VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

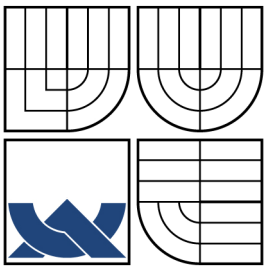
FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

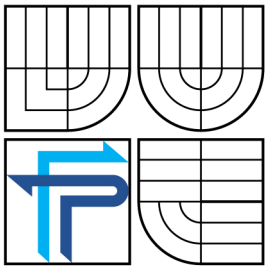
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VLASTIMIL ŠIMČÍK
AUTHOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFROMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ELEKTRONICKÉ PLATEBNÍ SYTÉMY
ELECTRONIC BANKING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VLASTIMIL ŠIMČÍK
AUTHOR

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

BRNO 2009

Vysoké učení technické v Brně | Akademický rok: 2008/2009
Fakulta podnikatelská | Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Šimčík Vlastimil

Manažerská informatika (6209R021)

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

Elektronické platební sytémy

v anglickém jazyce:

Electronic banking

Pokyny pro vypracování:

Úvod
Systémové vymezení problému
Cíl práce
Přehled informačních zdrojů světa
Použité metody řešení problému
Současný stav řešené problematiky
Analýza problému
Návrh řešení
Zhodnocení návrhu řešení
Závěr
Seznam použitých informačních zdroju
Přílohy

Seznam odborné literatury:

PRÁDKA, M., KALA J. Elektronické bankovnictví, 1. vyd. Praha: Computer Press, 2000. ISBN 80-7226-328-5.
GRUBLOVÁ, E. aj. Internetová ekonomika, 1. vyd. Ostrava: Repronis, 2002. ISBN 80-7329-006-6.
TONDR, L. Podnikáme s Internetem, 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-729-9.
FRANCU, M. Internet pro podnikatele, 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-623-3.
VRABEC, V., WINTER, J. Internet, podnikatelská príležitost nebo hrozba?, 1. vyd. Praha: Management Press, 2000. ISBN 80-7261-026-0.

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

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2008/2009.

L.S.

Ing. Jirí Kríž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 26.05.2009

Abstrakt

Tato práce pojednává o elektronických platebních systémech (EPS) v rámci E-Commerce, se zaměřením hlavně na jejich rozdělení a požadavky na zabezpeční těchto transakcí, jakožto i o stručný nástin jak historie a tak i výhledu do budoucna. Cílem je ukázka aplikace EPS jako součásti funkčního obchodního celku budoucnosti.

Klíčová slova

Elektronická komerce, Elektronické bankovnictví, Elektronické peníze,
Elektronické platební systémy, Kryptografie, Transakce

Abstract

This work deals with electronic payment systems (EPS) in the context of E-Commerce, focusing mainly on their distribution and the security of these transactions, as well as a brief outline of history and as well as prospects. The aim is to sample application EPS as part of a functional business unit future.

Key words

E-Commerce, E-Banking, E-Money, EPS, Kryptography, Transaction

Bibliografická citace VŠKP dle ČSN ISO 690

ŠIMČÍK, V. *Elektronické platební systémy.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. 61 s. Vedoucí bakalářské práce Prof. Ing. Jiří Dvořák, DrSC.

Čestné prohlášení

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

V Brně, dne 29. května 2009 . . . . . .

podpis

Poděkování

Na tomto místě bych rád poděkoval zejména mé rodině a mým přátelům, kteří mne podporovali při mých studiích a i když to občas nebylo lehké, vždy mi dokázali podat pomocnou ruku a podpořit mne. Dále bych rád poděkoval profesorskému sboru a vedení fakulty za příjemné prostředí a atmosféru, kterou dokázali vytvořit během výuky a že nám studentům vždy dokázali vyjít vstříc a podat pomocnou ruku v nesnázích.

Obsah:

Úvod

Jako téma své bakalářské práce jsem si zvolil analýzu eletronických platebních systémů, používaných v současné době v rámci elektronického bankovnictví a elektronické commerce vůbec.

V současné době se totiž již elektronické bankovnicví, ale vůbec, veškerá E-commerce stala běžnou součástí denního života firem i jednotlivců a do budoucnosti se bude tato „zavislost“ stále více prohlubovat, neboť tzv. elektronická cesta, se svojí schopností přenosu dat rychlostí jinak nedosažitelnou, nám již v současné době naznačuje možnosti, které nelze dobudoucna nejen nevyužít, ale přímo i naznačuje cesty, kterými je nutno se zabývat. Ať už to bude přímo o elektronických platbách, nebo o dalších možnostech elektronických médii, jako různé průzkumy trhu, reklamní činnost, statistické možnosti a spoustu jiných.

V první teoretické části se budu podrobněji věnovat něco historii platebních systémů vůbec, poté historii elektronických platebních systémů až k současnému stavu. Dále se budu zabývat rozdělením platebních systémů z různých hledisek, ať už dle platebního instrumentu, formy vzájemné komunikace mezi entitami nebo doby mezi příkazem k platbě a samotným převodem peněz a mnoha dalšímy charakteristikami. Druhá teoretická část se bude zabývat zabezpečení eletronických plateb a elektronických transakcí vůbec, jak zabezpečit jejich důvěryhodnost, integritu, bezpečnou autorizaci, interoperabilitu, dostupnost a spolehlivost, anonymitou a utajením transakcí atd.

V části praktické se potom pokusím nastínit využití elektronických platebních systému v praxi a modelovat plně automatizovaný nákupní systém s vyčleněním lidské síly pouze do role kontrolni, bezpečnostní a podpůrné a zhodnotit přínos tohoto jak z hlediska prodávajícího, tak z hlediska nakupujícího.

1. Vymezení problému a cíle

1.1. Vymezení problému

Účelem této práce je zanalyzovat současnou situaci na trhu s elektronickými platebnímy systémy, vytvořit přehled o jejím využití a na základě těchto poznatků navrhnout vlastní návrh implementace EPS do společensky užitného procesu.

1.2. Cíl práce

Cílem mé práce je návrh automatického nákupního systému pro použití v super a hypermarketech, který by měl odstranit nejen činitele negativně působící na nakupující, ale bude navíc ekonomicky výhodný i pro provozovatele.

1.2.1. Užitý metodologický aparát

Při zpracování své bakalářské práce budu využívat logicko systematickou metodu pro nalezení optimálního modelu.

Logicko systematická metoda na nalezení optimálního modelu

Postup v případě metody:

- analyzuji současnou situaci, znázorním základní prvky
- k základním prvkům přidám nové poznatky a názory získané studiem a diskusemi a analyzuji je
- následně na základě předchozích analýz zformuluji závěry
- po zanalyzování a formulaci všech nových závěrů, a přidání všech nových poznatků, dojdu k hledanému cíli.

Vymezení způsobů získávání autentických a objektivních informací a jejich zdrojů

- tématická literatura
- internet
- materiály institucí, které tvoří, používají nebo se zabývají EPS a průzkumy veřejného mínění
- komunikace s uživateli

2. Teoretické poznatky

2.1. Trocha z historie

2.1.1. Historie obchodu a peněz

Ve velmi dávné historii, na počátku samého obchodování, když ještě nebyly vynalezeny peníze, se obchodovalo ve své nejprimitivnější formě tzv. barteru, což je přímá výměna zboží a služeb za jiné zboží a služby. Postupem času však toto obchodování bylo více a více komplikovanější, a tak byl barter nahrazen různými formami peněz. Prvními penězi se staly fyzické komodity, jejichž hodnota byla velmi dobře známa (kukuřice, sůl, zlato). V důsledku několika žádoucích vlastností, jako byla například přenositelnost či dělitelnost, se stalo zlato a stříbro nejužívanějším platidlem a to asi do začátku 19. století.

Dalším krokem ve vývoji peněz bylo používání mincí a papírových bankovek, které již známe z vlastní zkušenosti. Důvěryhodnost peněžního systému byla garantována místní, národní či mezinárodní bankou, která kontrolovala tisk nových bankovek a ražbu nových mincí. Platba v hotovosti pomocí mincí a bankovek se stala a stále je nejpoužívanější formou směny peněz. V posledních letech však pozorujeme trend, kdy lidé placení v hotovosti stále více omezují, což je způsobeno především díky tomu, že lidé již nechtějí shromažďovat u sebe větší sumy peněz, ale mají je raději na svých peněžních kontech, kde se úročí a dále pak díky větší bezpečnosti svých finančních prostředků (když mi někdo ukradne platební kartu na PIN, ještě to neznamená, že přicházím o peníze, protože zloděj PIN nezná, ale když mi někdo ukradne peněženku s penězi, tak už se s nimi nesetkám).

Vznikly šeky, platební poukázky, "plastikové" peníze a "opravdové" peníze se přesunovaly hlavně mezi bankami po bezpečných finančních sítích, začalo se obchodovat přes telefon, mail, kdy se nakupující ani prodávající navzájem neviděli, a tak nebylo možné ověřit zda se nakupující či prodávající nepokouší o podvod. Peníze se tedy pomalu ale jistě začínají více a více přemísťovat elektronicky (nejvíce je to samozřejmě patrno v nejrozvinutějších částech světa a zemích, které udávají tempo celosvětového obchodu a které nejvíce ovlivňují finanční trhy atd.).[1]

2.1.2. Historie E-commerce

Elektronická komerce (e-commerce), EPS a elektronický obchod pomocí Internetu je mladý, nedobře definovaný ale velmi perspektivní a dynamicky se rozvíjející obor. Velké organizace používají elektronickou komerci již nějaký čas k provádění svých vlastních transakcí mezi sebou. Přitom vlastní **Elektronická výměna dat (EDI)** na soukromých počítačových sítích začala již v šedesátých letech. Přibližně stejně dlouho používají banky specializované sítě pro **Elektronický transfer peněz (EFT)**.
Na vzniku a rozvoji elektronické komerce se největší mírou podílela velká popularita Internetu. Díky tomu, že jej stále více a více firem používá ke své činnosti, se na Internetu rozšiřují možnosti elektronického obchodování mezi firmami a elektronická komerce se tak stává zcela běžnou součástí obchodu.

Pro mnoho lidí elektronická komerce znamená nákup či prodej výrobků a služeb přes Internet. To je však pouze jedním z mnoha aspektů elektronické komerce. Ta se od svých počátků týkala řízení nákupních a prodejních transakcí a následných převodů peněžních prostředků s využitím počítačových sítí. Nyní se však rozvinula natolik, že zahrnuje nákup a prodej nových komodit, jako jsou například elektronické informace. Současná elektronická komerce umožňuje provádění zcela nových typů transakcí přes počítačové sítě, které nemají svoji obdobu v reálném světě.

Elektronická komerce původně spočívala v transakcích mezi velkými korporacemi, bankami a jinými finančními institucemi. Právě využití Internetu jako prostředku k přenosu elektronické komerce ke koncovému spotřebiteli, vedlo ke změně pohledu na věc.
Internet rovněž způsobil vzestupný rozvoj průmyslové elektronické komerce, která se rozvíjí rychleji než kdy dříve. Malé firmy zjišťují, že své obchody mohou provádět on-line právě tak, jako jejich větší konkurenti, s využitím Internetu a elektronického obchodování lze významně snížit náklady a přispět tak k vyšší efektivitě.

Položíme-li si otázku *"Co je elektronická komerce?"*, musíme si nejprve uvědomit, z čeho se skládá tradiční komerce. Tradiční komerce zahrnuje více než jen prodej předmětu a následnou platbu. Prodejní cyklus bez využití elektronické komerce má typicky několik složek - firmy navrhují a vyrábějí nové výrobky, umisťují je na trhy,

distribuují je a poskytují podporu zákazníkům. Uspokojováním potřeb trhu dosahují příjmů.

Zákazníci však musí nejprve rozpoznat potřebu něčeho, ať už je to fyzický produkt, služba nebo informace. Předtím, než skutečně nakoupí, hledají informace o tomto produktu nebo službě, místo prodeje a porovnávají varianty, které nalezli (např. ceny, pověst firmy, služby…) Prodejní cyklus vůbec nekončí pouhým dodáním výrobku - měla by následovat podpora zákazníkovi, ze které plyne užitek oběma stranám: zákazníci dostanou fungující výrobek a dodavatelé se dozvídají o potřebách trhu. Mezitím banky a finanční instituce provádějí převod peněžních prostředků mezi prodávajícím a kupujícím, ať už jsou to individuální spotřebitelé nebo velké mezinárodní korporace. Elektronickou komercí pak můžeme chápat systém, který obsahuje nejen transakce realizující nákup či prodej zboží a služeb, které slouží k přímé tvorbě příjmů, ale i transakce, které podporují produkci příjmů. Typickým příkladem může být vytváření poptávky po daném zboží či službě nebo podpora prodeje a služby zákazníkům usnadňující komunikaci mezi obchodními partnery.

Elektronická komerce je postavena na výhodách a struktuře tradiční komerce s přidáním flexibility, kterou poskytují elektronické sítě. Usnadňuje různým skupinám spolupráci, řeší rychlou výměnu informací, odstraňuje fyzická omezení v důsledku čehož mohou například počítačové systémy na Internetu poskytovat podporu zákazníkům 24 hodin denně nebo přijímat a vyřizovat objednávky na výrobky či služby kdykoli a odkudkoli. Elektronická komerce zkrátka umožňuje vzniknout novým formám podnikání. Umožňuje firmám uzavřít prodejny, snížit potřebné zásoby a distribuovat výrobky pomocí Internetu.

Jako příklad si uveďme firmu Amazon.com se sídlem v Seattle ve státě Washington prodávající knihy. Tato firma nemá fyzické obchody, prodává všechny své knihy přes Internet a koordinuje dodávky knih přímo s vydavateli, takže nemusí udržovat žádné zásoby.[1]

2.2. Elektronické platební systémy (EPS)

V této kapitole jsou probírány elektronické platební systémy (EPS), jenž jsou rozděleny podle různých kritérií a vedle hlavních technologií jsou zde také uvedeny i podpůrné mechanismy, které do této problematiky náleží.

2.2.1 Rozdělení EPS

Zásadní charakteristikou EPS je, zda platební instrument (magnetická karta, čipová karta, osobní počítač) v sobě nese elektronickou hotovost (pracuje s přímým elektronickým modelem mincí a bankovek), pak se jedná o EPS s elektronickými penězi, či zda takovou hotovost neobsahuje, pak se jedná o EPS bez elektronických peněz.

Jedním z dalších kritérií pro klasifikaci modelů EPS je forma vzájemné komunikace mezi různými entitami. Tato forma modely dělí do dvou základních tříd na modely s přímou komunikací mezi plátcem a příjemcem a na modely s nepřímou komunikací. Při nepřímé komunikaci je platební operace vyvolána pouze jednou stranou a zahrnuje tak pouze iniciátora a banku(y). Plátci je pouze oznámena celá transakce a to jeho bankou.

Podle vztahu mezi dobou, kdy iniciátor platby (to je entita, která zahajuje platbu např. zákazník, který si vybírá zboří v internetovém obchodě) považuje tuto akci za ukončenou a časem, kdy se převedou peníze od plátce rozlišujeme mezi:

- předplacenými systémy (pre-paid payment systems)
- aktuálně placenými systémy (pay-now payment systems)
- systémy, kdy se platba provádí později (pay-later payment systems)

Pre-paid systémy se také někdy označují jako hotovostní (cash-like) modely a sem patří například dobíjecí kupóny, šeky. Dá se tedy říci, že zákazník si nejdříve zakoupí kredit a až bude potřebovat, tak se z něho odečte hodnota zboží, služeb, které si někdy v budoucnu zakoupí.

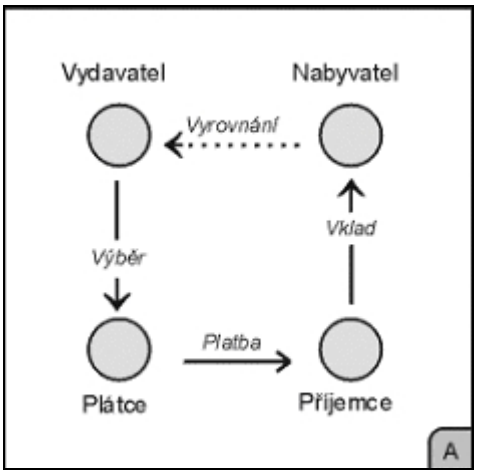
Poslední dva zmiňované (pay-now, pay-later) jsou si trochu podobné. V obou dvou případech musí mít uživatel zřízen účet v bance (na rozdíl od předplaceným systémů,

kdy to nutné není). Proto také tyto systémy jsou zařazeny mezi tzv. účtové (account-based) modely.

Z hlediska identifikovatelnosti plateb se EPS dělí na identifikovatelné a anonymní. U identifikovatelného EPS (s elektronickými penězi) má vydavatel elektronických peněz možnost identifikovat účastníky každé transakce, tzn. má možnost přesně sledovat cestu elektronických peněz. U anonymního EPS (s elektronickými penězi) se elektronické peníze chovají stejně jako běžné peníze, jakmile je zákazník od vydavatele elektronických peněz převezme, jejich vydavatel již nemá možnost zjistit, komu, kolik a za co zákazník zaplatil. Z hlediska implementace je anonymní EPS obtížněji implementovatelný než identifikovatelný EPS. Anonymita platebního systému je však zejména v posledních letech vlastnost spíše požadovaná, než nežádoucí.[3]

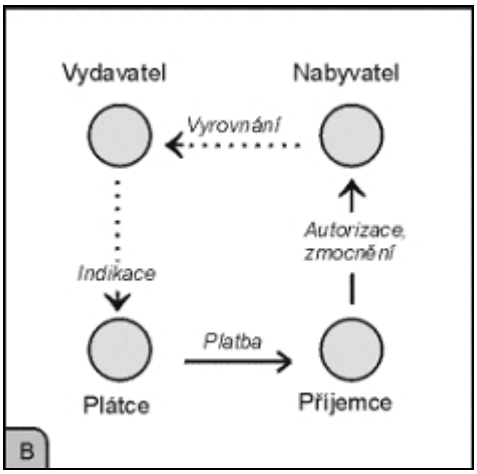
EPS se mohou také dělit podle nezbytného toku informací mezi zúčastněnými entitami:

- Obrázek 1 zobrazuje model EPS s přímou komunikací, typicky jde o předplacené systémy, kdy si zákazník předplatí svůj kredit a ten použije k provedení platby u obchodníka. Obchodník si následně kredit vymění u svého správce peněz za reálnou měnu a na konec ještě proběhne vyrovnání mezi správci peněz zákazníka a obchodníka.



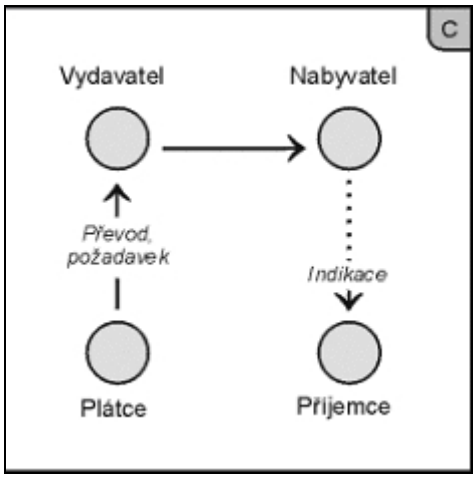
Obrázek 1 – EPS s přímou komunikací – zdroj: http://www.semper.org/info/

- Na obrázku 2 je také model EPS s přímou komunikací. Plátce však dává příjemci právo k převodu peněz od svého správce financí (typickým příkladem je nákup kreditní či debetní kartou, kdy převod peněz probíhá později než zakoupení zboží či dané služby).



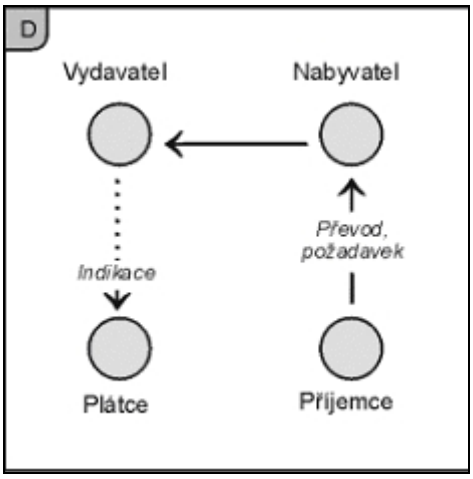
Obrázek 2 – EPS s přímou komunikací a právem převodu peněz – zdroj: http://www.semper.org/info/

- Obrázek 3 je model EPS s nepřímou komunikací, plátce zde podává požadavek svému správci peněz na převod finančních prostředků ke správci peněz příjemce. Patří sem třeba běžný příkaz k úhradě realizovaný např. pomocí internet bankingu.



Obrázek 3 – EPS s nepřímou komunikací – zdroj: http://www.semper.org/info/

- Obrázek 4 je také model EPS s nepřímou komunikací, ale tentokrát je z jednotlivých transakcí vyloučen samotný plátce. Jde např. o trvalý příkaz v bance, který dovoluje obchodníkovi čerpat z mého účtu určitou částku peněz.



Obrázek 4 – EPS s nepřímou komunikací a vyloučením plátce – zdroj: http://www.semper.org/info/

Dále se rozlišují dva základní způsoby realizace elektronických plateb:

- *on-line platby*

Před poskytnutím služby ověřuje obchodník s bankou platby od zákazníka (ověřování probíhá obvykle přes autorizační server na straně vydavatele či nabyvatele). On-line systémy zahrnují více komunikace a jsou považovány za více bezpečné než off-line platby. [online: http://www.semper.org/info/]

- *off-line platby*

Nepotřebují kontakt se třetí stranou během transakce. Je zamezováno dvojímu utrácení nějakou již provedenou operací a tak není nutné on-line spojení s bankou. Většina off-

line plateb k tomu používá nějaké hardwarové zařízení, které zamezují podvodům např. smart karty či softwarové prostředky např. elektronické peněženky. [online: http://www.semper.org/info/]

EPS jsou také děleny podle sumy, která je přenášena během transakce:

- *mikroplatby*

Tyto systémy jsou navrženy k podpoře velkého počtu malých plateb, několika penny za transakci místo několika dolarů. V letech 1995-1999 došlo k velkému nárůstu mikroplateb, v současnosti však dochází k migraci klasických čistě mikroplatebních modelů k modelům založených na kreditní bázi (což je model, který používá k platbám svoji vlastní měnu tzv. virtuální kredit). Největším problémem mikroplateb je cena samotných transakcí.[online: http://www.semper.org/info/]

- *platby s malou hodnotou*

Obvykle se platby s malou hodnotou provádějí použitím kreditních, debitních karet a široké uplatnění nacházejí zejména na Internetu. [online: http://www.semper.org/info/]

- *platby s velkou hodnotou*

Platby s velkou hodnotou především používají on-line systémy založené na asymetrické kryptografii využívající toho, že identita plátce je známá a ověřená. Můžeme sem zařadit internetové bankovní systémy, převody z účtu na účet atd. Nutnou podmínkou těchto systémů je zřízení účtu v nějaké bance. [online: http://www.semper.org/info/]

2.3. Bezpečnostní požadavky

Konkrétní bezpečnostní požadavky EPS se liší v závislosti na rysech jednotlivých systémů, obecně však mezi základní vlastnosti, které systémy musí mít patří: důvěrnost, integrita, utajenost, autorizace, interoperabilita, dostupnost a spolehlivost přenášených dat. Stejně jako ve světě klasických peněz, i ve světě elektronických plateb stále budou existovat rizika porušení důvěryhodnosti a bezpečnosti. Jde o to, aby použité kryptografické mechanismy a protokoly tato rizika minimalizovaly.[17]

Uplatňované bezpečnostní politiky šifrováním zpráv brání porušování důvěrnosti odposlechem a elektronickými (digitálními) podpisy brání nepoctivým zákazníkům, aby se podvodně vydávali se za jiné osoby, nepoctivým obchodníkům, aby falšovali elektronické platební příkazy zákazníků a konečně chrání i integritu přenášených dat. Používání důvěryhodného software brání krádežím v počítačových systémech pomocí různých trojských koňů.

2.3.1. Důvěrnost, integrita, autorizace

Důvěrnost musí zabezpečit, že neautorizované osoby nemohou odposlechem komunikací v síti nebo vniknutím do zúčastněných počítačů zjistit takové informace, jakými jsou příkazy, platby a účty zákazníka. Taková vlastnost se zajišťuje pomocí kryptografie. Aby se omezil výskyt krádeží a snížila se tudíž celková cena zpracování plateb, prověřuje se identita zúčastněných stran autentizací. Obchodník si musí být jistý, že zákazník je legitimní uživatel čísla účtu platné platební karty. Zákazník musí mít možnost identifikovat obchodníka, se kterým může bezpečně elektronicky obchodovat a musí si být jistý, že tento obchodník spolupracuje s finanční organizací, která akceptuje jeho platební kartu. Autentizace se implementuje digitálními podpisy a certifikáty. Zákazník zprávami reprezentujícími platební transakce sděluje co objednává, svoje personální data a platební instrukce Obsah zpráv se během přenosu nesmí změnit. Vlastnost integrity se obvykle implementuje digitálními podpisy.[17]

Celistvý platební systém také nedovoluje, aby se převáděly peníze od uživatele, který tuto akci neautorizoval. Umožňuje také odmítnutí přijetí platby bez souhlasu, aby

zabránil podobným věcem jako je např. uplácení. Autorizace tvoří u neanonymních EPS nejdůležitější složku v platebních systémech a může být prováděna třemi způsoby:

- *autorizace třetí stranou*

Ověřující stranou je typicky banka, která buď zamítne nebo potvrdí transakci použitím bezpečného venkovního kanálu (např. pošta, telefon). Typické použití je u objednávek po telefonu či mailu. Typické použití je u plateb typu CNP (Cardholder not present), dříve zvané MO/TO (Mail order/Telephone order). Kdokoliv, kdo zná data z kreditní karty může vyvolat transakci a odpovědný uživatel pak musí toto potvrdit nebo naopak říci, že jde o nepovolenou transakci. Obvykle pokud uživatel nepodá podnět proti dané transakci do 90 dní, je automaticky schválena.

- *heslem*

Transakce chráněná heslem požaduje, aby každá zpráva od autorizované strany zahrnovala šifrovanou část pro kontrolu. Tato část je vypočítána pomocí tajného klíče, který je znám pouze autorizující a ověřující straně.

- *digitálním podpisem*

V tomto typu autorizace požaduje ověřující strana digitální podpis autorizované strany. Digitální podpis zajišťuje nepopíratelnost původní zprávy, protože pouze majitel tajného podpisového klíče se mohl podepsat pod tuto zprávu (resp. podepsat se může každý, ale odpovídající digitální podpis majitele X může vytvořit pouze majitel X, protože ten je jediný kdo zná tajný klíč).[17]

2.3.2. Interoperabilita a utajenost

Je nutné, aby se na platebním systému současně podílely různé hardwarové a softwarové platformy. Každý obchodník může používat jiný počítačový systém, odlišné počítačové systémy mohou používat jednotliví zákazníci, certifikační autority rovněž nejsou vázány na konkrétní softwarovou či hardwarovou platformu, i banka obchodníka

si může volit svoji vlastní počítačovou platformu. Potřebná interoperabilita se dosahuje aplikací standardizovaného platebního protokolu. Takovým protokolem je např. protokol SET, který k záruce za interoperabilitu přirozeně přidává i záruky za udržování výše zmíněných vlastností.[17]

U neanonymních EPS mohou některé zúčastněné strany požadovat tzv. utajenost transakce, čímž se myslí to, že některé informace o dané transakci (např. jméno plátce, příjemce, celková suma, atd.) zůstanou utajeny vůči třetím osobám. [17]

2.3.3. Dostupnost a spolehlivost

Jednou z dalších důležitých vlastností EPS, je možnost provádět platby kdykoliv je to potřeba. Platební transakce musí být atomické - tj. provede se buď celá nebo žádná část transakce a nesmí se stát, že by systém zůstal v neznámem či nekonzistentním stavu. Žádný plátce by neakceptoval ztrátu peněz kvůli hardwarovým či softwarovým potížím. Dostupnost a spolehlivost tedy předpokládá především bezchybný chod všech počítačových komponent. A pokud už k nějakému problému dojde, je nezbytné mít vypracovaný plán návratu do původního konzistentního stavu. Chybové stavy zde nejsou dále probírány, protože většina EPS je explicitně ani neuveřejňují.[17]

3. Analýza současného stavu

3.1 Media EPS

V této části se budeme zabývat médii pro přenos a uskutečnování elektronických platebních transakcí

3.1.1. Karty

V současné době se používají platební karty několika druhů (řazeno podle vývojového hlediska):

Embosované karty: Typ a umístění embosovaného textu je specifikován standardem ISO 7811. Norma definuje embosování ve dvou oblastech - první je určena pro číslo karty (až 19 znaků), které identifikuje jak vydavatele, tak i držitele, a druhá oblast je vyhrazena na další údaje o držiteli, jako je jméno a adresa (4 řádky po 27 znacích).

Karty s magnetickým pruhem: Tento typ karet nese magnetický proužek, na kterém jsou uloženy údaje (250 B) o vlastníkovi, číslo karty atd. Kdokoliv s odpovídajícím čtecím zařízením na tyto karty si může přečíst uložené informace.

Čipové pamětové karty: Používají se pro jednoduché aplikace jako jsou předplacené telefonní karty, které mají chip s 60 nebo 120 pamětovými buňkami. Tyto buňky jsou použitelné jenom jednou, to znamená, že jakmile se paměťová jednotka použije, karta se dále stává bezcenná a může se vyhodit.

Čipové procesorové karty: Jak již název napovídá, karty obsahují mikroprocesor, který kontroluje přístup k informacím na kartě. Tyto karty zvyšují ochranu proti podvodům a používají se v těch nejdůležitějších (z hlediska bezpečnosti) aplikacích.

Optické karty: Zatím se vyrábějí bez procesoru, ale v budoucnu na tomto druhu karet jistě nebude chybět. Umožňují ukládání mnoha megabytů dat, nicméně údaje mohou být zatím zapsána jen jednou a nelze je smazat. Nacházejí využití například ve zdravotnictví, neboť jejich kapacita umožňuje uložení rentgenových snímků.

Kromě toho se platební karty dělí podle typu zúčtování na:

Debetní - jedná se o kartu, kterou lze platit nebo vybírat z bankomatu, pokud je na účtu, ke kterému byla karta vydána, dostatek peněz. K zúčtování dochází většinou chvíli po provedené transakci.

Kreditní - kartou se může nakupovat zboží nebo služby na úvěr. K zúčtování dochází až po určité bankou stanovené době. Úvěr se čerpá prostřednictvím revolvingového (opakujícího se) úvěrového limitu, který se obnovuje automaticky po splacení dlužné částky. Banky stanovují minimální výši splátky úvěru (obvykle 5 - 10 % z dlužné částky) a úvěrový limit (podle bonity klienta).

Charge - zde kartou nenakupujete na úvěr. Při zúčtování, které je také stanovené k určitému datu (obvykle 14 - 30 dní), musíte splatit celou dlužnou sumu. Charge kartou neboli kartou s odloženou splatností čerpáte samostatný úvěrový produkt, tak zvaný karetní úvěrový rámec účtu, poskytnutý k vašemu účtu.

Z hlediska bezpečnosti rozlišujeme logickou bezpečnost a fyzickou bezpečnost čipových karet:

Logická: Čipová karta je navrhnuta tak, že žádná funkce nebo kombinace funkcí nevede k odhalení citlivých údajů. To je dosaženo interním monitorováním všech operací prováděných uživatelem karty a vynuceným horním limitem funkcí, které se mohou provést za určitou dobu. Nedávné výzkumy však toto zpochybňují. Byl proveden útok založen na základě zahřívání karty, která se potom dostala do nekorektního stavu a při vyšetřování tohoto stavu se zjistilo, že následný útok na uložený tajný klíč byl mnohem jednodušší.

Fyzická: Speciální chemické vrstvy chrání čip na kartě proti analýze obsahu její paměti. Pokud jsou i tyto vrstvy odstraněny a čip je naprosto obnažen, jsou tu další těžkosti, které chrání obsah paměti proti neautorizovanému čtení a to díky faktu, že elektrické impulsy v paměťovém prostoru jsou velmi malé. Samozřejmě, že teoreticky je možné

obsah paměti analyzovat, ale musí být k tomu vynaloženo enormní úsilí, které stojí nemálo peněz.

V dnešní době dochází k celosvětovému nahrazování karet první generace (s magnetickým proužkem) a paměťových karet procesorovými smart kartami. Tyto karty jsou založeny na EMV (Europay-MasterCard-Visa standard pro vzájemnou kompatibilitu čipů a terminálů). Přechod na standard EMV se týká např. i Francie, která smart karty používá již několik let, ale většina používaných smart karet tento standard nesplňuje. Výměna starých karet za nové probíhá z několika důvodů. Jsou to především bezpečností důvody, protože riziko podvodů u nejmodernějších karet je mnohonásobně nižší a pak je to také větší komfort v užívání těchto karet. Jedna smart karta může kombinovat několik platebních mechanismů (Visa, Mastercard), může mít několik funkcí (vstup do knihovny, telefonní karta, zdravotní karta, karta na obědy) a v neposlední řadě mohou obsahovat mnohem více informací (zdravotní údaje pro případ nehody, předchozí bankovní operace prováděné daným uživatelem). Mezinárodními asociacemi byl stanoven termín 1.1.2005 [/online/ http://www.penize.cz/info/zpravy/zprava.asp?NewsID=1314] a od tohoto data musí všechny platební karty používané v Evropě nést v sobě čip a být standardu EMV.

3.1.2. Mobilní telefony

Zájem o mobilní telefony, jako autentizační zařízení pro platby, se neustále zvětšuje. Částečně za to může i nedostatek čtecích zařízeních pro smart karty u osobních počítačů. Předpokládalo se totiž, že tyto čtečky se stanou běžnou výbavou PC, což se nestalo a mobilní telefony tak můžeme použít pro různé druhy vzdálených i lokálních plateb. Můžeme s nimi platit za stahování dat do PC, telefonu, za nákup CD disků, knih, šatů po internetu, ale stejně tak v normálním kamenném obchodě, můžeme s nimi hradit parkovné, mýtné, různé zboží z prodejních automatů a nespočet dalších věcí.

Všechno to začalo s uvedením SMS zpráv s přidanou hodnotou, jejímž přijetím či posláním jsme si mohli stáhnout např. novou vyzváněcí melodii. Tento trh se rozrostl do velikosti přesahující 1 miliardu EUR pro samotnou Evropu [/online/ www.mobiletransaction.org] a stále roste díky neustálému uvádění nových digitálních

služeb. Je tu tedy stále ještě velký potenciál, čehož si uvědomovali hlavně mobilní operátoři a tak postupně vznikalo nespočet skupin a projektů, které v této oblasti mají své zájmy a postupně vyvíjejí nové standardy a nové projekty. Mezi ty největší patří Mobile Payment Forum, Mobile electronic Transaction (MeT) Initiative, PayCircle, The Mobey Forum a posledně ustanovená Mobile Payment Services Association tvořená největšími evropskými mobilními operátory (Vodafone, Orange, T-Mobile, Telefónica).

Nedlouho po té co přišel na svět WAP (wireless application protocol) bylo potřeba vyřešit z hlediska bezpečnosti, jak dopravovat bezpečně data mezi klientem a WAP bránou. SSL protokol nebylo možné použít, a tak vznikl nový protokol WTLS [O'Mahony, D., Peirce, M. a Tewari, H., *Electronic Payment Systems for E-Commerce*, Second Edition, Artech House 2002, ISBN 1-58053-268-3] (wireless transport layer protocol). Zprávy používané v WTLS jsou funkčně identické k těm v SSL (a jeho následníkovi TLS), avšak díky horší propustnosti linek se musely provést menší změny. Certifikáty použité ve WAPu jsou více kompaktní než X.509 a dialogy jsou strukturovány tak, aby se posílaly jenom ty certifikáty, které jsou absolutně nezbytné. Cesta mezi WAPovou bránou a webovým serverem je již dále zabezpečena protokolem SSL.

Všechny mobilní telefony si udržují detaily o identitě svého majitele v smart kartě, která se označuje jako SIM (subscriber identity module) karta. WTLS toto napodobilo a z tohoto konceptu specifikovalo WIM (wireless identity module), jež vykonává bezpečnostní funkce v aplikační úrovni WAPu, především ukládá a zpracovává informace potřebné k identifikace a autentizaci. Celé je to založeno na tom, že citlivá data (klíče) jsou uložena ve WIM a všechny operace s klíči se provádí taktéž v tomto modulu. WIM jako samostatný modul může být integrován na stejné kartě jako SIM (někdy označováno jako SWIM), dále může být tvořen jinou samostatnou smart kartou a nebo může být implementován softwarově (Java).

Mobilní telefon je na nejlepší cestě stát se ekonomicky zajímavým, bezpečným a dostupným platebním nástrojem. Proto je zájem mobilních operátoru v celém projektu pochopitelný. Taktéž banky, které vložily spoustu peněz do různých projektů

elektronických peněženek a jejichž přínos byl mizivý, mají zájem se spojit s mobilními operátory a vytvořit nový efektivní platební model. Každá platba provedená mobilním telefonem bude znamenat pro mobilní operátory další vítaný zdroj příjmů. Více bezhotovostních plateb ve větším množství obchodů přinese bankám nové příjmy a obchodníkům potenciálně o něco větší tržby.

Výhodou placení zboží a služeb prostřednictvím mobilních telefonů je v jejich snadné dostupnosti a masovém použití. Mobilní telefony v rukách zákazníků představují již vybudovaný základ nové platební infrastruktury, do které nebude nutné znovu investovat. Mobilní operátoři mají uzavřeny roamingové dohody ve většině zemí světa, mohou tedy zajistit placení téměř kdekoli na zemi. Jejich nevýhodou však je, že nemají mezinárodní clearingový a zúčtovací systém, který mají banky a jejich platební asociace.

Česká republika nestojí stranou tohoto vývoje. České banky před více než 10 lety zavedly jeden z nejmodernějších systémů platebních karet v Evropě (MUZO), Expandia Banka (dnes eBanka) a Paegas (nyní T-Mobile) zavedly v roce 1998 jako první na světě GSM banking. V dobíjení předplatných mobilních telefonů pomocí bankomatů nebo nyní i SMS zpráv se české banky opět zařadily mezi nejrychlejší inovátory.

3.1.3. Mikroplatby

Z běžných platebních nástrojů jako jsou platba v hotovosti, šeky, platební karty je pro placení malých částek nejvhodnější platba v hotovosti (cash). Cash je však zdola limitován hodnotou nejmenší mince (např. jeden eurocent). Existuje však takové zboží, či spíše služby, kterým toto může činit problém. Například internetový magazín by chtěl za každý přečtený článek od čtenáře inkasovat malou částku nebo podobně internetová encyklopedie by si nechala platit za každé nalezené slovo ve své databázi atd. Tradičně se tento problém řeší pomocí předplacení služeb za fixní částku na určité období. Zatímco platby předem zaručují, že bude poskytovateli za provedené služby zaplaceno, omezuje to spoustu zákazníků, kteří chtějí používat služby jen příležitostně. Také je omezena možnost danou službu pouze vyzkoušet.

Proto před několika lety vzniklo nespočet nových platebních schémat (mikroplateb), které jsou zaměřeny na tyto časté a nízkohodnotové platby na internetu, z nichž však jenom pár zůstalo a v současné době se ještě používají. Aby byly mikroplatby úspěšné a svým provozovatelům se vyplatily, je třeba, aby je používala obrovská masa lidí, resp. aby počet samotných plateb byl obrovský a to především proto, že cena mikroplatby a tím pádem i zisk z ní nesmí být pro obchodníka příliš veliký. Dá se říct, že existující finanční komunita pro tento nový druh plateb nenašla příliš velké pochopení, a tak se začali objevovat mikroplatební modely od převážně softwarových firem Millicent, PayWord, MicroMint, DirectPay, I Like Q, Monetka atd.

Tyto platební systémy efektivně přenáší velmi malé částky a samotný komunikační provoz, jenž stojí peníze, je v těchto systémech udržován na nejmenším možným minimu. Díky tomu, že zisk z každé platby je velice malý, musí mikroplatební systém být schopen ověřit každou platbu velice levně, zároveň však musí redukovat počet výpočetně náročných operací. Mikroplatby mohou také představovat kreditní schéma, kdy vzniká virtuální kredit (měna), pomocí níž jednotlivé uživatele můžeme odměňovat a tím i motivovat k požadovaným úkonům (návštěva webových stránek atd.).

Dnes s odstupem pár let již můžeme říci, že celkové uživatelské přijetí mikroplatebních systémů bylo velmi pomalé, možná také díky nedostatku podnotného obsahu, který není volně přístupný v nějaké formě jinde na internetu. Podobně obchodníci se zdráhali investovat do kvalitního obsahu, dokud neexistovala dostatečně velká základna uživatelů ochotných platit tyto malé částky. Drtivá většina uživatelů chápe internet jako bezplatný zdroj informací, tudíž není ani v nejmenším ochotna za informace platit, a raději věnuje mnohem více úsilí a nákladů, aby získala danou informaci nebo službu "zadarmo". Běžné (makro) platby nejsou pro zákazníky zas až tolik novou věcí. Na placení prostřednictvím nějaké služby jsme zvyklí z každodenního života a i přesto dnes hodně uživatelů internetu elektronickým platbám příliš nevěří. Naopak mikroplatby jsou pro všechny zcela novým pojmem a tím přirozeně jeho začlenění do podvědomí trvá mnohem déle.

V současnosti došlo k migraci klasických čistě mikroplatebních modelů k modelům založených na kreditní bázi. Platební portály neposkytují už mikroplatby jako jedinou a hlavní službu. Naopak je integrují do svých originálních platebních systémů. Služba je nabízena spíše jako doplňková. Pro tyto společnosti je výhodnější operovat s mikroplatbami jako s platbami klasickými. V dnešní době je výkon výpočetní techniky na takové úrovni, že už není nutné hledat pro mikroplatby vlastní model zabezpečení. Nicméně obvykle dochází k zvednutí, mnohdy i řádově, minimální částky, kterou je mikroplatba míněna. Mikroplatby ve své kreditní formě mají neocenitelnou roli jako prostředek k získávání uživatelů. Tím, že poskytovatel služeb nabízí uživatelům možnost získat odměnu v podobě mikroplateb, láká je k navštěvování jeho webových stránek a tím zlepšuje podmínky pro inzerci na svém webu, což se mu vrátí v podobě lépe ohodnocené reklamy. Mikroplatby tak mnohdy přebírají namísto role platebního nástroje roli nástroje marketingového.

3.1.4. Elektronické peníze

Peníze (pokud budeme brát jejich fyzickou podstatu) se postupem času vyvinuly z cenných platidel (vzácné kovy - zlato, stříbro) k "bezcenným" mincím a bankovkám, šekům až k systémům založeným na kreditní bázi. Se vznikem elektronické komerce se začalo uvažovat také o elektronické formě peněz. Elektronické peníze (e-peníze) lze považovat [Evropský parlament, *Směrnice evropského parlamentu a rady 2000/46/ES*, září 2000] za náhradu mincí a bankovek, které se ukládají na elektronickém médiu, jako jsou čipová karta nebo paměť počítače, a které jsou obecně určeny pro uskutečňování elektronických plateb v omezené výši.

Elektronické peníze lze dělit podle několika hledisek. Jedno dělení elektronických peněz může být podle jejich povahy na "token-based" nebo "balance-based":

1. Token-based el. peníze jsou opravdovou virtuální kopií skutečných mincí. Existují v předem definovaných hodnotách, které je pro rozměnění třeba poslat do vydávající banky. Každé minci je přitom přidělena určitá jedinečná číselná (registrační) hodnota, jejíž existence má zabránit problému dvojího utrácení. Z toho také vyplývá, že každá "mince" je použitelná pouze jednou. Typickým příkladem byl Ecash od firmy DigiCash.

2. Balance-based el. peníze jsou častější a mají podobu pouhého kladného nebo záporného zůstatku na elektronickém účtu. Do této kategorie jsme mohli zařadit např. český internetový platební systém I LIKE Q.

Dalším kritériem, podle kterého můžeme el. peníze dělit je jejich samotná implementace:

1. **Card-based el. peníze**, jak už název napovídá, jsou takové elektronické peníze, které jsou uloženy na nějakém přenosném médiu, typicky karta s integrovaným obvodem obsahující mikročip (smart karta). Tato "elektronická peněženka" zajišťuje různé kryptografické funkce a hlavně s ní můžeme platit i v reálném světě. Jako příklad můžeme uvést předplacené karty MasterCard, VISA.

2. **Software-based el. peníze** jsou takové, jenž se spravují přes software nainstalovaný na PC, PDA, běžící pod standardním operačním systémem. Typické použití je pouze přes počítačové sítě jako je internet.

Podle povahy emitenta členíme elektronické peníze na bankovní a nebankovní. Zatímco nebankovní elektronické peníze jsou takové, jejichž (zjednodušeně řečeno) emitentem není banka, bankovní elektronické peníze jsou potom takové elektronické peníze, které vydává právnická osoba disponující bankovní licencí v souladu s ustanovením § 6 zákona o bankách.

Elektronické peníze je třeba striktně vymezit vůči různým internetovým věrnostním systémům, jež jsou pouhou obdobou běžných věrnostních programů, jaké dnes nabízí každý větší supermarket. Jako typický příklad lze uvést tzv. fazole společnosti Eastbiz Net Inc. nebo dukáty od firmy Mafra a.s. Zásadní odlišnost spočívá v jejich omezené konvertibilitě v některou z existujících měn (a opačně) a z toho v úzkém poli využití typickém i pro věrnostní body obchodních řetězců. Internetové věrnostní body jsou marketingovým nástrojem pro získání nových zákazníků a nikoliv platební nástroj typu elektronických peněz.

3.2 Podpůrné mechanismy

Podpůrné mechanismy zahrnují takové technologie, které nejsou sami o sobě částí platebních transakcí, ale pomáhají je uskutečňovat, dělají je více účinné a nebo jednoduše zajišťují bezpečné zázemí pro aktuální transakce. Jestliže se v této kapitole budeme zabývat určitým systémem, tak jen z povrchního hlediska. Podrobně bude daný systém zkoumán a popsán ve třetí kapitole.

3.2.1. Autentizace držitele platební karty

Spotřebitelé stále nemají příliš velkou důvěru v posílání detailů o své platební kartě po internetu, ale ve skutečnosti jejich strach vychází ze špatného důvodu. Většina lidí se obává toho, že tato data budou zachycena na cestě k obchodníkovi, což je dnes již prakticky nemožné z důvodu toho, že na všech hlavních komerčních stránkách je použit protokol SSL, který šifruje všechny důležité detaily o platební kartě.

Ten podstatný problém, který si většina lidí neuvědomí, je to, že neexistuje cesta, jak autentizovat zákazníka při on-line platební transakci za použití platební karty. Tím je míněno to, že nemáme rozšířený mechanismus k potvrzení identity nakupujícího v době nákupu (samozřejmě je myšleno použití platební karty na internetu a ne v normálním kamenném obchodě, kde si prodavač vždy ověřuje, zda souhlasí váš podpis s podpisem na kartě). Proces nazývaný autentizace je tedy ověření totožnosti držitele platební karty během samotného placení touto kartou.

Jestliže chce on-line nakupující v dnešní době platit kartou na internetu, musí vždy zadat údaje o této kartě do formuláře na serveru obchodníka. Takto však může vzniknout situace, kdy kdokoliv cizí může do formuláře napsat údaje o cizí platební kartě za účelem podvodného nákupu a obchodník nemá šanci jak zjistit zda tyto údaje jsou pravé. Bez efektivní autentizace vznikají problémy jako např. nedostatek důvěry zákazníků, vyšší cena jednotlivých transakcí, ztráta příjmů pro obchodníky, vyšší cena samotných služeb, zpětné účtování pro banky a nakonec i poškození jména společností vydávající platbní karty. V důsledku toho se otevírají možnosti pro alternativní platební metody bez použití platebních karet.

Existuje několik řešení, které jsou zahrnuty v platebních systémech jako např. Card Security Code a Address Verification Service či bezpečnější a komplexnější řešení, např. MasterCard SecureCode, Verified by Visa či protokol SET.

SET

Vraťme se však na počátek samé ekomerce, kdy začátkem 90-tých let došlo k utvoření dvou největších konkurenčních konsorcií, vedených dominantními společnostmi poskytující kreditní karty. MasterCard spolu s Netscape Corporation, IBM a ostatními vytvořily v roce 1995 specifický systém SEPP (Secure Electronic Payment Protocol). Nedlouho na to druhé konsorcium vedené Visou a Microsoftem představilo odlišný a nekompatibilní systém nazvaný STT (Secure Transaction Technology). Pokud by tato situace setrvala, vedlo by to ke skutečnosti, kdy by každá transakce musela odpovídat specifickým podmínkám podle použité specifikace.

Začátkem roku 1996 konečně zvítězil zdravý rozum a společnosti MasterCard a Visa oznámily vzájemnou dohodu o vývoji jednotného systému, pojmenovaného SET (Secure Electronic Transaction).

Nutnou podmínkou k bezpečnému použití SETu je to, aby každý subjekt zúčastněný při platební transakci byl certifikován, tj. musí vlastnit digitální certifikát vydaný certifikační autoritou, která ověřila totožnost daného subjektu.

Vlastník karty zahájí platbu s obchodníkem používajícím SET. Obchodník poté použije SET k autorizaci platby. Platební brána může být ovládána poskytovatelem nebo sdružením poskytovatelů nebo přímo asociací poskytující kreditní karty. Tato platební brána je předřazená finanční síti a skrz ní poskytovatel karty může být kontaktován pro jednoznačné autorizace jednotlivých transakcí.[17]

3-D SET

Protože se SET na trhu neujal (důvody budou zmíněny později), rozhodlo se několik prodejců a vývojářů zainteresovaných v tomto projektu vyvinout jinou implementaci SETu tzv. server-based. Server-based SET model redukoval technologii, která musela

být použita u obchodníka a zákazníka na "malé" moduly (obchodník) a "tenké" digitální peněženky (zákazník).

Server-based SET neukládá digitální certifikáty na zákazníkovo zařízení, což otevírá možnost použít PDA, mobilní telefony a další zařízení při uskutečňování SET transakcí. Díky tomu, že tato mobilní zařízení nemají uložen žádný digitální certifikát, je nezbytné použít bezpečnostní mechanismy jako je SSL či WTSL při spojení těchto zařízení se serverem.

Server-based SET, jako jakýkoliv jiný systém založený na certifikaci, má určitá omezení, např. že používá certifikáty vydané pouze jednou certifikační autoritou. Hlavním nedostatkem však u server-based SETu je neschopnost spolupráce s SSL weby, které jsou v dnešní době odpovědné za většinu platebních transakcí.

Card security code, address verification service

Mezitím ekomerce pokračovala rostoucím tempem, stejně jako se zvětšoval počet podvodů při platbách. Tyto podvodné nákupy si díky médiím získaly velkou popularitu. Odhaduje se, že v tomto roce počet online plateb pomocí platebních karet dosahuje 2-4% z celkového počtu transakcí pomocí platebních karet, což je relativně málo. Nicméně možný výskyt podvodné transacke je v on-line světě 12x vyšší než ve fyzickém. Proto vznikly další podpůrné bezpečnostní mechanismy, které se těmto podvodům snaží předcházet.

Jedním z nich je i tzv. Card security code (CSC) spolu s Address verification service (AVS). CSC je vytištěn na každé platební kartě na zadní straně. Pomocí tohoto zadaného kódu, který zašleme on-line vydavateli této karty na ověření, si můžeme ověřit totožnost držitele karty. Tento kód nebývá nikde ukládán ani tištěn, je pouze na samotné kartě. Jak už název napovída, AVS ověřuje zda-li souhlasí zadaná adresa majitele karty s adresou uloženou v databázi vydavatele karty.

Je patrné, že ani tyto kontroly nedokáží úplně zabránit podvodné platbě, neboť pokud někdo zcizí majiteli jeho kartu a zná i jeho plnou adresu, může se za něj podvodně vydávat.

V roce 2001, pět let po představení SETu, hlavní karetní společnosti začali znovu vyvíjet nové autentizační standardy pro on-line platby. Tentokrát však ale ne společně, nýbrž každý zvlášť. Visa vyvinula systém nazvaný 3-D Secure a MasterCard uvedl svůj vlastní systém, který nazval Secure Paymnet Application.

Visa 3-D Secure ("Verified by Visa")

Toto řešení nevyžaduje, aby držitel platební karty musel používat dodatečný software na svém počítači, na druhou stranu je třeba, aby byl uživatel registrován u vydavatele své platební karty, či aby použil nějaký jiný autentizující mechanismus (např. čipová karta).

V momentě, kdy zákazník zmáčkne tlačítko "koupit" na obchodníkově webu, je aktivován plug-in (na straně obchodníka), který se dotáže VISA serveru, jestli je držitel karty zapsán v databázi VISA. Jestliže ano, pak je plug-inu předána webová adresa tzv. "Issuer Access Control Serveru", kde dochází k autentizaci zákazníka. Tomu vyskočí nové okno, kde vidí detaily o transakci a zároveň tam provádí svoji identifikaci a potvrzení objednávky. Tyto údaje následně zkontroluje vydavatel platební karty a digitálně se podepíše pod objednávku, kterou vrátí obchodníkovi. Obchodník údaje zkontroluje a pošle žádost k převodu peněz. Když vše dobře dopadne, může po 10-15 sekundách expedovat zboží.

MasterCard Secure Payment Application (SPA)

V květnu 2001 MasterCard představil své vlastní řešení Secure Payment Application. SPA je založeno na spolupráci s Universal Cardholder Authentication Field (UCAF) a byl navržen tak, aby minimalizoval náklady na zapojení u obchodníka. UCAF je víceúčelový mechanismus pro přenos dat implementovaný obchodníky a jejich bankami za účelem sbírání autentizujících informací generovaných zákazníky. Jakmile jsou tyto informace získány, jsou přenášeny k vydavatelům platebních karet za účelem autentizace zákazníka a autorizace platby. UCAF podporuje spoustu bezpečnostních a autentizujících přístupů, mimo SPA také např. čipové karty a další.

Podobně jako u "Verified by Visa" se musí zákazník autentizovat do SPA pomocí svého hesla či čipové karty. Vydavatel platební karty musí implementovat na své straně SPA server a zajistit distribuci SPA apletů ke svým zákazníkům. SPA server je odpovědný za generování specifických bezpečnostních tokenů (unikátní pro každou transakci), které jsou posílány obchodníkům, jejich bankám a zpět vydavatelům platebních karet pro kontrolu celé transakce. V důsledku toho MasterCard obnovil svoji vlastní bankovní síť Banknet (nákladem 160 miliónů dolarů), což je komunikační páteř pro autentizaci transakcí využívající bezpečnostní tokeny oficiálně nazývané Accountholder Authentication Value (AAV).

Uživatelé musí používat software na straně klienta (zmíněný SPA applet), jenž komunikuje s SPA systémem. Tyto malé klientské aplety nepřenáší žádné certifikáty jako SET peněženky. SPA applet je navržen tak, aby se "probudil", když uživatel vstoupí na SPA kompatibilní platební stránku.

3.2.2. Elektronické bankovnictví

Jednou z prvních forem elektronických plateb byl v prostředí obchodních firem, vedle nejrůznějších proprietárních aplikací, elektronický platební styk (Electronic Founds Transfer - EFT) založený na technologii elektronické výměny dat (EDI) používaný pro ovládání bankovních účtů na dálku realizované prostřednictvím elektronických komunikačních kanálů. Tradičně se taková výměna mezi finančními institucemi nazývá mezibankovní vyrovnání a probíhá v clearingovém centru (např. na mezinárodní úrovni zajišťuje SWIFT - mezinárodní počítačově řízená telekomunikační síť).

Nicméně s nástupem nových elektronických platebních systémů byl EFT aplikován více na výměnu bankovních transakcí (využitím EDI) a v poslední době je aplikován jako Home banking, kde jej využívá už běžný uživatel komunikující s bankou.

V dnešní době se stále důrazněji začíná prosazuje elektronické (též přímé) bankovnictví . Otázka, jak co nejsnáze spravovat peníze na bankovním účtu netrápí jen klienty, ale také samotné banky. I když se to zatím možná nezdá, cílem většiny bankovních domů je co nejvíc snížit počet poboček. Důvod je prostý a snadno pochopitelný - náklady, které neustále rostou.

Home banking

Tato forma práce s účtem je nejen pohodlná, ale také velice bezpečná. Služba je zabezpečena nejen heslem, ale také potřebou autorizačního certifikátu, který je instalován na počítači klienta. Přenos mezi počítačem a bankou je navíc většinou kódovaný.

Home banking obvykle umožňuje provádět téměř veškeré bezhotovostní úkony. Bohužel, je tato forma elektronického bankovnictví poměrně nákladná a je proto určena spíše pro bankovní klienty, kteří zpracovávají větší objem plateb a nebo potřebují mít trvalý přehled o stavu svého účtu, než pro běžné uživatele.

Kromě možnosti zadávat příkazy a provádět další operace s účtem obvykle home banking aplikace nabízí přístup do databáze banky a vyhledávání služeb, číselníků bank, kurzovních lístků, úrokových sazeb a podobně. Kromě toho je aplikaci možné propojit s vlastním ekonomickým systémem firmy, což umožňuje automatické předávání platebních příkazů a výpisů z účtu.

Home banking však má i své nevýhody. Kromě již zmíněné nákladnosti je to i vazba na konkrétní počítač s příslušným vybavením. Propojení mezi bankou a uživatelskou stanicí přitom probíhá prostřednictvím modemu a telefonu nebo sítě internetu.

GSM banking

Asi nejrozšířenější formou elektronického bankovnictví je mobilní bankovnictví, též nazývané GSM banking. U této služby existují tři druhy. První je SIM Toolkit. Zde banka do vašeho mobilního telefonu (na SIM kartu) nahraje vlastní bankovní aplikaci, která se objeví v menu vašeho telefonu. Při nahrávání aplikace je SIM karta zašifrovaná a nelze z ní získat žádné údaje, ani když vám ukradnou telefon. Současně je přístup k této aplikaci chráněn zvláštním bankovním PIN, které se nazývá BPIN. Potom vám tedy stačí listovat v menu aplikace správnou položku a vybrat některou ze základních služeb (např. zjišťování zůstatku na účtu, přehled historie pohybů na účtu, přehled kursů, zadávání příkazů). Na konec obdržíte informaci o vámi vybrané službě a to buď formou

textové zprávy na mobilní telefon, nebo formou e-mailu do e-mailové schránky, která je předem definovaná.

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

Konečně poslední formou GSM bankingu je WAP banking, což je, jak už název napovídá, technologie, která umožňuje spojení s bankovním účtem prostřednictví mobilního telefonu vybaveného technologií WAP (Wirless Application Protocol). WAP banking mohou využívat i majitelé osobních organizérů s aplikací umožňující přístup k WAP službám.

GSM banking tedy umožňuje ovládat účet prostřednictvím mobilního telefonu. Klient tak může některé transakce vyřizovat v podstatě odkudkoliv, kde má potřebný signál. Spektrum služeb jednotlivých bank v rámci GSM bankingu se liší. Zatímco některé nabízejí touto cestou pouze informace o zůstatku na účtu, jiné umožňují zadávání jednorázových i trvalých příkazů k převodu peněz, zakládání termínovaných vkladů a nebo třeba dobíjení předplacených karet.

Phone banking

To není nic jiného než komunikace s bankou a správa účtu prostřednictvím běžného či mobilního telefonu (musí mít možnost tónové volby). Stejně jako u GSM bankingu je možné touto cestou zjišťovat informace i zadávat příkazy, případně zakládat termínované vklady. Na rozdíl od GSM bankingu se u této služby neposílají příkazy bance, ale volá se na dané telefonní číslo - u některých bank je to dokonce i bezplatná linka - a veškerá komunikace probíhá buďto s automatem, nebo s operátorem či operátorkou.

Zvolí-li klient komunikaci s automatem, dostává instrukce podobně jako u hlasové schránky mobilního telefonu a příkazy zadává prostřednictvím klávesnice telefonu. Při komunikaci s operátorem (telefonním bankéřem) je možné dávat příkazy přímo hlasem. Služba je přitom zabezpečena buďto PIN-kódem, nebo heslem.

Internet banking

Zatímco pro využití home bankingu je nutná speciální aplikace, internet banking - nejnovější představitel elektronického bankovnictví - nic takového nevyžaduje. Klient musí mít pouze přístup k internetu a vhodný internetový prohlížeč. Klient tak může přistupovat k účtu z jakéhokoliv počítače připojeného k internetu, pouze se přihlásí k webové stránce banky a může pracovat.

Zabezpečení přenosu je přitom podobné jako u home bankingu. Banky jej řeší různě - například eBanka využívá kód generovaný speciálním autorizačním "kalkulátorem" a Živnostenská banka zase používá speciální autorizační program, který lze přenášet na disketě. Přenos mezi bankou a počítačem je přitom vždy kódován.

Standardizace

Normy v tomto segmentu elektronických platebních systémů jsou velmi skromné. Vyjímku tvoří Homebanking Computer Interface (HBCI), Open Financial Exchange (OFX) a Bank Internet Payment System (BIPS). Definují, jak mají vypadat systémy pro širokopásmou výměnu finančních dat a instrukcí mezi zákazníky a jejich finančními institucemi bez prostředníka. Výměna těchto informací probíhá na základě dialogu "request and response" (žádost a odpověď).

3.2.3. Elektronická peněženka

Elektronická peněženka (Electronic Wallet) je aplikace či služba, která pomáhá zákazníkům při on-line platebních transakcí tím, že si pamatuje tyto transakce, údaje o zákaznícím, obchodnících a další platební informace, které využívá k automatickému vyplňování údajů na obchodníkových stránkách a ulehčuje tak zákazníkovi samotné

nakupování. Zákazníci při používání elektronických peněženek mají také výhodu toho, že jejich informace jsou šifrovány a chráněny osobním kódem. Obchodníci zase využívají zvýšené ochrany proti platebním podvodům.

Je třeba říci, že pod pojmem elektronická peněženka se skrývají různé koncepty, které mají své specifické rysy a funkce, a které v současné době rozhodně nedosahují shody co se týká jejich charakteru a používání.

Elektronické peněženky byly implementovány mnoha různými způsoby: vestavěné komponenty v prohlížečích, pomocné aplikace prohlížečů, samotné klientské aplikace, serverové aplikace. Jednoduše řečenom, můžeme je rozdělit do dvou hlavních skupin: klientské a serverové. V rámci tohoto dělení jsou peněženky, které pracují pouze na stránkách určených obchodníků a pak ty, které mohou spolupracovat s různými obchodníky. Dnes existuje velké množství různých el. peněženek, mnoho z nich však je spojeno s mikroplatebními službami, které již nefungují a tak se snaží najít uplatnění

3.3 Platební mechanismy

V této kapitole se blíže seznámíme s dostupnými platebními mechanismy, které jsou rozděleny do několika oblastí dle použití. Tou první jsou kreditní, debitní a dobíjecí karty.

3.3.1. Platební karty

Většinu mechanismů pro platební karty určují normy organizace ISO. Normy ISO jsou mezinárodní normy, vydávané International Organization for Standardization (ISO) se sídlem v Ženevě. Tvorbou mezinárodních norem jsou pověřeny technické komise ISO. Mezinárodní standard ISO 8583 je použit při výměně informací mezi vydavatelem platební karty a bankou obchodníka při samotné platební transakci. Standardizace čipových (smart) karet je trvalý proces, který vychází z ISO 7816, což je norma popisující kontaktní identifikační karty s integrovanými obvody.

ISO 7816	Popis
ISO 7816-1	Fyzické charakteristiky
ISO 7816-2	Rozměry a umístění kontaktů
ISO 7816-3	Elektronické signály a přenosové protokoly

ISO 7816-4	Příkazy pro výměnu informací
ISO 7816-5	Číselný systém a registrační procedura pro identifikaci aplikací
ISO 7816-6	Meziprůmyslové datové elementy

Všechny vydávané smart karty již dnes podporují CEPS (Common electronic purse specification), což jsou všeobecné zveřejněné požadavky pro všechny komponenty nutné k implementaci programu globální elektronické peněženky založené na existujících platebních infrastrukturách.

Další důležitou normou je ISO 10202, což je norma popisující bezpečnostní architekturu finančních transakčních systémů používající karty s integrovanými obvody.

ISO 10202	Popis
ISO 10202-1	Životní cyklus karty
ISO 10202-2	Transakční proces
ISO 10202-3	Vztahy šifrovacích klíčů
ISO 10202-4	Bezpečné aplikační moduly
ISO 10202-5	Použití algoritmů
ISO 10202-6	Verifikace držitele karty
ISO 10202-7	Správa klíčů
ISO 10202-8	Hlavní principy a celkový přehled

Existují však i jiné standardizační společnosti např.:

* BankCards - Skupina ICC Specification Working Group vytvořila specifikaci EMV pro čipové karty, provádějící finanční transakce
* ANSI - podvýbor pro identifikační karty vytváří americkou část ISO/IECJTC1/SC17 WG4
* CEN (Com 'te Europeen de Normalization) - vytváří standardy pro platební čipové karty
* ECBS (European Committee for Banking Standards) - bankovní standardy pro evropské banky

* ETSI (European Telecommunications Standard Institute) - vytváří evropské standardy pro karty a mobilní telefony

3.3.2. Mikroplatby

Mikroplatební služby se za účelem snižování nákladů stále více stávají tzv. pre-pay (platba předem) či post-pay (platba později) službami. U obou případů se často používá elektronická peněženka, která poskytuje další užitečné funkce pro zákazníky. Jak již bylo zmíněno, postupem času se zjistilo, že jen pár vyvolených může díky mikroplatbám udělat ten opravdový úspěch na trhu platebních systémů (např. PayPal).

Pro transakce s malou hodnotou vytvořilo v roce 1999 konsorcium W3C specifikaci Common Markup for Micropayment Per-Fee-Links, která umožňovala uživatelům platit za elektronická data kliknutím na speciální odkazy (nazývané per-fee-link), které byly naprogramovány tak, že již v sobě obsahovaly požadované informace o dané platbě. Tyto požadované informace byly definovány v různých polích pomocí URI (Uniform resource identifiers) a obsahovaly např. cenu, text, obrázek, nadpis, detaily o platebním systému, který se má použít, identifikaci obchodníka, použitý jazyk a znakovou sadu atd. Různé implementace této specifikace jsou použity v platebních systémech jako Cartio či NewGenPay.

W3C konsorcium (World Wide Web Consortium), snažící se vést web ke svému plnému potenciálu se v důsledku této hlavní činnosti začalo zajímat o vývoj v oblasti elektronické komerce. Svoji roli však již dnes vidí W3C spíše jako prostředníka k zdůraznění hlavních technologií pro elektronickou komerci a identifikaci společných infrastruktur potřebných v této oblasti. W3C se již nesnaží specifikovat bankovní systémy ani schémata pro různé aplikace elektronické komerce a v důsledku toho se rozhodlo, že pozastaví všechny specifikační procesy.

V roce 1999 byl uveden na trh nový mikroplatební systém Jalda společností Ericsson a Hewlett Packard, který představoval bezpečnou platební metodu pro mobilní služby, ale byl aplikovatelný i do jiných odvětvích. Systém mohl pracovat s online vydavately

stejně jako s jinými webovými službami (např. kasina, obchody, internetoví provideři atd.). Ericsson a Hewlett Packard doufali, že Jalda se brzo stane internetovým standardem. Dnes jsou však oficiální stránky systému Jalda nepřístupné a budoucnost tohoto platebního systému je velmi nejistá.

Mezi další mikroplatební schémata, která vznikala v době ne až zas tak dávné patří např. Millicent, PayWord, MicroMint, nebo například Mikroplatby založené na pravděpodobnosti či zatím úspěšný projekt Peppercoin založený na principu elektronické loterie. Blíže budou jednotlivá schémata vysvětlena v třetí kapitole.

3.3.3. Elektronické šeky a účtové převody

Zatímco v USA jsou platby pomocí papírových šeků stále vysoce populární, v Evropě tomu tak není a chuť používat je čím dál víc menší. Tento klesající stav mají na svědomí dva důvody. Prvním je zpracování u papírových šeků, které je drahé a ten druhý mají na svědomí debetní karty, při jejichž použití každá transakce vyžaduje elektronickou verifikaci dostatečné hotovosti na účtu. To znamená, že jde prakticky o skoro stejnou operaci jako při použití šeku a navíc mnohem pohodlnější a s dalšími výhodami.

Je jasné, že zde vzniká potřeba pro platební systém podobný šekům, ve kterém jsou finanční prostředky přenášeny z účtu banky plátce na účet v bance příjemce v čase, kdy dochází k samotné transakci. Z hlediska bank by bylo co nejvíce žádoucí využít existující mezibankovní sítě pro převod hotovostí. V této malé podkapitolce je podán zevrubný pohled na platebních schémata založená na elektronickém šeku a alternativní metody umožňující přenos hotovosti mezi bankovními účty během platby. Některé z těchto platebních systémů se snaží využívat maximum z existujících bankovních infrastruktur, některé pracují v tomto ohledu zcela samostatně.

Platební přenosy mezi centralizovanými účty

Jestliže mají dvě strany bankovní účty u dvou různých bank, tak se platba mezi těmito stranami může uskutečnit přímo převodem z účtu plátce na účet příjemce nebo alternativně se může použít nepřímé platby, kdy se udělí právo příjemci k převodu financí např. pomocí elektronického šeku. V každém případě musí být zajištěno bezpečné prostředí, které tuto platbu s následným mezibankovním vyrovnáním uskuteční.

Jestliže mají jak plátce, tak příjemce účet u stejné centralizované on-line finanční společnosti, tak je převod mnohem jednodušší. Plátce se bezpečně připojí k této společnosti a informuje ji, aby přesunula určitou sumu z jeho konta na konto plátce. Nejsou potřeba žádné finanční-clearingové sítě. Tento centralizovaný účtový model se stal právě díky internetu velice populární a vzniklo nespočet platebních systémů využívající tento přístup. Každé schéma obvykle nabízí několik metod k uložení peněz na centralizovaný účet, který je obvykle otevřen on-line pomocí bezpečného webového rozhraní, chráněného protokolem SSL. Množství informací, které jsou při otevření účtu požadovány, není tak velké jako při otevírání běžného účtu v bance, obvykle stačí jen jméno, adresa a kontaktní detaily vlastníka účtu. Tyto platební systémy nejsou řízeny regulacemi národních bank a neposkytují možnosti opravdových certifikovaných bank. Protože jmění těchto společností není striktně jištěno jako u tradičních bank, je limitováno množství financí, které může na takových účtech být (např. $10,000 či méně).

Nejoblíbenější metodou naplnění těchto účtů je použití platební karty, buď kreditní či debetní. Platba je připsána straně, která udržuje centralizovaný účet. Další možností je on-line převod financí přes normální bankovní účet. Několik společností využívá jinou možnost naplnění účtů a to pomocí předplacených karet koupených ve fyzických obchodech. Takové předplacené karty jsou široce používány zejména v telekomunikačních společnostech, kde se využívají k nákupu kreditu na telefonní hovory. Spíše než přímý nákup předplacených karet je u některých firem využíván tzv. odměňovací systém, kdy např. v RocketCash platebním systému můžete získat určitou

částku tak, že si koupíte oblíbený nápoj a pod víčkem najdete kód, pomoci kterého si na svůj účet připíšete nějaké peníze.

Protože existuje mnoho odlišných a nezávislých platebních účtových systémů, má typický uživatel několik takových kont, které používá. Proto vznikají systémy, které dovolují převádět finance i z jiného systému (v systému RocketCash může být váš účet převedena hotovost z jiných systémů např. Cybergold či Beenz). Toto mohou také usnadňovat nezávislé třetí strany, které si za to ovšem berou nějaký poplatek. Podobně funguje výměna jedné měny za druhou v bankách, kde se za to většinou taky něco platí.

V systémech, kde je možnost plateb typu uživatel-uživatel, bývá příjemce upozorněn na příchozí platbu emailem. Jestliže má pak příjemce v takovém systému zřízen účet, může si tuto informaci ověřit v systému sám, pokud není registrovaným uživatelem, musí se nejprve zaregistrovat. Pokud se příjemce do určité doby nezaregistruje a nepotvrdí příjem dané částky, jsou peníze vráceny zpět na účet plátce.

Protože každá transakce musí být potvrzena příjemcem, není tento postup vhodný pro zpracování více transakcí během dne. Aby však tyto platební modely mohli používat i internetoví obchodníci, vzniklo speciální rozhraní nazvané Application Programming Interface (API), které umožňuje integrovat platební systém do webu obchodníka.

Základní myšlenkou je to, že zákazník si může vybrat platební systém na webu, poté je přenesen na stránky platebního systému, kde se mu objeví detaily transakce. Zákazník se přihlásí do platebního systému a autorizuje platbu běžným způsobem (přes SSL spojení). Jakmile je platba provedena, je o tom informován obchodník a zákazník je přenesen zpět na obchodníkům web k dokončení transakce či k obdržení zaplaceného zboží.

Předplacené karetní systémy, stejně jako předplacené telefonní karty, neumožňují výběr peněz zpět ze systému a jedinou možností je utratit je všechny on-line. U jiných schémat zůstávají finance na on-line účtu do té doby, než jsou převedeny zpět

tradičními platebními instrumenty (peníze jsou připsány na platební kartu nebo jsou uloženy na normální bankovní konto).

Koncept elektronického šeku

Stejně jako jeho papírový kolega, obsahuje i elektronický šek instrukce pro plátcovu banku, které říkají, kolik peněz a na jaký účet se mají převést. Fakt, že šek je v elektronické formě a je transportován přes počítačovou síť může dovolovat větší flexibilitu jeho držiteli. Mohou se také využívat nové služby, jako například možnost okamžitého ověření dostatku financí k proplacení. Bezpečnost je zvýšena kontrolou digitálního podpisu. Šekové platby mohou být jednoduše integrovány do elektronických objednávek a fakturovacích procesů.

3.3.4. Elektronické transakce

Přesný popis této kategorie je mnohem rozsáhlejší než v předchozích kategoriích, a proto ji můžeme rozdělit do dalších kategoriích podle typu platby (např. kreditní, debetní), úrovně a detailu zprostředkování (např. platby související s obchodními procesy), typu provozovatelů (banky, technologičtí provideři atd.) a zda transakce zahrnuje prostředníka (banky a jiné finanční instituce, "virtuální" ekomerční organizace pro platební procesy).

Řešení pro elektronické transakce všeobecně provádí přesně stanovené scénáře těchto transakcí, zahrnující objednávky, platby a jiné procesy spojené s platbami, instrukce, procedury a protokoly pro přenos financí mezi účty. Z těch nejdůležitějších řešení stojí za zmínku OBI (Opening Buying on the Internet) a IOTP (Internet Open Trading Protocol), které definují celkovou platební architekturu z obchodního hlediska a jsou vytvořeny tak, aby vyhovovaly existujícím a současně budoucím platebním mechanismům. Z tohoto hlediska se na ně může nahlížet jako na všeobecné elektronické komerční systémy.

4. Návrh vlastního řešení

4.1. Elektronické platební systémy jako součást automatizovaného nákupního systému v super a hypermarketech

V návrhu svého řešení bych rád nastínil využití elektronických platebních systémů v rámci automatizovaného provozu hypermarketů, supermarketů či jiných obchodních provozů obchodních řetězců. Toto řešení by mělo napomoci nejen k úspoře pracovních míst a tím i snížení nákladů provozovatele, ale také ke zvýšení plynulosti nákupů, sníženi nebo zrušení front u pokladen, lepší informovanosti nakupujících o cenách zboží i okamžitý přehled o celkové ceně nákupu jako takového. Naopak se v tomto mém návrhu nechci zaobírat organizačními a „behaviorálními“ otázkami jedninců, jako i kontrolou „poctivosti“ nakupujících.

Celkový koncept mého řešení je složen z několika vzájemně spolupracujících části které dohromady tvoří funkční celek a zajišťují bezproblémový průběh „nákupní transakce“ která se skládá z částí:

1. Identifikační – log-in fáze
2. Nákupní
3. Kontrolní
4. Platební
5. Odhlášovací – log-off fáze

Celý koncept je založen a vzájemném propojení HW, SW, komunikačních a mechanických prvků v architektuře klient - server. Ať už to jsou centrální server, kombinované komunikátory se čtečkou čárkovch kódů a karet, bezdrátové vysílače a přijímače, snímací rámy, ale i ovládací SW pro všechny části systému spolu s připojením do centrálního bankovního registru k porvádění on-line platebních aplikací.

4.2 Definice 3 hlavních části systému

a) **server**: centrální server připojený vysokorychlostním vedením k centrálnímu bankovnímu středisku za účelem on-line prováděných platebních transakci, jakožto i správě databáze zákazníků a poskytující služby využívané stálými zákazníky
b) **klient**: minipočítač s dotekovým displayem, snímačem čárových kódů a čtečkou karet či identifikačních tokenů nebo jiného zařízení umožnujícímu autentizaci(snímač otisku prstu, očniho pozadi) a umožňující bezdrátové připojení s centrálním serverem a který je pevně připojen k nákupnímu košíku
c) **příslušenství**: ostatní zařízení jako otočné zařízení pro jednotlivý vstup a východ zakázníků, snímací rámová čidla, kontrolní váhová čidla na výstupu atd.

4.3 Popis jednotlivých částí nákupní transakcí

4.3.1 Identifikační (log-in) fáze

Jako první část celého návrhu uvádím část identifikační a to z důvodu, že tato část defakto nastartuje celý systém do provozu a až do okamžiku opuštění areálu a vyjmutí identifikačního media, nebo odhlášení se ze systému bude provádět nakupujícího celou dobu strávenou v areálu. Identifikace by měla učinit z neznámé osoby osobu systému známou a dle množství nabízených a zákazníkem využívaných služeb by pak měla po celou dobu poskytovat informace nebo nabízet služby tomu poměrné.
Hlavní rozdělění se skládá ze dvou veličin a to:

a) zákazník stálý, systému známy s využívanými službanmi nabízenými obchodním řetězcem
b) zákazník náhodný, který si přišel pouze nakoupit

Dle tohoto rozdělní by poté interaktivní nákupní systém nabízel buď jen základní informace o nakoupených položkách, cenách, celkovém součtu ceny zboží u náhodného zákazníka a nebo dle úrovně využívaných služeb se k předchozímu výčtu může přidat i historie předešlých nákupů, kalorické hodnoty, interaktivní recepty spolu s navigací kde

jsou potřebné výrobky uloženy, průvodce nakupním centrem nebo i pripojením k síti WWW s předem omezeným výběrem internetových stránek s recenzemi na zboží případně recepty atd. A mohl bych pokračovat dále, myslím si, že množství nabízených služeb touto formou je skoro nepřeberné.

Další důležitou veličinou je identifikační médium. V rámci zachováni bezpečnosti by se jednalo o dvouprvkovou identifikaci, tzn. kdy je k autentizaci potřeba užít 2 nezávislých autentizačních médií. Nejčastěji používanou kombinací je kombinace něčeho, co vlastním a co vím. Tudíž mnou použitá kombinace by používala následující prvky:

a) **co vlastním:** karta, token, otisk prstu, zornice
b) **co vím:** heslo, pin

Samotný proces autentifikace a defacto aktivace celého systému by měla následující jednoduchý průběh: nakupující příjde do obchodu, vložením karty (tokenu) do minipočítače integrovaném v nákupním vozíku by byl vyzván k zadání oveřovacího hesla(pinu), po autorizaci by byl nákupní vozík uvolněn a zákazník přihlášen k centrálnímu systému obchodního centra.

4.3.2 Nálkupní fáze

Jak už bylo řečeno, systém by měl být schopen zajistit kompletní nákup od příjezdu, přes nákup až po placení a odchod bez účasti obsluhujícího personálu pouze za účasti nakupujícího. Dosažení tohoto je možno zajistit přesunutím snímače čarového kódu z pokladny přímo na vozík a integrovat tento do minipočítače integrovaného do nákupního vozíku. Tímto by bylo zajištěno nejen ukládání cen do výpisu nákupu, ale zároveň by suploval tolik častokrát dobře schované informační cenové automaty, kde by zákazník byl okamžitě informován o aktuální ceně bez nutnosti pobíhaní a hledání příslušného zařízení. Samozřejmě že zákazník by měl plnou kontrolu nad soupisem nákupu a mohl by kdykoliv položky měnit, přidávat, odebírat, opravovat, či měnit mezi různými režimy formy potvrzování položek a to buď automatickým po přiloženi k senzoru, či s vynucený potvrzením na dotykovém displayi. jak jsem nadále zmínil

v úvodu, samozřejmě by tímto využití minipočítače nekončilo, ale dle statutu zákazníka by díky tomuto zařízení bylo možno dodávat spoustu jiných služeb jako:

- vyhledání sortimentu na schématické mapě obchodu a zakladní informace o něm s navigací až k hledanému zboží
- nahrání seznamu nákupu z flashky nebo bezdrátovým připojením (wireless, bluetooth, infrared) či jeho naprogramováním přímo do minipočítače s jeho následným sledováním zbývajících položek
- informace o dostupnosti produktu
- informace o akčním zboží
- interaktivní kuchařka s okamžitým zobrazením kde lze potřebné suroviny nalézt, popřípadě i s hlídáním kompletnosti nakoupených surovin s upozorněním na chybějící a dalšími vlastnostmi
- přehled o minulých nákupech
- přístup na stránky s recenzemi zboží a internetovými kuchařkami
- atd....

Celý proces fáze nákupu by probíhal asi následujícím způsobem: nakupující se pohybuje s nákupním vozíkem po prostoru provozovny a to ať už pouze dle svého nákupního programu, nebo jen tak a nakupující takříkajíc pohledem, nebo na základě informací získaných z informačního panelu na základě zadaných dat či s využitím navigace až na místo vystavení zboží. Zde proběhne proces nelišící se od běžného nakupování pouze doplněný o sejmutí čarového kódu ze zboží. Po sejmutí kódu se objeví specifikace výrobku jako jsou název, cena, kalorická hodnota atd. a dle nastaveného módu se zboží buď automaticky přiřadí na list nakoupeného zboží a nebo bude vyžadováno jeho potvrzení. Tímto způsobem bude probíhat celý nákup a ve své podstatě se toto nijak neliší od fáze běžného nákupu dnes. Samozřejmě že systém založený na smínání čarového kódu by byl k ničemu, kdyby takto výrobky nebyly označeny a proto toto vyžaduje řešení i u výrobků, které se čarovými kódy neoznačují, jako zelenina, či pečivo. Nákup zeleniny se již dnes řeší v některých provozovnách samoobslužným vážením kde zákazník získá samolepící cenovku s čárovým kódem a touto podobnou metodou byse dalo vyřešit i pečivo (kde by byl narozdíl od hmotnosti

uveden počet kusů) a nebo automaty, kde po navolení počtu kusů by byl vyexpedován požadovaný počet kusů již zabalený a čarovým kódem vybavený.

4.3.3 Kontrolní fáze

Samotná kontrolní fáze by měla fakticky předcházet samotné fázi placení, ale protže se strany zákazníka může ke kentrole dojít kdykoliv, ať už jen z toho důvodu, aby se podíval, zdali už má vše nakoupeno, nebo jen ohledně momentální ceny. Osobně bych ještě kontrolní fázi rozdělil na dva mechanizmy. A to:

a) kontrolu ze strany nakupujícího
b) kontrolu ze strany provozovatele

Nyní se na obě podívám blíže:
a) kontrola ze strany nakupujícího – jak jsem již uvedl výše, tato kontrola se týká převážně množství nakoupeného zboží či aktuální ceny zboží již nakoupeného. K tomu by měla sloužit hlavně konzole minipočítače, na které by se měl zobrazovat stav nákupu a to jak již jeho celková cena tak i počet nakoupených položek a dle požadavku i celý seznam zboží, který by měl nákup obsahovat. Samozřejmě toto je nuté spojit s vizuální kontrolou nakupujícího, tedy kontrola ze strany nakupujícího je interaktivní činnost požadující zásah nakupujícího.

b) kontrola ze strany provozovatele – jak jsem na začátku této části věnované mému vlastnímu řešení uvedl, nechci se zde zaobírat technicko – bezpečtnostími detaily ze strany provozovatele, ale dovolte mi tedy jen malou úvahu o tomto. Jak zabezpečit aby to, co má nakupující v košíku bylo opravdu sejmuto snímačem a tím bylo opravdu na seznamu nákupu, který se pak použije v platební fázi... Pokud se zamyslíme nad tím, jestli tuto zabezpečovací roli hrají dneska obsluhy pokladen, tak musíme rovnou říci že ne, i když určité vědomí toho, že někdo stojí mezi mnou a východem a bude žádat nahlédnutí do tašky, dokáže spoustu lidí odradit od nepravostí. Ale pravda je ta, že většinu kradeného zboží se povede odhalit až za pokladnami a to po spolupraci detektivu chodících po areálu či obsluh bezpečnostních videosystémů, neustále

sledujících areál provozovny a jejich spolupracovníků hlídajících východy. Takže tyto mechanizmy by pravděpodobně fungovali i nadále, ale já osobně bych navrhoval kontrolní váhový mechanismus v podobě váhy integrované do podlahy v místě průchodu platebním místem. Tato váha by byla vybavena 4 prohlubněmi ve vzdálenosti odpovídající rozteči koleček vozíku do kterých by tato kolečka lehce vklouzla a odečtená váha by se porovnávala s váhou produktů uvedených na seznamu nákupu plus váhou košíku a v případě rozdílu většího než je stanovený vahový rozptyl(a to jak do plusu tak i do minusu) by na toto byl upozorněn nakupující výstražnou hláškou.
V případě že toto nebude korigováno, po průchodu platebním místem spustí alarm umístěný v minipočítači na vozíku a ochranná služba provede kontrolu.

4.3.4 Platební fáze

Fáze placení spočívá pouze ze samotného zaplacení obsahu nákupního vozíku, přestože za tímto se skrývá několik činnosti.

1) detekce „zaparkovaného“ koše na platebním místě
2) inicializace aktivátoru platební transakce
3) potvrzení platby, případné nahrání účtenky na USB, pomoci wireless zařízení či zaslání na email
4) průchod platebním místem

Operace probíhá tak, že po najetí na váhu v platebním místě, detektor umístěný na tomto místě uzamkne průchozí zábranu která se oblokuje až po provedení platební transakce a aktivuje v minipočítači volbu pro platbu. Tato volba automaticky provede vyúčtování obsahu vozíku a aktivuje volbu „Potvrdit platbu“ , „Oprava“ a „Zrušit“.
V případě že je vše v pořádku, tlačítko „Potvrdit platbu“ provede platbu s nezbytnými autorizačními kroky a uvede možnost zaslání účtenky ať už na zařízení které máte u sebe (wireless nebo USB), případně na e-mail, odblokuje průchozí zábranu a nakupující opustí platební místo. V případě nedostatku zjištěného kontrolním mechanizmem je možno použít tlačitko „Oprava“ k načtení chybějícího kusu zboží či naopak k vymazaní zboží ze seznamu, které bylo omylem naskenováno, nebo které bylo posléze z koše

vybráno ale nevymazáno ze seznamu. Tlačítko „Zrušit“ by bylo použito v případě zrušení platební transakce v případě nutného dokoupení zboží, nebo většího zásahu do obsahu nákupu, aby nedocházelo k blokování platebního místa. Po úspěšném porvedení platby a opuštění platebního místa se můžeme odebrat k poslední čáasti a to odhlášení se ze systému a zaparkování koše.

4.3.5 Odhlášovací (log-off) fáze

Po úspěšném průchodu platebního místa pojedem košík zaparkovat na místo. Protože minipočítač bude napájen akumulátory, bude nabíjení řešeno přes spojovací kabely, které zajišťují vozíky proti odcizení. Zařízení na zamezení nepropojování vozíků a tedy zabránění jejich nabíjení by fungovalo na pricipu zvukové siganlizace, kdy po vyjmutí karty či tokenu a odhlášení se tímto ze systému a zároveň nepřipojení vozíku na zabezpečovací kabel by po určitém časovém úseku došlo ke zvukové signalizaci tohoto stavu. Taktéž průchod s vozíkem mimo areál provozovny by byl hlášen zvukovou signalizací integrovanou u vchodů a východů provozovny.

4.4 Zhodnocení návrhu

Ve zhodnocení mého návrhu bych nejdříve započal hodnocením kladných dopadů a vlivů při aplikaci modelu na reálný provoz a tím vlastně i odpovězení na otázku, zali bylo dosaženo cílů, které byly stanoveny v úvodu této práce. Hodonocení kladných dopadů rozdělím na dvě části a to na zhodnocení z pohledu provozovatele, podnikatele a na zhodnocení ze stran uživatele, zákazníka.

4.4.1 Zhodnocení dopadu na provozovatele

Nejvíce sledované hledisko z hlediska podnikatele-provozovatele je vždy hledisko ekonomické. Pokud mám zhodonit můj návrh z tohoto pohledu, je jasné, že v prvotní míře je nutno se zaměřit na návratnost investice. Toto je dáno převážně velikostí provozu, kde v dnešních hypermarketech dochází z důvodu vykrytí špiček k masove paralelizaci pokladních systémů, které napomáhají ke zvládnutí stále vetšího náporu kupujících na únosnou míru. Tím je provozovatel zatěžován nejen po stránce nákupu nových technologií v masivním množství, ale je nucen tvořit i k tomu patřičný počet

pracovních míst a příjímaní agendy s tím spojené, jako je plánování obsazení směn (ať už z pohledu dovolených, či vykrývání nákupních špiček), dovolených, nemocenských, vzdělávání pro zaměstnance, prostě poskytování přiměřeného pracovního prostředí. Ale jak jsem již řekl, toto je hodně závislé na velikosti provozu a proto se má práce týká především velkých provozů jako super a hypermarketů, které pomalu vytlačli všechny ostatní provozovny a v nichž se potkává stále více lidí. Samozřejmě je toto možné aplikovat i na menší provozy, ale zde by již bylo potřeba diskutovat, zdali by toto přineslo ty ony očekáváné výsledky. Moje řešení je tedy zaměřeno převážně na velké provozy, kde mohou plně ukázat výhody systému a přinést požadované úspory. Pokud se podíváme pohledem pořizovacích nákladů, tak pokud by se jednalo o nový provoz, nebyl by nárust až tak kritický, jak se dalo očekávat. V dnešní době jsou platební místa vybavena elektronickými zařízeními typu pokladen, snímačů čarového kódu, traaskačních smínačů platebních karet a jejich příslušenstvím, plus vybavení kóje pro pracovníka. Protože většina činnost, které se zde vykonávají, by byla polo nebo plně automatizována a práce pokladního by se přenesla na zákazníka, tudíž i náklady na vybavení platebních míst by sesnížili o patřičnou částku, která by se ovšem přenesla do vybavení nákupního vozíku, hlavně jejího elektronického komunikátoru. Protože dnes je každý vetší provoz vybaven serverem s uložištěm dat a plně zasíťován, nepředpokládám v této oblasti většího nárůstu výdajů, jen použití jiných technologii. I když v celku by zajisté, alespoň v dnešní, nebo blízké budoucnosti přinesli pravděpodobně navýšení prvotních nákladů, toto by bylo v celé šíři kompenzováno úsporou za pracovní sílu a s ní spojenou agendou a věřím že díky zkvalitnění poskytovaných služeb a zvýšení plynulosti nakupování a odstraněním čekacích dob u pokladen, i k dalšímu přílivu zákazníků a tím k dalšímu ekonomickému růstu firmy. **Z tohoto hlediska byl mnou zadaný cíl splněn.**

4.4.2 Zhodnocení dopadu na zákazníka

Z hlediska dopadu na zákazníka můžeme vytknout několik zásadních aspektů a to přenesení činnosti dnešního pokladního na nakupujícího, což nemusí být vždy vnímáno jako kladný aspekt a druhým aspektem je odstranění čekacích dob u pokladen což je jeden, ne-li úplně nejzásadnější problém velkých provozoven. Dle průzkumu agentury Incoma Research je toto hlavním nedostatkem dnešních velkýcjh provozoen a tímto

ukazatelem se řídí i nakupující, zdali jít nakoupit do toho či onoho obchodu a tudíž je to faktor silně ovliňující příliv či odliv zákazníků. **„To, co nakupující vnímají v první řadě, je rychlost odbavení a fronty u pokladen. Jde o slabinu hypermarketových řetězců,“** (Zdeněk Skála, Incoma Research, http://www.strategie.cz/scripts/detail.php?id=311058). A samozřejmě spolu s těmito hlavními aspekty jsou ruku v ruce další věci, usnadňující komfort při nakupování, převážně informačního charakteru. Pokud se vrátím k hlavním aspektům, tak přenesení veškeré činnosti na zákazníka by měla přinést pozitivní dopad ve smyslu okamžité kontroly jak ceny tak i všeho, co bylo do košíku a tím i na účet vloženo a odpadá tím pozdější řešení reklamací při markování zboží a pod. Na druhou stranu toto může na někoho působit i jako negativum, ale to především díky zakořeněným zvyklostem, že chce být obsloužen, přitom zejména při této činnosti je namístě místo slova obsloužen požít spíše slov zdržován a kontrolován. Předpokládám proto že tyto negativní pocity později plně převládnou pocity plně pozitivní z neomezené kontroly nad celým procesem nákupu s možností kdykoliv cokoliv změnit. Navíc odstranění čekajících front odpadne spousta frustrace a dokáže zpříjemnit nákup i lidem, kteří toto považují pouze za nutné zlo. **Pokud tedy shrnu celkový přínos pro zákazníka po zavedení mnou navrhnutého systému, usnadnit a spříjemnit nákup jako takový, i v tomto bodě bylo mého cíle dosaženo.**

5. Závěr

Většina elektornické komerce na Internetu je prozatím stále založena na technologiích, které jsou buďto ve fázích experimentu, nebo ve stádiu neustálého, ale o to překotnějšího vývoje. Mnoho z nich také není prozatím dostupných v plném rozsahu pro použití v rámci Internetu. Avšak dynamika a stálé zavádění nových technologií toto posouvá stále více ke každodennímu jejímu používání a pomalému pronikání do vetšiny domácností po celém světě. Mezi nejzajímavější technologie bezesporu patří:

- *Elektroničtí agenti* – samoučící se programy, které dle zadaných parametrů sami dokáži provádět určité operace, jakoby vykonávané „lidským“ operátorem (různé automatické vyhledávání a nakupování zboží dle zadaných parametrů, či sbírání informací atp.)

- *Smart cards* – karty opatřené mikroprocesorem, jejichž použití se řídí patřičnou kounfigurací a je možno je dále programovat (různé elektronické „peněženky“, karty s možností on-line update implementovaného SW atd.)

- Rozvoj biotechnlogie a jeji implementace jak do modelů rozhodování, tak i do modelů identifikace atd...

V dnešní době, kdy dochází k neustálému navyšování propustnosti sítí a rychlosti komunikace, která přestává být pomalu omezena přenosovými rychlostmi se taktéž neustále navyšuje rychlost vyřizování transakčních požadavků, což pomalu ale jistě spěje k naplnění termínu „on-line“, kdy tento termín nebude značit pouze to, že příkaz bych zadán tzv. „po drátě“ a na proběhnutí celé takto zadané transakce se muselo čekat různá časová údobí, ale kdy opravdu takto zadaná transkace proběhne okamžitě a defacto v jeden okamžik se odrazí na obou účastnických stranách.

K dalšímu rozmachu využití EPS zákonitě dochází také s přesunem možnosti využití provádění transakcí z počítačů na různá jiná zařízení denní potřeby, jako jsou handheldy, netbooky, telefony, televice, ruzné terminály a vůbec zařízení, která člověka neváží k jednomu místu a nebrání mu využívat tyto možnosti, ať se ocitne

kdekoliv a kdykoliv se nám zamane. Avšak EPS a technologie s nimi vyvýjené nám neumožňují pouze provádění různých finančních převodů, ale díky nim je možno také, jak jsem se pokusi ilustrovat v mé praktické části, implementovat spoustu dalších technologií, které se dají využít k zvelebování lidského bytí a defacto posunu reality zase trochu blíže tomu, o čem jsme před pár lety mohli číst pouze v knihách autorů sci-fi, díky jejich fantazii a vizionářství, kde již mnohé bylo předpovězeno mnoho let dopředu a spousta dalších věci je již ve stádiu ať už výzkumu, nebo se již pomalu realizují.

Použitá literatura

1. FRANCU, M. *Internet pro podnikatele*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-623-3.

2. FRIMMEL, M. *Elektronický obchod:právní úprava*. 1.vyd. Prospektrum. Praha. 2002. 321 s. ISBN 80-7175-114-6

3. GRUBLOVÁ, E. aj. *Internetová ekonomika*, 1. vyd. Ostrava: Repronis. 2002. ISBN 80-7329-006-6.

4. JAMES, L. *Phishing bez záhad*. 1.vyd. Grada Publishing. Praha. 2007. 281 s. ISBN 978-80-247-1766

5. KOSIUR, D. *Principy a praxe elektronické komerce*. Computer Press. Brno. 2000.

6. MÁČE, M. *Platební styk-klasický a elektronický*. 1.vyd. Grada Publishing. Praha. 2006. 220 s. ISBN 80-247-1725-5

7. MATYÁŠ, V. a KRHOVJÁK, J. *Autentizace elektronických transakcí a autorizace dat i uživatelů*. Masarykova univerzita. Brno. 2008.

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

9. SEDLÁČEK, J. *E-komerce:internetový a mobil marketing od A do Z.* 1.vyd. BEN - technická literatura. Praha. 2006. 351 s. ISBN 80-7300-195-0

10. SCHLOSSBERGER, O. a HOZÁK, L. *Elektronické platební prostředky*. 1.vyd. Bankovní institut. Praha. 2005. 144 s. ISBN 80-7265-073-4

11. TONDR, L. *Podnikáme s Internetem*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-729-9.

12. VRABEC, V. a WINTER, J. *Internet, podnikatelská příležitost nebo hrozba?*, 1. vyd. Praha. Management Press. 2000. ISBN 80-7261-026-0.

13. WOODS, A. a WILLIAM W. *Internetová tržiště B2B pro 21.století*. 1.vyd. P.Wimmer. Unhošť. 2004. 277 s. ISBN 80-239-3899-1

14. /online/ Historie a současnost elektronického bankovnictví a e-komerce. Dostupné na http://www.fi.muni.cz/usr/jkucera/pv109/2001/xcodl.html

15. /online/ Designing a Generic Payment Service; 212ZR055, IBM Zurich Research Laboratory, 29 November 1996. Dostupné na http://www.semper.org/info/

16. /online/ http://www.e-komerce.cz

17. /online/ http://si.vse.cz/archive/proceedings/1999/bezpecnost-elektronickeho-obchodu.pdf

Další zdroje:

FORD, W., BAUM, M.S. *Secure Electronic Commerce*, Prentice Hall, 1998

FRANCU, M. *Internet pro podnikatele*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-623-3.

FRIMMEL, M. *Elektronický obchod:právní úprava*. 1.vyd. Prospektrum. Praha. 2002. 321 s. ISBN 80-7175-114-6

GHOSH, A. K. *E-commerce security*, John Wiley, 1998

GRUBLOVÁ, E. aj. *Internetová ekonomika*, 1. vyd. Ostrava: Repronis. 2002. ISBN 80-7329-006-6.

HANÁČEK, P. *Security of Electronic Money*, in SOFSEM ´99, Lecture Notes No. 1521,
Spinger-Verlag, 1998, 107-121

JAMES, L. *Phishing bez záhad*. 1.vyd. Grada Publishing. Praha. 2007. 281 s. ISBN 978-80-247-1766

KOSIUR, D. *Principy a praxe elektronické komerce*. Computer Press. Brno. 2000.

LACOSTE, G. *SEMPER: A Security Framework for the Global Electronic Marketplace*, SEMPER document 431LG042, IBM France, August 1996

MÁČE, M. *Platební styk-klasický a elektronický*. 1.vyd. Grada Publishing. Praha. 2006. 220 s. ISBN 80-247-1725-5

MATYÁŠ, V. a KRHOVJÁK, J. *Autentizace elektronických transakcí a autorizace dat i uživatelů*. Masarykova univerzita. Brno. 2008.

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

RUEPPEL, R. *Secure Banking over Internet: Recommendations from European Committe for Banking Standards*, ERCIM NEWS, 30, July 1997

SEDLÁČEK, J. *E-komerce:internetový a mobil marketing od A do Z.* 1.vyd. BEN - technická literatura. Praha. 2006. 351 s. ISBN 80-7300-195-0

SENDROVIC, I. *Security of Electronic Money*, Report by the Committe on Payment and Settlement Systems and the Group of Computer Experts of Central Banks of Group of Ten Countries (G-10), Basilej, ISBN 92-9131-119-7, 1996

SCHLOSSBERGER, O. a HOZÁK, L. *Elektronické platební prostředky*. 1.vyd. Bankovní institut. Praha. 2005. 144 s. ISBN 80-7265-073-4

TONDR, L. *Podnikáme s Internetem*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-729-9.

VRABEC, V. a WINTER, J. *Internet, podnikatelská příležitost nebo hrozba?*, 1. vyd. Praha. Management Press. 2000. ISBN 80-7261-026-0.

WAIDNER, M. *Open Issues in Secure Electronic Commerce*, in Final report of the ACTS Project AC026, SEMPER, 1998

WOODS, A. a WILLIAM W. *Internetová tržiště B2B pro 21.století*. 1.vyd. P.Wimmer. Unhošť. 2004. 277 s. ISBN 80-239-3899-1

ZLATUŠKA, J. *Analýza podmínek pro přechod ČR k informační společnosti*, Zpráva pro Radu vlády ČR pro výzkum a vývoj, duben 1998

ZLATUŠKA, J. *Srovnání vybraných charakteristik přechodu k informační společnosti v ČR a ve světě*, Zpravodaj ÚVT MU, Masarykova universita Brno, prosinec 1998

/online/ ECBS TC4, TR401, Secure Banking over Internet, March 1997, http://www.ecbs.org/download.html

/online/ Electronic Commerce and European Union, http://www.ispo.cec.be/Ecommerce/

/online/ http://www.e-parcel.org , domovská stránka firmy E-Parcel

/online/ http://www.surety.org , domovská stránka firmy Surety Digital Notary

/online/ UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, UNCITRAL, 1996, http://www.un.or.at/uncitral/en-index.htm

Rejstřík: