

Obsah

1 Úvod.....	4
1.1 Cíle práce.....	4
1.2 Přínosy práce.....	5
1.3 Struktura práce.....	5
2 Historie.....	7
2.1 Cíle kapitoly.....	7
2.2 Stručná historie platebních systémů.....	7
3 Rozdělení platebních systémů.....	10
3.1 Cíle kapitoly.....	10
3.2 Definice základních pojmů.....	10
3.3 Klasifikace platebních systémů.....	11
3.3.1 Rozdělení platebních systémů podle způsobu ověření platby.....	11
3.3.2 Rozdělení platebních systémů podle zařízení pomocí něhož je platba provedena.....	13
3.3.3 Rozdělení platebních systémů podle objemu plateb.....	13
3.4 Zaměření práce.....	14
4 Popis a analýza platebních systémů.....	15
4.1 Cíle kapitoly.....	15
4.2 Platební systémy, u nichž ověření platby není součástí nákupního procesu.....	16
4.2.1 Systémy, které umožňují využití informačních a komunikačních technologií.....	16
4.2.1.1 Bankovní převod.....	16
4.2.1.2 Platba kreditní/debetní kartou (ověření platby není součástí nákupní transakce).....	16
4.2.2 Systémy, které neumožňují využití informačních a komunikačních technologií.....	17
4.2.2.1 Platba u obchodníka.....	17
4.2.2.2 Platba na dobírku.....	18
4.2.2.3 Platba při převzetí.....	18
4.2.2.4 Další způsoby.....	18
4.3 Platební systémy, u nichž je ověření platby součástí nákupního procesu.....	19
4.3.1 Systém PayPal.....	20
4.3.1.1 Jak PayPal funguje.....	20
4.3.1.2 Výběr z PayPal účtu.....	21
4.3.1.3 Typy účtů.....	21
4.3.1.4 PayPal pro obchodníky.....	22
4.3.1.5 Kde a jaké možnosti PayPal nabízí.....	24
4.3.1.6 Bezpečnost.....	25
4.3.1.7 Související služby.....	25
4.3.1.8 Poplatky (náklady na PayPal).....	25
4.3.1.9 Je PayPal banka?.....	28
4.3.1.10 Výhody PayPalu.....	29
4.3.1.11 Problémy PayPalu.....	30
4.3.1.12 Právní kroky proti PayPalu.....	31
4.3.1.13 PayPal a VeriSign.....	32
4.3.1.14 Budoucnost PayPalu.....	32
4.3.1.15 PayPal a Česká republika.....	34
4.3.1.16 Zhodnocení.....	34
4.3.2 Platební systémy fungující na principu převodu z bankovního účtu.....	36
4.3.2.1 Platební systém eBanky.....	36
4.3.2.2 Platební brána NetBanka Živnostenské banky.....	38

4.3.3	Systémy fungující na principu platebních karet.....	40
4.3.3.1	Pay MUZO.....	40
4.3.3.2	Platby kartou na Internetu od České spořitelny.....	43
4.4	Shrnutí a závěry.....	45
5	Mikroplatební systémy.....	46
5.1	Vymezení pojmu mikroplatební systémy.....	46
5.2	Cíle kapitoly.....	46
5.3	Co jsou mikroplatební systémy.....	46
5.4	K čemu mohou sloužit mikroplatby a proč je potřebujeme.....	47
5.5	Možné problémy mikroplatebních systémů.....	49
5.6	Dopad zákona č. 124/2002 Sb. na mikroplatební systémy v ČR.....	49
5.7	Systém Monетка.....	50
5.7.1	O systému.....	50
5.7.2	Zabezpečení.....	51
5.7.3	Náklady.....	51
5.7.4	Zhodnocení.....	51
5.8	Systém i-plus.....	52
5.8.1	Co je systém i-plus a jak funguje.....	52
5.8.2	Jaký je vliv zákona č. 124/2002 Sb. na tento systém.....	53
5.8.3	Zhodnocení.....	53
5.9	Shrnutí a závěry.....	53
6	Mobilní platby.....	55
6.1	Cíle kapitoly.....	55
6.2	Úvod.....	55
6.3	Mechanismus fungování mobilních plateb.....	56
6.3.1	M-platba.....	56
6.3.2	Premium SMS.....	56
6.3.3	Speciální telefonní čísla.....	57
6.4	Možnosti, výhody a omezení mobilních plateb.....	57
6.4.1	Možnosti.....	57
6.4.2	Výhody.....	58
6.4.3	Omezení.....	58
6.5	Zabezpečení m-plateb.....	59
6.6	Integrace mobilních plateb do elektronického obchodování.....	60
6.7	Asociace pro mobilní platby.....	60
6.8	Co nabízejí jednotliví operátoři.....	61
6.8.1	T-Mobile m-platba.....	61
6.8.1.1	Fungování systému.....	61
6.8.1.2	Systém a jeho výhody pro zákazníka.....	63
6.8.1.3	Systém z pohledu obchodníka.....	63
6.8.1.4	Důvěryhodnost a rozšíření.....	63
6.8.1.5	Zhodnocení.....	64
6.8.2	M-Platby u Oskara/Vodafone.....	64
6.8.3	M-platby u EuroTelu.....	65
6.9	Shrnutí a závěry.....	65
7	Bezpečnost.....	67
7.1	Cíle kapitoly.....	67
7.2	Zabezpečení a rizika na straně obchodníka.....	67
7.3	Zabezpečení a rizika na straně uživatele.....	68
7.4	Zabezpečení přenosu dat.....	69
7.4.1	Protokol SSL.....	69

7.4.2 Protokol SOAP-over-SSL.....	70
7.5 Formy zabezpečení údajů o kreditních kartách.....	71
7.6 Technologie 3-D Secure.....	73
7.6.1 Výhody 3-D Secure.....	74
7.6.2 Proč „3-D“.....	74
7.6.3 Schéma fungování 3-D Secure.....	75
7.6.4 Požadavky na jednotlivé účastníky.....	77
7.6.5 Zhodnocení.....	77
7.7 Shrnutí a závěry.....	78
8 Případová studie konkrétní firmy.....	79
8.1 Stručný popis analyzované firmy.....	79
8.2 Výběr platebního systému.....	79
8.3 Náklady na zavedení systému.....	80
8.4 Očekávané přínosy ze zavedení platebního systému.....	81
8.4.1 Finanční přínosy.....	81
8.4.2 Ostatní přínosy.....	82
8.5 Závěry.....	82
9 E-billing.....	83
9.1 Co je to e-billing a k čemu slouží.....	83
9.2 Jak funguje e-billing.....	83
9.2.1 Model Seller Direct.....	84
9.2.1.1 Průběh transakce.....	84
9.2.1.2 Přínosy a úskalí modelu pro jednotlivé účastníky.....	85
9.2.2 Buyer Direct.....	86
9.2.2.1 Průběh transakce.....	86
9.2.2.2 Přínosy a úskalí modelu pro jednotlivé účastníky.....	87
9.2.3 Model Consolidator.....	87
9.2.3.1 Průběh transakce.....	88
9.2.3.2 Přínosy a úskalí modelu pro jednotlivé účastníky.....	89
9.3 Výhody a možné problémy e-billingu obecně.....	89
9.4 E-billing a legislativa Evropské Unie.....	90
9.5 Právní úprava e-billingu v ČR.....	91
9.6 Srovnání s klasickými systémy.....	92
9.6.1 Porovnání.....	92
9.6.2 Výhody, nevýhody a případné problémy.....	92
9.6.3 Náklady.....	94
10 Závěry.....	95
Definice pojmů.....	100
Seznam obrázků.....	102
Přehled literatury a zdrojů.....	103
Přílohy.....	108

1 Úvod

Nacházíme se přibližně v polovině první dekády třetího tisíciletí. Internet se již stal pro mnoho lidí běžnou součástí každodenního života, penetrace mobilních telefonů překročila sto procent. Zvykli jsme si na to, že na Internetu lze sehnat téměř vše, na co si jen vzpomeneme, zvykli jsme si na to, že mnoho z těchto věcí je k dispozici zadarmo. Pokud někdo nemůže něco sehnat, často dostane radu typu „podívej se na Internet, tam to určitě seženeš“. Mnoho předpovědí z konce minulého století slibovalo, že v této době budou nákupy přes Internet bezproblémové a zřejmě i docela běžné. Je tomu ale opravdu tak? Je opravdu tak jednoduché si „cokoli“ přes Internet objednat a zaplatit a obstarat si tedy zboží či služby bez toho, aby bylo nutné opustit teplo domova či kanceláře? Fakt, že na Internetu lze téměř všechno najít, případně i objednat, však ještě neznamená, že je tak jednoduché to přes Internet i zaplatit.

Mnoho firem už má své Internetové stránky, kde často nabízí své služby či propaguje své výrobky. Ale pokud by chtěly své výrobky či služby přes Internet i prodávat, jaké jsou jejich možnosti, jak mohou zajistit, aby jim zákazník zaplatil a ony mu tedy mohly dodat zboží?

Ač se o této problematice často mluví, ucelený přehled o platebních systémech dostupných v České republice není k dispozici. Mnoho firem, které by o prodeji přes Internet uvažovaly, nemají dostatek informací o tom, jaké mohou zákazníkům nabízet způsoby platby. A někteří zákazníci, kteří by často uvítali možnost objednat si zboží či službu z pohodlí domova, se pozastaví ve chvíli, kdy mají zaplatit. Často se bojí, že o své peníze přijdou, že takovéto transakce nejsou bezpečné.

Jaké jsou tedy možnosti placení za zboží a služby na Internetu v České republice a jaké jsou jejich výhody, problémy, dostupnost, zabezpečení a další záležitosti s nimi související, se snaží přiblížit text této práce.

1.1 Cíle práce

Cílem této práce je poskytnout popis a zevrubnou analýzu **elektronických platebních systémů dostupných obchodníkům a zákazníkům v České republice**. Tato práce se nezaměřuje jen na problematiku běžných platebních systémů, ale i mikroplatebních systémů dostupných v České republice. V této souvislosti též nelze opominout mobilní platby, o nichž se v poslední době často mluví, zejména, ale nejen, v souvislosti s mikroplatbami. Kvůli možnosti srovnání je jedním z cílů práce též popis a hlubší analýza platebního systému PayPal, který je leaderem ve zmiňované oblasti a proto ho nelze opominout. Mimo to, lze očekávat, že v budoucnu bude jeho plné využití možné i v České republice.

Kromě systému PayPal se práce nesnaží analyzovat ani popisovat jiné platební systémy, které jsou dostupné v jiných zemích.

V závěru práce bude ještě zmíněna problematika e-billingu (elektronického vystavování faktur), neboť tato oblast souvisí s platebními systémy v tom smyslu, že umožňuje plnou elektronizaci transakce, tedy bez použití klasických („papírových“) metod. Cílem tedy také je analyzovat právní prostředí v České republice, zda-li je na elektronické vystavování faktur dostatečně připraveno.

Cílovou zájmovou skupinou tohoto textu jsou čeští obchodníci a zákazníci a další čtenáři zabývající se nějakým způsobem touto problematikou.

1.2 Přínosy práce

Jako hlavní přínosy práce byly identifikovány následující:

- Podat informace o tom, jaké platební systémy jsou na českém trhu dostupné.
- Přiblížit problematiku legislativy, která se dotýká některých platebních systémů, zejména systémů mikroplatebních.
- Poskytnout analýzu platebních systémů dostupných v České republice – jaké jsou jejich silné a slabé stránky – výhody a nevýhody pro jednotlivé účastníky, zejména pro zákazníky a obchodníky, případně pro provozovatele systému.
- Nabídnout srovnání mezi jednotlivými systémy navzájem a se systémem PayPal, který je v daném oboru světovou jedničkou.
- Poskytnout hlubší analýzu systému PayPal.
- Analyzovat některé technologie používané při zabezpečení platebních systémů, zejména technologii 3-D Secure.
- Přiblížit problematiku e-billingu (elektronického vystavování faktur) a analyzovat právní prostředí v této oblasti v České republice.

1.3 Struktura práce

Práce začíná stručným přehledem některých historických událostí (ve 2. kapitole), které měly nějaký významnější dopad na formování budoucnosti platebních systémů.

Ve 3. kapitole je uvedeno rozdělení platebních systémů a poté následuje popis a analýza jednotlivých platebních systémů v kapitolách 4 („obyčejné“ platební systémy), 5 (mikroplatební systémy) a 6 (mobilní platby).

Kapitola 7 se potom zabývá problematikou bezpečnosti, která se prolíná všemi platebními systémy a která je pro jejich úspěch klíčová.

V 8. kapitole je uvedena případová studie konkrétní firmy, která uvažuje o zavedení některého z popisovaných platebních systémů.

Kapitola devátá přibližuje problematiku e-billingu a hlouběji analyzuje právní prostředí týkající se tohoto tématu v České republice.

Na konci práce jsou uvedeny definice, které vysvětlují některé termíny důležité pro pochopení textu.

2 Historie

2.1 Cíle kapitoly

Cílem této kapitoly je podat stručný přehled o historii platebních systémů, respektive zmínit některé z důležitých událostí, které měly vliv na další formování platebních systémů. Cílem není podrobně popsat celou historii, ale předložit čtenáři určité „milníky“, které se nějak podílely na vývoji v této oblasti.

2.2 Stručná historie platebních systémů

Historie elektronických platebních systémů se shoduje s historií elektronického obchodování jako takového.

Názory na vůbec první e-commerce společnost se liší. Podle některých názorů¹ byla první e-commerce společností The International Stamp Exchange založená v polovině osmdesátých let americkým podnikatelem Armandem Rousso. Podle jiných zdrojů² byla průkopníkem v elektronických platbách korporace National BankAmericard Inc. (později známá pod názvem VISA U.S.A.), když již v roce 1973 uvedla na trh systém BASE I, první globální elektronický systém pro ověřování platebních karet. Tento systém zkrátil dobu ověření karty z více než pěti minut na méně než jednu minutu.



Obrázek 2.1: Platební karta BankAmericard (dnes známá jako VISA)

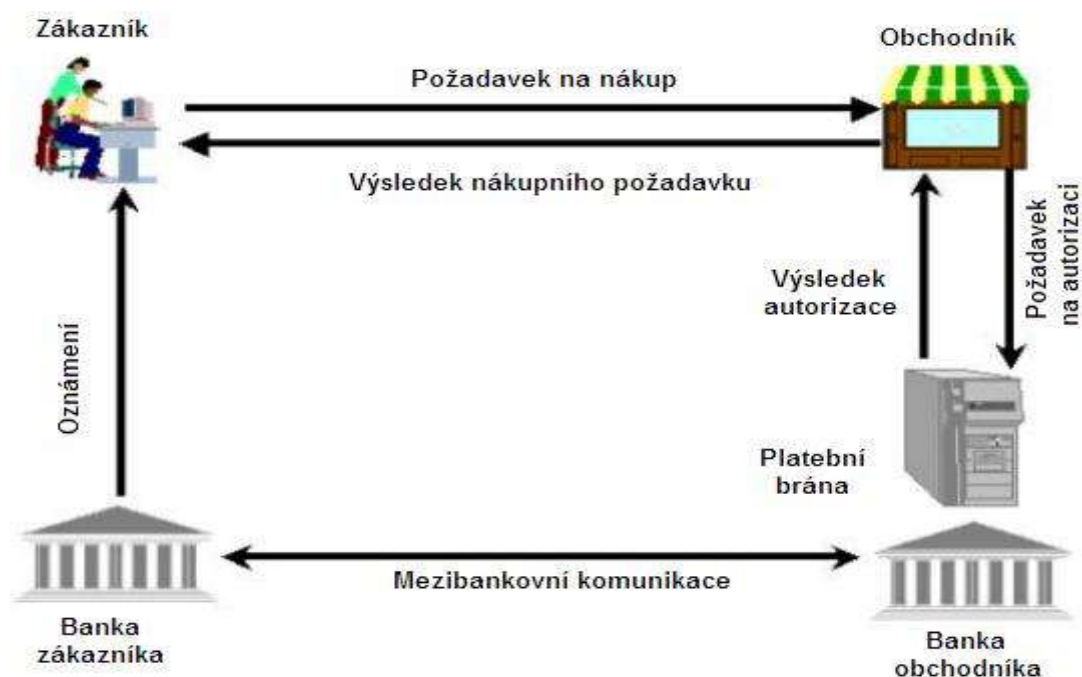
Zdroj: <http://www.grabbingsand.com/wordpress/wp-content/bankamericard.jpg>

V roce 1996 firmy VISA a MasterCard (ve spolupráci se společnostmi GTE, IBM, Microsoft, Netscape, Verisign a dalšími) vyvinuly systém SET (Secure Electronic Transaction). V současné době se tento systém nevyužívá, mimo jiné proto, že byl nahrazen systémem 3-D Secure, ale v druhé polovině devadesátých let se jednalo o systém, od kterého si světoví i čeští obchodníci slibovali mnohé. Jedná se o systém, který měl zabezpečovat transakce týkající se platebních/kreditních karet, které se uskutečňují v nezabezpečených sítích, tedy myšleno v

¹ <http://www.armandrousso.com/about.htm>

² http://usa.visa.com/about_visa/about_visa_usa/history.html

Internetu. SET používá SSL (Secure Socket Layer), STT (Secure Transaction Technology), Secure HTTP a některé aspekty PKI (Public Key Infrastructure). Provádění a ověřování transakcí funguje na principu digitálních klíčů a certifikátů mezi zákazníkem obchodníkem a bankou zákazníka.



Obrázek 2.2: Schéma fungování SET

Zdroj: <http://www2.ellinogermaniki.gr/ep/agroweb/htmls/lessons/commerce1/423.htm>

V roce 1998 Peter Thiel a Max Levchin založili platební systém PayPal. Původně byl systém PayPal zamýšlen pro posílání plateb pomocí zařízení PDA (Personal Digital Assistant).

V roce 1999 uskutečnila VISA první pokusnou platbu mobilním telefonem uskutečněnou v síti GSM ve městě Leeds ve Velké Británii. Společnost ve spolupráci se společnostmi Nokia a MeritaNordbanken of Finland také oznámila pilotní program umožňující platby pomocí mobilních telefonů a to jak u obchodníků v kamenných obchodech, tak na Internetu.

Od roku 2000 nejsou držitelé karet VISA odpovědní za podvody uskutečněné pomocí VISA karet, ke kterým dojde při platbách na Internetu. Do roku 2000 ručili držitelé VISA karet do částky 50 USD, jestliže nenahlásili krádež nebo jinou možnou neoprávněnou manipulaci s platební kartou do dvou pracovních dnů.

V roce 2001 uskutečnila VISA první platební transakci pomocí počítače Palm™. Společnosti VISA a Palm spolupracovaly s výrobcí platebních terminálů Ingenico a VeriFone na vytvoření technologie, která by umožnila bezpečný přenos informací o platbě mezi počítačem Palm a platebním terminálem VeriFone či Ingenico pomocí IR³ technologie.

V roce 2002 byl PayPal koupen aukční společností eBay a software pro PDA se přestal používat. Namísto něj se začalo používat webové rozhraní, které se stalo mezi uživateli eBay velmi populární. V roce 2004 dosáhla hodnota transakcí uskutečněných přes PayPal hodnoty 18,9 miliard amerických dolarů⁴.

³ IR – InfraRed – přenos dat pomocí infračerveného záření

⁴ <http://en.wikipedia.org/wiki/PayPal#Beginnings>

3 Rozdělení platebních systémů

3.1 Cíle kapitoly

Cílem této kapitoly je rozdělit platební systémy podle několika možných hledisek. Tato kapitola se zabývá pouze možným rozdělením platebních systémů, popis a analýza těchto systémů pak následují v dalších kapitolách.

3.2 Definice základních pojmů

Platební systém

Například Federal Financial Institutions Examination Council uvádí, že platebním systémem jsou:
*„Mechanismy, pravidla, instituce, lidé, trhy a smlouvy, které umožňují provádění plateb.“*⁵

Jinou definicí může být, že platební systém je:

*„Sada instrukcí a procedur používaných pro přesun vlastnictví a vypořádání závazků vycházejících ze směny zboží a služeb.“*⁶

Elektronický

*„Elektronický znamená vztahující se k technologii, která má elektrické, digitální, magnetické, bezdrátové, optické, elektromagnetické nebo podobné schopnosti.“*⁷

Elektronická platba

*„Elektronická platba je přesun finančních prostředků, která se uskutečňuje na Internetu mezi kupujícími a prodávajícími. Finanční prostředky mohou mít podobu elektronických peněz, zašifrovaných čísel kreditních karet nebo obdobných údajů a jsou spravovány bankou nebo nějakým prostředníkem.“*⁸

⁵ Zdroj: <http://www.ffiec.gov/ffiecinfobase/booklets/Wholesale/18.html>

⁶ Zdroj: <http://www.cashflowspecialistsinc.com/glossary/#P>

⁷ Zdroj: <http://janus.state.me.us/legis/statutes/10/title10sec9402.html>

⁸ Podle <http://www.ignou.ac.in/virtualcampus/adit/course/cst304/ecom2.htm>

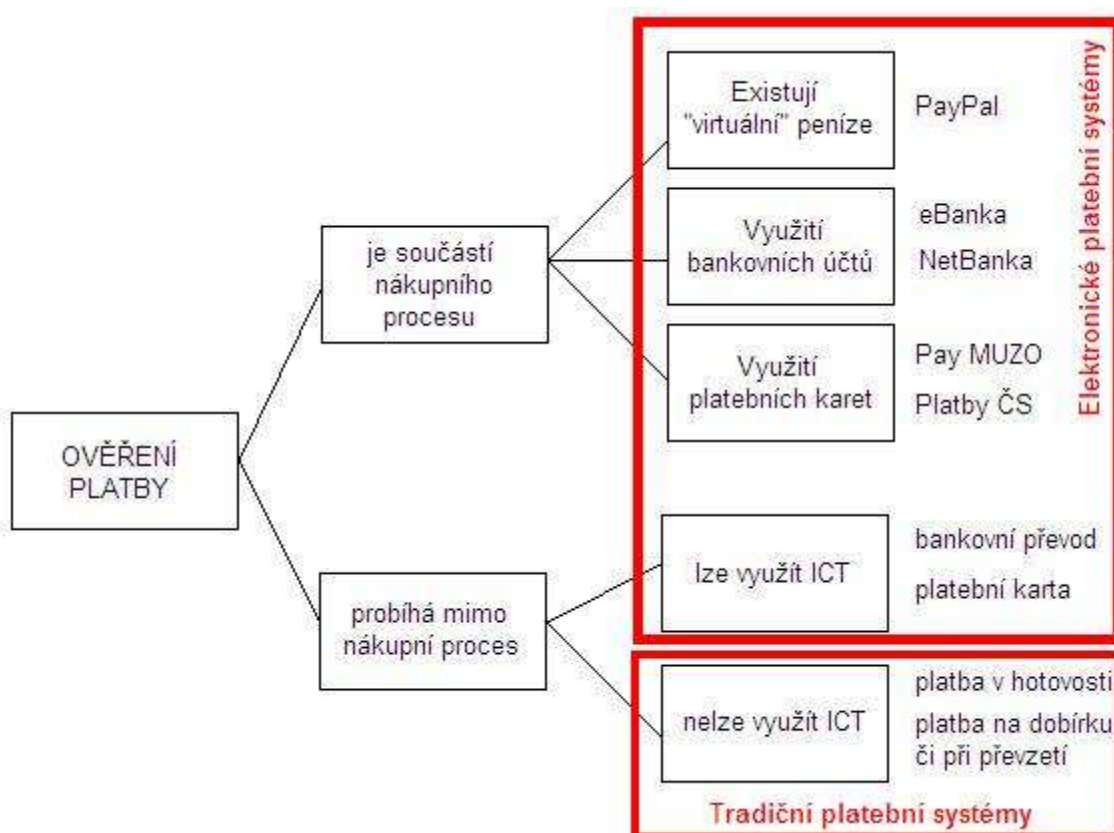
Elektronický platební systém

Na základě výše uvedených definic, můžeme tedy říci, že **elektronický platební systém je soubor pravidel, instrukcí, mechanismů a procedur, který umožňuje platbu provedenou kupujícím ve prospěch prodávajícího uskutečňovanou elektronicky.**

3.3 Klasifikace platebních systémů

Platební systémy lze dělit dle několika hledisek. Pro tuto práci je nejdůležitějším hlediskem způsob ověření platby (viz obrázek 3.1). Dalším hlediskem může být, zda se jedná o tradiční platební systémy nebo o elektronické platební systémy (vyznačeno též na obrázku 3.1). Pro rozdělení platebních systémů je důležité i zařízení, pomocí kterého je platba provedena (obrázek 3.2). Pro rozdělení platebních systémů lze použít i hledisko objemu plateb, tedy výše částky, která je pomocí platebního systému zaplácena (obrázek 3.3).

3.3.1 Rozdělení platebních systémů podle způsobu ověření platby



Obrázek 3.1: Rozdělení platebních systémů podle způsobu ověření platby

Jak ukazuje obrázek, ověření platby může být buď součástí nákupního procesu, nebo může probíhat mimo něj.

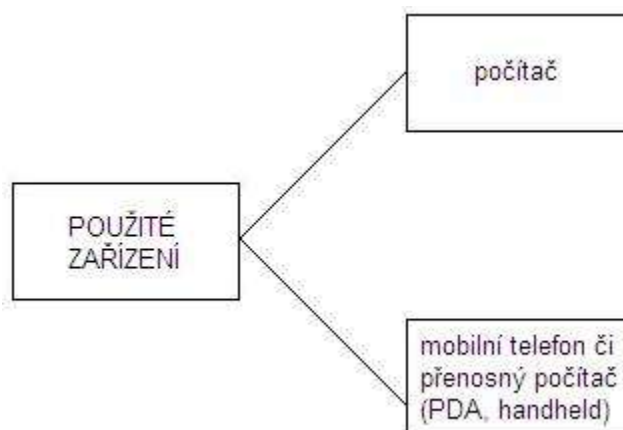
Jestliže je platba součástí nákupního procesu, znamená to, že nákupní transakce nemůže být dokončena bez toho, aby byla provedena platba. Zaplacení zákazníkem za objednanou službu nebo produkt je tedy nezbytnou podmínkou k tomu, aby obchodník začal vyřizovat objednávku. Tuto skupinu platebních systémů lze dále dělit na systemy, které využívají virtuálních účtů a ve kterých existují „virtuální peníze“⁹ (takovým je například PayPal), systemy využívající převodů mezi bankovními účty (například systemy eBanka či NetBanka) a systemy využívajících platebních karet (například systém Pay MUZO anebo platby kartou na Internetu od České spořitelny).

Naproti tomu, **jestliže platba není součástí nákupního procesu, znamená to, že nákupní transakce může být dokončena bez závislosti na tom, jestli byla provedena platba.** Platba tedy není realizována společně s objednávkou, je realizována jiným způsobem. Podle toho, jakým způsobem je platba realizována lze tuto skupinu systémů dále dělit na systemy, které umožňují využití informačních a komunikačních technologií (poskytnutí čísla platebních karty obchodníkovi, převod finančních prostředků na účet obchodníka například pomocí Internetového bankovníctví) a na systemy, které využití informačních a komunikačních technologií neumožňují (například platba v hotovosti, či na dobírku).

Všechny systemy, u kterých je ověření platby součástí nákupního procesu, a systemy, u kterých sice není ověření platby součástí nákupního procesu, ale které umožňují využití informačních a komunikačních technologií, lze označit za **elektronické platební systemy**. Systemy, u kterých ověření platby není součástí nákupního procesu a které ani neumožňují využití informačních a komunikačních technologií lze označit jako **tradiční platební systemy**. Viz též obrázek 3.1, vyznačeno červenou barvou.

⁹ Virtuálními penězi rozumíme tradiční peníze, které byly vloženy do elektronického platebního systému z důvodu zjednodušení platebních transakcí. (Zdroj: <http://www.webcorp.ru/page/oemoney.html>)

3.3.2 Rozdělení platebních systémů podle zařízení pomocí něhož je platba provedena

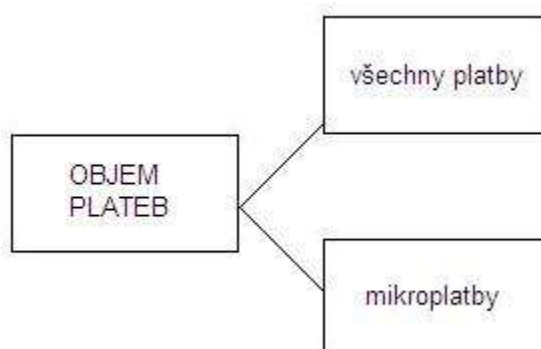


Obrázek 3.2: Rozdělení platebních systémů podle zařízení použitého pro provedení platby

Z hlediska zařízení, pomocí něhož je platba provedena, rozlišujeme **osobní počítač**, tedy zařízení, pomocí něhož lze zaplatit z domova, z kanceláře a podobně. Podstatným rysem takového zařízení je, že jej jeho uživatel nemá u sebe neustále.

Naopak zařízení, jako je **mobilní telefon či příruční počítač**, tzv. handheld či PDA, je zařízení, které má uživatel u sebe většinu času.

3.3.3 Rozdělení platebních systémů podle objemu plateb



Obrázek 3.3: Rozdělení platebních systémů podle objemu plateb

Podle objemu platby, nebo-li částky, která je pomocí systému placena, lze rozlišovat mikroplatební systémy a ostatní systémy. Platby uskutečňované pomocí mikroplatebních systémů se nazývají

mikroplatby. Mikroplatbou se myslí částka v řádu haléřů až stovek korun, přesná definice se liší podle státu. Například Evropská Unie definuje jako mikroplatbu takovou platbu, hodnota jejíž transakce nepřesáhne částku 15 EUR. Důležité je, že mikroplatebním systémem nazýváme takový systém, který se specializuje na mikroplatby, a není tedy pomocí něj možné platit částky, které neodpovídají definici mikroplatby. Naproti tomu ostatní (nemikroplatební) systémy umožňují platby jak malých částek (mikroplateb), tak částek vyšších.

3.4 Zaměření práce

Hlavním zaměřením této práce jsou systémy, u kterých je ověření platby součástí nákupního procesu a které jsou dostupné obchodníkům a zákazníkům v České republice. Tyto systémy jsou popsány a analyzovány ve čtvrté kapitole.

Systémům, ve kterých je platba provedena pomocí mobilního zařízení je věnována samostatná (pátá) kapitola.

Specifika týkající se mikroplatebních systémů jsou rozebrány v šesté kapitole.

Zaměřením této práce není detailní popis platebních systémů, u kterých ověření platby není součástí nákupního procesu, tedy ani popis systémů Internetového bankovníctví a podobně. Systémy, u kterých ověření platby není součástí nákupního procesu, jsou pouze zmíněny na začátku čtvrté kapitoly a to zejména z toho důvodu, že jsou v současné době pro placení za zboží a služby na Internetu stále ještě značně populární.

4 Popis a analýza platebních systémů

4.1 Cíle kapitoly

Cílem této kapitoly je popsat, zanalyzovat a zhodnotit nejvýznamnější platební systémy a jejich a silné a slabé stránky, které jsou dostupné zákazníkům a obchodníkům v České republice. Tedy ty systémy, se kterými se čeští uživatelé mohou setkat při svých nákupech na Internetu a které mohou české podniky obchodující na Internetu běžně implementovat. Předmětem zkoumání této kapitoly jsou běžné platební systémy, míněno ne mikroplatební systémy nebo mobilní platby. Ty jsou popsány v následujících kapitolách. Předmětem zkoumání v této kapitole je i systém PayPal, který nemůže být českými obchodníky implementován, ale do tohoto textu byl zařazen ze dvou hlavních důvodů. Prvním důvodem je, že žádný systém takového typu v České republice není a cílem je dát čtenáři možnost určitého srovnání. Druhým a neméně důležitým důvodem je, že systém PayPal je v oblasti platebních systémů tak významný, že jej nelze opominout. Navíc, ačkoli tento systém nemohou implementovat čeští obchodníci, tak čeští zákazníci se s ním setkat mohou, a v případě, že platí v zahraničních, zejména amerických, obchodech, tak se s ním pravděpodobně i setkají.

Tato kapitola bude přínosem jednak pro zákazníky, kterým umožní nahlédnout do problematiky fungování platebních systémů a některé z nich jim představí. Pro obchodníky je přínosem v tom smyslu, že jim může pomoci v rozhodování zda a jaký platební systém případně ve svých Internetových obchodech implementovat. Další stranou, pro kterou může být text užitečný, jsou existující či potenciální poskytovatelé platebních systémů, kterým umožní odkrýt některé výhody a problémy spojené s platebními systémy.

4.2 Platební systémy, u nichž ověření platby není součástí nákupního procesu

Platební systémy, u nichž ověření platby není součástí nákupního procesu můžeme dále rozdělit na systémy, které umožňují využití informačních a komunikačních technologií (jedná se tedy o systémy, které lze považovat za elektronické platební systémy) a na systémy, které toto využití neumožňují (tradiční platební systémy).

4.2.1 Systémy, které umožňují využití informačních a komunikačních technologií

4.2.1.1 Bankovní převod

Jedná se o poměrně jednoduchý způsob placení, kdy zákazník může provést celou transakci z domova nebo kanceláře. Pochopitelně je zapotřebí, aby měl u své banky aktivovanou službu Internetového, telefonního nebo GSM bankovníctví. Tyto služby jsou však běžně dostupné a většinou tedy nečiní zákazníkovi žádný problém. Platbu bankovním převodem lze provést i převodním příkazem zadaným osobně v bance, tento způsob je však velmi nepraktický, protože zákazník musí jít do banky a ztrácí tak veškeré výhody elektronického platebního systému.

Pro obchodníka je tento způsob platby poměrně atraktivní, neboť zákazník zaplatí obchodníkovi předem. Nevýhodou ovšem je, že peníze jsou na účet připsány s časovým zpožděním (konkrétní prodleva je závislá na bankách obchodníka a zákazníka) a celá transakce se tedy zdržuje.

Nicméně pro zákazníky tento způsob příliš zajímavý není, neboť se musí v podstatě spoléhat na solidnost obchodníka, musí věřit, že objednané zboží či službu opravdu poskytne.

4.2.1.2 Platba kreditní/debetní kartou (ověření platby není součástí nákupní transakce)

Tento způsob spočívá v tom, že zákazník na stránkách obchodníka vyplní formulář, který obsahuje údaje o jméně zákazníka, číslu platební karty a měsíce a roku expirace platební karty. Tato data jsou odeslána obchodníkovi, který provede „ručně“ platbu kreditní/debetní kartou – obvykle zavolá do banky, aby zjistil, zda je možné s uvedenou platební kartou transakci provést a poté ji provede na svém terminálu. Tato procedura však nějakou dobu trvá a tak zákazník neví ihned, stejně jako u platby bankovním převodem, jestli jeho objednávka bude kladně vyřízena.

Dalším problémem je, že citlivé údaje se musí sdělit přímo obchodníkovi, což znamená určité bezpečnostní riziko a vyžaduje tedy značný stupeň důvěry v obchodníka.

Přenos dat mezi zákazníkem a obchodníkem by měl být pochopitelně zabezpečen. Dostačující je protokol SSL a 128-bitové šifrování. Pokud tomu tak není, uskutečnění takové transakce je velmi nebezpečné i pokud zákazník svému obchodníkovi věří. Nezašifrovaná data totiž mohou být při přenosu snadno zachycena a zneužita.

Tento způsob není příliš obvyklý, přesto se však ještě v ojedinělých případech používá.

4.2.2 Systémy, které neumožňují využití informačních a komunikačních technologií

4.2.2.1 Platba u obchodníka

Tento způsob platby je obvykle spojen s fyzickým převzetím zboží v místě prodeje. Jeho implementace je pro obchodníka bezproblémová a nejsou s ní spojeny žádné dodatečné náklady. Zákazník si zboží vybere na Internetu (v e-shopu) a v podstatě si ho pouze „zamluví“. Poté se dostaví do prodejny obchodníka, kde je pro něj zboží připraveno, on si jej zkontroluje a zaplatí. Je možné platit v hotovosti nebo jakýmkoli jiným standardním způsobem (šek, platba kreditní či debetní kartou, ať už na on-line platebním terminálu nebo na imprinteru¹⁰, lidově označovaném též jako „žehlička“. Tento způsob platby je pro zákazníky atraktivní z toho důvodu, že umožňuje si zboží prohlédnout na vlastní oči před tím, než za něj zaplatí. Zákazník také ví, kde se nachází kamenný obchod společnosti, u které nakupuje, což je pro zákazníka určitou zárukou – ví, kde obchodník fyzicky sídlí a kde případně zboží reklamovat.



Obrázek 4.1: Imprinter

Zdroj:

http://www.usamerchantsolutions.com/sc_images/misc_pics/505_manual_imprinter.jpg

Výhodou také je, že jelikož platba probíhá v hotovosti, nevznikají žádné další náklady spojené s platbou ani pro zákazníka ani pro obchodníka.

Samozřejmě, tento způsob nemá žádné výhody on-line nakupování, zákazník používá Internetu pouze pro vyhledání zboží a obchodníka, který jej nabízí, a objednání si tohoto zboží. Nicméně tento způsob placení za zboží objednané na Internetu je v současné době v naší zemi stále hojně využíván.

¹⁰ Imprinter, často známý pod lidovým názvem žehlička, je off-line obchodní platební terminál. Jedná se o mechanické zařízení umožňující platbu kreditní či debetní embosovanou kartou v místech, která nejsou napojena on-line na ověřovací systém. Imprinter (žehlička) udělá mechanickou kopii jména, čísla a data expirace platební karty. Transakce je obvykle ověřována telefonicky zaměstnancem obchodníka.

4.2.2.2 Platba na dobírku

V současnosti v České republice velmi běžný způsob, jehož výhodou je, že je pro zákazníky bezpečný – zaplatí až zboží fyzicky převezmou.

Při platbě na dobírku se využívá služeb České pošty, která zajišťuje i doručení zboží na poštu místně příslušnou zákazníkovi. Bohužel, zákazník si musí pro zboží na poštu dojít, což uživatelskou přívětivost snižuje.

Za službu dobírka si Česká pošta účtuje částku 10,- Kč¹¹. Kromě toho si však obchodník obvykle ještě naučtuje poštovné a balné. Výši této částky nelze jednoznačně určit, neboť je závislá na několika faktorech, kterými jsou zejména velikost/hmotnost zasílaného balíku, rychlost doručení a další.

4.2.2.3 Platba při převzetí

Při tomto způsobu placení je zboží zákazníkovi doručeno až do domu a to buď zaměstnancem obchodníka provádějícího distribuci nebo kurýrní službou, s níž má obchodník smlouvu. Platba probíhá při převzetí zboží do rukou pracovníka. Pro zákazníky je tento způsob velmi pohodlný a také bezpečný – mohou si zboží před platbou prohlédnout a zkontrolovat, že je vše v pořádku. Nevýhoda je však v tom, že za doručení a platbu je obvykle účtován nějaký příplatek¹².

4.2.2.4 Další způsoby

Existují ještě i další možnosti placení, jako například poštovní poukázkou (složenkou) nebo šekem, ale ty nejsou v České republice příliš rozšířené.

¹¹ Dle informací uvedených na stránkách České pošty (www.cpost.cz) a poskytnutých pracovníkem zákaznického centra České pošty (telefonický rozhovor ze dne 30. prosince 2005)

¹² Výše příplatku nelze jednoznačně určit, je velmi proměnlivá. Závisí na vzdálenosti zákazníka od místa distribuce, velikosti doručovaného balíčku, zprostředkovateli (zda doručení provádí obchodník sám či kurýrní služba) a dalších faktorech. Například při doručení balíčku standardní velikosti kurýrní službou v rámci hlavního města se částky mohou pohybovat v relacích okolo dvou set korun.

4.3 Platební systémy, u nichž je ověření platby součástí nákupního procesu

Hlavním atributem platebních systémů, u nichž je ověření platby součástí nákupního procesu, je, že transakce se ověřuje on-line v reálném čase – zákazník i obchodník tedy ihned vědí, zda-li autorizace proběhla úspěšně a že tedy k přesunu částky od zákazníka k obchodníkovi opravdu dojde. To je hlavní výhoda těchto systémů, neboť obchodník může ihned začít expedovat zboží či poskytovat službu. Zákazník ví, že částku zaplatil a pokud by mu nebyla služba či zboží poskytnuto, může vzniklý problém okamžitě řešit, ví, že problém není s platbou.

Tyto systémy lze dále dělit na systémy s virtuálními účty, na kterých jsou uloženy „virtuální“ peníze, systémy využívající převodů mezi bankovními účty a systémy využívající platebních karet.

4.3.1 Systém PayPal



PayPal je systém, který se řadí mezi platební systémy, u nichž je ověření platby součástí nákupní transakce a které využívají virtuálních účtů. Dobití účtu je sice možné platební kartou nebo převodem z bankovního účtu, ale princip fungování PayPalu je založen na tom, že každý uživatel má svůj virtuální PayPal účet. PayPal sice umožňuje platby malých částek, ale **není považován za mikroplatební systém**. Navíc vzhledem k poplatkům není přijímání malých částek v mnoha případech ekonomicky výhodné.

PayPal je obecně považován za velmi dobrý systém, zajímavý jak pro zákazníky, tak pro obchodníky. Nicméně, jak ukážeme dále, má i své negativní stránky. Nicméně fakt, že se jedná o nejrozšířenější systém (např. podle Gartnera), lze asi těžko popřít. Tento systém obhospodařuje v současnosti kolem osmdesáti miliónů účtů v 56 zemích, což ho řadí mezi jeden z největších Internetových platebních systémů na světě.

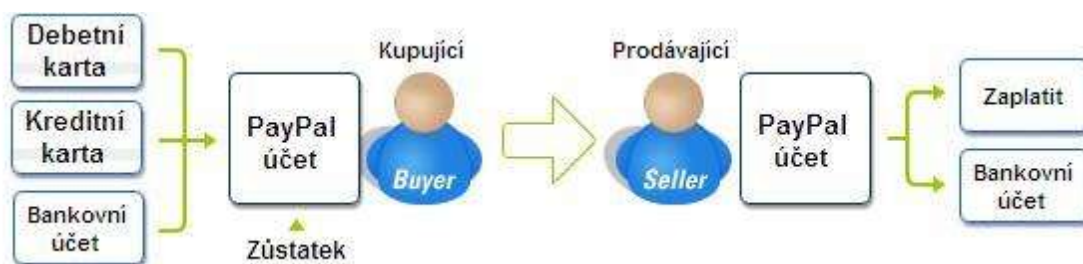
V současnosti bohužel není plně dostupný pro uživatele v České republice (viz dále), nicméně lze doufat, že postupem času zde bude nabízen. Pro obchodníky poskytující své zboží či služby na Internetu by jeho využívání mělo, hlavně v souvislosti s určitými potížemi se zavedením jiných platebních systémů, velkou přidanou hodnotu.

Síť PayPalu je založena na existující finanční struktuře bankovních účtů a kreditních karet, pomocí které vytváří globální platební systém fungující v reálném čase.

Obchodní model je založen zejména na zpoplatňování obchodníků za příchozí platby. Viz též dále.

4.3.1.1 Jak PayPal funguje

PayPal je systém, který umožňuje platby kreditní či debetní kartou, převodem z bankovního účtu anebo převodem prostředků z PayPal účtu. Výhodou je, že uživatel, který prostřednictvím systému odesílá platbu, nemusí příjemci odhalit číslo své kreditní karty ani jiné citlivé finanční informace.



Obrázek 4.2: Průběh platby v systému PayPal

Zdroj: http://www.my-it.info/ebay-easy/images/ebay-images/paypal_works.gif

System je patrně nejvíce známý z aukčního serveru eBay¹³, ale umožňuje zprostředkování jakýchkoli plateb, kromě samozřejmého nakupování na Internetu, též například vyrovnání dluhů s přáteli.



Příjemce, který musí mít samozřejmě zřízený PayPal účet, je identifikován svojí emailovou adresou. A co kdyby příjemce neměl zřízený PayPal účet? V tom případě se mu odešle email, který ho upozorní na příchozí platbu. Příjemce si poté založí účet a částka se mu na tento účet připiše.

Použití systému je pro uživatele velmi jednoduché. Například při placení na aukčním serveru eBay, stačí v podstatě kliknout na tlačítko „Pay Now“ (zaplatit nyní), vyplnit potřebné informace na stránkách PayPalu, a po kliknutí na tlačítko „Pay“ (zaplatit) je platba provedena.

4.3.1.2 Výběr z PayPal účtu

Je možno převést peníze na běžný účet, nechat si poslat šek a nebo samozřejmě nechat je na PayPal účtu a použít je pro další platby.

Výběr finančních prostředků z PayPal účtu jako takový není systémem zpoplatněn, nicméně záleží na tom, v jakém státě se nachází banka, do níž jsou peníze převáděny. Převody do bank v některých státech mohou být zpoplatněny, konkrétní výše poplatku je dána sazebníkem přijímající banky.

4.3.1.3 Typy účtů

PayPal nabízí tři typy účtů. Jsou jimi „**Personal**“ (osobní), který je zdarma, ale neumožňuje příjem plateb uskutečněných pomocí kreditních či debetních karet. Dále „**Premier**“, který již není zdarma, ale umožňuje přijímání všech¹⁴ způsobů plateb. A „nejvyšším“ typem účtu je „**Business**“, který je vhodný pro on-line obchodování a který také umožňuje přijímání všech způsobů plateb. Jedná se o účet organizace, ne tedy o účet osobní.

Jednotlivé typy účtů jsou podrobněji popsány dále.

Personal Account

Jedná se o osobní účet, který je vhodný například pro posílání plateb, placení za zboží na eBay nebo pro on-line předplatné. Jak již bylo řečeno, **neumožňuje ovšem přijímání plateb uskutečněných platebními kartami**. Na druhou stranu se však **neplatí za odeslané ani přijaté platby**. Účet též umožňuje využívání služeb programu „Ochrany kupujícího (PayPal Buyer Protection)“, což je program, kde PayPal nabízí pomoc kupujícím, kteří se cítí prodávajícím poškozeni – PayPal se

¹³ Převzetí společností eBay Inc. proběhlo v říjnu roku 2002.

¹⁴ Tedy převodem z PayPal účtu, převodem z bankovního účtu, platbu debetních či kreditní kartou, včetně platby uskutečněné přes virtuální terminál.

účastní vyjednávání a pomáhá problém řešit. I přesto však vznikají některé specifické problémy – viz dále.

Z výše uvedeného vyplývá, že tento typ účtu **není vhodný pro subjekty, které chtějí nabízet možnost on-line placení.**

Premier Account

Umožňuje jak posílání, tak i **přijímání plateb na vlastní jméno** - tedy na jméno fyzické osoby (**ne organizace**).

Tento typ účtu **umožňuje již e-commerce** na vlastních Internetových stránkách a to pomocí nákupního košíku PayPal. Dále umožňuje například placení předplatného či jiné opakované¹⁵ platby.

K tomuto typu účtu se již vztahuje tzv. „Ochrana prodávajícího (Seller Protection)“, což je program, který prodávajícímu kompenzuje ztráty v případě, že kupující změní svůj úmysl a žádá své peníze zpět – specifické problémy spojené s programem ochrany kupujícího viz dále.

K dispozici je také možnost integrace s Back-End aplikacemi, která umožní potvrzení transakce v reálném čase pomocí komunikace server-server.

Business Account

Jedná se již o **účet vhodný pro on-line obchodování na vyšší úrovni**. Nabízí vše jako Premier Account, ale má navíc další výhody, mezi něž kromě jiných patří, že jméno organizace se objevuje na výpisech platebních karet zákazníků. Také se lze k jednomu PayPal účtu přihlašovat pod několika uživatelskými jmény, z nichž každé má jinou úroveň přístupu.

4.3.1.4 PayPal pro obchodníky

On-line obchodníkům nabízí PayPal čtyři možná řešení pro pokrytí jejich potřeb. Všechna řešení¹⁶ on-line plateb nabízí i zpracování off-line plateb a to pomocí virtuálního terminálu, přes který lze zpracovávat objednávky uskutečněné prostřednictvím telefonu, faxu, či klasické pošty¹⁷.

PayPal Website Payments Standard

Zákazník nakupuje na stránkách obchodníka, platí na PayPal. Funguje to tím způsobem, že zákazník vybírá zboží na stránkách obchodníka a po zvolení platební možnosti PayPal je přesměrován na

¹⁵ Opakovaná platba je taková platba, kdy se za každé období (například jeden měsíc) strhne z účtu příslušná částka. Pro každé opakované stržení není potřeba další autorizace – ta se provede jednou a platba se pak uskutečňuje pravidelně každé období.

¹⁶ U některých řešení je virtuální terminál již součástí, u některých je možné ho přikoupit.

¹⁷ Tyto služby jsou označovány termínem „MOTO“, což je zkratka pro „Mail Order / Telephone Order“

platební bránu PayPalu. Jedná se o nenáročných způsob, jak začít s přijímáním platebních karet na Internetu. Integrace do nákupního košíku obchodníka je jednoduchá, zabere pouze několik minut. Pro obchodníky, kteří nemají do svých stránek integrován vlastní nákupní košík, nabízí PayPal zřízení PayPal nákupního košíku zdarma.

PayPal Website Payments Pro

Zákazník nakupuje i platí na stránkách obchodníka, PayPal je pro nakupujícího v podstatě transparentní (neviditelný), čímž obchodníkovi umožňuje plně kontrolovat celou transakci, informace poskytované zákazníkovi a design platební brány.

Značnou nevýhodou ovšem je, že toto řešení je dostupné pouze v USA.



Obrázek 4.3: Schéma fungování PayPal Website Payments Pro

Zdroj: http://www.eshubie.com/uploaded_images/spot_wpPro-785985.gif

Oproti Website Payments Standard však může být integrace do webových stránek obchodníka poněkud více komplikovaná. Na druhou stranu Website Payments Pro je již součástí některých nákupních košíků, a v tomto případě problémy s integrací odpadají.

PayPal Email Payments

Jedná se o zajímavou alternativu, která umožňuje provádění on-line plateb i bez existence webových stránek. Toto řešení funguje tak, že účet/faktura se odešle na e-mail zákazníka, ten klikne na odkaz, který ho přesměruje na stránky PayPalu, kde potom zaplatí. Výhodou emailových plateb je, že je naprosto technicky nenáročná. Je několik způsobů, jak vytvořit emailovou fakturu či účet

(on-line, v e-mailovém programu) a ani jeden z nich nevyžaduje žádné velké technické či jiné odborné znalosti.

PayPal jako další způsob on-line plateb

Toto řešení je vhodné pro obchodníky, kteří už na svých stránkách umožňují platbu kreditní/debetní kartou a chtějí rozšířit okruh svých zákazníků. V tomto případě si zákazník vybere, zda-li chce platit standardním způsobem platební kartou nebo přes PayPal.

Integrace do stránek obchodníka může být relativně jednoduchá a umožní využívat výhod zmíněných u předchozích řešení.

4.3.1.5 Kde a jaké možnosti PayPal nabízí

PayPal umožňuje platby v měnách: Americký dolar, Euro, Libra, Kanadský dolar, Yen, Australský dolar.¹⁸

Akceptované kreditní/debetní karty jsou Visa, EuroCard/MasterCard, American Express¹⁹, Discover.²⁰

Plné využití (tedy posílání plateb a elektronický převod finančních prostředků na účet v místní bance) služeb PayPal je možné v následujících zemích: Austrálie, Belgie, Dánsko, Francie, Finsko, Holandsko, Hong Kong, Irsko, Itálie, Japonsko, Jižní Korea, Kanada, Mexico, Německo, Norsko, Nový Zéland, Portugalsko, Rakousko, Řecko, Singapur, Španělsko, Švédsko, Švýcarsko, Tchajwan, Velká Británie, USA.

Možnost zřídit účet, ale vybírání finančních prostředků není možné elektronicky do místní banky (pouze do banky v USA nebo šekem) je možné v zemích: Argentina, Brazílie, Chile, Čína, Ekvádor, Indie, Jamajka, Uruguay.

Bez možnosti výběru šekem (tedy pouze na účet v bance v USA) mohou využívat PayPal uživatelé v těchto zemích: Dominikánská republika, Island, Izrael, Kostarika, Lucembursko, Malajsie, Thajsko, Turecko, Venezuela.

A konečně poslední skupina zemí, ve kterých je možné používat PayPal účet pouze na posílání plateb (nelze tedy vybrat finanční prostředky z PayPal účtu): Anguilla²¹, Česká republika, Estonsko, Jižní Afrika, Kypr, Litva, Lotyšsko, Maďarsko, Malta, Polsko, Slovensko, Slovinsko.²²

¹⁸ Zdroj: https://www.paypal.com/cgi-bin/webscr?cmd=p/sell/mc/mc_intro-outside

¹⁹ Nelze však použít American Express Corporate Card (firemní platební kartu). Společnost American Express zakázala provádění plateb přes systém PayPal tímto druhem platební karty. Zdroj: PayPal User Agreement

²⁰ Zdroj: https://www.paypal.com/cgi-bin/webscr?cmd=_merchant-outside

²¹ Ostrov v souostroví Malé Antily v Karibském moři o rozloze cca 100 km čtverečních

²² Zdroj: https://www.paypal.com/cgi-bin/webscr?cmd=_display-approved-signup-countries-outside

4.3.1.6 Bezpečnost

PayPal používá svoji proprietární technologii a společně s eBay zaměstnávají více než 1000 specialistů v oblasti bezpečnosti, kteří monitorují systém 24 hodin denně, 7 dní v týdnu. Nicméně, ani s těmito parametry není možné zaručit stoprocentní bezpečnost, jak vyplývá z poměrně vážných stížností některých zákazníků – viz dále.

Proprietární modely rizik monitorují neobvyklé aktivity a zabraňují jejich dalšímu pokračování. Systémy vyhodnocují u každé transakce stovky proměnných a pomáhají tak určit, zda nedochází k podvodu. Avšak i tyto modely rizik přinášejí některé problémy, které jsou popsány dále.

Dále má PayPal své unikátní metody pro verifikaci bankovních účtů a samozřejmě používá velmi silné šifrování. Všechny důvěrné informace jsou šifrovány na stanici klienta a posílány na PayPal server pomocí SSL protokolu s 128-bitovým klíčem²³.

Servery, na nichž je provozován systém PayPal jsou chráněny fyzicky a elektronicky a nejsou přímo připojeny do Internetu.

Cíle v oblasti bezpečnosti jsou:

- Identifikovat potenciální slabá místa a zabránit podvodům před tím, než se vůbec stanou.
- Zjistit probíhající podvod.
- Co možná nejvíce snížit ztráty, pokud už k podvodu dojde.
- Poskytovat maximální množství informací bezpečnostním složkám na celém světě, aby se zabránilo podvodníkům v jejich činnosti.

4.3.1.7 Související služby

Přes PayPal lze zajistit také dopravu. K dispozici jsou nástroje jako například „Kalkulačka dopravy (Shipping Calculator)“, která umožňuje počítat náklady na dopravu, ať už pevnou sazbou nebo procentem z prodejní ceny, nebo připočítat prodejní daň či daň z přidané hodnoty.

PayPal spolupracuje s U.S. Postal Service a zásilkovou službou UPS. Jedna z výhod například je, že uživatel může sledovat, kde se zásilka právě nachází jednoduchým kliknutím na tlačítko u svého PayPal účtu.

4.3.1.8 Poplatky (náklady na PayPal)

Poplatky za příchozí platby se účtují u účtů Premier a Business. U osobního účtu Personal Account se poplatky neplatí, ale není možné přijímat platby uskutečněné kreditní nebo debetní kartou.

²³ SSL - Secure Socket Layer - protokol pro bezpečný přenos dat. 128-bitová délka klíče je v současné době nejvyšší úroveň komerčně dostupného zabezpečení

U většiny řešení se neplatí žádný paušální poplatek, ten je pouze u řešení Website Payments Pro. Platí se jen poplatek za transakci, který činí 30 centů plus určité procento z hodnoty převáděných peněz. Procento je tím nižší, čím vyšší je objem uskutečněných transakcí. Pro příklad je uvedena následující tabulka, která uvádí poplatky pro jednotlivá řešení. Údaje jsou platné pro nakupující ze Spojených států.

	Poplatek za transakci	Měsíční poplatek	Měsíční poplatek za virtuální terminál²⁴
Website Payments Standard	0,30 USD plus 1,9% až 2,9%	není	20 USD
Website Payments Pro	0,30 USD plus 2,2% až 2,9%	20 USD	je v ceně
Email Payments	0,30 USD plus 1,9% až 2,9%	není	20 USD
PayPal jako další způsob plateb	0,30 USD plus 1,9% až 2,9%	není	20 USD

Tabulka 4.1: Poplatky za příchozí platby v systému PayPal

Zdroj: https://www.paypal.com/cgi-bin/webscr?cmd=_profile-comparison

Přesné procento poplatků v závislosti na výši měsíčních příjmů uvádí následující tabulka.

Objem transakcí	Poplatek
0.01 USD - 3,000.00 USD	2.9%+ 0.30 USD
3,000.01 USD - 10,000.00 USD	2.5% +0.30 USD
10,000.01 USD - 100,000.00 USD	2.2% +0.30 USD
nad 100,000.00 USD	1.9% +0.30 USD

Tabulka 4.2: Přesné procento poplatků v závislosti na výši měsíčních příjmů v systému PayPal

Zdroj: https://www.paypal.com/cgi-bin/webscr?cmd=_display-receiving-fees-outside

Výše uvedené poplatky jsou konečné. Žádné další poplatky, jako například zřizovací poplatky, poplatky za ochranu proti podvodům a podobně, se již neplatí.

Pro uživatele z Evropských zemí jsou poplatky za příchozí platby trochu jiné, konkrétně je to od 0,35 EUR a 1,9% až 3,4% z převáděné částky. Stejně tak pro uživatele z Kanady a dalších zemí se poplatky liší.

²⁴ Pomocí virtuálního terminálu lze zpracovávat objednávky uskutečněné prostřednictvím telefonu, faxu, či klasické pošty.

V případě, že při transakci dochází ke konverzi z měn, je k poplatkům navíc připočítáno 2,5%.

Při výběru finančních prostředků z PayPal účtu na účet vedený u banky ve Spojených státech se žádný poplatek neplatí, při mezinárodním převodu - tedy při výběru do jiné než Americké banky se poplatek platit může a nemusí. Zda-li se poplatek platí či ne a jaká je jeho výše je odvislé od státu, ve kterém se nachází banka u které je účet veden.

Jak to, že PayPal může nabízet tak nízké poplatky?

Po přečtení předchozího textu se nabízí otázka jak je možné, že si PayPal může dovolit účtovat tak nízké poplatky? Vždyť 1,9 % je méně, než si účtují banky za transakci provedenou platební kartou.

Důvodů je více.

Předně je třeba říci, že 1,9 %, jak bylo uvedeno výše, platí pouze v případě, že celková hodnota transakcí za daný měsíc přesáhne 100,000 USD. Jinak jsou procenta vyšší – až ke 2,9 procenta ve Spojených Státech. Pro některé jiné země jsou poplatky ještě vyšší.

A dále. Fixní částka 0,30 USD je účtována **ke každé transakci**. Zejména u malých transakcí to zvyšuje průměrné procento. Pro všechny transakce do výše deseti dolarů je tedy procentuální hodnota stržené částky vyšší než u běžných transakcí provedených platební kartou. Uvažme například obchodníka, který nabízí k dispozici stahování log, melodií či obrázků do mobilních telefonů, kde průměrná částka transakce je dva dolary a který má za den méně než 50 transakcí. Ten tedy za transakci zaplatí PayPalu $0,30 + 0,029 * 2$ USD, což je necelých 36 centů, ale tato částka tvoří 17,9 procenta z hodnoty transakce!

Kromě poplatků za příchozí transakce, si PayPal účtuje 2,5 % v případě, že při transakci dochází ke konverzi měn.

Z výše uvedeného vyplývá, že **v mnoha případech se nejedná o pouhých 1,9 %**, ale o částky vyšší, v některých případech i značně vyšší než jsou poplatky za uskutečnění transakce pomocí kreditní či debetní karty.

Kromě toho je důležitý fakt, že **je zpoplatněna každá příchozí transakce** na účtech Premier a Business, tedy **včetně transakcí, které nebyly provedeny kreditní/debetní kartou**. Při platbách uskutečněných přesunem prostředků z jednoho PayPal účtu na druhý bez použití platební karty, PayPal obdrží stále svých 30 centů plus příslušné procento, ačkoli náklady na tuto transakci jsou pro PayPal téměř nulové – v podstatě se jedná pouze o změnu několika málo záznamů v interních databázích systému.

A konečně, velmi významným faktem, je že **PayPal neplatí svým uživatelům žádné úroky** z prostředků, které mají na svých účtech, **ale při tom tyto prostředky sám dále investuje**. Konkrétně jsou peníze uloženy na účtu Wells Fargo Bank a v dalších fondech řízených touto

bankou²⁵. PayPal tedy investuje prostředky třetích stran a získává z toho rozdíl na úrocích. To je činnost, která je velmi podobná činnosti bank. Není zcela jasné, jestli PayPal je bankou či ne. Podrobněji se tomuto problému věnuje následující subkapitola.

4.3.1.9 Je PayPal banka?

Rozhodnutí o tom, jestli je PayPal banka, by mělo pro PayPal dalekosáhlé dopady. Finanční instituce jsou totiž v podstatě ve všech státech značně regulovány a musí mít ke své činnosti zvláštní povolení. Navíc regulace se týká i dalších obchodních aktivit, jako například podnikání v jiných oblastech a podobně.

Kromě těchto dopadů, jsou zde i významné dopady finanční – finanční instituce, především banky, musí mít určitou minimální výši základního kapitálu, musí udržovat určité povinné minimální rezervy a další.

Tato poměrně tvrdá regulace je dána, tím, že banka operuje s cizími penězi, takže je zde značný veřejný zájem na tom, aby její podnikání nebylo podvodné nebo jinak nežádoucí.

Nicméně, o tom jestli PayPal je či není banka či finanční instituce, se stále vedou dohady, názory na toto téma se liší.

PayPal je považován za tzv. „E-Transaction Company“, tedy za instituci, která zpracovává platby uskutečněné kreditní kartou a která umožňuje podnikům a jednotlivcům posílat a přijímat platby. Nicméně to, jestli jde o finanční instituci se liší i stát od státu.

Zdá se, že existuje vysoký stupeň podobnosti mezi tím, jak funguje PayPal a tím, jak funguje banka²⁶. Direktiva 2000/12/EC týkající se kreditních institucí říká, že „kreditní instituce znamená takové podnikání, jehož předmětem je získávání vkladů a jiných vratných prostředků od veřejnosti a poskytování úvěrů svým vlastním jménem“²⁷.

Na základě této definice se zdá, že PayPal se chová jako instituce přijímající vklady a měla být proto považována za banku, zejména kvůli různým regulacím. Naproti tomu však PayPal argumentuje, že nepoužívá prostředky uložené na účtech svých uživatelů. Ve smlouvě s uživatelem („User Agreement“) se říká, že „PayPal bude vždy udržovat vaše prostředky oddělené od svých firemních prostředků, nepoužije vaše prostředky na své provozní účely ani jiné firemní účely a nezpřístupní dobrovolně tyto prostředky svým věřitelům v případě krachu ani pro jiné účely“²⁸.

Podle tohoto odstavce PayPal tedy nepoužívá prostředky svých uživatelů. Jak již bylo zmíněno, tak

²⁵ Zdroj: Grossman, W. “Online payment systems: Easy money?” The Independent, September 9, 2002.

²⁶ Prezentace Andrése Guadamuze Gonzáleze z University of Edinburgh s názvem “PayPal and eBay: The legal implications of the C2C electronic commerce model”, uvedená na osmnácté konferenci BILETA: Controlling Information in the Online Environment z dubna 2003 v QMW v Londýně.

²⁷ Direktiva 2000/12/EC Evropské parlamentu a Evropské Rady z 20. března 2000 týkající se podnikání kreditních institucí, OJ L 126/1 2000, článek 1.

²⁸ Zdroj: PayPal User Agreement

je investuje místo svých uživatelů, ale sám je přímo nepoužívá. Tímto se tedy vyhýbá tomu, že by byl jednoznačně označen za finanční instituci.

Například Grossman²⁹ souhlasí s tím, že PayPal není finanční instituce, protože peníze, které přijdou na účet nejsou vloženy majitelem účtu, ale třetí stranou a dále, že PayPal tyto peníze dále nepůjčuje. Domnívám se, že tyto důvody nejsou úplně správné. Prostředky totiž nemusí být vždy vloženy na účet třetí stranou, může je tam vložit i sám majitel účtu. A argument o půjčování peněz také není zcela přesvědčivý, neboť PayPal dává peníze na účet banky, čímž ji v podstatě poskytuje půjčku.

Ve Spojených státech Federal Deposit Insurance Corporation (FDIC) též nepovažuje PayPal za banku³⁰ podle příslušné legislativy USA, ač některé důvody jsou poněkud zvláštní. Jedním z nich například je to, že PayPal není bankou, protože nemá bankovní licenci. Ale zde se pochopitelně nabízí otázka, jestli fakt, že PayPal nemá licenci lze automaticky vykládat jako skutečnost, že není bankou.

Těžko říci, jak by se na tuto záležitost dívala česká legislativa, nicméně PayPal by zřejmě bez bankovní licence v České republice podnikat nemohl, a to hlavně kvůli zákonu č. 124/2002 Sb. - více o tomto zákoně viz kapitola o mikroplatebních systémech.

Zajímavá je také úvaha, jak by vypadala situace v oblasti elektronických platebních systémů, kdyby se PayPal bankou stal. V takovém případě by zřejmě PayPal začal vydávat svoje platební karty anebo by se domluvil na určité formě spolupráce s již zavedenou společností působící v oblasti kreditních/debetních karet. V každém případě by však tato skutečnost měla značný dopad na oblast platebních karet obecně (ne jen na Internetové platby), neboť PayPal by se pravděpodobně stal velmi významným subjektem na tomto trhu. Pokud by ke každému PayPal účtu byla vydána platební karta, PayPal by se rázem stal třetím největším subjektem³¹ na poli debetních/kreditních karet a vzhledem ke svému rozšíření a konkurenceschopné výši poplatků za transakce by se patrně stal významnou konkurencí pro stávající hráče na trhu platebních karet.

4.3.1.10 Výhody PayPalu

Lze identifikovat následující výhody PayPalu:

- **Rychlost** – systém operuje v reálném čase, po stržení prostředků z účtu kupujícího (odesílatele), se tyto okamžitě objeví na účtu prodávajícího (příjemce).
- **Flexibilita** – systém akceptuje všechny rozšířené platební karty (VISA, EuroCard/MasterCard, Discover, American Express).
- **Globální dosah** – systém je dostupný v 56 zemí.

²⁹ Grossman, W. "Online payment systems: Easy money?" v The Independent, 9. září 2002

³⁰ Wolverton, T., "PayPal not a bank", CNet News, 12. března 2002.

³¹ Viz též obrázek v subkapitole „Budoucnost PayPalu“

- **Platby v různých měnách** – USD, Euro, Libra, Kanadský dolar, Yen, Australský dolar
- **Důvěrnost** – PayPal se zavazuje, že „... číslo kreditní karty, bankovního účtu či další finanční údaje nebudou NIKDY poskytnuty nikomu...“³². Nikomu se myslí druhá strana v transakcích uskutečněných v systému PayPal. Tento závazek neplatí v případě, že majitel účtu dá k poskytnutí takových informací výslovný souhlas anebo jestliže je poskytnutí těchto informací určitým subjektů vyžadováno zákonem.
- **Jednoduchost** – zřízení systému není spojeno z žádným poplatkem, pro používání systému stačí mít emailovou adresu a zaregistrovat se na stránkách PayPal.
- **Efektivnost** – Transakce jsou prováděny elektronicky, nepoužívá se žádných finančně náročných kanálů a náklady na transakci (myšleno pro PayPal!) nejsou závislé na objemu přesouvaných prostředků.
- **Důvěra zákazníků** – podle mnohých průzkumů³³ je PayPal nejdůvěryhodnějším platebním systémem svého typu na Internetu.
- **Uživatelská přívětivost** – Stránky systému PayPal jsou uživatelsky přívětivé (user friendly) a jejich použití je jednoduché.

4.3.1.11 Problémy PayPalu

Vzhledem ke globálnímu rozsahu nelze očekávat, že takovýto systém nebude mít své problémy. PayPal je má a některé z nich i poměrně vážné. Zde jsou ty nejzávažnější z nich, plný výčet patrně není možný.

- **Centralizovaný systém** – Společnost PayPal má kontrolu nad všemi účty a transakcemi. Díky tomu je pro uživatele složitější domáhat se svých práv v případě, že PayPal rozhodl v jejich neprospěch, neboť PayPal je autoritou poslední instance³⁴.
- **Zřeknutí se práv** – akceptování podmínek PayPalu znamená pro uživatele v podstatě zřeknutí se standardních práv na ochranu spotřebitele týkajících se transakcí provedených platební kartou.
- **Bezpečnostní chyby** – ačkoli PayPal tvrdí, že systém je bezpečný a je chráněn proti zneužití, v minulosti se objevily případy zneužití systému, kde jedna ze stran byla poškozena nekorektním chováním druhé strany. Zde jsou některé příklady.
 - Při platbě byla použita ukradená kreditní karta. Jelikož ověření karty provádí PayPal, tak v případě, že PayPal vyhodnotil transakci špatně (nechal „projít“ ukradenou kreditní

³² PayPal User Agreement, 2005

³³ Například podle průzkumu společností Gartner Inc., zdroj: <http://www.paypal.com/html/gartner-020102.html>

³⁴ Jak například uvádí Abrashevich, D. v Classification and Characteristics of Electronic Payment Systems, Technical University of Eindhoven, na straně 55.

kartu), tak prodávající utrpěl finanční újmu – nedostal zapláceno za poskytnuté služby/zboží.

- Prodávající úmyslně poslal kupujícímu prázdný balík a vybral veškerý zůstatek ze svého PayPal účtu. Následkem tohoto jednání utrpěl kupující finanční újmu, neboť poslal peníze, ale zboží nedostal.
- Problém se softwarem detekujícím podvod. Tento software automaticky zablokuje dotýčný účet pro výběr zůstatku, ale dále přijímá platby. Některé účty zůstaly takto zablokovány i několik měsíců.
- Jedno z pravděpodobně nejpromyšlenějších zneužití systému ukazuje následující scénář. Podvodník (prodávající) něco prodá kupujícímu, ale nic nepošle. Na základě toho kupující podá reklamaci typu „zboží nedoručeno“ („non-receipt“). Když podvodník zjistí, že byla podána reklamáce typu „zboží nedoručeno“, tak pošle kupujícímu prázdný balík. Při doručení balíku, podepíše kupující jeho převzetí, ale to ještě netuší, že je balík prázdný. Podvodník poskytne PayPalu číslo zásilky (prázdného balíku), načež PayPal prohlásí, že případ je uzavřen. To se samozřejmě kupujícímu nelíbí, ale PayPal řekne, že má důkaz, že zboží bylo doručeno. Jedinou možností, která kupujícímu zbývá, je podat reklamaci typu „zboží neodpovídá uvedenému popisu“ (not as described), načež ovšem PayPal řekne, že vzhledem k tomu, že před tím byla podána reklamáce typu „zboží nedoručeno“, tak není možné změnit typ reklamáce na „zboží neodpovídá uvedenému popisu“. Takto kupující utrpěl újmu tím, že zaplatil, ale nedostal zboží.

4.3.1.12 Právní kroky proti PayPalu

Vzhledem k výše uvedeným problémům bylo podáno na společnost PayPal několik žalob, především v USA. Jako příklad lze uvést žalobu podanou 20. února 2002 u Kalifornského nejvyššího soudu právní firmou Jacoby&Meyers. Žaloba obviňuje PayPal z přílišného „protekcionismu“ při omezování a správě uživatelských účtů³⁵. V žalobě se říká, že PayPal používá agresivní a příliš rozsáhlou politiku na odhalování podvodů, která způsobuje chybné zablokování uživatelských účtů a že společnost úmyslně zatajuje před uživateli informace týkající se zákaznických služeb a omezení účtů³⁶. Jedenáctého června 2004 se strany dohodly, že PayPal zaplatí 9,25 miliónů dolarů. Nicméně, tímto krokem PayPal nepřiznal žádné pochybení ze své strany.

³⁵ Případ číslo 02 1227 JF PVT, District Court for the Northern District of California v San Jose ve Spojených státech amerických.

³⁶ Jak uvádí http://www.aboutpaypal.org/paypal_lawsuit

Podobné žaloby byly podány též u Federálního soudu města San Fransisco a u Nejvyššího soudu státu New York³⁷.

V březnu 2004 bylo dokončeno šetření kanceláře Nejvyššího státního zástupce státu New York, z jehož závěrů plyne, že text smlouvy z uživatelem („User Agreement“) zkrsluje některé podmínky. Na základě dohody, společnost PayPal souhlasila, že text změní tak, aby podmínky byly uživatelům jasné a srozumitelné, a že zaplatí náklady na vyšetřování a pokutu v celkové výši 150 000 USD.

4.3.1.13 PayPal a VeriSign



Společnosti eBay (mateřská společnost PayPalu) a VeriSign oznámily 10. října 2005 strategickou alianci, podle které by tyto společnosti měly spolupracovat v oblasti platebních systémů a bezpečnosti e-commerce. Podle uzavřené smlouvy získá PayPal platební bránu VeriSign. VeriSign dále poskytne nástroje a služby týkající se zabezpečení plateb.

Důvodem pro uzavření této aliance ze strany PayPalu je získání platební brány VeriSign, která zpracovává platby v celkové hodnotě přesahující 40 miliard amerických dolarů, čímž zvýší svojí zákaznickou základnu o desítky tisíc MSP (malých a středních podniků).

Další součástí aliance je dohoda uzavřená na několik let, kde se eBay zavazuje, že bude investovat do vývoje technologií VeriSign, které umožňují a zabezpečují on-line platební transakce. Dle vyjádření Jeffa Jordana, presidenta společnosti PayPal, „platební brána společnosti VeriSign je oblíbený a trhem prověřený produkt, který dokonale doplňuje existující služby, které nabízí PayPal.“

Za platební bránu zaplatí PayPal okolo 370 miliónů amerických dolarů, splatných v hotovosti nebo v akciích společnosti eBay. V kombinaci se službami, které PayPal nabízí obchodníkům, by brána měla za rok vygenerovat dodatečných 100 miliónů USD zisku.

Akvizice je ještě předmětem různých regulačních a jiných schvalování a předpokládá se, že bude uzavřena někdy na konci roku 2005³⁸.

4.3.1.14 Budoucnost PayPalu

Podle viceprezidenta a ředitele výzkumu Gartner Financial Services, Avivaha Litana „díky své naprosto jednoznačně vedoucí marketingové pozici se PayPal velmi pravděpodobně stane dlouho očekávaným standardem pro nákupy na Internetu, obzvláště pro obchody s nižšími částkami. Podpora zákazníků a poptávka po alternativě ke kreditním kartám může vést Internetové

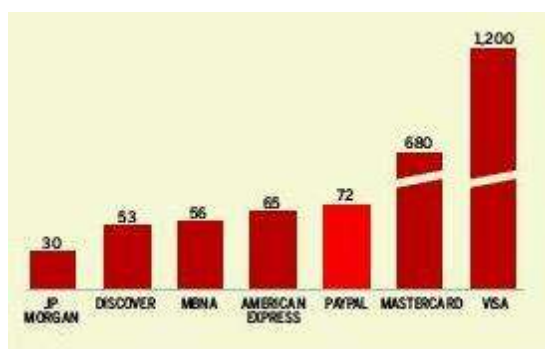
³⁷ Zdroj: Akron Beacon Journal ze dne 7. dubna 2005

³⁸ Zdroj: http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_035983.html

obchodníky k tomu, že budou přijímat platby prostřednictvím PayPalu, ačkoli náklady na něj jsou srovnatelné s náklady na transakce uskutečněné kreditními kartami.“

Zdá se tedy, že PayPal bude i nadále dominantním hráčem na trhu on-line plateb. Lze očekávat, že počet jeho uživatelů, které v současnosti roste tempem 20 000 nových uživatelů denně, poroste i nadále, zejména mezi uživateli eBay a malými a středními podniky. S rostoucím počtem uživatelů se může snadno stát, že velcí Internetoví prodejci budou donuceni nabízet platbu přes PayPal jako alternativu ke klasickým platbám uskutečněným kreditní či debetní kartou.

Analytici dále spekulují, že v nedaleké budoucnosti se můžeme dočkat platební karty PayPal, která bude vydávána ve spolupráci s bankou GE (General Electric). Podle analytika firmy Legg Mason Wood Walker Inc. Scotta N. Devitta „má PayPal dostatečné možnosti na to, aby v budoucnu konkuroval sektoru kreditních karet³⁹“.



Obrázek 4.4: Počet účtů jednotlivých poskytovatelů finančních služeb (v milionech)

Zdroj: článek "PayPal spreads its wings" od Roberta D. Hofa, BusinessWeek, květen 2005

Nicméně, jak tvrdí analytici společnosti Gartner Inc., před tím, než se PayPal stane celosvětovým leaderem, bude muset vybojovat mnoho sporů se státními orgány, které regulují finanční sektor, právě kvůli tomu, že služby, které PayPal poskytuje jsou velmi podobné těm, které poskytují banky. Například v USA již čtyři státy, včetně Kalifornie a New Yorku, zvažují regulaci PayPalu, možná právě i na základě stížností některých obchodníků. Podle analytiků společnosti Gartner Inc. se PayPal ve finále stane bankou, což zajistí lepší ochranu jak zákazníků, tak obchodníků. Nicméně, bude se jednat o banku, které bude zajišťovat hlavně Internetové platby.

³⁹ Zdroj: článek "PayPal spreads its wings" od Roberta D. Hofa uveřejněném v časopise BusinessWeek v květnu 2005

4.3.1.15 PayPal a Česká republika

Bohužel, v současné době je v České republice systém PayPal dostupný pouze pro posílání plateb. Lze odhadovat, že českými uživateli bude patrně používán pro placení za zboží na aukčním serveru eBay. Na jiných serverech již méně, neboť na těch je pro českého uživatele nemajícího zřízený PayPal účet patrně jednoduší platba kreditní/debetní kartou.

Čeští obchodníci tedy možnost přijímání plateb přes PayPal v současné době nemají a budoucí vývoj není jistý. Vyjádření⁴⁰ společnosti PayPal ohledně dostupnosti systému PayPal pro příjem plateb v České republice je následující: "... stále na tom pracujeme. Na druhé straně, zřízení naší služby v každé nové zemi či regionu zahrnuje komplexní změny kvůli jiným právním předpisům. Doufáme, že budeme rozšiřovat naši dostupnost, nicméně, kvůli složitostem spojeným s globálním rozšiřováním, nemůžeme poskytnout časový rozvrh..."

Zde je třeba podotknout, že PayPal při rozšiřování může narazit na právní problémy, zejména na takové, jaké postihly mikroplatební systémy (viz kapitolu o mikroplatebních systémech). S tímto také právě souvisí, jestli je PayPal banka nebo ne.

4.3.1.16 Zhodnocení

PayPal je největším platebním systémem svého druhu. V 56 zemích, kde působí, má kolem osmdesáti miliónů účtů, což ho řadí na třetí příčku mezi finančními institucemi.

Jeho obchodní model založený na existující infrastruktuře se jeví jako správný, nicméně je potřeba upozornit, že implementace úplně dokonalá není. Byly zmíněny určité problémy spojené mimo jiné i s bezpečností systému, z nichž některé vyústily až v soudní pře.

Systém nabízí různé druhy účtů od těch jednodušších pro fyzické osoby až po ty, jež dokáží uspokojit potřeby velmi náročných obchodníků, umožňující platbu v několika světových měnách a nabízející další doplňkové služby. A to vše za velmi rozumné poplatky, které jsou v některých případech již od 1,9 procenta.

Jednou z velkých otázek, které nebyly dosud uspokojivě zodpovězeny, zůstává, jestli je PayPal finanční instituce, případně přímo banka či nikoliv. Názory na tuto problematiku se liší a jsou též ovlivněny legislativou příslušného státu či země. Lze očekávat, že tato otázka bude v budoucnosti ještě častokrát řešena, a výsledek, který z jejího řešení vzejde, bude mít pro PayPal nemalé následky.

Jako hlavní přednosti PayPalu lze identifikovat rychlost, flexibilitu, globální dosah, důvěrnost, jednoduchost pro uživatele, efektivnost, důvěru zákazníků a další.

Naproti tomu, mezi problémy PayPalu se řadí to, že se jedná o centralizovaný systém, kde

⁴⁰ Podle emailové komunikace ze dne 7. října 2005

společnost má kontrolu nad všemi účty a transakcemi, což znesnadňuje uživatelům vymáhání jejich práv; to, že akceptováním podmínek PayPalu se uživatelé zřikají některých svých zákonných práv; a bohužel i to, že systém má některé bezpečnostní chyby.

Posledním vývojem týkajícím se platebního systému PayPal je uzavření strategické aliance mezi vlastníkem PayPalu, společností eBay Inc., a společností VeriSign (jež je patrně nejvíce známa jako certifikační autorita). PayPal by měl díky této transakci získat desítky tisíc dalších uživatelů z řad malých a středních podniků.

Co se týká použití PayPalu v České republice, tak uživatelům je v současnosti k dispozici pouze možnost posílání plateb. Nicméně, PayPal se chce rozšiřovat dále a můžeme tedy doufat, že časem se třeba dostane i do ČR. Avšak je třeba nebýt přehnaně optimističtí, neboť obzvláště zde může PayPal narazit na značné problémy s legislativou, která upravuje platební systémy u nás.

Do budoucna lze předpokládat, že systém se bude dále rozšiřovat a že bude získávat další a další uživatele, jak ve stávajících teritoriích, tak i na nových trzích, a snadno se může stát konkurentem pro stávající poskytovatele platebních karet.

Osobně se domnívám, že PayPal je dobrý systém, což konec konců prokázal i svou životaschopností, a že obzvláště po vyřešení některých svých problémů má reálnou šanci stát se de facto standardem v oblasti elektronických platebních systémů v oblasti Internetového obchodování.

4.3.2 Platební systémy fungující na principu převodu z bankovního účtu

4.3.2.1 Platební systém eBanky



První bankou v České republice, která nabídla službu, jež umožňuje snadné placení na Internetu, byla právě eBanka (dříve Expandia banka). Nevýhodou systému je, že klient i obchodník musí mít u eBanky účet, což je pro většinu zákazníků limitující faktor. Obchodník by si kvůli možnosti přijímat on-line platby patrně účet u eBanky zřídil, ale u zákazníků už je to méně pravděpodobné. Nicméně i přes toto omezení využívá nyní platební systém eBanky více než 600 Internetových obchodů.

Výhody pro obchodníky

Jelikož zavedení systému nevyžaduje instalaci zvláštního hardware ani software, celá procedura je relativně rychlá a hlavně finančně nenáročná.

Bezpečnost systému je garantována eBankou, což je samozřejmě pro obchodníky výhodné, navíc dodává celému systému kredibilitu. Jestliže klient i obchodník bance věří natolik, že jí svěří vedení svého bankovního účtu, tak není důvod, aby nedůvěřovali on-line platebnímu systému. Jelikož transakce probíhají on-line, tak obchodník poskytuje zboží či službu až po zaplacení a nemusí se tedy obávat nesolidního jednání ze strany zákazníka.

Jako další výhody lze uvést to, že obchodník obdrží zaplacení ještě před dodáním služby či produktu, což je určitě ekonomicky výhodné. Navíc nabízení systému eBanky jako platební možnosti s sebou nese i propagaci na stránkách eBanky, což, hlavně v začátcích, může obchodníkovi pomoci s marketingem.

Výhody pro zákazníky

Pro zákazníka je zřejmě nejdůležitější fakt, že systém je garantován eBankou a v případě jakýchkoli nesrovnalostí může vše řešit pouze se svojí bankou, která možnou nesrovnalost může dále řešit s obchodníkem, neboť ten je jejím klientem také.

Vzhledem k tomu, že transakce probíhá on-line, tak zákazník může svůj nákup produktu či služby uskutečnit až na poslední chvíli. Například zdravotní pojištění do zahraničí při nákupu přes systém eBanky je platné okamžitě a klient tak může odcestovat ihned a s platnou pojistkou.

Tím, že obchodník musí mít také účet u eBanky, je zaručena jeho určitá kredibilita. Zajímavé také je, že platební brána je dostupná nejen přes Internet, ale i přes WAP.

Jak systém funguje

Systém eBanky komunikuje se serverem obchodníka pomocí URL odkazů.

Nejdříve je v systému obchodníka vytvořena objednávka, včetně všech případných přírůžek, poplatků, daní a podobně. Následně je zákazník přesměrován na platební bránu eBanky. Údaje potřebné pro platbu, jako například identifikace obchodníka, jsou předávány pomocí parametrů v URL odkazu.

Platby, které byly prostřednictvím systému provedeny, lze prohlížet na serveru eBanky. Platby lze kontrolovat nejen manuálně (pracovníkem obchodníka), ale může k nim přistupovat automaticky i systém obchodníka.

Zřízení systému

Jak již bylo řečeno, nezbytnou podmínkou je, aby měl obchodník u eBanky veden svůj firemní účet. Kromě toho je však potřeba podepsat s eBankou smlouvu o poskytování platebního systému eBanky, což lze učinit pouze osobně, tedy ne přes Internet. Vyplnění objednávky lze sice učinit na Internetu, ale na základě objednávky bude teprve do tří dnů sjednána schůzka, kde budou projednány další podrobnosti.

Náklady na systém

Jak již bylo naznačeno, díky poměrně snadné implementaci nejsou pořizovací náklady na systém příliš vysoké. Obchodník musí nicméně zaplatit zřizovací poplatek eBance. Ten je stanovován individuálně, obvykle se pohybuje okolo 2 000 Kč, což je částka docela přijatelná. Dále se platí poplatek z každé transakce, který činí cca 1%. To se domnívám je pro naprostou většinu obchodníků bez problémů přijatelné. Žádný další poplatek za příchozí transakce na firemní účet klienta se už neplatí.

Co nabídne eBanka do budoucna

Podle vyjádření⁴¹ Pavly Plaché z klientského servisu eBanky se v současné době připravuje spuštění služby e-commerce acquiringu – tedy možnosti přijímání platebních karet na Internetu. Bohužel, ve chvíli psaní tohoto textu eBanka nemohla poskytnout podrobnější informace.

Zhodnocení

Ačkoli skutečnost, že pro využívání tohoto systému je nutné, aby zákazník i obchodník měli účet u eBanky, se může jevit jako poměrně problematická, domnívám se, že může být v některých

⁴¹ Podle emailové komunikace ze dne 6. října 2005

ohledech pro všechny zúčastněné strany přínosem. Pro obchodníka proto, že od klientů eBanky lze očekávat vyšší ochotu k Internetovým nákupům a obchodník by jim měl proto vyjít vstříc. Náklady na zavedení i provozování systému jsou relativně nízké, což je dalším argumentem pro jeho zavedení. Pro zákazníka je největší výhodou snadnost použití systémů a jeho kredibilita.

Na základě výše uvedeného si myslím, že by možnost placení eBankou neměla v elektronickém obchodě chybět.

4.3.2.2 Platební brána NetBanka Živnostenské banky

Platební bránou NetBanka mohou platit ve vybraných Internetových obchodech všichni klienti Živnostenské banky, kteří mají aktivovanou službu NetBanka. Obchodník mít účet u Živnostenské banky nemusí.



Systém funguje v podstatě na principu převodu z bankovního účtu zákazníka vedeného u Živnostenské banky. Poté, co si zákazník vybere platební metodu NetBanka, je přesměrován do NetBanky (rozhraní na serveru Živnostenské banky), kde se z pochopitelných bezpečnostních důvodů musí přihlásit do systému. Zákazník vybere z jakého ze svých účtů (pokud jich má u Živnostenské banky více) chce zaplatit a odešle platební příkaz.

Výhody pro obchodníky

Způsob zřízení této platební možnosti je pro obchodníky nenáročný – stačí se zaregistrovat, a podepsat souhlas s podmínkami, na základě čehož obdrží obchodník popis, jak provést implementaci platebního systému NetBanka do svého systému. Poté se již pouze ověří funkčnost platební brány a systém je připraven k využívání.

Vzhledem k výše uvedené nenáročnosti implementace a také faktu, že Živnostenská banka tuto službu poskytuje zdarma, se jedná o poměrně snadný způsob, jak nalákat klienty Živnostenské banky na služby či produkty poskytované obchodníkem. Navíc seznam Internetových obchodů, ve kterých lze NetBankou platit, je k dispozici na webových stránkách Živnostenské banky a obchodníkovi se tedy dostane i určitého způsobu propagace.

Zhodnocení

Tento systém je samozřejmě výhodný pro zákazníky Živnostenské banky, neboť jim umožňuje poměrně snadný a bezpečný způsob placení na Internetu a nepotřebují k tomu ani platební karty ani žádné další náležitosti. Na druhou stranu, počet obchodů, ve kterých lze NetBankou platit, není

nijak výrazně rozšířený. Jedná se o 24 obchodů, jejich přesný výčet lze najít na stránkách NetBanky⁴².

Pro obchodníky je na tomto systému zřejmě nejzajímavější fakt, že mohou přilákat zákazníky Živnostenské banky bez toho, aby si oni sami u ní zřizovali účet. Ovšem z celkového hlediska není výhodnost implementace tohoto systému zřejmá a domnívám se, že Internetový obchod se bez ní obejde. Lze o ní uvažovat jako o doplňkovém způsobu placení, nikoli však nějak zásadním.

⁴² Konkrétně na http://www2.zivnobanka.cz/cs/netbanka/platebni_brana.html

4.3.3 Systémy fungující na principu platebních karet

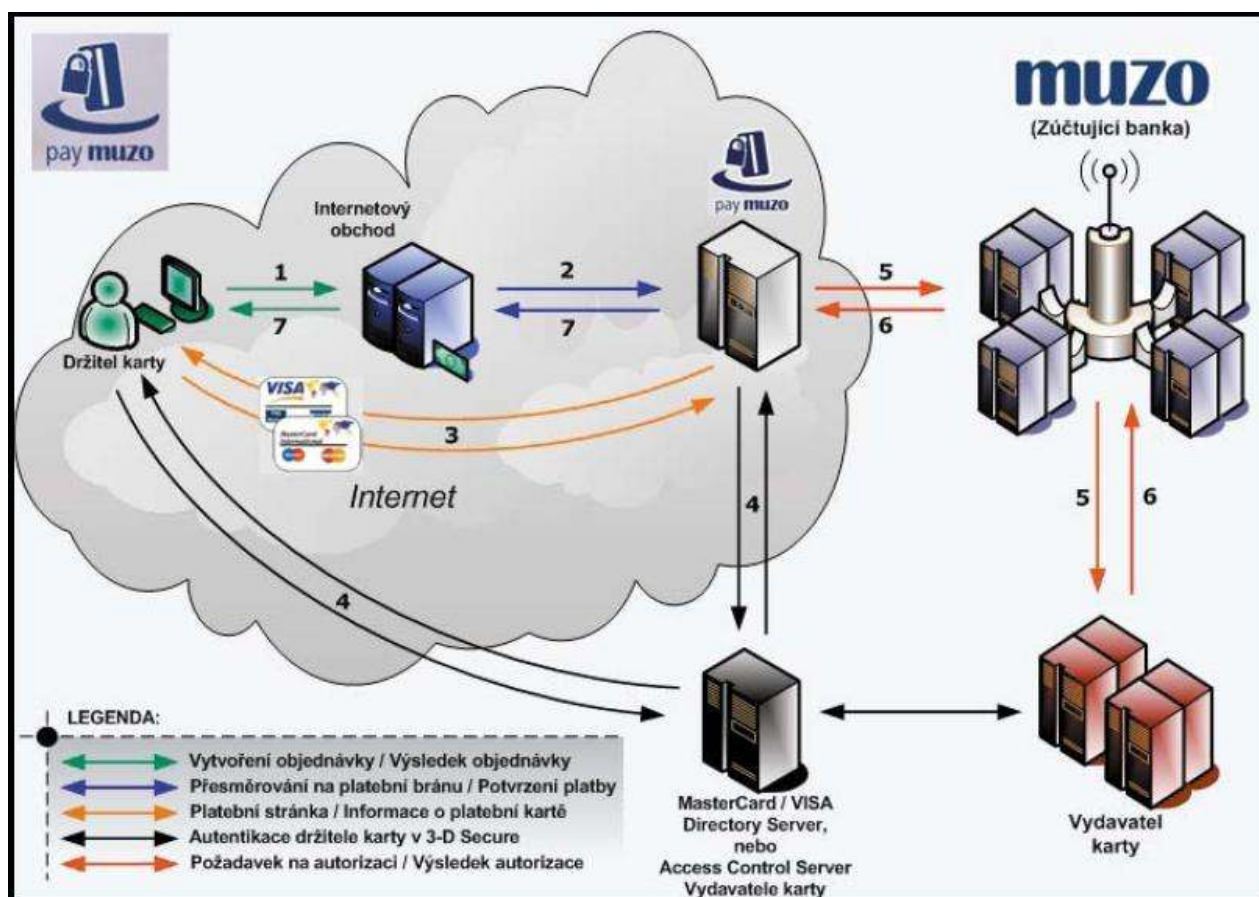
4.3.3.1 Pay MUZO

Pay MUZO je on-line platební brána společnosti Global Payments Europe⁴³. Pomocí tohoto systému mohou obchodníci na Internetu přijímat platební karty EuroCard/MasterCard, Maestro, VISA a VISA Electron. Zabezpečení komunikace probíhá podle standardu 3-D Secure (viz kapitola o bezpečnosti). Dále se pro vyšší bezpečnost využívá digitálního podpisu všech dat.



Jak systém funguje

Schéma fungování ukazuje následující obrázek.



Obrázek 4.5: Schéma fungování Pay MUZO

Zdroj: http://www.muzo.com/download/gp_paymuzo.pdf

⁴³ Společnost Global Payments Europe (dříve MUZO, a.s.) je dceřinou společností Global Payments Inc.

- 1 - Zákazník nakupuje v Internetovém obchodě a vybere jako způsob platby platební kartu.
- 2 - Systém obchodníka předá požadavek (ten obsahuje všechny potřebné údaje kromě informací o platební kartě) na provedení platby systému Pay MUZO. Tento požadavek je digitálně podepsán soukromým klíčem obchodníka, aby byla zajištěna integrita dat a nepopiratelnost požadavku od obchodníka.
- 3 - Zákazníkovi je zobrazena platební stránka systému Pay MUZO určená k vyplnění údajů o platební kartě (číslo, datum expirace a podobně). Zákazník tyto údaje vyplní a potvrdí požadavek k provedení platby.
- 4 - Systém Pay MUZO provede autentifikaci zákazníka v rámci standardu 3-D Secure. Pokud výsledek autentifikace povoluje pokračovat v procesu platby, Pay MUZO zašle požadavek na autorizaci objednávky na ACS (Access Control Server) vydavatele karty. V případě, že výsledek autentifikace nepovoluje pokračovat, proces platby je zastaven.
- 5 - Požadavek na autorizaci objednávky je prostřednictvím zúčtovací banky předán mezibankovními sítěmi vydavateli karty.
- 6 - Vydavatel karty provede autorizaci a její výsledek předá zpět systému Pay MUZO.
- 7 - Systém Pay MUZO doručí výsledek platby (ten je opět digitálně podepsán soukromým klíčem společnosti Global Payments Europe, aby bylo možné garantovat integritu dat) zpět do Internetového obchodu, který výsledek transakce zobrazí zákazníkovi.

Ve všech případech je vyžadováno zabezpečené spojení mezi zákazníkem a obchodníkem a mezi obchodníkem a aplikací Pay MUZO. Obchodník na svůj server musí nainstalovat SSL serverový certifikát, který umožňuje 128-bitové šifrování. Samozřejmě prohlížeč zákazníka musí 128-bitové šifrování podporovat také. Doporučuje se, aby zákazníci byli o této skutečnosti informováni na stránkách Internetového obchodu.

Na straně obchodníka není zapotřebí žádného speciálního systému pro Internetový obchod. Komunikace s platební bránou probíhá podle jasně definovaných pravidel, která jsou nezávislá na technologii, kterou obchodník používá pro svůj Internetový obchod⁴⁴.

Poplatky

Platí se zřizovací poplatek společnosti Global Payments Europe, který činí 8 000 Kč. Dále je této společnosti nutné platit roční poplatek ve výši 600 Kč a poplatek za autorizaci každé transakce,

⁴⁴Podle emailové komunikace s Lenkou Žákovou a Zuzanou Štěpánovou z útvaru péče o zákazníky Komerční Banky a informací uvedených na stránkách společnosti Global Payments Inc.

který činí 2 Kč. Kromě těchto dvou korun ještě obchodník zaplatí provizi pro zúčtovací banku ve výši dvou až pěti procent.

Partnerské banky

Patrně nejznámější je v současné době spolupráce s Komerční bankou. Jestliže má obchodník účet veden u Komerční banky, musí zajít na pobočku Komerční banky, kde sepíše smlouvu o akceptaci platebních karet. Poté bude kontaktován společností Global Payments Europe, se kterou též musí vstoupit do smluvního vztahu. Komerční banka vyžaduje provizi za každou provedenou transakci ve výši cca tři až pět procent.

Vedle Komerční banky nabízí platbu přes systém Pay MUZO i Československá obchodní banka (ČSOB), která službu nazývá ČSOB E-commerce – Internetová akceptace platebních karet. Funkčnost je stejná, obchodník musí mít u banky účet a musí s ní uzavřít smlouvu o akceptaci platebních karet. Přijímat lze platby kreditními/debetními kartami VISA a EC/MC. Poplatek za zřízení služby činí 13 200,- Kč, dále se platí měsíční poplatek ve výši 150,- Kč a z každé transakce si banka ještě strhne 2,5 až 3,5 procenta.

Podle vyjádření společnosti Global Payments Europe, společnost umožňuje spolupráci se všemi českými bankami, vyjma České spořitelny, která si služby Internetových plateb zajišťuje sama (viz dále).

Výhody pro obchodníky

Jedná se o systém, který umožňuje akceptaci debetních a kreditních karet na Internetu „se vším všudy“. Vzhledem k tomu, že v dnešní době má nějakou platební kartu téměř každý, tak spektrum potenciálních zákazníků je značné. Jedná se o „profesionální“ systém, který umožňuje přijímání plateb nejen od českých, ale i od zahraničních zákazníků a vzhledem k využití technologie 3-D Secure je i dostatečně kredibilní.

Výhody pro zákazníky

Systém umožňuje platbu komukoli, kdo vlastní klasickou plastovou nebo virtuální platební kartu, která není zablokována pro Internetové transakce. Pro zákazníka je platba kartou jednoduchá, nevyžaduje žádné zvláštní úkony kromě zadání potřebných údajů a nevyžaduje od zákazníka žádné další poplatky.

Zhodnocení

Technicky se jedná o dobrý, bezpečný a věrohodný systém, který nabízí obchodníkům příležitost přijímat platby od každého, kdo je držitelem příslušné kreditní/debetní karty, což je v současné době téměř každý. Pro zákazníky je velmi příjemná jednoduchost provedení platby, která není spojena s dodatečnými náklady nebo úkony. Nevýhodou systému je však to, že jsou zde poměrně vysoké náklady a to nejen investiční, ale co je horší, i provozní. Obchodníci tedy stojí před volbou, zda se jim nabízení takového systému vyplatí. Zvýšené náklady je sice možné promítnout do cen výrobků či služeb, na to ovšem budou nepříznivě reagovat zákazníci.

Obecně lze akceptaci platebních karet doporučit, nicméně stojí za zvážení, zda raději neuzavřít smlouvu s Českou spořitelnou, která si za v podstatě stejné služby účtuje mnohem nižší poplatky. Více o nabídce Internetových plateb od České spořitelny viz další subkapitola.

4.3.3.2 Platby kartou na Internetu od České spořitelny



O systému

Česká spořitelna nabízí placení kartou na Internetu pomocí standardu 3-D Secure. Oproti například Komerční bance nevyužívá služeb systému Pay MUZO (viz výše) ani jiného dalšího prostředníka, službu nabízí pomocí vlastní implementace.

Přesné fungování systému 3-D Secure je podrobně popsáno v kapitole o bezpečnosti a není tedy rozebráno zde. Co se týče konkrétní aplikace u České spořitelny, tak obchodník musí uzavřít smlouvu s Českou spořitelnou, načež dostane dokument, který poskytuje informace o tom, jaké technické zásahy jsou potřeba učinit v systému obchodníka. Po provedení těchto úprav se otestuje funkčnost systému a poté systém funguje již běžně.

Česká spořitelna umožňuje, aby zákazníci platili všemi druhy karet vydávaných společnostmi Visa a EuroCard/MasterCard. To znamená, že jsou akceptovány nejen klasické embosované karty EC/MC a VISA a virtuální platební karty těchto společností, ale také neembosované platební karty Maestro a VISA Electron.

Poplatky

Velkou výhodou nabídky České spořitelny je, že si neúčtuje **žádný poplatek za zavedení systému ani žádné další měsíční či roční paušální poplatky**. Jedinými poplatky jsou poplatky za transakce, které se ovšem platí i při transakci uskutečněné v kamenném obchodě. Poplatek za transakce nelze jednoznačně určit, neboť je domlouván s každým obchodníkem individuálně. Lze však předpokládat, že se pohybuje okolo 2,5%.

Výhody a zhodnocení systému

Výhody pro obchodníky i zákazníky jsou v podstatě stejné jako u systému Pay MUZO (viz výše). Nicméně, je tu pro všechny zúčastněné jeden zásadní rozdíl, kterým jsou náklady. Fakt, že neexistují náklady na zřízení a že další poplatky jsou „velmi rozumné“ dává tomuto systému značnou konkurenční výhodu.

Vzhledem k těmto faktům, se platby kartou na Internetu od České spořitelny jeví, alespoň v současné době, jako **nejlepší řešení mezi platebními systémy, které je na českém trhu dostupné.**

4.4 Shrnutí a závěry

V této kapitole byly popsány, zanalyzovány a zhodnoceny nejvýznamnější platební systémy dostupné v České republice, konkrétně systém eBanka, NetBanka, Pay MUZO a systém České spořitelny. Kromě těchto, řekněme domácích, systémů se kapitola extenzivně věnovala i systému PayPal, což je největší hráč na poli platebních systémů a který umožňuje srovnání s platebními systémy běžně dostupnými v ČR. U výše zmíněných systémů byla popsána jejich funkčnost, analyzovány silné a slabé stránky a rozebrány další související problémy.

Předmětem zkoumání zatím nebyly mobilní platby a mikroplatby, kterým se věnují až následující kapitoly.

U systému PayPal byly rozebrány některé jeho specifické problémy, které mimo jiné souvisí s tím, že se jedná o tak rozšířený systém. Analytici se většinou shodují v tom, že se z něj stane de facto standard v oblasti Internetových plateb a že bude značnou konkurencí pro tradiční poskytovatele kreditních/debetních karet.

Z řešení rozšířených na domácím trhu vyšly nejlépe patrně Internetové platby od České spořitelny, která nabízí velmi kvalitní systém používající technologie 3-D Secure a to za podstatně nižší poplatky, než musí platit obchodníci využívající služeb systému Pay MUZO. Na českém Internetu má stále své místo platební systém eBanky, ač bohužel jeho vázanost na jedinou banku je pravděpodobně největší překážkou jeho dalšího rozšiřování.

Kromě platebních systémů, u nichž je ověření platby součástí nákupního procesu, byly zmíněny i některé platební systémy, u nichž ověření platby součástí nákupního procesu není, jako například platba na dobírku a podobně, které jsou v současné době na českém Internetu stále ještě velmi rozšířené.

5 Mikroplatební systémy

5.1 Vymezení pojmu mikroplatební systémy

Pro účely této kapitoly budeme mít mikroplatebním systémem na mysli systém, který je nějakým způsobem provozován pouze na Internetu - nikoli prostřednictvím mobilních telefonů. O mobilních platbách bude pojednáno v následující kapitole.

5.2 Cíle kapitoly

Cílem této kapitoly je definovat, co je to mikroplatební systém, k čemu se používá nebo k čemu by se používat mohl a popsat a analyzovat mikroplatební systémy dostupné na českém Internetu. Tedy ty systémy, které mohou nabízet čeští obchodníci a které mohou být využívány českými zákazníky. Samozřejmě, součástí analýzy je prozkoumat nejen možnosti a výhody mikroplatebních systémů, ale také jejich záporné stránky a problémy, které jsou spojené s jejich provozem v ČR, a to nejen problémy související s technickou či obchodní stránkou věci, ale též problémy týkající se současné legislativy. V souvislosti s legislativou bude naznačeno, zda existují způsoby, jak ji obejít. Následující text může být přínosem nejen pro obchodníky a zákazníky, ale i pro provozovatele mikroplatebních systémů, respektive pro subjekty, které by měly zájem poskytovat mikroplatební systém (tak, jak je definován pro potřeby této kapitoly).

5.3 Co jsou mikroplatební systémy

Pomocí mikroplateb nebo-li mikroplatebních systémů se provádějí finanční operace s nízkými částkami. Konkrétně se jedná o částky v řádu korun až maximálně stovek korun. Evropská Unie definuje mikroplatby jako platbu do 15 EUR⁴⁵ (necelých 500 Kč).

Mikroplatby se začaly rozšiřovat až se vzrůstajícím využitím Internetu, neboť dříve nebylo potřeba platby a mikroplatby rozlišovat. Pokud bychom chtěli najít analogii v „klasickém“ (tedy ne on-line) nakupování, mohli bychom například uvažovat spotřebitele, který chce platit v maximální možné míře platební kartou. Ač ve většině případů je to možné, u velmi malých částek se zřejmě pořád vyplatí používat hotovost, neboť při nákupu novin či rohlíku proběhne transakce jednak rychleji, jednak použití platební karty by mohlo nákup výrazně prodražit - ač totiž obchodníci obvykle nezakazují použití platebních karet pro malé částky a ani tyto transakce nijak odlišně

⁴⁵ Zdroj: <http://www.lupa.cz/clanky/mikroplatby-vraceji-uder/>

nezpoplatňují, tak většina bank si účtuje několikakorunové částky typu „poplatek za položky“ a podobně.

5.4 K čemu mohou sloužit mikroplatby a proč je potřebujeme

Mohlo by se zdát, že by se pro platby malých částek daly používat standardní elektronické platební systémy a že není potřeba rozlišovat tyto standardní systémy od mikroplateb. Za určitých podmínek by tomu tak být mohlo, ale tyto podmínky nejsou v naprosto drtivé většině případů splnitelné. Ač to na první pohled vypadá, že náklady na transakci jsou stejné bez ohledu na převáděnou částku, není to tak úplně pravda.

Je tomu tak proto, že čím větší částky jsou převáděny, tím větší zabezpečení je potřeba. Nesnažím se tím říci, že mikroplatby by neměly být zabezpečené, to vůbec ne, ale přeci jen je rozdíl, jestli je díky případnému zneužití systému zpronevěřeno několik desítek nebo nanejvýš stovek korun, anebo jestli se jedná o částky statisícové nebo i vyšší. S tím souvisí i psychologický fakt - jestliže se jedná o nižší částky, lidé nejsou tolik omezeni nedůvěrou v elektronické platební systémy. Výhody těchto systémů tak převáží nad strachem z možné škody a lidé jsou ochotnější mikroplatby uskutečnit. Díky tomu i strana, která je příjemcem platby (například obchodník), musí vynaložit nižší úsilí a tím i nižší náklady na zabezpečení systému.

A jestliže bychom připustili, že náklady na transakci jsou ve všech případech (tedy bez ohledu na výši převáděné částky) stejné, tak tyto náklady jsou stejné pouze v absolutních hodnotách - relativně k výši částky nikoli, což platby malých částek znevýhodňuje.

Nabízí se otázka, zda není možné platbu malých částek řešit prostě platbou kreditní/debetní kartou, vždyť poplatek z transakce je někdy pouze procentuální a tedy náklady na provedení platby by byly velmi malé. Problém ovšem spočívá v tom, že většina bank si účtuje tzv. „poplatky za položky“, což je poplatek, který si banka naúčtuje za každou položku, která je na bankovním výpisu uvedena, tedy i za platbu kreditní/debetní kartou. Kvůli těmto poplatkům za položky by placení velmi malých částek platební kartou vyšlo dosti draho.

K čemu nám jsou tedy mikroplatby dobré?

Existují služby, které by bez mikroplateb vůbec neexistovaly a to prostě proto, že pokud by nebylo možné za ně platit, tak by je nikdo nenabízel.

Dále jsou zde služby, které vzhledem k tomu, že za ně nelze platit, jsou zdarma. To je sice obvykle pro uživatele výhodné, ale je třeba si uvědomit, že jestliže se za služby neplatí, tak taková služba bude ztrátová. A jestliže je nějaká služba ztrátová, tak se velmi snadno může stát, že úroveň takové služby bude klesat nebo služba úplně zmizí. A to už pro uživatele výhodné není. (Výjimkou jsou

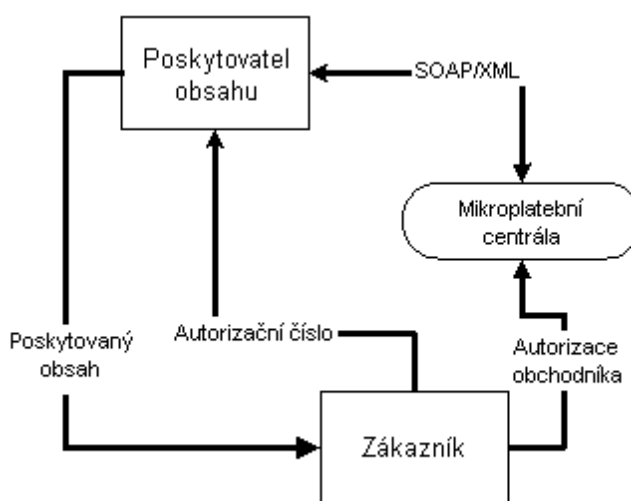
služby, jejichž cílem není jejich vlastní ziskovost, ale slouží pro „nalákání“ zákazníka na služby související).

Dalším přínosem mikroplateb může být zvýšení uživatelské přívětivosti. Na službách, které nelze zpoplatnit, se totiž poskytovatelé často snaží vydělávat tak, že současně se službou je dodávána „masivní“ reklama, která uživatele obvykle obtěžuje, v některých případech i odrazuje - například u tzv. „Bundled software“, kdy současně s užitečným programem se nainstaluje i nějaký reklamní software, který buďto uživatele obtěžuje nebo v horším případě sbírá citlivé informace o systému, o chování uživatele na Internetu a podobně. V případě, že existují mikroplatby, tak služba je zaplacená přímo a poskytovatel není závislý pouze na příjmu z reklamy. Nebo je možné nechat uživatele vybrat - buďto musí povinně shlížet reklamu nebo si zaplatí a službu/produkt má bez reklamy.

Typickými příklady, kde se dají velmi dobře využít mikroplatby je přístup do placených sekcí serverů, předplatné časopisů, platba za nějakou informaci, dary či příspěvky, drobný software a podobně.

Zajímavé může být i využití mikroplateb pro marketingové účely. Server může například dávat čtenářům malé částky za návštěvu určitých stránek, účast v anketě a tím si budovat čtenářskou základnu. Ta mu na oplátku umožní požadovat vyšší cenu za reklamu.

Možné schéma fungování mikroplatby při poskytování on-line obsahu ukazuje obrázek. Zákazník vloží do mikroplatební centrály (systému) číslo (identifikaci) obchodníka poskytujícího obsah a uvede jaké částky a jakým způsobem si ze zákaznickova účtu může obchodník strhávat. Na základě vyplnění těchto údajů obdrží zákazník autorizační číslo, které poskytne obchodníkovi. Obchodník (respektive systém obchodníka) se potom připojí do mikroplatební centrály pomocí SOAP/XML komunikace šifrované pomocí SSL (například pomocí protokolu SOAP-over-SSL) a uvede autorizační číslo (které mu poskytl zákazník) a částku, kterou chce z účtu zákazníka strhnout. Mikroplatební centrála potvrdí převod prostředků, na základě čehož obchodník poskytne zákazníkovi požadovaný obsah.



Obrázek 5.1: Schéma fungování mikroplatby při poskytování on-line obsahu

Zdroj:

<http://www.yafla.com/~dforbes/micropay/graphics/micro2.gif>

5.5 Možné problémy mikroplatebních systémů

Tak zcela největším problémem pro mikroplatební systémy (Internetové, ne mobilní) je zákon č. 124/2002 Sb., ale na tuto problematiku se zaměříme až v další subkapitole.

Jinak další problémy mikroplateb jsou podobné jako u běžných elektronických platebních systémů - tedy bezpečnost a důvěra, se kterou souvisí počet uživatelů systému.

Jak již bylo naznačeno výše, nabízí se otázka, zda mikroplatby jsou zabezpečené stejně dobře jako jiné elektronické platební systémy. Bylo již řečeno, že potřeba maximální bezpečnosti zde není až tak palčivá jako při platbách větších částek. Samozřejmě stále je potřeba odpovídajícího zabezpečení, které samozřejmě něco stojí.

Důvěra je problém, který také zřejmě není tak vážný jako u jiných elektronických platebních systémů jednoduše z toho důvodu, že možné finanční ztráty z těchto transakcí nejsou až tak velké. Na druhou stranu, pokud jsou od uživatele vyžadovány nějaké osobní informace, problémy s důvěrou zde být mohou, a to hlavně problémy typu - kam se dostanou moje osobní informace, kdo všechno se dozví za co jsem na Internetu platil a podobně. Existuje totiž mnoho uživatelů, kteří si nepřejí, aby takové informace byly dostupné komukoli. Nejmarkantnější je tento přístup zřejmě u použití mikroplatebních systémů pro přístup do placených sekcí některých serverů. Pro mnoho uživatelů může být v takových případech anonymita přímo zásadní.

5.6 Dopad zákona č. 124/2002 Sb. na mikroplatební systémy v ČR

Zákon č. 124/2002 Sb., O převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (Zákon o platebním styku), který nabyl účinnosti dne 1. ledna 2003, v §19 odst. 1 říká:



„Jiné osoby než banky, pobočky zahraničních bank a osoby k tomu oprávněné na základě jednotné bankovní licence podle zvláštního právního předpisu smějí vydávat elektronické peněžní prostředky jen po předchozím souhlasu České národní banky za těchto podmínek:

a) elektronický peněžní prostředek vydaný držiteli uchovává elektronické peníze v hodnotě nejvýše 4 500 Kč a současně celková částka závazků vydavatele vyplývající z nevypořádaných částek vydaných elektronických peněz nepřesáhne v žádném okamžiku částku 150 000 000 Kč,

b) elektronické peněžní prostředky jsou přijímány pouze omezeným počtem poskytovatelů služeb, kteří jsou ve vztahu k vydavateli osobou ovládanou, osobou ovládající nebo osobou ovládanou stejnou osobou jako vydavatel, nebo kteří jsou s vydavatelem spojeni finančním či obchodním vztahem, kterým je zejména společný postup při získávání odbytišť (marketing) nebo společná distribuční síť.“

Tento paragraf je pro většinu mikroplatebních systémů fatální, protože **bez licence České národní banky (ČNB) se mikroplatební systém provozovat nesmí**⁴⁶. Díky tomuto zákonu systémy jako DirectPay firmy Computer MCL či zřejmě nejznámější mikroplatební systém v České republice I like Q firmy Villusion přestaly fungovat. Naproti tomu systém Monetka firmy Computer Press výše uvedený zákon nezničil. Snad by se i dalo říci, že mu určitým způsobem pomohl - zničil totiž konkurenci. Samozřejmě k omezení došlo i pro systém Monetka - zmiňovaný zákon definuje v odst. 1 písmene b) paragrafu 19, že subjekty, které licenci dostanou, musí omezit elektronickou peněženku klientů limitem 4 500 Kč, což ovšem, co se týče vyloženě mikroplateb, není až takový problém.

Více o systému Monetka je popsáno v následující subkapitole.

5.7 Systém Monetka

Jak již bylo řečeno, systém Monetka je jediný systém (nepočítaje v to systémy využívající mobilních plateb), který „přežil“ zákon č. 124/2002 Sb. a to díky tomu, že s provozovatelem tohoto systému je vlastnický svázána firma poskytující Internetové obchody a dokáže tedy splnit podmínku uvedenou v odstavci 1 písmene b) §19 tohoto zákona a může jí být udělena výjimka od ČNB.



5.7.1 O systému

Naplnění peněženky probíhá pomocí bankovního převodu na účet provozovatele systému a maximální objem prostředků je 4 500 Kč (jak vyplývá z výše uváděného zákona).

Obchod probíhá standardně - zákazník si vybere zboží do nákupního košíku, vybere způsob platby Monetka a zaplatí. Zajímavou možností je storno objednávky v případě, že požadovaná obchodní transakce není uskutečněna do stanoveného termínu. V takovém případě se peníze ihned uvolní a jsou uživateli k dispozici.

Jelikož veškeré transakce probíhají v reálném čase, tak je vždy k dispozici aktuální zůstatek.

Co se týče sekce pro obchodníky, tak zde je určitá nevýhoda. Aby mohl například Internetový obchod přijímat platby prostřednictvím systému Monetka, vyplní formulář na Internetových stránkách Monetka.cz, na jehož základě je potom v průběhu několika pracovních dní kontaktován. Zřízení Monetky jako platební možnosti pro obchodníky není on-line a nějakou dobu trvá.

⁴⁶ Pokud provozovatel systému nevymyslí způsob, kterým se omezujícím podmínkám vyhnout – viz dále.

Bohužel, systémem Monetka se dá v současné době platit pouze na několika málo stránkách, přesněji řečeno v e-shopech provozovaných firmou Internet shops. Konkrétně se jedná o obchody Vltava.cz, Vltava2000.cz, Hyperlink.cz, CPbooks.cz a CPmedia.cz.

5.7.2 Zabezpečení

Veškerá komunikace mezi klientem a serverem je zabezpečena 128-bitovým šifrováním a data jsou přenášena pomocí protokolu SSL. Certifikát serveru Monetka.cz byl vydán certifikační autoritou VeriSign.

Samozřejmostí je dobrá heslová politika a spolehlivé zabezpečení serverů - opírá se o bezpečnostní technologie firmy Microsoft na platformě MS Windows 2003 Server.

5.7.3 Náklady

Zřízení a veškeré operace jsou zdarma, jediným nákladem, který musí zákazníci hradit, je poplatek za výběr peněz z elektronické peněženky, který činí 50 Kč. Samozřejmě, že 50,- Kč za výběr peněz není úplně málo, ale na druhou stranu, většina zákazníků bude systém používat proto, aby pomocí něho mohla platit za produkty a lze tedy očekávat, že výběry peněz zákazníky systému nebudou nijak časté.

Náklady pro obchodníky nelze v tomto případě určit, neboť jelikož obchodník musí být nějakým způsobem obchodně svázán s provozovatelem systému, tak náklady pro obchodníka budou zřejmě předmětem individuální dohody mezi obchodníkem a provozovatelem systému.

5.7.4 Zhodnocení

Co se týče zhodnocení pro obchodníky, tak to nelze v tomto případě aplikovat, neboť nabízet systém Monetka jako jednu z možností platby mohou pouze subjekty (obchody), které jsou nějakým způsobem majetkově či obchodně svázány s provozovatelem systému, tedy s firmou Internet shops. Pro zákazníky rozhodování také není složité, záleží na tom, zda nakupují ve výše uvedených obchodech, které systém nabízejí. Jestliže ano, obzvlášť pokud nakupují pravidelně, tak se používání Monetky patrně vyplatí. Pro jiné účely nelze Monetku použít.

5.8 Systém i-plus

5.8.1 Co je systém i-plus a jak funguje

Systém i-plus⁴⁷ nabízí v České republice společnost Paynet, která přišla jako první s pokusem obnovit mikroplatební systémy na českém Internetu po tom, kdy všechny předcházející systémy byly zastaveny či výrazně omezeny s příchodem zákona č. 124/2002 Sb., o němž je pojednáno výše.

Systém funguje tak, že poté, co se uživatel do systému zaregistruje, si dobíjí kredit podobně jako u mobilních telefonů (u předplacených služeb). Na prodejním místě si zakoupí kartu i-plus v hodnotě 400 Kč, setře stírací plochu, kde najde aktivační kód pomocí něhož si dobije kredit. Potom už může na Internetu platit.



Náklady pro zákazníky při platbě pomocí tohoto systému nevznikají, platí cenu, kterou požaduje obchodník, žádné další poplatky či přírážky zákazník neplatí.

Konkrétní výše nákladů pro obchodníky se nepodařilo zjistit, je závislá na individuální dohodě mezi obchodníkem a společností PayNet jakožto poskytovatelem systému.

Tato metoda – použití předplacených karet – je zajímavá v tom, že **zákazníkům umožňuje anonymní platby**, což pro mnoho uživatelů může být značným přínosem. Samozřejmě má všechny další výhody mikroplatebních systémů. Je však třeba zmínit, že vzhledem k tomu, že je nutné zakoupit kupon na prodejních místech, tak systém není „kompletně on-line“.

Nevýhodou však je, že ač byl systém spuštěn přibližně v polovině roku 2004, tak v současné době je málo míst, kde se dá tímto způsobem platit. Konkrétně je to platba za inzeráty v Annonci, přístup na dva „18+“ servery a server smobil.cz, kde si uživatelé mohou objednat loga, melodie a podobně do mobilních telefonů. Nerozšířenost tohoto systému je docela škoda, protože podle informací poskytnutých společností Paynet je systém ve světě značně rozšířený – například ve Francii ho používá čtvrtina populace, tedy 15 miliónů lidí.

Co se zabezpečení týče, tak je klasicky používán protokol SSL se 128-bitových šifrováním. SSL serverový certifikát byl vydán certifikační autoritou VeriSign, což lze považovat za dostatečnou záruku.

⁴⁷ Tento systém může být někdy označován také jako Gem-eCash, neboť společnost Paynet má na jeho provozování v České republice jen výhradní licenci a provozuje ho pod názvem i-plus. Systém Gem-eCash byl vyvinut společnostmi Gemplus International a Valista.

5.8.2 Jaký je vliv zákona č. 124/2002 Sb. na tento systém

Samozřejmě se nabízí otázka, jak je možné, že systém i-plus není ohrožen zákonem č. 124/2002 Sb. Řešení je poměrně chytré. **Zákazník totiž nenakupuje přímo u obchodníka.** Zákazník si přes systém i-plus v podstatě zboží či službu **jen objedná a koupí u obchodníka uskuteční společnost PayNet**, již také obchodník transakci fakturuje. Společnost Paynet pak příslušnou částku strhne z kreditu zákazníka. Stržení z kreditu tedy znamená platbu společnosti Paynet, ne obchodníkovi.

Tímto způsobem lze tedy obejít současnou legislativu, která měla tak zásadní vliv na činnost, lépe řečeno na znemožnění činnosti, mikroplatebních systémů. Zdá se, že s tímto modelem fungování mikroplatebních systémů by neměly být spojeny legislativní problémy, alespoň pokud nedojde k opětovné změně právních předpisů. Obdobný model používají i mobilní platby, o nichž je pojednáno v následující kapitole.

5.8.3 Zhodnocení

Domnívám se, že se jedná o velmi zajímavou myšlenku, která překonává problémy vyvolané zákonem č. 124/2002 Sb. Bohužel, vzhledem k tomu, že v České republice se na rozdíl od jiných zemí nepodařilo systém rozšířit, tak nelze říci, že by v současné době bylo jeho zavedení krokem, který by přinesl nějakou konkurenční výhodu. Nezbyvá než doufat, že s postupem času se systém rozšíří a mikroplatby na českém Internetu například tímto způsobem znovu ožijí.

5.9 Shrnutí a závěry

V této kapitole jsme definovali, že mikroplatební systém (jímž v této kapitole rozumíme nemobilní mikroplatební systém) je systém, kterým se provádějí finanční transakce dosahující malých částek, maximálně 15 EUR (tak, jak mikroplatby chápe EU). Dále byly zmíněny možnosti využití mikroplateb, k nimž patří například platby za zpřístupnění některého obsahu webového serveru, platba za konkrétní informace, platby za menší software a podobně, a jejich výhody, mezi než patří mimo jiné nižší náklady a s tím související fakt, že bez mikroplateb by bylo obtížné, či přímo nemožné, tyto služby poskytovat.

Kromě možností a výhod mikroplatebních systémů byly též rozebrány problémy, které s nimi souvisejí, a to především problém v současné době patrně nejpálčivější, kterým je legislativa, respektive zákon č. 124/2002 Sb, který zničil některé mikroplatební systémy. U systémů, které fungují i po zavedení tohoto zákona, bylo řečeno, proč je tento systém nezničil (systém Monetka, který se splňuje požadavky §19 zákona č. 124/2002 Sb.) nebo jakým způsobem jej obešli (systém i-plus, který se vyhýbá ustanovení §19 písm. b) zákona č. 124/2002 Sb.).

Závěrem je třeba říci, že v současné době není situace v České republice na poli mikroplatebních systémů nijak růžová. Zákazníkům se nenabízí příliš míst, kde mikroplatbami platit, obchodníci také nemají příliš šancí zavést systém, který by byl dostatečně rozšířený a poskytovatelé či případní zájemci o poskytování těchto systémů nemají zřejmě mnoho možností, jak svůj systém prosadit u Internetové populace.

6 Mobilní platby

6.1 Cíle kapitoly

V této kapitole se zaměříme na mobilní platby, tedy též na mikroplatby uskutečněné pomocí mobilních telefonů. Cílem je podat přehled o fungování mobilních plateb v České republice, jakým způsobem jsou zabezpečeny, jak jsou integrovány do elektronického obchodování, co nabízejí jednotliví mobilní operátoři v této oblasti, jaké jsou společné iniciativy týkající se mobilních plateb a co lze očekávat do budoucna. Budou zmíněny nejen přímo m-platby, ale krátce také další možné způsoby, jak platit pomocí mobilního telefonu.

Následující text se zaměří nejen na popis fungování, ale také na možnosti a výhody mobilních plateb, jejich možné problémy a omezení, případně možné překážky, které bude v případě většího rozšíření mobilních plateb nutné odstranit. Přínosem bude hlavně pro zákazníky, jimž může v souvislosti s m-platbami pomoci s volbou mobilního operátora, a pro obchodníky, jimž podá informace o tom, jestli se jim mobilní platby vyplatí vůbec zavést, případně jakého operátora by si měli vybrat za partnera.

6.2 Úvod

Jak již bylo naznačeno v předchozí kapitole, mobilní platby mají v současné době velký potenciál. Důvody pro to jsou zjevné. Mobilní telefon má dnes téměř každý a má ho po ruce v podstatě dvacet čtyři hodin denně. Navíc často ani není potřeba aktivovat nějakou speciální službu, mobilní telefon je na mobilní platby již připraven. Využití mobilních telefonů se předpokládá obvykle u částek desítek až stovek korun. Samozřejmě mobilním telefonem lze platit i částky větší, ale u nákupů za vyšší částky už je obvykle k dispozici možnost platby kreditní/debetní kartou nebo jiným způsobem. Pro mikroplatby v řádu desetníků mobilní telefony příliš vhodné nejsou, protože náklady na transakci by značně přesahovaly hodnotu transakce. Naproti tomu, mikroplatby v hodnotách korun už je možné provádět pomocí mobilních telefonů relativně snadno - transakce se sice i tak dost prodraží, ale tyto náklady jsou ve většině případů únosné. Z toho vyplývá, že zákon, který v podstatě zničil nemobilní mikroplatby (viz předchozí kapitola), m-platbám pomohl v tom smyslu, že zničil konkurenci. V současné době, pokud se hovoří o mikroplatbách, tak se často mají na mysli právě mobilní platby. Co se týče mikroplateb uskutečněných mobilním zařízením (telefonem), tak je výše zmiňovaný Zákon č. 124/2002 Sb. neomezuje ze stejného důvodu, jako je tomu u systému i-plus (viz výše).

6.3 Mechanismus fungování mobilních plateb

Existují v podstatě dva mechanismy fungování mobilních plateb. Prvním je m-platba, kde mobilní telefon funguje jako osobní platební terminál, druhým je „nestandardně“ zpoplatněná služba – buďto SMS zpráva, obvykle označovaná jako Premium SMS, nebo případně telefonát.

6.3.1 M-platba

Systém funguje tak, že zákazník si vybere službu či zboží na stránkách obchodníka a vybere m-platbu jako způsob platby.

Obchodník, tedy lépe řečeno systém na straně obchodníka, odešle požadavek na transakci na platební bránu mobilního operátora. Obratem je do systému obchodníka odesláno potvrzení o přijetí požadavku.

Zákazník je od obchodníka přesměrován na platební bránu mobilního operátora, kde se uživatel autentizuje a potvrdí platbu. Po úspěšné autentizaci a potvrzení platby je zákazník přesměrován zpět na stránky obchodníka a transakce se zaúčtuje v interních systémech mobilního operátora.

Systém obchodníka poté pošle dotaz, zda-li byla transakce úspěšně zaúčtována a jestliže ano, tak obdrží kladnou odpověď.

Zákazníkovi je následně zaslána potvrzovací SMS. Zákazníkovi je platba buďto připočítána k jeho měsíčnímu vyúčtování (u tarifních zákazníků) nebo stržena z jeho kreditu (u zákazníků využívajících služby předplacených karet).

6.3.2 Premium SMS

Tento způsob platby je založen na tom, že zákazník odešle krátkou textovou zprávu ve speciálním formátu (se speciálním textem) na speciální číslo. Tato SMS je zpoplatněna jinak (více) než běžná SMS a část peněz jde příjemci této zprávy.

Za zmínku ještě stojí, že existuje tzv. DMS, neboli dárcovská SMS, která funguje na stejném principu, ale velká část její ceny (obvykle minimálně 90%) jde na dobročinné účely.

6.3.3 Speciální telefonní čísla

V této souvislosti je třeba ještě zmínit, že kromě dvou výše uvedených způsobů, by se mezi způsoby platby mobilním telefonem ještě dalo zařadit volání na nestandardně zpoplatněná telefonní čísla. Tato možnost tu samozřejmě je, využívá se ovšem k platbám zřídka, obvykle jen ke stažení loga či vyzváněcí melodie a podobně.

Samozřejmě tato forma placení za služby není vázána čistě na mobilní telefon, lze ji využít u všech telefonních přístrojů, tedy i u pevných linek.

6.4 Možnosti, výhody a omezení mobilních plateb

6.4.1 Možnosti

Tak samozřejmě možnosti mobilních plateb jsou značné. To je dáno rostoucím trhem obchodování a podnikání na Internetu, stále zvyšující se poptávkou po elektronických platbách jak ze strany uživatelů, tak ze strany obchodníků, faktem, že mobilní telefon má dnes už každý atd..

V současné době se mobilní platby jeví jako ideální nástupce mikroplateb. Tedy pro zpřístupnění určitého obsahu na Internetu, platby za poskytnutou informaci, platby za software stažený z Internetu ať již do počítače či do mobilního telefonu apod.

Původně mobilní platby začínaly v podobě Premium SMS a to zejména pro stahování log, obrázků či vyzváněcích melodií do mobilních telefonů. Dále např. společnost T-Mobile začala instalovat automaty na nealkoholické nápoje, kde si bylo možné koupit Coca-Colu či jiný nealkoholický nápoj tím, že zákazník zavolal na nestandardně zpoplatněné telefonní číslo, na základě čehož mu byl automatem vydán nápoj.

Nicméně, mobilní platby lze využít pro platbu v podstatě čehokoli. Samozřejmě, že největší výhodou je to tam, kde klasické způsoby platby (hotovost, či platební karta) nejsou dostupné. Takto lze využívat mobilní platby k veškerým nákupům na Internetu, jako například knih, CD, filmů a podobně.

Využití k nákupu v prodejních automatech se také jeví jako dobrý způsob, neboť právě u automatů je často problém, že zákazník musí mít mince, což je opět další nepříjemnost, kterou musí řešit. Mobilní platby se tedy jeví jako ideální, neboť jediným požadavkem je mít u sebe mobilní telefon (což má dnes téměř každý) a v případě, že uživatel využívá předplacených služeb, tak dostatečnou výši kreditu.

6.4.2 Výhody

Velkou výhodou je, že platební síť je již vybudovaná. Mobilní telefon vlastní drtivá většina (penetrace SIM karet přesáhla na konci roku 2004 úroveň 100 procent⁴⁸) obyvatel České republiky a zvláště u zákazníků, u kterých je velká pravděpodobnost elektronické či mobilní platby (mladí lidé, lidé již běžně platící na Internetu apod.), dosahuje penetrace mobilních telefonů velmi vysoké úrovně.

Další výhodou je, že lidé mají obvykle v mobilní telefony důvěru, věří svému mobilnímu operátorovi a problémy s důvěrou v elektronické platební systémy se tak snižují. Je to dáno tím, že platební transakce je uskutečněna mezi zákazníkem a mobilním operátorem (který je až dále proplácí obchodníkovi)⁴⁹, takže zákazník se nemusí ani starat o důvěryhodnost obchodníka. Který byl stejně prověřen mobilním operátorem, což mu dodává určitou kredibilitu. A vzhledem k tomu, že mobilní operátoři jsou velké mezinárodní společnosti, tak jejich důvěryhodnost je už sama o sobě vysoká.

Co se týče koncového zařízení, tedy mobilního telefonu, tak je to zařízení, které má schopnosti poměrně slušného výpočetního výkonu a tedy mu nečiní problém šifrování a jiné zabezpečovací algoritmy. Navíc, jak se ukázalo u GSM bankingu, je to ideální způsob přihlašování - pomocí mobilního telefonu a na něj zasláné SMS je možné vygenerovat jednorázových kód pro přihlášení ke službě. Mobilní telefon má tedy v sobě v podstatě již zabudované autentizační zařízení a naučit se s ním pracovat není pro majitele mobilního telefonu nijak složité. A veškeré aplikace, které nějakým způsobem pracují se zabezpečenými daty, jsou v mobilním telefonu přístupné až po zadání hesla či PIN kódu, takže ani v případě ztráty či odcizení telefonu není možné zneužití m-plateb. Pro platby pomocí Premium SMS je samozřejmě situace jiná, k jejímu odeslání stačí držení telefonu, ale na druhou stranu, maximální částka za jednu Premium SMS se pohybuje v desítkách korun a v případě jejího zneužití nedojde tedy k vyšší újmě než v případě použití odcizeného mobilního telefonu k hovorům do zahraničí či na speciálně zpoplatněná telefonní čísla.

6.4.3 Omezení

Tak samozřejmě základním předpokladem pro využití mobilních plateb je vlastnictví mobilního telefonu. Nicméně, jak již bylo uvedeno, v tomto není příliš velký problém, protože penetrace mobilních telefonů je v tomto ohledu v České republice velmi dobrá.

⁴⁸ Jak uvádí http://www.telecom.cz/infocentrum/tiskove_centrum/tiskove_zpravy/clanek.php?tz=21032005_1

⁴⁹ To je právě způsob, který používá například také systém i-plus a který umožňuje platbu i přes to, že legislativa jinak takovým platebním systémům příliš nepřeje (viz předchozí kapitola).

Za omezení by se dalo též považovat, že ne všichni mobilní operátoři mají partnerských vztah se stejnými obchodníky. Naopak, v současné době má nejrozšířenější síť zřejmě T-Mobile, EuroTel a Oskar/Vodafone v podstatě nejsou významnými hráči. Nicméně, i když lze předpokládat v budoucnu rozšíření, pořád zde bude fakt, že mobilní platby budou navázány na mobilní operátory a tím pádem zákazník bude závislý na tom, jaká společnost je jeho poskytovatelem mobilních služeb. Že by si někdo pořídil SIM kartu ještě dalších dvou operátorů jen pro to, aby mohl platit pomocí mobilních plateb, není příliš pravděpodobné. To by však neplatilo, pokud by se operátoři shodli na jednotném postupu, v což lze doufat – viz dále Asociace pro mobilní platby.

U plateb pomocí mobilního telefonu se nabízí i otázka, jak velké nákupy lze jejich prostřednictvím provádět. Například m-platba od společnosti T-Mobile je limitována částkou 700,- Kč. Nicméně pro mnoho transakcí je taková částka dostatečná. Pokud bychom požadovali částky vyšší, je otázkou, jak jsou reálné celkově. Pro tarifní zákazníky to až takový problém není, ale zákazníci s předplacenou kartou obvykle nemají tak vysoký zůstatek kreditu.

Problémem může být i fakt, že u předplacených karet je transakce v podstatě anonymní. Na jednu stranu to může být pro zákazníka výhodou, ale na druhou stranu pro určité úkony může být zákonem požadována určitá věková hranice. A vzhledem k tomu, že předplacených služeb často využívají děti či mladiství, zvláště u větších částek by mohlo docházet k právním problémům typu, že mobilní operátor umožnil transakci, ačkoli uživatel k jejímu uskutečnění nebyl způsobilý.

S větším rozšířením mobilních plateb je potom také potřeba myslet na to, aby si zákazníci mohli kontrolovat výpisy z účtu okamžitě, ne čekat až na „papírové“ vyúčtování od operátora, které chodí jednou za měsíc.

Dále je potřeba zvýšit případné limity pro tarifní zákazníky. Někteří operátoři v případě, že celkový účet překročí určitou částku, zablokují používání mobilního telefonu. To je pro uživatele samozřejmě naprosto nepřijatelná situace, kterou budou muset mobilní operátoři nějakým způsobem řešit. U předplacených služeb je potřeba zajistit snadné dobíjení kreditu, neboť jedna platba za několik lístků do kina snadno může zbývající kredit uživatele vyčerpat. Nutno však říci, že možnosti dobíjení kreditu jsou již velmi dobré a tato záležitost by tedy neměla činit větší potíže.

6.5 Zabezpečení m-plateb

Jelikož protokol WAP (Wireless Application Protocol) není zabezpečený a protokol SSL, běžně používaný při Internetové komunikaci nebylo možné pro komunikaci s mobilním telefonem využít, byl vyvinut protokol WTLS (Wireless Transport Layer Security).

Zprávy zasílané protokolem WTLS jsou funkčně stejné jako zprávy zasílané v protokolu SSL, ale

vzhledem k tomu, že mobilní linky mají nižší propustnost, tak cílem je, aby objem přenášených dat byl nižší. Komunikace mezi WAP bránou a webovým serverem již probíhá na protokolu SSL.

Na straně klienta (tedy v mobilním telefonu) je tzv. WIM (Wireless Identity Module), který provádí bezpečnostní funkce na aplikační úrovni protokolu WAP. Veškeré citlivé údaje (klíče) jsou uloženy v modulu WIM, který může být integrován v SIM kartě, na samostatné kartě nebo může být implementován softwarově.

6.6 Integrace mobilních plateb do elektronického obchodování

Řešení této problematiky je nasnadě. V případě nákupu v Internetovém obchodě si zákazník jako způsob platby vybere jednoduše platbu prostřednictvím mobilního telefonu, ať už m-platbu nebo zřejmě méně častou možnost Premium SMS a pak již transakce probíhá podobným způsobem jako u jiných platebních systémů. U m-platby je zákazník nejdříve přesměrován od obchodníka k platební bráně mobilního operátora, kde provede platbu, a poté je přesměrován zpět k obchodníkovi. Samozřejmě probíhá také komunikace mezi obchodníkem a platební bránou mobilního operátora. Pro každou transakci je generováno jednoznačné ID transakce. Konkrétní způsob implementace je závislý na operátorovi a ten také obvykle tuto implementaci u obchodníka provádí.

Pokud by se jednalo o platbu pomocí Premium SMS, tak na stránkách obchodníka je zákazníkovi sděleno, v jakém formátu a na jaké číslo má SMS odeslat. Poté systém obchodníka zkontroluje, zda SMS byla přijata a na základě toho poskytne zákazníkovi službu či produkt.

6.7 Asociace pro mobilní platby

„Cílem Asociace pro mobilní platby (Mobile Payment Association, MPA) je stimulovat na českém trhu využití mobilních technologií pro finanční služby jako jsou mobilní bankovníctví, mobilní platby a transakce.“



Předmětem činnosti Asociace je vývoj a podpora bezpečných řešení mobilních plateb pro koncové uživatele, a to jak na českém trhu, tak i při roamingu.

Asociace byla založena v září roku 2002. Jejími (zakládajícími) členy jsou: Česká spořitelna, Československá obchodní banka (ČSOB), Český mobil (Oskar, nyní Oskar/Vodafone), EuroTel, GE Capital Bank (nyní GE Money bank), HVB Bank, Komerční banka, T-Mobile.

Členy MPA se mohou stát všechny banky (podle zákona č. 21/1992 Sb.) a mobilní operátoři (poskytovatelé telekomunikačních služeb, podle zákona č. 51/2000 Sb.).

V rámci asociace fungují tři pracovní skupiny. Jsou to: Business Group (obchodní skupina), která se zabývá především hledáním vhodných obchodních modelů pro mobilní platby. Dále Requirements & Technology Group (Skupina pro požadavky a technologie), která se zaměřuje na technickou stránku nezbytnou pro platby pomocí mobilního telefonu. A Marketing Group (Marketingová skupina), jejíž cílem je studovat potřeby zákazníků a požadavky trhu.

Velkým přínosem této asociace by měl být fakt, že sdružuje všechny mobilní operátory a pět velkých hráčů z českého bankovního trhu, což by mělo být výhodou pro zákazníky v tom smyslu, že vyvinutého systému by mohli využívat bez ohledu na to, služeb jakého mobilního operátora využívají a podpora ze strany bank by také byla k dispozici pro většinu uživatelů.

Bohužel, v současné době není o výsledcích práce Asociace pro mobilní platby příliš mnoho dostupných informací. Podle neoficiálních informací z věrohodných zdrojů bylo hlavním záměrem Asociace (v období jejího založení v roce 2002) zavedení společného systému mobilních plateb. Po zavedení systému mobilních plateb jednostranně ze strany T-Mobile však tento cíl přestal být reálný a aktivity Asociace pro mobilní platby jsou v tomto směru omezeny.

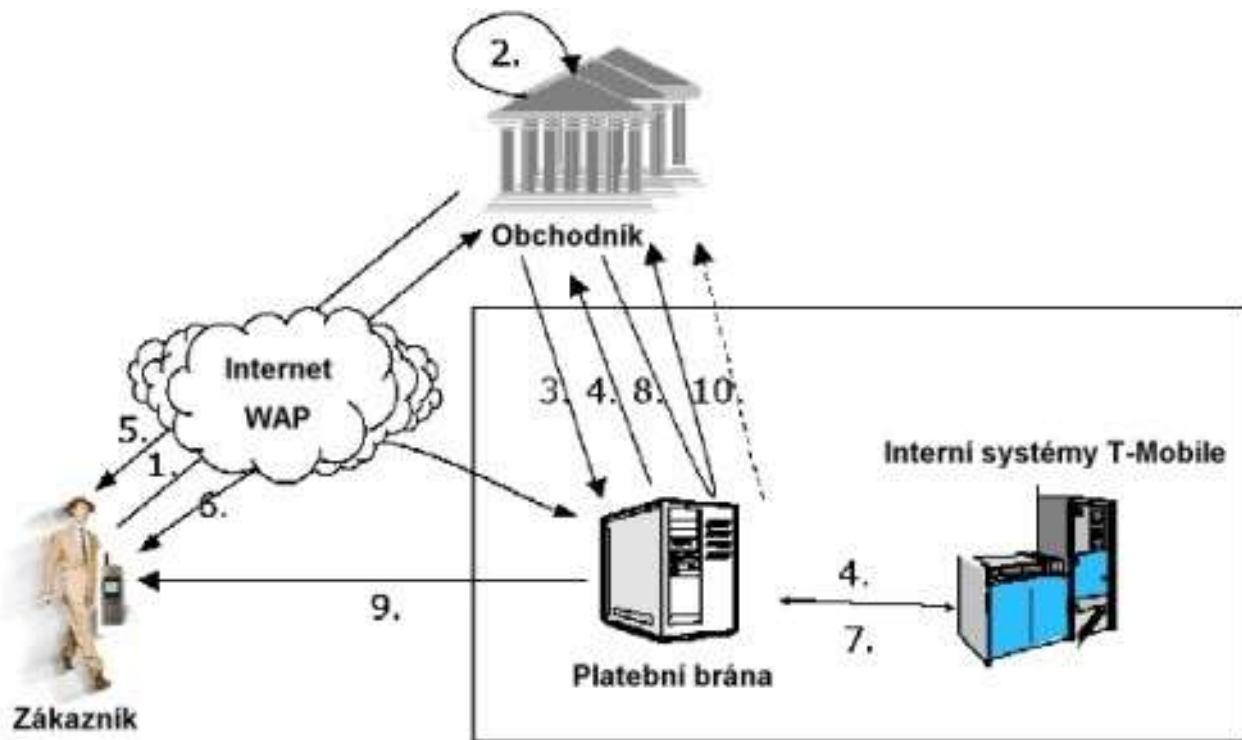
6.8 Co nabízejí jednotliví operátoři

Zatímco služby Premium SMS (a samozřejmě též službu nestandardně zpoplatněných telefonních čísel) nabízejí všichni tři čeští mobilní operátoři, tak u nabídky m-plateb jsou rozdíly značné. Nejlépe se na tom zdá být T-Mobile, Oskar/Vodafone se ani nesnaží příliš konkurovat a EuroTel se v této oblasti nijak výrazněji neangažuje.

6.8.1 T-Mobile m-platba

6.8.1.1 Fungování systému

Fungování systému ukazuje následující schéma.



Obrázek 6.1: Schéma fungování m-platby u T-Mobile

Zdroj: <http://t-mobile.cz/Web/Partnership/T-MobileM-platba.aspx>

1. Výběr zboží/služby na stránkách obchodníka, volba T-Mobile m-platby jako platebního prostředku.
2. Obchodník provede kontrolu dostupnosti a zablokování zboží.
3. Odeslání požadavku na transakci s požadavkem zákazníka na platební bránu T-Mobile.
4. Platební brána T-Mobile provede kontrolu obchodníka a vygeneruje unikátní ID transakce a spolu s potvrzením přijetí požadavku ho zašle zpět obchodníkovi.
5. Obchodník vygeneruje "Redirect" odpověď, kterou zákazníka přesměruje na platební bránu T-Mobile s ID transakce jako parametrem.
6. Zákazník se zadáním t-zones uživatelského jména a hesla autentizuje a v bezpečné zóně platební brány potvrdí platbu. Platební brána zobrazí zákazníkovi výsledek a přesměruje zákazníka zpět na stránky obchodníka.
7. Zaúčtování transakce v interních systémech společnosti T-Mobile Czech Republic.
8. Obchodník pošle SOAP dotaz na transakci s daným ID transakce. Je-li transakce úspěšně zaúčtována, vrátí T-Mobile SOAP zprávu s informací, že platba byla opravdu zaúčtována.
9. Zákazníkovi je zaslána konfirmační SMS s informací o stavu transakce a ID transakce.
10. Na konci časové periody je provedeno finanční vyrovnání.

6.8.1.2 Systém a jeho výhody pro zákazníka

Zákazníci společnosti T-Mobile mohou prostřednictvím této služby nakupovat služby nebo zboží u obchodníků, kteří mají se společností smlouvu. Pro většinu transakcí je potřeba, aby byl zákazník zaregistrován a musí mít aktivovanou službu m-platba. Oba dva úkony lze provést přes Internet a zaberou nanejvýš pár minut času.

Výhodou pro zákazníka je, že po provedení transakce je mu na mobilní telefon zaslána krátká textová zpráva s identifikačním číslem platby, která prokazuje, že zákazník za transakci zaplatil. Maximální limit jedné transakce je 700,- Kč.

Služba umožňuje placení buď na Internetu nebo přes WAP. Její použití je pro zákazníka zcela zdarma, pokud ovšem využívá tuto službu přes WAP, platí poplatky za použití WAPu dle svého tarifu. Přehled veškerých uskutečněných plateb si zákazník může kdykoli prohlédnout na Internetu.

Výhodou pro zákazníka je, že za transakci nic neplatí - zaplatí pouze cenu služby či zboží, neplatí nic navíc.

Pokud zákazník nemá k systému plnou důvěru, může si nastavit denní limit, který sníží případné ztráty ze zneužití. Navíc, každá transakce je na mobilní telefon oznámena SMS zprávou, takže při případném pokusu o zneužití by zákazník byl okamžitě informován a mohl začít vzniklý problém řešit.

6.8.1.3 Systém z pohledu obchodníka

Implementace na straně obchodníka je jednoduchá, obchodník obdrží implementační balíček, nemusí tedy provádět žádnou rozsáhlou implementaci sám.

Riziko zneužití by mělo být nízké či žádné, neboť T-Mobile vybírá částku od zákazníka, a jestliže tedy T-Mobile transakci autorizuje, tak není důvod, aby obchodník své peníze nedostal. Komunikace je zabezpečena protokolem SOAP-over-SSL, což chrání proti manipulaci dat při přenosu. Vzhledem k tomu, že veškeré transakce jsou on-line, tak platba je zpracována rychle.

Otázkou zůstává, jakou částku požaduje společnost T-Mobile z každé provedené transakce od obchodníka. Tuto informaci se mi nepodařilo ani přes velké usilí oficiálně zjistit, nicméně podle neoficiálních informací z věrohodných zdrojů se jedná o poplatek ve výši cca. 25 % z částky uskutečněné transakce, což je hlavní překážkou dalšího rozšíření tohoto systému.

6.8.1.4 Důvěryhodnost a rozšíření

Co se týče důvěryhodnosti, tak zákazníkům může pomoci to, že obchodník, u kterého nakupuje, je smluvně vázán se společností T-Mobile a lze tedy očekávat, že takový obchodník je alespoň do určité míry prověřen.

V současné době je možné platit u třinácti obchodníků, což je celkem osmnáct webových serverů. Jsou mezi nimi inzertní, herní či erotické servery, ale i další. Jejich plný výčet je možné najít na stránkách společnosti T-Mobile.

6.8.1.5 Zhodnocení

Ačkoli systém není rozšířen tak, jak by si jistě všechny zúčastněné strany přály, tak na základě výše uvedených informací a srovnání s nabídkou ostatních mobilních operátorů⁵⁰, se jeví jako **nejlepší systém mobilních plateb**, který je v současné době v ČR dostupný. Systém má všechny náležitosti, které jsou potřeba pro bezpečné provedení platby, umožňuje implementaci u obchodníka, která není nijak technicky náročná a nabízí zákazníkům poskytování této služby za velmi rozumné ceny, respektive při provedení transakce přes Internet (ne přes WAP), neplatí zákazník nic.

Jestliže v budoucnu dojde k jeho většímu rozšíření, má zřejmě reálnou šanci získat vedoucí postavení na trhu m-plateb a mikroplatebních systémů vůbec.

6.8.2 M-Platby u Oskara/Vodafone



Tak bohužel zákazníci společnosti Oskar/Vodafone, kteří by chtěli platit pomocí svého mobilního telefonu za služby či jiné produkty, mají v tomto ohledu smůlu. Oskar/Vodafone sice službu m-Platby má, ale bohužel tu je možné použít pouze pro platby za služby související s tímto mobilním operátorem - konkrétně dobít kredit na Oskartě, zaplatit fakturu, provést platbu předem za služby mobilního operátora nebo navýšit volací jistinu.

Lze sice platit prostřednictvím bankovního účtu nebo pomocí platební karty, jejichž seznam by byl vyhovující (EC/MC, Maestro, VISA, VISA Electron či American Express), ale podmínkou je, že banka, u které je veden účet či která vydala platební kartu, je partnerskou společností mobilního operátora. To znamená, že m-platbu prostřednictvím bankovního účtu mohou provádět zákazníci GE Money Bank, České spořitelny, ČSOB, Poštovní spořitelny a Živnostenské banky. Zákazníci, kteří by chtěli platit platební kartou, musí být zákazníky Komerční banky, eBanky nebo Volksbank CZ, případně vlastnit kartu YES společnosti Home Credit nebo úvěrovou či kreditní kartu České pojišťovny. A pokud zákazník dokáže splnit všechny výše uvedené podmínky, musí vlastnit jiný

⁵⁰ Viz dále

telefon než telefon značky Bosch, který je pro službu technicky nezpůsobilý, stejně jako telefon Siemens S40.

Kromě výše uvedeného existují ještě další omezení týkající se limitů placených částek. Částka pro platby za vyúčtování a platbu předem musí být minimálně 100 Kč, navýšení jistiny musí být minimálně v hodnotě 500 Kč.

Co se týče maximálních limitů, tak s těmi by naprostá většina zákazníků neměla mít problém. Oskartu lze dobít až do výše 10 000 Kč a maximální celková platba za služby operátora je stanovena na 999 999 Kč, což je patrně mnohem více, než zákazníci běžně požadují.

6.8.3 M-platby u EuroTelu



Zákazníci společnosti EuroTel mohou využít službu m-platby pro platbu za lístky do kina. Ne však do jakéhokoli kina, EuroTel v tomto ohledu spolupracuje pouze s řetězcem multikin Palace Cinemas. Samotný proces rezervace a zaplacení vstupenky také není úplně jednoduchý a navíc celá transakce vyjde zákazníky poměrně draho. Nejdříve bude zákazníkovi samozřejmě naúčtována částka za použití služby (Internet, WAP, EuroTel Asistent, informační linka kina) pomocí které provedl rezervaci a dále mu ještě bude naúčtováno 10 Kč za použití m-platby. Pro tarifní zákazníky je limit 1000 Kč měsíčně, což znamená jít ve dvou lidech do kina třikrát a dost.

V minulosti spolupracovala společnost EuroTel se Citibank na projektu Juice, kde byla zákazníkům nabízena platba pomocí virtuální platební karty Juice Pay, ale tento projekt byl v roce 2001 zrušen.

6.9 Shrnutí a závěry

Ačkoli patrně nejdůležitější podmínky pro fungování mobilních plateb, kterými jsou dostatečně vysoká penetrace mobilních telefonů a schopnost mobilního telefonu fungovat jako platební terminál, jsou v České republice splněny, tak nabídka m-plateb je pro zákazníky velmi limitována. Jediným operátorem, který nabízí m-platbu v rozumné míře se jeví T-Mobile, Oskar/Vodafone umožňuje m-platbu pouze pro zaplacení za své vlastní služby a EuroTel nabízí platbu pouze za lístky do kina společnosti Palace Cinemas a to ještě za poměrně vysokou provizi, kterou musí zákazník zaplatit. Nabídka jednotlivých mobilních operátorů se tedy značně liší. Na druhou stranu, existuje zde Asociace pro mobilní platby (MPA), která by měla usilovat o vytvoření a nasazení univerzálního systému, který by mobilní platby umožňoval. Nicméně v současné době není vůbec jisté, jestli nějaký takový systém bude nasazen. Pokud by tedy neuspěly snahy MPA a mobilní operátoři šli každý svou vlastní cestou, tak patrně nejlepší výchozí situaci má T-Mobile, protože, jak

již bylo uvedeno, ten už m-platby nabízí způsobem, jakým by zřejmě mohly v budoucnu fungovat. Proto, aby se stal leaderem na českém trhu je potřeba větší rozšíření jeho m-plateb. Úplně špatnou výchozí pozici nemá ani Oskar/Vodafone, jehož systému m-plateb se jeví jako dobrý, ale tím, že v současnosti neumožňuje platby za nic jiného, než za své služby, tak těžko odhadovat možný budoucí vývoj. Co se týče Eurotelu, tak nad ním visí značné množství otazníků, neboť nabídka jeho služeb je velmi omezená a i pokud by nebyla, tak většímu rozšíření bude patrně bránit vysoká cena pro zákazníka.

Byly též zmíněny další způsoby, jak platit pomocí mobilního telefonu, jimiž jsou Premium SMS a volání na nestandardně zpoplatněná telefonní čísla. Byl též specifikován způsob integrace m-plateb do elektronického obchodování.

Samozřejmě důležitou složkou veškerých plateb, a tedy i těch mobilních je bezpečnost. Bylo naznačeno, jak jsou m-platby zabezpečeny a jakých protokolů se využívá.

Kromě možností, které jsou v mnoha případech shodné s mikroplatebními systémy, a výhod, kterými jsou hlavně rozšířenosti mobilních telefonů a jejich schopnosti fungovat jako platební terminál, byly též zmíněny možné problémy, jako například omezení výše transakce, někdy i anonymita zákazníka, a překážky, které bude nutné do budoucna odstranit – umožnění on-line přístupu k výpisu o transakcích a zvýšení finančních limitů na poskytované služby.

Závěrem musím bohužel sdělit, že možnosti m-plateb se v současné době nejeví jako ideální, ba naopak, že jim k ideálu chybí mnoho. Nicméně, předpoklady nejsou úplně špatné a ke zlepšení, respektive většímu rozšíření, by v budoucnosti mohlo dojít.

7 Bezpečnost

7.1 Cíle kapitoly

Jelikož bezpečnost je jedním ze základních požadavků na platební systémy, tak ji ani zde nelze opominout. V této kapitole se zaměříme především na to, kde a jaká rizika vznikají. Kromě obecných zásad a rizik týkajících se bezpečnosti také zmíníme specifické způsoby zabezpečení údajů o kreditních kartách.

Dále bude popsána a zanalyzována technologie 3-D Secure, která je v současnosti pravděpodobně nejvíce zmiňována v souvislosti s elektronickými platebními systémy.

Následující text by měl být přínosem jak pro zákazníky, tak i pro obchodníky v tom smyslu, že čtenáři přibližuje aspekty týkající se bezpečnosti platebních systémů a s tím také související zabezpečení kreditních/debetních karet. Užitečný bude i pro všechny další čtenáře, kteří se nějakým způsobem o uvedenou problematiku zajímají.

7.2 Zabezpečení a rizika na straně obchodníka

Na straně obchodníka leží v oblasti bezpečnosti velká zodpovědnost. Jedná se o zabezpečení proti útokům a o zabezpečení dat pro případ, že dojde k jejich poškození - ať v důsledku útoku, technického selhání či přírodní katastrofy.

Platební systémy samozřejmě vyžadují velmi vysoký stupeň zabezpečení, neboť v případě zneužití jsou následky velmi vážné, v některých případech pro uživatele, obchodníka či oba, dokonce fatální. Platební systém u obchodníka má poměrně „velkou šanci“ stát se terčem většího počítačového útoku a tomu je třeba zabezpečení přizpůsobit.

Obchodník by měl tedy disponovat takovým systémem, který je dostatečně bezpečný na to, aby v něm mohly být uchovávány citlivé informace a aby tyto informace nemohly být zneužity. Systém obchodníka by měl být zabezpečen mimo jiné firewallem a antivirovým programem. Nejedná se však jen o dobrou ochranu proti útokům „z venku“, tedy vzdáleným útokům provedeným pomocí počítače, ale také o dobré vnitřní směrnice, předpisy a kontrolní mechanismy, aby data nemohla být zneužita zaměstnanci obchodníka.

Je pochopitelné, že žádný systém, bohužel ani ten platební, nemůže být stoprocentně bezpečný. Je tedy nutné, aby data byla vhodně zálohována a v případě jejich ztráty, ať už z jakéhokoli důvodu, byla snadno obnovitelná.

7.3 Zabezpečení a rizika na straně uživatele

Samozřejmě rizika na straně uživatele nejsou tak rozsáhlá jako na straně obchodníka, nicméně je potřeba jim věnovat velkou pozornost. Primárním důvodem je fakt, že uživatel se při výběru aplikace ve většině případů neřídí příliš technickými informacemi či bezpečnostními parametry, ale spíše reputací obchodníka. Ten by měl tedy dbát i na zabezpečení na straně uživatele, protože uživatel je ve značné informační nevýhodě a o zabezpečení toho obvykle moc neví.

Nechvalným případem jsou v české historii systémy Internetového bankovníctví některých bank. Byly případy, že klientům banky byly z účtu odcizeny peníze právě díky nedostatečnému zabezpečení na straně uživatele. Banka se pak hájila tím, že *jejich* systém je bezpečný. Samozřejmě, že chyba vznikla na straně uživatele, ale banky neposkytovaly dostatečné informace o tom, jak důležité zabezpečení je, natož aby uživatelům radily, jak jej provést. Uživatel, jehož počítač se stal terčem úspěšného počítačového útoku (což není nijak neobvyklá záležitost), snadno přišel o své peníze na bankovním účtu.

Na straně uživatele je platební systém obvykle zabezpečen kombinací jména a hesla, což je standardní ochrana. Liší se pochopitelně systém od systému, ale v mnoha případech může být tato ochrana nedostatečná. Kromě tohoto nejzákladnějšího zabezpečení je zde možnost využití certifikátů, které má uživatel uložené u sebe - v praxi to často znamená na pevném disku, což ovšem není příliš bezpečné. V případě prolomení ochrany osobního počítače je totiž ukraden i tento certifikát. Tento problém je možné snadno řešit tak, že certifikát je uložen na disketě nebo na jiném vyjímatelném paměťovém médiu. Z důvodu menší uživatelské přívětivosti však ukládání jinam než na pevný disk počítače není u uživatelů příliš obvyklé.

Dalším způsobem, jak lze systém na straně uživatele zabezpečit, jsou čipové karty. Jedná se o bezpečné řešení, které ovšem není, alespoň zatím, příliš rozšířené. Je k němu totiž zapotřebí, aby k počítači uživatele bylo připojeno zařízení pro čtení čipových karet. Pokud je počítač takto vybaven, uživatel jen přiloží kartu a tím se umožní provedení transakce.

Poměrně jednoduchý způsob, jak se útočník může dostat k cizím penězům, respektive si za cizí peníze něco koupit, je zneužití platební karty. Ač přístup k aplikaci je obvykle chráněn alespoň jménem a heslem, tak kreditní či debetní karta může být samozřejmě použita k platbě jakýmkoli uživatelem, který zná potřebné údaje. Těmito údaji jsou především číslo platební karty a datum expirace. Někdy jsou karty chráněny ještě speciálním bezpečnostním kódem (viz dále), který by měl zvýšit bezpečnost, ale bohužel, tento kód není vyžadován vždy.

České banky ani nedoporučují využívat klasickou platební kartu na Internetu kvůli zvýšenému

riziku zneužití. Jako alternativu nabízejí virtuální platební kartu, což není karta v pravém slova smyslu. Jsou to pouze údaje potřebné k provedení transakce - číslo karty, datum expirace a bezpečnostní kód. Pokud si to klient vyloženě přeje, je možné použít i klasické (plastové) platební karty, ale ve většině případů je potřeba banku požádat o odblokování⁵¹ platební karty pro platby na Internetu. Většina českých bankovních ústavů totiž vydává platební karty zablokované pro Internetové platby. To ovšem klient často zjistí, až když se pokusí s kartou poprvé zaplatit například v nějakém e-shopu a dostane se mu odpovědi, že transakci nelze autorizovat.

Zákazníci by si při placení na Internetu také měli dát pozor, z jakého počítače se k aplikaci zajišťující platbu přihlašují. Ačkoli platební systém jako takový může být zabezpečen dobře, přihlašování z veřejných míst (typicky Internetových kaváren) může představovat značné bezpečnostní riziko. Na počítači totiž může běžet program, který zaznamenává, jaké klávesy byly stisknuty a získat tak údaje, které pak mohou být zneužity.

Taktéž přihlašování z veřejných hotspotů⁵² může často představovat bezpečnostní riziko, neboť komunikace s přístupovým bodem (Access pointem) obvykle není šifrována. Data, která jsou komunikována mezi klientem a přístupovým bodem mohou být velmi snadno odchycena. Na druhou stranu, pokud je komunikace zabezpečena, například protokolem SSL (viz dále), tento problém odpadá, neboť citlivá data jsou zašifrována již v počítači zákazníka a není tedy problém, že jsou přenášena v jinak nezabezpečené bezdrátové síti.

7.4 Zabezpečení přenosu dat

7.4.1 Protokol SSL

Komunikace mezi uživatelem (klientem) a obchodníkem (serverem) bývá obvykle zabezpečena pomocí protokolu SSL, v současné době se používá 128-bitové⁵³ šifrování. Uživatel jeho použití pozná podle toho, že protokol v URL adrese je označen HTTPS⁵⁴ nebo podle zámku objevujícího se v dolní části obrazovky Internetového prohlížeče. U mobilních plateb to potom může být SOAP-over-SSL, tak jak jej například v České republice využívá společnost T-Mobile.

⁵¹ Pro odblokování karty je obvykle nutné zajít na pobočku. Klient si zde může také nastavit limit pro Internetové platby, což zvyšuje bezpečnost užívání kreditní/debetní karty pro platby na Internetu.

⁵² Hotspot je místo, ze kterého se lze připojit do Internetu pomocí bezdrátové sítě WiFi (standard 802.11)

⁵³ Protokol SSL umožňuje teoreticky i 40-bitové šifrování, ale tato šifra již byla prolomena a v současné době tedy neposkytuje dostatečné zabezpečení

⁵⁴ Protokol HTTPS je protokol HTTP, který používá pro komunikaci protokol SSL. Obvykle neběží na portu 80, jako standardní HTTP, nýbrž na portu 443.

Protokol SSL (Secure Socket Layer) byl vyvinut v roce 1994 firmou Netscape pro bezpečný přenos dokumentů v Internetu. Protokol využívá šifrování, které používá soukromý a veřejný klíč. Veřejný klíč je znám všem, soukromý je znám pouze příjemci zprávy. V běžně používaných prohlížečích je protokol SSL implementován.

Na straně serveru je SSL certifikát, který šifruje data a slouží k jednoznačné identifikaci webového serveru.

Certifikát je možné získat dvěma způsoby. První je, že si jej obchodník vytvoří sám. Tato varianta je samozřejmě levnější, ale také méně důvěryhodná - certifikát si totiž takto může vytvořit každý. Druhou variantou je jeho získání od certifikované autority (ve světě například VeriSign, v ČR 1. certifikační autorita), která je pro zákazníka jakýmsi garantem. Samozřejmě za předpokladu, že se jedná o renomovanou certifikační autoritu, jakou je právě třeba uváděný VeriSign.

Ačkoli zákazník obvykle pozná, že se jedná o certifikát, který nebyl vydán certifikovanou autoritou, tak mnoho uživatelů stejně v transakci pokračovat bude. Pokud certifikát nebyl vydán certifikovanou autoritou, Internetový prohlížeč na to upozorní hláškou, která uživatele varuje, že certifikát nebyl rozpoznán.

Protokol SSL je (při použití 128-bitového šifrování) bezpečný, ač se v minulosti objevily pokusy o jeho napadení. Nicméně, tyto útoky byly zaměřeny převážně na jeho implementaci v Internetovém prohlížeči Netscape a nikoli na protokol SSL jako takový.

Veškeré problémy, které byly s bezpečností SSL ať již u prohlížeče Netscape nebo u prohlížeče Internet Explorer, byly vyřešeny bezpečnostními záplatami.

7.4.2 Protokol SOAP-over-SSL

Protokol SOAP-over-SSL, lze využívat mimo jiné pro komunikaci u mobilních plateb – například v České republice ho pro své m-platby implementuje společnost T-Mobile.

Protokol SOAP (Simple Object Access Protocol) poskytuje strukturu zasílání zpráv pro přenos informací přes web. Jedná se o protokol založený na jazyce XML, který umožňuje propojovat systémy přes web nezávisle na platformě, což je jeho podstatnou výhodou. Protokol SOAP obaluje existující funkcionalitu rozhraním implementujícím standard SOAP (SOAP Wrapper) a umožňuje různým systémům číst, dešifrovat a směrovat informace obsažené ve zprávě.

Nejčastěji se SOAP používá jako náhrada vzdáleného volání procedur (Remote Procedure Call, RPC), tedy v modelu požadavek/odpověď. Jedna aplikace pošle v XML zprávě požadavek druhé aplikaci, ta požadavek obslouží a výsledek zašle jako druhou zprávu zpět původnímu iniciátorovi komunikace.

Protokol SOAP sám o sobě není bezpečný. Právě proto se používá tzv. „SOAP-over-SSL“, což je protokol SOAP, který je šifrován pomocí SSL, což garantuje jeho bezpečnost.

7.5 Formy zabezpečení údajů o kreditních kartách

Přirozeně často zmiňovaným tématem ohledně bezpečnosti placení na Internetu je bezpečnost platebních karet, respektive kombinace čísla kreditní/debetní karty, data expirace, případně bezpečnostního kódu.

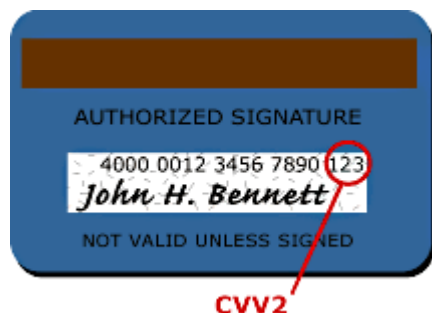
Vydavatelé platebních karet se snaží karty všemožně chránit. Některé způsoby jsou účinné více, jiné méně. Následující odstavec zmiňuje některé z nich. Nutnou podmínkou pro platbu kreditní či debetní kartou je její držení, v případě platby na Internetu potom znalost čísla karty a data expirace. Při platbě, kdy je majitel karty přítomen osobně, je někdy vyžadován podpis, který se musí shodovat se vzorem uvedeným na zadní straně karty. Vzhledem k tomu, že tyto bezpečnostní prvky se poslední dobou ukazují jako nedostatečné, objevily se další způsoby ochrany karet. Při osobní účasti majitele karty, tedy v kamenném obchodě, jsou některé platební karty chráněny tak, že přední strana karty obsahuje, mimo jiné, také fotografii⁵⁵ majitele. Jiným způsobem ochrany je vyžadování zadání osobního identifikačního čísla (PIN, Personal Identification Number), což je čtyřmístný číselný kód, který je držiteli karty vydán spolu s platební kartou a který slouží jako poměrně spolehlivý⁵⁶ bezpečnostní prvek. Při výběru hotovosti z bankomatu je vyžadován vždy, při platbě u obchodníka pouze někdy. Zda-li je PIN u obchodníka vyžadován se odvíjí od typu karty (u neembosovaných platebních karet bývá PIN kód obvykle vyžadován, u embosovaných méně), způsobu uložení informací na kartě (u čipových karet je PIN kód vyžadován častěji než u karet, které mají pouze magnetický proužek) a terminálu obchodníka (PIN kód lze zadávat pouze v on-line platebních terminálech, v případě použití imprinteru prostě není, kam jej zadat).

To jsou základní zabezpečení platebních karet, ale existují i systémy, které jsou pro platby na Internetu lepší, respektive bezpečnější.

⁵⁵ V ČR vydává takové karty například CitiBank.

⁵⁶ Byly odhaleny útoky na zjištění PIN kódu, kdy v prostoru bankomatu byla nainstalována minikamera, která snímala klávesnici bankomatu. Kromě PIN kódu je ke zneužití karty potřeba získat ještě alespoň kopii magnetického proužku, která byla obstarávána speciálním zařízením namontovaným v blízkosti dveří v prostoru bankomatu. Často je prostor bankomatu přístupný pouze po protažení karty čtecím zařízením u dveří, takže pokud to držitel karty udělal, tak v tu chvíli byl jeho magnetický proužek zkopírován a po zjištění PIN kódu z kamery byla vytvořena karta se zkopírovaným magnetickým proužkem a se znalostí PIN kódu tak došlo ke zneužití karty a okradení právoplatného majitele platební karty.

Bezpečnostní kód je velmi důležitým způsobem zabezpečení karty. Bývá označován jako CVV2⁵⁷ či CVC2⁵⁸, případně i jinak⁵⁹. U klasických plastových embosovaných⁶⁰ platebních karet VISA nebo EC/MC se nachází na zadní straně karty nad podpisem – kódem jsou vždy poslední tři čísla, bez ohledu na to, kolik se jich tam celkem nachází.



Obrázek 7.1: Umístění kódu CVV2 na platební kartě VISA

Zdroj: http://switzerland.isyours.com/images/card_CVV2.gif

Kód u platebních karet EuroCard/MasterCard se nazývá CVC2 a povinně ho mají všechny kreditní i debetní karty od prvního ledna roku 1997. Platební karty VISA obsahují povinně kód, který se jmenuje CVV2, od prvního ledna roku 2001. Kód je počítán podle určitého matematického algoritmu, který ovšem není znám, a tak při zjištění čísla kreditní/debetní karty není možné tento bezpečnostní kód dopočítat, což poskytuje vysoký stupeň ochrany. U virtuálních platebních karet určených speciálně pro placení na Internetu, je tento kód uveden samostatně, obvykle na řádku hned pod datem expirace.

Problémem ovšem je, že ne vždy je tento kód pro provedení transakce vyžadován. Je zřejmé, že pokud vyžadován není, je bezpečnost použití platební karty značně snížena.

Obchodníci, kteří vyžadují zadávání kódu CVC2/CVV2 mohou dosáhnout výrazného snížení reklamací klientů. Podle některých zdrojů⁶¹ až o 26%.

Patrně nejbezpečnějším systémem, který je v současné době majitelům platebních karet nabízen, je zamykání platební karty. Pro uskutečnění transakce je nutné kartu nejdříve odemknout – obvykle pomocí mobilního telefonu. Po provedení transakce je možné kartu opět uzamknout, případně lze nastavit, aby se karta po provedení transakce uzamkla sama. Tato funkce však chrání kartu pouze při užití v bankomatech, on-line platebních terminálech či na Internetu. Proti transakcím

⁵⁷ CVV2 – Card Verification Value

⁵⁸ CVC2 – Card Verification Code

⁵⁹ Například u karet American Express se tento kód nazývá CID (Card Identifier). Na rozdíl od karet VISA či EC/MC se nachází na přední straně nad číslem karty a má čtyři číslice, nikoli jen tři.

⁶⁰ Neembosované karty Maestro například tento kód nemají.

⁶¹ Například <http://www.gcefcu.org/images/card.htm>

uskutečněným pomocí imprinteru (žehličky) tento způsob kartu nechrání. V České republice nabízí tuto službu eBanka a nutno podotknout, že se jedná v České republice a možná i ve světě o unikátní službu. Zamykání karty má však i jednu nevýhodu – kartu nelze zamykat v případě, že její držitel s ní chce provádět opakované platby (například platit měsíčně předplatné), neboť při zamčené kartě nelze provést žádnou platbu.

Co se týče bezpečnosti kreditních/debetních karet, tak je ještě třeba zmínit, že klasické plastové platební karty jsou v současnosti k dispozici ve dvou variantách, co se způsobu uložení dat týče. První, starší variantou je magnetický proužek. Tato varianta nemá žádnou znatelnou výhodu, zato má jedno velké bezpečnostní riziko – magnetický proužek lze zkopírovat (viz též výše). Pokud tedy například v restauraci zákazník platí kartou a neohlídá si, aby po celou dobu provádění transakce na kartu viděl, může se mu stát, že během chvíle bude jeho karta zkopírována (v podstatě bude vyroben její identický duplikát) a později zneužita.

V současné době jsou již vydávány i platební karty, jejichž údaje jsou uloženy na čipu. Problémem je, že alespoň v současné době, jsou data uložena jak na čipu, tak i na magnetickém proužku a to zejména z toho důvodu, že ne všechny platební terminály jsou schopny přečíst data z čipu. Přínosem pro bezpečnost by bylo, kdyby časem karty měly data uloženy pouze na čipu, odkud je nelze zkopírovat. Kartu by potom nebylo možné zkopírovat a ani tedy výše popsáním způsobem zneužít. Zákazník už by se nemusel starat o to, aby na svou platební kartu viděl po celou dobu provádění transakce.

7.6 Technologie 3-D Secure

Technologie (přesněji řečeno autentifikační protokol) 3-D Secure⁶² byla vyvinuta společnostmi Visa a MasterCard pro vyšší zabezpečení transakcí prováděných platební kartou na Internetu. Všude tam, kde je technologie pro platbu aplikována, najde zákazník logo s nápisem „VERIFIED by VISA“ pro platby kreditní či debetní kartou VISA, případně VISA Electron nebo logo s nápisem „MasterCard SecureCode“ pro platbu kartou EuroCard/MasterCard, případně Maestro. Grafická podoba – viz obrázky níže.

⁶² 3-D Secure nebo také 3-Domain Secure.



Obrázek 7.3: Logo VERIFIED by VISA

Zdroj: http://www.visaeurope.com/iusevisa/images/iuse_v_verified.gif



Obrázek 7.2: Logo MasterCard SecureCode

Zdroj: http://www.camtech.com.au/NR/rdonlyres/DF1D8395-3093-42CD-93C6-CED34BB0771B/0/Mastercard_Securecode.gif

Nejdůležitějším rysem technologie 3-D Secure je, že za ověření zákazníka (majitele karty) je zodpovědný vydavatel karty, nikoli obchodník či zákazník. Tento model nabízí vyšší bezpečnost a v případě nesrovnalostí zjednoduší analýzu provedených bankovních transakcí.

Hlavním impulsem pro zavedení bezpečnější technologie byl právě fakt, že prudce narůstal počet transakcí provedených platební kartou, o nichž majitelé karet tvrdili, že je neautorizovali.

Podle údajů společnosti Visa International⁶³ lze pomocí autentifikace plateb dosáhnout až osmdesátiprocentního snížení podvodů a sporných transakcí.

Technologie 3-D Secure používá pro šifrování dat běžně dostupného protokolu SSL (viz výše).

7.6.1 Výhody 3-D Secure

Pro obchodníky je integrace technologie 3-D Secure do jejich systému nenáročnou záležitostí, stačí pouze softwarový plug-in na straně serveru obchodníka. Interakce obchodníka se zákazníkem není nijak významně omezena. Díky vyšší bezpečnosti (která je v současnosti propagována i společnostmi VISA a EuroCard/MasterCard a některými bankami) je pro obchodníka snadnější přesvědčit zákazníka, aby uskutečnil nákup pomocí platební karty.

Vyšší bezpečnost je samozřejmě vítána i zákazníky a jejich bankovními ústavy.

7.6.2 Proč „3-D“

Zkratka 3-D znamená 3-Domain (třídoménový). Tři domény jsou následující: doména vydavatele⁶⁴, doména nabyvatele⁶⁵ a styčná doména⁶⁶.

Vydavatel je zodpovědný za registraci majitele karty do systému 3-D Secure a prověření jeho totožnosti a poté za jeho ověření při každé on-line platební transakci.

Nabyvatel je zodpovědný za zajištění, že každý obchodník, který se podílí na on-line transakci, dodržuje podmínky uvedené ve smlouvě s nabyvatelem a za zpracování ověřených transakcí.

⁶³ Konkrétně zdroj http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

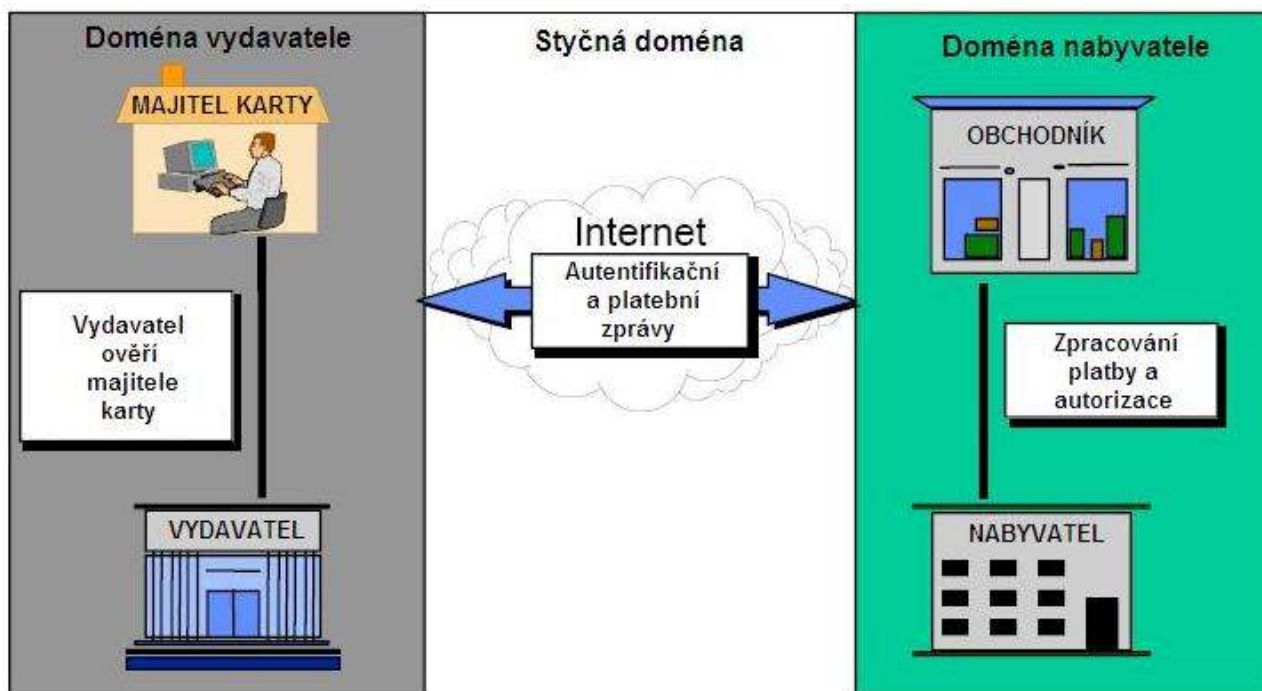
⁶⁴ Jedná se o systémy a funkce na straně vydavatele (typicky banky zákazníka) a zákazníků

⁶⁵ Jedná se o systémy a funkce na straně nabyvatele (typicky banka obchodníka) a obchodníků

⁶⁶ Jedná se o systémy, funkce a zprávy umožňující komunikaci mezi doménami vydavatele a nabyvatele

Styčná doména umožňuje uskutečnění transakce mezi vydavatelem a nabyvatelem v prostředí Internetu⁶⁷.

Schéma fungování – viz obrázek.



Obrázek 7.4: Tři domény v 3-D Secure

Podle http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

7.6.3 Schéma fungování 3-D Secure

3-D Secure se skládá ze dvou hlavních funkcí. A to z registrace a z ověřování (autentifikace).

Aby mohl klient (majitel kreditní/debetní karty) využívat pro platby na Internetu technologie 3-D Secure, musí být pro použití této služby zaregistrován⁶⁸. Při registraci klient poskytne vydavateli informace prokazující jeho totožnost a zvolí si heslo a případně tzv. „Personal Assurance Number“⁶⁹. Po ověření údajů vydavatelem je klient zaregistrován pro používání 3-D Secure.

Registrační server vydavatele udržuje záznamy o všech klientech, kteří jsou v systému zaregistrováni, a zprostředkovává tyto údaje speciálním serveru vydavatele, který se nazývá „Access Control Server (ACS)“. ACS slouží pro ověření klienta při každé prováděné transakci.

Po dokončení registrace může klient již nakupovat ve všech Internetových obchodech, které mají integrovaný plug-in pro 3-D Secure. Tento plug-in (Merchant Server Plug-in, MPI) umožňuje získat

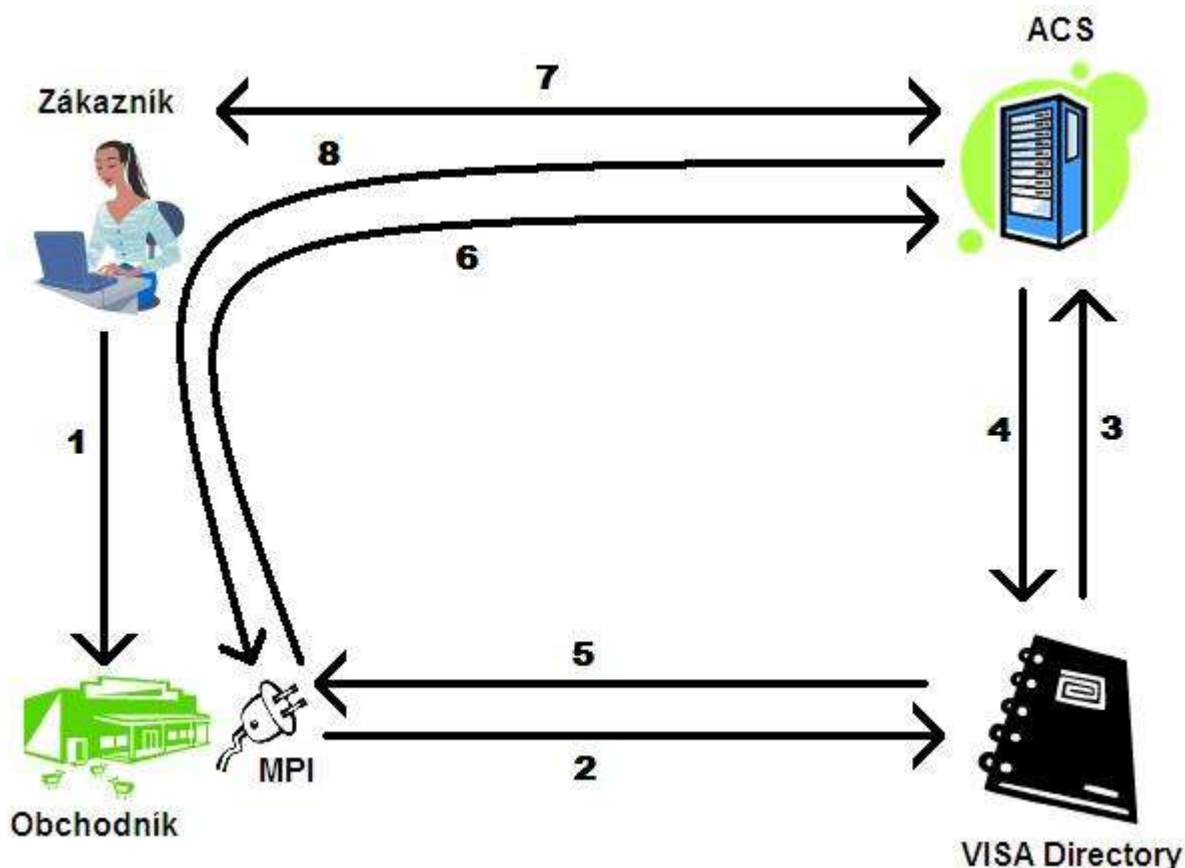
⁶⁷ dle http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

⁶⁸ V některých případech provádí registraci automaticky banka uživatele, který se už o vlastní registraci nemusí starat.

⁶⁹ Konkrétní implementace závisí na vydavateli.

informace o klientovi a připojit se na Access Control Server vydavatele pro ověření, že klient je registrován ve 3-D Secure.

Průběh transakce zobrazuje obrázek.



Obrázek 7.5: Průběh transakce v systému 3-D Secure

Transakce probíhá tak, že po žádosti zákazníka (1) o placení kartou pomocí 3-D Secure, plug-in na straně obchodníka (MPI) pošle (2) dotaz do Visa Directory⁷⁰. Visa Directory přes Access Control Server ověří (3), jestli je zákazník (jeho platební karta) registrován v systému 3-D Secure. Pokud výsledkem je (4), že zákazník je v systému 3-D Secure registrován, tak do systému obchodníka je zaslána (5) URL adresa příslušného ACS (Access Control Serveru). Plug-in na serveru obchodníka (MPI) potom pošle (6) přes prohlížeč zákazníka požadavek na ověření⁷¹ na server ACS. Následně ACS provede (7) ověřovací proceduru (autentifikaci) tak, jak ji definoval vydavatel – například může být od zákazníka vyžadováno heslo. Výsledek této autentifikace je odeslán (8) přes prohlížeč

⁷⁰ Visa Directory je systém, který přes Internet poskytuje informace o vydavatelích a o umístění jejich ACS.

⁷¹ Access Control Server provádí ověřování dvakrát! Nejdříve spolu s Visa Directory ověřuje, zda je uváděná platební karta registrována v systému 3-D Secure a pokud ano, tak potom se ověřuje, že zákazník je ten, za koho se vydává.

zákazníka zpět do serverového plug-inu obchodníka. Pokud vše proběhne v pořádku, výsledek je vrácen do systému obchodníka a transakce může normálně pokračovat⁷².

Detailní popis systému a jeho fungování lze najít na stránkách společnosti Visa International⁷³.

7.6.4 Požadavky na jednotlivé účastníky

Obchodník musí do své serverové aplikace integrovat Merchant Server Plug-in, který je nezbytný pro komunikaci s Visa Directory a ACS servery, při které se ověřuje, zda je zákazník registrován v systému 3-D Secure. Integrace serverového plug-inu nijak neovlivní vzhled obchodníkovy aplikace (například on-line nákupního košíku).

Nabyvatel (typicky banka obchodníka) musí mít uzavřenu smlouvu s obchodníkem, který platbu prostřednictvím 3-D Secure nabízí. Může též nabízet pomoc obchodníkům při implementaci a podobně. V systému nabyvatele jsou také uložena veškerá data týkající se obchodníka jako jsou hesla, certifikáty atd.

Ze strany zákazníka nevyžaduje platba přes 3-D Secure žádné složité procedury. Jediné, co musí zákazník udělat, je registrovat se do systému 3-D Secure, což lze v mnoha případech udělat on-line na stránkách vydavatele (typicky banka zákazníka), případně to vydavatel udělá automaticky. Pro zákazníka probíhá transakce velmi podobně jako bez použití 3-D Secure a nevyžaduje žádný speciální hardware nebo software.

Vydavatel je zodpovědný za registraci zákazníků do systému a za jejich autentifikaci při každé transakci uskutečněné přes 3-D Secure. Informace o registrovaných zákaznících jsou na ACS serveru vydavatele, který tyto informace poskytuje serverovým plug-inům obchodníků⁷⁴.

7.6.5 Zhodnocení

Vzhledem k tomu, že se jedná o technicky dobrý systém, který byl vyvinut leadery v oblasti platebních karet a že byl adoptován mnoha renomovanými bankami, domnívám se, že systém má dobrou šanci pro své další rozšíření. Na druhou stranu, je třeba jisté míry opatrnosti, neboť do systému SET (Secure Electronic Transaction) byla též vkládána velká očekávání, která se ovšem nenaplnila. Nicméně, vzhledem k výše uvedeným vlastnostem systému 3-D Secure si myslím, že předpoklad jeho dalšího rozvoje je reálný.

⁷² Dle http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

⁷³ Například konkrétně v dokumentu http://international.visa.com/fb/paytech/secure/pdfs/3DS_70015-01_System_Overview_external_v1.0.2_May_2003.pdf

⁷⁴ Podle http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

7.7 Shrnutí a závěry

Byly identifikovány tři základní oblasti, kde může vzniknout riziko týkající se platebních systémů. V první řadě jsou to rizika na straně obchodníka, kde patrně největším rizikem je „nabourání“ systémů obchodníka a zneužití získaných dat. Nicméně, systémy obchodníků bývají obvykle zabezpečené relativně dobře a na řadu přichází rizika na straně zákazníka. Bylo uvedeno, že zákazníci nemají často dostatečné znalosti na to, aby možná rizika, kterými je například nabourání se do domácího počítače uživatele, eliminovali, a je tedy na obchodnících a poskytovatelích systémů, aby jim s tou problematikou pomohli. Nejběžnějším zabezpečením je stále ještě kombinace uživatelského jména a hesla, ale jsou k dispozici již i sofistikovanější a bezpečnější způsoby, kterými jsou například certifikáty nebo čipové karty. Kromě zabezpečení na straně obchodníka a zákazníka, je ještě potřeba zabezpečit data při přenosu. V této souvislosti bylo pojednáno o protokolu SSL, který se používá pro běžné Internetové platební transakce a dále také o protokolu SOAP-over-SSL, který se používá pro zabezpečenou komunikaci při transakcích prováděných mobilními telefony.

Co se týče plateb kreditní či debetní kartou, tak bylo zmíněno několik způsobů zabezpečení, jako je například bezpečnostní kód (CVV2, CVC2, CID), zamykání platební karty a další.

V souvislosti s platebními kartami bylo analyzováno využití technologie 3-D Secure, její fungování a výhody a požadavky na jednotlivé účastníky transakcí prováděných pomocí této technologie.

8 Případová studie konkrétní firmy

8.1 Stručný popis analyzované firmy

Jedná se malou firmu s počtem zaměstnanců v řádu jednotek. Firma podniká v oblasti vývoje software, webových stránek a aplikací, propagace na Internetu, poradenství v oblasti hardware a software, zpracování dat, správy sítí, web hostingu a dalších souvisejících službách. Firma v současnosti nenabízí žádný platební systém, u kterého by ověření platby bylo součástí nákupního procesu. Transakce uskutečněné přes Internet jsou v drtivé většině případů placeny pomocí převodu z bankovního účtu. Tato varianta je prozatím přiměřeně dostačující pro pokrytí většiny obchodních transakcí v rámci ČR, ale neumožňuje, kvůli vysokým bankovním poplatkům a větším problémům s důvěrou, platební transakce se zahraničními klienty.

Ideálním řešením pro firmu by byl systém, který bude umožňovat platbu co největším počtem debetních/kreditních karet a bude umožňovat platby nejen z České republiky, ale i ze zahraničí. Výhodou by také bylo, kdyby systém mohl být transparentní – to znamená, že firma by mohla plně kontrolovat vzhled platební brány a uživatel by se vůbec nemusel dozvědět na jaké platební bráně (jakého platebního systému) se nachází.

Není třeba zdůrazňovat, že systém by měl bezpečný a důvěryhodný, dostatečně flexibilní a náklady na jeho zavedení a provoz by měly dosahovat co nejlepšího poměru cena/výkon.

Zavedení systému ve firmě by též mělo posloužit k tomu, že tento systém a pomoc s jeho implementací mohou být v budoucnu nabízeny i těm zákazníkům, kteří si u firmy objednali vývoj některých webových aplikací, například Internetového obchodu.

8.2 Výběr platebního systému

Pokud se vezmou v úvahu všechny požadavky na „ideální“ systém, tak je na první pohled zřejmé, že žádný z v práci popisovaných systémů jim plně nevyhovuje. Byla zvažována i varianta zřízení účtu v zahraniční bance a používání pouze zahraničního platebního systému, ale v této fázi bylo rozhodnuto, že bude výhodnější implementovat systém běžně dostupný v České republice s tím, že možnost nabízení elektronických plateb přes zahraniční platební systém v kombinaci se zahraničním bankovním účtem zůstane otevřena pro další fázi⁷⁵ – tj. další rozšiřování platebních možností. Hlavním důvodem pro zamítnutí této možnosti v první fázi zavedení nového elektronického platebního systému byly určité těžkosti se zřízením a vedením bankovního účtu v

⁷⁵ O další fázi implementace on-line plateb nejsou v současné době dostatečné informace a také není předmětem tohoto textu.

zahraniční bance a vysoké poplatky účtované při mezinárodních platbách – to znamená, že převod peněz na firemní účet v České republice by se prodražil, což by muselo být zahrnuto v ceně obchodních transakcí a snižovalo by tak do určité míry cenovou konkurenceschopnost firmy.

Bylo též rozhodnuto, že bude ponechána možnost platby přes bankovní účet a předpokládá se, že tato možnost bude u domácích zákazníků, alespoň v blízké budoucnosti, hojně využívána. Kromě této možnosti placení bude vybrán jeden z platebních systémů popsaných v této práci, který by měl být následně zaveden. Vybraný systém by měl co nejlépe splňovat potřeby firmy a pokud možno by se měl blížit „ideálnímu“⁷⁶ systému.

Z popisovaných systémů by firmě patrně nejlépe vyhovoval systém PayPal, ale ten v současné době bohužel není pro obchodníky z České republiky dostupný. Mikroplatební systémy a systémy mobilních plateb byly vyřazeny z důvodu omezení výše částky.

Dále byl vyřazen systém NetBanka z toho důvodu, že neumožňuje přijímat platby od zahraničních zákazníků. Ze stejného důvodu byl vyřazen i systém eBanka, nicméně je o něm uvažováno pro případnou další fázi, pokud by cílem bylo zlepšit možnosti elektronických plateb uskutečňovaných zákazníky z tuzemska. Tento systém by se jevil jako dobrý v tom smyslu, že umožňuje rychlé a pohodlné provedení platební transakce. Nicméně byl by stejně považován za doplňkový a to z toho důvodu, že podmínkou je, že zákazník musí mít účet u eBanky.

Zbývají tedy systémy Pay MUZO a Platby kartou od České spořitelny. Vzhledem k tomu, že oba tyto systémy jsou z hlediska funkčnosti pro firmu velmi podobné, tak primárním faktorem pro rozhodování byly pořizovací a provozní náklady. Hlavně z těchto důvodů byl jako nejvýhodnější systém vybrán systém Platby kartou od České spořitelny. Jeho výhodou je též skutečnost, že stačí uzavřít smlouvu s Českou spořitelnou, nevystupuje zde již další třetí subjekt, jakým je v případě systému MUZO společnost Global Payments Inc.

8.3 Náklady na zavedení systému

Jelikož zřízení systému je zdarma a neplatí se žádné další měsíční paušální poplatky za jeho provoz, tak jediné náklady, které vzniknou, budou náklady související s vyčleněním firemních zdrojů na implementaci. Náklady, které vzniknou tím, že je potřeba platit z každé transakce určité procento bance, jsou již obsaženy v kalkulaci nákladů na produkt a nejsou tedy uváděny zde.

Veškeré technické firemní zdroje jsou pro implementaci dostačující. Nebude třeba nakupovat žádný dodatečný hardware ani software. Všechny vzniklé náklady budou tedy osobní náklady. Předpokládá se cena jednoho člověkodne ve výši 3000 Kč.

⁷⁶ Ideálnímu v tom smyslu, jak jej chápe firma a jak je popsán výše.

<i>Typ nákladové položky</i>	<i>Odhadovaný počet člověkodní</i>	<i>Odhadované náklady (Kč)</i>
Komunikace s bankou, administrativní úkony	3	9000
Design řešení	4	12000
Implementace	15	45000
Testování	2	6000
Školení příslušných pracovníků	2	6000
Spuštění ostrého provozu	0,5	1500
CELKEM	26,5	79500

8.4 Očekávané přínosy ze zavedení platebního systému

Pro zkoumanou firmu je zavedení elektronického platebního systému nejen možným přínosem, ale z hlediska akceptace plateb od zahraničních zákazníků přímo nezbytností.

Byly identifikovány možné přínosy finančního a nefinančního charakteru.

8.4.1 Finanční přínosy

Hlavní přínos se očekává v oblasti příjmů plateb od zahraničních zákazníků. V současné době totiž nebylo možné přijímat platby ze zahraničí, což bylo hlavní překážkou poskytování služeb zahraničním subjektům.

Pro první rok po zavedení platebního systému se předpokládá měsíční zisk⁷⁷ ze zahraničních operací cca. 500 USD měsíčně, což je přibližně asi 12 400 Kč⁷⁸. Znamenalo by to, že náklady investované do implementace systému by se firmě vrátily za necelých šest a půl měsíce. Za první rok by tak nasazení nového platebního systému vygenerovalo od zahraničních zákazníků dodatečný zisk ve výši 69 300 Kč.

Co se týče tuzemských klientů, tak se zvýšení obrátu a tedy i zisku z tohoto zákaznického segmentu nepředpokládá a to hlavně z toho důvodu, že tuzemští zákazníci jsou obvykle ochotni platit i jinak než pomocí nového platebního systému – například již výše zmiňovaným bankovním převodem.

⁷⁷ Je myšlen přímo zisk, tedy dodatečně získané tržby od nichž se odečtou náklady dodatečně vynaložené na poskytnuté služby. Zvláště v prvním roce se předpokládá, že náklady budou vyšší hlavně z důvodu vynaložení marketingových nákladů na získání určité základny zahraničních zákazníků. Po získání této klientské základny se pro další roky předpokládá nárůst ziskové marže.

⁷⁸ Pro přepočítání na Kč byl použit průměrný kurz USD/CZK za listopad 2005 tak, jak jej uvádí ČNB.

8.4.2 Ostatní přínosy

Nejdůležitějším přínosem je již uváděné proniknutí na zahraniční trhy. Kromě popsaných finančních přínosů lze ještě zmínit fakt, že firma bude mít již připravený funkční nástroj do budoucna až on-line placení bude běžné a bude vyžadováno i v tuzemských podmínkách.

Kromě přímých přínosů plynoucích z implementace nového platebního systému může firma v budoucnu nabízet implementaci a poradenství v této oblasti těm svým zákazníkům, kteří si u ní objednali vytvoření Internetového obchodu, či kteří na firemních serverech mají hostovány své Internetové obchody a uvažují o zavedení on-line plateb v těchto obchodech.

8.5 Závěry

Z výše uvedené analýzy provedené na základě poskytnutých dat vyplývá, že firmě by se zavedení výše uváděného platebního systému mělo vyplatit a lze ho doporučit jednak kvůli poměrně rychlé návratnosti investice a jednak kvůli další možné expanzi v budoucnu.

Na konec je ještě třeba zmínit, že uvedená analýza nemůže být aplikována na všechny firmy, které by chtěly zavést on-line placení přes Internet. Záleží vždy na charakteru firmy a konkrétních podmínkách. Obecně lze říci, že on-line placení může být přínosem pro firmy, které jsou schopny své výrobky či služby přes Internet také dodávat, neboť se jim otevřou další trhy. U firem poskytujících fyzické produkty je třeba řešit i jiné problémy, zejména problémy s dopravou produktu zákazníkovi a s tím související dodatečné náklady.

9 E-billing

9.1 Co je to e-billing a k čemu slouží

Definice E-billingu

E-billing označuje elektronické systémy pro zpracování a rozesílání faktur, složenek, výpisů z účtů a dalších dokumentů, které zasílají společnosti svým zákazníkům, a zpracování plateb vztahujících se k těmto dokumentům. E-billingové systémy umožňují firmám (vydavatelům) zasílat finanční dokumenty svým zákazníkům elektronickou cestou a zákazníkům nabízejí přístup ke všem těmto dokladům na jednom místě na Internetu 24 hodin denně s možností okamžitého placení nebo podle naplánovaného kalendáře.⁷⁹

E-billingem se tedy rozumí systém, který slouží k vystavování dokumentů jako například faktur v elektronické podobě a jejich následnému zasílání obchodním partnerům (zákazníkům).

V souvislosti s e-billingem se používají dva termíny. Prvním je Electronic Bill Payment and Presentment (EBPP), který se používá pro označení procesů zaměřených na konečného spotřebitele, tedy B2C aplikací. Druhým je Electronic Invoice Payment and Presentment (EIPP), který označuje procesy mezi podniky, tedy B2B aplikace. Termínem, který zastřešuje EBPP a EIPP je potom Electronic Presentment and Payment. V následujícím textu bude většinou používán termín e-billing, což je v současnosti nejběžněji používaný termín.

Výstupem z e-billingového systému je elektronická faktura, neboli e-bill. Ta obsahuje všechny informace, které by byly uvedeny na klasické papírové faktuře, ale jejich formát může být jiný. Používají se formáty LEDES⁸⁰, .pdf, .tif, .doc, .rtf, .txt a další formáty.

9.2 Jak funguje e-billing⁸¹

Při e-billingu obvykle vystupují tři strany. Jsou jimi biller (ten, kdo vydává účet), zákazník a banka. Případně ještě prostředník.

Existují tři modely e-billingu. Ty se nazývají⁸² Seller Direct, Buyer Direct a Consolidator.

⁷⁹ Zdroj: <http://www.villusion.cz/index.phtml?lang=cz&ref=newspressrelease20020415>

⁸⁰ LEDES – Legal Electronic Data Exchange Standard standardizuje formát a obsah souborů elektronických faktur.

⁸¹ Podle <http://www.ebilling.org/EIPP/B2b.pdf>

⁸² Tyto termíny uvádí například <http://www.ebilling.org/EIPP/B2b.pdf> a v textu byly ponechány ve svých původních anglických termínech, neboť překlad do českého jazyka by byl poněkud kostrbatý.

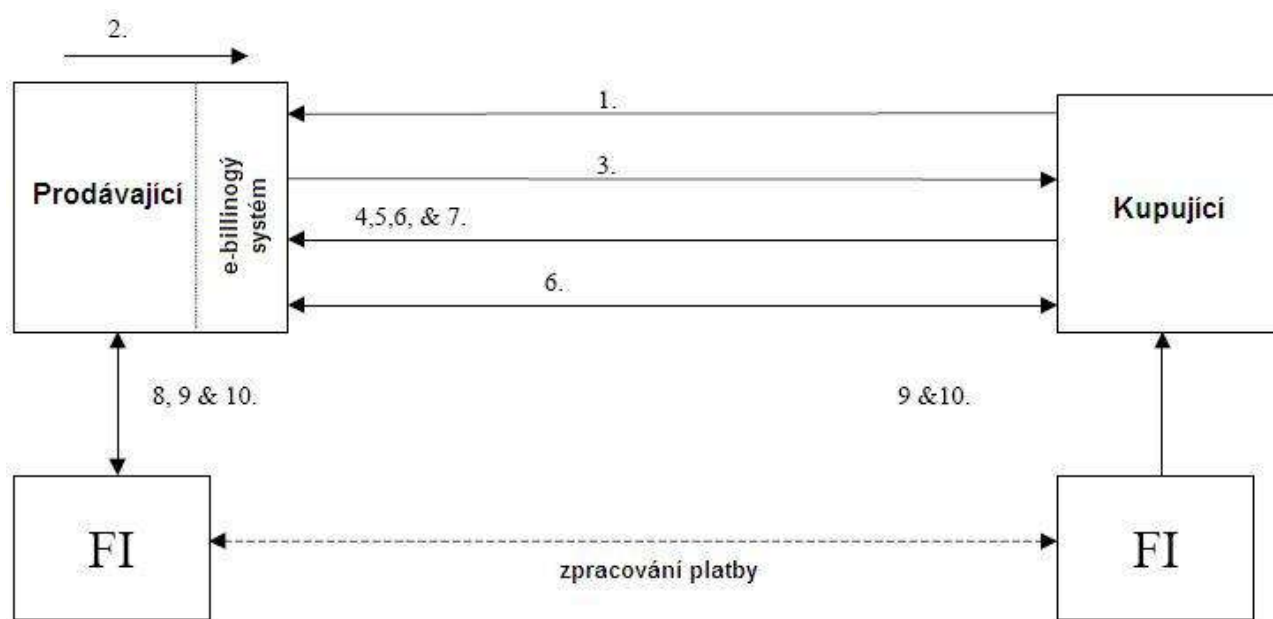
9.2.1 Model Seller Direct

Podstatou tohoto modelu je, že e-billingová aplikace je pod kontrolou prodávajícího – tedy toho, kdo dodává zboží či službu, fakturuje a přijímá platbu. Jedná se o model 1:N, kdy prodávající vyžaduje, aby zákazníci získávali jím vydané faktury z jeho systému. Systém často také obsahuje další funkce řízení pohledávek a závazků, nástroje pro řešení nesrovnalostí, analytické nástroje a funkce/nástroje umožňující platbu. Zákazník je na novou fakturu obvykle upozorněn e-mailovou zprávou.

Tento model je už poměrně zaběhlý a většinou se používá tam, kde již existuje určitý vztah mezi obchodními partnery a kde existují tedy již nějaká obchodní pravidla. Proávajícím bývá společnost, která vystavuje velké množství faktur.

Předpokladem je, že prodávající má dostatečně přesvědčivé nástroje k tomu, aby přiměl své zákazníky k akceptování tohoto modelu. Proávajícím je obvykle firma velké obchodní síly z oboru výroby, telekomunikací, finanční instituce a podobně. Pokud firma postrádá dominantní postavení, může nabízet svým zákazníkům určité výhody, jestliže oni přistoupí na tento model.

9.2.1.1 Průběh transakce



Obrázek 9.1: Průběh transakce v modelu Seller Direct

Zdroj: <http://www.ebilling.org/EIPP/B2b.pdf>

1 - Registrace do systému – obvykle probíhá na webových stránkách prodávajícího.

2 - Vystavení faktury v e-billingovém systému nebo jejího vložení do systému.

- 3 - Oznámení kupujícímu, že byla vystavena faktura.
- 4 - Přihlášení kupujícího do systému, kde je mu zobrazena příslušná faktura.
- 5 - Prohlédnutí faktury kupujícím. V závislosti na e-billingovém systému mohou být v tomto kroku odeslána potřebná data týkající se faktury do systému kupujícího.
- 6 - Řešení nesrovnalostí – součástí systému je nástroj, pomocí kterého může kupujícího upozornit na případné nesrovnalosti. Jeho námitky potom mohou být vyhodnoceny systémem automaticky nebo jsou odeslány na další analýzu zaměstnanci prodávajícího.
- 7 - Autorizace platby vnitřními obchodními procesy kupujícího (jejímž výsledkem je souhlas s úplným či částečným uhrazením faktury) a vlastní úhrada faktury – nakupující může fakturu uhradit plně nebo z části.
- 8 - Přijetí platby bankou prodávajícího.
- 9 - Ohlášení platby/úhrady prodávajícímu. V závislosti na e-billingovém systému může dojít k automatickému zaúčtování v účetním systému prodávajícího.
- 10 - Banka prodávajícího potvrdí provedení platby.

9.2.1.2 Přínosy a úskalí modelu pro jednotlivé účastníky

Výhodou pro prodávajícího je, že je schopen kontrolovat všechny stránky systému, co se týče formátu dat, grafické úpravy, řízení transakcí atd. Díky tomu je snadnější integrace e-billingového systému do dalších systémů podniku. Vzhledem k tomu, že zákazníci do systému nejčastěji přistupují přes webové stránky obchodníka, tak ten svůj Internetový portál může dobře využívat pro marketingové účely.

Na druhou stranu, prodávající nese veškeré investiční i provozní náklady, které se zavedením a provozováním systému souvisí a musí garantovat určitou dostupnost a bezpečnost systému. Další ne vždy jednoduchou záležitostí je přesvědčit zákazníky, aby tento model akceptovali, neboť pro ně to může být dosti složité. Navíc musí prodávající vycházet zákazníkům vstříc v tom ohledu, aby implementace tohoto modelu byla pro ně vůbec možná.

Na straně kupujícího jsou naopak velmi nízké náklady, v podstatě nulové, neboť jedinou nutnou aplikací je webový prohlížeč a elektronická pošta, což jsou aplikace dostupné v podstatě ve všech firmách. Navíc, v některých případech může kupující těžit z výhod, které prodávající nabízí za používání tohoto modelu.

Nevýhodou pro kupujícího je, že musí akceptovat systém „tak, jak je“, nemůže si dělat žádné úpravy, ani co se týče obchodních procesů ani technických specifikací, což může mít značný dopad na další vnitropodnikové systémy kupujícího. V případě velkého množství dodavatelů uplatňujících tento model musí řešit výše uvedené problémy několikrát.

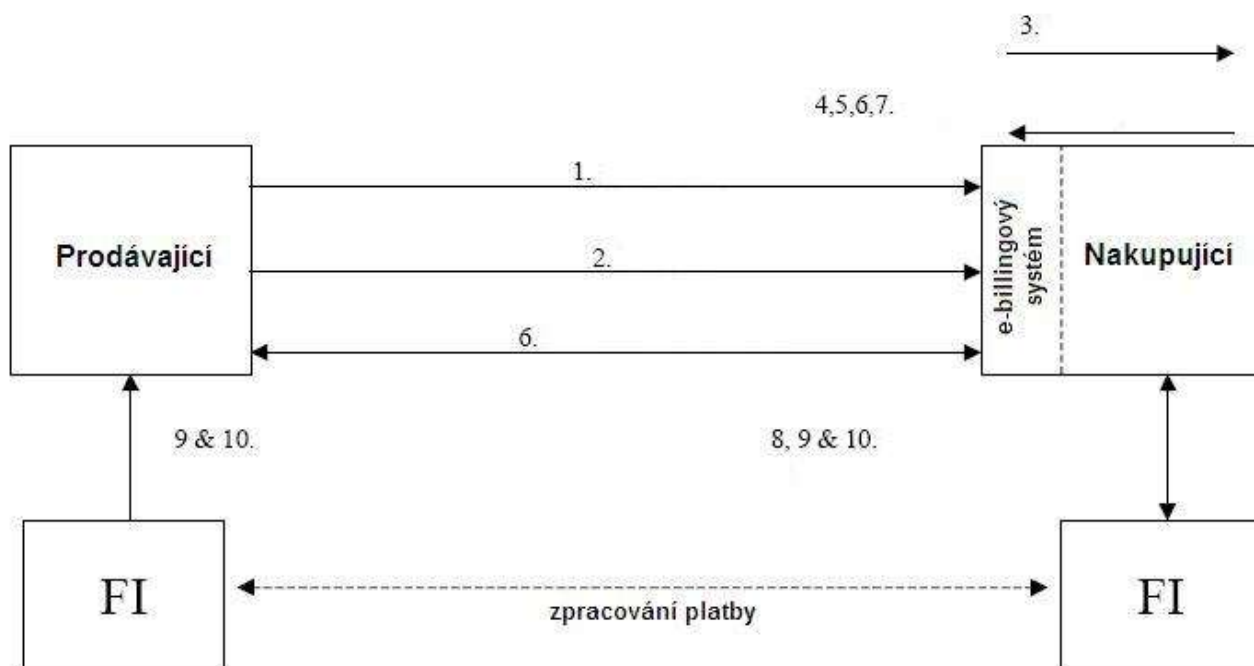
9.2.2 Buyer Direct

Tento model je opakem modelu předchozího – billingová aplikace je pod kontrolou kupujícího. Těž se jedná o model 1:N a systém také často obsahuje další funkce jako jsou řízení pohledávek a závazků, nástroje pro řešení nesrovnalostí, analytické nástroje, funkce/nástroje umožňující platbu a podobně. Stejně tak, jako u předchozího modelu, existuje již vzájemný vztah dodavatele a odběratele a obchodní pravidla jsou definovaná a známá.

U tohoto modelu je to zákazník (kupující), kdo vyžaduje, aby prodávající vložil fakturu do systému. Na rozdíl od předchozího systému Seller Direct se jedná o poměrně nový model, který se objevuje jako reakce na to, že právě kupující mívají v B2B transakcích velmi často dominantní pozici.

Model je vhodný zejména pro podniky, které objednávají a nakupují zboží od velkého množství dodavatelů.

9.2.2.1 Průběh transakce



Obrázek 9.2: Průběh transakce v modelu Buyer Direct

Zdroj: <http://www.ebilling.org/EIPP/B2b.pdf>

- 1 - Registrace do systému na webových stránkách kupujícího.
- 2 - Prodávající vydá fakturu a vloží ji do e-billingového systému kupujícího. Pochopitelně musí respektovat požadavky na formát faktury, které určil kupující

- 3 - Systém může informovat příslušného pracovníka kupujícího o tom, že byla do systému vložena nová faktura.
- 4 - Kupující (respektive příslušný pracovník odběratele) se podívá na fakturu, buď přes e-billingový systém nebo přes jiný vnitropodnikový systém, který umožní přístup k faktuře a který je do e-billingového systému napojen.
- 5 - Je zkontrolována faktura, aby mohla být předána k odsouhlasení.
- 6 - V případě nesrovnalostí nabídne systém nástroje pro jejich řešení.
- 7 - Autorizace platby vnitřními obchodními procesy kupujícího (jejímž výsledkem je souhlas s úplným či částečným uhrazením faktury) a vlastní úhrada faktury – nakupující může fakturu uhradit plně nebo z části.
- 8 - Banka kupujícího provede platbu.
- 9 - E-billingový systém provede aktualizaci dalších příslušných vnitropodnikových systémů.
- 10 - Banky potvrdí úspěšné provedení platební transakce.

9.2.2.2 Přínosy a úskalí modelu pro jednotlivé účastníky

Přínosy a problémy pro jednotlivé účastníky jsou stejné jako u předchozí modelu, ale to, co platilo pro nakupujícího, zde platí pro prodávajícího a naopak.

Přínosy pro kupujícího tedy jsou kompletní kontrola všech aspektů systému, možnost snadnější integrace do dalších vnitropodnikových systémů a aplikací, zatímco možnými problémy jsou výše investičních a provozních nákladů, nutnost přesvědčit prodávající, aby přistoupili na používání tohoto modelu e-billingového systému a podobně. Nutno však podotknout, že při velké obchodní síle kupujícího není přiměření dodavatelů k akceptaci tohoto modelu až tak problematické.

Výhodou pro prodávajícího mohou být nižší (až téměř nulové) náklady na provoz e-billingového systému (stačí základní kancelářské aplikace), rychlejší inkaso plateb a posílení vztahu s odběratelem (kupujícím). Mezi úskalí prodávajícího naopak patří složitější integrace do dalších vnitropodnikových aplikací, nutnost dodržovat podmínky nastavené kupujícím a podobně.

9.2.3 Model Consolidator

Jedná se o poměrně nový model, který se objevuje jako reakce na problémy, které vznikají u modelů Seller Direct a Buyer Direct.

Jedná se o model M:N, který slouží jako rozhraní pro kupující i pro prodávající. Kromě těchto dvou subjektů zde vystupuje ještě prostředník (Consolidator⁸³), kterých kromě e-billingového systému

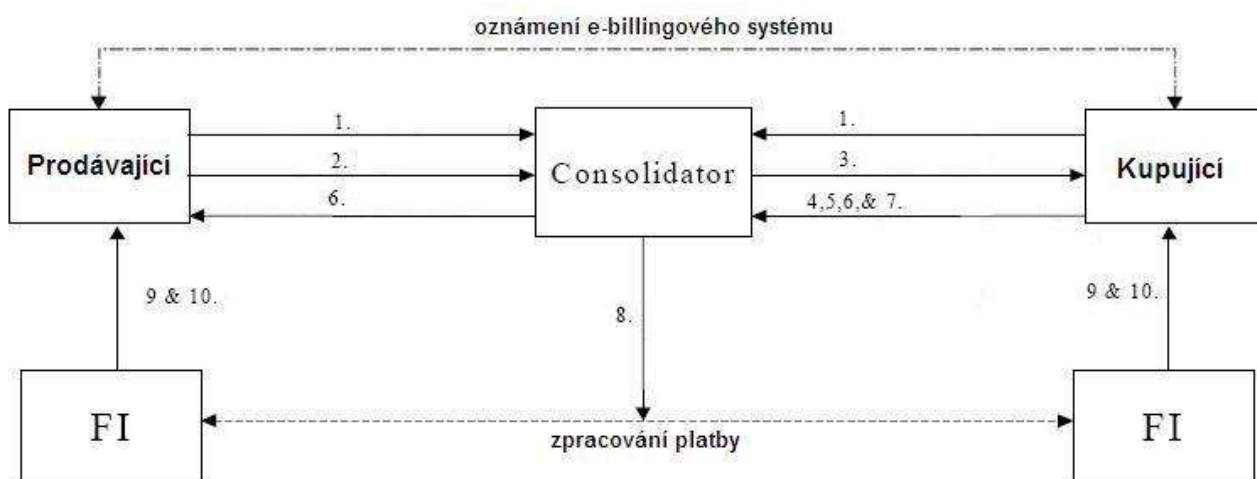
⁸³ Výraz consolidator by se dal do češtiny přeložit jako sjednotitel, nicméně překlad je dosti kostrbatý a proto je v textu běžně uváděn anglický výraz.

často nabízí další služby obvykle finanční povahy, jako je factoring (odkup krátkodobých pohledávek), pojištění, zpracování plateb a další služby.

Tento model je tedy použitelný jak pro kupujícího, tak pro prodávajícího, přechod na něj může iniciovat prodávající (neboť on faktury vystavuje a chce tedy po svých zákaznících, aby si je prohlíželi v konkrétním e-billingovém systému) nebo kupující (pro kterého je výhodné, aby dodavatelé ukládali faktury do e-billingového systému).

Systém může nabízet i dalších služby, funkce a nástroje, které byly uvedeny u předcházejících dvou systémů (funkce řízení pohledávek a závazků, nástroje pro řešení nesrovnalostí, analytické nástroje apod.) a samozřejmě obvykle má funkci automatického odeslání upozornění kupujícímu, pokud je do systému vložena nová faktura.

9.2.3.1 Průběh transakce



Obrázek 9.3: Průběh transakce v modelu Consolidator

Zdroj: <http://www.ebilling.org/EIPP/B2b.pdf>

1. - Kupující a prodávající se zaregistrují do systému na stránkách subjektu, který ho poskytuje (Consolidator). E-billingový systém pošle o této skutečnosti obchodním partnerům oznámení.
2. - Prodvávající vloží do systému fakturu podle pravidel definovaných Consolidátorem.
3. - Systém odešle oznámení kupujícímu, že mu byla vystavena faktura.
4. - Kupující se přihlásí do systému a prohlédne si svoji fakturu.
5. - Faktura je prohlédnuta kupujícím a případně odeslána do jeho vnitropodnikových systémů.
6. - Jsou řešeny případné nesrovnalosti – buď ručně anebo je systém řeší automaticky podle pravidel, která byla poskytnuta prodávajícím

7. - Kupující autorizuje platbu a systém započne s jejím uskutečňováním.
8. - Proveďte se platba.
9. - Je odeslána informace o provedení platby do systému prodávajícího, případně i kupujícího.
10. - Platba je potvrzena ještě standardním způsobem kupujícímu a prodávajícímu.

9.2.3.2 Přínosy a úskalí modelu pro jednotlivé účastníky

Přínosy i problémy tohoto modelu jsou pro prodávajícího i kupujícího podobné.

Přínosem určitě je, že prodávající/kupující může obsluhovat fakturaci z jednoho místa a že může využít služeb, které Consolidator nabízí, které by prodávající/kupující třeba neuměl zajistit. Samozřejmě lze také počítat s nižšími investičními náklady. U provozních nákladů už to není tak zřejmé a záleží na specifických podmínkách.

Velkou výhodou pro prodávajícího i kupujícího je, pokud Consolidator nabízí jako jednu ze služeb také konverzi různých formátů dat, což pak jednotlivým účastníkům značně usnadňuje integraci e-billingového systému do navazujících vnitropodnikových systémů či aplikací.

Naproti tomu nevýhod je u tohoto modelu více. Stejně jako u modelů Seller Direct či Buyer Direct je nutné přesvědčit obchodní partnery, aby tento systém používali. Dále musí být dodržována pravidla stanovená Consolidátorem a mohou nastat problémy s integrací e-billingového systému do vnitropodnikových systémů. Navíc systém nemusí umožňovat ideální komunikaci s obchodním partnerem.

Výhodou modelu samozřejmě je, že Consolidator může být zajímavý pro větší množství nakupujících a prodávajících a nemusí mít s nimi vždy dlouhodobější obchodní vztah – mnoho účastníků totiž do systémů vstoupí proto, že to po nich požaduje jejich obchodní partner.

9.3 Výhody a možné problémy e-billingu obecně

Mezi možné problémy patří:

První problémy či složitosti se patrně objeví při zavádění e-billingu. Přejít na e-billing totiž může být dosti pomalý a organizačně a technicky nejjednodušší. Vzhledem k těmto problémům lze očekávat v implementačním období výrazné zpomalení inkasa pohledávek, v horších případech i jeho zastavení.

Do procesu implementace, ale i dalšího běhu musí být významně zapojeno IT oddělení a musí dobře komunikovat s uživateli billingového systému. Uživatelé billingového systému musí dobře komunikovat nejen s IT oddělením, ale se všemi pracovníky, kteří mají s billingem něco do činění.

Dalším nárokem na pracovníky, kteří se nějakým způsobem podílejí na procesu billingu, je dostatek technických znalostí.

Jedním ze základních problémů při využívání e-billingu je také jeho integrace do navazujících vnitropodnikových systémů (typicky částí ERP).

Naopak výhodami jsou:

Výhody zavedení e-billingového systému mohou být finanční a nefinanční.

Co se týče nefinančních přínosů tak přichází v úvahu například značně zjednoduší sledování fakturačního procesu a snadněji a rychleji dostupné informace⁸⁴ pro management. Dále je to fakt, že není potřeba ručního vkládání dat o fakturách do systému a tedy následně i eliminace chyb při označování faktur. Dalšími výhodami mohou být zvýšení produktivity, zlepšení zákaznických služeb a tedy vztahů se zákazníky a rozvinutí dalších obchodních příležitostí⁸⁵. Samozřejmě také je třeba zmínit zlepšení vztahů s obchodními partnery (pokud obchodní partner použití e-billingového systému požaduje a podnik jej přijme). Mimoto management podniku určitě ocení zkrácení doby, která uplyne mezi vystavením faktury a přijetím platby za tuto fakturu, čímž už se dostáváme k finančním přínosům. S kratší dobou úhrad zcela jednoznačně souvisí zlepšení cash-flow podniku. Další přínosy jsou v úspoře nákladů a jsou jimi snížení nákladů spojených s chybami ve fakturách, se špatným vystavováním dokladů a dalšími chybami, které vznikají při vystavování faktur, snížení nákladů na manipulaci s fakturami, snížení nákladů na poštovné a tisk dokladů a určité snížení nákladů na zaměstnance. Příklad úspory nákladů - viz dále subkapitulu o nákladech na e-billing.

9.4 E-billing a legislativa Evropské Unie

Evropská Unie dospěla k rozhodnutí, že je třeba právně upravit nejen papírovou, ale také elektronickou⁸⁶ podobu daňových a dalších dokladů. EU vidí potřebu právního rámce pro elektronickou fakturaci pro to, aby bylo možné zajistit řádné fungování vnitřního trhu EU. Je tedy potřeba „na úrovni Společenství vypracovat harmonizovaný seznam údajů, které musí být uváděny na fakturách pro účely daně z přidané hodnoty, a zavést řadu společných opatření vztahujících se k elektronické fakturaci a elektronickému uchovávání faktur a k vlastnímu provádění a zadávání fakturačních operací“⁸⁷.

⁸⁴ Jestliže podnik obdrží fakturu dříve, management ji může dříve zahrnout do svých analýz a tedy i promítnout nové skutečnosti do rozhodovacích procesů.

⁸⁵ Zavedením e-billingového systému se podnikem například otevře možnost spolupráce s podniky, které e-billingový systém u svých obchodních partnerů vyžadují.

⁸⁶ Přenosem a uchováváním faktur "elektronickými prostředky" se rozumí přenos nebo zpřístupnění příjemci a uchovávání za užití elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat a využití přenosu po drátě, rádiového přenosu nebo jinými optickými nebo elektromagnetickými technologiemi.

⁸⁷ Směrnice Rady 2001/115/ES, důvod (4)

Údaje, které faktury, tedy i ty v elektronické podobě, musí minimálně obsahovat, jsou uvedeny v příloze „Náležitosti faktury“.

Uváděná směrnice povoluje uvádět ceny v jakékoli měně.

Faktury mohou být zasílány elektronicky jen v případě, že s tím zákazník souhlasí. Kromě této podmínky je však třeba zajistit, že „věrohodnost původu a neporušenost obsahu jsou zaručeny“⁸⁸. Ty mohou být zaručeny buď zaručeným elektronickým podpisem⁸⁹ nebo prostřednictvím elektronické výměny informací (EDI)⁹⁰. Věrohodnost původu a neporušenost obsahu, stejně tak jako čitelnost, faktur se vztahuje i na jejich uchovávání - jak uvádí Směrnice Rady 2001/115/ES ze dne 20. prosince 2001, kterou se mění směrnice 77/388/EHS s cílem zjednodušit, modernizovat a harmonizovat podmínky pro fakturaci ve vztahu k dani z přidané hodnoty (Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax).

9.5 Právní úprava e-billingu v ČR

Situace v oblasti vystavování faktur pouze v elektronické podobě je v České republice poněkud problematická a to z toho důvodu, že existuje několik výkladů současných zákonů a názory na tuto problematiku se liší.

V zásadě jsou pro tuto problematiku nejdůležitější dva zákony. A sice zákon o DPH a zákon o účetnictví. Problém je v tom, že zejména u zákona o účetnictví neexistuje jeho jednoznačný výklad ohledně toho, jestli vystavování faktur v elektronické podobě je či není možné.

Do budoucna bude patrně důležité, jak se k dané problematice postaví finanční úřady, případně jestli proběhne nějaké soudní řízení, jehož výsledkem by byl jasný výklad současné právní situace.

Další část této subkapitoly (podrobná analýza právní úpravy e-billingu v České republice) je obsahem důvěrné části diplomové práce.

⁸⁸ Směrnice Rady 2001/115/ES, článek 2 písm. c)

⁸⁹ Směrnice Rady 2001/115/ES přesně říká „zaručeným elektronickým podpisem ve smyslu čl. 2 odst. 2 směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy; členské státy však mohou požadovat, aby se zaručený elektronický podpis zakládal na kvalifikovaném osvědčení a byl vytvořen prostředky pro bezpečné vytváření podpisu ve smyslu čl. 2 odst. 6 a 10 uvedené směrnice;

⁹⁰ Tak jak ji vymezuje doporučení Komise 1994/820/ES ze dne 19. října 1994 v článku 2; členské státy však mohou za podmínek, které stanoví, požadovat souhrnný dokument na papíře.

9.6 Srovnání s klasickými systémy

9.6.1 Porovnání

	<i>E-billing</i>	<i>Papírové faktury</i>
Způsob doručení	Faktura může být doručena každé účtovací období na emailovou adresu zákazníka.	Faktura je doručena klasickou poštou.
Množství platebních možností	Vzhledem k větší flexibilitě lze u dodavatelů využívajících e-billing očekávat též nabízení většího počtu platebních možností.	Obvykle přibližně několik málo možností platby.
Uchovávání faktur	V elektronické podobě v počítači či na jiných médiích, případně je možné vytisknout a uchovávat v papírové podobě.	V podstatě jen v papírové podobě.
Úprava faktury	Může být i různá pro různé zákazníky, větší flexibilita, možnost zobrazení například barev podle vkusu.	Obvykle stejná pro všechny zákazníky.
Bezpečnost dat při přenosu	Data mohou být šifrována, ale není to podmínkou.	Bezpečnost dat je zaručena třetí stranou (pošta, tiskárna).
Právní úprava	Často se liší stát od státu.	Obvykle bývá i v různých státech podobná.
Přístup k faktuře	24 hodin denně, 7 dní v týdnu, odkudkoli na světě.	Po obdržení faktury je její znovuzískání obvykle složité.
Náklady (viz též dále)	Vyšší investiční na počátku, nižší na každou fakturu.	Investiční mohou být nízké, vyšší na každou fakturu.

9.6.2 Výhody, nevýhody a případné problémy

Způsob doručení

Pro zákazníka i vystavovatele je většinou elektronická cesta jednodušší. Faktura je doručena rychleji, případné problémy mohou být řešeny rychleji. V případě nedoručení není znovuvystavení nijak výrazněji problematické. Odpadají problémy s poštou.

Možnosti platby

Nabízené možnosti platby nemusí být přímo závislé na způsobu vystavování faktur. Na druhou stranu u elektronických faktur lze předpokládat možnost elektronické platby a navíc je zde možnost integrace – zákazník může být pouhým kliknutím přesměrován na platební bránu.

Uchovávání faktur

U elektronických faktur je možnost uchovávat fakturu buďto v elektronické nebo papírové podobě. V případě vytištění však mohou být problémy se zaručením pravosti. U klasický faktur pouze v papírové podobě⁹¹. Možnost volby je pro zákazníka přínosem, elektronické uchovávání faktur má výhody zejména v možnosti vyhledávání, jednoduší archivace apod. Na druhou stranu při uchovávání v elektronické podobě může docházet k problémům s prokazováním pravosti či s čitelností faktur – data mohou být uložena ve formátech, jehož čtení počítačem po několika letech může být problematické.

Úprava faktury

U elektronických faktur je možné, aby si zákazník nastavil, jak chce fakturu vidět. Například si může měnit barvu textu či grafiky, případně rozložení jednotlivých políček. Pro lidi s vadou zraku (barvoslepost) může být možnost nastavení barev klíčová.

Bezpečnost dat

Klasické faktury bývají často podepsány zodpovědnou osobou. Nároky na zaručení pravosti nejsou tak velké jako elektronického podepisování faktur. Navíc u elektronických faktur lze narazit na problémy týkající se právní úpravy tohoto tématu.

Právní úprava

V některých státech nemusí platná legislativa použití elektronických faktur vůbec umožňovat – například i v ČR existují v této oblasti stále určité otazníky. Navíc tato oblast je často upravována několika různými předpisy – například zákony o elektronickém podpisu (podepisování faktur), o účetnictví (přenos a uchovávání faktur), daňové zákony a další.

⁹¹ Elektronické uchovávání papírových faktur by bylo možné jen v případě naskenování faktury do počítače a její následné uchovávání tam. Nicméně faktura bude uložena jako obrázek a hlavně nebude pravděpodobně zaručena nijak její pravost.

Přístup k faktuře

U elektronických faktur je obvykle možno si je prohlížet 24 hodin denně, 7 dní v týdnu. Stačí k tomu přístup k Internetu a faktura může být zobrazena odkudkoli na světě. Naproti tomu papírové faktury lze prohlížet jen na místě, kde jsou uchovávány.

9.6.3 Náklady

Náklady na oba typy faktur jsou závislé na mnoha proměnných. U elektronických faktur je to zejména to, jestli podnik má vlastní systém nebo jestli využívá služeb třetích subjektů. U papírových faktur je to podobné, některé podniky si tisknou faktury samy, některé využívají služeb specializovaných tiskáren.

Záleží také na tom, jaké informace chce podnik zasílat společně s fakturou. Může se jednat o dodatečné informace týkající se zboží či služeb uvedených na faktuře nebo může jít o nějaké propagační či informační materiály. Samozřejmě dodatečné náklady na doručení těchto dalších informací jsou vyšší u papírových faktur, zejména proto, že se proporcionálně zvyšují náklady na tisk těchto dokumentů. Dále větší množství materiálů obvykle vyvolá vyšší náklady na poštovné. Naproti tomu u elektronických faktur jsou dodatečné náklady značně nižší – může se jednat třeba jen o odkaz na stránky dodavatele.

Obecně lze říci, že u elektronických faktur má podnik vyšší investiční náklady na zřízení takového systému, ale potom profituje z nižších nákladů na každou fakturu. Nejdříve je třeba převést data do vhodné formy, aby byla využitelná pro elektronickou fakturaci. Uvádí se⁹², že tyto náklady jsou v rozmezí 50 000 až 100 000 amerických dolarů. Kromě toho, jestliže chce podnik využívat systému provozovaného třetí stranou, zaplatí dalších cca. 35 000 až 50 000 USD za zřízení takového systému. Tyto náklady u papírových faktur odpadají.

Náklady na vytvoření jedné elektronické faktury činí, podle průzkumu společnosti Gartner Inc.⁹³, cca. 2 USD za každou elektronickou fakturu, zatímco náklady na vytvoření a doručení papírové faktury činí cca. 5 dolarů. Tato studie, jíž se zúčastnilo 100 velkých společností, které posílají v průměru 75 000 faktur/účtů měsíčně, dále říká, že podnik může elektronickou fakturací ušetřit až 2,7 miliónu USD ročně.

⁹² Zdroj: L. Gibbons Paul, "E-billing: The check is in the ether", http://itmanagement.earthweb.com/erp/article.php/11072_609781_3

⁹³ Ebilling can cut costs, <http://www.itworldcanada.com/a/CIO/072a65a2-2f4f-4014-94a4-1d28f5ea223e.html>

10 Závěry

Ne všechny platební systémy fungují stejně, ne všechny mají stejné výhody či nevýhody. Nejde jen o rozdíly mezi konkrétními platebními systémy, ale existují i rozdíly v tom, na jakém principu platební systémy fungují. Platební systémy můžeme tedy dělit podle několika hledisek.

Prvním je, zda-li se jedná o platební systémy, u nichž je ověření platby součástí nákupního procesu, nebo o systémy, u nichž ověření platby součástí nákupního procesu není.

Platební systémy, u kterých se ověření platby součástí nákupního procesu, lze dále dělit na ty, které používají virtuální účty, kde mají zákazníci uloženy své virtuální peníze. V České republice systémy tohoto typu běžně nenajdeme, pouze pokud bychom uvažovali i mikroplatební systémy. Systémem tohoto typu je například PayPal, jeden z nejrozšířenějších platebních systémů na světě. Systém PayPal je mezi uživateli Internetu značně populární, má dokonce více uživatelů než například společnost American Express. Systém nabízí mnoho výhod jak pro zákazníky, tak pro obchodníky, nicméně bohužel má své určité problémy týkající se bezpečnosti a omezování práv uživatelů. Tyto problémy vyústily hlavně ve Spojených státech amerických až v soudní spory. Některé z těchto problémů vznikají mimo jiné proto, že systém PayPal není považován, alespoň zatím, za banku a nepodléhá tedy tak přísným regulacím. Nicméně, v současné době se vedou diskuse o tom, jestli PayPal banka je či není. Výsledné rozhodnutí v této záležitosti bude mít pro PayPal dalekosáhlé důsledky. Navzdory všem možným problémům se však mnoho odborníků domnívá, že PayPal se stane de facto standardem pro Internetové platby a že počet jeho uživatelů se bude dále zvyšovat.

Dalším typem platebních systémů, u nichž je ověření platby součástí nákupního procesu jsou systémy využívající převody mezi bankovními účty. Mezi tyto systémy patří v České republice eBanka a NetBanka. Problém s těmito systémy ovšem je, že jsou vázány na konkrétní banku, čímž je omezen okruh zákazníků, kteří mohou tento systém využívat. Ač tyto systémy mohou být ve své podstatě dobré, tak právě díky tomuto omezení nelze čekat masovější rozšíření.

A konečně třetím typem tohoto druhu platebních systémů jsou systémy, v nichž se platí pomocí kreditních či debetních karet. V současné době existují v ČR dva způsoby implementace systémů tohoto typu. Buďto přes společnost Global Payments a její systém Pay MUZO a jednu z jejích partnerských bank, kterými jsou ČSOB či Komerční Banka anebo přes systém České spořitelny. Oba typy systémům jsou do značné míry podobné, oba používají zabezpečení pomocí technologie 3-D Secure, liší se hlavně obchodními podmínkami. Systém České spořitelny se v celkovém hodnocení jeví jako nejlepší, neboť kromě toho, že systém je bezpečný a důvěryhodný, Česká spořitelna nevyžaduje žádné poplatky ani za zavedení ani za používání tohoto systému, strhává si jen rozumné procento z každé transakce.

Druhým hlediskem, podle kterého lze platební systémy dělit, je výše maximální částky, kterou lze pomocí systému zaplatit. Rozlišujeme běžné platební systémy, u kterých není typicky částka omezována a mikroplatební systémy, pomocí nichž se platí částky ve výši haléřů až stovek korun. Přesná výše maximální částky se liší stát od státu, například Evropská Unie definuje jako mikroplatby transakce nepřesahující částku 15 EUR. S mikroplatebními systémy je to však v České republice poněkud složité, neboť současná legislativa jejich existenci velmi ztěžuje, ne-li přímo znemožňuje. Po zavedení této legislativy v roce 2002 přestala fungovat většina nejznámějších mikroplatebních systémů u nás. Ale i ty systémy, které se nějakým způsobem s nepříznivou legislativou vypořádaly, nejsou mezi uživateli českého Internetu nijak značně rozšířené.

Dalším hlediskem, které lze pro rozdělení platebních systémů použít, je zařízení, pomocí kterého se transakce provádí. Rozlišujeme běžné počítače (doma či v kanceláři) a mobilní zařízení, jakými jsou mobilní telefony či příruční počítače. Ani mobilní platby nejsou u nás zatím příliš rozšířené. Nejlépe se na tom zdá být T-Mobile, který umožňuje platbu mobilním telefonem v několika obchodech. Oskar/Vodafone nemá špatnou technologii m-plateb, ale bohužel v současné době je možné m-platby využít jen pro placení služeb poskytovaných tímto mobilním operátorem. EuroTel se v oblasti m-plateb nijak výrazněji neangažuje. Žádné větší výsledky nejsou viditelné ani ze strany Asociace pro mobilní platby.

Při hodnocení platebních systémů je třeba brát v potaz velký počet faktorů, některé ze základních faktorů uvádí následující tabulka, aby byla čtenáři dána určitá možnost srovnání. Pro hodnocení byly vybrány všechny platební systémy u nichž je ověření platby součástí nákupního procesu (neboť ty jsou hlavním předmětem této práce), dále mikroplatební systémy popisované v této práci a mobilní platby od T-Mobile (m-platby od ostatních dvou mobilních operátorů nebyly do hodnocení zařazeny, neboť vzhledem ke svému malému rozšíření by byly s ostatními uváděnými platebními systémy jen těžko srovnatelné). Tabulka hodnocení vychází z textu této práce a vyjadřuje hodnocení autora, které je založené na informacích, které vzešly z analýzy materiálů získaných v průběhu psaní této práce.

<i>Vlastnost</i>	<i>PayPal</i>	<i>eBanka</i>	<i>NetBanka</i>	<i>Pay MUZO</i>	<i>ČS</i>	<i>Monetka</i>	<i>i-plus</i>	<i>T-Mobile</i>
Náklady⁹⁴ pro zákazníky	Žádné	Žádné	Žádné	Žádné	Žádné	Žádné	Žádné	Žádné
Složitost pro zákazníky (založení / používání)	Jednoduché / jednoduché	Jednoduché / jednoduché	Jednoduché / jednoduché	Jednoduché / jednoduché	Jednoduché / jednoduché	Jednoduché / jednoduché	Jednoduché / střední ⁹⁵	Střední ⁹⁶ / jednoduché
Náklady pro obchodníka (založení / používání)	Nízké / střední ⁹⁷	Nízké / nízké	Nízké / nízké	Vysoké / vysoké	Nízké / nízké	N/A	Nepodařilo se zjistit	Nízké / pravděpodobně vysoké
Složitost zřízení pro obchodníka	Nízká až střední ⁹⁸	Střední	Střední	Vysoká	Střední	N/A	Střední	Střední
Rozšířenost⁹⁹ (v ČR / ve světě)	Žádná / Velmi velká	Střední / Žádná	Malá / Žádná	Velká / Žádná ¹⁰⁰	Velká / Žádná	Velmi malá / Žádná	Velmi malá / Velká ¹⁰¹	Malá / Žádná
Vhodnost pro mikroplatby	Ano i ne ¹⁰²	Ne	Ne	Ne	Ne	Ano	Ano	Ano
Anonymita¹⁰³	Ne	Ne	Ne	Ne	Ne	Ne	Ano	Ano i ne ¹⁰⁴
Přijímání plateb ze zahraničí	Ano	Ne	Ne	Ano	Ano	Ne	Ne	Ne
Reputace	Středně dobrá	Dobrá	Dobrá	Dobrá	Dobrá	Dobrá	Středně dobrá	Dobrá

Tabulka 10.1: Srovnání vybraných platebních systémů

⁹⁴ Máme na mysli dodatečné náklady; předpokládá se tedy, že jsou splněny určité podmínky (např. zákazník má účet u banky či je držitelem platební karty apod.)

⁹⁵ Po utracení kreditu je potřeba vždy najít prodejce a koupit si nový kupón.

⁹⁶ Je nutná registrace na www.t-zones.cz, která nějakou dobu zabere.

⁹⁷ Platí ve většině případů. Záleží však také na tom, jaký typ účtu obchodník má.

⁹⁸ Záleží na konkrétním řešení, které obchodník požaduje.

⁹⁹ Máme na mysli počet implementací u obchodníků.

¹⁰⁰ Co se týče implementace u českých bank.

¹⁰¹ Systém je však provozován pod jiným jménem.

¹⁰² PayPal je vhodný pro mikroplatby pouze při platbě z jednoho PayPal účtu na jiný PayPal účet, který je ještě navíc typu „Personal“. Pro platby uskutečněné kreditní/debetní kartou či pomocí bankovního účtu nebo v případě, že účet příjemce je typu „Business“ nebo „Premier“ PayPal pro mikroplatby vhodný příliš není.

¹⁰³ Zda-li je relativně nesnadné zjistit (i pro poskytovatele platebního systému) identifikaci plátce.

¹⁰⁴ Pro zákazníky využívající předplacených služeb Twist je anonymita možná, pro zákazníky mající některý z tarifů nikoli.

S problematikou platebních systémů úzce souvisí i otázka bezpečnosti. Obecně lze identifikovat rizika na straně obchodníka (nabourání do jeho systémů), rizika na straně uživatele (zneužití přihlašovacích údajů či údajů o platebních kartách) a rizika při přenosu dat. Rizika při přenosu dat lze řešit například šifrováním přenášených dat. Používá se obvykle protokol SSL, pro mobilní platby pak protokol SOAP-over-SSL. V současné době je pravděpodobně nejmodernější technologií technologie 3-D Secure vyvinutá společnostmi VISA a EuroCard/MasterCard používaná pro zabezpečení transakcí uskutečněných pomocí kreditní či debetní karty. Jedná se bezpečnou technologii, která má podporu nejen nejvýznamnějších hráčů působících v oblasti platebních karet, ale i velkých bank.

Co se týče problematiky e-billingu, tak existují tři modely. Jsou jimi modely Seller Direct, Buyer Direct a Consolidator. Jednotlivé modely mají jak výhody, tak nevýhody pro různé účastníky. Zavedení konkrétního modelu často závisí na ekonomické síle jedné ze stran. Problematika e-billingu v České republice není úplně jasná vzhledem k různým výkladům současných zákonů. Ač z uvedené analýzy vyplývá, že současná legislativa by neměla čistě elektronickou fakturaci vylučovat, existují i názory, které legislativu vykládají tak, že elektronická fakturace není v současné době možná. Rozhodující v této otázce bude pravděpodobně názor finančních úřadů na tuto problematiku, či případné soudní rozhodnutí, které by podávalo jasný výklad stávající legislativy.

Text práce tedy postihuje problematiku elektronických platebních systémů dostupných v České republice. Byly popsány a analyzovány běžné platební systémy, mikroplatební systémy a mobilní platby, uvedeny jejich silné a slabé stránky a výhody a nevýhody pro jednotlivé účastníky. Též byl poměrně zevrubně analyzován systém PayPal, čímž byla dána čtenáři možnost srovnání nejen mezi různými systémy dostupnými v ČR, ale i srovnání se světovým leaderem. U analyzovaných systémů byla také rozebrána otázka bezpečnosti, která je pro jejich životaschopnost klíčová.

Kromě platebních systémů byla nastíněna i problematika e-billingu, nebo-li elektronické fakturace, která v kombinaci s elektronickými platebními systémy umožňuje plnou elektronizaci celé transakce.

Tam kde to bylo vhodné, byla poskytnuta i právní analýza dané problematiky provedená na základě současné české legislativy.

Ačkoli nelze říci, že by dostupnost elektronických platebních systémů pro zákazníky a obchodníky byla v České republice ideální, lze konstatovat, že elektronické placení možné je a na jeho využívání stačí využít přiměřených zdrojů.

Definice pojmů

(Terminologický slovník)

<i>Termín</i>	<i>Význam</i>
Termíny přejaté z terminologického slovníku katedry informačních technologií	
HTTP	Protokol pro přenos dokumentů v → Internetu (používá se nejčastěji na → WWW)
SOAP	→ XML protokol 2. generace překonává slabiny předchozích dvou. Prostřednictvím mechanismu jmenných prostorů (→ XML Namespaces) je snadno rozšiřitelný. Kvůli podpoře binárních dat byl definován i protokol SOAP s attachmenty.
XML	XML (eXtensible Markup Language) je značkovací jazyk obsahující příkazy definující syntax (strukturu) dokumentu, definovaný doporučením → W3C (WWW Consortium). Navazuje na něj řada dalších standardů/technologií např. → DTD (Document Type Definition), → XSTL (XSL Transformations), → SOAP (Simple Object Access Protocol).
Další termíny	
3-D Secure	Systém pro zabezpečení transakcí prováděných platební kartou na → Internetu.
ACS	Access Control Server - server sloužící pro ověření klienta při každé prováděné transakci v systému → 3-D Secure.
Bezpečnostní kód	Kód, který je vytištěn na → kreditní/debetních kartě, ale není součástí jejího čísla. Používá se pro snížení rizika podvodu u plateb, kde není karta fyzicky přítomna, jako jsou platby přes → Internet.
CID	Card Identifier – → bezpečnostní kód na kartách American Express a Discover
CVC2	Card Validation Code – → bezpečnostní kód na kartách EuroCard/MasterCard
CVV2	Card Verification Value – → bezpečnostní kód na kartách VISA
Debetní karta	Platební karta, která je vázána k jednomu konkrétnímu bankovnímu účtu. Při provedení transakce se sníží zůstatek na účtu o hodnotu transakce. Použitelný zůstatek na účtu je zásadní pro určení, zda-li transakce bude autorizována nebo ne.
E-commerce	→ Elektronické podnikání.
Embosovaná karta	Platební karta, které má údaje vytištěné reliéfovým písmem.
GSM	Global System for Mobile communication – Původně evropský, ale v současné době i světový standard pro mobilní komunikace. Hovor uskutečněný v síti GSM je v digitální kvalitě a je kódován.
Imprinter	Off-line obchodní → platební terminál. Jedná se o mechanické zařízení umožňující platbu → kreditní či → debetní → embosovanou kartou v místech, která nejsou napojena on-line na ověřovací systém.
Kreditní karta	Platební karta, která není vázána ke konkrétnímu bankovnímu účtu. Dluh na kreditní kartě musí být následně vyrovnán. Kreditní karta má obvykle stanoven limit, který je důležitý pro určení, zda-li transakce bude autorizována či ne.

<i>Termín</i>	<i>Význam</i>
MPI	Merchant server Plug-In – Plug-in, který musí mít integrovány všechny → Internetové obchody, které chtějí využívat technologii → 3-D Secure. Tento plug-in umožňuje získat informace o klientovi a připojit se na → ACS.
PDA	Personal Digital Assistant – přenosné zařízení umožňující výpočetní, telefonní, faxové a síťové služby. PDA se často nazývá také → Palmtop či kapesní počítač.
PIN	Personal Identification Number – tajné číslo, které je známo pouze držiteli platební karty a slouží pro autorizace transakcí. Tento bezpečnostní prvek je však aplikován pouze u některých transakcí – vždy při výběru z bankomatu, někdy při platbě u obchodníka, avšak nikdy u plateb na Internetu. Pro Internetové platby se používá → bezpečnostní kód.
PKI	Public Key Infrastructure – systém digitálních certifikátů a certifikačních autorit, který ověřuje strany komunikující spolu v síti → Internet. Využívá šifrovací technologie založené na veřejných a soukromých klíších.
Platební brána	Rozhraní do sítě umožňující zpracování → kreditních/debetních karet. Typicky se jedná o kombinaci → hardware a → software.
Platební terminál	Často též označovaný jako POS (Point Of Sale) – terminál, ať už on-line nebo off-line, používaný pro čtení informací zaznamenaných na platebních kartách.
RPC	Remote Procedure Call – umožňuje volání procedur na jiných počítačích v síti
S-HTTP	Secure Hypertext Transmission Protocol – nadstavba protokolu → HTTP umožňující bezpečné posílání souborů v síti → WWW.
SET	Secure Electronic Transaction – standard pro posílání citlivých údajů, jako je číslo → kreditní karty a podobně, v síti → Internet.
SIM	Subscriber Identity Module – karta, obsahující informace jako je telefonní číslo, údaje o síti, → PIN kód a další data jako například telefonní seznam apod. SIM karta je potřeba k reálnému "oživení" mobilního telefonu.
SSL	Secure Socket Layer – protokol využívající šifrování pro zabezpečený přenos dat v → Internetu.
STT	Secure Transaction Technology – softwarová technologie umožňující bezpečný způsob zpracování finančních transakcí v elektronických sítích.
VISA directory	Systém, který přes → Internet poskytuje informace o vydavatelích platebních karet a o umístění jejich → ACS.
WAP	Wireless Application Protocol – komunikační protokol používaný pro přístup mobilních zařízení, jako například mobilních telefonů, do sítě → Internet
WIM	Wireless Identity Module – místo v mobilním telefonu, kde jsou bezpečně uloženy informace, které se přenášejí při transakcích uskutečněných protokolem → WAP
WTLS	Wireless Transport Layer Security – protokol, který umožňuje zabezpečenou komunikaci na protokolu → WAP

Seznam obrázků

- Obrázek 2.1: Platební karta BankAmericard (dnes známá jako VISA)
- Obrázek 2.2: Schéma fungování SET
- Obrázek 3.1: Rozdělení platebních systémů podle způsobu ověření platby
- Obrázek 3.2: Rozdělení platebních systémů podle zařízení použitého pro provedení platby
- Obrázek 3.3: Rozdělení platebních systémů podle objemu plateb
- Obrázek 4.1: Imprinter
- Obrázek 4.2: Průběh platby v systému PayPal
- Obrázek 4.3: Schéma fungování PayPal Website Payments Pro
- Obrázek 4.4: Počet účtů jednotlivých poskytovatelů finančních služeb (v milionech)
- Obrázek 4.5: Schéma fungování Pay MUZO
- Obrázek 5.1: Schéma fungování mikroplatby při poskytování on-line obsahu
- Obrázek 6.1: Schéma fungování m-platby u T-Mobile
- Obrázek 7.1: Umístění kódu CVV2 na platební kartě VISA
- Obrázek 7.2: Logo MasterCard SecureCode
- Obrázek 7.3: Logo VERIFIED by VISA
- Obrázek 7.4: Tři domény v 3-D Secure
- Obrázek 7.5: Průběh transakce v systému 3-D Secure
- Obrázek 9.1: Průběh transakce v modelu Seller Direct
- Obrázek 9.2: Průběh transakce v modelu Buyer Direct
- Obrázek 9.3: Průběh transakce v modelu Consolidator

Přehled literatury a zdrojů

Knihy

- Donát, J.: E-Business pro manažery, 1. vyd. Praha: Grada 2000. 84s. ISBN 80-247-9001-7
- Ellinger, E. P., Lomnicka, E., Hooley, R.: Modern Banking Law, 3. vyd. Oxford: Oxford University Press 2002. 920s. ISBN 0199248311
- Evans, D. S., Schmalensee R.: Paying with Plastic: The Digital Revolution in Buying and Borrowing, 2. vyd. Cambridge: The MIT Press 2005. 360s. ISBN 0-262-55058-X
- Garfinkel S., Spafford G., Schwartz A.: Practical Unix and Internet Security, 3. vyd. Sebastopol: O'reilly & Associates 2003. 954s. ISBN 0-596-00323-4
- Kou, W.: Payment Technologies for E-Commerce, 1. vyd. New York: Springer 2003. 344s. ISBN 3-540-44007-0
- McClure, S., Scambray, J., Kurtz, G.: Hacking bez tajemství, 3. vyd. Brno: Computer Press 2003. 612s. ISBN 80-722-6948-8
- O'Mahony, D., Peirce, M., Tewari, H.: Electronic Payment Systems, 1. vyd. Norwood: Artech House Publishers 1997. 254s. ISBN 0-89006-925-5
- Radu, C.: Implementing Electronic Card Payment Systems, 1. vyd. Norwood: Artech House Publishers 2002. 484s. ISBN 1-58053-305-1

Články

- Bureau of National Affairs. "Electronic Payments: Paypal Funds Eligible for Pass-Through Insurance From FDIC as Deposits by Agent", BNA Newsletter, Vol 7 No. 12, March 20, 2002, p.254.
- Cox, P.: PayPal and FBI team up. Wall Street Journal, US edition, 2001. ISSN 1815-8455.
- Hof, R. D.: PayPal spreads its wings. BusinessWeek, květen 2005. ISSN 0007-7135.
- Kment, V.: Ryze elektronické účetnictví zatím není možné. Computerworld č. 36, 2005, s. 16. ISSN 0010-4841.
- Sapsford, J.: PayPal Sees Torrid Growth With Money-Sending Service. The Wall Street Journal, February 16, 2000. ISSN 0002-371X
- Sorkin, D. E.: Payment Methods for Consumer-to-Consumer Online Transactions. 35 Akron Law Review 1, 2001. ISSN 1815-8455
- Wolverton, T.: PayPal not a bank. CNet News, March, 2002.

Další zdroje

Abrazhevich, D.: Classification and Characteristics of Electronic Payment Systems. Disertační práce obhájená na Technical University of Eindhoven.

Akron Beacon Journal ze dne 7. dubna 2005

Directive 94/19/EC of the European Parliament and of the Council of Europe of 16 May 1994 on deposit-guarantee schemes, OJ L 135, 1994.

Direktiva 2000/12/EC Evropského parlamentu a Evropské Rady z 20. března 2000 týkající se podnikání kreditních institucí, OJ L 126/1 2000, článek 1.

Financial Services and Markets Act 2000 (FSMA).

González A. G: PayPal and eBay: The legal implications of the C2C electronic commerce model. Prezentace uvedená na osmnácté konferenci BILETA: Controlling Information in the Online Environment. Londýn, duben 2003.

PayPal User Agreement

Směrnice Rady 2001/115/ES ze dne 20. prosince 2001, kterou se mění směrnice 77/388/EHS s cílem zjednodušit, modernizovat a harmonizovat podmínky pro fakturaci ve vztahu k dani z přidané hodnoty.

Zákon č. 124/2002 Sb. O převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku).

Zákon č. 227/2000 Sb. O elektronickém podpisu

Zákon č. 235/2004 Sb. O Dani z přidané hodnoty

Zákon č. 563/1991 Sb. O účetnictví

Internetové odkazy¹⁰⁵

AboutPayPal.org: Another California Class Action Suit against PayPal.

http://www.aboutpaypal.org/paypal_lawsuit

Armand Rousso.com: Armand Rousso. <http://www.armandrousso.com/about.htm>

Asociace pro elektronickou komerci: APEK pro manažery.

<http://www.apek.cz/appek/appek.nsf/Edit/%C3%9Avod~Pro%20mana%C5%BEery?Open&area=%C3%9Avod&grp=Pro%20mana%C5%BEery&lng=>

Barnfield, T., John, R., Luks, L., Williamson, P.: Electronic Billing.

<http://www.alanet.org/conf/handouts/FM21.ppt>

Cash Flow Specialists, Inc.: Glossary. <http://www.cashflowspecialistsinc.com/glossary/#P>

Catt: Mikroplatební systémy a Monetka. http://catt.bloguje.cz/72679_item.php

¹⁰⁵ Pokud není u odkazu uvedeno jiné datum, odkazy jsou funkční ke dni 22.12.2005

CP Books, a. s.: Jak je to bezpečné. <http://www.monetka.cz/Layout/Public/Pages/Safety.asp>

CP Books, a. s.: Jak naplnit peněženku. <http://www.monetka.cz/Layout/Public/Pages/Charge.asp>

CP Books, a. s.: Jak platit na internetu. <http://www.monetka.cz/Layout/Public/Pages/Payments.asp>

Česká společnost pro systémovou integraci: Budoucnost ebillingu v České republice.

http://www.cssi.cz/publ_si_clanek.asp?typ=1&kod=229

Česká spořitelna, a.s.: Akceptování platebních karet - platby kartou na internetu.

http://www.csas.cz/banka/application?pageid=documentpage03&docid=5400/Ostatni/SC_NW01_024781.htm&portal=internet&lang=cs&navid=nav11025_akceptovani_pl_karet_pl_internet&type=cms&tree=firmy_mesta&segment=segment03

Český Telecom, a.s.: Auditované finanční výsledky Českého Telecomu za rok 2004.

http://www.telecom.cz/infocentrum/tiskove_centrum/tiskove_zpravy/clanek.php?tz=21032005_1

Ebanka, a.s.: Platební systém eBanky. http://www.ebanka.cz/FF_PlatebniSystemEBanky.htm

Ebanka, a.s.: Zamykání platební karty. http://www.ebanka.cz/OFF_ZamykaniPlatebniKarty_PP.htm

Ebilling.org: Business-to-Business EIPP: Presentment Models and Payment Options.

<http://www.ebilling.org/EIPP/B2b.pdf>

Ebilling.org: Welcome to eBilling.org. <http://www.ebilling.org/default.html>

Ellinogermaniki Agogi: Payment Protocol SET.

<http://www2.ellinogermaniki.gr/ep/agroweb/htmls/lessons/commerce1/423.htm>

Eurotel Praha, s.r.o.: Go přináší platby mobilním telefonem.

http://www.eurotel.cz/jnp/cz/companyInfo/pressCenter/cz-companyInfo-pressRelease-2002-pr_2002_09_121.html

Federal Financial Institutions Examination Council: Glossary.

<http://www.ffiec.gov/ffiecinfobase/booklets/Wholesale/18.html>

Gemplus solution: i-plus on line prepaid solution pro nákup datových služeb na internetu.

<https://www.i-plus.cz/> [11.12.2005]

Global Payments Europe: Nabídka pro obchodníky.

http://www.muzo.com/download/gp_paymuzo.pdf

Global Payments, Inc.: Bezpečné platby na webu.

<http://www.globalpaymentsinc.com/Europe/czech/products/secure-web.html>

Gpayments: Visa 3-D Secure vs. MasterCard SPA. http://www.gpayments.com/pdfs/GPayments_3-D_vs_SPA_Whitepaper.pdf

Gulf Coast Educators Federal Credit Union: CVV2 & CVC2 Information.

<http://www.gcefcu.org/images/card.htm>

Hřebabecký, J.: Co jsou mikroplatby.

<http://www.supersvet.cz/rservice.php?akce=tisk&cislocianku=2005071301>

Indira Gandhi National Open University: Electronic Payment Systems.

<http://www.ignou.ac.in/virtualcampus/adit/course/cst304/ecom2.htm>

Information Gatekeepers Inc.: Gartner survey shows PayPal leading the online P2P payment market;

Market Intelligence. <https://www.paypal.com/html/gartner-020102.html>

Internet Info, s.r.o.: Slovníček pojmů. <http://www.mesec.cz/ucty-a-karty/platebni-karty/pojmy/>

Jupitermedia Corporation : SSL: Your Key to E-commerce Security.

<http://www.webopedia.com/DidYouKnow/Internet/2005/ssl.asp>

Jupitermedia Corporation : SSL. <http://www.webopedia.com/TERM/S/SSL.html>

Kaščejev, D.: Co jsou elektronické peníze (Čto takoe elektronie deňgi).

<http://www.webcorp.ru/page/oemoney.html>

Kosek, J.: Využití webových služeb a protokolu SOAP při komunikaci.

<http://www.kosek.cz/diplomka/html/websluzby.html>

Maine State Legislature Office of the Revisor of Statutes: Commerce and Trade - Definitions.

<http://janus.state.me.us/legis/statutes/10/title10sec9402.html>

Microsoft Corporation: Stručný slovník technických pojmů.

<http://www.microsoft.com/cze/enterprise/eai/slovník.asp>

Micheloud & Co.: CVV2 and CVC2 security codes.

<http://switzerland.isyours.com/e/faq/CVV2.html>

Ncipher Corporation Ltd.: Securing 3-D Secure.

<http://www.ncipher.com/resources/downloads/files/datasheets/3d-secure.pdf>

Oskar Mobil, a.s.: Co to jsou M-Platby?. http://www.oskarmobil.cz/services/m_platby.php

PayPal: Data Security and Encryption. [https://www.paypal.com/cgi-](https://www.paypal.com/cgi-bin/webscr?cmd=p/gen/security-outside)

[bin/webscr?cmd=p/gen/security-outside](https://www.paypal.com/cgi-bin/webscr?cmd=p/gen/security-outside)

PayPal: Choose the Right Payment Solution for Your Business. [https://www.paypal.com/cgi-](https://www.paypal.com/cgi-bin/webscr?cmd=_profile-comparison)

[bin/webscr?cmd=_profile-comparison](https://www.paypal.com/cgi-bin/webscr?cmd=_profile-comparison)

PayPal: Merchant Tools. https://www.paypal.com/cgi-bin/webscr?cmd=_merchant-outside

PayPal: Multiple Currencies. [https://www.paypal.com/cgi-bin/webscr?cmd=p/sell/mc/mc_intro-](https://www.paypal.com/cgi-bin/webscr?cmd=p/sell/mc/mc_intro-outside)
[outside](https://www.paypal.com/cgi-bin/webscr?cmd=p/sell/mc/mc_intro-outside)

PayPal: PayPal Helps Keep You Safe. [https://www.paypal.com/cgi-](https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecurityFraud-outside)

[bin/webscr?cmd=xpt/general/SecurityFraud-outside](https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecurityFraud-outside)

PayPal: PayPal Shipping Center. [https://www.paypal.com/cgi-bin/webscr?cmd=p/ship/center-](https://www.paypal.com/cgi-bin/webscr?cmd=p/ship/center-outside)
[outside](https://www.paypal.com/cgi-bin/webscr?cmd=p/ship/center-outside)

PayPal: Send Money. <https://www.paypal.com/cgi-bin/webscr?cmd=p/ema/index-outside>

PayPal: Sign Up for a PayPal Account. https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run#

PayPal: Transaction Fees for Domestic Payments—United States. https://www.paypal.com/cgi-bin/webscr?cmd=_display-receiving-fees-outside

PayPal: Use PayPal for Fast, Easy, and Secure Payments Worldwide. https://www.paypal.com/cgi-bin/webscr?cmd=_display-approved-signup-countries-outside

PayPal: What Is PayPal?. <https://www.paypal.com/cgi-bin/webscr?cmd=xpt/bizui/WhatIsPayPal-outside>

Piják, M.: Platit z mobilu jde stále snadněji. <http://www.mesec.cz/clanky/platit-z-mobilu-jde-stale-snadneji/>

T-Mobile Czech republic, a.s.: Seznam obchodníků pro m-platbu. <http://t-mobile.cz/Web/Business/TarifySluzby/MobilniPlatby/SeznamObchodnikuProM-platbu.aspx>

T-Mobile Czech republic, a.s.: T-Mobile m-platba. <http://t-mobile.cz/Web/Partnership/PreProdukty/T-MobileM-platba.aspx>

Telekurs Card Solutions AG: 3D-Secure. <http://www.saferpay.com/threedsecure.asp>

Thales e-Security: 3-D Secure. http://www.thales-ecurity.com/Solutions/3D_Secure.shtml

VeriSign, Inc.: PayPal to Acquire VeriSign's Payment Gateway Business; eBay and VeriSign Form Strategic Alliance for Online Commerce and Security. http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_035983.html

Villusion, a.s.: Společnost Villusion připravuje jako první v ČR systém eSIPO pro zpracování a rozesílání elektronických účtů a plateb. <http://www.villusion.cz/index.phtml?lang=cz&ref=newspressrelease20020415> [16.10.2005]

Visa International: 3-D Secure: Introduction. http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf

Visa International: 3-D Secure: System Overview. http://international.visa.com/fb/paytech/secure/pdfs/3DS_70015-01_System_Overview_external_v1.0.2_May_2003.pdf

Visa U.S.A.: History (of Visa). http://usa.visa.com/about_vis/about_vis_usa/history.html

Živnostenská banka, a.s.: Platební brána. http://www2.zivnobanka.cz/netbanka/platebni_brana.html

Přílohy

Náležitosti faktury (zdroj: Směrnice Rady 2001/115/ES)

- datum vydání,
- pořadové číslo založené na jedné nebo více sériích, které jednoznačně určuje fakturu,
- identifikační číslo plátce daně z přidané hodnoty, pod nímž osoba podléhající dani dodala zboží nebo poskytla služby,
- identifikační číslo plátce DPH (je-li zákazník povinen platit daň z dodaného zboží nebo poskytnutých služeb nebo bylo-li mu dodáno zboží podle čl. 28c části A, uvedené v odst. 1 písm. c)), pod nímž mu bylo zboží dodáno nebo služby poskytnuty,
- plné jméno a adresa osoby podléhající dani a jejího zákazníka,
- množství a druh dodávaného zboží nebo rozsah a druh poskytovaných služeb,
- den, kdy bylo uskutečněno nebo dokončeno dodání zboží nebo poskytování služeb, nebo den, kdy byla provedena platba na účet uvedená v písm. a) druhém pododstavci, pokud jej lze určit a liší se ode dne vystavení faktury,
- základ daně pro každou sazbu nebo osvobození, jednotková cena bez daně a veškeré slevy nebo rabaty, pokud nejsou obsaženy v jednotkové ceně,
- použitá sazba DPH,
- splatná částka daně, není-li použit zvláštní režim, pro který tato směrnice tento údaj nepřipouští,
- v případě osvobození od daně nebo je-li daň povinen zaplatit zákazník, odkaz na příslušné ustanovení této směrnice, na odpovídající vnitrostátní ustanovení nebo na jakýkoli údaj o tom, že dodání je osvobozeno od daně nebo předmětem postupu zpětného vyúčtování,
- jde-li o dodání nových dopravních prostředků ve Společenství, údaje uvedené v čl. 28a odst. 2,
- je-li používán režim rozdílů, odkaz na článek 26 nebo 26a, na odpovídající vnitrostátní ustanovení nebo na jakýkoli jiný údaj, že byl použit režim rozdílů,
- je-li osoba podléhající dani daňovým zástupcem ve smyslu čl. 21 odst. 2, identifikační číslo plátce DPH tohoto daňového zástupce, uvedené v odst. 1 písm. c), a jeho plné jméno a adresa.