**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Bakalářská práce**

# Zabezpečení PDF dokumentů

**Stanislav Doležal**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Doležal Stanislav

Informatika

Název práce

**Zabezpečení PDF dokumentů**

Anglický název

**PDF Documents Security**

---

**Cíle práce**

Bakalářská práce je tematicky zaměřená na problematiku PDF dokumentů, zejména na možnosti jejich zabezpečení. Hlavním cílem práce je vyhodnotit možnosti zabezpečení PDF dokumentů, dílčí cíle bakalářské práce jsou pak:

-charakterizovat PDF dokumenty

-analýza a testování možností zabezpečení PDF dokumentů

-zhodnocení výsledků testování, analýzy, poznatků a učinění závěrečného zhodnocení

**Metodika**

Metodika práce je založena na studiu dostupných odborných textů, dostupné odborné literatury a testování možností zabezpečení PDF dokumentů.

Na základě získaných teoretických a praktických poznatků budou formulovány závěry bakalářské práce.

**Harmonogram zpracování**

1)Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 6/2013

2)Zpracování přehledu problematiky dle informačních zdrojů: 7/2013 - 8/2013

3)Vypracování vlastního řešení, diskuze a zhodnocení výdledků: 9/2013 – 11/2013

4)Tvorba finálního dokumentu bakalářské práce: 11/2013 – 2/2014

5)Odevzdání bakalářské práce a teze: 3/2014

**Rozsah textové části**
30-50 stran

**Klíčová slova**
PDF, Portable document format, zabezpečení, heslo, certifikát, digitální podpis, začernění, šifrování

**Doporučené zdroje informací**
Adobe Creative Team. Adobe Acrobat 8 Oficiální výukový kurz: ComputerPress, 2008.
http://help.adobe.com/cs_CZ/acrobat/pro/using/index.htm
http://www.jaknapdf.cz/
http://www.digitalmedia.cz/produkty/adobe/acrobat/srovnani-verzi.aspx

**Vedoucí práce**
Brechlerová Dagmar, RNDr., Ph.D.

**Termín odevzdání**
březen 2014

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

**doc. Ing. Zdeněk Havlíček, CSc.**
Vedoucí katedry

**prof. Ing. Jan Hron, DrSc., dr. h. c.**
Děkan fakulty

V Praze dne 30.10.2013

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zabezpečení PDF dokumentů" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 12.3.2014 _____

Poděkování

Rád bych touto cestou poděkoval RNDr. Dagmar Brechlerové, Ph.D. za ochotu, cenné rady a konzultace při vedení bakalářské práce.

# Zabezpečení PDF dokumentů

---

## Security PDF documents


**Souhrn**

Bakalářská práce se zabývá problematikou zabezpečení PDF dokumentů. Cílem práce je zmapovat volně dostupné možnosti tohoto zabezpečení, poskytnout návod na jejich aplikaci, následně otestovat spolehlivost a doporučit jejich praktické využití.

V teoretické části se práce zaměřuje na komplexní představení PDF formátů. Práce se věnuje bezpečnosti obsahu souborů PDF, nezabývá se možností napadení souborů PDF škodlivým softwarem.

**Summary**

The Bachelor´s thesis deals with the issue of PDF documents security. An aim of the thesis is to chart freely available possibilities of the security, to offer directions for their application and as follows to test their reliability and to recommend their practical use.

In the theoretical part the thesis aims at comprehensive introduction of PDF formats. The bachelor´s thesis also deals with the safety contents of PDF files. It does not deal with the possibility of a noxious software attack of PDF files.



**Klíčová slova:** PDF, zabezpečení, heslo, certifikát, šifrování, začernění

**Keywords**: PDF, security, password, certificate, encryption, black out

# Obsah

## Seznam obrázků



## Seznam Tabulek

# 1 Úvod

Formát PDF se v průběhu vývoje postupně stal jedním z nejvyužívanějších formátů pro práci a pro přenos elektronických dokumentů a jeho obliba stále roste. K oblibě tohoto formátu přispívá jeho všestrannost, široké spektru využití v různých oborech, otevřenost formátu plynoucí z jeho standardizace a samozřejmě také možnosti zabezpečení.

Nutnost zabezpečení komunikace mezi subjekty je známa již od samého vývoje lidstva. Před nástupem moderní technologie byly využívány různé metody pro skrytí komunikace nebo jejího obsahu. Dnešní doba moderních technologií vyžaduje vysokou míru zabezpečení komunikace mezi subjekty a fakt, že velká část předání informací funguje na principu digitálního přenosu dat, je důkazem nutnosti zabezpečení těchto přenosů, na které je kladem velký důraz. Formát PDF se snaží nabídnout uživatelům několik druhů zabezpečení sloužící pro různé účely.

Cílem teoretické části práce je poskytnout čtenáři informace o vývoji, fungování a metodách zabezpečení PDF formátů. Praktická část je zaměřena na konfiguraci a testování volně dostupných metod zabezpečení.

# 2 Cíl práce a metodika

Bakalářská práce je tematicky zaměřená na problematiku PDF dokumentů, zejména na možnosti jejich zabezpečení. Hlavním cílem práce je prozkoumat a vyhodnotit volně dostupné možnosti zabezpečení PDF dokumentů. Charakterizování PDF dokumentů, analýza a testování možnosti zabezpečení a následné závěrečné zhodnocení jsou dílčí cíle této práce.

Bakalářská práce má dvě části – teoretickou a praktickou. Teoretická část se zaměřuje na historii PDF dokumentů, vysvětlení jejich funkčnosti, struktury a volně dostupných možností zabezpečení.

V praktické části jsou tyto možnosti prozkoumány, testovány a s ohledem na znalosti nabyté v teoretické části testovány.

# 3 O PDF

## 3.1 Co je PDF

Adobe Portable Document Format, zkráceně PDF, je univerzální formát souborů, který zachovává písma, formátování, barvy a grafické prvky zdrojového dokumentu bez ohledu na aplikaci nebo platformu, na které byl tento dokument vytvořen. Soubory Adobe PDF jsou kompaktní a bezpečné. Může je sdílet, prohlížet a tisknout kdokoli, kdo má nainstalovaný volně dostupný program Adobe Reader. Uživatelé programu Adobe Acrobat mohou dalším uživatelům přidělit různá oprávnění. Ti pak mohou dokument upravovat nebo komentovat, mohou ho digitálně podepsat, vyplňovat a ukládat formuláře PDF nebo dopisovat text na libovolné místo stránky. V dokumentu PDF může uživatel na jedné stránce použít vice jazyků, například češtinu a japonštinu. Tištěné dokumenty PDF mají vždy odpovídající okraje a stránkování. Soubory PDF lze zabezpečit proti nežádoucím změnám nebo tisku, případně je možné omezit přístup k tajným informacím v nich obsažených [1].

Formát PDF je v dnešní době definován jako otevřený standard, který je spravován Mezinárodní organizací pro normalizaci (ISO) se sídlem ve městě, ležícím na jihozápadním cípu Švýcarska, na hranici s Francií, Ženevě. Standardizací je zaručena integrita a dlouhodobá životnost těchto souborů [2].

## 3.2 Historie PDF

PDF začínal jako interní projekt ve společnosti Adobe. Společnost chtěla vytvořit neutrální platformu pro výměnu dokumentů. PostScrip, který byl také vytvořen společností Adobe roku 1985, byl už populární v tiskové komunitě, ale nebylo prakticky možné ho použít pro zobrazení na obrazovce počítače, zejména pro náhodný přístup ke stránce. K tomu, aby se v PostScriptu zobrazila strana 50, musely se nejdříve zpracovat strany 1-49. Hlavní myšlenkou bylo použít podmnožinu grafického jazyka PostScript spolu s doplňkovými údaji a vytvořit strukturovaný jazyk pro samostatné dokumenty, které mají být zobrazeny na jakémkoli počítači nebo z něj tištěny. PDF 1.0 bylo ohlášeno v roce 1993 spolu s programem Acrobat Distiller, který sloužil pro vytváření a úpravu PDF souborů a programem Adobe Reader. Ten sloužil pouze k prohlížení PDF souborů. Skupina těchto programů byla vydána pouze jako placené programy.

Americké daňové úřady začaly dodávat daňová přiznání ve formátu PDF, včetně licence, aby umožnily svým uživatelům si stáhnout Acrobat Reader zdarma. Později byl Acrobat Reader k dispozici všem bez nákladů, což vedlo k masivnímu rozšíření tohoto formátu a jeho využívání k výměně dokumentů online. V následujících 10 letech po pomalém startu byly přidány předtiskové funkce a formát PDF předstihl PostScript jako jazyk volby v polygrafickém průmyslu. Dnes je PostScript jen obecný jazyk pro popis stránky poznámky [3].

Důležitým dnem pro PDF bylo datum 1. července roku 2008. Toho dne byl formát vydán jako otevřený standard ISO 32000-1 Mezinárodní organizací pro normalizaci, což vedlo k dalšímu rozšíření tohoto formátu. Podvýbor ISO, odpovědný za údržbu a rozvoj tohoto formátu se zavázal k tomu, že budoucí verze formátu budou zveřejněny jako další část této normy. V současnosti má norma podobu standard ISO 32000-1:2008 [4]. Dalo by se říct, že PDF je v tuto chvíli standardem pro přenos elektronických dokumentů nezávislým na platformě.

### 3.2.1 Verze PDF

Minulý rok slavila firma Adobe dvacáté výročí existence formátu PDF, který je jejím mateřským produktem. Formát je po tuto dobu rozšiřován o další funkcionality a postupně upravován. PDF soubory jsou zpětně kompatibilní, což se ovšem nedá říci o dopředné kompatibilitě. Ta nemůže být garantována z důvodu chybějících implementací nových funkcionalit. V tabulce 2.1 je možno vidět vývoj verzí formátu PDF s kompatibilními verzemi Adobe Acrobat. Jednoduchá pomůcka pro zjištění verze Adobe Acrobat je sečtení prvních dvou čísel verze PDF viz tabulka 2.1.

**Tabulka 3.1 - Přehled verzí PDF**

| PDF verze | Verze Acrobat | Rok uvedení | Přehled nových funkcí |
|---|---|---|---|
| 1.0 | 1.0 | 1993 | První vydání |
| 1.1 | 2.0 | 1996 | Barevné prostory nezávislé na zařízení, šifrování (40 – bitů), pojmenované cíle, hypertextové odkazy, článek vlákna |
| 1.2 | 3.0 | 1996 | Prvky AcroForm (interaktivních formulářů), filmy a zvuky, další metody komprese, podpora UniCode |
| 1.3 | 4.0 | 2000 | Další barevné prostory, přidané (v příloze) soubory, digitální podpisy, anotace, maskované obrazy, přechodové výplně, logická struktura dokumentu, předtisková podpora |
| 1.4 | 5.0 | 2001 | Průhlednost, šifrování 128 bity, lepší forma podpory, metadata XML, označení PDF, komprese JBIG2 |
| 1.5 | 6.0 | 2003 | JPEG 2000, XFA, šifrování pomocí veřejného klíče, vlastní metody šifrování, volitelný obsah skupin |
| 1.6 | 7.0 | 2004 | Fonty OpenType, 3D obsah, šifrování AES, nové barevné prostory |
| 1.7 (později základ ISO normy) | 8.0 | 2006 | XFA 2.4, rozšíření architektury veřejného klíče, nové typy objektů |
| 1.7 rozšíření1 | 9.0 | 2008 | Šifrování AES 256 bity |
| 1.7 rozšíření2 | 9.1 | 2009 | XFA 3.0 |
| 1.7 rozšíření3 | X | 2011 | Zlepšení šifrování, zlepšení digitálních podpisů PAdES, Zdokonalení formulářů XFA |
| 1.7 rozšíření4 | XI | 2012 | Žádné klíčové změny |

Zdroj: [3]

### 3.2.2 Využití a standardy PDF

Standard PDF v různých modifikacích pronikl do všech možných specifických odvětví. Několik z nich bylo již vydáno jako platná podmnožina formátu PDF Mezinárodní organizací pro normalizaci a staly se z nich ISO standardy, jiné jsou zatím stále ve vývoji. Na první pohled se tyto soubory nemusí od běžných lišit, většinou ani neliší, jsou na ně však aplikovány jiné nároky z pohledu funkcionality nebo z pohledu obsahu.

**Tabulka 3.2 - Standardy PDF z ISO**

| **Specifikace PDF** | **Účel** | **Popis** |
|---|---|---|
| PDF<br>ISO 32000 | Standardní PDF | Tato norma je základem pro všechny budoucí generace standardů PDF |
| PDF / A<br>ISO 19005 | Archivace | Poskytuje specifikace pro vytvoření, zobrazení a tisk digitálních dokumentů používaných pro dlouhodobé uchování. Neumožňuje odkazy na externí obsah |
| PDF / E<br>ISO 24517 | Inženýrství | Poskytuje specifikace pro vytvoření, zobrazení a tisk digitálních dokumentů používaných v technických (inženýrských) pracovních postupech. Vhodné pro stavby, výrobu a geoprostorové procesy. Podporuje interaktivní média, včetně animací a 3D zobrazení |

| | | |
|---|---|---|
| PDF / X<br>ISO 15930 | Tisková produkce | Poskytuje specifikace pro vytvoření, zobrazení a tisk finálních tiskových stran. Obsahuje pokyny, které ovlivňují zásadní aspekty tisku, například barevný prostor. |
| PDF / UA<br>ISO 14289 | Univerzální přístup | Poskytuje sadu pokynů pro vytváření souborů PDF, které jsou všeobecně přístupné. Pomáhají zlepšit čitelnost dokumentů pro osoby se zdravotním postižením, jako je například zrakové postižení nebo snížená pohyblivost |
| PDF / VT<br>ISO 16612-2 | Variabilní a transakční tisk | Poskytuje specifikace pro vytvoření, zobrazení a tisk variabilních tiskových souborů. Jsou jimi například bankovní výpisy nebo obchodní faktury |

Zdroj: [5]

Výše uvedená tabulka dokazuje implementaci technologie PDF ve veliké škále odvětví. Hlavním odvětvím je tisková produkce, kde se formát stal důležitou součástí pracovního i výrobního procesu. V archivaci se klade velký důraz na dostupnost dokumentů v řádu desítek let i delšího období. Z tohoto důvodu je velké omezení funkcí dostupné v jiných typech dokumentů, například JavaScriptu [6]. PDF proniklo také do distribuce elektronických knih a je jedním z využívaných formátů distributorům elektronických knih. Vhodný je i pro tvorbu interaktivních formulářů, korekturu textů a ke komentování jednotlivých souborů.

Ochrana dat a bezpečnost obchodních transakcí je v moderním světě velmi důležitou součástí. To dovedlo některé organizace k vytvoření vlastních PDF standardů, jak ukazuje tabulka 2.3.

**Tabulka 3.3 - Standardy PDF jiných organizací**

| Specifikace PDF | Účel | Popis |
|---|---|---|
| PAdES | Digitální podpisy v Evropské unii | Poskytuje standard umožňující bezpečnější bezpapírové obchodní transakce v celé Evropě, v souladu s evropskou legislativou. |
| PDF Healthcare | Zdravotnictví | Poskytují postupy a pokyny pro zachycení, výměnu, uchovávání a ochranu zdravotnických informací. |

Zdroj: [5]

## 3.3 Programové vybavení

Čtení, vytváření, konverze. Tato tři klíčová slova v dnešní době zná každý, kdo se kdy setkal s PDF dokumenty. Charakterizují také hlavní kategorie programového vybavení pro práci s PFD dokumenty – software pro čtení PDF, software pro vytváření (editaci) PDF a software pro konverzi souborů jiných formátů, než je PDF, právě do něj. Kategorie pro pokročilou práci se soubory PDF a centralizovanou správu se nazývá serverová řešení. Ve chvíli, kdy byla technologie uvedena na veřejnost jako otevřený standard, začalo vznikat velké množství řešení ve všech kategoriích výše uvedených.

Originálním softwarem se dá tedy nazvat produkt vyrobený společností Adobe, která vytvořila formát PDF. OD roku 2006 již společnost Adobe není vlastníkem tohoto otevřeného standardu. I přes tuto skutečnost firma velice neochotně poskytovala komplexní informace o technologii. Další problém vznikl v nekompletnosti specifikace standardu ISO 32000:1-2008, Adobe totiž neposkytla testovací sadu souborů užitých k testování programu Adobe Reader.

Tudíž vývojáři třetích stran vyvíjejí software, který vytváří soubory PDF rozdílně, chybně nebo software, jenž nedokáže korektně soubory zobrazit. Tyto informace moc nekorespondují s prvotní myšlenkou tohoto standardu, jímž měla být přenositelnost a otevřenost [7].

„Správná“ a kompletní technologie PDF je implementována pouze v produktech Adobe. Z toho důvodu se dále bude tato práce zaobírat pouze jimi.

**Tabulka 3.4 - Přehled produktů PDF Adobe**

| **Kategorie** | **Produkty Adobe** | **Podporující platformy** |
|---|---|---|
| Čtení PDF | Adobe Reader | Windows, Mas OS, Linux, Solaris |
| Vytváření a editace PDF | Adobe Acrobat Standard | Windows, Mas OS |
| | Adobe Acrobat Pro | |
| | Adobe Acrobat Suite | |
| Konverze souborů do PDF | Adobe Distiller (nyní součást Adobe Reader) | Windows, Mas OS |
| Serverová řešení | Adobe LiveCycle Enterprise Suite | AIX, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Solaris, Windows Server |

Zdroj: Autor BP

Integrace a zásuvné moduly do dalších aplikací jsou v této době pro tyto programy již samozřejmostí. Příkladem je integrace programu do různých kancelářských balíků nebo webových prohlížečů. Mobilní verze aplikací nejsou v tabulce uvedeny z důvodu omezené funkcionality.

## 3.4 Struktura PDF dokumentu

Soubor PDF je složen ze čtyř základních komponent, které po sobě následují přesně v tomto pořadí – hlavička (Header), tělo (Body), tabulka odkazů (Xref Table) a přívěs (Trailer) viz obrázek 2.1.

**Obrázek 3.1 - Základní struktura PDF dokumentu**


Zdroj: [8]

Hlavička souboru obsahuje informaci, která určuje verzi PDF a také znak, jenž zaručí čtení souboru jako binárního, nikoli textového. Soubory PDF jsou zpětně kompatibilní, což umožnuje čtení souboru například PDF 1.3 ve verzi programu PDF 1.5. Tělo se skládá z posloupnosti veškerých objektů nesoucí obsah dokumentu, jimiž mohou být fonty, obrázky, texty, záložky, pole formulářů a další. Tabulka odkazů obsahuje ukazatele na každý objekt v dokumentu, na jeho datový začátek a délku v bajtech, což zjednodušuje přístup k objektům. To umožňuje náhodný přístup k objektům. Objekty, které se nikdy nepoužívají, se nikdy nebudou číst, což v praxi znamená, že jednoduchá operace, jakou je počítání počtu stránek v dokumentu PDF, může být rychlá i ve velkých dokumentech. Přívěs má na první řádce jen slovo trailer. Další řádky obsahují odkazy na tabulku odkazů, klíčové odkazy obsažené ve slovníku přívěsu, další důležitá metadata . Na poslední řádce je znak konce souboru PD, jenž má vždy tvar %% EOF (end od file) [3].

### 3.4.1 Objekty

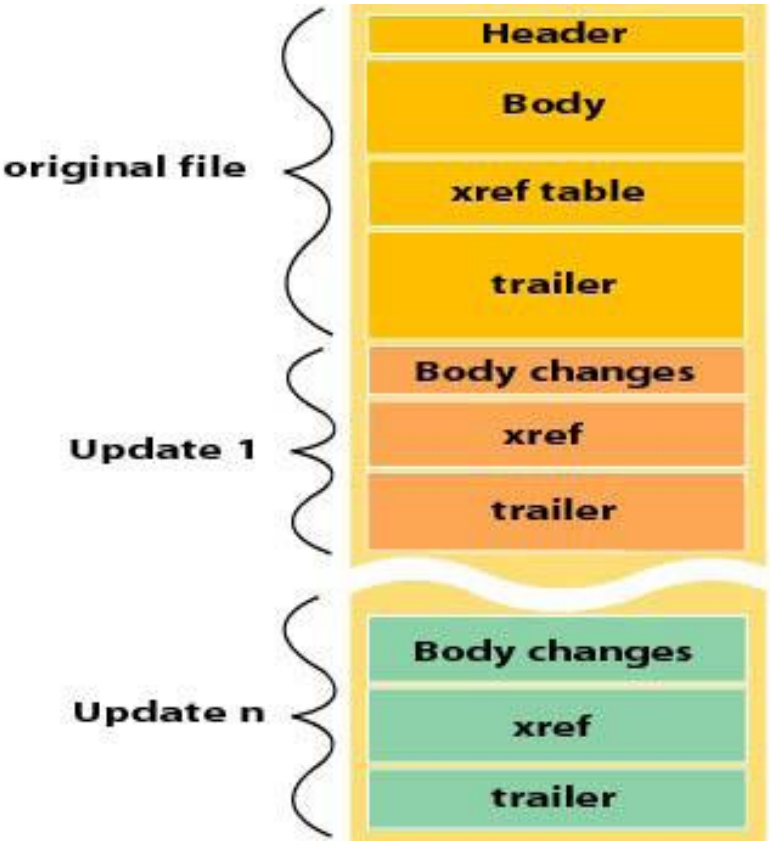
PDF může obsahovat základní a složené objekty uložené v komponentě tělo. Základních objektů je pět, jsou jimi celá a reálná čísla, různě kódované řetězce, jména používající se pro klíče ve slovnících, hodnota boolean reprezentována slovy true (pravda) a false (nepravda) a objekt null, jehož klíčové slovo je NULL. Složené objekty jsou tři.

Pole obsahující uspořádanou kolekci jiných objektů, slovníky mapující jména objektů a stream obsahující binární data, tudíž může obsahovat prakticky libovolnou informaci Stream je například využíván pro obrázky, písmo nebo vložené přílohy do PDF dokumentu. Ty se mohou vkládat v libovolném formátu.
Obsahuje i způsob propojení objektů nepřímým odkazem, jenž vytváří spojení z jednoho objektu do druhého. Objekt řetězec může obsahovat například text dokumentu a je jedním z objektů, ve kterém bývá uložen vlastní obsah dokumentu, většina dalších obsahových prvků je uložena právě v objektu typu stream. Ostatní zbylé typy objektů jsou ve většině případů využívány pro popis struktury dokumentu [3].

### 3.4.2 Ukládání a update

Jedna z výhod PDF dokumentu plynoucí z jeho struktury je inkrementální ukládání dat. Inkrementální aktualizace umožňuje připojit změněné objekty a přívěs na konec souboru a aktualizovat tabulky odkazů, takže není zapotřebí celý soubor znovu ukládat, což by v případě větších souborů mohlo trvat delší dobu. Stane se tak v případě, je-li soubor modifikován a uložen příkazem „Uložit". Pouze se připojí k původní struktuře dokumentu nové komponenty tělo, tabulka odkazů a přívěs, viz obrázek 2.2. Komponenty nesou jen informace o změnách oproti původnímu souboru. Dá se tak sledovat verze souboru, ale znamená to, že s každou touto změnou se velikost souboru zvětšuje i přes vymazání některých částí dokumentů. Po deseti uloženích příkazem „Uložit" je uživatel vyzván k uložení dokumentu příkazem „Uložit jako", aby došlo ke zmenšení souboru. Jestliže tak uživatel učiní, skutečně se velikost souborů zmenší. Veškeré úpravy se sjednotí do základní struktury a není možné vrátit se k předchozím verzím dokumentu. Pozornosti při ukládání souborů je třeba věnovat určitě v případě, že se jedná o digitálně podepsaný dokument. Užitím možnosti „Uložit jako" se podpisy aplikují do původní verze dokumentu a stávají se pak neplatnými. Není totiž možné dohledat data podepsání a uživatele, který dokument podepsal [8].

**Obrázek 3.2 - Struktura PDF souboru a inkrementální změny**




Zdroj: [8]

# 4 Zabezpečení dokumentu

Obliba a rozšířenost formátu PDF ve velké škále odvětví nevyhnutelně vedla ke zvyšujícím se nárokům na zabezpečení těchto dokumentů. Pro organizace používající tento formát je ochrana klíčovým prvkem. Únik důvěrných informací, smluv, kontaktů, strategických plánů podniku a dalších dokumentů by mnohdy mohlo vést i ke krachu mnoha společností používajících tento formát. Kritéria definující trvalé zabezpečení dokumentu jsou tato:

- Důvěrnost – Kdo by měl mít přístup k dokumentům?
- Autorizace – Jaká oprávnění má mít uživatel pro práci s dokumentem?
- Odpovědnost – Co může příjemce s dokumentem udělat?
- Integrita – Jak víte, že byl dokument změněn?
- Autenticita – Jak víte, odkud dokument přišel?
- Nepopíratelnost – Může signatář odepřít podepsání dokumentu?

Obrázek 3.1 naznačuje těchto šest klíčových kritérií pro poskytnutí trvalého zabezpečení dokumentu [9].

**Obrázek 4.1 - Šest klíčových kritérií pro poskytnutí trvalého zabezpečení dokumentu**


Zdroj: [10]

Zabezpečení se vztahuje na dvě hlavní oblasti: na aplikaci (software) a na obsah. Zabezpečení aplikace znamená přizpůsobení funkcí, aby chránila zranitelná místa, bránila útokům a dalším rizikům. Zabezpečení obsahu zahrnuje používání funkcí produktu Adobe Acrobat k ochraně integrity obsahu PDF. Tyto funkce slouží k zabezpečení před nežádoucími úpravami dokumentu, k ochraně citlivých osobních informací, k zabránění tisku PDF dokumentů, atd [11].

Existují tři hlavní metody zabezpečení PDF dokumentů: zabezpečení pomocí hesla, certifikátu nebo služby Adobe LiveCycle Policy Server.

Zabezpečení heslem poskytuje jednoduchý způsob, jak sdílet dokumenty mezi uživateli, kde sdílení hesla je možné, nebo je-li požadována vysoká úroveň zpětné kompatibility. Zásady zabezpečení heslem nevyžadují určení všech příjemců dokumentu.
Zabezpečení certifikátem poskytuje vysokou úroveň bezpečnosti, eliminuje potřebu sdílení hesel a umožňuje přiřadit různá oprávnění různým uživatelům, jejichž identity lze ověřit a spravovat. Plnou kontrolu, trasování historie nebo řídit přístupová či omezující práva dokumentu umožňuje služba Adobe LiveCycle Policy Server [12]. Vývoj, implementaci a kompatibilitu šifrovacích algoritmů v jednotlivých verzích PDF naznačuje tabulka 3.1.

**Tabulka 4.1 – Používané šifrovací algoritmy a jejich kompatibilita**

| **Verze Acrobat** | **Zabezpečení heslem** | **Zabezpečení certifikátem** | **Zabezpečení službou LiveCycle** |
|---|---|---|---|
| 1.0 | - | - | - |
| 2.0 | 40bit RC4 | - | - |
| 3.0 | 40bit RC4 | - | - |
| 4.0 | 40bit RC4 | - | - |
| 5.0 | 40bit RC4 & 128bit RC4 | 40bit RC4 & 128bit RC4 | - |
| 6.0 | 40bit RC4 & 128bit RC4 | 40bit RC4 & 128bit RC4 | - |
| 7.0 | 128bit RC4 & AES | 128bit RC4 & AES | 128bit RC4 & AES |
| 8.0 | 128bit RC4 & AES | 128bit RC4 & AES | 128bit RC4 & AES |
| 9.0 | 256bit AES | 256bit AES | 256bit AES |
| X | 256bit AES | 256bit AES | 256bit AES |
| XI | 256bit AES | 256bit AES | 256bit AES |

Zdroj: [12]

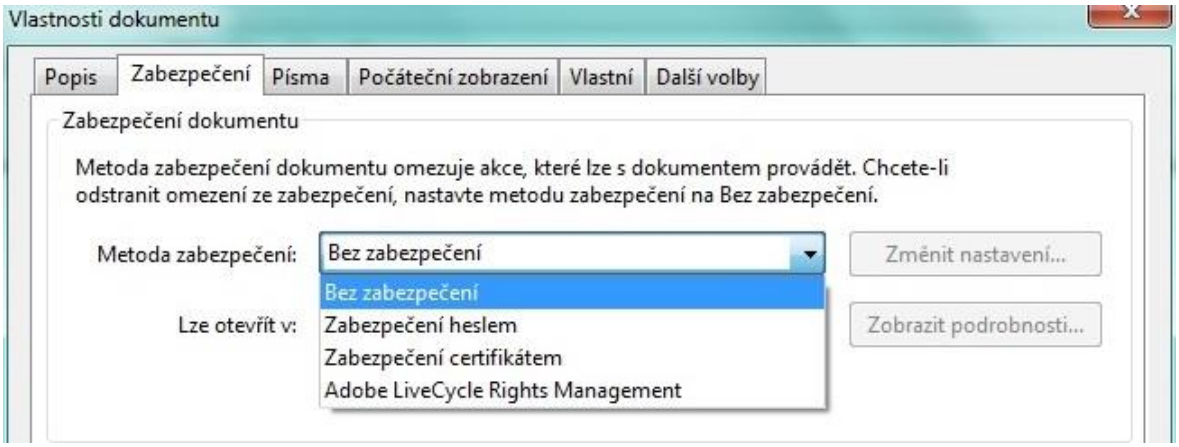
Soubory Adobe PDF je možné zabezpečit už při prvním vytvoření nebo kdykoli později. Je možnost dokonce zabezpečit i soubory, které dostane uživatel od někoho jiného, pokud ovšem autor dokumentu nezakázal změny zabezpečení dokumentu [1].

Máme-li vytvořen dokument PDF, lze jej zabezpečit pomocí softwaru z kategorie vytváření a editace PDF programem Adobe Acrobat, který ovšem není zdarma. Vyzkoušet si ho může uživatel po dobu 30 dní zdarma.

Otevřít zabezpečený soubor lze však i v programu Adobe Reader, který je zdarma. Neumožňuje však zabezpečit vytvořený dokument, je určen pouze pro čtení zabezpečených i nezabezpečených souborů.

Zvolit si metodu zabezpečení v programu Adobe Acrobat je možno na pozici „Soubor / Vlastnosti“, funkční je i klávesová zkratka Ctrl+D, v druhé záložce „Zabezpečení“. Výřez okna s možnosti výběru metod je zachycen obrázkem 3.2.

**Obrázek 4.2 - Záložka zabezpečení s možností výběru metody zabezpečení**




Zdroj: Autor BP

Všechny výše uvedené metody zabezpečení jsou zde v rozbalovacím menu s názvem Metoda zabezpečení k dispozici, včetně metody bez zabezpečení.

## 4.1 Zabezpečení heslem

Zabezpečení heslem poskytuje jednoduchý způsob pro sdílení šifrovaných dokumentů. Uživatelsky je nastavení toho typu zabezpečení velmi jednoduché a používá se v případě, pokud příjemci dokumentu nemají své digitální identifikátory [13]. Jako u všech metod zabezpečení, také zabezpečení heslem může omezit dokument u operací, jako je otevření, tisk a editace dokumentu. Vzhledem k tomu, že zabezpečení heslem neposkytuje různá oprávnění pro různé uživatele, každý, kdo dokument otevře, bude mít stejná oprávnění [12].

Bezpečnost šifrování obsahu PDF dokumentů není přímo závislá na heslu zadaném uživatelem. Šifrovací klíč je vypočítáván ze zadaného hesla a dalších parametrů včetně konkrétního nastavení oprávnění.

Délka šifrovacího klíče, použitého pro skutečné šifrování dokumentu, je nezávislá na délce zadaného hesla a je odvozena z délky použitého šifrovacího klíče.

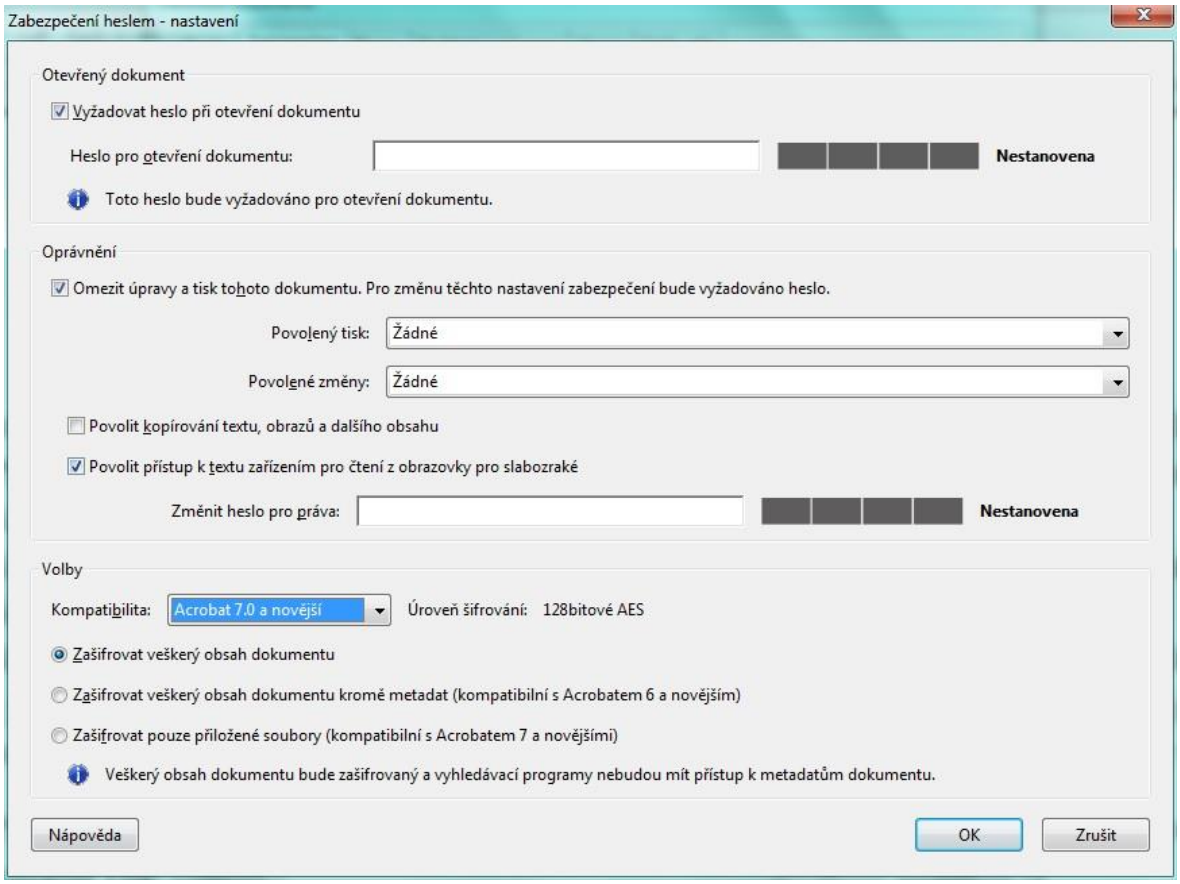
Šifrování PDF interně pracuje s šifrovacími klíči v délce 40, 128 nebo 256 bitů jak naznačuje tabulka 3.1 v závislosti na verzi PDF. Jedná se o symetrické šifrování.

Je všeobecně známo, že jména, přezdívky, data narození, jména dětí a podobně by neměla být použita jako hesla, protože mohou být snadno uhodnuty nebo systematicky prolamovány. Průzkumy ukázaly, že značný počet hesel je právě jméno uživatele, manžela, domácího mazlíčka, dětí, přezdívka z dětství nebo jednoduché číselné kombinace [14].

### 4.1.1 Nastavení metody zabezpečení heslem

Metodu zabezpečení heslem je možno nastavit v okně „Soubor / Vlastnosti / Zabezpečení / Zabezpečení heslem“. Možnosti nastavení této metody jsou zobrazeny na obrázku 3.3.

**Obrázek 4.3 - Možnosti nastavení zabezpečení metodou zabezpečení heslem**




Zdroj: Autor BP

V okně, které ukazuje obrázek 3.3, jsou dostupné následující možnosti:

**Otevřený dokument**

- Vyžadovat heslo při otevření dokumentu – slouží k nastavení hesla pro otevírání dokumentu. Volba není dostupná při vybrání volby Zašifrovat pouze přiložené soubory
    - Heslo pro otevření dokumentu – místo pro vepsání konkrétního hesla, které musí uživatel zadat pro otevření dokumentu

**Oprávnění**

- Omezit úpravy a tisk tohoto dokumentu – omezí přístup k nastavení zabezpečení souboru PDF
    - Povolený tisk – Určuje úroveň tisku povolenou uživatelům pro dokument PDF. Možnosti jsou: žádné, nízké rozlišení (150 dpi), vysoké rozlišení
    - Povolené změny – Určuje, které úpravy jsou v dokumentu PDF povolené. Žádné, což zabrání uživatelům provádět jakékoli dále zmíněné změny. Vložení, odstranění a natočení stránek. Vyplnění polí formulářů a podepsání existujících polí podpisu. Přidávání poznámek, vyplnění polí formulářů a podepsání existujících polí podpisu. Vše kromě vyjmutí stránek
    - Povolit kopírování textu, obrazů a dalšího obsahu – nevybráním této volby nemůže uživatel žádným způsobem kopírovat jakýkoliv obsah
    - Povolit přístup k textu zařízením pro čtení z obrazovky pro slabozraké – umožňuje uživatelům použít hlasová zařízení. Tato volba je dostupná pouze u vysoké úrovně šifrování (128bitové RC4 nebo AES) a nesmí být povoleno kopírování textu, obrazů a dalšího obsahu
    - Změnit heslo pro správu – místo pro vepsání konkrétního hesla

**Volby**

- Kompatibilita – Umožňuje vybrat z několika verzí Adobe Acrobat (Reader), které budou moci dokument otevřít nebo s ním pracovat. Přímo určuje použitý šifrovací algoritmus
    - Úroveň šifrování – algoritmus šifrování měnící se s volbou kompatibility
- Zašifrovat veškerý obsah dokumentu – zašifruje veškerý obsah dokumentu i metadata.

- Zašifrovat veškerý obsah dokumentu kromě metadat – metadata zůstanou nezašifrována, vše ostatní je zašifrováno
- Zašifrovat pouze přiložené soubory – umožňuje plný přístup k dokumentu, heslo je vyžadováno pouze při manipulaci s přiloženými soubory. Obsah dokumentu není šifrovaný [15]
-

Adobe umožňuje v dokumentech formátu PDF nastavovat dva typy hesel – heslo pro omezení otevření dokumentu nazýváno heslem uživatele a heslo vlastník sloužící pro omezení funkcionalit dokumentu. Uživatel je oprávněn nastavit tato hesla samostatně nebo společně viz obrázek 3.3. Z bezpečnostního důvodu není možná identita těchto hesel. Zadáním jakéhokoli typu hesla a uživatel soubor uloží, dojde k automatickému připojení informace o zvoleném druhu zabezpečení do přívěsu souboru a vytvoří se odkaz na objekt v těle souboru, jenž obsahuje konfiguraci zvoleného typu zabezpečení [16].

Pokud je nastaveno uživatelské heslo, pokusí se software z kategorie vytváření a editace PDF tento soubor otevřít. Před dešifrováním a otevřením souboru program vyzve uživatele k zadání hesla, které je v tomto případě nutné nastavit, je z něj totiž odvozen šifrovací klíč. Není možno nechat toho políčko prázdné. Uživatel se znalostí hesla může po jeho zadání a otevření souboru zrušit toto zabezpečení a soubor uložit nechráněný.

Naopak otevření a dešifrování souboru, při zvolení volby zabezpečení heslem typu vlastník, se provede okamžitě a není vyžadováno heslo pro otevření dokumentu. Uživatel okamžitě dokáže soubor otevřít a možnosti práce s dokumentem jsou již řízeny konfigurací, kterou zvolil vlastník souboru. Při znalosti hesla typu vlastník je uživatel oprávněn konfiguraci změnit nebo zrušit, bez znalosti hesla nikoli. Není možnost zakázat kopírování souboru, uživatel může soubor kdykoli vytvořit kopii tohoto souboru s jiným názvem, ale soubor se uloží se stejnou konfigurací jako výchozí soubor.

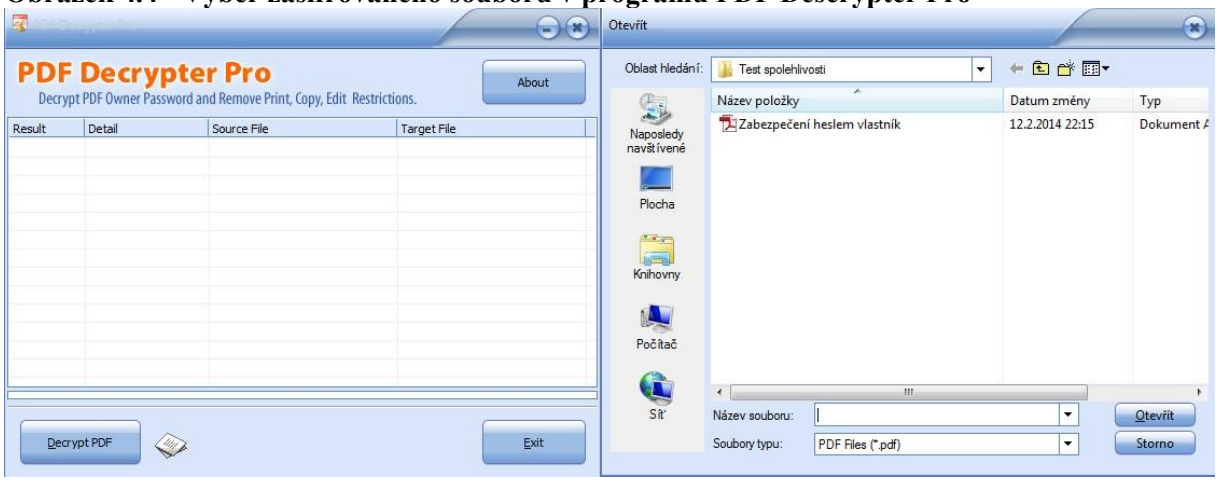
Kombinace obou typů zabezpečení heslem je možná. Při pokusu uživatele o otevření souboru je uživatel vyzván k zadání hesla. V tomto případě má na výběr z hesla typu uživatel nebo vlastník. Při zadání hesla typu uživatel se soubor otevře a funkcionalita některých prvků je řízena konfigurací, která je nastavena od vlastníka souboru. Dá se následně odstranit je po zadání typu hesla vlastník. Zadá-li však uživatel typ hesla vlastník, soubor se otevře a jeho obsah není nijak omezen.

### 4.1.2 Spolehlivost hesla vlastník

Jak již bylo výše zmíněno, k otevření dokumentu zabezpečeného heslem typu vlastník, není potřeba znát toto heslo. Dokument je tedy po použití softwaru určenému k editaci nebo čtení PDF dokumentu dešifrován, následně otevřen a uživatel může vidět obsah. Omezení a funkcionalita dokumentu jsou řízeny samotným softwarem z kategorie pro čtení nebo vytváření a editaci PDF dokumentů. Informace o šifrování jsou v dokumentu uloženy v šifrovacím slovníku, který je jednotkou v položce Encrypt v přívěsu slovníku dokumentu. Jelikož je formát PDF otevřeným standardem a nejen společnost Adobe vytváří programy, které umí číst soubory typu PDF, mohou různé programy od různých autorů přistupovat ke čtení dokumentu a implementaci funkcí zabezpečení rozdílnou cestou [16].

Odlišnosti implementace využívá například použitá aplikace, sloužící k odstranění omezení funkcionalit dokumentu a hesla typu vlastník, na které byla testována spolehlivost použití hesla typu vlastník PDF Descrypter Pro [17]. Po nainstalování a otevření aplikace je nutné vybrat soubor zabezpečený heslem vlastník, který chceme dešifrovat. Aplikace umožňuje soubor vybrat tlačítkem „Descrypt PDF“ viz obrázek 3.4 nebo ho jednoduše přetáhnout do programu. Po provedení této operace je soubor bez potvrzování v řádu jednotek sekund dešifrován, zbaven všem omezení a znovu uložen pod jiným názvem. Velká rychlost dešifrování souboru u všech aplikací naprogramovaných k tomuto účelu je způsobena tím, že stačí pouze okomentovat část přívěsu, ve které je uložena informace o zašifrování souboru.

**Obrázek 4.4 - Výběr zašifrovaného souboru v programu PDF Descrypter Pro**




Zdroj: Autor BP

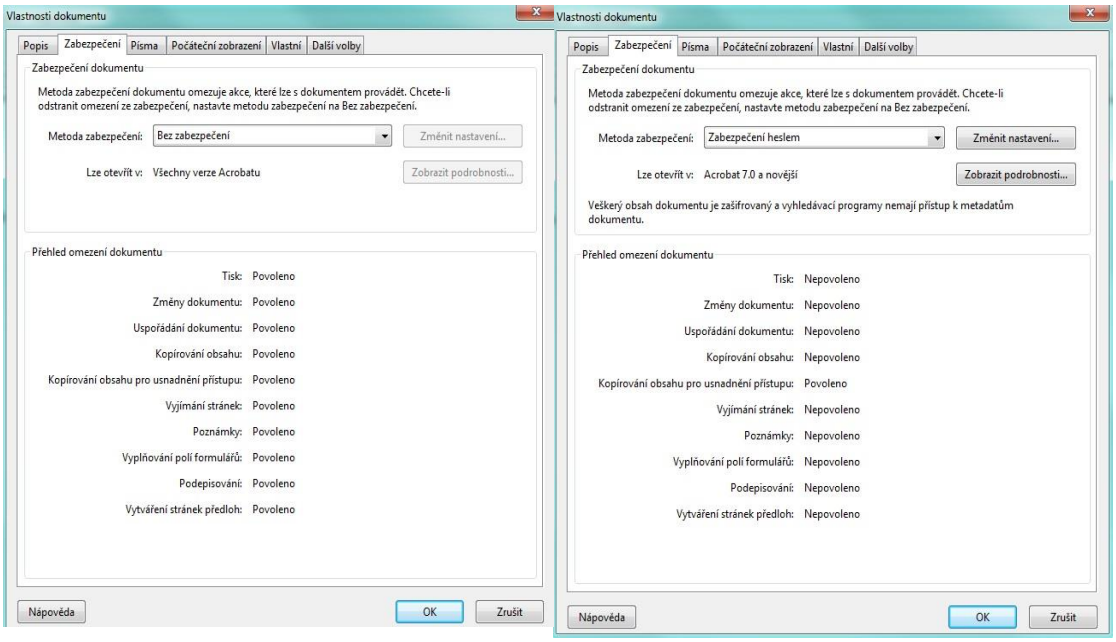
Po provedení této operace je v programu možno vidět úspěšnost dešifrování, cestu k původnímu i dešifrovanému souboru viz obrázek 3.5.

**Obrázek 4.5 - Zobrazení informací o dešifrování souboru**


Zdroj: Autor BP

Pro testování spolehlivosti tohoto typu zabezpečení byla zvolena dvě hesla s různou délkou a použití různých znaků (číslice, velká i malá písmena a jiné znaky). První heslo bylo aplikací Adobe Acrobat ohodnoceno jako slabé a mělo tvar AKb12cz. Druhé @cb128bZx52$ heslo bylo ohodnoceno jako nejlepší. Obě hesla byla prolomena během chvilky, což znamená, že na prolomení zabezpečení nemá síla hesla žádný vliv. Kompatibilita a úroveň šifrování v tomto případě také nemá žádný vliv, jelikož implementace tohoto zabezpečení je u všech verzí PDF stejná.

**Obrázek 4.6 - Přehled omezení zabezpečení typem vlastník - šifrovaný soubor (vlevo) ,dešifrovaný soubor (vpravo)**




Zdroj: Autor BP

Obrázek 3.6 názorně ukazuje přehled omezení dokumentu mezi zabezpečeným souborem a dešifrovaným souborem aplikací PDF Decrypter Pro.

### 4.1.3 Spolehlivost hesla uživatel

K otevření dokumentu, zabezpečeného heslem typu uživatel, je třeba znát toto heslo, jak je již výše uvedeno. Bez jeho znalosti není možnost otevřít dokument. Po zadaná tohoto hesla proběhne samotné dešifrování dokumentu. Odstranit informaci o zabezpečení dokumentu není již tak jednoduché jako v předchozím případě, okomentovat část dokumentu s informací o hesle nelze, jelikož je tato informace uložena přímo v objektu. Uživatel musí zadat heslo, na které je pak aplikován algoritmus. Po provedení algoritmu dostaneme hodnotu hash, která se porovná s hodnotou uvedenou v objektu, který obsahuje informace o šifrování. V případě shody proběhne dešifrování dokumentu a lze jej otevřít [16].

Na prolomení tohoto druhu zabezpečení je nutné použít útok hrubou silou (brute force attack). V praxi to znamená, že uživatel nebo program musí vyzkoušet všechny hesla, dokud nenarazí na to správné. Tato metoda je závislá na jazykové sadě a délce zvoleného hesla.

V červnu roku 2011 byla vydána stručná analýza čtyřiceti tisíc hesel uniklých ze společnosti Sony. Tento únik informací může velice napomoci při použití útoku hrubou silou. Jak již bylo zmíněno, jedním z důležitých aspektů síly hesel je jeho délka. U devadesáti tří procent uživatelů mělo heslo délku mezi šesti až deseti znaky a padesát procent z nich mělo délku hesla menší než osm znaků. Důležitou roli hraje i charakterový typ znaků (čísla, velká a malá písmena a ostatní znaky). V pouhých čtyřech procentech hesel bylo použito tři a více charakterových typů znaků. Stručněji řečeno, v polovině hesel byl použit pouze jeden charakterový typ znaků a v devíti z deseti případů byla použita pouze malá písmena. V pouhém jednom procentu analyzovaných hesel bylo současně použito písmeno a číslice. Toto zjištění není nijak překvapující, ale určitě pro ochranu soukromí uživatelů alarmující [18]. Velká část populace používá latinskou abecedu, která obsahuje 26 znaků. Po přičtení stejného množství znaků psaného velkými písmeny a 10 arabských číslic dostaneme číslo 62. Dále je třeba v úvahu brát speciální znaky včetně mezery, kterých je celkem 33 (,.:;-?!‘“()+/<=>[]{}~%&#$*@\^_`|) po přičtení těchto znaků dostaneme číslo 95. Další a složitější znaky nejsou z důvodu komfortnosti vkládání a omezení různých znakových příliš využívány. Tabulka 3.2 znázorňuje množství kombinací v návaznosti na délku hesla a počet znaků potřebných pro zjištění správného hesla.

**Tabulka 4.2 - Přehled vybraného počtu možných kombinací a zaokrouhleného výpočetního času**

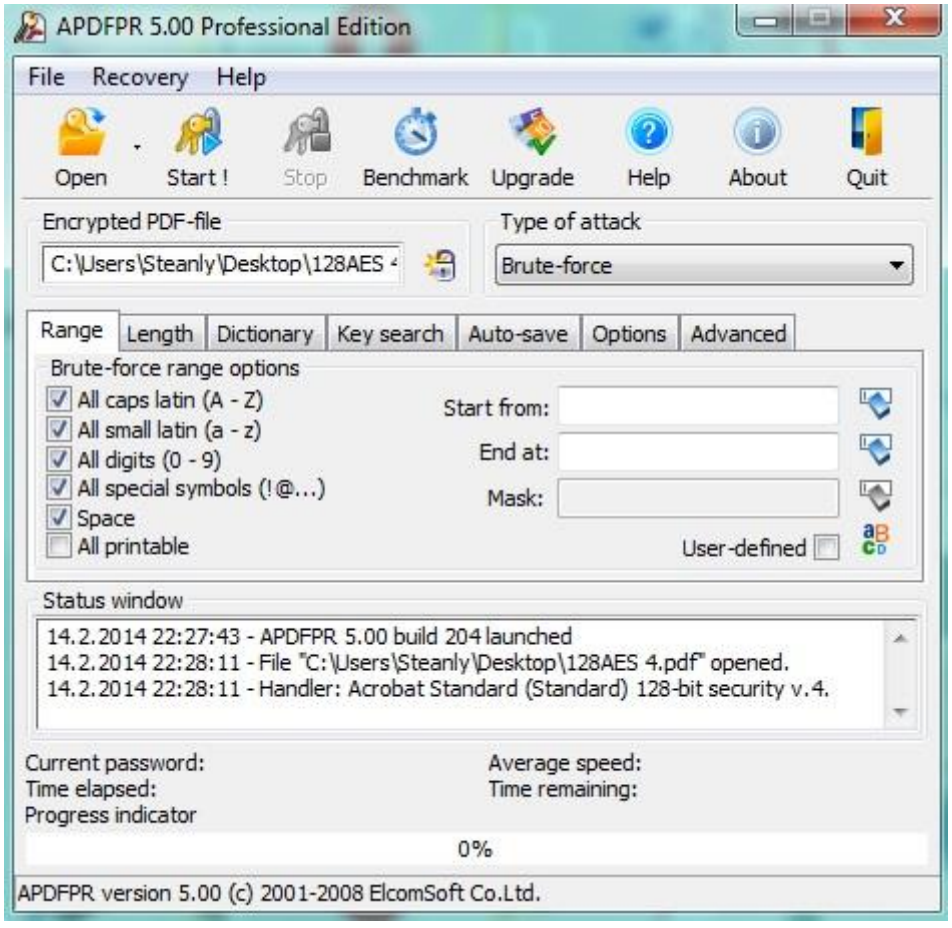
| **Počet použitých znaků** | **Délka hesla** | **Počet možných kombinací (matematických variací)** | **Čas potřebný pro získání hesla** | | |
|---|---|---|---|---|---|
| | | | **128 bit RC4** | **128 bit AES** | **256 bit AES** |
| 36 znaků | 4 | $36^4$ | 7 sek | 7 sek | 9 sek |
| | 6 | $36^6$ | 1,5 hod | 1,5 hod | 1,75 hod |
| | 8 | $36^8$ | 41 dní | 41 dní | 48 dní |
| | 10 | $36^{10}$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| 52 znaků | 4 | $52^4$ | 2 min | 2 min | 2,5 min |
| | 6 | $52^6$ | 3,5 dne | 3,5 dne | 4,5 dne |
| | 8 | $52^8$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| | 10 | $52^{10}$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| 62 znaků | 4 | $62^4$ | 4 min | 4 min | 5 min |
| | 6 | $62^6$ | 11 dní | 11 dní | 13 dní |
| | 8 | $62^8$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| | 10 | $62^{10}$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| 95 znaků | 4 | $95^4$ | 23 min | 23 min | 27 min |
| | 6 | $95^6$ | 145 dní | 145 dní | 167 dní |
| | 8 | $95^8$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |
| | 10 | $95^{10}$ | Vice jak 1 rok | Vice jak 1 rok | Vice jak 1 rok |

Zdroj: Autor BP

Vliv na rychlost zjištění hesla má i rychlost použité počítačové sestavy. K této práci byl použit notebook s procesorem Intel Core i5-2430M, operační pamětí 4 GB a grafickou kartou Radeon HD 6590M. K testování útoku hrubou silou byl použit program Advanced PDF Password Recovery od společnosti Elcomsoft [19]. Tento program obsahuje vestavěnou aplikaci pro měření orientačního času zjištění hesla v závislosti na druhu zabezpečení a použitém šifrování (Benchmark) viz tabulka 3.2. Bohužel čas přesahující jeden rok již není zobrazen přesně.

Pro testování útoku hrubou silou byl v programu Adobe Acrobat XI dokument vytvořen a zašifrován. Zvolena byla konfigurace zabezpečení heslem typu uživatel a nastaven algoritmus AES s délkou klíče 128 bitů. Po načtení souboru do programu, které program umožňuje použitím tlačítka „Open“ nebo přetažením souboru do programu (funkce drap and drop), bylo programem rozpoznáno zabezpečení dokumentu a program správně zvolil útok hrubou silou (brute force attack) viz obrázek 3.7.

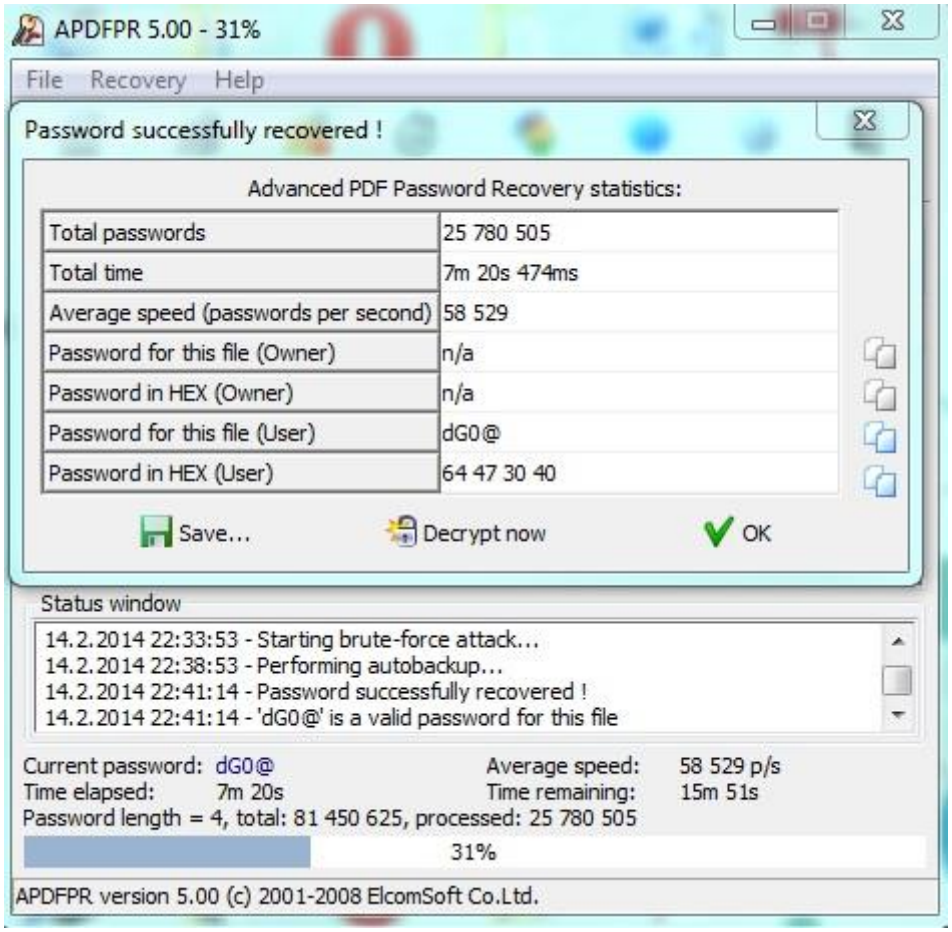
**Obrázek 4.7 - Rozeznání zabezpečeného PDF souboru v programu Advanced PDF Password Recovery**




Zdroj: Autor BP

V programu byly vybrány všechny znaky a kvůli době prolamování hesla nastavena délka hesla v záložce Length (délka) na čtyři znaky. V záložce Advance (postup) bylo nastaveno hledání hesla typu uživatel (User password). Po stisknutí tlačítka „Start“ začal program zkoušet možná hesla ve výše zmíněné délce.

**Obrázek 4.8 - Úspěšné nalezení hesla typu vlastník pomocí programu Advanced PDF Password Recovery**




Zdroj: Autor BP

Program úspěšně nalezl heslo ve tvaru dG0@. Toto heslo bylo nalezeno za necelých 7,5 minuty, což program odhadl na 31% celkového času na vyzkoušení všech hesel ze sady 95 znaků a délky hesla 4 znaky.

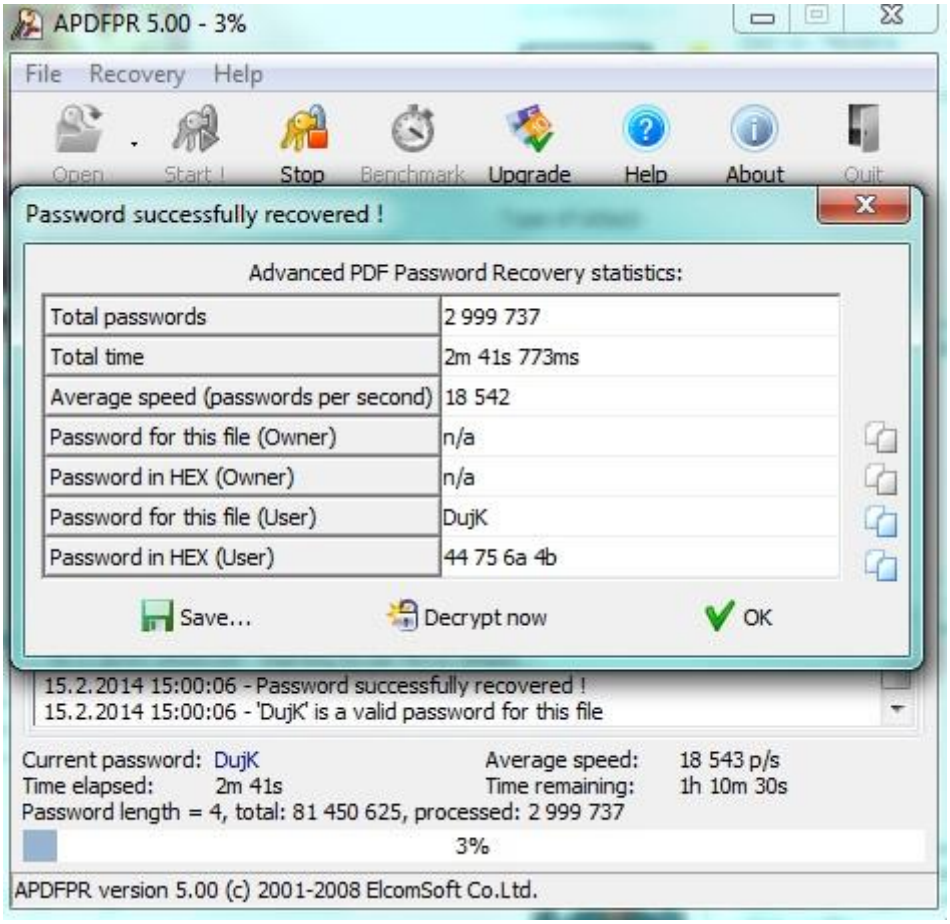
Statistiky zobrazené na obrázku 3.8 si může uživatel programu uložit tlačítkem „Save“ do textového souboru a tlačítkem „Decrypt now“ přeuložit soubor pod vybraným jménem jako formát PDF zbavený použitého druhu zabezpečení.

### 4.1.4 Spolehlivost obou hesel současně

Zabezpečit soubor formátu PDF lze i oběma typy hesel současně, jak je výše zmíněno. Pro otevření souboru je nutné znát aspoň jeden typ hesla. Po zadání dojde k dešifrování souboru a dle zadaného hesla jsou dále řízená nastavená oprávnění. V nejčastějším případě použití obou hesel zároveň zná uživatel heslo typu uživatel pro otevření dokumentu. V tomto případě lze ve stejném programu, ve kterém bylo testováno zabezpečení uživatele typu vlastník, toho heslo zadat, program ihned heslo odstraní a pomocí principu, který využívá zmíněný program použitý při zabezpečení dokumentu heslem typu vlastník. Tato operace je vyřešena v řádu jednotek vteřin.

Ovšem, jestliže neznáme žádné z hesel, umí program Advanced PDF Password Recovery po použití útoku hrubou silou obě hesla najít. To není zapotřebí, programu stačí, když najde pouze heslo uživatel, které slouží pro otevření dokumentu a dál postupuje jako v případě zabezpečení heslem typu vlastník. Soubor pro testování tohoto typu zabezpečení byl vytvořen a zabezpečen rozdílnými hesly. Načten do programu a v záložce „Advance“ (postup) zvolena možnost „Any Password“ (jakékoli heslo).

**Obrázek 4.9 - Úspěšné nalezení hesla typu vlastník, při zabezpečení souboru oběma hesly, pomocí programu Advanced PDF Password Recovery**




Zdroj: Autor BP

Obrázek ukazuje nalezení hesla typu uživatel, které mělo tvar DujK. Opět, jako v předchozím případě, byla přesně zadána délka hesla kvůli snížení dešifrovacího času. Soubor lze uložit nebo si uložit statistiky o dešifrování souboru uložit jako v předchozím případě.

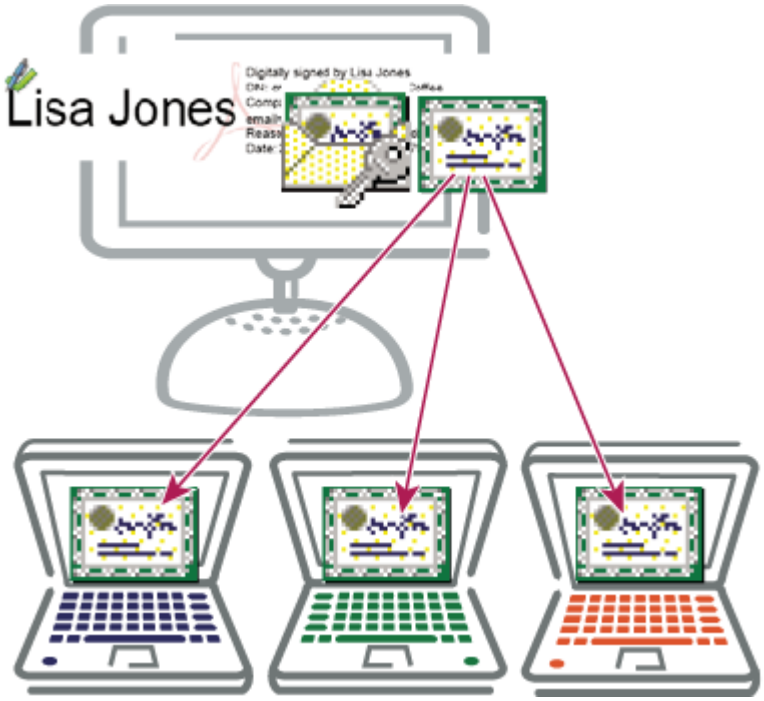
## 4.2 Zabezpečení certifikátem

Použití zabezpečení certifikátem je další metodou, kterou standard PDF nabízí. Tato technologie lze použít k digitálnímu podepisování a verifikování podpisů nebo k šifrování a dešifrování dokumentů [20]. V certifikátu pro zabezpečení PDF dokumentů je uložena komponenta digitálního identifikátoru představovaná veřejným klíčem.

Digitální identifikátor prokazuje totožnost a je v něm obvykle uvedeno jméno, e-mailová adresa, název vystavující organizace, sériové číslo a datum ukončení platnosti. Digitální identifikátor se používá pro digitální podpisy a zabezpečení dokumentů pomocí certifikátů.

Bezpečnostní ovladač používající technologii veřejného klíče šifrování je využíván ve standardu PDF [16]. Certifikáty používané v zabezpečení PDF dokumentů se skládají ze dvou částí – veřejné a privátní. Privátní část certifikátu obsahuje privátní klíč sloužící k dešifrování dokumentu, veřejná část obsahuje veřejný klíč sloužící k zašifrování dokumentu. Privátní klíč je bezpečně uložen u autora, veřejný klíč je sdílen [21].

**Obrázek 4.10 - Naznačení funkčnosti digitálního identifikátoru**




Zdroj: [21]

Digitální podpis ujistí příjemce dokumentu, od koho jej přijal. Šifrování zajišťuje, že obsah bude moci zobrazit pouze uživatel určení správcem dokumentu [22]. Práce se bude dále zaměřovat pouze na zabezpečení PDF dokumentů certifikáty, sloužící k zašifrování dokumentu.

Možnost použití certifikátu jako druhu zabezpečení je dostupné od verze Adobe Acrobat 5.0 (verze 4.1) viz tabulka 3.1.

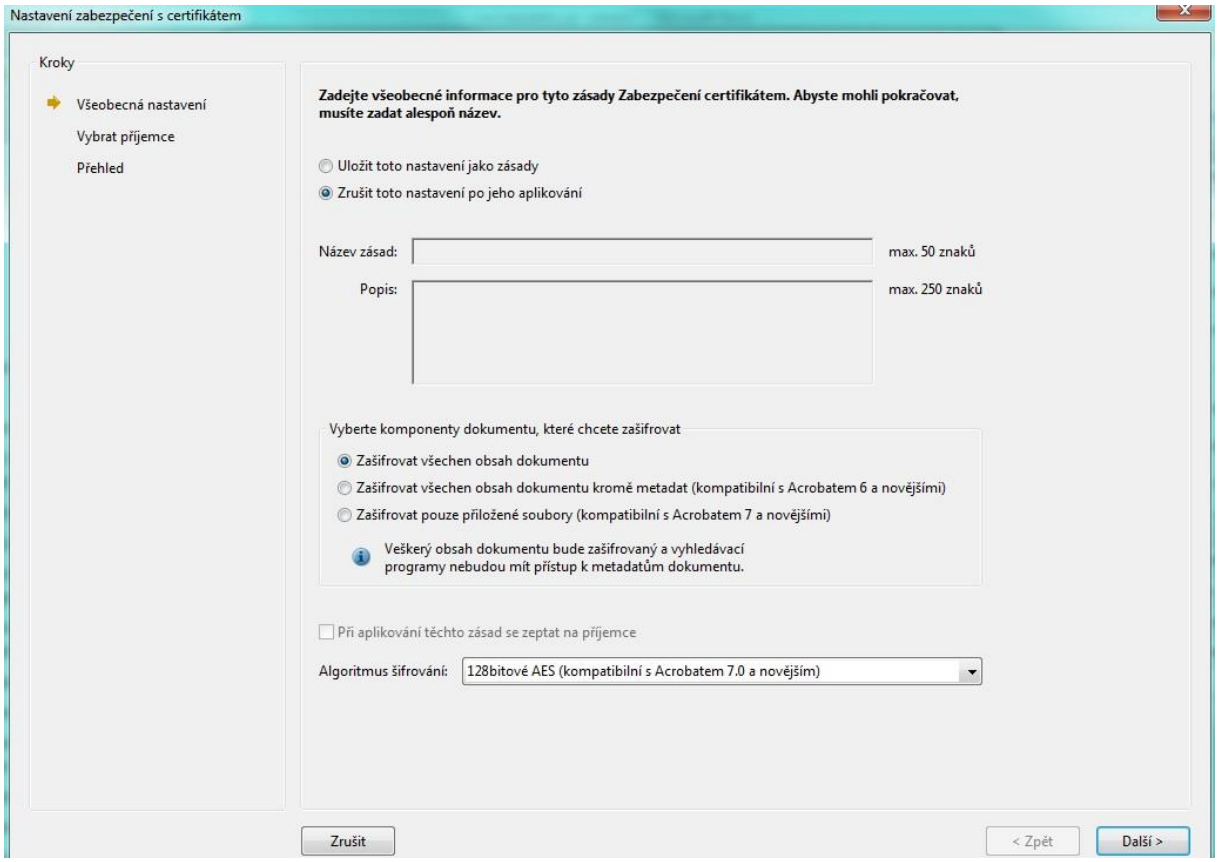
V současné době je podporována zpětná kompatibilita s verzí Adobe Acrobat 6.0 (verze 5.1) a novějšími verzemi. Software Adobe Acrobat umožňuje vytvoření vlastního certifikátu nebo jeho získání pomocí jiných certifikačních autorit, což je v asymetrické kryptografii subjekt, který vydává digitální certifikát.

Certifikát pro účely této práce byl vytvořen prostřednictvím softwaru Adobe Acrobat.

### 4.2.1 Nastavení metody zabezpečení certifikátem

Metodu zabezpečení certifikátem je možno nastavit v okně „Soubor / Vlastnosti / Zabezpečení / Zabezpečení certifikátem“, viz obrázek 3.2. Možnosti nastavení této metody a jednotlivé kroky postupu nastavení tohoto druhu zabezpečení zobrazují obrázky 3.5, 3.6, 3.7 a 3.8.

**Obrázek 4.11 - Krok 1/4 - Možnosti zabezpečení metodou certifikátů**



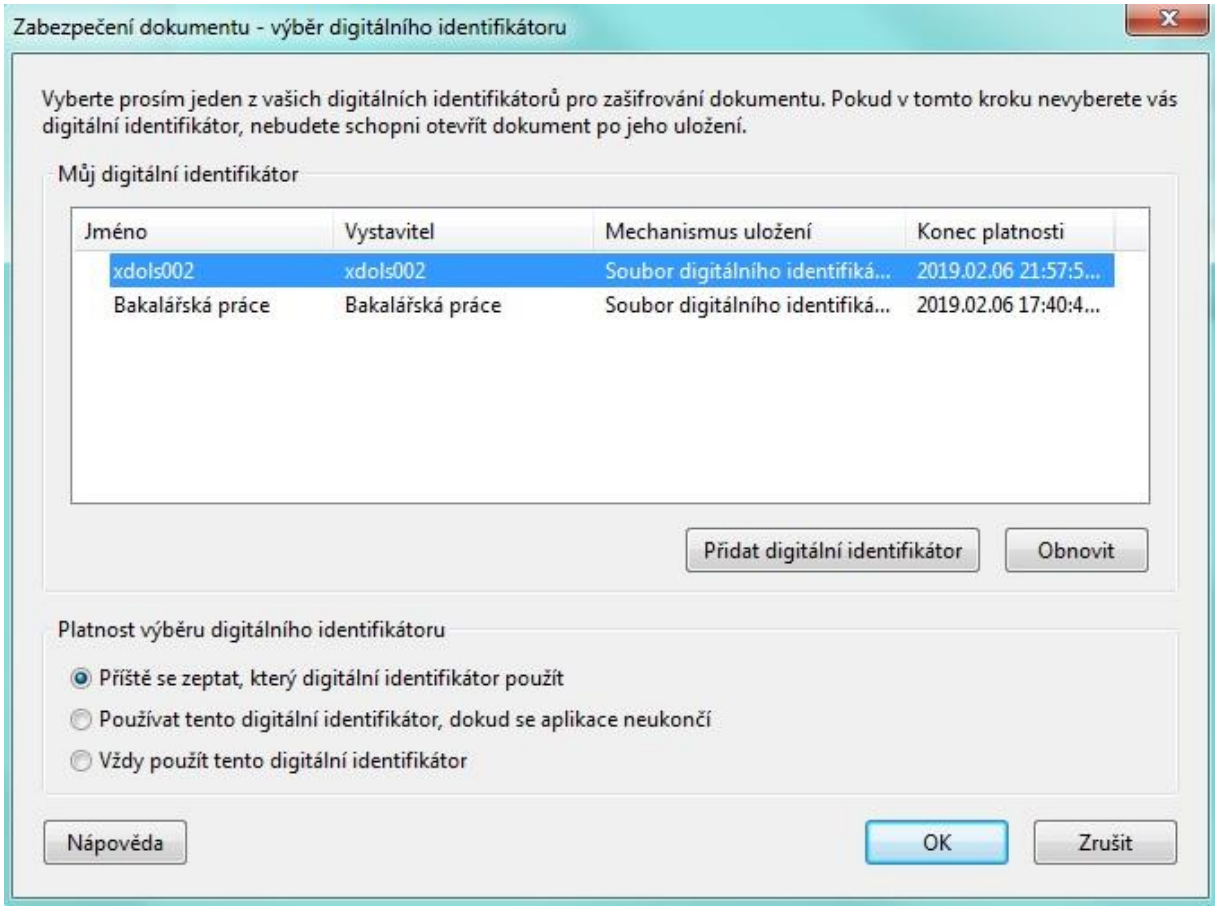

Zdroj: Autor BP

V okně, zobrazeném na obrázku 3.5, jsou dostupné následující možnosti:

- Uložit toto nastavení jako zásady – označením této volby se uloží konfigurace zabezpečení jako šablona pro stejné použití na jiném souboru v budoucnu
    - Název zásad – jméno šablony
    - Popis – popis šablony
- Zrušit toto nastavení po jeho aplikování – konfigurace zabezpečení je pouze jednorázová
- Vyberte komponenty dokumentu, které chcete zašifrovat – obsahuje tři možnosti zašifrování prvků dokumentu (stejné s možnostmi v konfiguraci zabezpečení heslem popsané výše)
- Při aplikování těchto zásad se zeptat příjemce -
- Algoritmus šifrování – výběr kompatibilní verze programu a šifrovacího algoritmu

Po vybrání algoritmu šifrování a komponent dokumentu, které mají být zašifrovány, je uživatel vyzván k výběru digitálního certifikátu, který bude použit pro zašifrování souboru. Je zde možnost použití několika existujících digitálních identifikátorů - uloženého v souboru (jelikož certifikát má své heslo, uživatel ho musí znát a zadat) uloženého na serveru, nahrání ze zařízení připojeném k počítači nebo vytvořením vlastního digitálního identifikátoru. Tímto se práce dále nezaobírá a používá vytvořený vlastní identifikátor chráněný heslem, který používá formát PKCS#12.

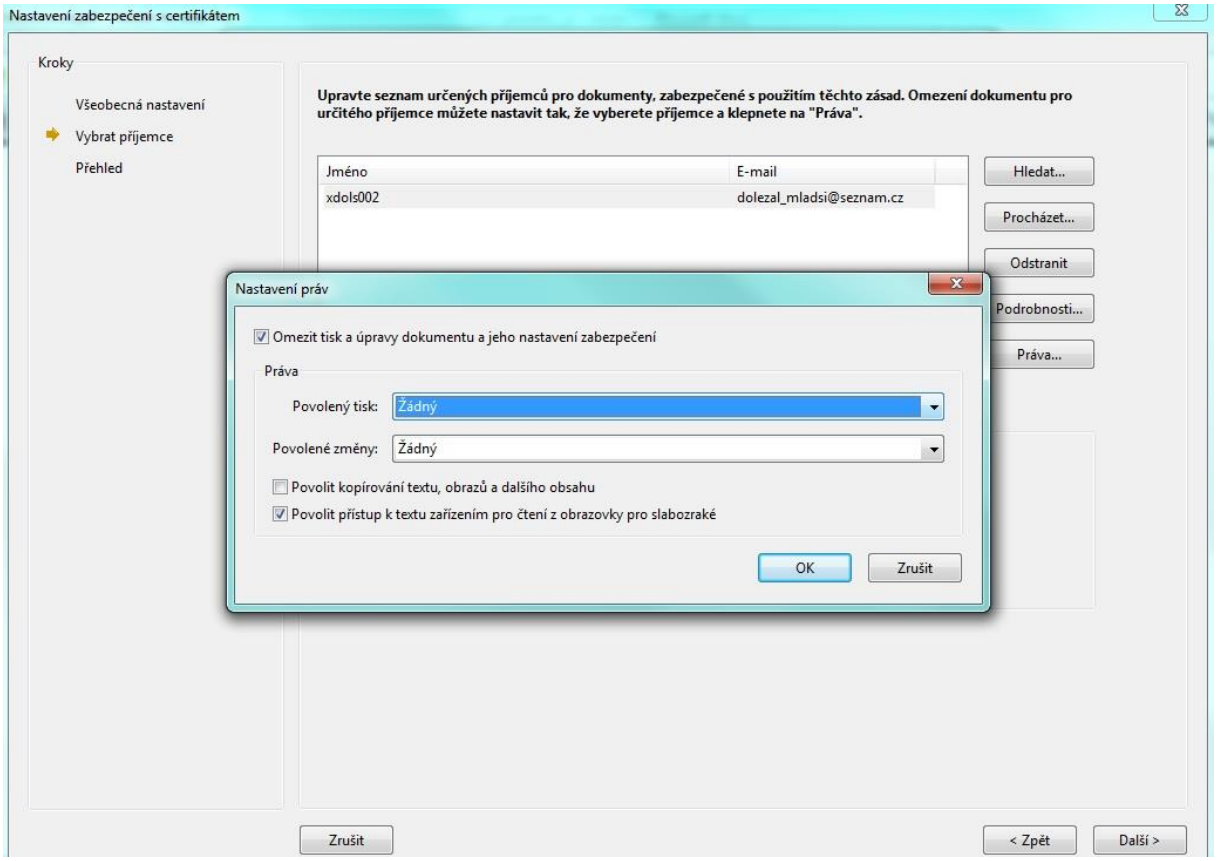
**Obrázek 4.12 - Krok 2/4 Možnost výběru nebo vytvoření digitálního identifikátoru**




Zdroj: Autor BP

Obrázek 3.6 jen názorně ukazuje možnosti vybírání identifikátorů a možnosti výběru jeho platnosti. Ve třetím kroku se nastavují práva pro práci s dokumentem a vybírají se příjemci dokumentu. Mít veřejný certifikát každého příjemce nebo skupiny je nutné, bez toho je nelze přidat. Pokud není přidán certifikát vlastníka souboru, nemůže ho následně otevřít [22].

**Obrázek 4.13 - Krok 3/4 nastavení zabezpečení certifikátem s aktivní volbou „Práva“ a jedním veřejným certifikátem**



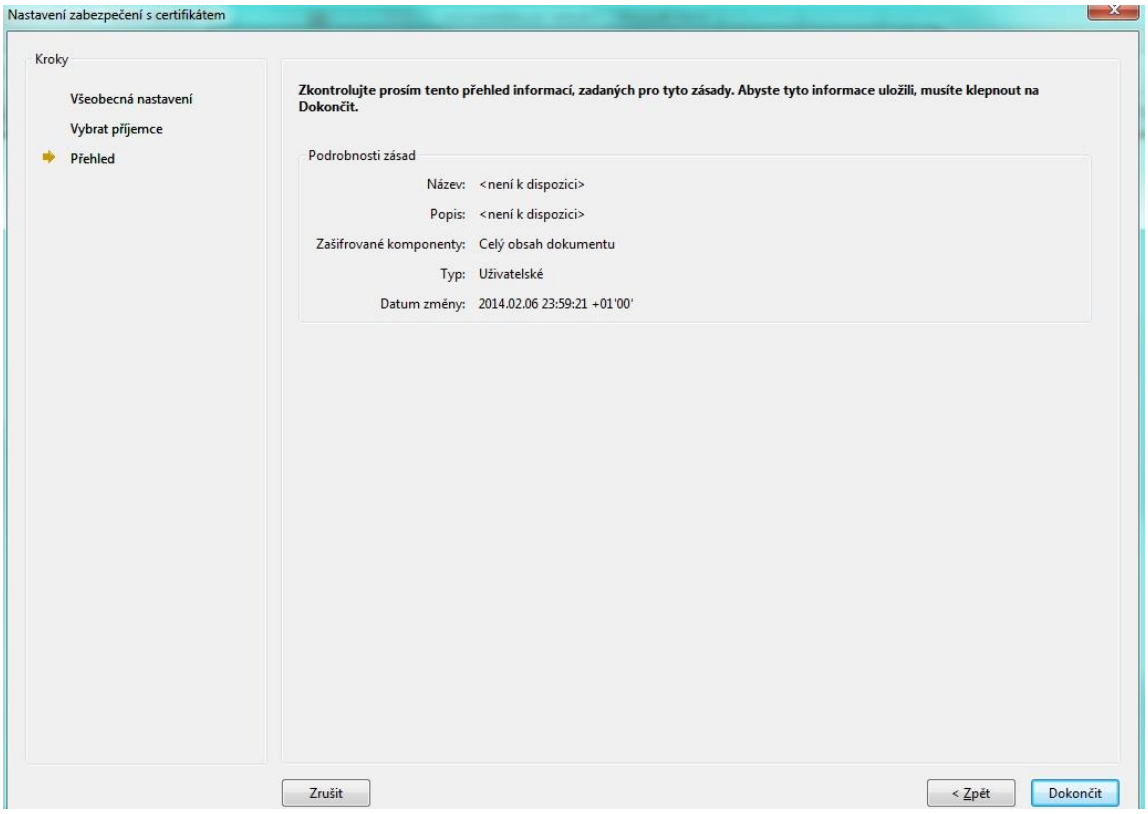

Zdroj: Autor BP

Krok 3/4 obsahuje následující možnosti:

- Hledat – je zde možné vyhledávat identity na adresářovém serveru nebo v seznamu důvěryhodných identit
- Procházet – ruční vyhledání a výběr souboru obsahující certifikáty důvěryhodných identit
- Odstranit – slouží k odebrání uživatelé ze seznamu určených příjemců dokumentu
- Podrobnosti – zobrazí podrobnosti o konkrétním certifikátu
- Práva – nastavují se zde stejné parametry jako v metodě zabezpečení heslem typu vlastník (povolení tisku a změn)

Poslední krok slouží k revizi nastavení zabezpečení souboru, viz obrázek 3.8. Po dokončení se však nastavení zabezpečení na dokument neaplikuje, dokud není dokument uložen. Před uložením jde dále měnit nastavení zabezpečení.

**Obrázek 4.14 - Krok 4/4 Přehled podrobností bezpečnostních zásad aplikovaných na dokument**



Zdroj: Autor BP

Po uložení je dokument zašifrován pomocí veřejných certifikátů, mohou dokument otevřít pouze uživatelé ze seznamu určených příjemců dokumentu po zadání hesla. Stejně jako při použití zabezpečení heslem kombinací obou typů hesel (uživatel a vlastník) je dokument po zadání hesla dešifrován a zobrazen, můžou však být nastavením oprávnění omezené některé funkcionality dokumentu.

### 4.2.2 Spolehlivost zabezpečení certifikátem

Asymetrická šifra využívá veřejný a privátní klíč. Tento druh šifry je v technologii PDF použit pro autentifikaci uživatele a jeho oprávnění. Také je šifra dále využívána k šifrování interního, již symetrického klíče, jenž je dále užíván k vlastnímu šifrování objektů typu stream a string [16]. Pro šifrování privátního klíče je však využito symetrické šifrování. Privátní klíč je jeden pro všechny uživatele a na jeho základě je soubor šifrován.

Tento druh šifrování jedním klíčem je shodný s metodou zabezpečení heslem. Hlavním rozdílem mezi těmito typy zabezpečení je, že pro různé příjemce dokumentu je klíč šifrován dále použitím hybridního šifrování, což ve výsledku umožňuje pro různé příjemce jiná oprávnění.

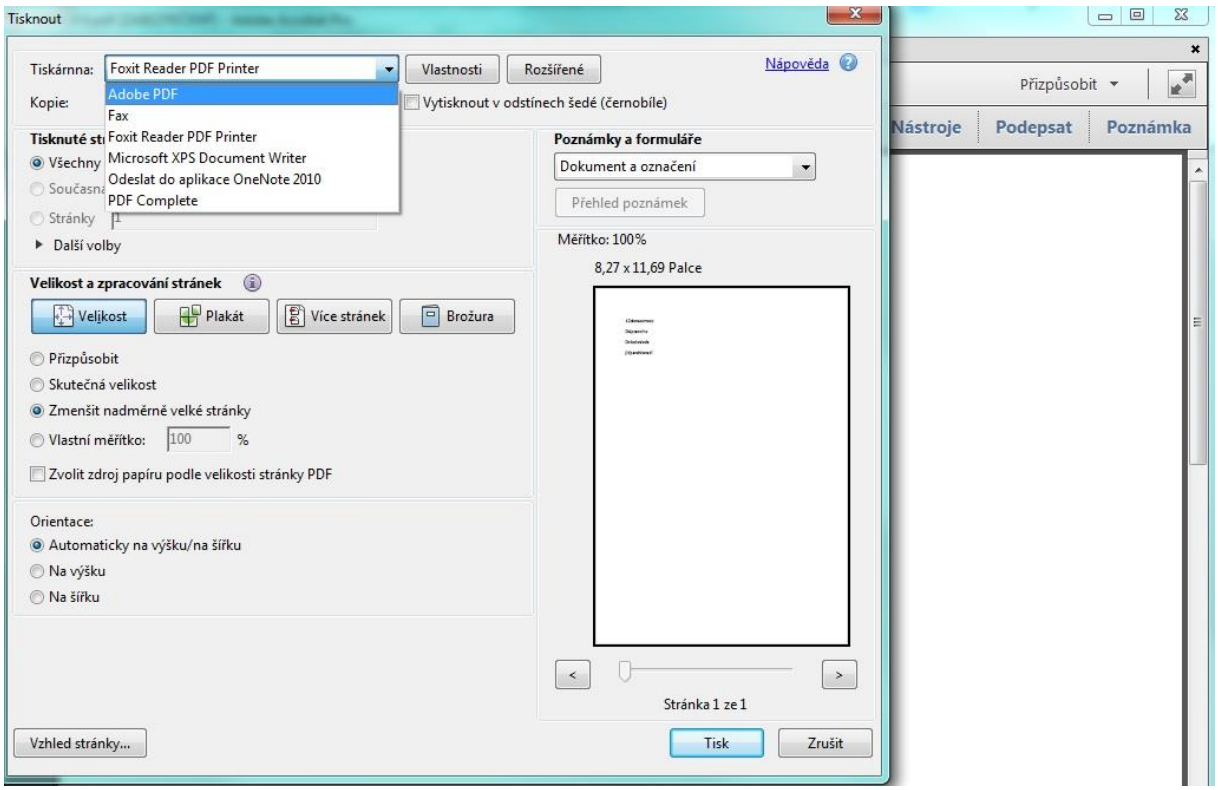
Informace o zabezpečení je uložena do přívěsu dokumentu a odkaz na objekt v části tělo, obsahující detaily ohledně daného zabezpečení, je oproti zabezpečení heslem rozšířen o parametr Recipients. Recipients obsahuje pole binární pole objektů. V těchto polích je uložen seznam příjemců se stejnými oprávněními a šifrovaný symetrický klíč každého uživatele pomocí veřejného klíče příjemce [16].

Jak je výše zmíněno, pro otevření souboru zabezpečeného certifikátem je vyžadováno heslo pro otevření, což je obdobné jako u zabezpečení heslem typu vlastník. Jestliže příjemce heslo nezná, dá se usoudit, že dokument se neměl dostat do jeho rukou. V takovém případě přichází v úvahu útok na symetrický interní klíč, který má v dnešní době délku 128 nebo 256 bitů, použitím útoku hrubou silou. V druhém případě, kdy dokument obdržel správný příjemce, se předpokládá, že zná privátní klíč pro otevření dokumentu. Po jeho zadání je soubor dešifrován, následně otevřen a funkcionality dokumentu jsou řízené předchozím nastavení odesílatele.

Nenašel jsem žádný software, který by umožnil zároveň dešifrování souboru PDF zabezpečeného certifikátem a následně odstranil oprávnění. Nelze ani otevřenému dokumentu upravovat ani odstranit konfiguraci zabezpečení dokumentu. Existuje způsob, jak odstranit omezení funkcionalit. Odstranění funkcionalit dokumentu lze provést jen za předpokladu, že autor nezakázal tisk dokumentu. Program Adobe Distiller, který je do systému nainstalován společně s programem Adobe Acrobat, instaluje do systému počítače tzv. virtuální tiskárnu, která je integrována ve všech programech. Tento krok provedou i některé programy pro čtení PDF dokumentů.

Ve většině případů však nedokáží otevřít dokument zabezpečený certifikátem. Jestliže otevřený dokument, zabezpečený certifikátem, otevřeme v aplikaci Adobe Acrobat a zvolíme příkazy „Soubor / Tisknout“, je možné vidět tiskárny nainstalované v počítači. V prvním případě byla zvolena tiskárna Adobe PDF, viz obrázek 3.15.

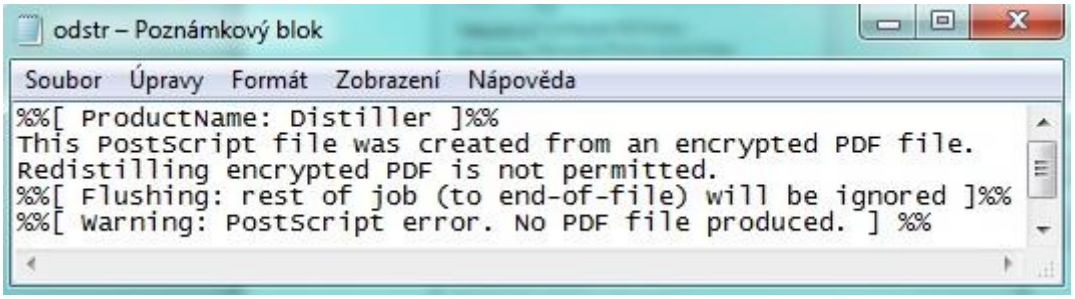
**Obrázek 4.15 - Výběr tiskárny v programu Adobe Acrobat**




Zdroj: Autor BP

Proces ukládání souboru však skončil chybovou hláškou, že ukládaný soubor je vytvářen ze zabezpečeného dokumentu a opětovné šifrování PDF dokumentu není povoleno, viz obrázek 3.16.

**Obrázek 4.16 - Chybová hláška při pokusu tisku souboru pomocí virtuální tiskárny Adobe PDF**




Zdroj: Autor BP

Jako druhá možnost byla zvolena tiskárna Foxit Reader PDF Printer vytvořená předem nainstalovaným programem Foxit Reader společnosti Foxit [23]. Soubor byl během několika vteřin uložen a virtuální tiskárna neuložila údaje týkající se omezení funkcionalit dokumentu. Vzniknul nezabezpečený soubor, ve kterém není nastavené žádné omezení funkcionalit.

## 4.3 Zabezpečení AdobeLiveCycle

Adobe LivyCycle je serverová platforma, která automatizuje procesy dokumentů. Tento software je postaven na společné serverové architektuře. V roce 2005 byl uveden na trh první produkt s předponou LiveCycle, sloužící pro rozšířenou práci s dokumenty, podporující verzi 7.0 produktu Adobe Acrobat.

Vývoj serverového řešení produktů založených na platformě Java EE běžel již dříve a pro uživatele byly dostupné produkty od roku 2001 [24]. Jednotlivé komponenty řešení LiveCycle se zabývají – pořizováním dat, zabezpečením informací, řízením procesů, správou dat a výstupem dokumentů [25]. Tato práce se bude dále zabývat softwarem z kategorie zabezpečení informací, jenž je systémem zabezpečení, založený na serveru poskytující dynamickou kontrolu nad PDF dokumenty, s názvem Adobe LiveCycle Rights Management.

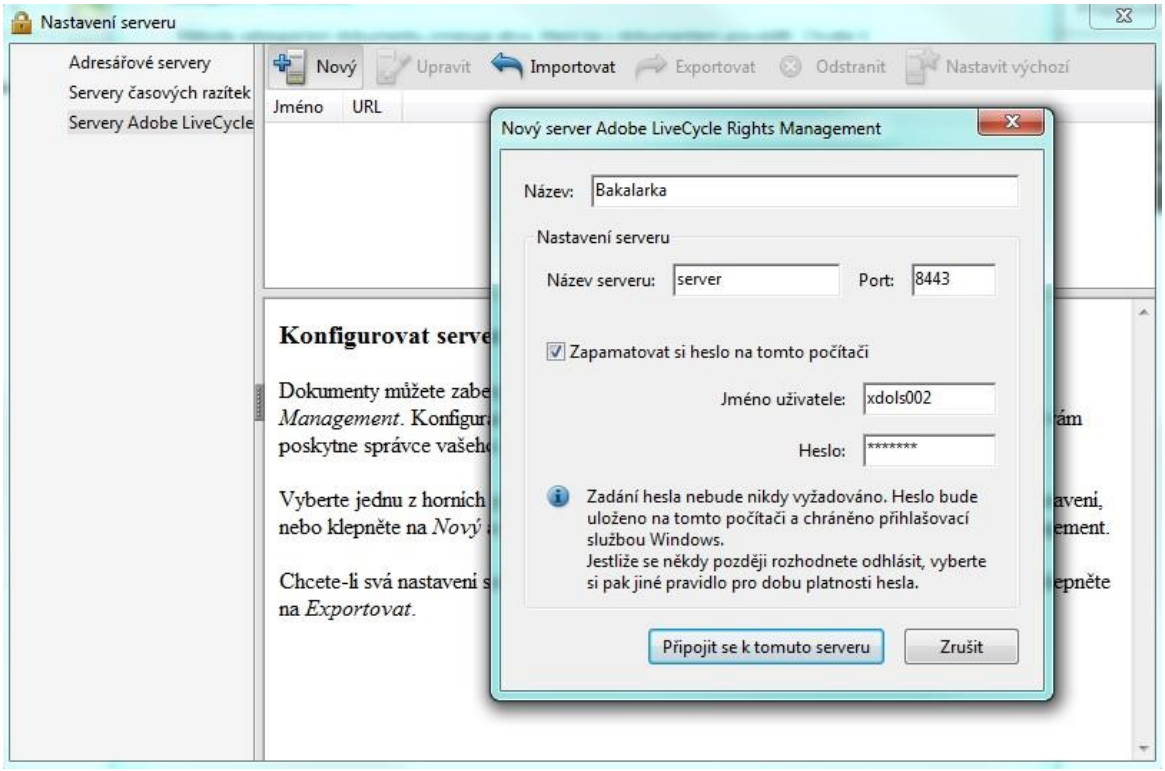
Je zde možná i podpora zabezpečení souborů jiného formátu než PDF, například formátů kancelářských aplikací Microsoft Office a CAD dokumentů. Dále se bude práce zaměřovat pouze na zabezpečení PDF souborů.

Jako v předchozích zmíněných metodách zabezpečení PDF dokumentů, lze i pomocí služby LiveCycle přidávat dokumentům různá oprávnění a šifrovat je. Pokročilé funkce umožňují dokument trasovat, nastavovat dobu platnosti, sledovat historii, měnit oprávněná v průběhu doby platnosti. Na server se systémem Adobe LiveCycle Rights Management se ukládají pouze zásady zabezpečení konkrétních souborů, avšak nikoli samotné PDF soubory. Z tohoto důvodu musejí v některých situacích být uživatelé připojeni k serveru, aby mohli s dokumentem pracovat dle jejich oprávnění [26].

### 4.3.1 Nastavení LiveCycle

Nastavení zabezpečení touto metodou je stejně jako ostatní druhy zabezpečení dostupné v okně „Soubor / Vlastnosti / Zabezpečení / Adobe LiveCycle Rights Management“, viz obrázek 3.2. V případě, že není uživatel připojen k serveru Adobe LiveCycle Rights Management, je vyzván programem k vybrání serveru nebo nastavení připojení k serveru. Vytvoření připojení je zobrazeno na obrázku 3.17.

**Obrázek 4.17 – Nastavení připojení k serveru Adobe LiveCycle**




Zdroj: Autor BP

- Název – pouze orientační název serveru pro připojení
- Název serveru – jméno serveru Adobe LiveCycle nebo IP adresa serveru
- Port – port serveru služby Adobe LiveCycle
- Jméno uživatele – uživatelské jméno zaregistrovaného uživatele ke službě LiveCycle
- Heslo – heslo zaregistrovaného uživatele ke službě LiveCycle

Aby spojení se serverem proběhlo bez problémů, musí administrátor vytvořit uživatelský účet služby LiveCycle. Bez uživatelského účtu se nelze k serveru připojit. Po úspěšném spojení se serverem je uživatel přesměrován do webového rozhraní, kde může nastavit veškerá zabezpečení dokumentu (přidání uživatelů nebo skupin pro příjem dokumentu, nastavení oprávnění pro práci dokumentu každému uživateli nebo skupině, možnost čtení dokumentu bez připojení uživatele k serveru, nastavení sledování historie a doba expirace dokumentu, přidání vodoznaku, zakázání čtení dokumentu, jestliže jsou v programu Adobe Reader nainstalovaní zásuvné moduly třetí strany, výběr šifrovacího algoritmu a nastavení zašifrování různých částí dokumentu). Po uložení veškerých nastavení je v programu Adobe Acrobat je zobrazena položka vytvořeného zabezpečení [27].

Vybráním položky a uložením dokumentu je vybrané zabezpečení aplikováno na dokument. Hlavní rozdíl oproti ostatním metodám zabezpečení je možnost nastavení omezení funkcionalit dokumentu bez jeho šifrování, sledování historie dokumentu, vložení vodoznaku a nastavení doby expirace dokumentu. O zranitelnosti a prolomení tohoto druhu zabezpečení nelze mluvit, pokud minimálně při prvním otevření dokumentu neproběhne autentifikace uživatele vůči serveru LiveCycle. Bez znalostí přihlašovacích údajů lze uvažovat útok hrubou silou na uživatelské jméno a heslo. To je ovšem složitější kvůli zvyklostem serverů blokovat přihlášení uživatele po několikanásobném neúspěšném pokusu o přihlášení.

## 4.4 Ochrana důvěrného obsahu

V předchozích případech bylo popisováno zabezpečení dokumentu jako celku, nebyl brán na zřetel na jeho obsah a informace v něm obsažené. Za určitých podmínek šlo prolomit každé zabezpečení na dokument aplikované. Program Adobe Acrobat umožňuje i práci s obsahem dokumentu včetně odstranění volitelných slov, stránek nebo informací, které si autor sám zvolí pomocí následujících nástrojů.

### 4.4.1 Funkce Odstranit skryté informace

Před distribucí PDF dokumentů dalším uživatelům může vzniknout potřeba odstranit důvěrný obsah nebo soukromé informace, které můžou prozradit autora dokumentu. Obvykle po vytvoření dokumentu jsou v metadatech obsaženy informace o dokumentu a jeho obsahu, jako jsou jméno autora, klíčová slova a informace o copyrightu. Pro odstranění těchto informací je v programu Adobe Acrobat integrovaná funkce Odstranit skryté informace. Tato funkce umožňuje prohledat dokument a výše uvedené informace odstranit. Autor dokumentu může pomocí této funkce odstranit i obsah, který může nežádoucím způsobem změnit vzhled dokumentu [28]. Funkce umožňuje, včetně metadat, odstranit následující položky:

- Přiložené soubory – k PDF dokumentům lze jako přílohu připojit soubory libovolného formátu
- Záložky – jsou odkazy s reprezentativním textem, který se používá k otevření určitých stránek v PDF dokumentech
- Poznámky a označení – zahrnují všechny poznámky přidané do PDF dokumentu pomocí nástrojů pro poznámky a označování, včetně souborů přiložených jako poznámky
- Pole formulářů – zahrnuje samotné pole formulářů (včetně polí podpisu) a všechny akce a výpočty související s poli formulářů. Po odstranění této položky se všechna pole formulářů sloučí s obsahem a není dále možné pole vyplňovat, upravovat ani podepsat
- Skrytý text na stránkách – v dokumentu může být obsažen text, který má stejnou barvu jako pozadí, je skryt za jiným obsahem nebo je průhledný

- Skryté vrstvy - PDF dokument může obsahovat více vrstev, které mohou být viditelné či nikoli. Po odstranění skrytých vrstev se tyto vrstvy odstraní a zbylé se se sloučí do jedné vrstvy
- Vložený index pro vyhledávání – urychluje hledání v souboru. Odstranění této položky se zmenší velikost dokumentu, ale prodlouží se doba jeho prohledávání
- Odstraněný nebo oříznutý obsah – soubory PDF v sobě někdy zachovají obsah, který byl odstraněn a není již viditelný. Například oříznuté nebo odstraněné stránky a obrazy
- Vazby, akce a JavaScript – jedná se o webové vazby, akce přidaní průvodcem akcí a kód JavaScriptu v dokumentu
- Objekty s přesahem – objekty, navzájem se přesahující, mohou být obrazy, vektorové grafiky, přechody nebo vzorky

Funkce prohledá dokument, pokud obsahuje některou z výše uvedených položek, je možné pomocí zaškrtávajícího pole vybrat položky, které mají být z dokumentu odstraněny. Po odebrání některé z položek jsou z dokumentu odebrány také digitální podpisy, rozšíření programu Adobe Reader, pracovní postupy a informace o dokumentech přidané aplikacemi jiných výrobců, než je Adobe. Po odstranění položek je dokument nutné uložit, aby došlo k aplikování změn v dokumentu.

### 4.4.2 Funkce Redigování

Redigování je označení pro proces trvalého odstranění pouze viditelného textu nebo grafiky z dokumentu. To je hlavní rozdíl oproti funkci Odstranit skryté informace, která dokáže odstraňovat i skryté informace. V programu Adobe Acrobat lze text k redigování vybrat ručně (Označit pro redigování), vyhledávat slova nebo slovní spojení automaticky (Hledat a odstranit text) nebo redigovat celé stránky dokumentu (Označit stránky k redigování). Po označení veškerého textu a zvolení Aplikovat redigování se veškerý odstraněný obsah nahrazen značkami pro redigování, které jsou ve výchozím nastavení černé rámečky. Vzhled značek pro redigování může uživatel libovolně nastavit. Může volit barvu výplně redigované oblasti, použít překrytí vlastním textem nebo nechat redigovanou oblast prázdnou.

# 5 Závěr

Bakalářská práce se zabývala možnostmi zabezpečení PDF dokumentů. V souladu s cílem práce byla představena technologie PDF, prozkoumány volně dostupné metody zabezpečení a následně otestována jejich spolehlivost. Následující řádky slouží k porovnání volně dostupných metod zabezpečení a doporučí čtenářům práce nejspolehlivější metodu zabezpečení dokumentů formátu PDF.

Z testovaných metod shledávám nejkritičtější metodu zabezpečení heslem typu uživatel. Při tomto zabezpečení dochází k omezení funkcionalit dokumentu. Pouhým okomentování přívěsu dokumentu, ve kterém je uložena informace o zabezpečení, dokáže program, napsaný k účelu prolomení tohoto zabezpečení, v řádu jednotek vteřin odstranit informace o zabezpečení a dokument přeuložit bez známek jakéhokoli omezení funkcionalit. Metody zabezpečení, kdy dochází k omezení přístupu k dokumentu, shledávám jako středně rizikové. Při použití velmi silného hesla může být prolomení zabezpečení skoro nemožné z důvodu časové náročnosti. Nejspolehlivější metodou zabezpečení se po testování jevila metoda zabezpečení pomocí certifikátu, která bez možnosti tisku nelze prolomit. Metoda zabezpečení certifikátem umožňuje i digitální podepisování dokumentů, tím se však tato práce nezabývá.

Triviální způsob zabezpečení dokumentů heslem je využitelný ke zpřístupnění dokumentu skupině uživatelům, jimž stačí sdělit heslo nebo jim omezit jen některé funkcionality dokumentu. Je třeba dbát ohled na možnosti napadení tohoto druhů zabezpečení. Při nutnosti povolení tisku dokumentů a zvolení velmi silného hesla, jehož prolomení by útočníkovi trvalo několik let, se však tento způsob jeví jako přijatelný. Příjemci dokumentu musejí ovšem počítat se sníženou komfortností vkládání hesla.

Bohužel, části zabezpečení pomocí metody Adobe LiveCycle Rights Management, nemohla být věnována větší část práce, jelikož není volně dostupná. Po nastudování materiálu je její využití zejména v korporátní sféře, kde je kladen vysoký důraz na utajení informací obsahující dokument a znemožnění jejich šíření.

Pro skrytí obsahu a citlivých informací uvnitř dokumentu je možno využít i nástroje pro to určené, které fungují spolehlivě. Redigování viditelného textu je praktické zejména pro odstraňování důvěrných informací zobrazených v textu, jimiž mohou být rodná čísla, adresy bydliště, telefonní čísla nebo čísla bankovních účtů.

Pro potřeby odstranit skryté informace o dokumentu, jeho autorovi, copyrightu, skrytého textu a dalších je v programech Adobe Acrobat integrované funkce Odstranit skryté informace.

V dnešní době považuji formát PDF za technologii, která dopomohla ke snazšímu publikování elektronických dokumentů, které nebylo do rozšíření formátu možné. Cíl práce byl dosažen díky nastudování literatury a vypracování praktické části.

Hlavními přínosy pro čtenáře této práce shledávám informovanost o volně dostupných metodách zabezpečení, nastínění jejich snadné a komfortní implementaci, prohloubení znalostí o struktuře a funkčnosti PDF dokumentů. Věřím, že vývojáři formátu PDF v budoucnu dokáží odstranit skulinky ve volně dostupných metodách zabezpečení.

# 6 Použité zdroje


1. Adobe Creative Team. *Adobe Acrobat 8.* Brno : Computer Press, a.s., 2008. ISBN 978-80-251-2002-6.

2. O Adobe PDF. *Adobe.* [Online] [Citace: 22. 1 2014.] http://www.adobe.com/cz/products/acrobat/adobepdf.html.

3. Whitington, John. *PDF Explained.* Sebastopol : O'Reilly Media,Inc., 2012. ISBN: 978-1-449-31002-8.

4. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 32000-1:2008.* [Online] [Citace: 22. Leden 2014.] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502.

5. Adobe Acrobat Engineering. *Adobe.* [Online] 8. 2 2014. http://acroeng.adobe.com/wp/?page_id=303 .

6. PDF Standards. *PlanetPDF.* [Online] [Citace: 29. 1 2014.] http://www.planetpdf.com/enterprise/article.asp?contentID=7877&rss.

7. Is PDF an open standard? *PlanetPDF.* [Online] [Citace: 28. 1 2014.] http://www.planetpdf.com/enterprise/article.asp?ContentID=Is_PDF_an_open_standard&page=1.

8. Quick overview of PDF file format. *Adobe.* [Online] [Citace: 28. 1 2014.] http://partners.adobe.com/public/developer/tips/topic_tip31.html.

9. Security. *Adobe.* [Online] [Citace: 3. 2 2014.] http://www.adobe.com/security/pdfs/acrobat_livecycle_security_wp.pdf.

10. A primer on electronic document security. *Adobe.* [Online] [Citace: 10. 2 2014.] http://www.adobe.com/security/pdfs/acrobat_livecycle_security_wp.pdf.

11. Přehled zabezpečení v aplikaci Acrobat a v dokumentech PDF. *Adobe.* [Online] [Citace: 2. 4 2014.] http://help.adobe.com/cs_CZ/acrobat/using/WSbba457e6030d283f-5b649469138c0a5cc00-8000.html.

12. Document Security for the Acrobat Family of Products. *Adobe.* [Online] [Citace: 4. 2 2014.] http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_Reader_SecurityMethods.pdf.

13. Steward, Sid. *PDF HACKS.* Sebastopol : O'Reilly Media, Inc., 2004. ISBN 0-596-00655-1.

14. PDF Security. *PDFlib.* [Online] [Citace: 5. 2 2014.] http://www.pdflib.com/knowledge-base/pdf-security/encryption/.

15. Zabezpečení dokumentů pomocí hesel. *Adobe.* [Online] [Citace: 5. 2 2014.] http://help.adobe.com/cs_CZ/acrobat/standard/using/WSD012A4E1-51D1-4bcd-BA9F-EF03C6F20BB6.html.

16. PDF Reference sixth edition. *Adobe.* [Online] [Citace: 5. 2 2014.] http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf.

17. Home. *PDF Descrypter Pro.* [Online] [Citace: 12. 2 2014.] http://www.pdfdecrypter.com.

18. A brief Sony password analysis. *troyhunt.com.* [Online] [Citace: 14. 2 2014.] http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

19. Advanced PDF Password Recovery. *Elcomsoft.* [Online] [Citace: 14. 2 2014.] K testování útoku hrubou silou byl použit program Advance PDF Password Recovery od společnosti Elcomsoft .

20. Padova a Padova, Ted. *Acrobat X PDF Bible.* Indianapolis : Wiley Publishing, Inc., 2011. ISBN 978-0-470-61291-0.

21. Digitální identifikátory. *Adobe.* [Online] [Citace: 7. 2 2014.] http://help.adobe.com/cs_CZ/acrobat/using/WS11dd809af63f0e1e-43e0464b12b4384d3b6-8000.html#WS3870a95df603bbc460dee4912fd5e1ec86-8000.

22. Adobe. *Adobe.* [Online] Zabezpečení PDF pomocí certifikátů. [Citace: 6. 2 2014.] http://help.adobe.com/cs_CZ/acrobat/using/WS58a04a822e3e50102bd615109794195ff-7d8b.w.html.

23. Product Downloads. *Foxit.* [Online] [Citace: 16. 2 2014.] http://www.foxitsoftware.com/downloads/.

24. A Brief History of Adobe LiveCycle. *blogs.adobe.com.* [Online] [Citace: 10. 2 2014.] http://blogs.adobe.com/livecycle/2008/04/a_brief_history_of_livecycle.html.

25. Adobe LiveCycle. *macron software.* [Online] [Citace: 10. 2 2014.] http://www.macronsoftware.cz/cz/produkty-technologie/livecycle/396/.

26. Zabezpečení PDF pomocí serveru Adobe LiveCycle Rights Management ES. *Adobe.* [Online] [Citace: 2. 10 2014.] http://help.adobe.com/cs_CZ/acrobat/using/WS58a04a822e3e50102bd615109794195ff-7d65.w.html.

27. Rights Management Portfolio. *Adobe.* [Online] [Citace: 23. 2 2014.] http://www.adobe.com/go/lc_rtsmgt.

28. Odstranění důvěrného obsahu z PD. *Adobe*. [Online] [Citace: 20. 2 2014.] http://helpx.adobe.com/cz/acrobat/using/removing-sensitive-content-pdfs.html#remove_hidden_information_options.