bankomaty i na nestřežených místech

Internetová stránka banky: http://www.csas.cz

Obr. 15 Logo České spořitelny

3.1.2 Airbank

Banka AirBank začala nabízet své služby v České republice v roce 2011. Je členem investiční a finanční skupiny PPF, která patří k největším investičním a finančním skupinám ve střední a východní Evropě. Přístup do internetového bankovnictví je šifrován protokolem https a certifikátem vydaným u společnosti Verisign. Slogan této banky zní "I banku můžete mít rádi", ale na rozdíl od jiných bank v ČR nenabízí žádné další možnosti autentizace klienta při vstupu do internetového bankovnictví. Nabízí pouze ověření uživatele uživatelským jménem a heslem, které patří k nejslabším typům zabezpečení přístupu do internetového bankovnictví. Banka od roku 2012 nabízí k účtu i bezkontaktní platební karty. Velká nevýhoda této banky je ve způsobu zabezpečení autentizace a vstupu klienta do internetového bankovnictví, kdy nabízí pouze zabezpečení přístupu pomocí přihlašovacího jména a hesla. Na rozdíl od většiny bank tato banka na svých internetových stránkách neinformuje klienty o možných nebezpečích, které mohou nastat při neopatrném používání platební karty. Jako jediná také nenabízí žádné možnosti pojištění platební karty proti ztrátě, nebo krádeži [25].

Zabezpečení autentizace klienta:

- nabízí pouze pomocí přihlašovacího jména a hesla

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Možnost změny PIN kódu i na bankomatu
- Banka rozšiřuje síť bankomatů pouze v uzavřených prostorách, které jsou nepřetržitě hlídány bezpečnostními kamerami.
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- podpora 24 hodin denně

Nevýhody

- Zabezpečení autentizace klienta pouze pomocí přihlašovacího jména a hesla
- Banka nenabízí žádné možnosti pojištění karty proti krádeži, nebo ztrátě
- Chybí pojištění platby na internetu bez přítomnosti karty

Internetová stránka banky: https://www.airbank.cz/

Obr. 16 Logo Airbank

3.1.3 ČSOB

Tato banka byla založena v roce 1964. Ke konci roku 2012 měla přes 1349 tisíc uživatelů internetového bankovnictví a přes 890 bankomatů na území celé České republiky. Pro přihlášení k internetovému bankovnictví má klient možnost výběru mezi identifikačním číslem, PIN kódem a SMS klíčem, nebo pomocí čipové karty. Autorizace platby probíhá pomocí šifrovaného SMS klíče, nebo čipové karty. Zabezpečení internetového bankovnictví systémem 3D Secure. Umožňuje správu účtu pomocí telefonu službou ČSOB Mobil 24. Následný přístup ke službám a aktivní operace mobilního bankovnictví jsou ověřovány číselným BPIN číslem. Vydává platební karty společností MasterCard, Visa i Diners Club [26].

Zabezpečení autentizace klienta:

- v nabídce banky zabezpečení přístupu pomocí identifikačního čísla, PINU, SMS klíče i pomocí čipové karty

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Možnost změny PIN kódu karty i na bankomatu
- Způsob autorizace pomocí SMS klíče odeslaného šifrovanou zprávou i pomocí čipové karty
- Banka informuje o bezpečnostních zásadách pro používání karty a internetového bankovnictví
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- po 3. chybném pokusu o přihlášení je internetové bankovnictví zablokováno a pro odblokování je nutné navštívit fyzicky pobočku banky
- Podpora 24 hodin denně

Nevýhody

- Bankomaty i na nestřežených místech
- Pojištění platební karty se nevztahuje na transakce s použitím PIN kódu, za které ČSOB nepřebrala zodpovědnost a na platby na internetu bez přítomnosti platební karty
- Banka nabízí pojištění transakce za použitím PIN kódu, pouze pokud dojde k jeho prozrazení pod hrozbou násilí

Internetová stránka banky: http://www.csob.cz/

Obr. 17 Logo ČSOB

3.1.4 Komerční banka

Tato banka byla založena roku 1990. Pro přístup do internetového bankovnictví banka nabízí ze dvou možností autorizace. Pomocí certifikátu, nebo pomocí čipové karty. Banka nabízí pouze základní pojištění platební karty proti odcizení, které neochraňuje klienty proti nebezpečím online transakcí na internetu. Šifrování komunikace pro internetové bankovnictví a využívání e-Card je zabezpečeno pomocí SSL certifikátu. Největší výhoda, ale zároveň i nevýhoda této banky je, že umísťuje bankomaty i na špatně zabezpečené místa v okolí obchodních domu do míst, které nejsou střeženy kamerovým systémem, a tak své klienty vystavuje nebezpečí skimmingu. Banka vydává platební karty společností VISA, MasterCard a Maestro [27].

Zabezpečení autentizace klienta:

- zabezpečení přístupu pomocí certifikátu, nebo za použití čipové karty

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Možnost změny PIN kódu karty i na bankomatu
- Banka informuje ve zkratce o bezpečnostních zásadách pro používání karty a internetového bankovnictví
- Banka nabízí pojištění platebních karet proti ztrátě a krádeži
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Po třetím chybném pokusu o přihlášení je internetové bankovnictví zablokováno a pro odblokování je nutné fyzicky navštívit pobočku banky
- Internetové bankovnictví zobrazuje 10 posledních přihlášení (datum, čas, IP adresa)
- Autorizační SMS klíč odeslán šifrovanou SMS zprávou
- Podpora 24 hodin denně

Nevýhody

- Bankomaty i na nestřežených místech
- Banka nabízí pojištění transakce za použitím PIN kódu pouze pokud dojde k jeho prozrazení pod hrozbou násilí
- Nenabízí pojištěné platby na internetu a bez přítomnosti karty

Internetová stránka banky: http://www.kb.cz/

Obr. 18 Logo Komerční banky

3.1.5 Mbank

Tato banka patřící do německé skupiny Commerzbank a působí na českém a slovenském trhu od konce roku 2007. Mezi hlavní výhody této banky patří nulový poplatek za základní bankovní operace a vedení účtu. Zabezpečení autentizace klienta je pouze pomocí přihlašovacího klientského čísla a hesla, které se musí skládat minimálně z osmi znaků složených z číslic a písmen. Na rozdíl od ostatních bank využívá mBank jako šifrovací protokol TLS 1.0. Tento šifrovací protokol, který se stará o zabezpečení komunikace je nástupce protokolu SSL. Oproti verzi SSL 3.0 nemá žádné výraznější rozdíly. Tato banka jako jedna z mála nemá vlastní bankomaty, a to ani na svých pobočkách [28].

Zabezpečení autentizace klienta:

- zabezpečení přístupu pouze pomocí přihlašovacího ID a hesla

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Způsob autorizace pomocí hesla a autorizační SMS
- Banka informuje o bezpečnostních zásadách pro používání karty a internetového bankovnictví
- Banka nabízí pojištění platebních karet proti ztrátě a krádeži
- Pojištění transakce za použití PIN kódu
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Po třetím chybném pokusu o přihlášení je internetové bankovnictví zablokováno a pro odblokování je nutné navštívit fyzicky pobočku banky
- Podpora 24 hodin denně, banka provozuje linku bezpečnosti

Nevýhody

- Zabezpečení přístupu pouze pomocí přihlašovacího ID a hesla
- Pojištěné platby na internetu pouze v případě ztráty, nebo odcizení karty

Internetová stránka banky: http://www.mbank.cz/

Obr. 19 Logo Mbank

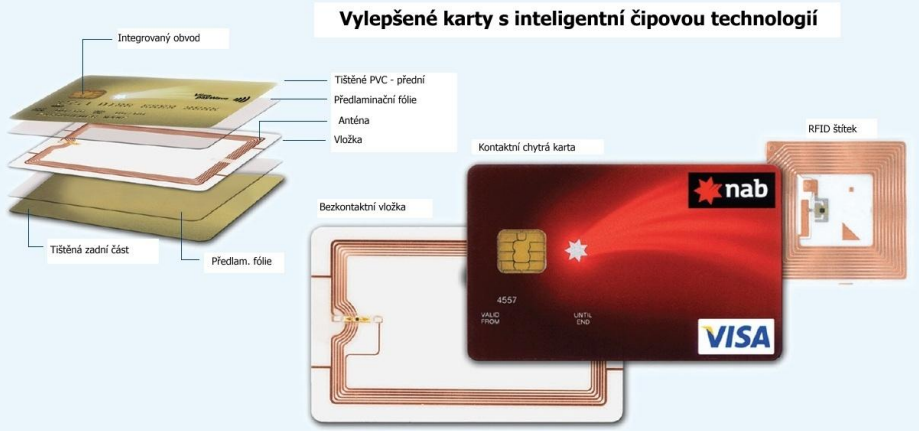
3.2 Bezkontaktní platby v ČR

Bezkontaktní platební karty zažívají od konce roku 2011, kdy přišly do České republiky, velký vzestup. První průzkumy, které měly zjistit zájem o tuto možnost bezhotovostní platby, ukázaly podle karetní asociace MasterCard, že více než tři čtvrtiny populace České republiky má o tento typ platby zájem. V průzkumu bylo zjištěno (celkem v 84%), že platba bezkontaktně by byla nejvíce oceněna v supermarketech a malých obchodech s potravinami, ale i v restauracích a ve veřejné dopravě. Na většině míst, kde byla donedávna možnost bezhotovostní platby platební kartou, jsou nyní platební terminály vybaveny i snímačem pro bezkontaktní platby. Banky tuto možnost bezhotovostní platby prezentují jako velmi bezpečnou už jen tím, že nemusíte kartu vydávat z ruky a po celou dobu máte možnost dohlížet na její průběh.

Obr. 20 Označení terminálů podporujících bezkontaktní platby

Na rozdíl od platby běžnou platební kartou, vybavenou magnetickým proužkem nebo čipem, kde bylo zapotřebí vložit kartu do terminálu, umožňují bezkontaktní platby rychlejší platbu za zboží pouhým přiložením platební karty k terminálu bez nutnosti zadávat PIN kód nebo kartu vkládat fyzicky do terminálu. Tato technologie lze velmi

snadno zabudovat např. do mobilního telefonu, hodinek, nebo klíčenek. Dokonce je možné provádět bezkontaktní platby i přes peněženku, nebo přímo z kabelky a tím vznikají otázky ohledně zabezpečení a bezpečnosti celé technologie bezkontaktních plateb.



Obr. 21 Bezkontaktní platební karta

3.2.1 Zabezpečení

Princip bezkontaktní platby funguje na technologii NFC (Near Field Communication), která je rozšířením standardu RFID. NFC technologie, schválená v roce 2003 jako ISO/IEC standard, využívá ke komunikaci elektromagnetickou indukci, což je zásadní rozdíl od bezdrátového připojení k internetu (Wi-Fi), který využívá rádiové vysílání. S vývojem této technologie a následným využitím pro bezkontaktní platby vznikaly otázky ohledně zabezpečení, protože veškerá komunikace mezi bezkontaktní platební kartou a terminálem je nešifrovaná. U této technologie se uvádí potřebná vzdálenost pro navázání spojení maximálně 4 cm. Tato extrémně krátká vzdálenost představuje hlavní argument bank a obhájců bezpečnosti této technologie.

Rozdělení NFC podle volby provozu

- *aktivní* - oba prvky jsou aktivní a mohou si mezi sebou vyměňovat informace
- *pasivní* - jeden z prvků je aktivní vysílač a druhý je pouze pasivní prvek - pasivní prvky jsou napájeny elektromagnetickým polem, které vysílá vysílač

	NFC
Kompatibilita s RFID	Ano (ISO 18000-3)
Tvůrce standardu	ISO/IEC
Standard	ISO 13157
Typ sítě	Point-to-point
Kryptografie (šifrování)	Ne s RFID
Dosah	< 0,2 m
Frekvence	13,56 MHz
Rychlost přenosu dat	424 kbit/s
Čas pro konfiguraci přenosu	< 0,1 s
Spotřeba energie	< 15 mA

Tab. I. Specifikace NFC

Celá technologie NFC plateb vychází se staršího RFID fungujícího na principu pasivních prvků, které jsou běžně k vidění v každém větším obchodu s oblečením jako malé šedé krabičky připevnění na oblečení. Jakmile se tento pasivní prvek dostane do dosahu vysílače (u vchodu/východu z obchodu), spustí vysílač hlasitý alarm a chrání tak zboží proti krádeži. Vysilač zahajuje komunikace na frekvenčním pásmu 13,56 MHz a svým vysíláním vytváří magnetické pole, které napájí obvody v přijímačích a ty se mohou zapojit do komunikace. V důsledku zvýšení bezpečnosti a minimalizaci neoprávněných transakcí vznikl kompromis mezi rychlejší platbou a dostatečným zabezpečením. Pro platbu bezkontaktní kartou byly v důsledku absence ověřování PIN kódem stanoveny následující bezpečnostní mechanismy.

Bezpečnostní limity

Pro vyšší míru zabezpečení existují tři bezpečnostní limity počtu plateb, po jejichž dosažení v daném dnu nelze platit dále platit bezkontaktně, ale pouze za použití čipu s ověřením totožnosti pomocí PIN kódu.

- *Soft limit (online terminály)* - je nastaven počet transakcí, které lze uskutečnit pomocí online terminálů. Po vyčerpání tohoto limitu je transakce zamítnuta a nastává pouze možnost platby za použití čipu nebo magnetického proužku.

- *Soft limit (offline terminály)* - je nastaven počet transakcí, které je možné uskutečnit pomocí offline terminálů. Po vyčerpání tohoto limitu je transakce zamítnuta a nastává pouze možnost platby za použití čipu nebo magnetického proužku.
- *Pevný limit (hard limit)* - karta má pevně stanoven počet, který je možné daný den uskutečnit bezkontaktně. Po vyčerpání tohoto limitu je transakce zamítnuta a nastává pouze možnost platby za použití čipu nebo magnetického proužku.

Územní limit

Územní limit platby je maximální hodnota platby, u které není vyžadováno ověření PIN kódem. Tento limit je v České republice nastaven na 500 Kč a platí pro každou jednotlivou platbu. Pokud je tedy platba vyšší než 500 Kč, bude vždy plátce vyzván k zadání PIN kódu. Zároveň pro zvýšení bezpečnosti může být klient k ověření totožnosti vyzván k zadání PIN kódu náhodně i u plateb menších než je nastaven limit pro dané území.

Stát	Limit
Česká republika	500 Kč
Čína	100 CNY (290 Kč)
USA	50 USD (1000 Kč)
Rumunsko	100 RON (600 Kč)
Švýcarsko	40 CHF (840Kč)
Průměr v Evropě	25 EUR (625 Kč)

Tab. II. Uzemní limity pro bezkontaktní platby v zahraničí

Vzdálenost

Vzdáleností rozumíme maximální možnou dálku bezkontaktní platební karty od platebního terminálu. Jednotlivé banky obvykle udávají maximální vzdálenost dva až čtyři centimetry.

3.2.2 Možné rizika

Banky s příchodem bezkontaktních karet tuto technologii velmi rády srovnávají v kontextu bezpečnosti se stejnou úrovní zabezpečení jako u klasických karet s magnetickým proužkem, u kterých je ověřování totožnosti klienta kontrolováno znalostí PIN kódu. Ve

skutečnosti se bezkontaktní platební karty nedají se zabezpečením klasických karet srovnávat.

Hlavní chyby technologie NFC u použití bezkontaktních platebních karet

- Veškerá komunikace mezi kartou a platebním terminálem není šifrovaná, a tak lze přenos odposlechnout, pozměnit a narušit.
- Většina platebních terminálů pracuje offline (neověřuje platnost karty)
- Hrozí vysoké riziko okopírování/zjištění údajů z platební karty

První ukázka toho, že bezpečnost bezkontaktních plateb je velmi špatná byla předvedena na konferenci Defcon, která se koná v Las Vegas. Princip spočíval v zachycení komunikace a získáním důležitých údajů mezi NFC čipem (v tomto případě v mobilním telefonu) a platebním terminálem.

Dalším důkazem toho, že platba bezkontaktních platebních karet není bezpečná předvedl Renaud Lifchitz na konferenci Hackito ergo sum, kde prezentoval jak lze snadno získat data z platebních karet vybavených NFC čipem.

3.2.3 Jak se chránit

Existují pouze dva základní způsoby jak se chránit proti možnému nebezpečí spojenému s využíváním bezkontaktních platebních karet:

- nepoužívat bezkontaktní platební karty (jediný nejbezpečnější způsob)
- nosit kartu ve speciálním pouzdře, které nepropouští rádiové signály. Tato karta lze zakoupit za 99Kč například na www.cryptalloy.cz

3.3 Možnosti a způsoby zneužití platebních karet

3.3.1 Skimming

U skimmingu na rozdíl od Lisabonské smyčky nedochází ke krádežím karty, ale ke kopírování údajů z magnetického proužku. Nejčastěji ke kopírování karet dochází:

- *přímo u bankomatu* - za pomoci speciálního zařízení, které je schopné přečíst údaje z magnetického proužku. Tyto údaje slouží k výrobě kopie karty a vytvoření padělku

- *u obchodníků* (čerpací stanice, restaurace, hotely atd.) - před vrácením karty zákazníkovi zaměstnanec data z karty zkopíruje a následně tato data, potřebná pro vytvoření kopie, sám využije pro výrobu kopie karty nebo data dál předá/prodá

Nejčastěji ke skimmingu dochází na bankomatech, kde za pomoci speciálního zařízení, které je namontováno do štěrbiny na vkládání karty, útočník získává data uložená na magnetickém proužku. Kopírovací zařízení je vytvořeno ze stejného materiálu a barvy, která je na bankomatu, a proto držitel karty netuší, že se stal obětí skimmingu. V dnešní době je většina bankomatů vybavena průhledným nástavcem, který je namontován na štěrbině pro vložení karty. Přidáním tohoto bezpečnostního prvku na bankomaty si banky slibují snížení počtu podvodů skimmingu na jejich klientech [22] .

Obr. 22 Průhledný nástavec (antiskimming)

Banky proti tomuto typu útoku bojují častějšími kontrolami bankomatů a školením zaměstnanců, kteří mají na starosti doplňování hotovosti do bankomatů. Rovněž se brání proti tomuto typu podvodu znemožněním výběru hotovosti z bankomatu v určitých zemích. Například turisté z USA nemohou použít své platební karty pro výběr z bankomatu na území České republiky. Pro potřebnou částku musí navštívit banku, která jejich totožnost sama ověří z cestovního dokladu.

K odpozorování PIN kódu používají útočníci horní prostor bankomatu, na který nainstalují minikameru, která nahraje zadávání PIN kódu. Dalším způsobem, jak získat PIN, je překrytí klávesnice bankomatu falešnou klávesnicí. Tento typ útoku se začíná čím dál více

objevovat po celém území České republiky. Zatímco v minulém roce objevili kriminalisté na jižní Moravě pouze čtyři případy skimmingu, během letošního roku se toto číslo k dnešnímu vyšplhalo už na 16 případů.

Obr. 23 Falešná dvojitá klávesnice

Jak se bránit: Uchovávat PIN v tajnosti - při zadávání PIN kódu se snažit druhou rukou schovat klávesnici. Používat bankomaty střežené kamerovým systémem, nejlépe umístěné uvnitř budovy banky, a pravidelně kontrolovat výpisy transakcí.

Metody detekce: Sledovat, zda nejsou na bankomatu provedeny nějaké úpravy, nebo dokonce i konstrukční změny. Pokud dojde k odhalení pokusu o skimming, je důležité neodcházet od bankomatu a ihned kontaktovat policii nebo banku, ke které bankomat náleží. Útočník se pravděpodobně pohybuje v okolí 50m od napadeného bankomatu. Banky by samy měly bojovat proti tomuto typu podvodu snahou informovat nejen své klienty, ale i širokou veřejnost o principech tohoto útoku.

Černý trh: V dnešní době se jedná většinou o internetová fóra, internetové stránky a IRC komunikační kanály, na kterých se scházejí lidé za účelem nákupu nebo prodeje všeho potřebného pro jakoukoliv nelegální činnost. Lze zde koupit prakticky všechno potřebné od technických výkresů bankomatu přes prázdné platební karty až po hotové řešení skimmovacího zařízení, u kterého se cena pohybuje v řádech několika tisíc dollarů. Tuto cenu určují vlastnosti, typ provedení a schopností zařízení. Cena těchto zařízení je velmi vysoká, ale jedná se o velmi výnosný byznys, kterému se věnují v drtivé většině dobře organizované skupiny z Bulharska a Rumunska. Pokud je taková skupina dobře organizovaná a sehraná, není pro ni problém získat za pouhý jeden den přes 100 klonů platebních karet, kdy za jeden tento klok získají v průměru i 500 euro. To znamená, že

návratnost investice do potřebného zařízení pro skimming lze určit pouze podle schopností skupiny, která se této ilegální činnosti věnuje.

Nejvíce žádaným zbožím na černém trhu jsou v dnešní době ukradené záznamy z platebních karet, které nazýváme dumpy. Ceny těchto dumpů se odvíjejí hlavně podle toho, z jakého státu pocházejí, nebo jestli obsahují PIN kód. Mezi nejdražší karty se řadí platební karty typu GOLD, které obsahují PIN kód. Cena takové karty se pohybuje v rozmezí od 300 do 500 dolarů. Naopak nejlevější platební karty lze pořídit i za cenu nižší než 10 dolarů za kus. Ty nejlevnější karty pocházejí z USA a jedná se o debetní karty bez PIN kódu. Funkčnost těchto karet není nikdy zaručena, protože mohou být dávno nahlášeny jako kradené a zablokované. Cena ověření funkčnosti, nebo dokonce i zůstatku na platební kartě, se na černém trhu pohybuje od pěti do deseti dolarů a odvíjí se od počtu kusů k ověření.

Obr. 24 Ukázka skimmovacího zařízení

3.3.2 Phishing

Phishing je odvozen od anglického slova "fishing", které znamená rybaření. Jedná se o útok na klienty banky za pomoci emailu [8]. Útočník rozešle hromadný email klientům banky s informací o nutné aktualizaci přihlašovacích údajů, neprovedené platbě, nebo i jako výzkum spokojenosti klientů s využíváním služeb banky. Podvodné emaily většinou obsahují aktivní link, který odkazuje na podezřelou webovou stránku, která nepatří bance klienta. Následně útočník čeká, která oběť se na tyto emaily chytí. Cílem tohoto útoku je získat přihlašovací údaje, bezpečnostní otázky využívané při obnově přihlašovacích údajů a různé další údaje potřebné pro následné zneužití. Na první pohled jsou tyto emaily velmi podobné oficiálním zprávám, které odesílá přímo banka klienta. Je velké množství případů,

kdy jsou tyto emaily psané velmi špatnou češtinou, nebo jsou dokonce celé anglicky [19]. Cena tohoto podvodu je stanovena pouze na velikosti databáze emailů klientů dané banky .

ČESKÁ SPOŘITELNA

Vážený kliente/klientko,

Jelikož využíváte služeb naší banky, tzn. osobní účet v České spořitelně, ke kterému máte aktivovanou debetní kreditní kartu VISA a v poslední době jsme zaznamenali na Vašem účtu podezřelé platební transakce, je potřeba aktualizovat data Vaší kreditní karty , v opačném případě bude Vaše kreditní karta zablokovaná a Váš účet pozastaven na dobu neurčitou. Chceme pouze ověřit, že transakce na Vašem účtě opravdu provádíteVy, jako disponent účtu a ne někdo jiný.

Pošlete nám prosím níže vyplněné parametry:

Jméno a příjmení: _____
Rodné číslo: _____/_____
Bydliště: _____
Tel.číslo:_____
Číslo kreditní karty: _____
Platnost karty od a do: _____
CVC kód (poslední 3 čísla na zadní straně): _____

Vizitka zaměstnance:

Bankéř klientského centra
Pro rozvoj
platebních karet

Bezpečnost při platbách kartou
Kontrola klientu a jejích platebních karet
Česká spořitelna,a.s.
csas@csas.cz - cic-csas@tym.cz

S pozdravem
Bankéř klientského centra

Česká spořitelna,a.s., Praha 4 Olbrachtova 1929/62 PSČ 140 00, IČ 45 24 47 82
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 1171

Obr. 25 Příklad podvodného emailu u České spořitelny

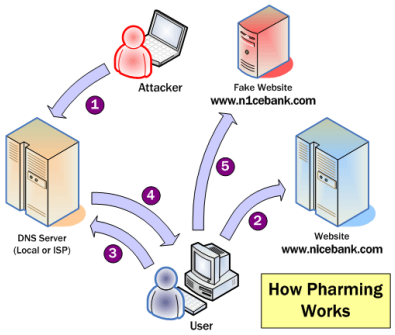
Jak se bránit: nereagovat na podezřelé emaily. Banky v žádném případě nekomunikují s klienty o přihlašovacích údajích pomocí emailu. Chránit své přihlašovací údaje, nestahovat do PC žádné soubory z neznámých zdrojů. Používat aktualizovaný antivirový software.

Metody detekce: Tento typ podvodu může banka detekovat pouze díky svým klientům, kteří poznají pokus o phishing a celou záležitost nahlásí své bance. Banky by tedy měla všechny své klienty informovat o tomto typu nebezpečí. Pouze klient, který je s tímto typem útoku seznámen ho může poznat a následně nahlásit bance. Banka by následně měla všechny své klienty varovat pomocí informace zveřejněné na svých internetových stránkách i u vstupu do internetového bankovnictví, nebo dokonce i pomocí informativního

emailu o posledním nahlášeném pokusu o phishing. Nejlépe v tomto směru informuje své klienty Česká spořitelna, která jako jediná taková varování vydává.

3.3.3 Pharming

Tento způsob spočívá v podstrčení falešných webových stránek, které jsou přesnou kopií stránek internetového bankovnictví klienta. Tento typ útoku spočívá v napadení DNS serveru na LAN sítí.. Po tomto útoku útočník pozmění IP adresy webového serveru za IP adresu podvrženého serveru (obrázek č. 21). Jakmile se klient pokouší připojit do internetového bankovnictví jeho banky (www.nicebank.com) tak se mu místo oficiální webové stránky banky zobrazí přesná kopie banky (www.n1cebank.com). Na první pohled tato kopie nemusí být vůbec rozdílná od oficiální stránky. Při zadávání přihlašovacích údajů na fiktivní stránce banky a pokusu o přihlášení se tyto důležité informace uloží do databáze útočníka a stránka buď dále nereaguje, nebo po pokusu o přihlášení vypíše hlášku typu "Omlouváme se, ale probíhá údržba serveru." a další. Dále může nastat situace, kdy se na předhození podvodné stránky využívá napadení počítače klienta virem. Tento vir pozmění IP adresy v souboru hosts a princip podvodu a útoku na účet klienta je pak stejný jako při útoku na DNS server [8]. Pro zvýšení úspěchu používají útočníci podobných názvů URL, jako mají zdrojové banky (např. pro KB a URL internetového bankovnictví www.mojebanka.cz by útočník využil něco jako www.mojrbanka.cz).



Obr. 26 Princip pharmingu

Jak se bránit: Pozorně kontrolovat URL webové stránky. Proti tomuto typu podvodu se v dnešní době můžeme bránit používáním aktualizovaných verzí antivirových programů, díky kterým tuto hrozbu včas odhalíme.

Metody detekce: V tomto případě je metoda detekce stejná jako u phishingu. Pokud klient nepozná podvržené webové stránky a nenahlásí tento pokus o pharming své bance, ta jen velmi těžko pozná pokus o získání důležitých informací touto metodou. Proto je nutné neustále klienty o tomto typu útoku a o nutnostech dodržovat základní pravidla obrany před touto metodou informovat. Banky by opět měli své klienty preventivně informovat o principech pharmingu, a předejít tak jejich zneužití. Všechny banky v České republice využívají zabezpečené připojení pomocí certifikátů. Pokud klient v prohlížeči pravidelně kontroluje správnost URL při autentizaci vstupu do internetového bankovnictví, nemusí se této metody podvodu obávat.

3.3.4 Lisabonská smyčka

Tento způsob, zvaný lisabonská smyčka, se dá označit za předchůdce skimmingu. Na rozdíl od něj se však útočník nesnaží získat data zkopírováním údajů, ale jeho cílem je získat, respektive odcizit platební kartu a PIN. Celý způsob spočívá v tom, že útočník zablokuje otvor pro vkládání karty tak, že bankomat nemůže s kartou pracovat. Karta nejde vysunout a ani zasunout. Útočník tedy přesvědčí oběť k opětovnému vložení PIN kódu, který se poté snaží odpozorovat. V okamžiku, kdy poškozený vlastník karty vzdává svůj boj s bankomatem a odchází nahlásit do banky závadu, se pachatel zmocňuje platební karty a se znalostí PIN kódu odchází s kartou do jiného bankomatu pro finanční hotovost. V dnešní době plné chytrých telefonů a mobilního internetu nebude pro útočníka potřeba znalost PIN kódu a jen s třemi údaji na kartě může provádět online nákupy za Vaše peníze.

Jak se bránit: Nezadávat PIN za přítomnosti další osoby a mít nastavený co možná nejmenší limit pro platbu na internetu. Neopouštět bankomat a raději se s bankovní společností spojit telefonicky a obrátit se na telefonní kontakt, který bývá uveden na bankomatu pro případ problémů s vyjmutím karty z bankomatu.

3.4 Srovnání vybraných bank na území ČR

Pro srovnání bank v České republice jsem vybral pět nejznámějších bank: Česká spořitelna, ČSOB, Komerční banka, Mbank a Airbank, kterou díky sloganu "i banku můžete mít rádi" a televiznímu marketingu zná v České republice snad každý. Podle mého zjištění se v České republice nevyskytuje banka, která by pro přístup do internetového bankovnictví neměla šifrovanou komunikaci. Právě díky tomu je sníženo riziko pharmingu na minimum. Z vybraných bank využívají všechny banky zabezpečení komunikace pomocí

SSL 3.0 certifikátů. Výjimku tvoří pouze Mbank, která pro šifrování přenosu informací mezi klientem a internetovým bankovnictvím využívá protokolu TLS 1.0, jež se od protokolu SSL 3.0 nijak výrazně neliší. Všechny z bank se od sebe vzájemně odlišují pouze možností autentizace klienta při vstupu do internetového bankovnictví a pojištěním platebních karet proti krádeži a zneužitím. Jsou banky, které nabízejí pojištění v základní nabídce při vedení běžného účtu, to je ale většinou bezvýznamné a nijak nezvyšuje možnost zabezpečení financí klienta. Jedná se o pojištění transakce za použití PIN kódu, ale pouze v případě, byl-li kód vyzrazen pod hrozbou násilí či ohrožené života. Klient musí takovou událost ohlásit své bance nejpozději do jedné hodiny. Problémem je, že se taková událost velice těžko dokazuje a podle bankovních klientů, kteří se s touto zkušeností setkali, se banky snaží spíše vyhnout odškodnění. Dalším důležitým faktorem v bezpečnosti platebních karet a internetového bankovnictví je možnost autorizace plateb. Ta je ale u všech bank v České republice stejná. Autorizace probíhá pomocí šifrovaného SMS kódu, který je zasílán na mobilní telefon vlastníka účtu.

3.4.1 Jednotlivé body pro srovnávací tabulku

1. Autentizace klienta při vstupu do internetového bankovnictví
    A. pouze pomocí přihlašovacího jména/čísla a hesla
    B. pomocí certifikátu
    C. pomocí SMS klíče
    D. čipovou kartou
2. Autorizace platby
    A. pomocí generovaného SMS kódu
3. Šifrovací protokol pro internetové bankovnictví
    A. SSL 3.0
    B. TLS 1.0
4. Možnost nastavení a změny výšky limitu platby po každé transakci
    A. ANO
    B. NE
5. Pojištění platby na internetu a bez přítomnosti platební karty
    A. ANO
    B. NE
    C. Pouze v případě ztráty, nebo odcizení

6. Pojištění transakce za použití PIN kódu
    A. ANO
    B. NE
    C. NE (Pouze pokud dojde k vyzrazení PIN kódu pod hrozbou násilí)
7. Umístění bankomatů
    A. Bezpečné - místa pouze pod dohledem kamerových systémů
    B. Méně bezpečné - místa s rizikem Skimmingu

3.4.2 Srovnávací tabulka vybraných bank na území ČR

	Airbank	Česká spořitelna	ČSOB	Komerční banka	mBank
Autentizace klienta	Pouze pomocí klientského přihlašovacího jména a hesla	Pomocí klientského čísla a hesla, nebo pomocí certifikátu	Pomocí Identifikačního čísla, PINU, SMS klíče, nebo čipové karty	Pomocí certifikátu, nebo čipové karty	Pouze pomocí klientského čísla a hesla
Autorizace platby	Šifrovaná SMS	Šifrovaná SMS	Šifrovaná SMS	Šifrovaná SMS	Šifrovaná SMS
Šifrovací protokol	SSL 3.0	SSL 3.0	SSL 3.0	SSL 3.0	TLS 1.0
Limity transakce	ANO	ANO	ANO	ANO	ANO
Pojištění platby na internetu	NE	pouze v případě ztráty či odcizení	pouze v případě ztráty či odcizení	NE	pouze v případě ztráty či odcizení
Pojištění transakce (s PIN)	NE	ANO	Pouze v případě vyzrazení PIN kódu pod hrozbou násilí	Pouze v případě vyzrazení PIN kódu pod hrozbou násilí	ANO
Umístění bankomatů	Bezpečné	Méně bezpečné	Méně bezpečné	Méně bezpečné	Banka nemá bankomaty

Tab. III Srovnávací tabulka vybraných bank v České republice

Z vybraných bank se zabezpečení nejlépe věnuje Česká spořitelna. Česká spořitelna i na svých internetových stránkách aktivně varuje své klienty před možným nebezpečím, jaho principech a metodách útoků. Pro přístup do internetového bankovnictví má klient možnost sám zvolit typ autentizace pomocí certifikátu, a na rozdíl od ostatních bank se srovnatelným způsobem zabezpečení internetového bankovnictví nabízí i možnost pojištění transakce za použití PIN kódu. Naopak mezi banky, které si se zabezpečením klientů u internetového příliš hlavu nelámou, patří banka Airbank. Ta používá pouze zastaralý způsob autentizace klienta a nenabízí žádné pojištění proti zneužití platební karty. Až na tyto rozdíly se jednotlivé banky u nás mezi sebou příliš neliší a vždy záleží spíše na klientovu rozhodnutí, pro kterou banku se rozhodne.

4 ZABEZPEČENÍ PLATEBNÍCH KARET U BANK V ZAHRANIČÍ

4.1 Poštová banka, a.s. - Slovensko

Pojišťovňa Poštovej banky vznikla v roce 1940 pod názvem Pojišťovňa Tatra. V roce 2008, kdy Poštová banka koupila 100% podíl akcií ve společnosti Poisťovňa Tatra, se stala členem skupiny Poštová banka. V tomto roce byl zároveň i změněn název na Poisťovňa Poštovej banky. Nyní mezi její nejznámější produkty patří tzv. Poštomat, díky kterému mohou majitelé platebních karet VISA a MasterCard vybírat hotovost na i na pobočkách Slovenské pošty přes POS-terminál. Mezi službami banky je i GSM banking. Pro přístup do internetového bankovnictví je pouze možnost autentizace klienta pomocí zastaralého přihlášení pomocí klientského jména a hesla. Tato banka vydává platební karty pouze od společnosti MasterCard [29].

Zabezpečení autentizace klienta:

- Možnost přihlášení do internetového bankovnictví pouze pomocí přihlašovacího jména a přístupového hesla

Výhody

- Autorizace transakce je zabezpečena pomocí jednorázového hesla zaslaného formou šifrované SMS zprávy na mobilní telefon klienta banky, nebo pomocí tokenu
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Po třech špatných pokusech o přihlášení se bankovnictví uzamkne na dobu 30 minut
- Nabízí možnost nastavení limitu (i časového limitu výšky platby) v internetovém bankovnictví
- Šifrování komunikace pomocí SSL certifikátu

Nevýhody

- Autentizace klienta pouze pomocí přihlašovacího jména a přístupového hesla
- Pojištěné platby na internetu pouze v případě ztráty, nebo odcizení karty
- Banka nenabízí žádné pojištění platební karty, transakcí s, nebo bez použití PIN kódu

- Transakční limit nabízí banka pouze pro výběr z bankomatu, pro internetové bankovnictví je limit zůstatek na účtu

Internetová stránka banky: http://www.postovabanka.sk/

Obr. 27 Logo Poštové banky

4.2 Oberbank – Rakousko

Tato Rakouská banka byla založena roku 1869 v Linci. Je součástí uznávaného společenství tří bank "3 Banken Gruppe" spolu s BTV a BKS Bank. Banka využívá 128bitové SSL kódování pro zabezpečení komunikace. Tato banka jako jedna z mála nabízí klientům autorizaci plateb pomocí TAN kódů (Transakční autorizační kódy), které klient získá v počtu 99 kusů poštou. Banka nenabízí žádné vyšší zabezpečení přístupů do internetového bankovnictví, kdy nemá žádnou možnost výběru a je odkázán na zastaralou autentizaci pomocí klientského čísla a hesla. Autorizace je prováděna pomocí TAN kódů, nebo šestimístným kódem zasílaným při pokusu o autorizaci platby na mobilní telefon klienta. Nabízí platební karty: Maestro, MasterCard, Diners Club White a Diners Club. Banka nabízí pojištění ztráty dokladů, klíčů, telefonu apod., jen ne pojištění platební karty pro platby na internetu [30].

Zabezpečení autentizace klienta:

- Nabízí pouze pomocí klientského čísla a hesla

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Automatické odhlášení internetového bankovnictví po 15 minutách neaktivity
- Banka nabízí pojištění pro případ finanční ztráty z důvodu opakovaného vydání PIN kódu, odcizení hotovosti
- Podpora 24 hodin denně

Nevýhody

- Zabezpečení autentizace klienta pouze pomocí přihlašovacího jména a hesla
- Banka v základu nenabízí žádné možnosti pojištění karty proti finanční ztrátě za použití PIN
- Chybí pojištění platby na internetu bez přítomnosti karty u karty Maestro.

Internetová stránka banky: http://www.oberbank.at/

Obr. 28 Logo Oberbank

4.3 LBBW Bank - Německo

Landesbank Baden-Württemberg je komerční bankou, ale zároveň i centrální bankou spořitelen v Baden-Württembersku, Sasku a Porýní-Falcku. Patří mezi největší banky v Německu s centrálou ve Stuttgartu, Karlsruhe, Mohuči a v Mannheimu. Tato banka nabízí i možnost zabezpečení pomocí eCode čipové karty pro autentizaci klienta při vstupu do internetového bankovnictví i pro autorizace aktivních operací. Díky možnosti použití zabezpečení pomocí autentifikátoru nabízí tato banka nejvyšší možné zabezpečení pro ověření plateb klienta [31]. Banka vydává platební karty společností Maestro a MasterCard. .

Zabezpečení autentizace klienta:

- V nabídce banky zabezpečení přístupu pomocí přihlašovacího jména a OTP hesla odesílaného na mobilní telefon klienta, nebo i pomocí eCode čipového kalkulátoru.

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu (denní, týdenní, po změně zůstatku)
- Způsob autorizace pomocí SMS klíče odeslaného šifrovanou zprávou
- Možnost zabezpečení autentizace klienta i autorizace plateb pomocí čipového kalkulátoru
- Banka informuje ve zkratce o bezpečnostních zásadách pro používání karty a internetového bankovnictví
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Podpora 24 hodin denně

Nevýhody

- Banka nenabízí možnost změny transakčních limitů v internetovém bankovnictví
- Chybí pojištění platby na internetu bez přítomnosti karty
- Banka nabízí pojištění transakce za použitím PIN kódu, pouze pokud dojde k jeho prozrazení pod hrozbou násilí

Internetová stránka banky: http://www.lbbw.de/

Obr. 29 Logo LBBW

4.4 Evropsko-Ruská Banka - Rusko

Tato banka je první a zároveň i jediná banka s ruským kapitálem, která se může pyšnit novou bankovní licencí na území Evropské unie. Díky této licenci může zakládat pobočky v jakékoliv členské zemi Evropské unie. Klient má na výběr ze dvou typů autentizace

přístupu do internetového bankovnictví. Zpoplatněným přístupem pomocí certifikátu na kryptografickém USB klíči, který je navíc chráněn PIN kódem. Druhá možnost zabezpečení je pomoci mobilního klíče. Klientem zvolený typ autentizace je stejný i pro autorizace aktivních operací internetového bankovnictví [32]. Tato banka vydává platební karty společnosti VISA. Tato banka nemá vlastní bankomaty.

Zabezpečení autentizace klienta:

- Zabezpečení přístupu pomocí placeného certifikátu, nebo pomocí mobilního klíče

Výhody

- Zaslání SMS, nebo emailu o pohybu účtu
- Zabezpečení plateb pomocí přihlašovacího jména a digitálního certifikátu (eToken), nebo za pomoci uživatelského jména, hesla a SMS klíče.
- Banka nabízí pojištění platebních karet proti ztrátě a krádeži
- Automatické odhlášení internetového bankovnictví po delší nečinnosti klienta
- Autorizační SMS klíč odeslán šifrovanou SMS zprávou

Nevýhody

- Banka nabízí žádné pojištění platební karty
- Nemožnost nastavení limitu platby

Internetová stránka banky: http://www.erbank.eu/

Obr. 30 Logo ERB

4.5 Srovnání vybraných zahraničních bank

Pro srovnání zahraničních bank jsou zvoleny stejné kritéria jako ve srovnání vybraných bank v České republice. Ke komparaci byly vybrány čtyři zahraniční banky, přičemž

některé z nich mají pobočku i v České republice. Metodika zabezpečení platebních karet u zahraničních bank se příliš neliší od metodiky zabezpečení bank v České republice. Jako nejnižší možný typ zabezpečení autentizace klienta je ověření pouze klientského čísla a hesla. U autorizace aktivních operací, mezi které patří převody finančních prostředků z jednoho účtu na druhý, převládá i v zahraničí ověření pomocí generovaného kódu, který je odesílán šifrovaně na mobilní telefon klienta.

4.5.1 Srovnávací tabulka vybraných zahraničních bank

	Poštová Banka	Oberbank	LBBW Bank	Evropsko-Ruská banka
Autentizace klienta	Pouze pomocí klientského přihlašovacího jména a hesla	Pouze pomocí přihlašovacího jména a hesla	Přihlašovací jméno a hesla, OTP heslo, nebo kalkulátor	Pomocí place-ného certifikátu, nebo mobilního klíče
Autorizace platby	Šifrovaná SMS, nebo za pomoci Tokenu	Šifrovaná SMS, nebo pomocí TAN kódu	Šifrovaná SMS, nebo pomocí kalkulátoru	Šifrovaná SMS, eToken, nebo přihlašovací jméno a heslo
Šifrovací protokol	SSL 3.0	SSL 3.0	SSL 3.0	SSL 3.0
Limity trans-akce	ANO	NE	NE	NE
Pojištění platby na internetu	NE	NE	NE	NE
Pojištění transakce (s PIN)	NE	NE	Pouze v případě vyzrazení PIN kódu pod hroz-bou násilí	NE

Tab. IV Srovnávací tabulka vybraných zahraničních bank

Z vybraných zahraničních bank je na tom nejlépe Německá LBBW Bank. Tato banka nabízí stejnou metodu autentizace klienta a stejné možnosti zabezpečení aktivních operací v IB jako Evropsko-Ruská banka, ale navíc nabízí i možnost pojištění platební karty.

Bankou, která podle srovnávací tabulky dopadla nejhůře, je Rakouská Oberbank, která nabízí staré možnosti autentizace klienta, nenabízí žádné možnosti nastavení limitů plateb, které by si mohl klient sám editovat v internetovém bankovnictví. Jediná banka, která má vlastní bankomaty je Poštová banka, avšak má své pobočky pouze na území Slovenska.

5 SROVNÁNÍ METODIKY ZABEZPEČENÍ PLATEBNÍCH KARET V ČESKÉ REPUBLICE SE ZAHRANIČÍM

Zabezpečení platebních karet v zahraničí se od zabezpečení v České republice moc neliší. Používají se stejné certifikáty na šifrování komunikace, kde stejně jako v České republice převládá 128bitové zabezpečení komunikace pomocí SSL certifikátu. Hlavními rozdíly v zabezpečení nejsou mezi jednotlivými zeměmi, ale hlavně mezi bankovními institucemi. Nelze tedy přesně určit jaká země má nejlepší možné zabezpečení platebních karet a v čem se jednotlivé země liší. Metodiky zabezpečení se tedy liší pouze u jednotlivých bankovních organizací, nikoli podle země, ve které působí. Můžeme najít v České republice banku, která si například se zabezpečením aktivních operací svých klientů příliš hlavu neláme a stejně snadno takovou banku můžeme najít i v zahraničí, protože míru zabezpečení transakcí a platebních karet neurčují zákony, ale sami banky podle svého uvážení. Při porovnání srovnávacích tabulek vybraných bank na území České republiky a bank zahraničních je vidět, že Česká republika na tom není tak špatně, jak se může zdát. Naopak je tomu u bank, které nabízejí své služby ve více zemích jako například Evropsko-Ruská banka, která se může díky bankovní licenci Evropské unie rozrůstat do všech států EU. Tato banka nabízí ve všech svých pobočkách na území Evropské unie stejné možnosti, metodiky zabezpečení platebních karet i internetového bankovnictví jako má pro své klienty u své kmenové banky, která má sídlo v Rusku. Dalším a hlavně výrazným rozdílem mezi zahraničními bankami a těmi v České republice je síť bankomatů.

Zabezpečení platebních karet

Jako nejhorší způsob zabezpečení pro autentizaci klientů banky se dnes v celé Evropě dá považovat přihlášení do internetového bankovnictví pouze pomocí klientského jména/čísla a hesla. Tento způsob autentizace patří k těm rychlejším metodikám přihlášení do internetového bankovnictví, ale je zastaralý a nepatří k nejlepším možnostem ochrany důležitých informací účtu klienta. Bohužel, některé z levnějších bank, které lákají své klienty pod reklamou vedení účtu, výběry z bankomatu a další služby zdarma se tato metodika dá považovat za standard, na kterém banky nechtějí nic měnit. Jako standard, který převládá u autorizace platby a aktivních operací na účtu je ověřování pomocí generovaného SMS kódu, který je platný pár minut a pouze pro jednu požadovanou transakci. Mezi nejlepší možné zabezpečení autentizace klienta a autorizace aktivních

operací se dá považovat zabezpečení pomocí čipového kalkulátoru, který nabízí Německá banka LBBW Bank a Česká ČSOB.

Limity transakce

Jako hlavní chybu v zabezpečení a ochraně financí svých klientů, které se banky mohou dopustit, je neumožnění změny limitu platby pro internetové platby a aktivní operace. Některé banky, mezi které patří i slovenská Poštová banka, mají tuto službu dokonce zpoplatněnou, a tím neumožňují svým klientům základní ochranu proti neoprávněným platbám na internetu. Další zahraniční banky vybrané pro srovnání zabezpečení s metodikou zabezpečení v České republice nenabízejí žádnou takovou možnost.

Pojištění platebních karet

Ne každá banka nabízí možnost pojištění platební karty pro platby na internetu, pro transakce s nebo bez použití PIN kódu. Banky se většinou předhánějí v lepší propagaci o nabídce pojištění platebních karet svých klientů, ale žádná z těchto bank nenabízí řešení, které by opravdu ochránilo klienty před možnými podvody s platebními kartami. Většinou banky nabízejí pojištění proti finanční ztrátě za použití PIN kódu, ale pouze pod podmínkou, že k jeho prozrazení dojde pod hrozbou násilí. Toto prozrazení pod hrozbou musí klient banky dokázat a není to vždy tak snadné jak se může na první pohled zdát.

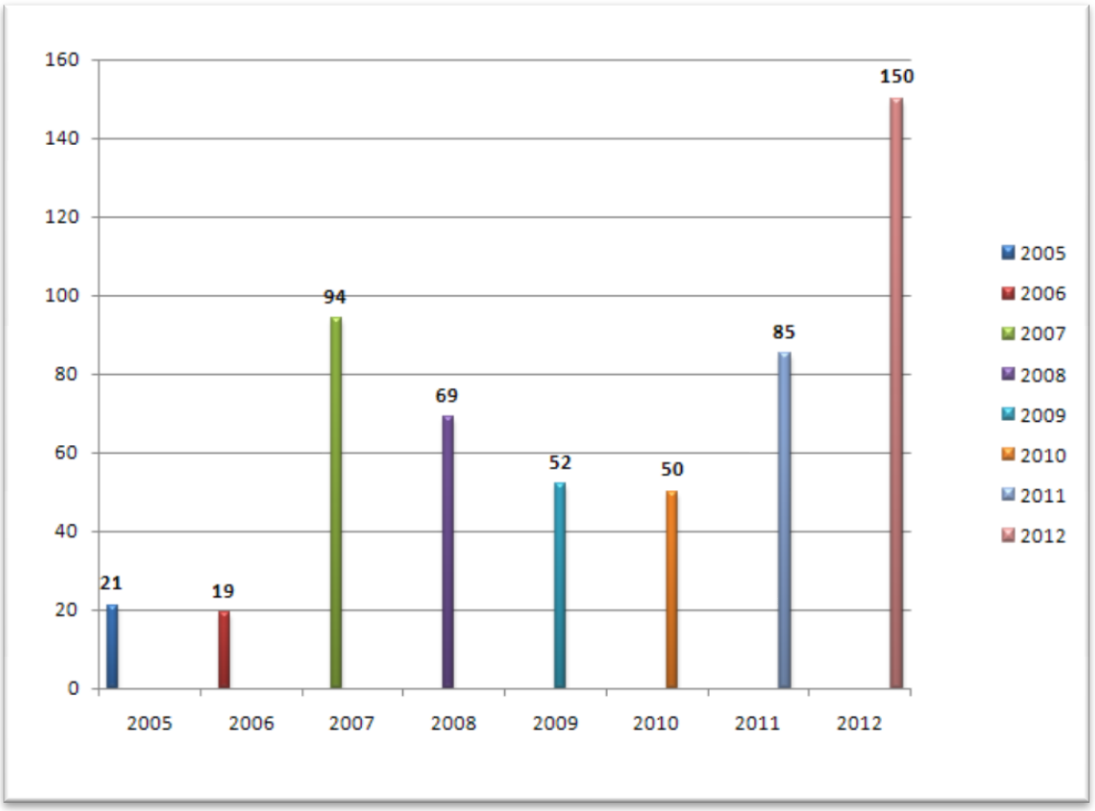
Závěrečné srovnání

Ve výsledném srovnání jsou na tom v oblasti zabezpečení platebních karet a internetového bankovnictví daleko lépe banky, které leží na území České republiky. Oproti zahraničí můžeme u nás najít banky:

- Které nám dovolují změny limitů plateb účtu pro platby na internetu
- Nabízejí více možností pojištění platební karty a plateb kartou na internet, které v zahraničí hledáme velmi těžko
- Umožňují stejné zabezpečení aktivní a pasivních operací
- Nabízejí klientům stejné možnosti autentizace pro vstup do internetového bankovnictví
- Využívají stejné metody šifrovaní komunikace mezi klientem a internetovým bankovnictvím

6 NÁVRHY PRO ÚPRAVU A ZVÝŠENÍ ZABEZPEČENÍ

Zabezpečení platebních karet a možnosti ochrany, které poskytují jednotlivé banky světa svým klientům, se liší už od prvního přihlášení do internetového bankovnictví. Banky se neliší ve způsobu šifrování dat, zde převládá 128bitové šifrování pomocí SSL protokolu a jen zřídka narazíme na jiný šifrovací protokol. V tomto ohledu je ochrana šifrování komunikace mezi klientem a bankou dostačující, a pokud hrozí klientovi, že se stane obětí podvodu, z 99% je tomu tak důsledkem nedbalosti, nebo dokonce i neznalosti této problematiky. V dnešní době převládá autorizace platby a všech aktivních operací účtu u klientského bankovnictví pomocí generovaného kódu odeslaného na mobilní telefon klienta banky. Tuto metodiku ověření klienta nalezneme jak u bank, které nabízejí vedení účtu zdarma, tak i u bank, kde je vedení účtu zpoplatněno. Banky se dále liší pouze v dalších možnostech a způsobech autorizace a autentizace klienta. Největším problémem dnešní doby není zabezpečení přístupu do internetového bankovnictví nebo ověření transakce. Největší hrozbou je samotná nepozornost uživatelů platebních karet, kteří jsou mnohdy schopní nevědomě dát svoji kartu z rukou či spustit z očí (např. při platbě na benzinové pumpě). Dokud nebudou uživatelé více obezřetní a budou ignorovat možná nebezpečí a rizika, nebude nikdy vyvinuto dokonalé zabezpečení platebního systému. Mezi největší nebezpečí, která mohou vzniknout při používání platebních karet, stále patří a bude patřit špatná uživatelská ochrana důležitých údajů uvedených na platební kartě. Není nic snadnějšího, než jako zaměstnanec benzinové pumpy sehrát při platbě před zákazníkem divadlo a upustit kartu při zasouvání do platebního terminálu na zem pod pult, kam zákazník nevidí. Při zvedání kartu jen v rychlosti otočit z obou stran na kameru umístěnou pod pultem, a tím získat potřebné údaje pro platby na internetu. Mezi stále častější techniky k získání důležitých údajů z platební karty, na které můžeme v České republice narazit, je skimming. Techniky organizovaných gangů se natolik zlepšují, že ani zaměstnanec banky dnes nemusí poznat rozdíl mezi bezpečným bankomatem a tím, kde je ukryto skimmovací zařízení připravené ke kopírování elektronických údajů z platební karty. Za tuto hrozbu, která může potkat kohokoliv z nás, mohou především banky, které nevhodně umísťují bankomaty na místa, která lze špatně kontrolovat a střežit. Jen za rok 2012 stoupl počet případů skimmingu oproti roku 2011 z 85 na 150 případů, kdy bylo nalezeno na bankomatu nainstalované skimmovací zařízení.



Obr. 31 Přehled skimmingu na území ČR v období let 2005 až 2012

Jak bojovat proti skimmingu

Proti tomuto typu podvodu musí bojovat hlavně banky, a to nejlépe následujícími způsoby:

- Budovat síť bankomatů pouze na místech dobře zabezpečených kamerovým systémem. Umístění bankomatů v prostorách a vstupních halách banky.
- Časté kontroly bankomatů
- Vzájemná spolupráce všech bank po celém světě
- Vytvoření jednotného typu bankomatu využívaného všemi bankami v celé Evropě.
    - Tento bankomat by měl mít celou přední část vyrobenou pouze z jednoho kusu oceli, která by zabraňovala konstrukční změny jednotlivých částí bankomatu (osvětlení, podavač bankovek, akceptor karet atd.)
    - Stejné rozměry a umístění jednotlivých zařízení bankomatu (klávesnice, akceptor karet atd.) a díky tomuto by uživatel mohl snadněji poznat, jestli je na bankomatu přidáno něco, co tam nepatří.

Jak bojovat proti phishingu

Proti phishingu lze bojovat z velké části pouze jedním způsobem. Je nutné informovat širokou veřejnost o praktikách a nebezpečích, které se skrývají za touto metodou podvodu. Pouze neznalý uživatel se může stát obětí tohoto typu útoku. Banky a další organizace, které se zabývají bezpečnostními incidenty, mezi které patří i tento typ útoku, se v poslední době snaží varovat své uživatele a klienty před touto praktikou. Podle statistiky bezpečnostní organizace CSIRT (Computer Security Incident Response Team) počet těchto incidentů v roce 2012 vzrostl oproti předchozímu roku o 15 incidentů na konečných 159 incidentů za rok 2012.

Hlavní zásady ochrany před phishingem:

- Nebýt příliš důvěřivý
- Používat pouze známé adresy
- Nenechat se vystresovat
- Snažit se hledat hlavní příznaky podvodných emailů, mezi které patří: jazykové problémy, zaslání důvěrných informací a falešné odkazy v textu zprávy
- Nemít strach se zeptat a zavolat si i na telefonní číslo, které je uvedené na oficiálních stránkách společnosti/banky. Nepoužívat kontakty uvedené v těle emailu.
- Používat antivirový program, firewall a antispyware. Snažit se mít veškerý software aktualizovaný
- Používat pouze bezpečný a aktualizovaný prohlížeč s phishingovou ochranou (IE, FireFox, Chrome, Opera), mezi kterou patří pluginy SpoofGuard, TrustToolbar, Netcraft Toolbar a Google Toolbar

Jak se chránit proti pharmingu

Proti tomuto typu útoku je velmi těžké se bránit. Hlavní zásadou, která je potřeba pečlivě dodržovat, je aktualizovaný antivirový software. Pharming může být natolik propracovaný, že ani zkušený uživatel tento útok nemusí poznat. Nejlepší ochranou by bylo nevkládat do internetového prohlížeče název webové stránky (např. www.mojebanka.cz), ale přímo IP adresu, která směřuje doopravdy na internetové bankovnictví banky. Jedinou ochranou v boji proti tomuto typu útoku je snaha bank více informovat své klienty o tomto nebezpečí.

Jak se bránit při fyzickém odcizení karty

Jedinou možnou ochranou je mít uložené telefonní číslo na banku, u které má klient vydanou platební karty, i na více místech. Mobilní telefon, peněženka atd. Při ztrátě nebo krádeži platební karty je nutné co nejrychleji platební karty zablokovat. Všechny banky po celém světě jsou schopné provést blokaci platební karty do několika minut. Hlavní prevencí proti odcizení nebo ztrátě platební karty a financí na účtu je neustálá informovanost klientů a následné poskytnutí bezplatné blokace karty. Uživatel platební karty nesmí mít PIN kód uložen společně s platební kartou na stejném místě. Všechny banky musí být schopny poskytnout svým klientům možnost změny PIN kódu, zjednodušit tak uživatelům si tento kód zapamatovat, a tudíž nemít potřebu si jej poznamenávat na papírky do peněženky či jiná místa. Pokud by navíc banky poskytovali možnost aktivace/deaktivace platby kartou na internetu, tato možnost by byla prováděna pomocí mobilního telefonu a autentizace klienta by byla zabezpečena za pomoci speciálního kontrolního hesla. Díky této ochraně by měl uživatel možnost kdykoliv veškeré internetové platby zakázat (např. při cestě do zahraničí), a tím i získat daleko více času a prostoru pro zjištění ztráty, nebo odcizení platební karty.

Zvýšení zabezpečení u vydávání platebních karet

Stále se na území České republiky vyskytují banky, které odesílají platební karty a PIN kódy poštou. Tento způsob by měl být zrušen. Předání platební karty společně s PIN kódy by mělo probíhat pouze osobně na pobočce banky. Při předání platební karty a dalších důvěrných informací by byl klient ověřen průkazem totožnosti, a tím by se zamezilo možnosti, že by se mohl platební karty zmocnit někdo jiný než klient, který o kartu u banky požádal.

6.1 Bezpečnější bezhotovostní platby bezkontaktní kartou

Platby bezkontaktní platební kartou nabízí většina bank po celé Evropě. Tyto platební karty pracují na principu RFID zařízení a jejich využití v bankovnictví pro bezkontaktní platby je "stejné" jako např. u cestovních pasů s tím rozdílem, že přenos mezi bezkontaktní platební kartou a terminálem schopným komunikovat s tímto typem karet je nezabezpečený. Data, které nalezneme v elektronickém pasu, jsou digitálně podepsána vydávající institucí a díky tomu nebude moci padělatel vytvořit bez patřičného soukromého klíče správný digitální podpis. Tento způsob ochrany nazýváme pasivní

autentizace. Cestovní pasy jsou oproti bezkontaktním platebním kartám chráněny proti odposlechu základním řízením přístupu (Basic Access Control). Tento způsob zabezpečení funguje tak, že čtečka načte tři základní informace o majiteli pasu, mezi které patří číslo pasu, datum narození a datum vypršení platnosti cestovního pasu. Tyto data se hašují funkcí SHA-1 pro následné získání 3DES klíčů, které jsou následně využity pro autentizaci a stanovení společného šifrovacího klíče, kterým je zabezpečena celá následná komunikace. U této metody (pasivní autentizace) existuje možnost padělání karty, pokud by se útočníkovi podařilo odposlechnout komunikaci a následným offline útokem dešifrovat obsah získaných přenášených dat. Další a daleko zabezpečenější technologií je aktivní autentizace, u které je soukromý asymetrický klíč přímo a bezpečně uložen v čipu pasu. U této metody zabezpečení se nemůže stát, že by tento klíč opustil čip (čtečka se pouze přesvědčuje o existenci tohoto klíče v čipu). U této metody neexistuje zatím možnost, že by padělatel vytvořil kopii čipu, a tím se tato metoda zabezpečení používání čipu stává bezpečnou.

Způsob zabezpečení bezkontaktních platebních karet je pouze pomocí výšky povoleného limitu platby, u kterého není potřeba zadávat PIN kód. Tento limit se neliší bankami vydávajícím bezkontaktní platební karty, ale zemí ve které touto kartou platíme. V České republice je tento limit ve výši 500 Kč. Bezhotovostní platby se začínaly ukazovat v České republice koncem roku 2011, ale už v té době testovali ve Francii daleko lepší typ ochrany těchto. Tento systém vyvinula společnost Natural Security podle které je tento systém odolný proti zneužití a zároveň zajišťuje ochranu soukromí. Princip tohoto zabezpečení funguje tak, že otisk klienta prstu je pevně uložen v čipu bezkontaktní platební karty. Tato karta tento otisk bezkontaktně odešle do čtečky, která tento ho následně porovnává s otiskem prstu klienta a následně autorizuje platbu. Biometrická čtečka takto komunikuje s bezkontaktní kartou bez nutnosti kartu vytahovat. Čtečka si dokáže všechny potřebné informace k platbě a ověření sama stáhnout na maximální vzdálenost dva metry.

ZÁVĚR

Cílem a hlavním tématem této diplomové práce bylo vytvoření analýzy bezpečnosti platebních karet. Práce je rozdělena na dvě hlavní části, teoretickou a praktickou, přičemž všechny zvolené body byly vypracovány dle zadání.

Teoretická část je věnována seznámení se s historií, postupnému vývoji platebních karet, jejich rozdělení a jednotlivými ochranným prvkům platebních karet. Rovněž je zde zpracována také historie a základní funkčnost bankomatů. Velkou část této teoretické části tvoří popis zpracovávání transakcí, mezinárodního standardu EMV a zabezpečení elektronických platebních systémů. Jedná se o následující platební systémy, které jsou známé a oblíbeně po celém světě: PaySec, PayU, Paypal a Moneybookers - Skrill.

První část se dále věnuje bezhotovostní platbě a internetovému bankovnictví, zabezpečení komunikace pomocí šifrovacích protokolů SSL, anebo v dnešní době velmi využívané metodě zabezpečení 3D Secure, kterou banky díky autorizaci platby, která je chráněna pomocí generovaného SMS kódu, odeslaného na mobilní telefon klienta, označují za nejbezpečnější možnou metodu platby na internetu. Nejefektivnější metodou bezpečné online platby je v současnosti zřejmě kombinace elektronického platebního systému a 3D-Secure.

Pro vypracování praktické části této diplomové práce jsem zvolil následujících pět českých bank: Česká spořitelna, Airbank, ČSOB, Komerční banka a Mbank. U jmenovaných českých bank jsem určil a následně srovnal základní metodiky zabezpečení platebních karet a internetového bankovnictví s několika známými zahraničními bankami. Konkrétně se jedná o následující zahraniční banky: slovenská Poštová banka, rakouská Oberbank, Evropsko-Ruská banka s hlavním sídlem v Rusku a německý LBBW Bank. Praktická část dále obsahuje zabezpečení bezkontaktních platebních karet, které v poslední době zažívají nejen v České republice, ale i po celé Evropě velký vzestup. Jsou zde popsány především všechna možná rizika, nebezpečí a hlavní typy útoků a podvodů jako jsou skimming, phishing, pharming či takzvaná Lisabonský smyčka. Cílem všech těchto útoků se můžeme stát třeba při platbě kartou za nákup v obchodním centru, nebo při online nákupu zboží na internetu.

V závěru této práce jsou navrženy vhodné úpravy pro zvýšení bezpečnosti, které by mohly tato rizika spojená s užíváním platebních karet snížit na minimum, a lépe tak chránit uživatele platebních karet před možnou finanční ztrátou.

ZÁVĚR V ANGLIČTINĚ

The main topic of this thesis was to create a safety analysis of payment cards. The work is divided into two main parts, theoretical and practical, all selected points were drawn according to the assignment.

The theoretical part is dedicated to introducing with the history, gradual development of payment cards, their distribution and various security features of credit cards. There is also compiled a history and basic functionality of ATMs. A large part of this theoretical part comprises a description of transaction processing, EMV and security of electronic payment systems. These are the following payment systems, which are well known and appreciated throughout the world: PaySec PayU, Paypal and Moneybookers - Skrill. The first part also deals with cashless payment and online banking, secure communication using SSL encryption protocol, or nowadays a security method used by 3D Secure by banks due to payment authorization, which is protected by a generated SMS code sent to the mobile phone client, indicate the safest possible method of payment on the Internet. The most effective method of secure online payments is now probably the combination of the electronic payment system and 3D-Secure.

For the development of the practical part of this thesis I chose these five Czech banks: Česká spořitelna, Airbank, ČSOB, Komerční banka and Mbank. For the appointed Czech Banks i diagnosed and subsequently compared basic methodology of security and internet banking with several well-know foreign banks. Specifically, the following foreign banks: Slovak Poštová banka, Austrian Oberbank, European-Russian Bank with headquarters in Russia and German LBBW Bank. The practical part contains the security of contactless payment cards, which recently experienced not only in the Czech Republic, but also throughout Europe big rise. Are described mainly all possible risks, hazards and major types of attacks and frauds such as skimming, phishing, pharming or so-called Lisbon loop. The aim of all these attacks can become necessary when paying by card shopping center, or online purchasing goods on the Internet.

In conclusion of this thesis is designed appropriate adjustments for increased security that could these risks associated with the use of credit cards reduced to a minimum, so as to better protect payment card users from possible financial loss.

SEZNAM POUŽITÉ LITERATURY

Knižní tituly:

[1] JUŘÍK, Pavel. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet*. 1. vyd. Praha: Grada, 2003, 312 s. ISBN 80-247-0685-7.

[2] JUŘÍK, Pavel. *Platební karty: ilustrovaná historie placení*. 1. vyd. Praha: Libri, 2012, 204 s. ISBN 978-80-7277-498-2.

[3] JUŘÍK, Pavel. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vyd. Praha: Grada, 2006, 296 s. ISBN 80-247-1381-0.

[4] SCHLOSSBERGER, Otakar. a Ladislav HOZÁK. *Phishing bez záhad.1*. Vyd. 1. Praha: Grada, 2007, 220 s. ISBN 80-726-5073-4.

[5] SCHLOSSBERGER, Otakar. *Platební služby*. Vyd. 1. Praha: Management Press, 2012, 325 s. ISBN 978-80-7261-238-3.

[6] PŘÁDKA, Michal; KALA, Jan. *Elektronické bankovnictví: rady a tipy*. Vyd. 1. Praha: Computer Press, a.s., 2000, 166 s. ISBN 80-722-6328-5.

[7] NEHYBOVÁ, Marta. *Bankovní služby nejen pro podnikatele:1870-2006: velká encyklopedie.*. Brno: Miroslav Nehyba, 1999, 140 s. ISBN 80-902-6454-5.

[8] JAMES, Lance. *Phishing bez záhad*. Vyd. 1. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[9] JUŘÍK, Pavel. *Svět platebních a identifikačních karet*. 2. přeprac. vyd. Praha: Grada, 2001, 175 s.,[25] s. barev. obr. příl. ISBN 80-247-0195-2.

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

[11] SCHLOSSBERGER, Otakar a Ladislav HOZÁK. *Elektronické platební prostředky*. 1. vyd. Praha: Bankovní institut vysoká škola, 2005, 144 s. ISBN 80-7265-073-4.

[12] SCHLOSSBERGER, Otakar. *Platební služby*. Vyd. 1. Praha: Management Press, 2012, 325 s. ISBN 978-80-7261-238-3.

Internetové zdroje:

[13] Platební karta. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2013-05-15]. Dostupné z: http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta

[14] Platební karty a jejich druhy. *Peníze.cz* [online]. [cit. 2013-05-15]. Dostupné z: http://www.penize.cz/15744-platebni-karty-a-jejich-druhy

[15] *PaySec - nakupování na internetu* [online]. [cit. 2013-05-15]. Dostupné z: http://www.paysec.cz

[16] *PayU* [online]. [cit. 2013-05-15]. Dostupné z: http://www.payu.cz

Jak používat službu PayPal. *Help for English* [online]. [cit. 2013-05-15]. Dostupné z: http://www.helpforenglish.cz/article/2010032203-jak-pouzivat-sluzbu-paypal

[17] *PayPal* [online]. [cit. 2013-05-15]. Dostupné z: https://www.paypal.com

[18] *Skrill* [online]. [cit. 2013-05-15]. Dostupné z: http://corporate.skrill.com

[19] Dávejte si pozor na platební kartu! Podvodníci jsou stále vynalézavější. *Peníze.cz* [online]. 2013 [cit. 2013-05-15]. Dostupné z: http://www.penize.cz/platebni-karty/248343-davejte-si-pozor-na-platebni-kartu!-podvodnici-jsou-stale-vynalezavejsi

[20] *Měšec.cz - Váš průvodce finančním světem* [online]. 1998 – 2013 [cit. 2013-05-15]. Dostupné z: http://www.mesec.cz/

[21] Tisková zpráva - Vývoj v oblasti karet za 2012. In: [online]. [cit. 2013-05-15]. Dostupné z: http://aktuality.cardzone.cz/TZ_SBK_15-02-2013.pdf

[22] Dajte si pozor na skimming! Viete rozpoznať sfalšovaný bankomat?. *IT News* [online]. 2013 [cit. 2013-05-15]. Dostupné z: http://www.itnews.sk/spravy/bezpecnost/2013-03-04/c154590-dajte-si-pozor-na-skimming-viete-rozpoznat-sfalsovany-bankomat

[23] SSL protokol (1) - princip a přínosy. *Svět sítí - Informace ze světa počítačových sítí* [online]. 2002 [cit. 2013-05-15]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=SSL-protokol-1-princip-a-prinosy-2542002

[24] *Česká spořitelna* [online]. [cit. 2013-05-15]. Dostupné z: http://www.csas.cz/

[25] *Air bank* [online]. [cit. 2013-05-15]. Dostupné z: http://www.airbank.cz

[26] *ČSOB* [online]. [cit. 2013-05-15]. Dostupné z: http://www.kb.cz/

[27] *Komerční banka* [online]. 2013 [cit. 2013-05-15]. Dostupné z: http://www.kb.cz/

[28] *MBank* [online]. 2013 [cit. 2013-05-15]. Dostupné z: http://www.mbank.cz/

[29]*Poštová banka* [online]. 2012 [cit. 2013-05-15]. Dostupné z: http://www.postovabanka.sk/

[30] *Oberbank* [online]. [cit. 2013-05-15]. Dostupné z: http://www.oberbank.at/

[31] *Landesbank Baden-Württemberg* [online]. [cit. 2013-05-15]. Dostupné z: http://www.lbbw.de/

[32] *Evropsko-ruská banka* [online]. 2013 [cit. 2013-05-15]. Dostupné z: http://www.erbank.cz/

Akademické práce:

[33] *Systém elektronických plateb* [online]. Brno, 2009 [cit. 2013-05-15]. Dostupné z: http://is.muni.cz/th/99184/fi_m/. Diplomová práce. Masarykova univerzita.

[34] *Online platební systémy v České Republice a výběr vhodné varianty pro internetový obchod* [online]. Praha, 2010 [cit. 2013-05-15]. Dostupné z: http://info.sks.cz/www/zavprace/soubory/68440.pdf. Bakalářská práce. Vysoká škola ekonomická.

[35] *Systémy platebních karet* [online]. Brno, 2011 [cit. 2013-05-15]. Dostupné z: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=37531. Diplomová práce. Vysoké učení technické.

[36] *Bezpečnost používání platebních karet* [online]. Zlín, 2011 [cit. 2013-05-16]. Dostupné z: http://dspace.k.utb.cz/handle/10563/16651. Diplomová práce. Univerzita Tomáše Bati.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISO	International Organization for Standardization - Mezinárodní organizace pro standardizaci
USA	United States of America - Spojené státy americké
TLS	Transport Layer Security - Transportní vrstva zabezpečení
ID	Identification - Identifikace
IP	Internet protocol - Internetový protokol
TAN	Transaction Authorization Number -Transakční autorizační číslo
OTP	One Time Password - Heslo pro jedno použití
ČNB	Česká národní banka
CD	Compact disk - Kompaktní disk
SMS	Short message service - Krátké textové zprávy
EPS	Electronic Payment System - Elektronické platební systémy
APDU	Datová jednotka aplikačního protokolu
SET	Secure Electronic Transactions - Bezpečné elektronické transakce
PCI	Peripheral Component Internconnect - Propojení periferních zařízení
SSL	Secure Socket Layer
USD	Americký dolar
RFID	Radio Frequency Identification - Identifikace pomocí rádiové frekvence
URL	Uniform Resource Locators - Jednotný popis umístění zdroje

SEZNAM OBRÁZKŮ

SEZNAM TABULEK