

České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra počítačů



Bakalářská práce

Portál pro zabezpečenou distribuci PDF dokumentů

Jan Hovorka

Vedoucí práce: Ing. Martin Komárek

Studijní program: Softwarové technologie a management, Bakalářský

Obor: Web a multimedia

21. května 2012

Poděkování

Na tomto místě bych rád poděkoval svému vedoucímu práce, Ing. Martinu Komárkovi, za příkladné vedení práce a přínosné rady.

Dále bych rád poděkoval své rodině a přátelům za pozitivní motivaci a pomoc při tvorbě této práce.

Prohlášení

Prohlašuji, že jsem práci vypracoval samostatně a použil jsem pouze podklady uvedené v příloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 21. 5. 2012

.....

Abstract

This bachelor thesis deals with the design and implementation of portal for secure distribution of PDF documents. The portal allows teachers to upload PDF documents. These PDF documents are offered to students to download for free or after payment.

The student proceed to the application using received link to PDF document, which can be downloaded for free, or after payment. Before download all documents are labeled with watermark, which contains student's username and the date of download.

Abstrakt

Tato bakalářská práce se zabývá návrhem a implementací portálu pro zabezpečenou distribuci PDF dokumentů. Portál umožňuje vyučujícím vkládat do systému dokumenty ve formátu PDF. Tyto PDF dokumenty jsou nabídnuty studentům zdarma, nebo po zaplacení ke stažení.

Student přistoupí do aplikace pomocí obdržného odkazu na PDF dokument, který si po zaplacení, nebo zdarma stáhne. Dokumenty jsou před stažením označeny vodoznakem, který obsahuje uživatelské jméno studenta, který dokument stáhl a datum stažení.

Obsah

1	Úvod	1
1.1	Motivace	1
1.2	Historie	1
2	Popis problému, specifikace cíle	3
2.1	Popis problému	3
2.2	Cíle práce	3
2.3	Rešerše	4
2.3.1	Amazon	4
2.3.2	Google Books	4
2.3.3	Google Play Books	4
2.3.4	Palmknihy	5
3	Zabezpečení PDF dokumentů	7
3.1	Zobrazení PDF dokumentů autorizovaným osobám	7
3.1.1	Zabezpečení heslem	7
3.1.2	Digital Rights Management	7
3.2	Označení PDF dokumentů	8
3.2.1	Vodoznak	8
3.3	Shrnutí	9
4	Platby přes Internet	11
4.1	Elektronické peněženky	11
4.1.1	PayPal	11
4.1.1.1	Website Payments Standard	12
4.1.1.2	Express Checkout	13
4.1.1.3	Instant Payment Notification	13
4.1.2	PaySec	13
4.1.3	Rozhraní Merchant API	14
4.2	Platba platební kartou	14
4.2.1	ČSOB	15
4.2.2	Česká spořitelna	15
4.3	Převody peněz	15
4.4	Srovnání a výběr	16
4.4.1	Finanční srovnání	16

4.4.2	Výběr	16
5	Analýza	17
5.1	Uživatelé	17
5.1.1	Uživatelské role	17
5.2	Požadavky	18
5.2.1	Funkční požadavky	18
5.2.2	Nefunkční požadavky	19
5.3	Případy užití	19
6	Implementace	21
6.1	Použité technologie	21
6.1.1	Programovací jazyk a framework	21
6.1.2	Server	21
6.1.3	Databáze	22
6.2	Integrace FELid	22
6.2.1	Nastavení Apache serveru	22
6.2.2	Získání atributů aplikací	23
6.2.3	Práce s uživatelem v aplikaci	25
6.3	Integrace PayPal	25
6.3.1	Vytvoření PayPal účtu	25
6.3.2	Buy Now tlačítko	25
6.3.3	Ověření platby	27
6.3.4	Zpřístupnění odkazu ke stažení	27
6.3.5	Připomínkování PDF dokumentů	29
7	Testování	31
7.1	Testování viditelnosti vodoznaků	31
7.2	Testování integrace FELid	32
7.3	Testování integrace PayPal	32
8	Závěr	35
A	Seznam zkratk	39
B	Obsah přiloženého CD	41

Seznam obrázků

3.1	Proces distribuce elektronických knih pomocí Adobe Digital Publishing for eBook[6]	8
4.1	Proces nákupu s použitím tlačítka Buy Now[17]	12
4.2	Proces požadavku a odpovědi s použitím IPN[15]	14
7.1	Vložený vodoznak v popředí PDF vytvořeného z MS Powerpoint	31
7.2	Vložený vodoznak v pozadí PDF vytvořeného z MS Powerpoint	32
7.3	Potvrzení nákupu na PayPal	33
7.4	PayPal stránka prodejce	33
7.5	PayPal stránka nakupujícího	33

Seznam tabulek

4.1 Srovnání poplatků spojených s implementací platebních metod	16
---	----

Kapitola 1

Úvod

V této kapitole bude popsána motivace pro vznik portálu pro zabezpečenou distribuci PDF dokumentů.

1.1 Motivace

V dnešní době, kdy je nedostatek kvalitních studijních materiálů, je potřeba podporovat vznik těchto materiálů. U vyučujících se projevuje nevole k tvorbě kvalitních elektronických studijních materiálů, a to především z důvodu téměř nemožné kontroly nad jejich distribucí. Potencionální autoři kvalitních studijních materiálů nechtějí investovat svůj volný čas do psaní s tím, že se jejich díla budou nekontrolovatelně šířit po celém Internetu. Tradiční metoda distribuce studijních materiálů, formou skript, nemusí být v mnoha případech řešením. V některých oborech, zejména technických, se standardy mění tak rychle, že není dost dobře možné vydávat dostatečně rychle aktualizovaná skripta vyhovující současným trendům.

V okamžiku, kdy by měli vyučující možnost dostatečné kontroly nad šířením svých studijních materiálů, mohli by rozšířit spektrum kvalitních, volně dostupných studijních materiálů ke svým kurzům. Tyto materiály by byly dostupné pouze studentům ČVUT ke kvalitní přípravě ke studiu.

Další možností motivace vyučujících k vytváření kvalitních studijních materiálů by byla možnost zpřístupnit tyto materiály studentům ČVUT za určitý finanční obnos. Pokud budou tyto kvalitní studijní materiály za rozumnou, a pro studenty přijatelnou cenu lehce přístupné, sníží se potřeba studentů shánět nelegální, většinou i nekvalitní a nevhodné materiály z různých neověřených zdrojů.

Z výše uvedeného vyplývá, že vytvoření kvalitního portálu pro zabezpečenou distribuci elektronických studijních materiálů, by mohlo zvýšit chuť vyučujících k tvorbě kvalitních studijních materiálů. Zároveň by vznik tohoto portálu mohl zlepšit kvalitu přípravy studentů na úspěšné absolvování studia na vysoké škole.

1.2 Historie

Tato bakalářská práce rozšiřuje již existující polofunkční prototyp[2] vyvinutý na fakultě v rámci studentských prací. Tento prototyp umožňuje vložit do PDF dokumentů vodoznak s

informacemi na základě vyplnění formuláře. Zároveň je možné tyto dokumenty volně stahovat pomocí vygenerovaného obsahu.

Kapitola 2

Popis problému, specifikace cíle

2.1 Popis problému

Tato práce si klade za cíl vytvořit portál, který umožní zabezpečeně distribuovat elektronické studijní materiály ve formátu PDF. Portál si bude muset poradit s těmito problémy:

- Umožnit autorům vložit vytvořený PDF dokument do systému a nabídnout ho ke stažení.
- Zajistit, že se k PDF dokumentům dostanou pouze studenti ČVUT FEL.
- Umožnit studentům zdarma si stáhnout PDF dokumenty.
- Umožnit vybrané PDF dokumenty stáhnout až po zaplacení předem stanovené finanční částky.
- Každý stažený PDF dokument označit vodoznakem s informacemi o uživateli, který daný dokument stáhl.
- Umožnit připomínkovat jednotlivé stránky, či části, pomocí diskuzních příspěvků.

Tato bakalářská práce rozšiřuje již existující polofunkční prototyp vyvinut na fakultě v rámci studentských prací. Tento prototyp, umožňuje vložit do PDF dokumentů vodoznak s informacemi na základě vyplnění formuláře. Zároveň je možné tyto dokumenty volně stahovat pomocí vygenerovaného obsahu.

2.2 Cíle práce

Cílem této práce je dokončit výše zmíněný prototyp tak, aby dokázal vyřešit uvedené problémy. Konkrétně se jedná o implementaci komponent.

- FELid pro autentizaci uživatelů v rámci sítě ČVUT FEL.
- Upravit tvorbu vodoznaku tak, aby obsahoval informace o uživateli, získané ze systému FELid[1].

- Umožnit připomínkování jednotlivých stránek či částí pomocí diskuzních příspěvků.
- Analyzovat a následně implementovat možnost rozšíření portálu o možnost komerčního prodeje PDF dokumentů.

2.3 Rešerše

S ohledem na specifičnost zadání práce je těžké najít existující projekty, které by byly alespoň z části podobné. Přesto zde může být zmíněno pár projektů zabývajících se distribucí elektronických materiálů (většinou knih).

2.3.1 Amazon

Amazon[7] je asi nejznámější prodejce elektronických knih na světě. Ačkoliv elektronické knihy nejsou jediným obchodním artiklem Amazonu, stal se Amazon známým hlavně prodejem knih jak tradičních, tak i elektronických. Se svojí nabídkou elektronických knih se Amazon řadí mezi největší distributory na světě.

Na Amazonu se dá nalézt spousta studijních materiálů, vhodných ke studiu na ČVUT FEL. Pro mnohé ale může být překážkou absence překladu knih do českého jazyka. Další nevýhodou může být potřeba speciální čtečky pro čtení knih. Čtečky pro formáty používané Amazonem se dají sehnat zdarma pro všechny běžné operační systémy, a to jak desktopové, tak i mobilní.

Samozřejmostí na webu Amazonu je kvalitní přehledná kategorizace knih a kvalitně vyřešené fulltextové vyhledávání knih. Knihy jsou lehce dohledatelné přes název, jméno autora, žánr atd. Další výhodou je hodnocení knih a komentáře od ostatních uživatelů.

Amazon samozřejmě neposkytuje elektronické knihy zdarma. Prodává je. S tím je spojená nutnost registrace na webu a provádění elektronických platebních operací.

2.3.2 Google Books

Google Books[10] je počín společnosti Google, Inc. Google Books využívá nejsilnější stránky Google a to je fulltextové vyhledávání. Google Books prohledává kompletní texty knih, které Google naskenoval a převedl do elektronické podoby, kterou umístil do své databáze.

2.3.3 Google Play Books

Google Play[11] Books od společnosti Google, Inc. je aplikace pro distribuci elektronických knih. Hlavní výhodou Google Play Books je integrace s chytrými mobilními telefony, tablety i osobními počítači. Google Play Books udržuje knihy v cloudu a je možné k nim přistupovat z kteréhokoli zařízení připojeného ke Google Play Books pod Google účtem.

Google Play Books zatím není přístupný v České republice, ale ve světě se pyšní obrovskou knihovnou, čítající více než 4 miliony elektronických knih¹.

¹Stav v březnu 2012 uváděný firmou Google

2.3.4 Palmknihy

Palmknihy.cz je lokální projekt v České republice, který nabízí více než 900 knih v češtině, včetně učebnic a odborných knih. Knihy zakoupené na webu palmknihy.cz je možné číst na různých typech zařízení, jako jsou čtečky, tablety, chytré mobilní telefony a osobní počítače.

Zřejmě největší nevýhodou tohoto projektu je zatím malá nabídka knih. Knihy je možné zakoupit pomocí bankovního převodu nebo platební kartou.

Kapitola 3

Zabezpečení PDF dokumentů

Zabezpečení distribuce PDF dokumentů není jednoduchý proces. PDF dokumenty je v dnešní době možné prohlížet na mnoha různých zařízeních. Díky tomu je těžké omezit možnost jejich distribuce. Při zabezpečení distribuce PDF dokumentů je možné vydat se dvěma směry. První směr je snažit se zamezit zobrazení PDF dokumentů osobám, které nejsou autorizovány k jejich prohlížení. Druhý směr je omezit přístup k PDF dokumentům pouze autorizovaným osobám. Tyto dokumenty nějakým způsobem označit a při jejich úniku lze vystopovat, která osoba je pustila do oběhu, a pro příště této osobě zamezit přístup k chráněným dokumentům.

3.1 Zobrazení PDF dokumentů autorizovaným osobám

Nejprve budou analyzovány některé metody z první skupiny zabezpečení. A to možnosti jak umožnit zobrazení PDF dokumentů pouze autorizovaným osobám a nikomu jinému.

3.1.1 Zabezpečení heslem

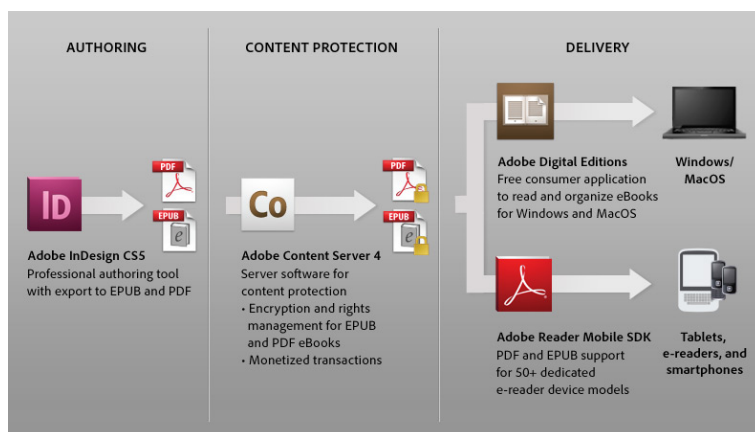
Nejjednodušším způsobem jak zabezpečit PDF dokument proti přečtení je zaheslování. Programy, jako je například Adobe Acrobat umožňují zaheslovat PDF dokument tak, aby nešel otevřít bez zadání hesla, nebo aby nešel dokument tisknout, anebo z něj kopírovat obsah. Zaheslováním dokumentu v Adobe Acrobat vzniká problém s otevřením dokumentu. Pokud se člověk snaží otevřít dokument zaheslovaný programem Adobe Acrobat v jiném programu na prohlížení PDF dokumentů (např. Preview.app na Mac OS) má smůlu a dokument neotevře ani se znalostí hesla.

Další nevýhodou prostého zaheslování PDF dokumentu je množství různě kvalitních programů, které takovéto PDF dokumenty otevrou i bez znalosti hesla.

3.1.2 Digital Rights Management

Digital Rights Management (dále jen DRM) je ochrana, jejímž účelem je kontrolovat, či omezovat používání obsahu digitálních médií[19]. Obvykle DRM zašifruje digitální média tak, že je spojí s identitou uživatele (který dokument pořídil) a tím znemožní šíření mezi ostatními uživateli.

Na trhu s DRM pro elektronické knihy působí tři hlavní hráči. Apple a Amazon mají každý vlastní DRM pro elektronické knihy, které prodávají ve svých obchodech zaměřených na elektronické knihy. Třetím hlavním hráčem na trhu je firma Adobe¹ se svým Adobe DRM, který využívá například i Google[9].



Obrázek 3.1: Proces distribuce elektronických knih pomocí Adobe Digital Publishing for eBook[6]

Pro použití Adobe DRM je potřeba využít několik produktů společnosti Adobe. Naznačeno na obrázku 3.1. Konkrétně se jedná o software Adobe Content Server 4, který se stará o zakódování DRM do PDF dokumentu (případně EPUB). Pro bezproblémové čtení dokumentů s Adobe DRM je potřeba, aby uživatel měl na svém zařízení nainstalovaný Adobe Digital Editions (zdarma pro MS Windows a Mac OS), nebo Adobe Reader Mobile SDK (při čtení dokumentu na mobilních zařízeních nebo elektronických čtečkách).

Nejedná se o levné řešení. Adobe doporučuje jako prodejce pro Evropu společnost Ctrl-Publishing AB se sídlem ve Stockholmu, která prodává licenci Adobe Content Server za 10000 USD. Kompletní ceník zde [8].

3.2 Označení PDF dokumentů

Z druhé skupiny zabezpečení bude analyzován způsob označení PDF dokumentů. Tento způsob ochrany nedokáže zabránit volnému šíření dokumentů, ale umožňuje vystopovat uživatele, který daný dokument začal šířit.

3.2.1 Vodoznak

Vodoznak je nejznámější forma označení dokumentů. Používá se u tištěných dokumentů, známek, kolků i bankovek [21]. Vodoznaky lze snadno vkládat i do elektronických dokumentů. Velmi často se vodoznaky používají u fotografií zveřejněných volně na Internetu, aby nedošlo k jejich zneužití.

¹<http://www.adobe.com/>

Pro vkládání vodoznaků do PDF dokumentů existuje řada klasických desktopových nástrojů a programů. Tyto programy umožňují vložit do PDF dokumentů textové informace na předem určené místo. Mimo klasické desktopové aplikace existuje i řada knihoven pro různé programovací jazyky, které dovolují vložit vodoznak do PDF dokumentu automaticky, bez účasti správce aplikace.

3.3 Shrnutí

V rozšiřovaném prototypu [2] byla již implementována metoda vkládání vodoznaku do PDF dokumentu, a to především proto, že se jedná o metodu nenáročnou na implementaci. Také odpadá nutnost nutit uživatele číst dokumenty na specifických zařízeních, pomocí specifických programů. V neposlední řadě se jedná o metodu, která nemá finanční náklady na provoz a lze jí zcela automatizovat.

Kapitola 4

Platby přes Internet

V druhé části této bakalářské práce je potřeba vypořádat se s problémem spojeným s prováděním plateb za PDF dokumenty přes Internet. V této kapitole je provedena analýza možných řešení pro implementaci tohoto problému. K analýze bylo vybráno několik možných řešení, jako je využití elektronické peněženky, platby platební kartou, nebo platby převodem peněz z účtu na účet.

4.1 Elektronické peněženky

Elektronické peněženky jsou webové aplikace, které umožňují provádět platby přes Internet bez nutnosti pamatovat si údaje z platební karty. Stačí znát přihlašovací údaje k webové peněženke. Uživatel si spáruje svůj osobní účet webové peněženky se svou platební kartou. Po té se uživatel, při platbě podporující danou elektronickou peněženku, prokáže přihlašovacími údaji a aplikace si sama strhne platbu ze spárované platební karty.

4.1.1 PayPal

PayPal¹ je rychlejší, bezpečnější cesta k provádění a přijímání plateb na Internetu[13]. PayPal vznikl jako hlavní platební systém pro největší internetovou aukční síň Ebay² a je považován za etalon mezi elektronickými peněženkami. Pro využívání služeb systému PayPal je potřeba nejprve si vytvořit účet a spárovat ho s platební kartou. PayPal si ověří pravost zadaných údajů tím, že strhne drobnou částku z uvedené platební karty.

Po vytvoření PayPal účtu má uživatel přístup mimo placení i k přijímání plateb na účet. Díky tomu může uživatel platbu uhradit ze zůstatku na svém PayPal účtu. Pokud uživatel nemá na svém účtu žádné finance, PayPal automaticky strhne peníze potřebné k platbě z platební karty. PayPal nabízí řadu možností pro implementaci platebního systému do webových aplikací. V následujících podkapitolách jsou popsány některé z nich.

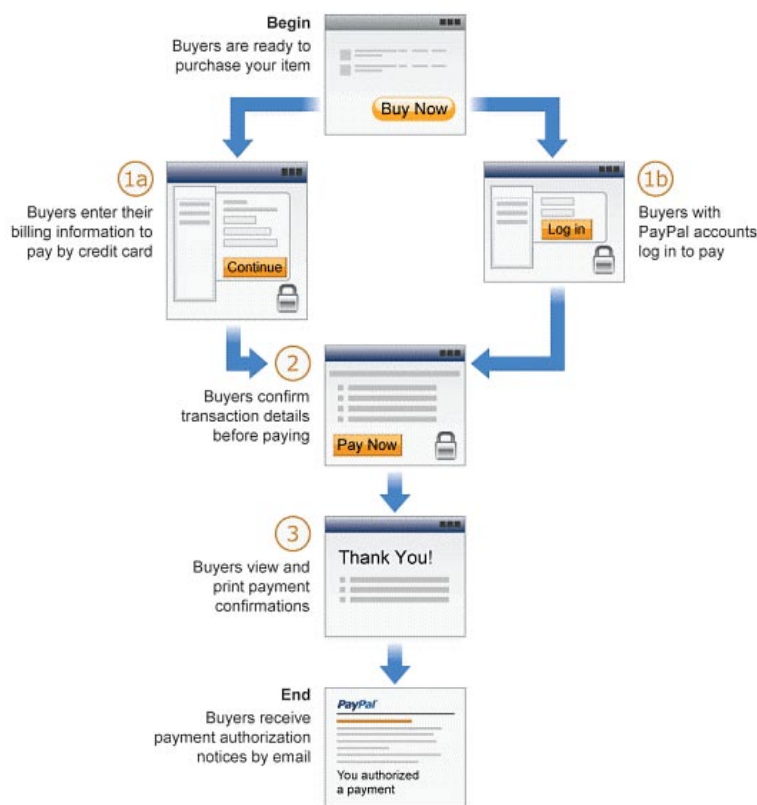
¹<https://www.paypal.com>

²<http://www.ebay.com>

4.1.1.1 Website Payments Standard

Website Payments Standard (někdy též PayPal Payments Standard) je služba, která umožní vložení PayPal tlačítek do HTML webové aplikace. Website Payments Standard nevyžaduje žádný zřizovací poplatek. PayPal si pouze strhává poplatek a procenta z příchozích částek. Výhodou také je možnost zaplatit platební kartou bez nutnosti vlastnit PayPal účet. Tato služba PayPal nabízí čtyři základní typy tlačítek pro různé scénáře použití. Mezi tyto tlačítka patří:

- **Buy Now** - Slouží k jednorázové platbě za zboží. Umožňuje koupit jeden nebo více kusů jednoho druhu zboží.
- **Add to Cart** - Přidává zboží do nákupního košíku na PayPal účtu nakupujícího. Uživatel může pomocí PayPal nákupního košíku provést platbu najednou za více položek.
- **Subscribe** - Toto tlačítko je používáno k vyvolání pravidelných plateb opakujících se po určitém časovém období.
- **Donate** - Slouží k výběru peněžních částek jako darů.



Obrázek 4.1: Proces nákupu s použitím tlačítka Buy Now[17]

Tato čtyři tlačítka lze velmi jednoduše integrovat do webové aplikace pomocí prostého HTML a přesto dokáží pokrýt velké množství platebních operací. Pro potřeby této bakalářské práce se jako nejvhodnější kandidát k implementaci jeví tlačítko Buy Now.

Na obrázku 4.1 je vidět proces nákupu s použitím tlačítka Buy Now. Celý proces se skládá z pěti kroků:

1. Stisknutí tlačítka Buy Now na webu prodejce vyvolá přesměrování na web PayPal
2. Na webu PayPal se kupující buď přihlásí ke svému PayPal účtu, nebo vyplní údaje potřebné k platbě platební kartou.
3. Následuje potvrzení údajů jako je kupovaný předmět, cena a platební údaje.
4. Po provedení platby se uživatel dostane na stránku s informací o úspěchu platby.
5. Nakupující obdrží informace o transakci na e-mailovou adresu uvedenou při platbě (spárovanou s PayPal účtem).

4.1.1.2 Express Checkout

Express Checkout je další cesta jak umožnit uživatelům provádět elektronické platby. Vhodná jako doplňková metoda k již implementované cestě[14]. Express Checkout se integruje pomocí vlastního API a proto není jeho integrace tak jednoduchá jako u Website Payments Standard. Na druhou stranu zase umožňuje efektivněji pracovat s procesem nákupu. Hlavním cílem Express Checkout je vytvořit co nejjednodušší a nejefektivnější nákupní proces pro uživatele (zákazníka) webové aplikace, do níž je integrován.

Express Checkout dává obchodníkovi větší kontrolu nad celým procesem, než tomu je u Website Payments Standard. Při implementaci této metody je PayPal využit pouze k platbě a pak se vrátí na webovou aplikaci, kde dojde k dokončení procesu. Narozdíl od Website Payments Standard, kde došlo k přesměrování zpět na web obchodníka až po úplném dokončení platebního procesu, který je celý vykonán na straně PayPal.

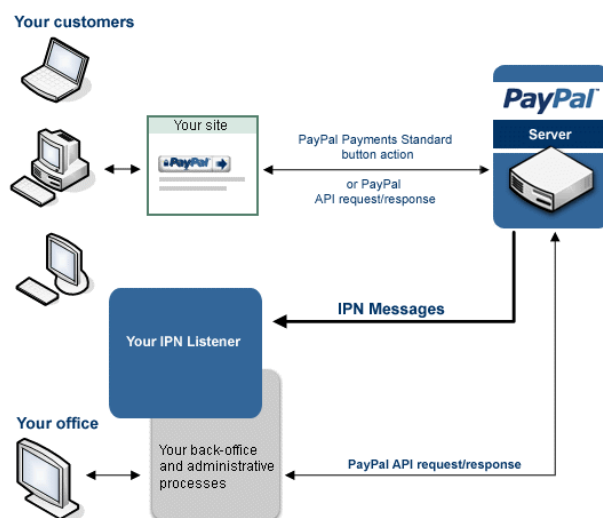
4.1.1.3 Instant Payment Notification

Instant Payment Notification (dále jen IPN) je systém, kterým PayPal komunikuje s webovými aplikacemi o stavu transakce.[15] Díky této službě může prodejce automatizovat proces nákupu. Na obrázku 4.2 je vidět proces komunikace mezi aplikací prodejce a PayPal serverem. Aplikace prodejce musí mít nastavený tzv. IPN listener, který dokáže zpracovat IPN zprávu. IPN zpráva je vlastně jen HTTP POST request, který je automaticky odeslán na nastavenou URL adresu a obsahuje potřebné informace o stavu transakce. Kompletní přehled IPN proměnných je k nalezení zde [16].

4.1.2 PaySec

PaySec³ je česká elektronická peněženka od Československé obchodní banky (dále ČSOB). PaySec je univerzální on-line platební řešení pro platby na Internetu na bázi předplaceného

³<http://www.paysec.cz/>



Obrázek 4.2: Proces požadavku a odpovědi s použitím IPN[15]

konta. Pomocí Konta je možné platit u obchodníků, kteří platbu PaySec podporují, nebo provádět platby mezi Konty PaySec [25].

PaySec pracuje obdobným způsobem jako PayPal. Nakupující uživatel je přesměrován na platební bránu PaySec, kde autorizuje transakci a následně je zpět přesměrován na webovou aplikaci prodejce. Narozdíl od PayPal nepracuje PaySec přímo s platební kartou uživatele. Uživatel si musí nejprve vložit peníze na své Konto PaySec (pomocí bankovního převodu, nebo platební kartou). Částky za provedené transakce jsou pak strhávány z Konta PaySec.

4.1.3 Rozhraní Merchant API

Rozhraní Merchant API popsané v příručce [25] je webová služba, která umožňuje prodejcům provádět kontrolu stavu transakce, která prošla platební branou PaySec. Narozdíl od PayPal IPN, kde informace o stavu transakce přichází automaticky po autorizování platby kupujícím, se u Merchant API musí prodejce na stav transakce dotázat sám.

4.2 Platba platební kartou

Platba platební kartou nevyžaduje po kupujícím vlastnit účet u nějaké elektronické peněženky. Stačí pouze opsat údaje z platební karty. Na druhou stranu velké množství potenciálních kupujících odmítá předat tyto choulostivé údaje webovému obchodu.

Pro zavedení platby platební kartou je potřeba implementovat platební bránu od nějaké banky. České banky využívají pro implementaci bran řešení postavené na protokolu 3-D Secure. 3-D Secure je protokol na bázi XML navržený jako bezpečnostní vrstva pro online transakce kreditními a platebními kartami[18].

4.2.1 ČSOB

Československá obchodní banka (dále jen ČSOB), nabízí platební bránu pro akceptaci platebních karet, určenou internetovým obchodníkům, registrovaným v ČR, kteří požadují rozšíření platebních metod o možnost platby kartou za zboží či služby nabízené v rámci jejich e-shopu[24]. ČSOB využívá řešení GP webpay od společnosti Global Payments Europe, s.r.o.. Toto řešení akceptuje karty MasterCard, Maestro, VISA a VISA Electron.

Podmínkou provozování platební brány od ČSOB je alespoň jeden účet vedený u ČSOB, na který jsou částky z transakcí připisovány. Pro realizaci akceptace platebních karet je potřeba zabezpečení SSL protokolem s minimálně 128b šifrováním. Služba pracuje s měnami CZK, USD, GBP a EUR.

Poplatky spojené s implementací akceptace platebních karet u ČSOB se řeší individuálně. Ve většině případů jde o jednorázový poplatek za instalaci ve výši 13200 CZK, dále je potřeba odvádět procenta z transakcí. Obvykle 3% - 5%.

4.2.2 Česká spořitelna

Česká spořitelna (dále jen ČS) nabízí obdobně jako ČSOB řešení postavené na protokolu 3-D Secure. Pokud se kupující rozhodne využít k platbě platební kartu, vyplní údaje o platební kartě na Platební stránce České spořitelny. Česká spořitelna zajistí bezpečný zakódovaný přenos dat a obchodníkovi pouze sdělí výsledek autorizace a dává tím pokyn k vyřízení objednávky[27].

Podmínkou provozování platební brány je zabezpečení SSL protokolem. Služba pracuje s měnami CZK, USD, GBP a EUR. Platební brána podporuje mimo českého jazyka také anglický a německý jazyk.

Poplatky spojené s implementací akceptace platebních karet u ČS jsou obdobné jako u ČSOB. Také se řeší individuálně. Ve většině případů jde o jednorázový poplatek za instalaci ve výši 10000 CZK, dále je potřeba odvádět procenta z transakcí stejně jako u ČSOB 3% - 5%.

4.3 Převody peněz

Převod peněz z účtu na účet je nejjednodušší na implementaci, ale vyžaduje časté zásahy ze strany správce webové aplikace a je časově náročný na zpracování. Při provedení platby je potřeba vygenerovat fakturační údaje pro kontrolu od koho daná platba přišla (nejčastěji variabilní symbol) a spojit je s konkrétním uživatelem. Uživatel provede převod na daný účet s požadovaným variabilním symbolem. Po té je potřeba ze strany správce aplikace kontrolovat účet, dokud se na něm neobjeví platba (obvykle do druhého pracovního dne od zadání platebního příkazu k převodu peněz). Až se platba objeví na účtu, musí správce nastavit v aplikaci, že platba byla úspěšně provedena a kupený dokument nastavit jako stáhnutelný pro kupujícího.

Tato metoda není moc efektivní, je časově náročná a vyžaduje neustálou kontrolu ze strany správce aplikace, proto byla hned zavrhnuta.

	Zřizovací poplatek	Měsíční poplatky	Poplatek za transakci
Web Payments Standard	0 CZK	0 CZK	3,4% + 10,00 CZK
Express Checkout	0 CZK	0 CZK	3,4% + 10,00 CZK
PaySec	0 CZK	0 CZK	1 CZK
ČSOB	13 200 CZK	150 CZK	cca 3% + 2 CZK
ČS	10 000 CZK	150 CZK	3% - 5%
Převod	0 CZK	0 CZK	0 CZK

Tabulka 4.1: Srovnání poplatků spojených s implementací platebních metod

4.4 Srovnání a výběr

Všechny zde analyzované metody mají své výhody a nevýhody. Pro potřeby této práce je brán ohled hlavně na finanční náklady na provoz plateb přes Internet a také na náročnost implementace. Finanční srovnání je uvedeno v následující podkapitole. Náročnost implementace je pro všechny metody velmi podobná. Jedná se o HTML formuláře, které komunikují s poskytovatelem služby pomocí HTTP POST požadavků. Metoda bankovního převodu z účtu na účet není poskytována jako služba a je třeba jí implementovat od nuly. Přesto není implementace této metody náročná, jedná se opět o formulář a generování variabilních symbolů.

4.4.1 Finanční srovnání

Finanční náklady na provoz těchto metod jsou uvedeny v tabulce 4.1. U akceptace platebních karet od ČSOB a ČS se jedná o orientační hodnoty. Konkrétní částky je potřeba dojednat individuálně se zástupci dané banky. U PayPal metod jsou poplatky uvedené v tabulce pro měsíční příjmy do 70000 CZK. Při vyšších měsíčních příjmech se procenta z transakce snižují. Spodní hranice je 1,9%.

4.4.2 Výběr

Po zvážení všech potřeb této bakalářské práce byl z možných řešení okamžitě vyškrtnut bankovní převod. Tato metoda je sice nejméně nákladná na provoz po finanční stránce, ale za to je velmi náročná na správu ze strany administrátora aplikace a tudíž nevhodná k použití. Jako další možnosti byly zavrhnuty metody využívající akceptace platebních karet od ČSOB i ČS a to hlavně kvůli vysokým finančním nákladům na zřízení. Ve výsledku zbyla jen metoda elektronické peněženky, ze které byla nakonec vybrána varianta PayPal Payments Standard, z důvodů jednoduché implementace i možnosti provést platbu z platební karty bez nutnosti vlastnit PayPal účet.

Kapitola 5

Analýza

5.1 Uživatelé

Předpokládá se, že s aplikací budou pracovat různí uživatelé z akademického prostředí ČVUT FEL. Činnosti těchto uživatelů půjdou rozdělit do dvou hlavních skupin.

První skupinou budou uživatelé, kteří budou aplikaci zásobovat obsahem. Tedy hlavně vyučující a další zaměstnanci školy. Jejich primární činností bude nahrát vybraný PDF dokument do aplikace, nastavit jeho vlastnosti a sdílet ho pomocí systémem vygenerovaných odkazů. Mezi další činnosti bude patřit editace vlastností PDF dokumentů, případně nahrazení dokumentu aktuální verzí a v neposlední řadě také mazání dokumentů.

Nejpočetnější skupina uživatelů aplikace bude tvořena studenty, kteří budou na základě získaných odkazů stahovat požadované materiály ve formě PDF dokumentů.

5.1.1 Uživatelské role

Na základě analýzy uživatelů systému byly navrženy uživatelské role. Pro jednoduchost jsou role navrženy tak, aby je bylo možné generalizovat. Generalizace uživatelských rolí znamená, že uživatel s rolí vyššího stupně má zároveň vlastnosti uživatelů s rolemi nižších stupňů. Uživatelské role byly zvoleny takto:

- **Host** je jakýkoliv uživatel, který vstoupí do aplikace a nepřihlásí se. Takový uživatel nemá prakticky žádné práva v aplikaci a bude mu zobrazena pouze úvodní stránka. Při pokusu vykonání jakékoliv aktivity v systému bude vyzván k přihlášení se přes FELid.
- **Student** je přihlášený uživatel, který je v systému FELid evidován jako student. Student má právo stáhnout si pomocí odkazu PDF dokument, který bude před stažením označen vodoznakem se jménem studenta a datem stažení dokumentu.
- **Vyučující** je také přihlášený uživatel, který je v systému FELid evidován jako zaměstnanec fakulty. Vyučující má stejné právo stahovat PDF dokumenty jako Student a zároveň může do aplikace vkládat a následně i spravovat nové dokumenty. Každý uživatel s rolí Vyučující bude mít právo spravovat pouze PDF dokumenty, které sám do systému vložil.

- **Administrátor** bude přihlášený uživatel, který bude mít právo spravovat aplikaci. Administrátor bude mít stejná práva jako Vyučující s tím, že narozdíl od něj bude mít přístup ke správě všech dokumentů od všech možných Vyučujících.

5.2 Požadavky

V této sekci jsou uvedeny požadavky na portál z pohledu zadání práce.

5.2.1 Funkční požadavky

Funkční požadavky nám říkají, jaké akce bude systém umožňovat uživatelům provádět. Tyto akce jsou pokryty případy užití. [12]

1. Systém bude umožňovat vyučujícím vkládat studijní materiály.
 - Každý přihlášený uživatel s uživatelskou rolí Vyučující bude moci přidat pomocí jednoduchého formuláře nový PDF dokument.
 - Při vkládání PDF dokumentu do systému bude možné nastavit PDF dokumentu základní parametry.
 - Dokument zůstane uložen v aplikaci s vygenerovanou adresou, přes kterou bude možné dokument stáhnout.
2. Systém bude umožňovat vyučujícím upravovat parametry vložených dokumentů.
 - Každý přihlášený uživatel s uživatelskou rolí Vyučující bude mít možnost upravovat parametry dokumentů, které vložil do systému.
3. Systém bude umožňovat vyučujícím měnit a mazat dříve nahrané PDF dokumenty.
 - Každý přihlášený uživatel s uživatelskou rolí Vyučující bude mít možnost zaměnit dříve nahraný PDF dokument za novější verzi.
 - Další možností pro uživatele s uživatelskou rolí Vyučující bude možnost odstranění dříve vloženého PDF dokumentu ze systému. Odkazy směřující na smazaný dokument budou nefunkční.
4. Systém bude umožňovat prodej PDF dokumentů.
 - Každý přihlášený uživatel s uživatelskou rolí Vyučující bude mít možnost nastavit aplikaci tak, aby umožnila stažení PDF dokumentu až po provedení platby.
5. Systém bude umožňovat studentům stahovat PDF dokumenty.
 - Každý student, který vstoupí do aplikace přes odkaz na stažení PDF dokumentu a přihlásí se do systému, bude mít možnost tento dokument stáhnout.
 - Stažený PDF dokument bude označen vodoznakem obsahujícím informace o tom, kdy byl dokument stažen a také o tom, kým byl stažen.

6. Systém bude umožňovat administrátorovi provádět jakékoliv úpravy v systému.

- Přihlášený uživatel s uživatelskou rolí Administrátor bude mít možnost měnit nastavení všech PDF dokumentů vložených do systému včetně jejich smazání.

5.2.2 Nefunkční požadavky

Nefunkční požadavky představují určitá omezení a vlastnosti, které musí daný systém splňovat. [12]

1. Systém bude přehledný a snadno ovladatelný.

- Systém bude navržen tak, aby bylo co nejjednodušší ho ovládat.
- Studentům bude stačit pouze odkaz na stažení PDF dokumentu a přihlášení k FELid na to, aby se dokument stáhl.
- Žádné klikání na odkazy ke stažení. Stažení začne automaticky hned po přihlášení.

2. Systém bude vyvinut na platformě Ruby on Rails

- Systém bude napsaný v programovacím jazyku Ruby ¹ s použitím frameworku Ruby on Rails².

5.3 Případy užití

V této kapitole se nacházejí případy užití vycházející z funkčních požadavků na aplikaci.

UC01 Přihlášení uživatele

Uživatelské role: Student, Vyučující, Administrátor

Scénář: Scénář začíná vstupem uživatele na stránku, která vyžaduje přihlášení.

1. Uživatel vstoupí na stránku vyžadující přihlášení.
2. Systém přesměruje uživatele na web s formulářem pro přihlášení do FELid.
3. Uživatel vyplní jméno, heslo a přihlásí se.
4. Systém po přihlášení přesměruje uživatele zpět na požadovanou stránku a vyhodnotí uživatelskou roli.

Vyhovuje: Uživatel je vpuštěn na požadovanou stránku.

Nevyhovuje: Uživatel je informován o nedostatečných právech a je přesměrován na úvodní stránku aplikace.

UC02 Vložení PDF dokumentu

Uživatelské role: Student, Vyučující, Administrátor

Scénář: Scénář začíná přístupem přihlášeného uživatele s vyhovující rolí na stránku pro správu PDF dokumentů.

¹<http://www.ruby-lang.org>

²<http://www.rubyonrails.com>

1. Uživatel klikne na tlačítko přidat nový PDF dokument.
2. Systém zobrazí formulář pro vložení nového PDF dokumentu.
3. Uživatel vyplní název dokumentu, anotaci, typ distribuce (případně cenu), text umístěný do zápatí dokumentu, připojí požadovaný PDF dokument, zaškrtně povolení tisku nebo povolení kopírování textu a odešle formulář.
4. Systém vyhodnotí validitu vstupních dat.

Validní: Dokument je vložen do systému a je mu vygenerována adresa na stažení.

Nevalidní: Uživatel je přesměrován zpět na formulář s výpisem chyb. Dokument není uložen do systému.

UC03 Stažení PDF dokumentu

Uživatelské role: Vyučující, Administrátor

Scénář: Scénář začíná přístupem přihlášeného uživatele s vyhovující rolí na příslušný odkaz.

1. Uživatel zadá odkaz pro stažení PDF dokumentu.
2. Systém vyhodnotí existenci PDF dokumentu pod tímto odkazem.

Existuje: Dokument je označen patřičným vodoznakem a automaticky začíná stahování.

Neexistuje: Uživatel je upozorněn na neexistenci PDF dokumentu.

Kapitola 6

Implementace

6.1 Použité technologie

Použité technologie vycházejí z velké části z prototypu aplikace[2]. Pro jednodušší rozšiřování aplikace je většina použitých technologií zachována. Jelikož se jedná o webovou aplikaci, je celá aplikace dostupná z webového prohlížeče. Aplikace se nachází na adrese <https://simple.felk.cvut.cz/>. Na této adrese už běžel prototyp aplikace, který umožňoval nahrávat na server PDF dokumenty (komukoliv bez omezení). Aplikace byla napsaná v programovacím jazyku Ruby pod frameworkem Ruby on Rails (dále jen RoR).

6.1.1 Programovací jazyk a framework

Programovací jazyk Ruby s frameworkem RoR byl zachován pro snazší rozšiřování prototypu. Ze stejného důvodu byla i dodržena původní verze frameworku RoR a to 3.0.5 přesto, že v současné době je framework RoR dostupný ve verzi 3.2.3. Změny mezi verzemi 3.0.x, 3.1.x a 3.2.x jsou tak zásadní, že by aktualizování aplikace na aktuální verzi vyžadovalo přepsání velké části aplikace a tím by nezbyl čas na požadované rozšíření prototypu.

6.1.2 Server

Jak bylo už napsáno výše, jedná se o webovou aplikaci, a tudíž je potřeba pro chod aplikace použít webový server. V případě této bakalářské práce běží server na operačním systému Debian GNU/Linux¹.

Jako webový server je použit server Apache 2². Apache má nainstalované doplňky pro SSL, Rewrite pro htaccess, Shibboleth pro FELid, Phusion Passenger pro spuštění RoR aplikace. Aplikace běží jako Virtual Host se zapnutým SSL. Pomocí htaccess je veškerý přístup na adresu <http://simple.felk.cvut.cz/> přesměrován na <https://simple.felk.cvut.cz/>. Více o nastavení Apache serveru pro SSL je k nalezení v sekci 6.2.1.

¹<http://www.debian.org/>

²<http://httpd.apache.org/>

Soubor `.htaccess`, který se stará jen o přesměrování na HTTPS vypadá takto:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}%
```

6.1.3 Databáze

Aplikace vyžaduje ukládání dat do databáze, a proto bylo potřeba zvolit vhodný databázový systém. V tomto případě byl zvolen systém SQLite³. SQLite je relační databázový systém obsažený v relativně malé knihovně napsané v C. Je vyvíjen D. Richardem Hippem a šířen pod licencí public domain[20]. Databáze vytvořená systémem SQLite je uložena v jednom souboru na disku a je jednoduché jí přesouvat, kopírovat nebo zálohovat. Pro kontrolu stavu databáze je vhodné použít nástroj SQLite Manager⁴, který je dostupný jako doplněk do webového prohlížeče Mozilla Firefox⁵. Pomocí tohoto doplňku lze otevřít databázový soubor vytvořený systémem SQLite a ten následně prohlížet a spravovat.

Díky použití frameworku RoR není problém kdykoliv zvolený databázový systém změnit pomocí RoR Migrations. O RoR Migrations lze najít podrobné informace v těchto zdrojích[4][23].

6.2 Integrace FELid

FELid je globální autentizační a autorizační systém pro webové aplikace na síti FEL. Poskytuje jednotný a bezpečný způsob přihlášení uživatelů a přenos jejich údajů do různých aplikací na webu. Zároveň podporuje jednorázové přihlášení (tzv. Single Sign-On). Znamená to, že se uživatel přihlašuje pouze do první použité aplikace a u dalších aplikací už nemusí zadávat svoje přihlašovací údaje[1].

FELid je postaven na projektu Shibboleth⁶. Shibboleth pracuje jako modul Apache 2 serveru a vyžaduje na serveru nainstalovaný a nastavený Shibboleth Service Provider (návod na instalaci Service Provideru lze nalézt zde[26], návod na nastavení zde[5]). Další podmínkou pro provoz FELid je X.509 certifikát, kterým se podepisují zprávy odesílané poskytovateli identit (Shibboleth Identity Provider⁷). Použitý certifikát musí jako Common Name položku obsahovat hostname serveru (v případě této bakalářské práce tedy `simple.felk.cvut.cz`)

6.2.1 Nastavení Apache serveru

Pro bezproblémový chod FELid na webovém serveru je potřeba správně nastavit webový server Apache (v tomto případě ve verzi 2). Apache musí mít povolený SSL na portu 443

³<http://www.sqlite.org/>

⁴<https://addons.mozilla.org/en-US/firefox/addon/sqlite-manager/>

⁵<http://www.mozilla.org/en-US/firefox/new/>

⁶<http://shibboleth.net/>

⁷Identity Provider je server poskytující informace o uživateli sítě vůči kterému si Service Provider ověřuje identitu uživatele, který se chce přihlásit do webové aplikace.

(minimálně pro URL adresy, které budou vyžadovat autentizaci přes FELid). V případě této bakalářské práce je nastavený SSL pro celý web.

Nejdůležitější části z konfiguračního souboru pro Virtual Host `default-ssl`.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
ServerName simple.felk.cvut.cz
DocumentRoot /var/www/pdfapp/public/

<Directory /var/www/pdfapp/public>
    Options ExecCGI FollowSymLinks
    AllowOverride all
    Order allow,deny
    Allow from all
</Directory>

<Location /pdfdown>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>

<Location /vlozipdfs>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>

SSLEngine on

SSLCertificateFile /etc/apache2/security/simple.felk.cvut.cz.pem
SSLCertificateKeyFile /etc/apache2/security/simple.felk.cvut.cz.key

</VirtualHost>
</IfModule>
```

Nejdůležitější z celého nastavení SSL Virtual Host jsou části `<Location>`. V části `location` se definuje pro jakou URL adresu je požadována autentice pomocí FELid. V případě této aplikace se jedná o adresy `/pdfdown` a `/vlozipdfs`.

6.2.2 Získání atributů aplikací

Po úspěšném přihlášení přes FELid získá server údaje o přihlášeném uživateli. Tyto údaje je potřeba předat aplikaci, aby s nimi bylo možné dále pracovat. Tyto údaje jsou přístupné přes serverové proměnné. V RoR se k serverovým proměnným přistupuje přes proměnnou `request.env`.

Nejvhodnější řešení je definovat přihlášeného uživatele v `ApplicationController.rb`

```
class ApplicationController < ActionController::Base
  protect_from_forgery

  helper_method :current_user

  private

  def authenticated?
    request.env['felid-uid'].present?
  end

  def fel_id
    {
      :user_id      => request.env['felid-uid'],
      :user_email   => request.env['felid-mail'],
      :user_role    => request.env['felid-employeeType']
    }
  end

  def current_user
    @current_user = fel_id if authenticated?
  end
end
```

Metoda `authenticated?` ověřuje zda se mezi serverovými proměnnými vyskytuje proměnná `felid-uid`. Pokud se tato proměnná na serveru vyskytuje, je uživatel přihlášen. Dále se vytvoří asociativní pole `fel_id`, které obsahuje unikátní identifikátor přihlášeného uživatele `felid-uid`, e-mail přihlášeného uživatele `felid-email` a vztah přihlášeného uživatele k fakultě `felid-employeeType`. Nakonec se vytvoří proměnná `@current_user` přístupná z views aplikace, do které se nahraje pole `fel_id`, pokud je uživatel přihlášený. Pokud uživatel přihlášený není, je v proměnné `@current_user` objekt `nil`.

Díky definování atributů získaných z FELid v `ApplicationController`, má celá aplikace přístup k údajům o přihlášeném uživateli uloženým v proměnných `fel_id` a `@current_user`. To umožňuje například vložení uživatelského jména do PDF dokumentu.

Ukázka části kódu `StahnoutpdfsController.rb`

```
class StahnoutpdfsController < ApplicationController
  .
  .
  def stahnoutpdfko
    .
    .
  end
end
```

```

        @username = fel_id[:user_id]
      .
      .
    end
  .
  .
end

```

6.2.3 Práce s uživatelem v aplikaci

Z důvodu nutnosti evidování údajů o platbách uživatelů za PDF, je potřeba vyřešit ukládání informací o uživateli do databáze. Jedním z důvodů využití FELid bylo vyhnutí se nutnosti vyžadovat po uživateli klasickou formu registrace. Z tohoto důvodu bylo nutné vymyslet postup jak vložit do databáze údaje o uživateli vytažené z FELid. Nakonec byl implementovaný model User, který shromažďuje tyto údaje. Před některými akcemi, které vyžadují vytažení načtení informací o uživateli z databáze, konkrétně při vložení PDF do systému a také při zakoupení PDF přes PayPal, se provede následující kousek kódu.

```

user = User.find_by_username(current_user)
if !user
  user = User.new(:username => current_user, :uploaded => 0)
  user.save!
end

```

Tento kus kódu se nejprve podívá do databáze jestli uživatel s daným uživatelským jménem (fel-uid) v databázi existuje, a pokud ne, tak ho vytvoří a nastaví mu velikost všech vložených PDF na 0⁸

6.3 Integrace PayPal

6.3.1 Vytvoření PayPal účtu

Pro vývoj integrace PayPal je potřeba si nejprve vytvořit účet se kterým se bude provádět testování vývoje. Účet se vytváří na stránce <https://developer.paypal.com/>. Pod tímto účtem je potřeba vytvořit testovací uživatele. Minimálně jednoho prodejce a jednoho nakupujícího.

6.3.2 Buy Now tlačítko

Metoda pro vygenerování PayPal URL ke koupi PDF dokumentu[22]. Nachází se v modelu `Vlozitpdf.rb`

⁸ Aplikace je nastavena tak, že každému uživateli, který se prokáže přihlášením přes FELid umožní nahrávat PDF dokumenty. Aby nedošlo k zahlcení, je nastaveno omezení na celkovou možnou kapacitu nahraných souborů. Tato hodnota je nastavena na 5MB a je možné jí změnit v konfiguraci aplikace.

```

def paypal_url(current_user)

  invoice = "I" + Time.now.to_i.to_s
  user = User.find_by_username(current_user)
  if !user
    user = User.new(:username => current_user, :uploaded => 0)
    user.save!
  end
  purchase = Purchase.new(:user_id => user.id, :pdf_id => id, :invoice => invoice)
  purchase.save!

  values = {
    :business => "hovorj_1336642396_biz@fel.cvut.cz",
    :cmd => "_xclick",
    :upload => 1,
    :return => "https://simple.felk.cvut.cz/vlozitpdfs/",
    :invoice => invoice,
    :currency_code => "GBP",
    :notify_url => "https://simple.felk.cvut.cz/notify/"
  }

  values.merge!({
    "amount" => price,
    "item_name" => "PDF dokument: " + name,
    "item_number" => id,
    "quantity" => 1
  })

  "https://www.sandbox.paypal.com/cgi-bin/webscr?" + values.to_query
end

```

Po kliknutí na tlačítko **Checkout with PayPal** se vytvoří záznam v tabulce **Purchases**, který obsahuje unikátní číslo faktury generované pro daný PDF dokument a pro daného uživatele. Záznam dále obsahuje unikátní identifikátory uživatele i PDF dokumentu. Hodnota **purchased_at** zůstane prázdná. Podle této hodnoty aplikace určuje zda byl PDF dokument uživatelem zakoupen. Pokud je tato proměnná prázdná, aplikace pozná, že dokument zatím nebyl zakoupen (transakce zatím úspěšně neproběhla).

Do PayPal URL je potřeba vložit všechny potřebné údaje (v kódu nazvané **values**). Konkrétně se jedná o email prodejce (při testování aplikace jde o email testovacího prodejce), typ tlačítka, návratovou adresu, číslo faktury, měnu⁹, adresu na kterou má PayPal poslat IPN zprávu a informace o zakoupeném produktu.

Aplikace zatím běží v testovacím režimu, a proto je zpráva odeslaná na testovací PayPal Sandbox, který simuluje reálné prostředí, ale neprovádí přesuny reálných peněz mezi účty

⁹Měna je v současném testovacím stavu nastavena na GBP, protože přednastavení testovací uživatelé v PayPal účtu nemají možnost zvolit účet v českých korunách a díky tomu docházelo k neúspěšnému provedení transakce.

nakupujícího a prodejce.

6.3.3 Ověření platby

Ověření platby vychází z příchozí zprávy PayPal IPN. PayPal IPN přichází na adresu definovanou v PayPal URL jako `notify_url`. Konkrétně se jedná o `https://simple.felk.cvut.cz/notify/`. Tato adresa je pomocí routování přeměrována na akci `create` v `PurchasesController`. Pokud PayPal IPN zpráva obsahuje informaci `payment_status` s hodnotou `Completed`, byla transakce úspěšně provedena. Následně se v tabulce `Purchases` najde nákup s číslem faktury uvedeném v PayPal IPN zprávě. Tento záznam se upraví tak, že se hodnota `purchased_at` nastaví na aktuální datum a čas (tím se považuje nákup za dokončený).

Ukázka z `routes.rb`

```
match "notify" => "purchases#create", :via => :post
```

`PurchasesController.rb`

```
class PurchasesController < ApplicationController
  protect_from_forgery :except => [:create]

  def create
    if params[:payment_status] == "Completed"
      purchase = Purchase.find_by_invoice(params[:invoice])
      purchase.update_attribute(:purchased_at, Time.now)
    end
    render :nothing => true
  end
end
```

RoR má vestavěnou ochranu proti CSRF¹⁰, a proto blokuje všechny požadavky POST, PUT a DELETE, které přicházejí z Internetu. PayPal IPN je HTTP POST požadavek, a tudíž je RoR frameworkem blokován. Z tohoto důvodu je potřeba tuto ochranu vypnout pro akci `create`. To se dělá pomocí:

```
protect_from_forgery :except => [:create]
```

6.3.4 Zpřístupnění odkazu ke stažení

Zpřístupnění odkazu na stažení PDF dokumentu uživateli, který ho zakoupil se řídí hodnotami v tabulce `Purchases`.

Ukázka kódu, který zpřístupňuje odkaz na stažení zaplaceného PDF dokumentu uživateli, který ho zakoupil.

`VlozitpdfsController.rb`

¹⁰http://en.wikipedia.org/wiki/Cross-site_request_forgery

```

class VlozitpdfsController < ApplicationController
  def index
    @vlozitpdfs = Vlozitpdf.all
    user = User.find_by_username(fel_id[:user_id])
    if user
      @purchases = Purchase.where("user_id = ?", user.id)
      @paid = false
    end
  end
end
.
.
end

views/vlozitpdfs/index.html.erb

.
.
<% if !@purchases.nil? %>
  <% @purchases.each do |purchase| %>
    <% if purchase.pdf_id == vlozitpdf.id && !purchase.purchased_at.nil? %>
      <td>
        <%= link_to "https://#{self.request.host}/pdfdown/
          #{vlozitpdf.hashString.to_s}", "pdfdown/" + vlozitpdf.hashString.to_s %>
      </td>
      <% @paid = true %>
    <% end %>
  <% end %>
  <% if @paid == false %>
    <td>
      <%= link_to(image_tag("btn-paypal.gif"),
        vlozitpdf.paypal_url(current_user[:user_id]), :class => "no-back") %>
    </td>
  <% end %>
<% end %>
<% if @purchases.nil? && @paid == false %>
  <td>
    <%= link_to(image_tag("btn-paypal.gif"),
      vlozitpdf.paypal_url(current_user[:user_id]), :class => "no-back") %>
  </td>
<% end %>
.
.

```

Proměnná `@purchases` obsahuje všechny záznamy z tabulky `Purchases`, které obsahují aktuálního uživatele, který s aplikací pracuje. Aplikace tyto záznamy prohlédne a hledá zda se mezi nimi nevyskytne záznam obsahující unikátní identifikátor daného PDF dokumentu

a zároveň zda byl tento dokument již zakoupen uživatelem. Pokud takový záznam najde zobrazí aplikace odkaz ke stažení tohoto PDF dokumentu. V jiném případě aplikace zobrazí tlačítko Checkout with PayPal.

6.3.5 Připomínkování PDF dokumentů

Připomínkování PDF dokumentů znamená, že přihlášení uživatelé mohou k jednotlivým PDF dokumentům přidávat komentáře. Komentáře lze psát a číst v sekci s detailem PDF dokumentu. Implementace vychází z [3].

Ukázka kódu pro zobrazení a přidání komentářů.

views/vlozitpdfs/show.html.erb

```
.
.
<h2>Komentáře: </h2>
<% @vlozitpdf.comments.each do |comment| %>
  <p>
    <b>Uživatel: </b>
    <%= comment.author %>
  </p>

  <p>
    <b>Komentář: </b>
    <%= comment.content %>
  </p>
<% end %>

<h2>Vložit komentář: </h2>
<%= form_for([@vlozitpdf, @vlozitpdf.comments.build]) do |f| %>
  <div class="field">
    <%= f.hidden_field :author, :value => current_user[:user_id] %>
  </div>

  <div class="field">
    <%= f.label :content, "Text komentáře" %><br />
    <%= f.text_area :content %>
  </div>
  <div class="actions">
    <%= f.submit "Komentovat" %>
  </div>
<% end %>
```

Jedinou změnou oproti implementaci popsané v [3] je umístění skrytého formulářového pole, kterým se vkládá do komentáře uživatelské jméno získané z FELid.

Kapitola 7

Testování

7.1 Testování viditelnosti vodoznaků

Vkládání vodoznaků do PDF dokumentů bylo otestováno na více druzích PDF dokumentů a ukázalo, že existují dvě možnosti jak vložit vodoznak do PDF dokumentu. Rozšiřovaný prototyp[2] používá kombinaci dvou nástrojů. **Prawn**¹ pro vytvoření PDF dokumentu s vodoznakem a **pdftk**² pro vložení PDF s vodoznakem do původního PDF dokumentu.



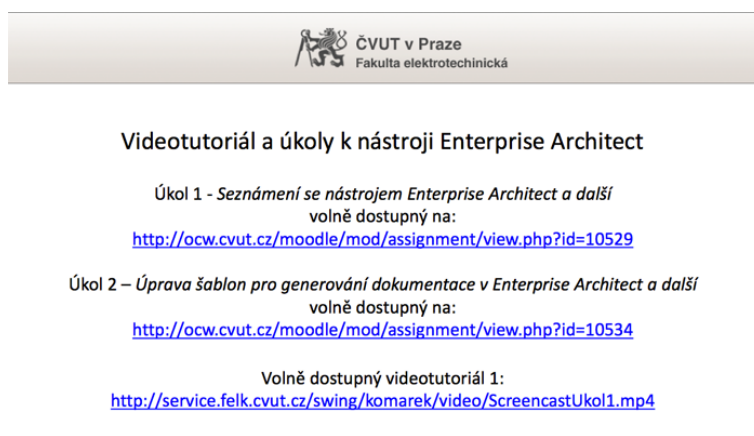
Obrázek 7.1: Vložený vodoznak v popředí PDF vytvořeného z MS Powerpoint

pdftk nabízí dvě možnosti vložení vodoznaku do dokumentu. První možnost je vložit vodoznak jako pozadí originálního PDF. Druhá varianta vloží vodoznak do popředí PDF dokumentu přes původní obsah (ukázka na obrázku 7.1). Testování ukázalo, že první varianta vložení vodoznaku není použitelná pro některé druhy PDF dokumentů. Konkrétně se jedná o PDF vytvořená pomocí programu Microsoft Powerpoint (ukázka na obrázku 7.2), nebo PDF vytvořená pomocí Google Docs. Ani druhá varianta není bez chyby. Při vkládání vodoznaku

¹<http://prawn.majesticseacreature.com/>

²<http://www.pdflabs.com/tools/pdftk-the-pdf-toolkit/>

do popředí dokumentu dochází ke snížené čitelnosti, protože původní obsah je na některých místech zakrytý vodoznakem.



Obrázek 7.2: Vložený vodoznak v pozadí PDF vytvořeného z MS Powerpoint

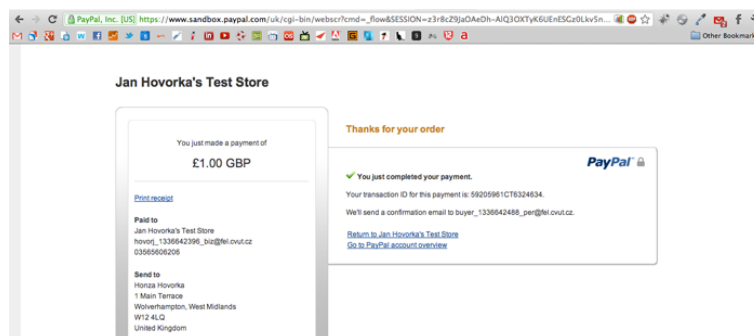
Testování ukázalo, že asi nejvhodnější by bylo vytvořit kombinaci obou variant vložení vodoznaku. V místech, kde by vodoznak nesnižoval čitelnost původního dokumentu, by se vložil vodoznak na popředí a na jiné místo by se vodoznak umístil do pozadí PDF dokumentu.

7.2 Testování integrace FELid

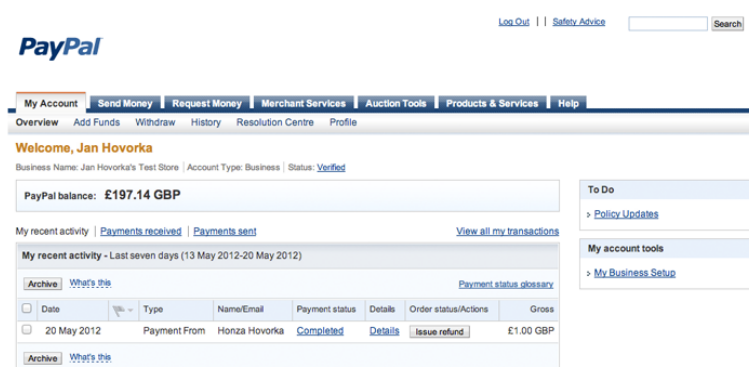
Integrace autentizace a autorizace FELid je obtížná na otestování, protože je k testování potřeba vlastnit existující účty. Z tohoto důvodu byla aplikace otestována pomocí dvou uživatelů. Autora této bakalářské práce a jeho vedoucího. Testování ukázalo, že integrace proběhla úspěšně. Do aplikace je možné se přihlásit přes FELid a zároveň aplikace dokáže dále pracovat s atributy získanými po přihlášení. Ukázka práce s uživatelským jménem získaným z FELid je k vidění na obrázku 7.1, kde je uživatelské jméno vloženo jako vodoznak do PDF dokumentu.

7.3 Testování integrace PayPal

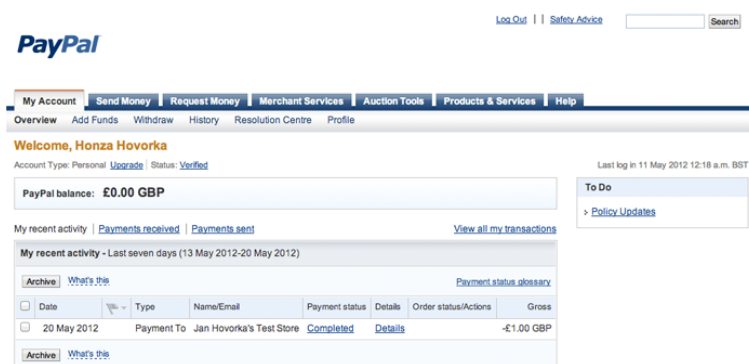
Úspěšnost integrace PayPal lze otestovat pomocí vytvořených testovacích uživatelů PayPal. Aplikace je napojena na testovacího prodejce a PayPal tlačítko směřuje na testovací adresu <https://www.sandbox.paypal.com/>, kde se nasimuluje pomocí testovacího nakupujícího uživatele celá transakce. PayPal potvrdí zaplacení za PDF dokument (na obrázku 7.3). Úspěch transakce je možné vidět na stránce prodejce (obrázek 7.5) i na stránce nakupujícího (obrázek 7.4). Na stránce prodejce je možné vidět připsání částky 1 GBP za prodej a na stránce nakupujícího naopak stržení částky 1 GBP za nákup.



Obrázek 7.3: Potvrzení nákupu na PayPal



Obrázek 7.4: PayPal stránka prodejce



Obrázek 7.5: PayPal stránka nakupujícího

Kapitola 8

Závěr

Zadání bakalářské práce bylo úspěšně zpracováno. Aplikace zvládá všechny úkony definované v zadání. Požadované analýzy byly podrobně vypracovány a sepsány. Na základě analýz byla aplikace doplněna o požadovanou funkčnost. Integrace s FELid je plně funkční. Možnost komerčního prodeje byla realizována pomocí PayPal Web Standard. Aplikace úspěšně přijímá PayPal IPN zprávy o úspěšnosti transakce. Do budoucna je potřebné napojit aplikaci na reálný PayPal účet, aby bylo možné PDF dokumenty skutečně prodávat. Další nutné vylepšení ve spojení s PayPal je upravení aplikace tak, aby byla schopná reagovat na neúspěšné transakce a o neúspěchu správně informovala uživatele.

Další vývoj aplikace by se měl zaměřit na vymyšlení správné kombinace vodoznaků na popředí i v pozadí dokumentu se zaměřením na čitelnost dokumentu. Aplikace by mohla obsahovat administrační rozhraní, ve kterém by bylo možné měnit konfigurační proměnné. Jako další možné vylepšení by mohla aplikace logovat všechny možné aktivity uživatelů spojené se získáváním PDF dokumentů. Například pokus o stažení dokumentu vyžadujícího přihlášení nebo zaplacení bez oprávnění ke stažení.

Zpracování této bakalářské práce nutilo k nastudování mnohých zajímavých technologií a postupů při její realizaci. Tyto nově nabyté zkušenosti jsou velmi cenné a je pravděpodobné jejich využití v praxi.

Literatura

- [1] *FELid — O systému FELid* [online]. [cit. 26.3.2012]. Dostupné z: <<http://wiki.feld.cvut.cz/net/felid/about>>.
- [2] *Prototyp aplikace na vkládání vodoznaků do PDF dokumentů* [online]. [cit. 17.5.2012]. Dostupné z: <<http://code.google.com/p/vykazovani-vyuky-cvut/>>.
- [3] *Ruby on Rails Guides: Getting Started with Rails* [online]. [cit. 19.5.2012]. Dostupné z: <http://guides.rubyonrails.org/getting_started.html#adding-a-second-model>.
- [4] *Ruby on Rails Guides: Migrations* [online]. [cit. 18.5.2012]. Dostupné z: <<http://guides.rubyonrails.org/migrations.html>>.
- [5] *Konfigurace service provideru* [online]. [cit. 18.5.2012]. Dostupné z: <<https://wiki.fel.cvut.cz/net/admin/aai/provoz/konfigurace/index>>.
- [6] Adobe Systems Incorporated. *Adobe Digital Publishing Solution for eBooks* [online]. [cit. 20.5.2012]. Dostupné z: <<http://www.adobe.com/digitalpublishing/ebook/>>.
- [7] Amazon.com, Inc. *Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs and more* [online]. [cit. 26.3.2012]. Dostupné z: <<http://www.amazon.com>>.
- [8] CtrlPublishing AB. *Buy Adobe Content Server license* [online]. [cit. 20.5.2012]. Dostupné z: <<http://www.ctrlpublishing.com/consultants/products/adobe-content-server/buy-adobe-content-server-license>>.
- [9] Dave Dickson: Adobe Digital Publishing. *Google adopts Adobe eBook DRM* [online]. [cit. 20.5.2012]. Dostupné z: <<http://blogs.adobe.com/digitalpublishing/2010/12/google-ebooks.html>>.
- [10] Google, Inc. *Google Books* [online]. [cit. 26.3.2012]. Dostupné z: <<http://books.google.com>>.
- [11] Google, Inc. *Google Play* [online]. [cit. 26.3.2012]. Dostupné z: <<https://play.google.com/about>>.
- [12] J. Arlow a I. Neustadt. *UML2 a unifikovaný proces vývoje aplikací*. nám 28. dubna 48, 635 00 Brno : Computer Press, 2nd edition, 2007.

- [13] PayPal. *About PayPal* [online]. [cit. 16. 5. 2012]. Dostupné z: <<https://www.paypal-media.com/about>>.
- [14] PayPal. *PayPal Express Checkout Integration Guide* [online]. 2012. [cit. 16. 5. 2012]. Dostupné z: <https://cms.paypal.com/cms_content/US/en_US/files/developer/PP_ExpressCheckout_IntegrationGuide.pdf>.
- [15] PayPal. *PayPal Instant Payment Notification Guide* [online]. 2012. [cit. 17. 5. 2012]. Dostupné z: <https://cms.paypal.com/cms_content/US/en_US/files/developer/IPNGuide.pdf>.
- [16] PayPal. *IPN and PDT Variables* [online]. 2012. [cit. 17. 5. 2012]. Dostupné z: <https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=developer/e_howto_html_IPNandPDTVariables>.
- [17] PayPal. *PayPayl Payments Standard Integration Guide* [online]. 2012. [cit. 16. 5. 2012]. Dostupné z: <https://cms.paypal.com/cms_content/US/en_US/files/developer/PP_WebsitePaymentsStandard_IntegrationGuide.pdf>.
- [18] Příspěvatelé Wikipedie. *3-D Secure* [online]. [cit. 17. 5. 2012]. Dostupné z: <http://en.wikipedia.org/wiki/3-D_Secure>.
- [19] Příspěvatelé Wikipedie. *Digital rights management* [online]. [cit. 20. 5. 2012]. Dostupné z: <http://en.wikipedia.org/wiki/Digital_rights_management>.
- [20] Příspěvatelé Wikipedie. *SQLite* [online]. [cit. 18. 5. 2012]. Dostupné z: <<http://cs.wikipedia.org/wiki/SQLite>>.
- [21] Příspěvatelé Wikipedie. *Watermark* [online]. [cit. 20. 5. 2012]. Dostupné z: <<http://en.wikipedia.org/wiki/Watermark>>.
- [22] Ryan Bates. *RailsCasts #142 PayPal Notifications* [online]. [cit. 19. 5. 2012]. Dostupné z: <<http://railscasts.com/episodes/142-paypal-notifications?view=asciicast>>.
- [23] S. Ruby, D. Thomas, D. Heinemeier Hansson. *Agile Web Development with Rails*. Pragmatic Bookshelf, 4th edition, 2011.
- [24] Československá obchodní banka, a.s. *ČSOB E-commerce* [online]. [cit. 17. 5. 2012]. Dostupné z: <<http://www.csob.cz/cz/firmy/podnikatele/platebni-karty/stranky/csob-e-commerce.aspx>>.
- [25] Československá obchodní banka, a.s. *Příručka pro použití Platební brány PaySec* [online]. 2011. [cit. 17. 5. 2012]. Dostupné z: <<http://www.paysec.cz/CmsPage.aspx?Id=gatewayManual>>.
- [26] Česká akademická federace identit eduID.cz. *Instalace Shibboleth SP 2 ze zdrojových kódů* [online]. [cit. 18. 5. 2012]. Dostupné z: <<http://www.eduid.cz/wiki/eduid/admins/howto/deploy/sp/install/source/index>>.
- [27] Česká spořitelna, a. s. *Akceptace platebních karet* [online]. [cit. 17. 5. 2012]. Dostupné z: <http://www.csas.cz/banka/content/inet/internet/cs/sc_1585.xml>.

Příloha A

Seznam zkratek

ČVUT	České vysoké učení technické
FEL	Fakulta elektrotechnická
PDF	Portable Document Format
DRM	Digital Rights Management
SDK	Software development kit
USD	United States dollar
EUR	Euro
GBP	Pound sterling
CZK	Czech koruna
HTML	HyperText Markup Language
API	Application programming interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
SSL	Secure Sockets Layer
XML	Extensible Markup Language
URL	Uniform resource locator
GNU	GNU's Not Unix!
RoR	Ruby on Rails
IPN	Instant Payment Notification
ČSOB	Československá obchodní banka
ČS	Česká spořitelna

Příloha B

Obsah příloženého CD

Zde se nachází obsah příloženého CD. Seznam souborů a adresářů. Včetně informací o tom, co v nich hledat.

- **Implementace/** - Zdrojové soubory aplikace, kompletní RoR aplikace.
- **Text/** - Tento dokument v PDF i se zdrojovým kódem systému L^AT_EX.
- **PayPal test account/** - Informace o testovacím účtu PayPal k testování aplikace.
- **Vodoznaky/** - Ukázky PDF dokumentů opatřených vodoznaky.
- **readme.txt** - Textový soubor s informacemi o disku.