

On-line platby a jejich zabezpečení

On-line Payment Methods and Their Security

Zuzana Mašláňová

Bakalářská práce
2018



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Zuzana Mašláňová**
Osobní číslo: **A14258**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Forma studia: **prezenční**

Téma práce: **On-line platby a jejich zabezpečení**
Téma anglicky: **On-line Payment Methods and Their Security**

Zásady pro vypracování:

1. Provedte literární rešerši na téma možnosti on-line plateb za zboží nebo služby.
2. Popište systémy pro on-line platby, které jsou využívány v současnosti.
3. V praktické části se zaměřte na vybrané metody a popište způsoby jejich implementace spolu s výhodami a nevýhodami daného řešení.
4. Popište postup při implementaci vybrané on-line platební metody do e-shopu.
5. Zaměřte se na bezpečnost on-line plateb a popište možnosti zabezpečení.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MÁČE, Miroslav. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.**
2. **ŠPAČEK, Bronislav. Nakupování na internetu. Vyd. 1. Praha: Computer Press, 2002, 95 s. ISBN 80-7226-612-8.**
3. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovníctví. Vyd. 1. Praha: Computer Press, 2000, 166 s. ISBN 80-7226-328-5.**
4. **STŘIHAVKA, Marek. Vaše bezpečnost a anonymita na Internetu. Vyd. 1. Praha: Computer Press, 2001, 87 s. ISBN 80-7226-586-5.**

Vedoucí bakalářské práce:

doc. Ing. Jiří Vojtěšek, Ph.D.

Ústav řízení procesů

Datum zadání bakalářské práce:

1. prosince 2017

Termín odevzdání bakalářské práce:

25. května 2018

Ve Zlíně dne 14. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 22.05.2018

Mašláňová

.....
podpis diplomanta

ABSTRAKT

V práci je rozebrána problematika elektronických platebních systémů a způsoby jejich zabezpečení. Cílem bakalářské práce je navrhnout řešení pro realizaci transakcí internetového obchodu.

Bakalářská práce se dále zabývá a popisuje možnosti elektronického platebního styku, bezpečnostními protokoly používanými k ochraně při komunikaci mezi servery a nejčastějšími praktikami podvodného jednání útočníků.

V praktické části je bakalářská práce zaměřena na výběr vhodného elektronického platebního systému pro internetový obchod. Detailněji popisuje možnosti a nároky na implementaci jednotlivých platebních systémů.

Klíčová slova: bezpečnost, elektronický platební systém, SET, SSL, OFX, 3-D Secure, BIPS, NPP, HBCI, implementace

ABSTRACT

The thesis deals with issues of electronic payment systems and ways of their security. The aim of the bachelor thesis is to design solutions for the realization of transactions of the e-shop.

Bachelor thesis deals with the possibilities of electronic payment system, security protocols used for protection during communication between servers and the most frequent fraudulent practices of attackers.

In the practical part, the bachelor thesis is focused on the selection of a suitable electronic payment system for the e-shop. It describes in detail the possibilities and requirements for the implementation of individual payment systems.

Keywords: security, electronic payment system, SET, SSL, OFX, 3-D Secure, BIPS, NPP, HBCI, implementation

Chtěla bych poděkovat doc. Ing. Jiří Vojtěškovi, Ph.D. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval. Také jsem vděčná zaměstnancům Raiffeisenbank, Komerční banky a Československé obchodní banky za informace a čas, které mi poskytli.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 ELEKTRONICKÉ PLATEBNÍ SYSTÉMY	11
1.1 PLATEBNÍ KARTY	11
1.1.1 Výhody a nevýhody platebních karet.....	14
1.2 PLATEBNÍ PROCESORY	15
1.2.1 Realizace platby přes platební procesor	16
1.2.2 Výhody a nevýhody platebních procesorů	18
1.3 WAP BANKING.....	19
1.4 INTERNETBANKING.....	20
1.5 HOMEBANKING	21
1.6 TELEFON	21
1.6.1 Phone banking	21
1.6.2 GSM banking	23
1.6.3 Bezkontaktní platba mobilním telefonem	24
2 BEZPEČNOST ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ	25
2.1 LIDSKÝ FAKTOR V ELEKTRONICKÉ BEZPEČNOSTI	25
2.2 PREVENCE	26
2.3 PROTOKOLY PRO ELEKTRONICKÉ PLATEBNÍ SYSTÉMY	28
2.3.1 Secure Electronic Transaction (SET).....	28
2.3.2 Secure Socket Layer (SSL)	29
2.3.3 Open Financial Exchange (OFX).....	29
2.3.4 3-D Secure.....	30
2.3.5 The Bank Internet Payment System (BIPS).....	30
2.3.6 Network Payment Protocol (NPP)	30
2.3.7 Homebanking computer interface (HBCI).....	31
II PRAKTICKÁ ČÁST	32
3 ZALOŽENÍ E-SHOPU	33
3.1 VÝBĚR E-SHOP SYSTÉMU	33
4 IMPLEMENTACE PLATEBNÍHO SYSTÉMU DO E-SHOPU	37
4.1 BANKOVNÍ PŘEVOD	39
4.1.1 Výběr podnikatelského účtu.....	40
4.2 PLATEBNÍ KARTY	41
4.2.1 Implementace platební brány do e-shopu	42
4.3 PLATEBNÍ PROCESORY	43
4.3.1 Implementace EPS PayPal do e-shopu provozovatele Webnode	44
4.3.2 Implementace EPS PayPal do vlastního e-shopu	46

4.3.3 Implementace EPS PayPal do eshop systému.....	49
ZÁVĚR	53
SEZNAM POUŽITÉ LITERATURY.....	54
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	58
SEZNAM OBRÁZKŮ	59
SEZNAM TABULEK.....	60
SEZNAM PŘÍLOH.....	61

ÚVOD

V důsledku globalizace trhu vznikla potřeba převádět finanční prostředky mezi kupními stranami co nejrychleji, nejlevněji a především v mezinárodním měřítku.

Prvními nástroji elektronického platebního styku se staly debetní platební karty, dalším významným posunem byl vznik speciálních telefonních linek pro provádění transakcí bez nutnosti banku navštívit, avšak největší rozmach byl zaznamenán s příchodem internetu.

S rozvojem bezhotovostního platebního styku je samozřejmě kladen velký důraz na bezpečnost prováděných transakcí, která je zde důležitým aspektem nejen pro převod samotný, ale také pro uživatele. Pokud uživatel nevěří v bezpečnost systému, nesvěří mu své prostředky a systém se stává zbytečným. Proto je práce zaměřena nejen na popis jednotlivých systémů, ale také na jejich bezpečnost.

Avšak i sebedokonalejší bezpečnostní systém může selhat vinou lidského faktoru, proto se práce zabývá i sociálním inženýrstvím a nejčastěji používanými podvodnými praktikami.

Praktická část je soustředěna na výběr a implementaci vybrané platební metody do internetového obchodu. Obsahuje důležitá kritéria pro výběr vhodné platební metody a popisuje tři nejčastější možnosti platby v e-shopu.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

Elektronickou transakcí můžeme nazvat každou metodu bezhotovostního převodu peněz z jednoho účtu na druhý, uskutečněného pomocí elektronické reprezentace platebních nástrojů – obvykle přes síťové spojení. [1]

Základním a nejdůležitějším prvkem těchto systémů je vysoká míra jejich zabezpečení. Na druhém místě jsou nízké náklady na prováděné transakce. [1]

Dobrý platební systém musí být navržen tak, aby byl nezávislý na různých platformách a počtu uživatelů. Provozovatel systému musí být zároveň držitelem licence vydané centrální bankou. Každá z platebních transakcí musí být provedena kompletně a současně musí být jednotlivé transakce na sobě nezávislé. [1, 2]

Základními elementy v takovém systému jsou plátce, příjemce a finanční instituce. Finanční institucí je ve většině případů banka. Avšak se zde můžeme setkat i s tzv. třetí stranou. Například u převodu peněz přes platební procesory (PayPal, 2Checkout, aj.). [3]

1.1 Platební karty

Platební karty patří v dnešní době mezi nejpoužívanější instrumenty platebního styku. Nejsou však regulovány zákonem, nýbrž jejich vydavatelé, tedy bankami. Ty se řídí regulacemi mezinárodních asociací a pravidla pro vydání a používání platebních karet stanovují svým klientům v obchodních podmínkách, jež jsou součástí smlouvy o běžném účtu nebo samostatné smlouvy. [2]

Majitelem platební karty není klient, ale instituce, která platební kartu vydala. Uživateli je platební karta pouze zapůjčena k užívání za určitých podmínek stanovených emitující institucí. [2]

Náležitosti platebních karet podléhají mezinárodním standardům, které určují mezinárodní karetní asociace. [2]

Každá karta musí obsahovat následující prvky:

- označení vydavatele, tedy název a logo příslušné banky,
- číslo platební karty – 16 až 19 numerických znaků, první dva určují druh karty, následujících pět znaků identifikuje banku, která kartu vydala a zbylé znaky identifikují držitele karty,

- část čísla BIN (Bank Identification Number) – číslo přidělené dané bance karetní asociací,
- platnost platební karty – datum začátku a konce doby platnosti, přičemž začátek není nutný, ale konec platnosti musí být uveden vždy,
- jméno držitele karty s omezením do 27 znaků,
 - v případě služebních karet je uveden i název podniku
- podpisový proužek – vzor podpisu držitele karty,
- záznam dat.

Účastníky bezhotovostní transakce provedené platební kartou jsou:

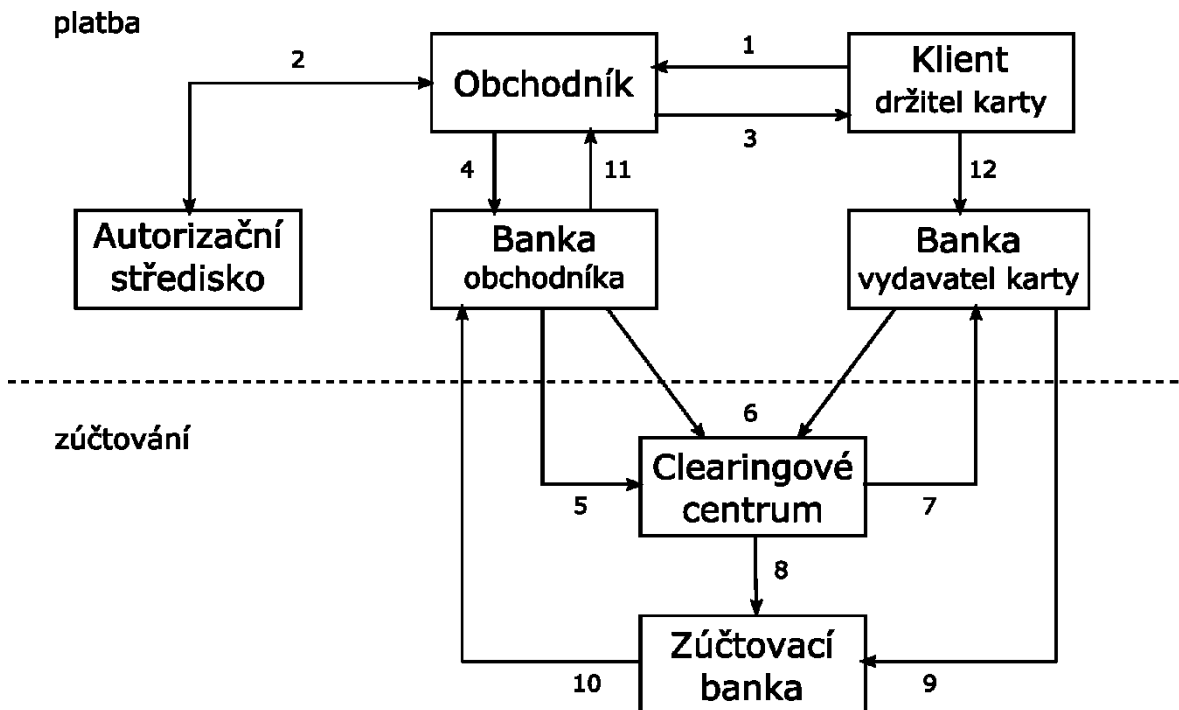
- Držitel karty (plátce).
- Banka (emitující instituce).
- Banka (obchodníka).
- Obchodník (příjemce).
- Autorizační středisko.

Celý proces platby kartou je zobrazen na obr. 1 a probíhá následovně. Při platbě za produkt nebo službu poskytne držitel karty údaje z ní obchodníkovi, ten údaje odešle do autorizačního střediska. Tam jsou zkontrolovány ochranné prvky na kartě – kontrola čísla karty, doby platnosti karty, a jestli byla zapsána na seznam zakázaných karet (odcizena). Dále ověří finanční krytí, tedy je-li na příslušném účtu dostatek financí. V případě potřeby i PIN kód (Personal Identification Number). Celý proces trvá jen několik sekund. Je-li platba autorizována, vydá obchodník plátcovi prodejní doklad. [2]

Nyní přichází druhá část procesu, kterou již běžný uživatel nevnímá. Informace o platbě jsou odeslány bance obchodníka, ta zahájí tzv. clearingové zúčtování s bankou plátce (vydavatelem karty). [2]

Přenos transakce do clearingového systému probíhá online, pomocí sítě na níž jsou napojeny všechny banky provozující danou službu. Systém provede clearing (zúčtování vzájemných operací při bezhotovostních transakcích) všech uskutečněných plateb v průběhu celého dne a banky dostanou seznam transakcí, které jsou buď ve prospěch, nebo na vrub účtů jednotlivých klientů. [2]

Clearingové centrum vydá příkaz k vyrovnání sald, které provádí tzv. zúčtovací banka (centrální banka, jenž slouží jako zúčtovací centrum pro všechny komerční banky). [2]



Obr. 1. Průběh transakce provedené kartou a její zúčtování [2]

Legenda

- 1 předložení karty k placení obchodníkovi
- 2 autentizace platby
- 3 vystavení prodejního dokladu
- 4 předání informace o platbě bance obchodníka
- 5 předání informací o provedených platbách
- 6 clearingové zúčtování mezi napojenými bankami
- 7 předání informace o provedených platbách
- 8 příkaz k vyrovnání sald mezi bankami
- 9 zatížení nostro účtu banky, která kartu vydala
- 10 převedení částky na nostro účet obchodníka
- 11 připsání částky transakce snížené o bankovní provizi
- 12 zatížení účtu držitele karty částkou transakce

Zjednodušeně řečeno, zúčtovací (clearingová banka) na konci každého dne provede součet jednotlivých transakcí za celý den a provede zúčtování pomocí nostro účtů, které má každá banka u zúčtovací banky veden. Tímto způsobem je namísto několika tisíc transakcí provedena pouze jedna. [2]

1.1.1 Výhody a nevýhody platebních karet

Hlavním důvodem, proč banky svým klientům poskytují tuto službu a emitují platební karty je snížení nákladů. Banky různými způsoby vybízejí své klienty, aby platily u obchodníků přímo kartou nikoli hotovostí. Pomineme-li, že banka má za takovou transakci smluvně danou odměnu, jsou zde další dva hlavní aspekty.

Abychom se vrátily k otázce nákladů, pořízení a provoz bankomatů je velmi nákladný. Navíc pokud si na začátku měsíce klient vybere veškerý zůstatek, banka o tyto peníze přijde, zatímco by je mohla dále investovat a vydělávat.

Banky nevydělávají vlastními penězi, ale penězi svých klientů. Každá banka je licencovaná centrální bankou, u nás je to Česká národní banka. Ta stanovuje výši finančních rezerv, které banky musí mít na jejím účtu pro případ úpadku, jedná se o tzv. bankovníctví částečných rezerv. Ovšem až 98 % z peněz vkladatelů mohou dále investovat.

Ale i klienti bank z tohoto systému čerpají výhody. Mezi ty největší pravděpodobně patří rychlý a jednoduchý přístup k financím v podstatě v jakoukoliv denní dobu, kterýkoliv den týdne. Kvůli vyzvednutí peněžní částky již není nutné navštívit banku, čímž klienti šetří čas a nejsou limitováni otevírací dobou pobočky, navíc uspoří za poplatky spojené s výběrem hotovosti.

Některé banky nabízejí svým klientům různé benefity za používání platebních karet. Používáním platebních karet, při dodržení pravidel bezpečného používání, můžeme hovořit o vyšší bezpečnosti oproti držení hotovosti. [2]

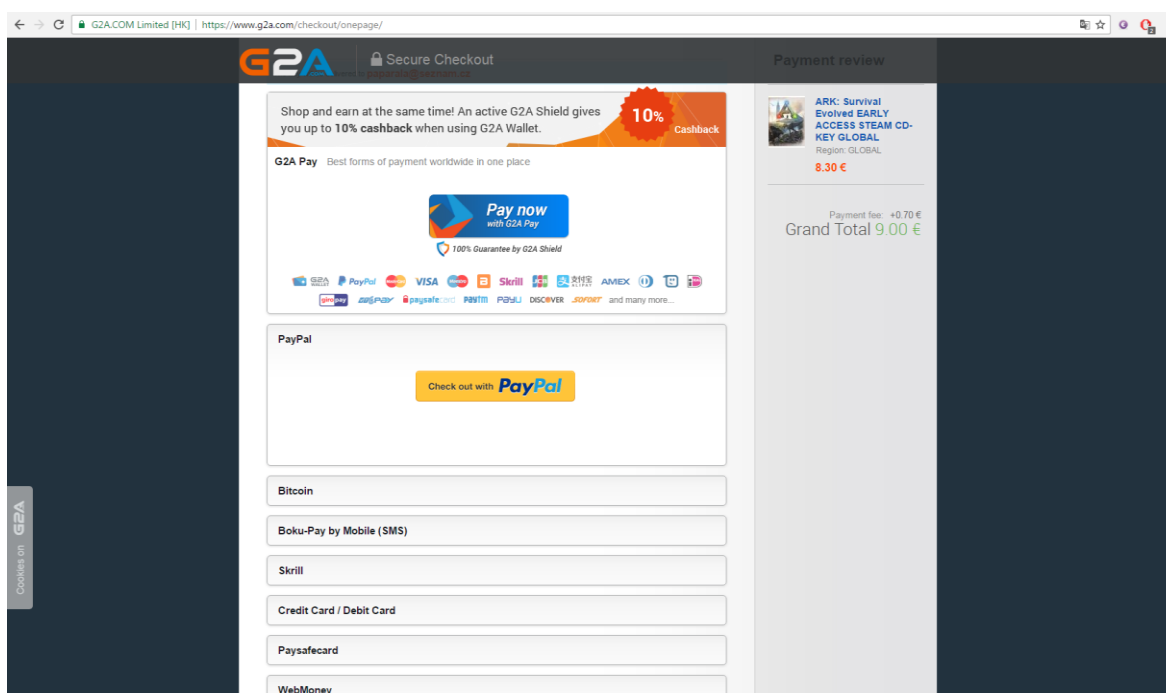
Avšak tento typ služeb skýtá i nevýhody a určitá bezpečnostní rizika. S vydáním či držením karty mohou být spjaty poplatky a zneužití karty je velmi jednoduché, pokud si ji držitel řádně nezabezpečí nebo v případě ztráty nezablokuje.

Nakonec jsou zde výhody pro obchodníky. Rozmach e-shopů není spojen pouze s nižšími cenami, než je to u produktů z kamenných prodejen, často jsou ceny za zboží stejné, někdy i vyšší. Dle psychologických průzkumů, lidé mnohem více utrácejí „virtuální“ peníze, než-li ty reálné. Navíc obchody nabízejí nejrůznější věrnostní programy, dopravu zdarma nad určitou hodnotu zakoupeného zboží, cashback apod. Zákazníci tedy utrácejí více a obchodníci mají větší obrat.

1.2 Platební procesory

Platební procesory nebo online peněženky jsou systémy zprostředkovávající transakci mezi obchodníkem a zákazníkem. Ačkoli některé z nich uvádějí ve svém názvu slovo „bank/banka“, opravdovými bankami nejsou. Jedná se o nebankovní společnosti, kterým byla vydána licence na zprostředkování plateb online platebními kartami některou bankou a autorizačním centrem. [3]

Společnost, jenž tuto transakci zprostředkuje, si účtuje určité procento z převedené částky. To je stanoveno ve smlouvě s obchodníkem, popřípadě v obchodních podmínkách pokud se jedná o převod v rámci jejich systému. Je na rozhodnutí obchodníka, zda-li poplatek za provedenou transakci uhradí on nebo jeho zaplacení bude požadovat od zákazníka. [3]



Obr. 2. Platba přes platební procesor navýšena o poplatek [4]

Mezi nejčastěji užívané platební procesory na českém trhu můžeme považovat mezinárodně nejrozšířenější PayPal, oblíbený především díky používání po celém světě nebo společnost Skrill, dříve známou pod jménem MoneyBookers. [5]

Z tuzemských společností, které operují i na mezinárodní úrovni, můžeme jmenovat například GoPay nebo PaySec. V případě tuzemských platebních procesorů můžeme považovat za určitou výhodu, že podléhají doзору naší centrální banky, kterou je Česká národní banka. [5]

1.2.1 Realizace platby přes platební procesor

Poté co zákazník zvolil způsob platby převod přes vybraný platební procesor, je přeměřován na zabezpečený server s platební formou daného platebního procesoru. Zde se buď přihlásí ke svému účtu, který má u společnosti veden nebo je vybídnut k vyplnění údajů ze své platební karty.

Humble Bundle

Your order summary

Descriptions	Amount
Purchase Amnesia: Fortnight 2017 (tr... Item description: Purchase Amnesia F... Item price: \$1.00 Quantity: 1	\$1.00
Item total	\$1.00
	Total \$1.00 USD

Choose a way to pay

▼ **Pay with my PayPal account** **PayPal**

Log in to your PayPal account to complete the purchase

Email

PayPal password

This is a private computer. [What's this?](#)

[Forgot your email or password?](#)

► **Create a PayPal account**
And pay with your debit or credit card

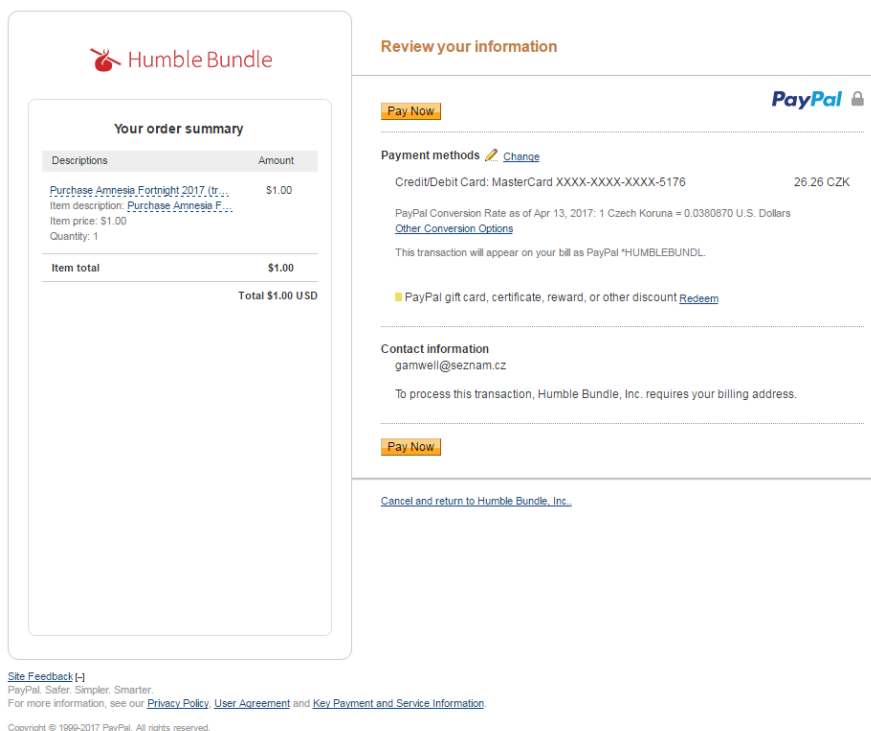
[Cancel and return to Humble Bundle, Inc.](#)

[Site Feedback \(+\)](#)
PayPal. Safer. Simpler. Smarter.
For more information, see our [Privacy Policy](#), [User Agreement](#) and [Key Payment and Service Information](#).

Copyright © 1999-2017 PayPal. All rights reserved.

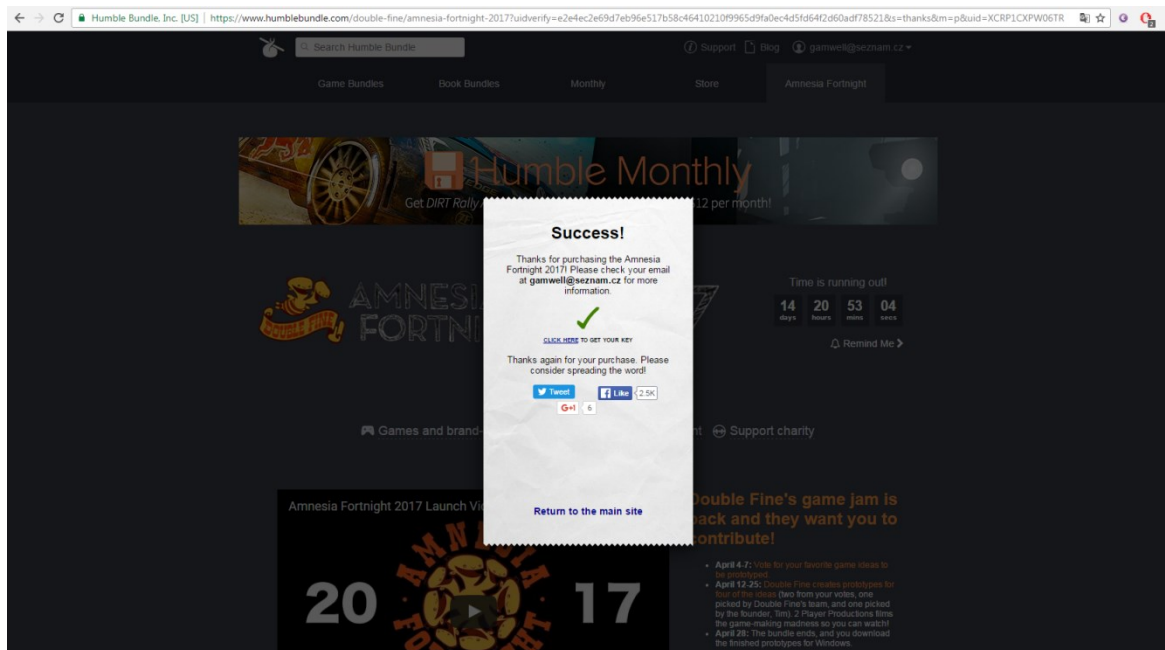
Obr. 3. Platební procesor PayPal – přihlášení [6]

Zákazník je vyzván ke kontrole zadaných údajů. Případně může zvolit jinou platební kartu.



Obr. 4. Platební procesor PayPal – kontrola údajů [7]

Po potvrzení se opakuje proces ověření a provedení transakce, jenž je popsán v podkapitole o platebních kartách. Pokud vše proběhne v pořádku, je zákazník přeměrován zpět na stránku obchodníka.



Obr. 5. Stránka obchodníka s potvrzením o úspěšné platbě [8]

1.2.2 Výhody a nevýhody platebních procesorů

Proč je tedy pro zákazníka výhodné upřednostnění této metody online transakce namísto přímého použití platební karty? Především proto, že nemusí poskytovat citlivé údaje ze své karty obchodníkovi. Celý proces transakce se děje prostřednictvím třetí strany a obchodník k těmto informacím nemá žádný přístup. Což je výhodou pokud tyto údaje nechceme obchodníkovi poskytovat nebo pokud jeho stránky nejsou řádně zabezpečeny. Samozřejmě v případě, že třetí straně důvěřujeme.

Tento způsob je oblíben především na aukčních portálech nebo v případě transakce mezi osobami, které se navzájem neznají a nedůvěřují si. Zákazník totiž sice zaplatí za zboží v momentě jeho nákupu, ale prodejce své peníze dostane teprve poté, co zákazník potvrdí přijetí zboží.

Dalším důvodem je jednoduchost celé transakce. Pokud máme u společnosti zajišťující tuto službu veden účet, stačí se přihlásit, zkontrolovat údaje a transakci odsouhlasit. Opět je zákazníkovi ušetřen čas a vyhne se případným komplikacím při chybném opsání údajů z platební karty.

Jak je patrné výše v textu, ne všechny platební procesory vyžadují registraci spojenou s vedením účtu. Některé fungují pouze jako zprostředkovatel platby, u jiných je založení účtu podmínkou. Většina společností založení a vedení účtu nabízí zdarma, ale některé vyžadují jednorázový registrační poplatek.

Po založení účtu a případném ověření uživatele, si klient může požádat o jednorázové převedení peněz ze svého bankovního účtu na účet u této společnosti nebo tyto účty propojit platební kartou. V takovém případě se ve vyúčtování každá následující platba zprostředkovaná daným platebním procesorem zapíše jako platba kartou.

Některé společnosti u provázání platební karty s účtem uživatele požadují ještě dodatečné ověření. Například společnost PayPal od svých klientů vyžaduje ověření platební karty tak, že z účtu, pro který je karta vedena strhne částku zhruba padesát korun českých, na vyúčtování pak klient společně se strženou částkou nalezne i čtyřmístný kód, který po zadání do systému kartu aktivuje a zmíněných padesát korun je připsáno na jeho účet, který mu společnost vede a může je dále využít, jedná se tedy pouze o ověřovací převod. Pokud by do

vypršení termínu tento čtyřmístný kód klient do systému společnosti nezadal, došlo by k vrácení částky na bankovní účet, ke kterému karta náleží. Na PayPal účtu by došlo ke smazání příslušné karty.

Pro prodejce tento způsob provedení transakce není tolik výhodný. Spíše navyšuje možnosti pro zákazníky nebo se používá v případě, že obchodník nemá stránky zabezpečeny.

Prodejce si musí založit u některé společnosti, jejíchž služeb chce využívat, obchodní účet. Registrace probíhá podobně jako u běžného účtu, s tím rozdílem, že společnost obvykle požaduje ještě další ověření, jako je například zaslání kopií dokladů (řidičský průkaz, telefonní vyúčtování aj.) k ověření adresy. [3]

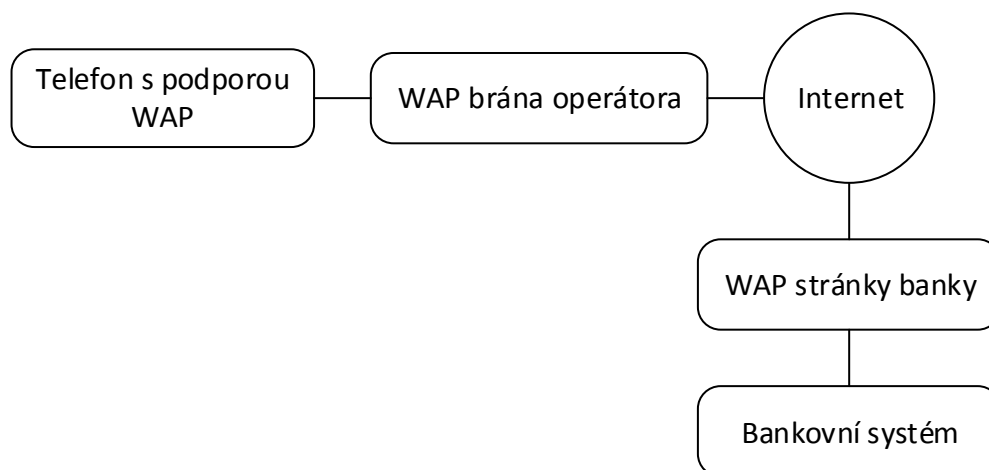
Po úspěšné registraci a následném ověření je účet aktivní a prodejce jej může využívat. Pokud jeho zákazník využije tento typ transakce, je obchodníkovi připsána finanční částka na jeho účet u společnosti snížená o poplatek za zprostředkování. Nevýhodou platebních procesorů je minimální objem pro převedení peněz z peněženky u společnosti na bankovní účet. [3]

Dále jsou zde vysoké poplatky při převodu na bankovní účet. Případně pokud je převáděná částka v cizí měně, banka tuto částku převede na korunu v druhém nejhorším kurzu. Při stržení poplatku bance a směně cizí měny na koruny může obchodník přijít o značnou část peněz. [3]

1.3 WAP banking

Jedná se o službu, která předcházela internetbankingu a pro její používání potřebuje uživatel pouze telefon s funkcí WAP (Wireless Application Protocol) a připojení k internetu – postačí GPRS (General Packet Radio service). Služba je zabezpečena šifrováním a ověření probíhá za pomoci autorizačního klíče. [9]

Uživatel se přes prohlížeč v mobilním telefonu přihlásí ke svému bankovnímu účtu a poté již může zadávat transakce, zjistit zůstatek na účtu atd. Spektrum poskytovaných služeb závisí na bance. [9]



Obr. 6. Komunikace s bankou prostřednictvím WAP [9]

Ačkoliv tuto službu ještě některé telefony poskytují, v současné době ji žádná česká banka nenabízí. Důvodem je malý rozsah služeb a nízký zájem klientů, je tedy považována za zastaralou a banky se zaměřují spíše na modernější nástroje jako například internetbanking. [9]

1.4 Internetbanking

V dnešní době už většina bank pro své klienty provozuje internetové bankovníctví. Jedná se o službu, která klientům banky umožňuje provádět změny na účtu, aniž by museli navštívit banku. Což vyhovuje jak klientům, tak usnadňuje práci jednotlivým pobočkám a šetří jejich náklady.

Pro ovládní internetového bankovníctví je třeba mít účet u banky, jenž tuto službu svým klientům poskytuje a přístup k internetu. Dále je nutné mít tuto službu u své banky aktivovanou. Pokud tomu tak není, stačí přijít na pobočku a nechat si internetbanking aktivovat.

Klient může prostřednictvím internetového bankovníctví posílat příkazy k jednorázové úhradě, nastavit inkaso, vidět aktuální zůstatek na účtu, zobrazit si podrobnou historii pohybů na účtu a banka mu eviduje i výpisy z účtu. Vše na jednom místě, takže má absolutní přehled o svých finančních tocích. [2]

Některé banky navíc svým klientům nabízejí prostřednictvím internetového bankovníctví možnost zřídit si spořicí účet, dobít předplacenou mobilní kartu, investovat apod. [2]

Veškeré bezhotovostní transakce, které banka provede mimo svůj interní systém, jsou realizovány prostřednictvím jejího účtu u clearingového centra. Pokud banka posílá peníze jiné bance, je tato částka z jejího účtu u clearingového centra odečtena a přičte se na clearingový

účet banky druhé a naopak. Na konci dne se všechny transakce sečtou a clearingové centrum provede pouze jednu platební operaci mezi centrem a bankou namísto milionů denně. [2]

1.5 Homebanking

Způsob komunikace mezi klientem a bankou prostřednictvím počítače s připojením k internetu a specializovaného softwaru. Charakteristickým rysem je vázanost na konkrétní počítač. Je využíván především firmami pro velké objemy transakcí. [9]

Homebanking má mnoho podob, odlišuje se v zabezpečení, použité technologii realizace jednotlivých operací i režimy, v kterých pracuje – offline, semi online, online. Lze jej pomocí speciálního softwaru propojit s internetovým bankovníctvím. [9]

1.6 Telefon

Snaha bank ušetřit náklady a zároveň nabídnout svým klientům zajímavé služby přinesla možnost disponovat se svým bankovním účtem prostřednictvím telefonu.

Zajímavostí může být i možnost přispět pomocí telefonního bankovníctví ke snížení chudoby a zlepšení životních podmínek v zemích třetího světa. [10]

1.6.1 Phone banking

Prostřednictvím telefonního bankovníctví může klient uskutečnit prakticky všechny základní bankovní operace. Ty můžeme rozdělit na tzv. aktivní a pasivní operace. [9]

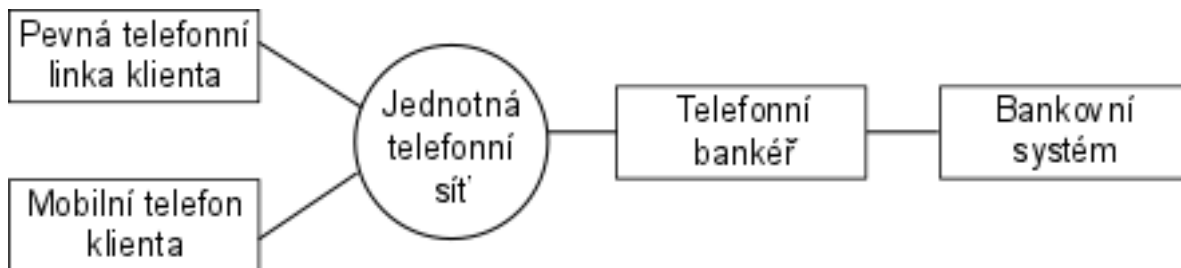
Mezi aktivní operace se řadí příkaz k úhradě, trvalý příkaz k úhradě, příkaz k inkasu, platba do zahraničí a založení, změna nebo zrušení termínovaného vkladu.

K pasivním operacím patří dotaz na zůstatek na účtu, informace o pohybech na účtu, informace o zadaných transakcích – provedených i neuskutečněných, informace o produktech a službách, které banka klientům nabízí, úrokové sazby a kurzovní lístek.

Za zřízení phone bankingu si účtuje většina bank poplatek, výše poplatku bývá do sta korun, dále je měsíční poplatek, ten se pohybuje v řádek desítek korun. [9, 11]

Provádění bankovních transakcí tímto způsobem bývá levnější než při zadávání na pobočce, avšak některé banky účtují svým klientům vyšší poplatky než u jiných nástrojů, právě proto, aby je přinutili tyto metody transakcí používat více. [9, 11]

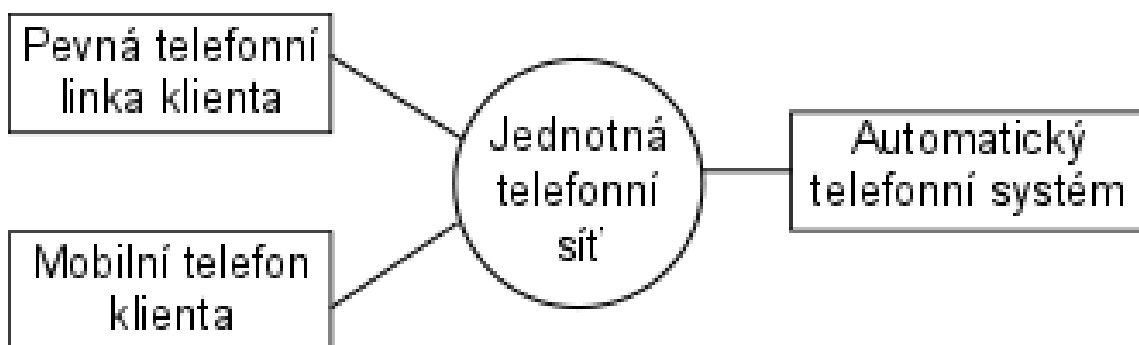
V počátcích vzniku telefonního bankovníctví existovala pouze tzv. call centra, do kterých zákazník zavolal a živý člověk na druhé straně po ověření totožnosti klienta provedl požadované operace. [9]



Obr. 7. Komunikace s bankou přes živého telefonního bankéře [9]

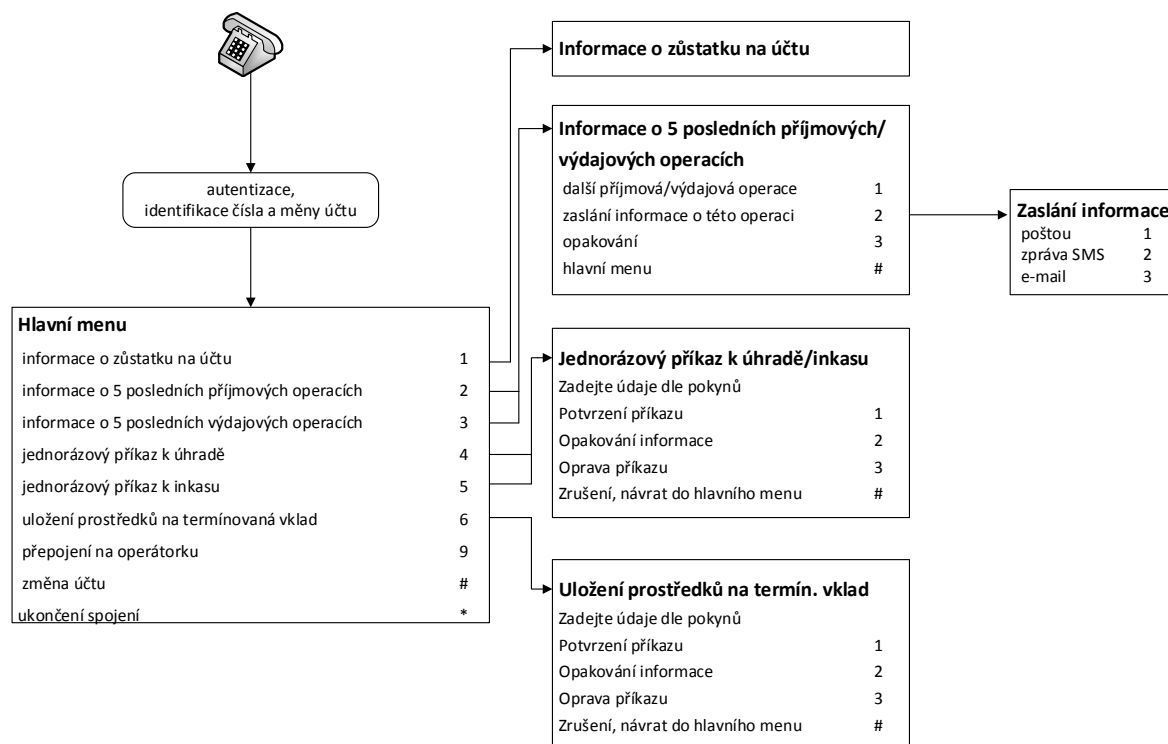
Tento systém funguje dodnes avšak s postupem času a v závislosti na vývoji technologií je možné, aby určité operace prováděl systém automaticky. Čímž banky opět ušetří, jelikož provoz takového systému je mnohem levnější než provoz telefonního centra a vyplácení mezd zaměstnancům. [9]

Podmínkou pro používání jakéhokoli automatického telefonního systému je telefon s tónovou volbou – přístroj každé jednotlivé číslici přiřadí jiný tón, systém tak rozpozná, jakou volbu jste zvolili. [9]



Obr. 8. Komunikace s bankou přes automatický telefonní systém [9]

V současnosti se nejčastěji můžeme potkat s kombinací obou. Pokud zákazník tuto službu zavolá, automat mu přehraje nejčastější volby a většinou jako poslední uvádí možnost přepojení na operátora. [9]



Obr. 9. Struktura automatizovaného telefonního systému [9]

1.6.2 GSM banking

Jedná se o ovládání bankovního účtu prostřednictvím krátkých šifrovaných sms zpráv. Využívání této služby však vyžaduje speciální sim kartu a telefon, který GSM banking podporuje. Jedná se o velmi bezpečnou metodu, navíc uživatel nepotřebuje přístup k internetu, postačí mu i slabý signál potřebný k odeslání sms zprávy. [9, 12]

Ačkoliv je tento systém velmi spolehlivý a bezpečný, je také zastaralý a mezi klienty bank nepříliš využívaný. Některé banky již tuto službu zrušily, jiné ji sice ještě stále provozují, ale aktivně ji zákazníkům nenabízejí a její další provoz plánují v brzké době ukončit. [9]

I když se jedná o velmi jednoduchý a bezpečný systém, jeho handicapem jsou nutnost zadávat veškeré údaje ručně, omezené bankovní služby a další. Pracné ruční zadávání řeší GSM SIM Toolkit. Uživatel musí vyplnit pouze požadované údaje, namísto zapamatování jednotlivých hesel. [9, 12]

Banky se v současné době zaměřují spíše na internetové bankovníctví a především jeho zabezpečení. [12]

1.6.3 Bezkontaktní platba mobilním telefonem

Platit v obchodech mobilním telefonem stejně jako platební kartou se aktuálně stává velmi oblíbeným trendem a díky své popularitě je její vývoj zaměřen nejen na poskytování bankovních služeb, nové bezpečnostní technologie – například ověření otiskem prstu, ale také další bonusové služby, z nichž můžeme zmínit třeba uschovávání účtenek, jenž svým klientům slibuje ČSOB. [13]

Jedná se o novou metodu, která se bude nadále vyvíjet. Pro zaplacení pomocí mobilního telefonu, potřebuje zákazník mít ve svém zařízení nainstalovanou aplikaci a na něm připojenou podporovanou platební kartu. Emitenty platebních karet jsou banky a je tedy důležité, aby banka zákazníka tuto metodu transakcí podporovala. V současnosti je služba nabízena ČSOB a KB, ale i další bankovní společnosti se chtějí v blízké době do tohoto projektu zapojit.

Služba je poskytována zdarma, navíc ČSOB své klienty motivuje finančním bonusem čtyřistakorun za dvacet provedených plateb, akce je však časově omezená. [14]

Další možností jak platit mobilním telefonem, je speciální SIM karta od poskytovatele telekomunikačních služeb, jenž má smlouvu s danou bankou. Tato volba skýtá jisté nepohodlí v případě, že zákazník má jiného operátora nebo účet u jiné banky a musel by si zřízovat nový účet. Navíc pokud si klient takovou SIM kartu zvolí, přijde o možnost LTE připojení.

Náhradní možností obou variant je samolepka, kterou zákazníkovi vydá banka a kterou si může nalepit například na mobilní telefon. Avšak už se nedá říci, že se jedná o platbu provedenou telefonem. [15, 16]

2 BEZPEČNOST ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

S nástupem elektronických plateb se také objevily obavy z jejich možného zneužití. Bankovní společnosti kladou na bezpečnost velký důraz, ovšem nejslabším článkem všech systémů jsou právě lidé.

2.1 Lidský faktor v elektronické bezpečnosti

Nejen v minulosti, ale i v dnešní době se objevují případy zneužití citlivých údajů vedoucích k obohacení útočníka. Napsat počítačový virus – nejlépe tak, aby byl nezjistitelný – je velmi časově náročné a vyžaduje určitý stupeň znalosti problematiky. Mnohem jednodušší je získat informace například prostřednictvím tzv. sociálního inženýrství.

Sociální inženýrství lze definovat jako způsob podvodného jednání či manipulace lidí, jehož cílem je získat utajené informace uživatele nebo organizace. [17]

Pretexting

Technika získávání informací za využití smyšleného scénáře, případně použití dříve zjištěné informace. Firmy své klienty ve většině případů prověřují relativně snadno dostupnými informacemi (jméno matky za svobodna, rodného čísla,...). [17, 18, 19]

Metodu využívají především soukromý detektivové, mohou tak získat od běžného zaměstnance výpis z účtu, výpisy hovorů atd. Získané informace lze využít při komunikaci se zaměstnancem na vyšší pozici. Tímto způsobem lze z drobných, mnohdy podceňovaných, informací vytěžit mnohem citlivější data. [17, 18, 19]

Quid pro quo

Quid pro quo neboli něco za něco je metoda podvodu, kdy útočník volá na náhodná čísla společnosti a vydává se za pracovníka technické podpory. V případě, že najde nespokojeného zaměstnance, nabídne mu pomoc. Může jej touto metodou přinutit třeba k instalaci infikovaného programu a získat tak přístup k jeho počítači nebo celé síti. [17, 18]

Baiting

Metoda je založena na zvědavosti či sobeckosti lidí, její název je z anglického slova bait, v překladu návnada. Útočník nastraží paměťové médium tak, aby jej oběť snadno našla –

například před domem, oběť se může domnívat, že médium patří členu domácnosti. Po vložení paměťového média do počítače dojde k instalaci viru, s jehož pomocí útočník získá přístup k počítači nebo k celé firemní síti.[17, 19]

Phishing

Jedná se o druh internetového podvodu. Prostřednictvím e-mailových zpráv jsou rozeslány podvodné maily obsahující výzvu k předání citlivých informací oběti. Zpráva vypadá například jako e-mail od banky klienta, kde ho žádá, aby na danou e-mailovou adresu odeslal své přihlašovací údaje. Jako záminku si může zvolit třeba změnu hesla nebo jinou operaci. [17, 18, 19]

Pharming

Propracovanější verze internetového podvodu, kdy se klient přihlásí do internetbankingu, ale je speciálním programem přeměrován na podvodnou stránku, vizuálně zcela totožnou s originálem. Útok je cílen na DNS server, který slouží k překladu IP adres na doménová jména. Uživatel není schopen rozpoznat rozdíl, zloděj získá přihlašovací údaje k jeho bankovnímu účtu, a pokud klient nepoužívá další zabezpečení, jako třeba potvrzení přes sms zprávu, je účet plně pod kontrolou hackera. [17, 18, 19]

2.2 Prevence

Nejdůležitějším bezpečnostním prvkem je vzdělávání v dané problematice. Dříve rodiče varovali své potomky před rozhovory s cizími lidmi, aby s nimi nikam nechodily a nic si od nich nebraly. V současnosti by mezi tyto poučky měli zahrnout i poučení o virtuální bezpečnosti a nejen pro mladší generaci, ale také poradit svým rodičům či prarodičům.

Nejlepší prevencí je nikomu nesdělovat osobní informace a poučit své okolí, protože útočník může dané informace získat jejich prostřednictvím. Neotvírat e-maily od neznámého či podezřelého adresáta a rozhodně nestahovat přílohy – mohou být infikované.

Důležité je také chování na sociálních sítích a při prohlížení webových stránek. Při brouzdání na webu se nabízejí vyskakovací okna, křičící slogany typu: „Vyhráli jste milion, pro výhru klikněte zde.“, po kliknutí získáte výhru v podobě škodlivého softwaru. Častými příčinami viru v počítači jsou stažená videa (Stmívání.exe), hry, hudba, software – velmi oblíbený zdroj obětí v době torrentů, mezi favority stále patřící porno stránky.

Na sociálních sítích lidé často postují fotografie interiéru bytu, stěžují si, co jim v domě nefunguje, pochlubí se, kdy, kam a na jak dlouho jedou na dovolenou...poté se majitelé vrátí z dovolené do holobytu. Zloději šli najisto, věděli jak se do bytu dostat, a kde jsou cenné věci.

U platebních karet by uživatel měl dbát nejen na svůj PIN kód, ale kartu by neměl vůbec zpřístupnit ostatním. Pokud útočník s platební kartou přijde fyzicky do styku, může si opsat nebo ofotit obě její strany, což mu pro placení na internetu zcela stačí. Při platbě jsou zadávány pouze údaje uvedené na kartě, pokud nemá oběť nastaveno potvrzování sms zprávami, limit pro transakce přes internet nebo přímo vypnutou službu elektronických transakcí, může přijít o všechny své finance.

S tím souvisí i doporučení, nemít na běžném účtu veškeré své peníze. Termínované účty sice nabízejí zhodnocení uložené částky, ale ta je po určitou dobu blokována. Klienti bank proto často nechávají na svém běžném účtu tzv. finanční rezervu pro případ, kdy by nutně potřebovali peníze. Řešením je zřídit si druhý účet, ke kterému klient nebude mít platební kartu a v případě potřeby si může peníze vybrat na pobočce banky nebo si je převést prostřednictvím internetového bankovníctví na účet jiný.

Pokud zákazník platí v kamenném obchodě kartou, měl by si uschovat nebo řádně zničit účtenku z POS terminálu. Také účtenky z bankomatů by měli být pečlivě uschovány nebo zničeny. Jedná se o doklady obsahující citlivé údaje. V dnešní době jsou obvykle z čísla karty viditelné pouze čtyři poslední číslice, ale není to pravidlem. Zloději stačí prohledat odpadkový koš, získá číslo karty a může jít nakupovat.

V některých internetových obchodech lze platit kartou i bez CVV/CVC (Card Verification Value/Code) kódu nebo bez PIN kódu. V tuzemských e-shopech je vyžádání CVV/CVC pravidlem, ale v jiných zemích tomu tak není.



Obr. 10. Rub platební karty s CVV2 kódem [20]

V moderní době rychlého bezkontaktního placení kartou, kdy limit pro zadání je 500 korun – pokud si klient u své banky nepožádá o změnu nastavení – není problém utratit roční úspory během pár hodin.

2.3 Protokoly pro elektronické platební systémy

Při přenosu nebo zadávání citlivých informací je žádoucí, aby tato data byla řádně zabezpečena. K zabezpečení se využívá mnoho druhů protokolů, z nichž je běžnému uživateli pravděpodobně nejznámější SSL (Secure Socket Layer) protokol, s kterým se může setkat například na stránkách internetového bankovníctví své banky. [21]

2.3.1 Secure Electronic Transaction (SET)

Jedná se o komplexní protokol zabezpečující elektronické transakce. Zajišťuje důvěrnost přenášených informací, ověření stran, mezi nimiž komunikace probíhá a integritu prováděných plateb. Využívá k tomu symetrické či asymetrické šifrování, hashovací funkce a digitální podpis. [21]

Symetrické a asymetrické šifrování

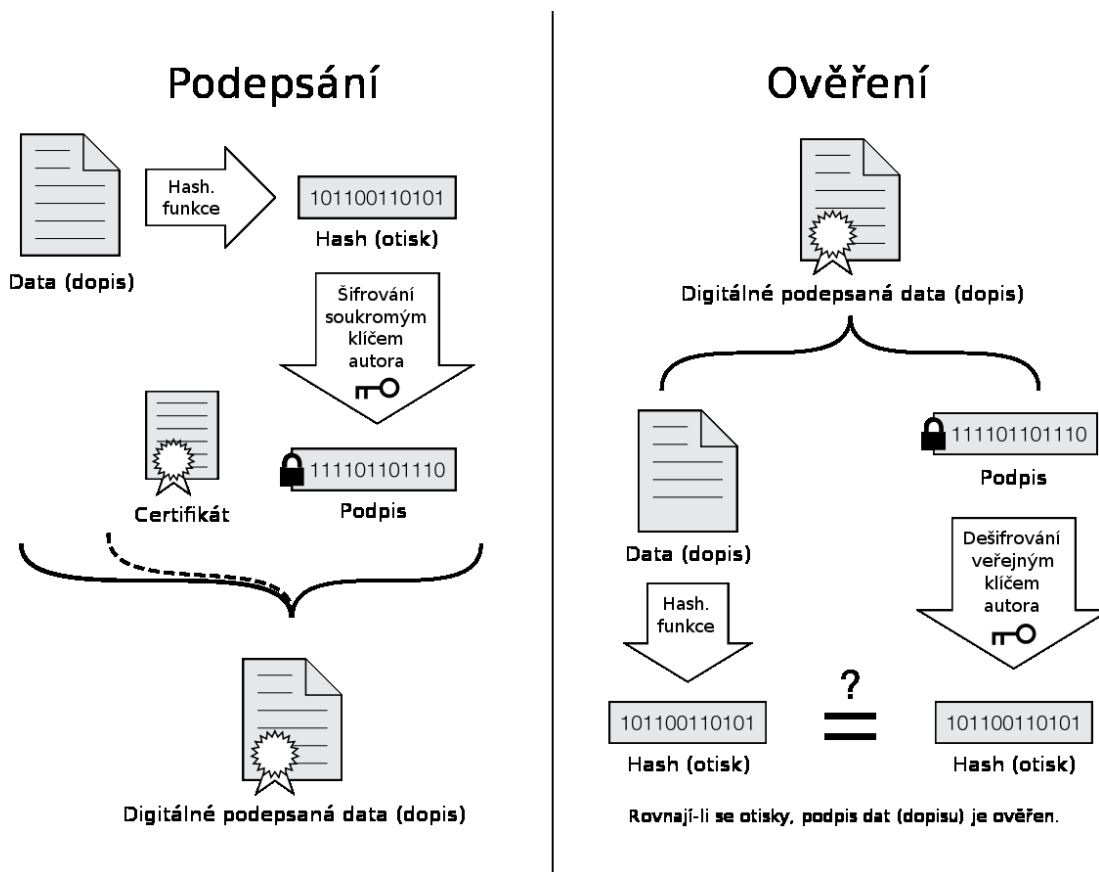
Zatímco u symetrického šifrování sdílí odesílatel i příjemce stejný klíč pro šifrování i dešifrování zpráv, pro šifrování asymetrické jsou použity klíče dva – veřejný a soukromý. Odesílatel zašifruje zprávu pomocí veřejného klíče, příjemce ji dešifruje klíčem soukromým. [21]

Hashovací funkce

Pomocí hashovacího algoritmu je daná informace převedena na tzv. hash – digitální otisk. Tento otisk se nedešifruje, ale pouze se porovná s již existující databází. Používá se například při přihlašování do systému. Výhodou je, že pokud by se do databáze někdo dostal, získané informace jsou pro něj bezcenné. [21]

Digitální podpis

Používá se pro ověření digitálních informací s využitím asymetrického šifrování a hashe. Odesílatel převede informace na hash, který zašifruje soukromým klíčem. Příjemce pro dešifrování použije veřejný klíč, a pokud se otisky shodují, zpráva je ověřena. [21]



Obr. 11. Digitální podpis [22]

2.3.2 Secure Socket Layer (SSL)

V současné době hojně používaný nekomerční protokol pro zabezpečení datových přenosů mezi serverem a klientem. Zajišťuje šifrování dat a autentizaci serveru digitálními certifikáty. Uživatel jej může poznat podle začátku url adresy „https://...“ případně ikonou zámku. [23]

SSL certifikáty používají asymetrické šifrování. Zabezpečení dat touto metodou je doporučeno pro všechny webové stránky shromažďující důvěrné informace a hesla. [23]

2.3.3 Open Financial Exchange (OFX)

Definuje standart pro přímou elektronickou výměnu dat mezi finanční institucí a jejím klientem. Systém funguje na základě požadavku a odpovědi (request-response systém), které jsou ukládány do textových souborů a následně formátovány pomocí XML (Extensible Markup Language). [21]

OFX aplikace zašle požadavek druhé OFX aplikaci, která zprávu zpracuje a následně vrátí odpověď s požadovanými daty. V momentě vytvoření zprávy, ji nelze dodatečně upravovat, protože zprávy jsou zabezpečeny různými hashovacími funkcemi. OFX podporuje SSL protokol, který zprávy šifruje a zajišťuje jejich integritu a autentizaci. [21]

2.3.4 3-D Secure

Protokol pracuje na bázi XML zpráv, které posílá přes šifrované SSL spojení. Šifrování probíhá pomocí digitálních podpisů, čímž je zaručena důvěryhodnost serveru i klienta. Používá se jako další vrstva zabezpečení při platbě kartou přes internet. [24]

Model je založen na principu tří domén:

Doména vydavatele – má na starost přihlašování držitele karty do systému 3-D Secure.

Doména nabyvatele – definuje proces sloužící k ověření identity nabyvatele, obchodník si tímto způsobem ověří, zda jedná s bankou, s kterou podepsal smlouvu,
– zodpovídá za zpracování autorizovaných transakcí.

Komunikační doména – usnadňuje přenos zpráv mezi doménou vydavatele a doménou nabyvatele.

2.3.5 The Bank Internet Payment System (BIPS)

Systém umožňující klientům zasílat zabezpečené platební instrukce přes webové rozhraní nebo e-mailem na server své banky, která tyto transakce následně uskuteční. [21]

BIPS schéma je založeno na infrastruktuře veřejných klíčů. Každý klient má X.509 certifikát používaný k vytváření podpisů a šifrování citlivých dat. Každá odeslaná zpráva je digitálně podepsaná a obsahuje certifikát odesílatele a jedinečný transakční identifikátor. [21]

2.3.6 Network Payment Protocol (NPP)

Platební protokol založený na systému BIPS, kde každá NPP zpráva je složena z několika atributů – typ a množství platby, detail příjemce a plátce a další. K šifrování zpráv se používají symetrické šifry. [21]

2.3.7 Homebanking computer interface (HBCI)

Specifikuje komunikaci mezi systémem uživatele a výpočetním centrem banky. Každá zpráva je složena z hlavičky, podpisové hlavičky, obchodních segmentů, podpisového traileru a samotné zprávy.

Zpravidla je k autorizaci uživatele do bankovního systému použito heslo. Každý uživatel má svůj digitální podpis. Pro šifrování se užívá symetrických i asymetrických šifer. [21]

II. PRAKTICKÁ ČÁST

3 ZALOŽENÍ E-SHOPU

Hlavním předpokladem pro založení e-shopu je jeho orientace, kterou by podnikatel měl zvážit již v podnikatelském plánu: Jaký druh zboží bude obchod prodávat? Kdo je zákazník? Bude obchod konkurenceschopný?

Business plán je důležitým pilířem podnikání. Odhaduje se, že polovina internetových obchodů nepřežije ani první rok svého provozu. Ačkoliv existují i případy úspěšných podnikatelů, jejichž podnikání žádný podnikatelský plán nepředcházelo.

Podnikatelský plán se vytváří především pro samotného podnikatele, aby mohl objektivně posoudit, zda je pro něj na trhu místo a je schopen své zboží prosadit a být konkurenceschopný.

Nejdůležitějším aspektem je zákazník. Ten si od nás zboží kupuje, proto ho naše nabídka musí oslovit, zaujmout, musí mít důvod proč nakoupit zrovna u nás. Zde je třeba provést průzkum, který ukáže, co zákazník hledá, očekává, co mu vadí na konkurenci a co mu můžeme nabídnout.

Častou chybou zákaznického průzkumu je provést analýzu nejčastěji vyhledávaných slov, tím sice zjistíme, co lidé nejčastěji vyhledávají, ale nedostaneme výsledek, který by nám řekl, co zákazníci požadují.

Zákazníci si vybírají zboží nejen na základě ceny či obsahu nabídky, ale zajímají je především záruky (spolehlivost obchodu, možnost vrácení zboží,...), komfort – jenž je jedním ze základních aspektů nakupování na internetu a další. Zákazník si nekoupí zboží jen proto, že ho máte ve své nabídce. [23]

S průzkumem můžeme začít ve svém okolí, například jaká služba zákazníkům u konkurence chybí, co by změnily, co je při výběru zajímavé a na co se ptají nebo jaké problémy řeší. Dobrým zdrojem informací v tomto případě může být třeba portál Heureka.cz, kde v sekci **Recenze** můžeme čerpat ze zkušeností zákazníků a získat zdarma cenné informace. [25]

3.1 Výběr e-shop systému

Na trhu se nabízí velké množství již hotových e-shopových systémů, některé si lze pronajmou nebo koupit, ale mnoho z nich existuje i s licencí opensource – jsou zdarma, avšak technická podpora není zprostředkována firmou, ale závisí pouze na pomoci ostatních uživatelů a příznivců na příslušném fóru.

Výhodou opensource řešení je nízká počáteční investice. Za systém samotný se neplatí, případnou pomoc může uživatel najít na příslušném fóru nebo u některých systémů lze podporu zakoupit.

Významnou investicí při vzniku internetového obchodu jsou lidé, kteří se starají o jeho chod – vybudování, aktualizace, přidávání nových produktů, vyřizování objednávek, atd. Pokud se jedná o prodej v malém měřítku a prodejce je schopen si vše zaopatřit sám, mohou být náklady s opensource minimální – pouze investovaný čas, ale nulové finanční investice.

Dalším řešením je pronájem či zakoupení licence. Výhodami pronájmu je především stálá a okamžitá technická podpora. Ceny pronájmu se liší i v závislosti na vybraném balíčku, kde základní řešení může být bezplatné – například FREE balíček od shoptet, jehož součástí je 19 modulů, možnost napojení na EET systém a prodej až deseti položek. [26]

Takové řešení je vhodné pro velmi malé či začínající obchody (s možností dalšího rozšíření) nebo na zkoušku, v případě že si nejsme jisti koupí dražšího balíčku. Pomineme-li tuto základní a velmi strohou verzi, pohybují se ceny pronájmů průměrně od 300 Kč do 5 000 Kč.

Licenci si lze pořídit již od deseti tisíc, uživatel však musí pamatovat, že si koupil pouze produkt a případnou podporu si musí dokoupit zvlášť. [27]

Byly vybrány čtyři různé systémy pro srovnání, jejichž krátký popis je níže. Detailnější přehled je v tabulce v příloze P II.

PrestaShop

Systém je postaven na PHP Smarty funkcích, je přeložen do více než 25 světových jazyků a jeho podpora je zajištěna na fóru, kde si aktivně pomáhá více než 500 000 uživatelů. Využívá funkci AJAX, díky které lze do obchodu přidat například různé moduly, z nichž jsou mnohé různými vývojáři poskytovány zdarma. [28]

Je zde poskytován průvodce nastavením, podporuje více měn a jazykové mutace. Provoz systému je na vlastní doméně, kterou si uživatel musí zajistit zvlášť. [28]

shoptet

Aplikace shoptet je také napsána v PHP jazyce s MySQL databází. Na rozdíl od Presta Shop je v ceně pronájmu započítán i hosting, avšak uživatel již nemá přístup ke zdrojovému kódu, veškerý servis zajišťuje společnost shoptet, s.r.o. [29]

BASIC	BUSINESS	NEJOBLIBENĚJŠÍ PROFI	ENTERPRISE
247 Kč / měsíc	842 Kč / měsíc	1 267 Kč / měsíc	2 117 Kč / měsíc
až 100 položek ?	až 1 000 položek ?	až 5 000 položek ?	až 40 000 položek ?
30 modulů v ceně ?	46 modulů v ceně ?	61 modulů v ceně ?	72 modulů v ceně ?
Připraveno na EET ?	Připraveno na EET ?	Připraveno na EET ?	Připraveno na EET ?
Pokladní systém ?	Pokladní systém ?	Pokladní systém ?	Pokladní systém ?
emailů: 3 ?	emailů: 5 ?	emailů: 10 ?	emailů: 15 ?
uživatelé: 3 ?	uživatelé: 5 ?	uživatelé: neomezeně ?	uživatelé: neomezeně ?
1 000 Kč na Google AdW ?	1 000 Kč na Google AdW ?	1 000 Kč na Google AdW ?	1 000 Kč na Google AdW ?
		+ dárek ZDARMA ?	+ dárek ZDARMA ?
OBJEDNAT	OBJEDNAT	OBJEDNAT	OBJEDNAT

Obr. 12. Shoptet – srovnání jednotlivých balíčků [26]

Nabízena je FREE verze, kde uživatel může prodávat 10 položek, má k dispozici devatenáct modulů, jeden uživatelský účet a jeden mail. Ceny dalších balíčků i s poskytovanými službami najdete na obrázku číslo 12. [26]

UPgates

Ceny balíčků UPgates jsou oproti cenám shoptet trochu vyšší, avšak do částky je započítána i cena za doménu druhého řádu, kterou obě předchozí aplikace neměly.

BRONZE	SILVER POPULAR	GOLD	PLATINUM
450 Kč/měsíc	1 450 Kč/měsíc	1 950 Kč/měsíc	2 950 Kč/měsíc
Všech 104 modulů - seznam	Všech 104 modulů - seznam	Všech 104 modulů - seznam	Všech 104 modulů - seznam
50 produktů	1 000 produktů	10 000 produktů	30 000 produktů
1 GB prostoru	3 GB prostoru	5 GB prostoru	10 GB prostoru
1 jazyk	Neomezeně jazyků	Neomezeně jazyků	Neomezeně jazyků
1 uživatel	Neomezeně uživatelů	Neomezeně uživatelů	Neomezeně uživatelů
Konfigurator grafiky - více	Konfigurator grafiky - více	Konfigurator grafiky - více	Konfigurator grafiky - více
Export / Import dat - více	Export / Import dat - více	Export / Import dat - více	Export / Import dat - více
E-mailing - více	E-mailing - více	E-mailing - více	E-mailing - více
Plná technická podpora	Plná technická podpora	Plná technická podpora	Plná technická podpora
Vyzkoušet zdarma	BONUS! 8 hodinový videokurz ZDARMA	BONUS! 8 hodinový videokurz ZDARMA	BONUS! 8 hodinový videokurz ZDARMA
Vyzkoušet zdarma	Vyzkoušet zdarma	Vyzkoušet zdarma	Vyzkoušet zdarma

Obr. 13. UPgates – srovnání jednotlivých balíčků [30]

Zakoupení licence není možné, poskytován je pouze pronájem, jehož cena se pohybuje od 450 Kč do 2 950 Kč měsíčně v závislosti na vybraném řešení. [30]

ShopSystem

Na rozdíl od výše zmíněných je kromě MySQL podporována databáze mariadb. Jsou nabízeny tři možnosti – Lite nebo Full verze a e-shop na míru. [31]

Lite verze je určena spíše pro menší e-shopy, oproti tomu Full verze disponuje mnoha pokročilými moduly a marketingovými nástroji. [31]

Měsíční pronájem Lite verze je 1 200 Kč a Full verze 2 200 Kč. Odkoupení licence je pro Lite verzi za 39 000 Kč a Full verze za 79 000 Kč. V ceně je hosting a technická podpora na dva roky, poté si klient musí platit 3 000/4 000 Kč ročně. [31]

4 IMPLEMENTACE PLATEBNÍHO SYSTÉMU DO E-SHOPU

Platební systém je klíčovým prvkem každého internetového obchodu. Nejen že usnadňuje práci a šetří čas majitele obchodu i zákazníků, ale také zvyšuje důvěryhodnost obchodu. Může být i důležitým faktorem při rozhodování zákazníka, který e-shop si k nákupu vybrat.

Obchodník by si měl stanovit kritéria, na jejichž základě zvolí správný platební systém nebo jejich kombinaci. Příkladem může být zaměření na určitou věkovou skupinu, zeměpisnou polohu, výši poplatku za provedenou transakci, náročnost implementace a další.

Především pro nezkušené a začínající podnikatele mohou být tato kritéria klíčová a rozhodnout mezi úspěšným začátkem kariéry nebo postupným zadlužením končícím krachem jeho společnosti.

Technologická kritéria [32]

- Způsob zabezpečení
 - způsob jakým je systém zabezpečen, a které technologie využívá
 - průběh autorizace plateb, pokud ji systém nabízí
- Náročnost integrace
 - časová náročnost
 - dovednostní požadavky na implementátora
 - podpora poskytovatele
- Cena implementace
 - vstupní poplatek
 - celková cena implementace
- Plug-in
 - úroveň integrace do systému e-shopu,
 - výčet systémů e-shopů, které jsou podporovány
 - API (Application Programming Interface) – definuje, jakým způsobem jsou volány funkce knihovny ze zdrojového kódu
- Způsob platby
 - možnosti plateb, které systém podporuje
 - způsob provedení transakce přes zvolený EPS
- Podpora od provozovatele

- role poskytovatele při napadení nebo výpadku systému
- možnost detailního náhledu obchodníka na průběh transakce
- informace sdílené poskytovatelem EPS obchodníkovi
- Notifikace
 - informovanost obchodníka a zákazníka o průběhu platby
 - způsob předání informací
 - míra poskytovaných detailů

Ekonomická kritéria [32]

- Poplatky pro obchodníka/zákazníka
 - výše fixního poplatku pro obchodníka za přijatou platbu a kolik procent z obratu požaduje provozovatel EPS, případně možnost individuálního nastavení
 - výše fixního poplatku pro zákazníka, pokud je stanoven
- Možnost přijímat více měn
 - možnost přijímat a vést účet ve více měnách
- Časová náročnost platebního procesu
 - délka platebního procesu
 - doba, za kterou bude obchodníkovi suma připsána na účet, a kdy ji bude moci plně využít
- Rozšířenost metody mezi zákazníky
 - cílová skupina
 - rozšířenost na trhu

Sociální kritéria [32]

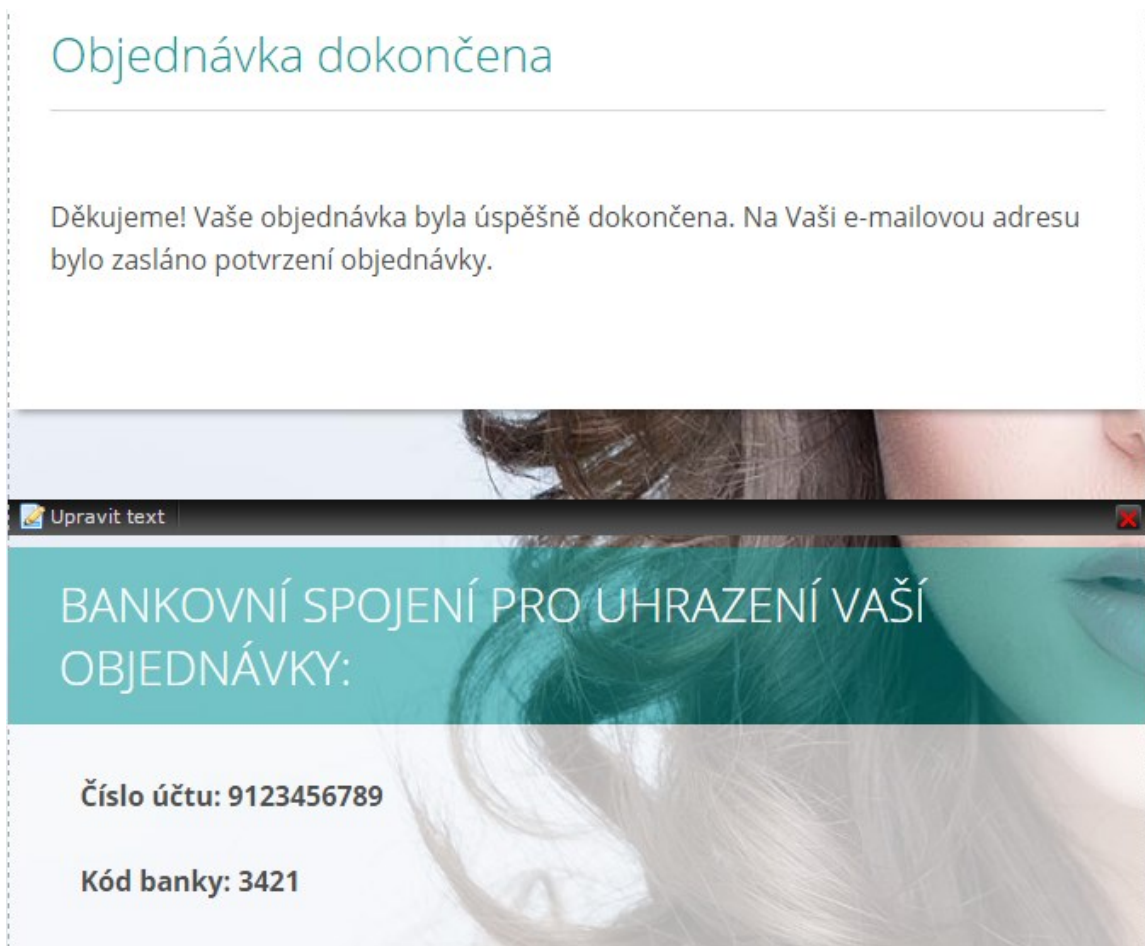
- Ochrana zákazníka
 - způsob ochrany citlivých informací zákazníka
- Jazyková podpora
 - jazyky, které jsou systémem nabízeny, případně možnost volby dle IP adresy zákazníka
- Uživatelské prostředí
 - Způsob navržení uživatelsky příjemného prostředí pro zákazníka, systém by měl být snadný a přehledný

- Mobilita systému
 - podporovaná zařízení, případně potřeba certifikátů pro komunikaci s daným systémem

4.1 Bankovní převod

Z pohledu implementace pravděpodobně nejsnadnější řešení, které zvládne i nezkušený uživatel. Další výhodou jsou minimální náklady, jelikož je stržen pouze poplatek za příchozí platbu – v případě jiných druhů online transakcí se k fixnímu poplatku zaúčtuje i procento z transakce, které je určeno ve smlouvě.

Provozovatel e-shopu navíc nemusí řešit technické zabezpečení platby, pouze sdělí prostřednictvím e-mailu nebo systémové stránky e-shopu svému zákazníkovi číslo účtu a částku, případně další údaje (variabilní symbol aj.).



Obr. 14. Systémová stránka – dokončení objednávky [33]

Zákazník si pak sám zvolí způsob úhrady, internetové bankovníctví, složenka, atd. Průběh transakce se odehrává mimo režii obchodníka a tím je zbaven odpovědnosti za bezpečnost převodu.

Ze zákona není stanoveno, že pro podnikání je nutné mít založen speciální účet, postačuje i běžný bankovní účet. Což je výhodné například pro živnostníky, jimž na účtu neprobíhá velký počet transakcí – vedení běžného účtu a případné poplatky jsou často nižší než u podnikatelských účtů nebo zpoplatněny nejsou. [34]

Ovšem ne všechny banky toto podporují. Ve svých obchodních podmínkách mohou deklarovat, že v případě zjištění využívání osobního účtu k podnikání bude tento účet zrušen a převeden na účet podnikatelský. [34]

4.1.1 Výběr podnikatelského účtu

Výběr podnikatelského účtu podle požadavků současných, ale i budoucích, je zcela klíčové a může ušetřit i náklady. Důležitými faktory pro rozhodování, a které by měly vycházet z podnikatelského záměru, jsou především k jakému účelu a také jak často bude účet využíván – denně, týdně,... [34]

Následně je třeba zvolit banku, u níž bude účet založen. Vhodné je vyhledat a porovnat informace o poskytovaných službách z webových stránek jednotlivých bank nebo portálů zaměřených na finance. [34]

Důležitý je i komfort internetového bankovníctví, zda-li je k účtu nabízena platební karta zdarma, výše poplatků za hotovostní i bezhotovostní transakce, je-li možné mít účet veden v cizí měně v případě mezinárodních transakcí. Pokud chce podnikatel využívat hotovostní transakce (vklad/výběr), měl by si zjistit dostupnost bankomatů a poboček bankovních domů v dané lokalitě. [34]

Při výběru účtu je vhodné zvážit, jestli bude podnikatel chtít v budoucnu implementovat platební bránu pro platby kartami, ne všechny bankovní domy tuto službu nabízejí. S rovnání podnikatelských účtů zaměřené na živnostníky a drobné podnikatele je uvedeno v příloze P I. Zkoumanými položkami jsou zřízení a vedení účtu, příchozí a odchozí tuzemská platba, měsíční poplatek za používání embosované platební karty a měsíční tarif za využívání internetového bankovníctví.

4.2 Platební karty

V České republice jsou transakce platebními kartami dostupné prostřednictvím 3-D Secure systému, který provozují dvě největší karetní asociace – MasterCard a Visa. Systém je nabízen Českou spořitelnou, Československou obchodní bankou, Komerční bankou a Raiffeisenbank.

Obchodník platí bance z každé transakce smluvně určené procento, poplatek se obvykle pohybuje v rozmezí 1 % - 4 %, případně může banka vyžadovat měsíční poplatek nebo poplatek za implementaci či za aktivaci obchodníka. Pro začínající e-shop je klíčové rozhodnutí, jestli platbu kartou budou implementovat nebo se jim tento krok z ekonomického hlediska nevyplatí. Banky navíc obchodníka velmi důkladně prověří – výpis z obchodního rejstříku, ne starší než tři měsíce. Časová náročnost implementace závisí na rozsahu e-shopu.

ČSOB nabízí obchodníkům, kteří s podnikáním teprve začínají balíček Start. Pokud má klient vyšší obrát nebo poptává jiné služby či jejich kombinaci, může využít kontaktního formuláře a banka mu následně pošle individuální nabídku.

Balíček Start

Začínáte? Nebo chcete platby kartou vyzkoušet a nevíte, jak oblíbené u vašich zákazníků budou? Pak pro vás máme balíček Start. Vyšší bankovní provize pro vás automaticky nastavíme dle obrátu vašeho obchodu za minulý měsíc. Vždy tak, aby pro vás byla nejvýhodnější.

2,05 %

do 10 000 Kč

1,75 %

do 20 000 Kč

1,45 %

nad 20 000 Kč

Jednorázový implementační poplatek – 1890 Kč.
Měsíční paušální poplatek – 99 Kč

V balíčku získáte:

- firemní účet pro nové klienty ČSOB na rok zdarma **Zdarma**
- platební terminál do prodejny **Sleva**

Mám zájem o balíček Start

Obr. 15. Přehled služeb nabízených balíčkem Start od ČSOB [35]

Brána nabízí podporu elektronické evidence tržeb (EET), pro e-shopy mají povinnost vést evidenci od března roku 2017, dále nabízí různé pluginy. ČSOB slibuje svým klientům velmi snadnou implementaci, ta je zpoplatněna – v základním balíčku částkou 1 890 Kč.

Měsíční paušální poplatek s balíčkem Start činí 99 korun. Poplatek z každé provedené transakce se pohybuje v rozmezí 1,45 % - 2,05 % v závislosti na obratu firmy.

ČSOB je však jediným bankovním domem, jenž nabízí balíček s pevnými cenami. Běžnou praxí je kontaktovat banku přes kontaktní formulář na webových stránkách nebo osobní schůzkou. Na základě informací dodaných klientem připraví banka individuální nabídku a ceník poskytovaných služeb – dle získaných informací žádný pevný sazebník neexistuje, vše je na domluvě mezi bankou a jejím klientem.

Připravíme nabídku na služby, které váš e-shop potřebuje

Obratem vás budeme kontaktovat

<input type="text" value="jméno"/>	<input type="text" value="příjmení"/>
<input type="text" value="firma"/>	<input type="text" value="IČO"/>
<input type="text" value="telefon"/>	<input type="text" value="e-mail"/>

Mám zájem o:

- balíček Start
- nabídku na platební terminály do kamenné prodejny
- souhlasím se zpracováním výše uvedených údajů pro účely nabídky na akceptaci platebních karet
- individuální podmínky akceptace karet
- vedení firemních účtů a další finanční služby pro internetové obchodníky

Odeslat žádost o nabídku

Obr. 16. Kontaktní formulář ČSOB pro individuální nabídku služeb [35]

4.2.1 Implementace platební brány do e-shopu

Pro implementaci platební brány do e-shopu je nutné mít veden podnikatelský účet u banky, která má smlouvu se zprostředkovatelem platební brány. V české republice zajišťuje provoz platební brány pro elektronické platby společnost GP webpay, jenž spolupracuje s Raiffeisenbank, komerční bankou, Československou obchodní bankou, Unikredit bank a Erste group. [36]

Konkrétně Raiffeisenbank si za implementaci účtuje poplatek okolo 3 000 Kč (v ceníku není uvedena a na pobočce neznali přesnou částku). Klient musí podepsat převzetí odpovědnosti

za zpracování osobních údajů – zákon č. 101/200 Sb. o ochraně osobních údajů. Implementaci zprostředkovává v případě Raiffeisenbank externí firma, Revo payments, která klientovi poskytne dokumentaci i s příslušnými informacemi včetně skriptů v PHP a JAVA. [37]

Součástí procesu implementace platební brány je testování ve zkušební verzi. E-shopu jsou poskytnuta čísla platebních karet určených k testování systému, po úspěšném nastavení a odzkoušení se opět kontaktuje firma zprostředkovávající implementaci, která následně službu zprovozní. [37]

Dle informací uváděných na webových stránkách společnosti GP webpay trvá implementace zkušeným programátorům průměrně dva až tři dny. [37]

„Číslo karty, její expirace i CVC slouží pouze k autorizaci platby v platební bráně GP webpay a nikdy nejsou předávány obchodníkům. Obchodník se pouze dozví, zda platba proběhla v pořádku. E-shopům tím odpadá nutnost zavádět náročná bezpečnostní opatření.

O bezpečí jejich zákazníků se stará provozovatel platební brány GP webpay, Global Payments Europe, který pravidelně prochází přísnými bezpečnostními audity. Ty zaručují, že citlivé údaje nebudou zneužity.“ [37]

Provedené transakce se ukládají na speciální konto, z kterého se po určité době, tzv. zúčtovací období, převede v rámci zúčtování na podnikatelské konto klienta. Délku zúčtovacího období si klient banky volí sám (denní, týdenní, měsíční,...). [37]

4.3 Platební procesory

Platbu zprostředkovává třetí strana, kterou je nebankovní společnost. Nutností je vedení podnikatelského účtu u dané společnosti a propojení stránek e-shopu se stránkami společnosti, která platební procesor provozuje.

Ceník PayPal

Založení a vedení účtu je zdarma, stejně jako převod peněz mezi bankovním účtem a účtem u společnosti PayPal. Platba obchodníkovi za nakoupené zboží je také zdarma, ale přijetí platby od zákazníka na účet obchodníka je již zpoplatněno (1,9 % – 3,4 % + 10.00 CZK). [38]

Transakce mezi účty v rámci společnosti, je příjemci účtován poplatek 3,4 % + 10.00 CZK. V případě platby kartou, rozhoduje odesílatel, která strana poplatek uhradí. Na další poplatky uživatel narazí v případě konverze měn nebo převodu mezi státy. [38]

4.3.1 Implementace EPS PayPal do e-shopu provozovatele Webnode

Pro implementaci platební metody prostřednictvím společnosti PayPal, je nutné mít u ní veden business účet. Založení není zpoplatněno, společnost si pouze vyžádá osobní údaje a odvětví podnikání.

Někteří poskytovatelé ve snaze zjednodušit svým klientům implementaci EPS do jejich e-shopu, tuto volbu již přednastavili. Klientovi poté stačí pouze nastavit požadovanou metodu transakce a propojit účet u poskytovatele EPS s účtem e-shopu.

Webnode nabízí svým klientům zřízení a vedení základní verze e-shopu zdarma. Pokud klientovi nestačí nabídka služeb základního modelu, může upgradovat na Premium verzi, která se pohybuje v rozmezí od 167 Kč měsíčně do 834 Kč za měsíc, v závislosti na zvoleném balíčku služeb. [39]

V důsledku podpory platební metody přes procesor PayPal, je implementace do internetového obchodu na doméně Webnode pro jejich klienty velmi snadné. Stačí v nastavení e-shopu zvolit možnost nastavení způsobu plateb a přidat platbu novou – PayPal, účet se shoduje s e-mailem, kterým se klient přihlásí do systému PayPal.



Typ platby: PayPal

Název platby
PayPal

PayPal účet
bakalarka.eshop@gmail.com

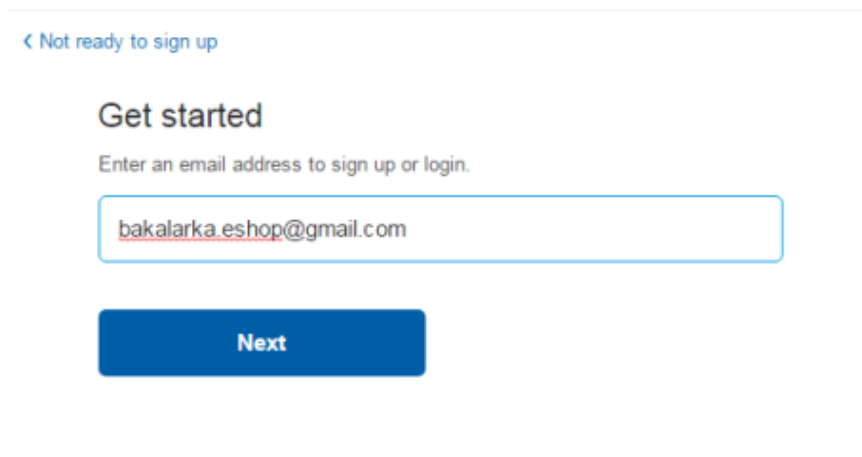
Cena
0

Uložit nebo Zpět

Obr. 17. Volba metody platby při implementaci do e-shopu [40]

Po dokončení nastavení je vygenerován unikátní kód, sloužící k identifikaci příslušného obchodníka. Vkládá se na stránky společnosti PayPal, tím se oba servery propojí.

U společnosti PayPal je nutné mít založený účet a následně oba servery propojit. Pro přihlášení, potažmo k založení PayPal účtu, je používána již existující emailová adresa, sloužící také k ověření uživatele.



< Not ready to sign up

Get started

Enter an email address to sign up or login.

Next

Obr. 18. Registrace nového uživatele [41]

Po zadání e-mailové adresy, prostředku komunikace a zároveň sloužící jako unikátní přihlašovací jméno, je klient vyzván k vyplnění osobních údajů a předmětu podnikání.

Po dokončení registrace lze nastavit v sekci „My selling tools“ integrování notifikačního systému do e-shopu.

My Profile

- My business info** > Email address, address, phone, password, more.
- My money** > Bank accounts, cards and more.
- My settings** > Notifications, customer ID, more.
- My selling tools** > Getting paid, shipping, more.

Selling online		
PayPal buttons	Manage my payment buttons.	Update
Credit card statement name	My business name on card statements is: BAKALARKA	Update
Sales tax	Set up sales taxes for multiple regions.	Update
Website preferences	Return customers to my website after they pay with PayPal.	Update
API access	Manage API credentials to integrate my PayPal account with my online store or shopping cart.	Update
Invoice templates	Create and manage my invoices.	Update
Getting paid and managing my risk		
My automatic payments	Manage the subscriptions and automatic payments that I offer my customers.	Update
Instant payment notifications	Integrate PayPal payment notifications with my website.	Update
Block payments	Limit payments, add instructions, and more.	Update
Customer service message	Create a personalised message for customer disputes.	Update
Shipping my items		
Shipping calculations	Create unique shipping methods for each customer.	Update

Obr. 19. Nastavení funkce Notifikace – PayPal [41]

Do kolonky „Notification URL“ se zadá adresa vygenerovaná systémem webnode. Službu je nutné aktivovat, protože v defaultním nastavení je vypnutá.

Edit Instant Payment Notification (IPN) settings [Back to My Profile](#)

PayPal sends IPN messages to the URL that you specify below.

To start receiving IPN messages, enter the notification URL and select **Receive IPN messages** below. To temporarily stop receiving IPN messages, select **Do not receive IPN messages** below. PayPal continues to generate and store IPN messages until you select **Receive IPN messages** again (or turn off IPN).

Notification URL

IPN messages

Receive IPN messages (Enabled)
 Do not receive IPN messages (Disabled)

Obr. 20. Propojení notifikačního systému PayPal s e-shopem [41]

Po uložení nastavení je propojení aktivní a připraveno k provozu. Díky podpoře ze strany provozovatele je celý proces rychlý a snadný, vhodný především pro začátečníky.

E-shop je možné zobrazit zde.

4.3.2 Implementace EPS PayPal do vlastního e-shopu

Pro implementaci platební brány PayPal do vlastního e-shopu je třeba mít aktivní PayPal účet (Premiere) a nastavit URL adresu pro zpětnou vazbu od PayPal. Opět bude použita platba přes IPN (Instant Payment Notification).

Po přihlášení k PayPal účtu je nutné aktivovat službu IPN, způsobem popsáním v předchozí podkapitole. Avšak při zadávání „Notification URL adres“ je nutné nastavit vlastní adresu, tu určí správce webových stránek e-shopu.

Správce musí dále nastavit na stránkách e-shopu prvek, kterým může zákazník po dokončení objednávky platbu zrealizovat a také zadat, jaké údaje bude systém zaznamenávat (číslo objednávky, název zboží, suma k úhradě). [42]

```
1 <?php
2
3 $vas_email = "muj@email.cz"; // = Login na PayPal
4 $nazev_zbozi = "Notebook Sony"; // Název zboží & objednávky
5 $cislo_objednavky = 12345; // Číslo objednávky pro naše vnitřní účely
6 $castka = 32000; // Musí být celé kladné číslo
7
8 ?>
9
10 <form action="https://www.paypal.com/cgi-bin/webscr" method="post" target="_blank">
11 <input type="hidden" name="cmd" value="_xclick">
12 <input type="hidden" name="business" value="<?=$vas_email?>">
13 <input type="hidden" name="lc" value="GB">
14 <input type="hidden" name="item_name" value="<?=$nazev_zbozi?>">
15 <input type="hidden" name="item_number" value="<?=$cislo_objednavky?>">
16 <input type="hidden" name="amount" value="<?=$celkova_castka?>.00">
17 <input type="hidden" name="currency_code" value="CZK">
18 <input type="hidden" name="shipping" value="0.00">
19 <input type="hidden" name="bn" value="PP-BuyNowBF:btn_buynowCC_LG_global.gif:NonHostedGuest">
20 <input type="submit" value="Zaplatit Pay Pal &raquo;" name="submit" />
21 
22 </form>
```

Obr. 21. Kód platební brány na stráně e-shopu [42]

Po dokončení objednávky klikne zákazník na připravené tlačítko pro platbu přes bánu PayPal, přihlásí se ke svému účtu nebo zadá údaje z platební karty a transakci potvrdí.

Pro zjištění, zda-li platba proběhla v pořádku, je třeba přidat další část php kódu.

```
1 <?
2
3 // Načteme si údaje o provedené platby
4 $item_name = $_POST['item_name']; // Náš název zboží
5 $item_number = $_POST['item_number']; // Naše číslo objednávky
6 $payment_status = $_POST['payment_status']; // Status platby
7 $payment_amount = $_POST['mc_gross'];
8 $payment_currency = $_POST['mc_currency'];
9 $receiver_email = $_POST['receiver_email']; // Email toho, kdo platbu přijal
10 $payer_email = $_POST['payer_email']; // Email toho, kdo platbu odeslal
11
12 ?>
```

Obr. 22. Zpracování platby [42]

V případě požadavku na vyšší zabezpečení je kód mnohem složitější.

```
1 <?php
2
3 // read the post from PayPal system and add 'cmd'
4 $req = 'cmd=_notify-validate';
5
6 foreach ($_POST as $key => $value) {
7     $value = urlencode(stripslashes($value));
8     $req .= "&$key=$value";
9 }
10
11 // post back to PayPal system to validate
12 $header .= "POST /cgi-bin/webscr HTTP/1.0\r\n";
13 $header .= "Content-Type: application/x-www-form-urlencoded\r\n";
14 $header .= "Content-Length: " . strlen($req) . "\r\n\r\n";
15 $fp = fsockopen ('ssl://www.paypal.com', 443, $errno, $errstr, 30);
16
17 // assign posted variables to local variables
18 $item_name = $_POST['item_name'];
19 $item_number = $_POST['item_number'];
20 $payment_status = $_POST['payment_status'];
21 $payment_amount = $_POST['mc_gross'];
22 $payment_currency = $_POST['mc_currency'];
23 $txn_id = $_POST['txn_id'];
24 $receiver_email = $_POST['receiver_email'];
25 $payer_email = $_POST['payer_email'];
26
27 if (!$fp) {
28     // HTTP ERROR
29 } else {
30     fputs ($fp, $header . $req);
31     while (!feof($fp)) {
32         $res = fgets ($fp, 1024);
33         if (strcmp ($res, "VERIFIED") == 0) {
34             // check the payment_status is Completed
35             // check that txn_id has not been previously processed
36             // check that receiver_email is your Primary PayPal email
37             // check that payment_amount/payment_currency are correct
38             // process payment
39         }
40         else if (strcmp ($res, "INVALID") == 0) {
41             // log for manual investigation
42         }
43     }
44     fclose ($fp);
45 }
46 ?>
47
48 ?>
```

Obr. 23. Zpracování platby – zabezpečená verze předchozího php kódu [42]

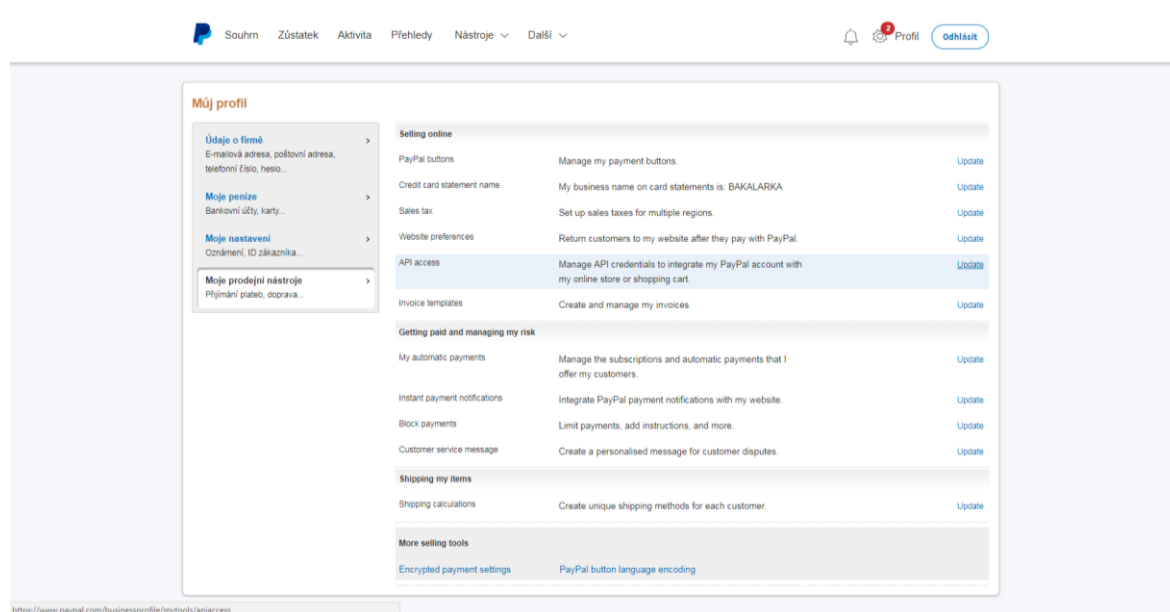
O každé úspěšně provedené transakci je klient informován prostřednictvím e-mailu. Tímto krokem je celý proces zabezpečen a připraven k použití. [42]

4.3.3 Implementace EPS PayPal do eshop systému

Pro implementaci je opět vyžadován Business účet vedený u společnosti PayPal. Jehož založení je popsáno již v minulé podkapitole.

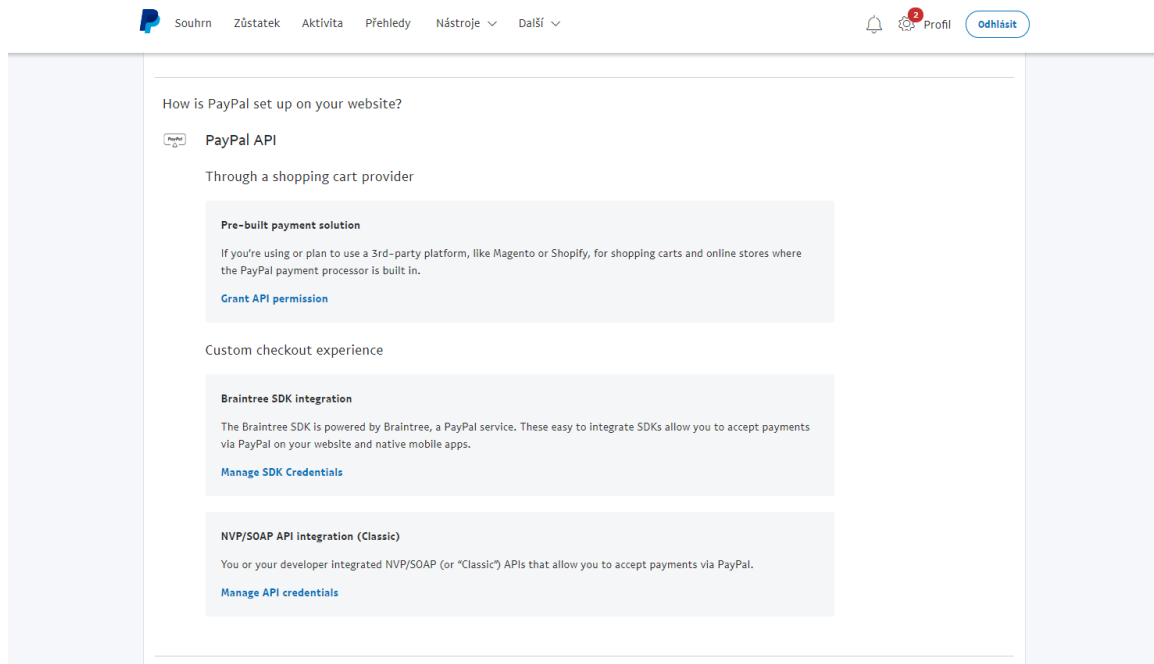
Platební spojení s PayPal bude provedeno v e-shopovém systému shoptet.

V nastavení klikneme na možnost *Profil a nastavení*, kde v sekci *Moje prodejní nástroje* klikneme na *Update u API access*.



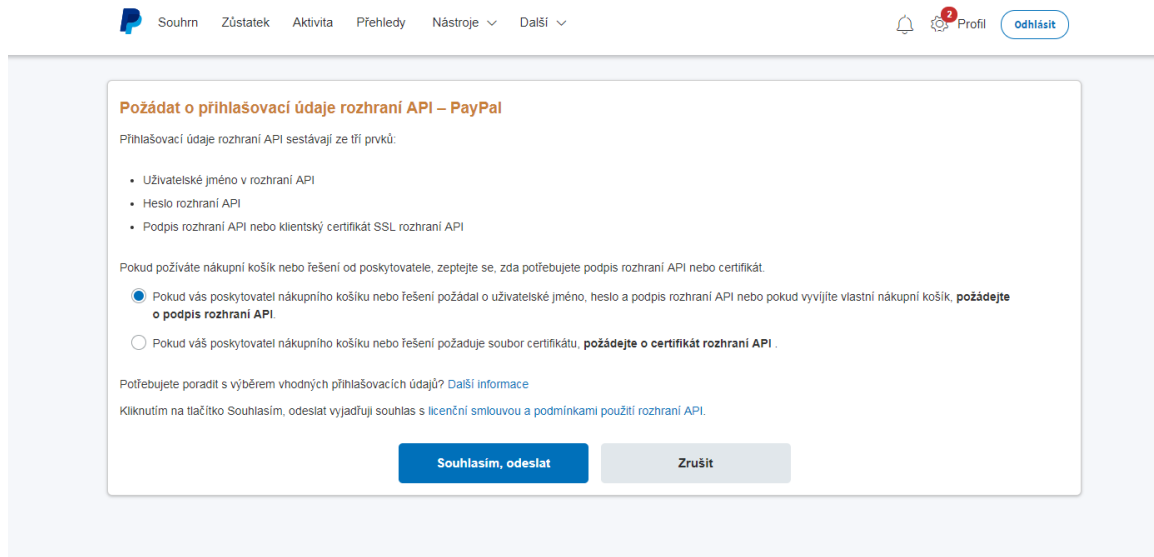
Obr. 24 Nastavení API access [41]

Na následující stránce zvolíme poslední možnost, tedy *Manage API credentials*.



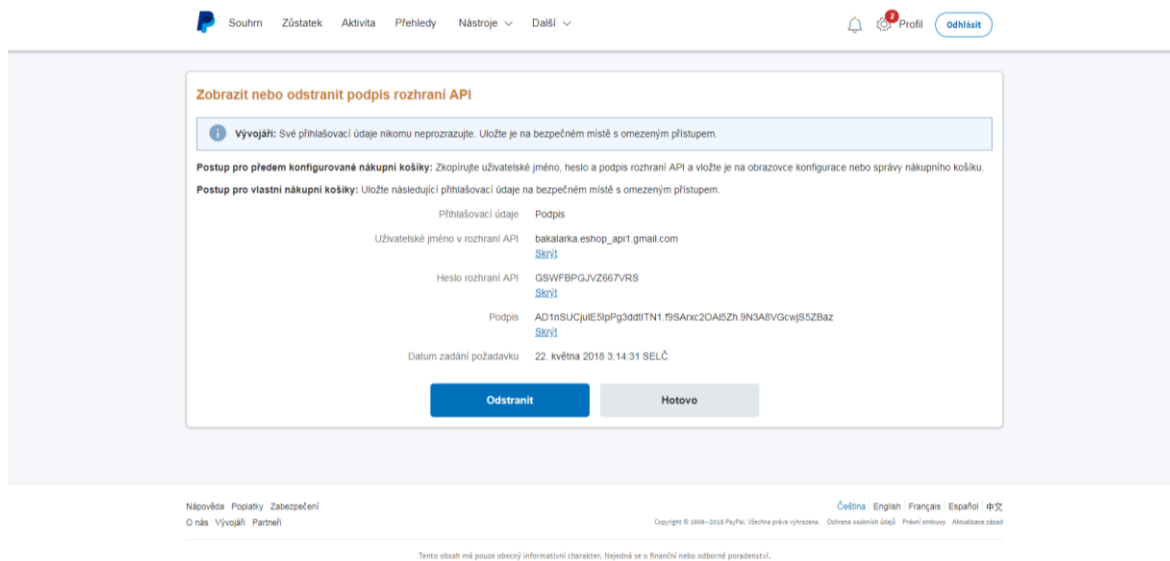
Obr. 25 Výběr řešení pro daný e-shop [41]

Z nabízených variant zvolíme požadavek o podpis rozhraní API.



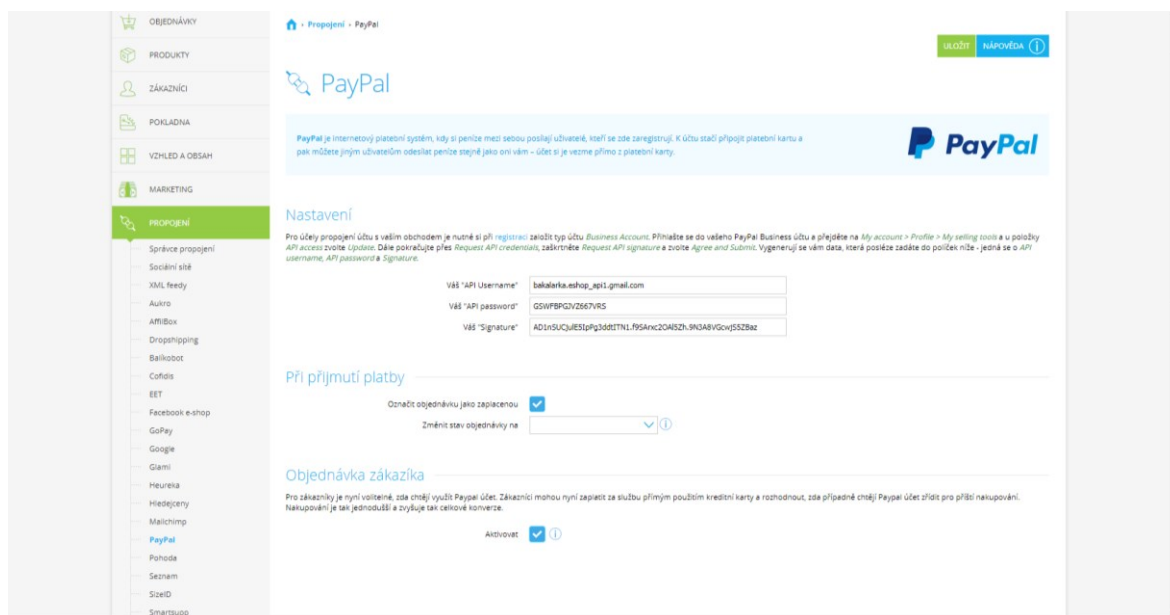
Obr. 26 PayPal – požadavek o podpis v API rozhraní [41]

Následně je systémem vygenerován podpis, heslo a uživatelské jméno v API rozhraní.



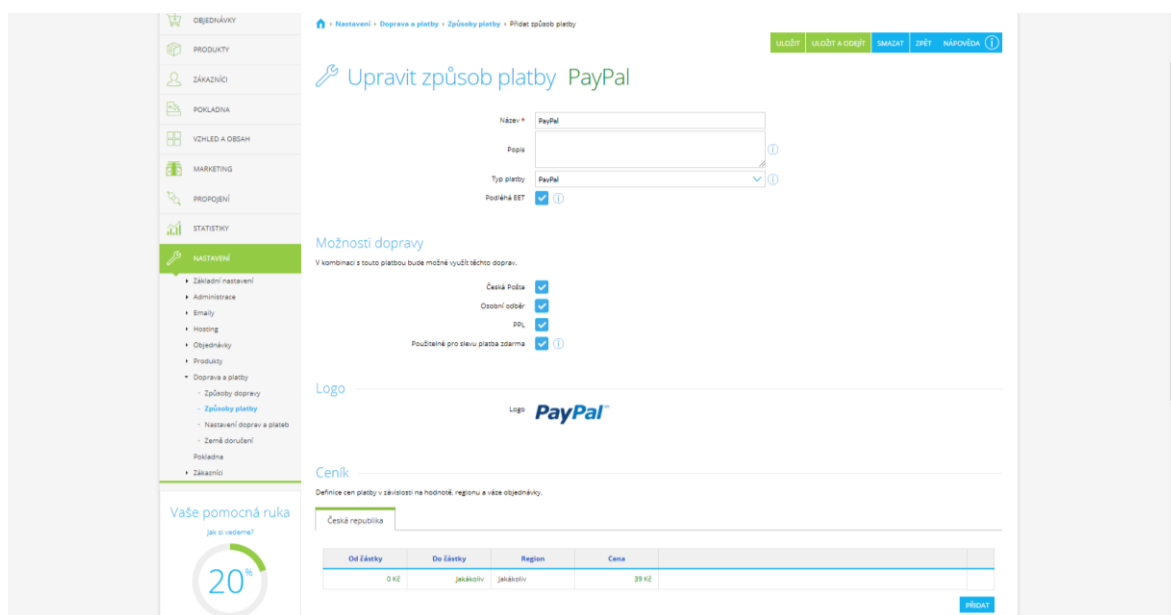
Obr. 27 PayPal – vygenerovaný podpis v API rozhraní [41]

Nyní je nutné v nastavení e-shopu tyto údaje vyplnit. Přejdeme do sekce *Propojení* a zvolíme možnost *PayPal*.



Obr. 28 Vytvoření spojení mezi PayPal a e-shopem [43]

V posledním kroku je nutné v kategorii *Nastavení* tuto možnost vytvořit a následně aktivovat. Klikneme v podkategorii *Doprava a platba* na možnost *Způsoby platby*.



Obr. 29 shoptet – vytvoření možnosti platby přes PayPal [43]

Po vyplnění uložíme a následně aktivujeme.

Výchozí	Pořadí	Nadpis	EET	Viditelnost	
<input checked="" type="checkbox"/>	1.	Hotově	Ano	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	2.	Dobírkou	Ne	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	3.	Převodem	Ne	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	4.	PayPal	Ano	<input checked="" type="checkbox"/>	

Obr. 30 shoptet – tabulka s přehledem platebních možností [43]

Tento ukázkový e-shop můžete nalézt na: <https://218817.myshoptet.com/>.

ZÁVĚR

Prvním cílem bakalářské práce bylo vypracovat stručný přehled používaných elektronických platebních systémů. Jejich případné výhody a nevýhody, které mohou přispět k rozhodování při výběru vhodného elektronického platebního systému pro začínající internetový obchod, jehož implementace je součástí praktické části bakalářské práce.

V druhé části mé bakalářské práce jsem se zaměřila na bezpečnostní složkou elektronických platebních systémů, kde jsem se zmínila také nejrozšířenější podvodné praktiky ze sociálního inženýrství často užívané útočníky k získání citlivých informací od obětí podvodu.

Nejúčinnější obranou proti takovému podvodnému jednání je dodržovat alespoň základní principy bezpečnosti, které jsou blíže popsány v podkapitole 2.2.

Hlavní část, tedy implementace elektronického platebního systému je také částí praktickou. Kapitola začíná výčtem a popisem kritérií, podle nichž se majitel internetového obchodu může rozhodnout, kterou z platebních metod chce do svého obchodu implementovat.

Dále jsem vypracovala stručný přehled jaké má daná metoda nároky na implementaci, tedy zda-li je implementace snadná či nikoli a poplatky, které si bankovní či nebankovní společnosti účtují za vedení účtu a zprostředkování platby, případně další související poplatky.

Vybrala jsem tři nejčastější možnosti, jakými může zákazník e-shopu provést elektronickou platbu – převod na bankovní účet, platba kartou a platba přes platební procesor.

Při zkoumání jakým způsobem probíhá implementace platební brány do e-shopu jsem často narážela na nedostatek informací. Při konzultaci v bankách jsem některé informace sice získala, ale přesný postup implementace krok za krokem neznám. Pouze jsem se dozvěděla, že společnost zprostředkovávající implementaci má přesný postup pro své klienty i s příslušnými skripty, ale nepodařilo se mi je získat.

Detailněji však popisují implementaci elektronického platebního systému tzv. platebního procesoru poskytovaného nebankovní společností PayPal.

SEZNAM POUŽITÉ LITERATURY

- [1] Jak platit elektronicky. Měšec [online]. Praha, 2003 [cit. 2017-03-21]. Dostupné z: <http://www.mesec.cz/clanky/jak-platit-elektronicky/>.
- [2] MÁČE, Miroslav. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.
- [3] Platební procesory. Marketing podnikání na Internetu od A do Z [online]. Praha, 2011 [cit. 2017-03-21]. Dostupné z: <http://wp.sms-praha.cz/?p=656>.
- [4] Platba přes platební procesor navýšena o poplatek. In: G2A [online]. [cit. 2017-04-25]. Dostupné z: <https://www.g2a.com/checkout/onepage/>
- [5] INTERNETOVÉ PENĚŽENKY. Finanční poradenství online [online]. [cit. 2017-05-22]. Dostupné z: <https://www.financni-poradenstvi.com/internetove-penezenky/>
- [6] Platební procesor PayPal – přihlášení. In:–Platební procesor PayPal PayPal [online]. [cit. 2017-04-25]. Dostupné z: www.paypal.com
- [7] Platební procesor PayPal – kontrola údajů. In:–Platební procesor PayPal PayPal [online]. [cit. 2017-04-25]. Dostupné z: www.paypal.com
- [8] Stránka obchodníka s potvrzením o úspěšné platbě. In: Humble Bundle [online]. [cit. 2017-04-25]. Dostupné z: <https://www.humblebundle.com/>
- [9] PŘÁDKA, Michal a Jan KALA. Elektronické bankovníctví. Vyd. 1. Praha: ComputerPress, 2000, 166 s. ISBN 80-7226-328-5.
- [10] Keňa řeší chudobu platbami mobilem, tvrdí studie Více. Mobilmania.cz [online]. 2017 [cit. 2017-05-22]. Dostupné z: <http://www.mobilmania.cz/clanky/kena-resi-chudobu-platbami-mobilem-tvrdi-studie/sc-3-a-1337228/default.aspx>
- [11] Phone banking. Peníze.cz [online]. Praha: Partners media, 2003 [cit. 2017-05-13]. Dostupné z: <http://www.penize.cz/investice/15758-phone-banking>
- [12] CHVÁTAL, Dalibor Z. Mobilní bankovní SIM Toolkit je odsouzen k zániku, je staromódní. Měšec.cz [online]. 2015 [cit. 2017-04-26]. Dostupné z: <https://www.mesec.cz/clanky/mobilni-bankovnictvi-bude-pohodlne-ale-mene-bezpecne/>
- [13] Další české banky chystají možnost placení mobilem. Ale jen pro Android Zdroj: <http://ekonomika.idnes.cz/novinky-v-bezkontaktnim-placeni-ceskych-bank-fa1->

- /ekonomika.aspx?c=A170109_193500_ekonomika_rny. IDNES.cz [online]. 2017 [cit. 2017-04-26]. Dostupné z: http://ekonomika.idnes.cz/novinky-v-bezkontakt-nim-placeni-ceskych-bank-fa1-/ekonomika.aspx?c=A170109_193500_ekonomika_rny
- [14] ČSOB Na nákupy: Peněženku i s kartou nechte v tašce. ČSOB [online]. 2017 [cit. 2017-05-22]. Dostupné z: <https://www.csob.cz/portal/lide/produkty/platebni-karty/csob-nanakupy?from=nanakupy.cz>
- [15] Místo platební karty mobil. Banky přišly s novým řešením. Peníze.cz [online]. 2016 [cit. 2017-05-22]. Dostupné z: <http://www.penize.cz/platebni-karty/315476-misto-platebni-karty-mobil-banky-prisly-s-novym-resenim>
- [16] Platíte s mobilem v obchodě. Jde to i bez plastové karty. Měšec.cz [online]. 2013 [cit. 2017-05-22]. Dostupné z: <https://www.mesec.cz/clanky/s-mobilem-v-obchode-jde-to-i-bez-plastove-karty/>
- [17] Social engineering. TechTarget Search Security [online]. 2014 [cit. 2017-05-22]. Dostupné z: <http://searchsecurity.techtarget.com/definition/social-engineering>
- [18] Social Engineering Fundamentals, Part I: Hacker Tactics. Symantec Connect [online]. 2001 [cit. 2017-05-22]. Dostupné z: <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>
- [19] MITNICK, Kevin D. a William L. SIMON. The art of deception: controlling the human element of security. Indianapolis, Ind.: Wiley, c2002. ISBN 0-7645-4280-x.
- [20] Jak nakupovat. Strikeshop.cz [online]. [cit. 2017-05-22]. Dostupné z: <http://www.strikeshop.cz/strikeshop/4-Jak-nakupovat/4-Nakup-platebni-kartou-navod>
- [21] Protokoly pro elektronické platební systémy. Security-Portal.cz [online]. 2007 [cit. 2017-05-22]. Dostupné z: <http://www.security-portal.cz/clanky/protokoly-pro-elektronick%C3%A9-platebn%C3%AD-syst%C3%A9my>
- [22] Nové trendy v elektronických komunikacích: Kryptografie [online]. Praha [cit. 2017-05-22]. Dostupné z: <https://publi.cz/books/232/Impresum.html>
- [23] ŠPAČEK, Bronislav. Nakupování na internetu. Praha: Computer Press, c2002. Svět na Internetu. ISBN 80-7226-612-8.

- [24] Co je to SSL. Thawte [online]. [cit. 2017-05-22]. Dostupné z: <http://www.ssl-thawte.cz/ssl/co-je-to-ssl/> Co je to SSL. Thawte [online]. [cit. 2017-05-22]. Dostupné z: <http://www.ssl-thawte.cz/ssl/co-je-to-ssl/> Co je to SSL. Thawte [online]. [cit. 2017-05-22]. Dostupné z: <http://www.ssl-thawte.cz/ssl/co-je-to-ssl/>
- [25] ZAORALOVÁ, Lenka. Systém elektronických plateb. Brno, 2009. Diplomová práce. Masarykova univerzita. Vedoucí práce Doc. RNDr. Václavu Matyášovi, M.Sc., Ph.D.
- [26] Shoptet.cz [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.shoptet.cz/cenik/>
- [27] Vybrat-eshop.cz [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.vybrat-eshop.cz/>
- [28] Vybrat-eshop.cz [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.vybrat-eshop.cz/eshop/prestashop>
- [29] Vybrat-eshop.cz [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.vybrat-eshop.cz/eshop/shoptet>
- [30] UPgates [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.upgates.com/cz/>
- [31] Vybrat-eshop.cz [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://www.vybrat-eshop.cz/eshop/shopsystem>
- [32] Online platební systémy v České Republice a výběr vhodné varianty pro internetový obchod [online]. Praha, 2010 [cit. 2017-05-22]. Dostupné z: <http://info.sks.cz/www/zavprace/soubory/68440.pdf>. Bakalářská práce. VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. Vedoucí práce Ing. Václav ŠUBRTA.
- [33] Systémová stránka – dokončení objednávky. In: Webnode [online]. 2017 [cit. 2017-05-22]. Dostupné z: <http://cms.bakalarka7.webnode.cz/es-order-finished/>
- [34] Srovnání bankovních účtů pro drobné podnikatele. Peníze.cz [online]. 2016 [cit. 2017-05-22]. Dostupné z: <http://www.penize.cz/podnikatelske-ucty/314792-srovnani-bankovnich-uctu-pro-drobne-podnikatele>
- [35] Platební brána ČSOB. ČSOB [online]. [cit. 2017-05-22]. Dostupné z: <https://platebnibrana.csob.cz/#podminky-a-ceny>

- [36] Jak si objednat platební bránu GP webpay? GP webpay [online]. [cit. 2017-05-22]. Dostupné z: <http://www.gpwebpay.cz/Order>
- [37] Nejčastější otázky. GP webpay [online]. [cit. 2017-05-22]. Dostupné z: <http://www.gpwebpay.cz/Faq>
- [38] Fees. PayPal [online]. [cit. 2017-05-22]. Dostupné z: https://www.paypal.com/webscr?cmd=_display-fees
- [39] Ceník internetových obchodů. Webnode [online]. [cit. 2017-05-22]. Dostupné z: <https://www.webnode.cz/eshop-cenik/>
- [40] Volba metody platby při implementaci do e-shopu. In: Webnode [online]. 2017 [cit. 2017-05-22]. Dostupné z: <http://user.bakalarka7.webnode.cz/e-shop/payment-types/detail/>
- [41] PayPal [online]. [cit. 2017-05-22]. Dostupné z: www.paypal.com
- [42] Platební brána PayPal - řešení. In: Webtrh.cz [online]. 2009 [cit. 2017-05-22]. Dostupné z: <https://webtrh.cz/47541-platebni-brana-paypal-reseni>
- [43] Shoptet [online]. Praha, 2018 [cit. 2018-05-21]. Dostupné z: <https://218817.myshoptet.com/admin/?email=bakalarka.eshop@gmail.com>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČSOB Československá obchodní banka

KB Komerční banka

EPS Elektronický platební systém

PÚ Podnikatelský účet

SEZNAM OBRÁZKŮ

Obr. 1. Průběh transakce provedené kartou a její zúčtování [2].....	13
Obr. 2. Platba přes platební procesor navýšena o poplatek [4].....	15
Obr. 3. Platební procesor PayPal – přihlášení [6].....	16
Obr. 9. Struktura automatizovaného telefonního systému [9].....	23
Obr. 10. Rub platební karty s CVV2 kódem [200].....	28
Obr. 11. Digitální podpis [22].....	29
Obr. 14. Systémová stránka – dokončení objednávky [33].....	39
Obr. 15. Přehled služeb nabízených balíčkem Start od ČSOB [35].....	41
Obr. 16. Kontaktní formulář ČSOB pro individuální nabídku služeb [35].....	42
Obr. 17. Volba metody platby při implementaci do e-shopu [40].....	44
Obr. 18. Registrace nového uživatele [41].....	45
Obr. 19. Nastavení funkce Notifikace – PayPal [41].....	45
Obr. 20. Propojení notifikačního systému PayPal s e-shopem [41].....	46
Obr. 21. Kód platební brány na straně e-shopu [42].....	47
Obr. 22. Zpracování platby [42].....	47
Obr. 23. Zpracování platby – zabezpečená verze předchozího php kódu [42].....	48

SEZNAM TABULEK

SEZNAM PŘÍLOH

- P I Srovnání vybraných podnikatelských účtů
- P II Srovnání vybraných e-shop systémů

PŘÍLOHA P I: SROVNÁNÍ VYBRANÝCH PODNIKATELSKÝCH ÚČTŮ

	Založení účtu	Vedení účtu	Příchozí platba	Odchozí platba	Platební karta	Internetbanking
ČSOB Podnikatelské konto	zdarma	115 Kč	6 Kč	3 Kč	zdarma	zdarma
Komerční banka Profi účet	zdarma	169 Kč	6 Kč	neuveдено	390 Kč	290 Kč
Raiffeisenbank eKonto START	zdarma	99 Kč	zdarma	zdarma	zdarma	200 Kč
Fio banka PÚ bez poplatků	zdarma	zdarma	zdarma	zdarma	zdarma	zdarma
mBank mKonto Business	zdarma	zdarma	zdarma	zdarma	29 Kč	zdarma

PŘÍLOHA P II: SROVNÁNÍ VYBRANÝCH E-SHOP SYSTÉMŮ – PLATEBNÍ PROCESORY

	shoptet	UPgates	PrestaShop	ShopSystem
PaySec	×	✓	✓	✓
Pay Muzo	×	✓	✓	✓
PayPal	✓	✓	✓	✓
GoPay	✓	✓	✓	✓
PayU	✓	✓	✓	✓
MoneyBookers	×	✓	✓	×