České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Tyrol** Martin

Studijní program: Softwarové technologie a management
Obor: Manažerská informatika

Název tématu:

Dlouhodobá archivace elektronických dokumentů

Pokyny pro vypracování:
1. Specifikace pojmu dlouhodobá archivace
2. Způsoby a možnosti dlouhodobé archivace
3. Analýza existujících řešení
4. Případová studie vhodného řešení s ohledem na legislativní požadavky

Seznam odborné literatury:
1. Cubr L.: Dlouhodobá ochrana digitálních dokumentů. Národní knihovna České republiky, 2010.
2. Peterka J.: Báječný svět elektrotechnického podpisu. CZ.NIC, 2011.

Vedoucí bakalářské práce: Ing. Pavel Náplava

Platnost zadání: do konce letního semestru 2014/2015

L.S.

Doc.Ing. Jaroslav Knápek, CSc.
vedoucí katedry

Prof.Ing. Pavel Ripka, CSc.
děkan

V Praze dne 10.2.2014

bakalářská práce

Dlouhodobá archivace elektronických dokumentů

Martin Tyrol

23. května 2014

Ing. Pavel Náplava

České vysoké učení technické v Praze
Fakulta elektrotechnická, Katedra ekonomiky, manažerství a humanitních věd

Poděkování

Rád bych zde poděkoval vedoucímu bakalářské práce Ing. Pavlu Naplávovi za jeho rady a čas, který mi věnoval při řešení dané problematiky. Dále děkuji všem respondentům, kteří mi poskytli potřebné informace. Děkuji i svým nejbližším za podporu v průběhu celého studia a při tvorbě bakalářské práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně, a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 23. 5. 2014 .....

Abstrakt

Bakalářská práce se zabývá dlouhodobou archivací dat. Teoretická část je věnována všem důležitým oblastem dlouhodobé archivace. Tyto oblasti zahrnují archivní formát PDF/A a zabezpečení dokumentů. Dále uvádí do problematiky legislativních a technických předpokladů pro zajištění archivace, jako jsou standardizované formáty a požadavky na digitální archiv.

Praktická část seznamuje se základními procesy v archivu. V případové studii analyzuje současnou a připravovanou evropskou legislativu. Na následném modelovém příkladu srovnává různé typy vedení archivace. V závěru je doporučen vhodný způsob archivace na základě vyhodnocení nákladů a vícekriteriální analýzy.

Klíčová slova

dlouhodobá archivace, legislativa, dlouhodobá čitelnost, přeshraniční uznávání, elektronická značka, elektronický podpis

Abstrakt

The bachelor thesis focuses on the long-term archiving. The theoretical part is devoted to all the important areas of long-term archiving. These areas include archival format PDF/A and document security. Also states to the problems of legal and technical preconditions for ensuring archiving, such as standardized formats and requirements for digital archive.

The practical part introduces the basic processes in the archive. The case study analyzes the current and forthcoming European legislation. At the next model example compares the different types of management archiving. In conclusion, it is recommended to use the archiving method based on cost evaluation and multi-criteria analysis.

Keywords

long-term archiving, legislation, long-term readability, cross-border recognition, electronic seal, electronic signature

Obsah

Zkratky

Zkratka	Vysvětlení
NDA	Národní digitální archiv
OAIS	Open Archival Information System
CCSDS	Consultative Committee for Space Data Systems
ETSI	European Telecommunications Standards Institute
UDO	Ultra Density Optical
LTV	Long Term Validation
SIP	Submission Information Package
AIP	Archival Information Package
DIP	Dissemination Information Package
PKI	Public Key Infrastructure
PDF	Portal Document Format
ISO	International Organization for Standardization
XMP	Extensible Metadata Platform
XML	Extensible Markup Language
CSV	Comma-separated values
RSA	Rivest-Shamir-Adleman
DSA	Digital Signature Algorithm
MD5	Message-Digest5
SHA	Secure Hash Algorithm
CRL	Certifikační revokační listy
ETSI	European Telecommunications Standards Institute
EU	Evropská unie
PAdES	PDF Advanced Electronic Signatures
XAdES	XML Advanced Electronic Signatures
CAdES	Cryptographic Message Syntax Advanced Electronic Signatures
SOA	Softwarově orientovaná architektura

Úvod

V dnešní době vzniká denně obrovské množství dat a velká část z nich je velmi důležitá. Jedná se o různé smlouvy, účetní doklady a podobně. Dokumenty vznikají nejen na počítači, ale nově i v mobilních telefonech a tabletech. Je nutné zajistit jejich čitelnost na desítky let nezávisle na úložišti.

Pokud chceme, aby je přijala státní správa nebo obstály u případného soudního sporu, potřebujeme zajistit, kdy který dokument vzniknul a zda nebyl pozměněn. Tato problematika je aktuální, a proto jsem si ji vybral jako téma bakalářské práce. Myslím si, že dnes je to veřejností neprávem opomíjená oblast. Věřím, že ukáži dlouhodobou elektronickou archivaci jako nezbytnou součást dnešní doby s ohledem na budoucnost.

Hlavními zdroji pro práci byly informace poskytovatelů dlouhodobé archivace. Tyto poskytovatele v České republice zmiňuji v kapitole 10 a popisuji jejich činnosti. Mezi další důležité zdroje, ze kterých jsem čerpal, jsou materiály Evropské komise, která formuje legislativou archivaci dat a jednotlivé technické normy.

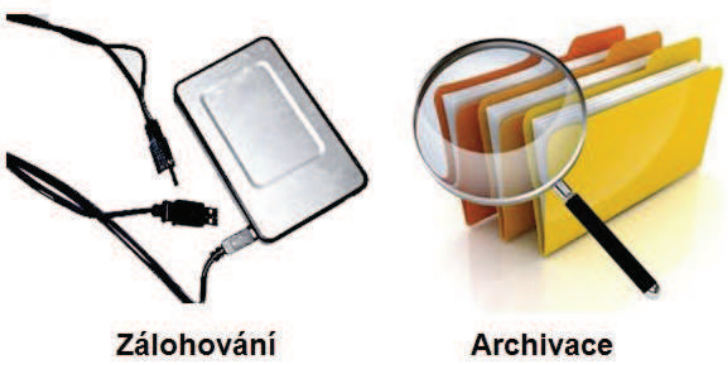
Bakalářskou práci jsem rozdělil na část teoretickou a praktickou, která obsahuje případovou studii.

Cílem teoretické části je seznámení se základními pojmy dlouhodobé archivace. Vysvětlím, jaké formáty je vhodné v archivaci používat, jaké jsou jejich jednotlivé verze. Popisuji legislativu, která vytváří podmínky pro jednotný způsob péče o archiválie.

Praktická část si klade dva cíle. Prvním cílem je v případové studii ukázat na třech modelových příkladech jejich finanční náklady. Protože není důležitá jen finanční stránka, obsahuje studie i vícekriteriální analýzu. Ta rozhoduje podle dalších parametrů. Tímto lze získat jasnou představu o výhodnosti jednotlivých variant. Druhým cílem praktické části je popsání rozdílů mezi současnou a připravovanou evropskou legislativou.

1. Rozdíl mezi archivací a zálohováním

Obrázek 1. Zálohování versus archivace. [1]



Společnosti generují obrovské množství dat. Jedním z řešení, jak se částečně ochránit proti lidské chybě, chybě hardwaru, či přírodní katastrofě, je zálohování. Protože existuje záložní kopie, situace je zachráněna. Příkladem můžou být účetní dokumenty, kde by bylo velmi bolestné o ně přijít.

Archivace a zálohování není to samé a často se tyto dva pojmy vzájemně prolínají a zaměňují. V nadcházející části jsou oba pojmy podrobněji popsány.

1.1. Zálohování dat

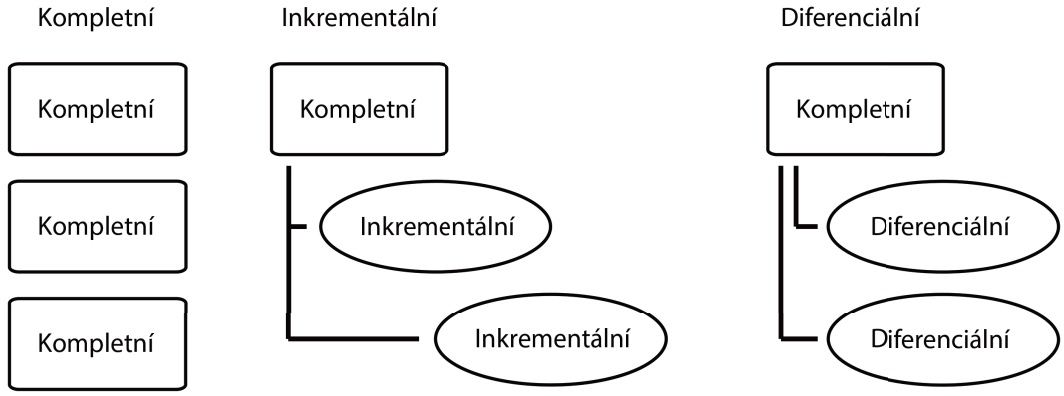
Důležitým rozdílem zálohování oproti archivaci je, že při zálohování vzniká kopie dat. Se zdrojovými daty se nic neděje. Záloha je navržena jako krátkodobé pojištění proti havárii. Archiválie (viz následující kapitola) je určena k použití i za několik dekád. Není přesně definovaný časový úsek, podle kterého by se rozhodovalo, zda je to zálohování nebo archivace.

Základní kritéria zálohování:

- Záloha musí být rychle přístupná. Jsou kladeny požadavky na rychlé čtení a zápis a také rychlost přístupu.
- Záloha by měla vydržet na daném médiu alespoň několik měsíců s důrazem na plnou integritu.
- Zálohu by mělo být možné rozdělit na několik médií (i různých), pro případ velkého objemu dat.

Existuje velké množství softwaru, který se zabývá automatickým zálohováním vybraných částí úložiště (či celého úložiště) v předem stanovený časový okamžik. Mezi další vlastnosti patří historie verzí dokumentů. Je tedy možné si prohlédnout například 5 posledních verzí dokumentu (záleží na nastavení).

Obrázek 2. Typy zálohování.[1]



Je několik typů možností zálohování (viz. obrázek 2):

- Kompletní – při každém zálohování se zálohují vždy všechna data, nevýhodou tohoto řešení je jeho náročnost na úložný prostor.
- Inkrementální – záloha se provádí pouze u těch dat, která byla modifikována od posledního provedení zálohování.
- Diferenciální – tento způsob je obdobou inkrementálního principu s tím rozdílem, že se zálohují všechna data od poslední kompletní zálohy.

Zálohování nevyžaduje žádné specifické požadavky na typ média, na které se bude ukládat. Je možné využít například cloudových úložišť nebo externích disků.

Pro zálohování je vhodné zvolit strategii, kdy jsou důležité zálohy umístěny fyzicky na odlišném místě, než kde je jejich zdroj. A to z důvodů možných požárů a přírodních katastrof.

1.2. Archivace dat

Archivace, často nazývaná jako dlouhodobá, je způsob dlouhodobého uložení dat. Příkladem archivace dat může být elektronická pošta, kde jsou důležité zprávy přesunuty do archivu. Oproti zálohování dat při archivaci obvykle není kladen důraz na možnost rychlé obnovy. Klíčovým požadavkem na archivaci je zajištění dlouhodobého uložení na a zajištění čitelnosti dokumentu na desítky let. Dále snadné a rychlé vyhledávání v archivu zajištěné pomocí indexace metadat. Rozdílem archivace oproti zálohování je fakt, že se zde používají formáty, které jsou přímo k dlouhodobé archivaci určené. Proprietární formáty (např. DOC) by za mnoho let nemusely být čitelné. Důvodem pro

[1] Obrázek vytvořil autor.

archivaci často bývá legislativa.

Základní požadavky na archivaci:

- Archiv pracuje s různými soubory, ale musí s nimi zacházet na stejné úrovni integrity.
- Nezáleží na rychlosti přístupu k archivu, ale záleží na velmi vysoké úrovni spolehlivosti a bezpečnosti.
- Kvalita médií.
- Sledování legislativy.

Aktuálně se data ukládají na magnetické disky a pásky. Vědci v laboratořích se snaží vyvinout způsob uložení dat do krystalu. To by znamenalo převrat v dlouhodobé archivaci, data by zde vydržela mnohem déle, než na současných médiích.

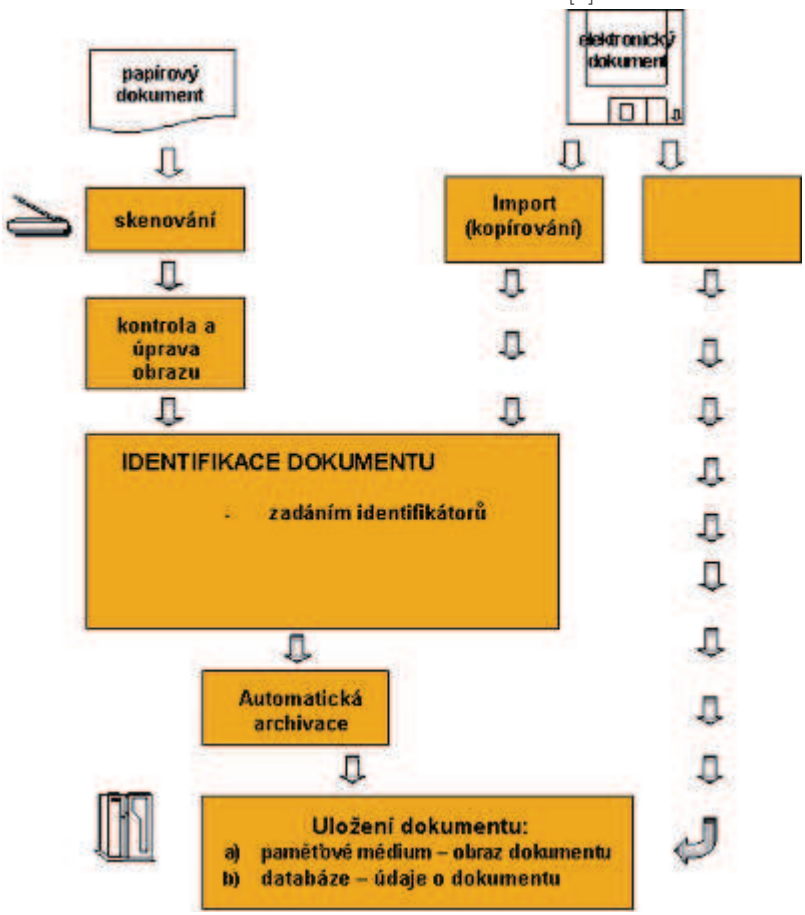
1.3. Shrnutí

Mezi archivací a zálohováním je rozdíl v rychlosti přístupu k datům, v chování k datům a jejich ukládání. Podrobné technické aspekty archivace jsou popsány v následujících kapitolách. Zálohováním se již dále nezabývám.

2. Archivace

Všechny důležité dokumenty je třeba archivovat. A jak znázorňuje zde zobrazený Obrázek 3, je jedno, zda se jedná o dokument analogový, či digitální. Analogové dokumenty je užitečné převést do digitální podoby. Následně s takto vytvořeným souborem budeme pracovat jako s běžnými digitálními daty.

Obrázek 3. Proces archivace. [2]



V dnešní době, kdy vzniká mnoho dat v elektronické podobě, je důležité se zabývat otázkou, jak je zabezpečit. A to tak, aby se daly přečíst v nezměněné podobě i za desítky a více let. Vývoj v oblasti počítačových technologiích jde velice rychle vpřed. Dokumenty vytvořené v určitém období, uložené na specifické médium, nemusíme být schopni za krátké období přečíst. Budou nová úložiště, která nebudou komunikovat s předchozími. To samé se týká systémů a programů. S těmito změnami souvisí zajištění bezpečnosti dokumentu, aby nebyl pozměněn a byl důvěryhodný.

Pro představu uvádím v následující tabulce druhy dokumentů a jejich délku archivace dle zákonů.

Tabulka 1. Příklady dokumentů a jejich archivační lhůty

Druh dokumentu	Počet let archivace
Stejnopisy evidenčních listů	3 roky
Účetní záznamy, kterými účetní jednotky dokládají formu vedení účetnictví	5 let
Účetní doklady	5 let
Účetní knihy	5 let
Odpisové plány	5 let
Inventurní soupisy	5 let
Účtový rozvrh	5 let
Pojistné na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti	10 let
Účetní uzávěrka	10 let
Výroční zpráva	10 let
Daňové doklady pro DPH	10 let
Mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění	30 let

Jak je vidět z tabulky 1 výše, jedním z mnoha příkladů je list důchodového zabezpečení. Ten musí být dle legislativy uchováván 30 let. U účetních dokladů je to 10 let. To jsou již lhůty, kdy vývoj v oblasti IT zajisté přinese mnoho novinek. Tedy další důvod zajistit dlouhodobou čitelnost. Mezi extrémní příklady patří zdravotnictví. U léčby duševních poruch je potřeba uchovávat zdravotnickou dokumentaci po dobu 100 let po narození. U pitevního protokolu, který slouží pro účely soudního lékařství, je doba stanovena na 150 let.

2.1. Archivování papírových dokumentů

Ještě v nedávné době bylo legislativou určeno, jaké všechny dokumenty je třeba archivovat v papírové podobě. Dnes již legislativa počítá s uchováváním v podobě digitální. Navzdory tomu, mnoho firem přesto stále uchovává data v papírově podobě. Důvodem jsou finanční náklady na zřízení digitálního archivu. Přes reálnou hrozbu sankcí ze strany úřadů za nevedení digitální archivace, se to v mnoha případech stále vyplatí. Příklady sankcí uvádím v podkapitole 2.2.

2.1.1. Specifika archivování papírových dokumentů

Nevýhodou archivování papírových dokumentů je náročnost na skladovací prostor. Šanony a kartotéky mají své rozměry, které se nedají upravit a určitou kapacitu v archivu zaberou. Při archivaci papírových dokumentů jsou kromě fyzického místa kladeny nároky na stálost prostředí (tedy teplota mezi 14 °C a 18 °C a vlhkost mezi 45 - 65 %). Dále musí být pečlivě vedeny záznamy o dokumentech, aby se dalo snadno najít, kde leží, z jakého data jsou a čeho se týkají. Výhodou archivace v papírové podobě je trvanlivost těchto archiválií. Po mnoha staletích používání pera a papíru je jasně dokázáno, že pokud archiválie nekoluje často z ruky do ruky, jako například v knihovně, má potenciál vydržet staletí. Tomuto nemůže konkurovat žádné médium. Optické disky a

magnetické disky vydrží řádově desítky let.

Určitý problém může nastat při archivování papírových dokumentů vytištěných na laserové tiskárně. Pokud je dokument skladován ve větším těžkém stohu, mohou se stránky slepit, písmenka se z povrchu papíru vytrhávají a nelze je přečíst. Tisk inkoustovou tiskárnou sice těmito nešvary netrpí, ale tato technologie má nedostatek v podobě malé odolnosti proti vlhkosti. Pozor i na barevný tisk, některé barvy jsou velmi nestabilní a snadno vyblednou.

2.1.2. Sankce za nesprávné archivování

Dojde-li ke zničení dokladů např. při požáru či povodni a doklady není možné již nahradit, je třeba tuto nepříjemnost u dokumentů, kterých se to týká, oznámit finančnímu úřadu. A určitě neopomenout pohromu doložit příslušnou dokumentací od policie. Pokud podnikatel nedodržuje archivaci dokumentů podle příslušných zákonů, hrozí mu pokuta až do hodnoty 3 % aktiv podniku. Stejně tak hrozí sankce pro firmy zapsané v obchodním rejstříku.

Při nedodržení zákonných lhůt nebo při celkové absenci uchovávání archiválií dochází k porušení předpisů a k pokutám.

- Při neuchovávání dokumentů hrozí pokuta až 5 000 Kč.
- Při neposkytnutí údajů státnímu archivu pro vedení evidence archiválií hrozí pokuta až 50 000 Kč.
- Při řádném nepečování o archiválie, jejich poškození, znehodnocení, ztrátě a odcizení, může být uložena pokuta až 100 000 Kč.
- Při zničení dokumentů bez souhlasu příslušného veřejného archivu, může být uložena pokuta až do výše 250 000 Kč.

Pro velké podniky se často finančně vyplatí nemít archiv a místo toho pravidelně platit výše uvedené sankce.

2.2. Shrnutí

Zde jsem vysvětlil, proč je důležitá archivace. Dále jsem popsal a v tabulce 1 více uvedl přehled daných lhůt pro archivaci vybraných dokumentů. Následoval krátký popis archivace papírových, dokumentů. A nyní bude následovat dlouhodobá digitální archivace a vše související s touto problematikou.

3. Dlouhodobá digitální archivace

Podkapitoly, které budou následovat, se zabývají formátem, do jakého je potřeba ukládat dokumenty. A co vše k nim přiložit pro dlouhodobou digitální archivaci. Popisuji metadata, tedy „data o datech“, která se přikládají k dokumentům. Následně rozebírám formát PDF/A, který je dnes považován za nejdůležitější formát v oblasti digitální archivace. Tento formát je obsažen v ISO normě[1] a má aktuálně 3 verze, každá z nich je dále blíže dělena podle úrovně shody s ISO normou.

3.1. Požadavky na elektronická data

I v dobách bez dnešní moderní techniky vznikala spousta papírových dokumentů, které bylo potřeba archivovat (např. účetní údaje). Všechny tyto listinné dokumenty vyžadovaly zkontrolování, správné uložení a péči. Tyto kroky jsou důležité, aby se dal dokument v budoucnu přečíst.

Archivace elektronických dokumentů z této analogie vychází, ale přidává i své vlastní požadavky. Ve výsledku musí být splněna tato kritéria:

- Použít otevřený formát a mít možnost dokument kdykoliv zobrazit.
- Zajistit nezávislost na úložišti.
- Zajistit nezpochybnitelný důkaz, že dokument nebyl pozměněn.
- Zajistit nezpochybnitelný důkaz, že dokument je pravý, čili ověřit podpisy.
- Dodržení platné legislativy, která stanoví jak provést výše uvedené body.

3.2. Metadata

Metadata jsou doprovodné informace o daném elektronickém dokumentu. Slouží k indexaci a vyhledávání. Zařazují dokument do časového kontextu. Mohou obsahovat informace o podpisu, konfiguraci, způsobu zpracování, využití a další informace. Metadata se dále dělí do kategorií podle kritérií na popisná, strukturální a administrativní.

3.2.1. Popisná metadata

Popisují dokument, čili jeho název, autora a typ, kategorii a další. Tento popis slouží k následnému určení, kam dokument zařadit.

[1] ISO 19005

Rozlišujeme několik typů popisných metadat:

- MARC (Machine Readable Cataloguing)[2] – umožňuje strojové zpracování a výměnu. Existují další specifikace této verze, např. mezinárodní formát MARC21. Metadata jsou uchována ve formátu XML MARCXML.

- MODS (Metadata Object Description Software)[3] – kompromisní formát mezi složitým MARC a jednoduchým DC. Klade důraz na popis digitálních zdrojů.

- DC (Dublin Core)[4] – jednoduchý, ale dostatečně rozsáhlý formát. Obsahuje 15 základních metadat prvků.

- TEI (Text Encoding Iniciative)[5] – formát v XML struktuře vhodný pro uchovávání a výměnu textových dokumentů v digitální podobě.

- VRA CORE (Visual Record Association)[6] – standard pro popis uměleckých předmětů a audiovizuálních dokumentů.

3.2.2. Strukturální metadata

Strukturální metadata popisují fyzickou a logickou strukturu digitálních zdrojů. Sdružují všechny části do logického celku a ukazují logickou provázanost jednotlivých dat a metadat.

3.2.3. Administrativní metadata

Administrativní metadata jsou technické údaje o digitálních objektech nebo právech a událostech, která se k nim vztahují. Jejich obsahem jsou informace o formátu, jsou zde zaznamenány změny provedené na obsahu dokumentu.

[2] http://www.loc.gov/marc/
[3] http://www.loc.gov/standards/mods/
[4] http://dublincore.org/
[5] http://www.tei-c.org/index.xml
[6] http://www.vraweb.org/projects/vracore3/

3.3. Normalizovaný formát PDF/A

Formát PDF/A je omezená verze formátu PDF (Portal Document Format), vyvinuta firmou Adobe Systems Inc. pro dlouhodobé ukládání dokumentů. Vlastností tohoto formátu je umožnění otevřít daný dokument v budoucích verzích softwarových nástrojů. A to beze ztráty jakékoliv informace, s jistotou zcela správného zobrazení, včetně odstínů barev.

Obrázek 4 znázorňuje, jak lze s tímto formátem jednoduše pracovat.

Obrázek 4. PDF/A [3]

Formát PDF/A má tři verze. Starší PDF/A-1, která je vydána v rámci standardů ISO, konkrétně ISO 19005-1:2005 a novější verze, PDF/A-2 ve standardu ISO 19005-2:2011 a PDF/A-3 obsažená v ISO 19005-3:2012.

Co se týče metadat, tak je zde požadavek, aby byla uložena ve formátu XMP a přiložena k souboru. Norma dále popisuje způsob omezení přístupu k některým informacím uvnitř dat. Je zakázáno použití šifrování a ochranu heslem, vše je potřeba řešit vně vlastního dokumentu. Další nespornou výhodou formátu je jeho zpětná kompatibilita v prohlížečích.

Je nutné zdůraznit, že tato norma nedefinuje strategii archivování ani požadavky na archivační systém. Jednoznačně nejkomplexnější používaný software je přímo od tvůrce

specifikace normy, společnosti Adobe, pojmenovaný Adobe Acrobat Pro.

3.3.1. Omezení PDF/A

Ve formátu PDF/A je řada omezení obsahu na rozdíl od klasického formátu PDF. Jsou zde zakázány spustitelné soubory, audio a video formáty. Dalším omezením je zákaz kódování. Veškeré fonty použité v dokumentu musí být legálně neomezené a musí být do daného dokumentu vloženy. Stejně tak je nutné, aby zde byly vloženy informace o použitém barevném profilu.

První dva standardy byly navrženy převážně podle požadavků profesionálních archivářů. Nejnovější, třetí, standard bere v potaz požadavky vlád, knihoven a byznysu.

3.3.2. PDF/A-1

Tato specifikace byla vydána v roce 2005 a je založena na verzi PDF 1.4 a obsahuje dvě úrovně: PDF/A-1a a PDF/A-1b.

- PDF/A-1b zajišťuje dlouhodobou reprodukovatelnost a korektní zobrazení, ale nezaručuje srozumitelnost a čitelnost. Tuto verzi jsem schválně zařadil na první místo, i když se to může dle pořadí písmen v abecedě zdát zvláštní. Tím důvodem je fakt, že verze s písmenem ‚b‘ je označovaná jako základní.

- PDF/A-1a je specifikace, která rozšiřuje specifikaci 1b o následující vlastnosti. Zaručuje, že text v dokumentu bude čten v přirozeném pořadí na všech zařízeních. Vyžaduje znakovou sadu Unicode. Vlastnost, kdy jsou v PDF dokumentu obsaženy metainformace, se označuje jako 'Tagged PDF'. Díky nim je pak možné rozlišit jednotlivé odstavce dokumentu, nadpisy, anotace, ap. Znalost struktury dokumentu umožňuje jeho přeformátování. To je výhodné pro čtení PDF slabozrakými lidmi nebo na obrazovkách menších zařízení, jako jsou mobilní telefony a tablety.

3.3.3. PDF/A-2

Specifikace je z roku 2011, obsahuje plnou kompatibilitu s verzí PDF/A-1, ale ne zpětnou. Standard je založen na verzi PDF 1.7, definovaný v ISO 32000-1. Je zde řada vylepšení od verze 1 formátu PDF/A. Konkrétně se jedná o podporu elektronického podpisu podle specifikace PAdES a také o možnost vložení více PDF/A souborů do formátu PDF/A-2. Tímto způsobem lze následně zálohovat vše do jednoho PDF/A souboru. Oproti verzi PDF/A-1 je zde povolena obrazová komprese JPEG2000. Tato norma obsahuje tři úrovně: PDF/A-2a, PDF/A-2b a PDF/A-2u.

- PDF/A-2a odpovídá plné ISO 19005-2 specifikaci.

- PDF/A-2b podobně jako PDF/A-1b poskytuje pouze nezbytný základ normy.

- PDF/A-2u rozšiřuje předchozí úroveň o požadavek mapovat všechny znaky v Unicode sadě.

3.3.4. PDF/A-3

Nejnovější specifikace z října roku 2012, založena na verzi PDF 1.7, definované v ISO 32000-1, přinesla pomyslnou revoluci v možnostech vložení dalších formátů do jednoho PDF/A dokumentu. Tato novinka umožňuje vložit libovolný formát, jako je např. XML, CAD, CSV do archivujícího formátu PDF/A, a vytvořit tak komplexní archivní objekt. Možným nebezpečím tohoto nového standardu je zneužití od uživatelů, kteří do PDF/A dokumentu přiloží například různé archivační balíčky (např. ZIP, TAR). Tím by se ztratil potenciál dlouhodobé udržitelnosti a také větší rozšířenost u široké veřejnosti. Je doporučeno přibalovat pouze mezinárodně standardizované formáty.

Podobně jako předchozí norma, obsahuje ta aktuální také tři úrovně: PDF/A-3a, PDF/A-3b, PDF/A-3u.

- PDF/A-3a odpovídá plné ISO 19005-3 specifikaci.
- PDF/A-3b splňuje nezbytný základ normy, ale nemusí obsahovat podrobnější informace.
- PDF/A-3u rozšiřuje předchozí úroveň o požadavek mapovat všechny znaky v Unicode sadě.

3.4. Shrnutí

Na předchozích řádcích jsem popsal, co jsou metadata, jak je dělíme a co všechno obsahují. Dále jsem se zabýval popisem archivačního formátu PDF/A a jeho tří specifikací. Každá z těchto specifikací má ještě vlastní detaily, podle kterých se dělí.

Následuje úvod do kryptografických algoritmů. Jejich znalost využijeme v zabezpečením PDF/A dokumentů všech specifikací elektronickým podpisem a časovým razítkem.

4. Kryptografické algoritmy

Kryptografické algoritmy popisují dva způsoby použití:

- Jak ze zprávy a klíče vytvořit šifru.
- Jak ze šifry a klíče rekonstruovat zprávu.

Tyto algoritmy se dělí na symetrické a asymetrické. Celá tato kapitola slouží pro pochopení digitálních podpisů a zabezpečení dokumentů, které zmiňuji v kapitole 5.

4.1. Symetrická šifra

Symetrické šifrování znamená, že se jak k šifrování, tak dešifrování dat používá jeden sdílený klíč. Což je problém, protože jej lze snadno odposlechnout. Symetrické šifry jsou rychlejší a jednodušší než asymetrické.

Symetrické šifry se dále dělí na dvě kategorie:

- Proudové šifry - šifrování zde probíhá postupně bit po bitu. Každý bit je tedy zvlášť zašifrován a následně zvlášť dešifrován. Až po kompletním rozšifrování je složen do původní podoby.
- Blokové šifry - jedná se o rozšířenější šifrování, které výchozí bitový sled rozdělí na bitová slova a ty poté doplní bitovou šifrou, tak aby měla všechna slova stejnou velikost.

Můžeme uvést příklad: Alice chce mluvit s Bobem. Zpráva, kterou mu chce poslat, je důvěrná a Alice nechce, aby si ji mohl přečíst někdo jiný kromě Boba. Alice tedy použije k zašifrování původní zprávy klíč. Šifrovaná zpráva je odeslána Bobovi, který zná klíč a použitou symetrickou šifru. Jen díky tomu je Bob schopen zprávu dešifrovat a přečíst.

4.2. Asymetrická šifra

Asymetrické šifry používají klíče dva – soukromý a veřejný. Veřejný klíč je dostupný každému a soukromý zná pouze vlastník klíče. Pokud je zpráva zašifrována veřejným klíčem, lze ji dešifrovat pouze pomocí odpovídajícího soukromého klíče. Z veřejného klíče nelze žádným způsobem odvodit klíč soukromý.

Asymetrické šifrování řeší problém s předáváním klíčů. Alici stačí vzít Bobův veřejný klíč a použít ho k šifrování zpráv. Bob je totiž jediný, kdo vlastní odpovídající soukromý klíč, a tím pádem je také jediný, kdo si může původní zprávu přečíst.

Ve srovnání se symetrickými šiframi jsou asymetrické šifry pomalé, a proto se většinou používají pouze k distribuci symetrického klíče. Alice a Bob pak mohou používat pouze symetrický klíč a nemusejí mít strach o důvěrnost svých zpráv.

4.3. Hashovací funkce

Je to transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je pak řetězec znaků s pevnou délkou, tzv. otisk. Je důležitou součástí kryptografických systémů pro digitální podpisy.

Každý hashovací algoritmus generuje otisk o určité délce. Tato délka je pevná, takže nezávisí na vstupní délce textu. Z hlediska bezpečnosti se doporučuje používat hashovací algoritmy, které mají výstup 160 a více bitů. Pokud bychom ve zprávě změnili byť jen jediné písmeno, tak dostaneme na výstupu úplně jiný obraz.

Kvalitní hashovací funkce musí splňovat tyto vlastnosti:

- Jednosměrnost - každá hashovací funkce musí být jednosměrná, neexistuje k ní inverzní algoritmus. K otisku nelze v časově omezeném úseku jednoznačně najít text, z kterého byl tento otisk vypočítán. Například certifikáty ke kvalifikovaným elektronickým podpisům jsou zpravidla vydávány s platností omezenou na rok. To už je časově omezený úsek.

- Bezkoliznost slabá – protože hashovacích algoritmů je malé množství a na druhou stranu existuje obrovské množství zpráv se stejným otiskem, existuje mnoho kolizí. V rozumném čase nesmíme být schopni k jednomu textu, u kterého známe i otisk, nalézt druhý text, který bude mít stejný otisk. Pro dané x nelze nalézt druhý argument $x \neq x'$, přičemž platí $h(x) = h(x') = y$.

- Bezkoliznost silná – také bychom neměli být schopni v rozumném čase nalézt jakékoliv dva různé texty se stejným otiskem. Od slabé bezkoliznosti se liší tím, že zde je hodnota x volena libovolně. To znamená, že v tomto případě si útočník může volit x i x' s jediným cílem, aby se obě x hashovaly na jednu hodnotu.

Jako příklady hashovacích funkcí jsou:

- Již nedoporučovaný SHA-1 s délkou 160 bitů.

- Aktuálně používaný SHA-2, algoritmy mají délku v bitech podle svého čísla za pomlčkou: SHA-224, SHA-256, SHA-384 a SHA-512.

- MD5, který již také není doporučován, délku má 128 bitů.

4.4. Shrnutí

Algoritmus SHA-2 není podporován ve verzích OS Microsoft Windows XP SP2 a nižší. A v nižších verzích než Microsoft Windows 2003 server.

Pro vytvoření digitálního podpisu se používají asymetrické kryptografické algoritmy s veřejným klíčem, nejčastěji RSA a DSA. DSA je pomalejší při podepisování než RSA, je však mnohem rychlejší při ověřování podpisu. Zde získané znalosti kryptografických algoritmů využijeme v následující kapitole 5, která se mimo jiné zabývá elektronickým podpisem.

5. Zabezpečení dokumentů

Tato kapitola se zabývá zabezpečením dokumentů. Základním prvkem je mít podepsaný dokument elektronickým podpisem. S touto problematikou souvisí infrastruktura veřejných klíčů a časové razítko.

5.1. Elektronický podpis

Elektronický podpis je ekvivalentem vlastnoručního podpisu na dokumentu. Elektronický podpis může vytvářet pouze konkrétní fyzická osoba jako aktivní projev své svobodné vůle. V počítačovém prostředí je jedním z hlavních nástrojů identifikace a autentizace osob. Tento podpis slouží k ověřování autenticity, tedy ověření daného subjektu, kterému elektronický podpis patří. Dále umožňuje ověřit integritu. Tím se rozumí, že podepsaný dokument nebyl pozměněn, či poškozen.

Podpis musí být zabezpečený šifrovacím algoritmem, dříve se používaly RSA, DSA, MD5, SHA. Od 1. ledna 2011 Ministerstvo vnitra České republiky doporučuje v oblasti časových razítek a podpisů používat algoritmus SHA-2. Mezi důležité součásti patří i zneplatnění certifikátů. Tato problematika je prodiskutována v části 5.5.

5.2. Elektronická značka

Firma, či jiná právnická osoba se nemůže vlastnoručně podepsat. Pokaždé to musí udělat fyzická osoba jednající jménem konkrétní právnické osoby, například její jednatel. Podobně to je s elektronickým podpisem, který patří pouze fyzické osobě, nemůže být tedy použit pro podepisování samotné firmy, ale pouze jejího zástupce. Tento problém řeší elektronická značka. Po věcné stránce se neliší od elektronického podpisu. Používá se zde soukromý a veřejný klíč za použití stejných postupů a metod při podepisování a ověřování dokumentů. Rozdíl nastává v právní stránce. Používá se tzv. kvalifikovaný systémový certifikát, který lze vydat jak fyzické osobě, tak i osobě právnické. Další rozdíl je v terminologii. Místo podepisování se zde zavádí pojem označování a místo podepisující osoby je nový pojem, označující osoba. A protože u elektronických značek probíhá označování strojově, je odstraněn předpoklad, že se označující osoba seznámila s obsahem toho, co označuje. Lze tedy značku přirovnat k otisku razítka. Příkladem může být například datová zpráva odeslaná organizační složkou státu.

Elektronické značky podle zákona[4], jsou značky, které splňují následující požadavky:

- Jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu.

- Byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou.

- Jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

5.3. Časové razítko

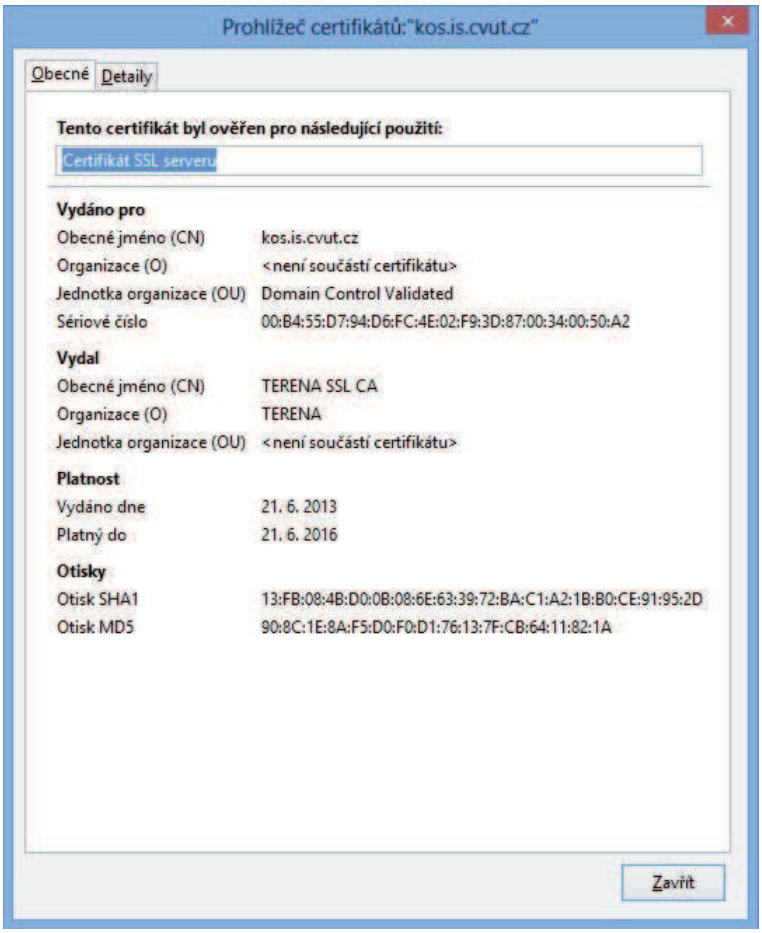
Chceme-li důvěryhodný dokument, musíme jej opatřit elektronickým podpisem. Každý elektronický podpis obsahuje informaci o datu a čase zhotovení. Tento údaj je ale zaznamenán na základě systémového času zařízení, na kterém je vytvořen. Tento lehce zneužitelný údaj vedl k zavedení časového razítka. To umožňuje prokázat nezměněnost dokumentu od vydání časového razítka. Tato technologie má podobně jako elektronický podpis omezenou platnost (minimálně 5 let). Je tedy třeba dokument ještě před vypršením platnosti razítka opatřit razítkem novým. Tím je prokazatelně zaručeno, že po dobu existence řady razítek nebyl dokument změněn a že existoval. Celý tento proces je názorně ukázán na obrázku 5.

Obrázek 5. Princip tvorby důvěryhodného dokumentu. [5]

5.4. Elektronický certifikát a jeho možnosti využití

Elektronický certifikát je digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita. Obrázek 6 zobrazuje, jak takový certifikát vypadá v internetovém prohlížeči Internet Explorer 11. Jsou zde také uloženy informace o identifikačních údajích podepsané osoby, identifikace vydavatele certifikátu, jednoznačné sériové číslo certifikátu, doba platnosti a další údaje.

Obrázek 6. Elektronický certifikát.[1]



5.4.1. Kvalifikovaný elektronický certifikát

Je to certifikát, který odpovídá zákonu o elektronickém podpisu [4] a byl vydán poskytovatelem certifikačních služeb.

Certifikát musí obsahovat:

- Označení, že je vydán jako kvalifikovaný certifikát podle zákona. [4]
- Jméno, data pro ověření podpisu.

[1] Obrázek vytvořil autor.

- Začátek a konec platnosti certifikátu.
- Elektronickou značku poskytovatele certifikačních služeb.

Tyto certifikáty jsou určeny výhradně pro elektronické podepisování (nikoliv například pro šifrování). Kvalifikovaný elektronický podpis zajišťuje integritu a autenticitu dat. Pro oficiální komunikaci se subjekty státní správy, pojišťoven apod. je zapotřebí právě tento certifikát, který byl vydán kvalifikovanou certifikační autoritou. Bezpečnost a důvěryhodnost těchto certifikačních autorit je kontrolována a standardizována příslušnými úřady.

Certifikát vydaný certifikační autoritou má předem dané případy použití:

- Slouží pro bezpečné ověření elektronických podpisů.
- Využití při elektronické archivaci dokumentů.
- Odesílat datové zprávy, podávání daňových přiznání.
- Elektronická komunikace se státní správou.

5.4.2. Komerční elektronický certifikát

Komerční certifikát je takový certifikát, který není spjat se zákonem o elektronickém podpisu a nemusí tedy splňovat náležitosti tohoto zákona. Certifikát vydává certifikační autorita podle vlastních směrnic a podmínek. Je na dané certifikační autoritě jaké si stanoví podmínky. Komerční certifikáty mají široké uplatnění. Ať už se jedná o šifrování e-mailů, zajištění autentizace či k elektronickému podepisování zpráv. Komunikující strany musí však obě důvěřovat dané certifikační autoritě.

5.5. Odvolání platnosti certifikátu

Každý certifikát lze zneplatnit ještě dříve, než mu skončí doba platnosti u příslušné certifikační autority, která si vede seznam zneplatněných certifikátů, tzv. revokačních listů (CRL). Důvodem nejčastěji bývá změna údajů. Dále ohrožení privátního klíče, které může být způsobeno odcizením klíče. Častým případem je také skutečnost, kdy je zpochybněna důvěryhodnost držitele.

Revokační listy se vydávají z důvodu, že nejde všechny tyto certifikáty stáhnout z oběhu, protože není možné dohledat všechny exempláře.

Z dříve vydaného certifikátu nelze poznat, zda byl odvolán. Proto je nutné sledovat aktuální vydané CRL seznamy.

5.6. Zaručený elektronický podpis

Zaručený elektronický podpis jsou digitální data, která podepisující osoba vytváří pomocí svého privátního klíče. Zajišťuje jimi integritu a nepopiratelnost původu podepsaných dat. Pro každý jednotlivý dokument se podpis odvozuje zvlášť.

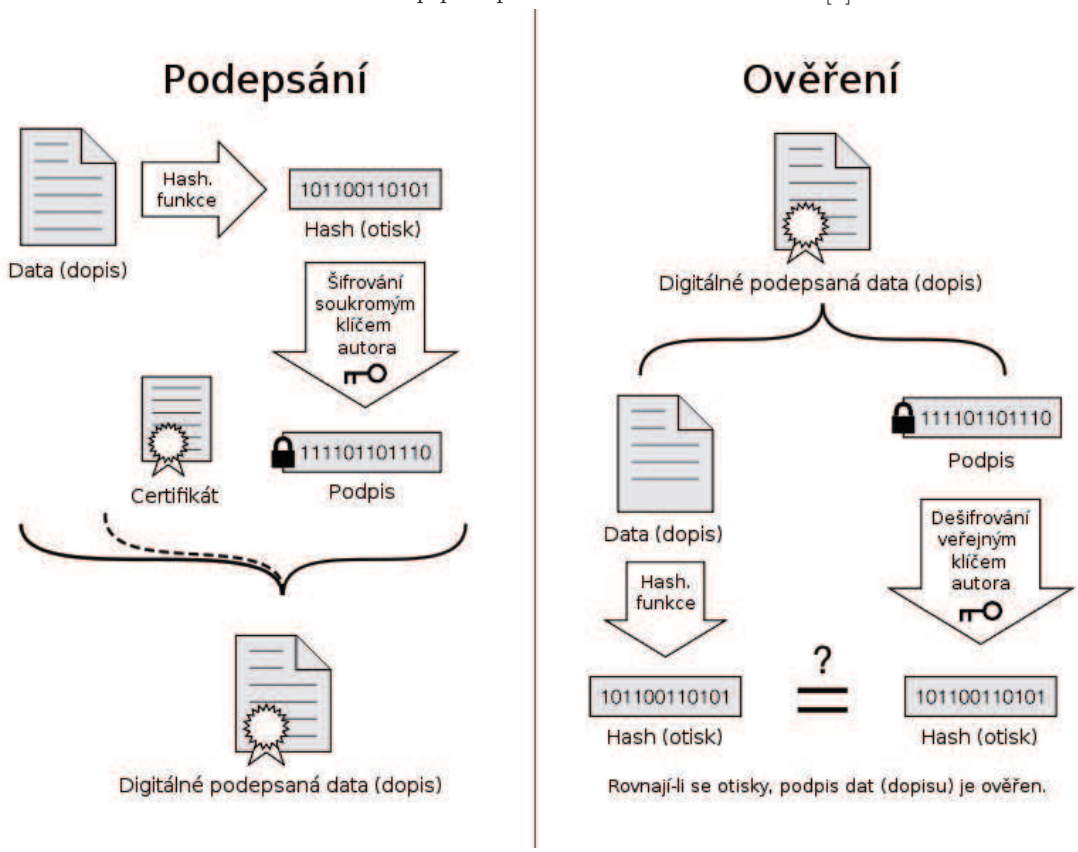
Dle zákona o elektronickém podpisu [4] je zaručený elektronický podpis definován jako podpis, který splňuje tyto požadavky:

- Je jednoznačně spojen s podepisující osobou.
- Umožňuje zjistit totožnost podepisující osoby.
- Byl vytvořen pomocí prostředků, které může podepisující osoba udržet plně pod svou kontrolou.
- Je spojen s daty tak, aby bylo možné zjistit jakoukoliv změnu těchto dat.

5.7. Realizace elektronického podpisu

Jak znázorňuje Obrázek 7, realizace podepsání dokumentu se provede následovně: Nad vybraným dokumentem se vypočte hash (otisk) dokumentu, ten se zašifruje pomocí privátního klíče. Příjemci se odešle samotný dokument, certifikát a vytvořený hash. Příjemce následně vytvoří vlastní hash dokumentu a ten porovná s tím, který mu byl poslán. Jejich porovnáním zjistí, zda se skutečně jedná o dokument, který odesílatel podepsal.

Obrázek 7. Princip podepsání a ověření dokumentu. [6]

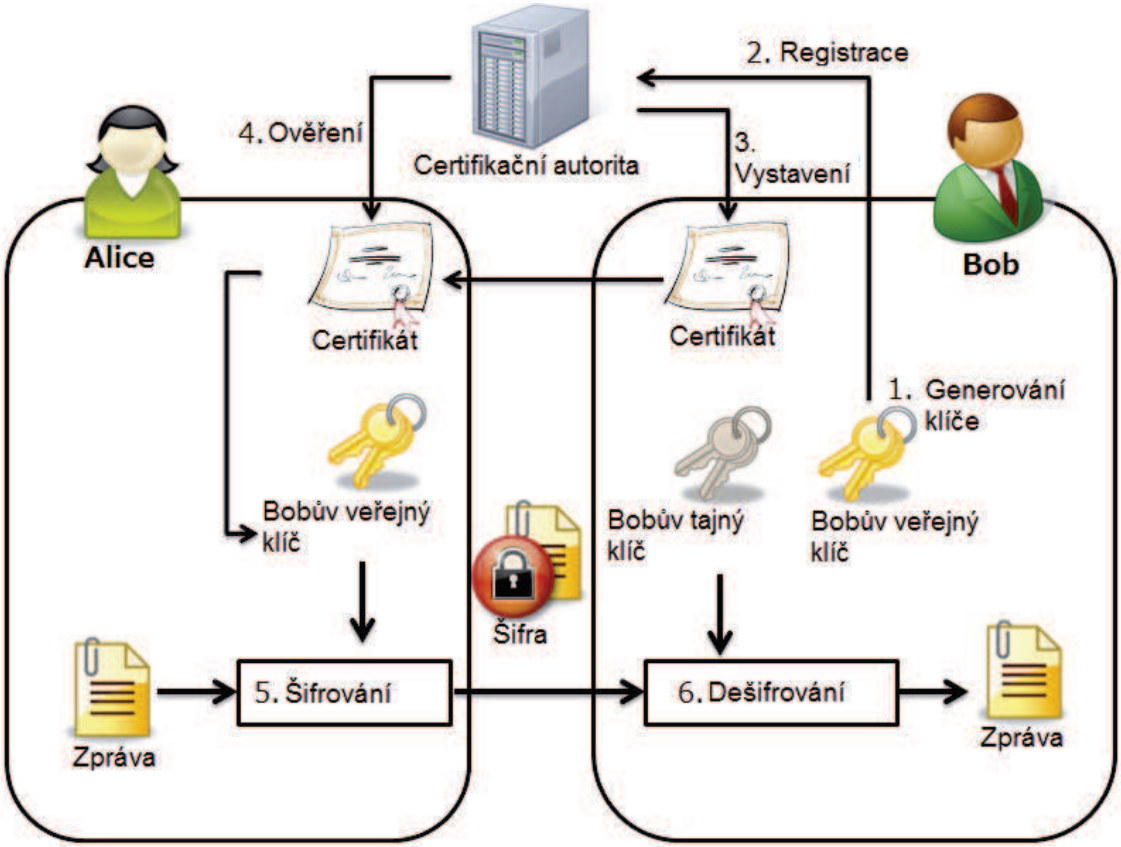


5.8. Infrastruktura veřejných klíčů

Infrastruktura veřejných klíčů, anglicky Public Key Infrastructure (PKI) je soubor organizačních a technologických nástrojů dovolující používat šifrování pomocí veřejných klíčů. Celý průběh infrastruktury je na obrázku 8. PKI umožňuje uživatelům v nezabezpečené veřejné síti si bezpečně vyměňovat data prostřednictvím použití privátního a veřejného klíče. Tento pár klíčů je získán a sdílen prostřednictvím důvěryhodné autority.

PKI poskytuje digitální certifikát, jehož prostřednictvím lze identifikovat jednotlivce nebo celé organizace. Spojuje v sobě řadu komponent - digitální certifikáty, klíče, asymetrickou kryptografii, certifikační autority a aplikace do celkové sítě bezpečnostní architektury.

Obrázek 8. Public Key Infrastructure – průběh.[7]



PKI ochraňuje informace několika následujícími způsoby:

- Prověření integrity zprávy.
- Autentizace přístupu.
- Nepopiratelnost transakce pomocí elektronického podpisu.
- Zajištění privátnosti zprávy při transportu skrz síť pomocí kombinace symetrických a asymetrických šifer.

Základní funkce PKI je:

- Vydávání certifikátů k veřejným klíčům.
- Odvolávání platnosti certifikátů.
- Vytváření a zveřejňování seznamu certifikátů.
- Vytváření a zveřejňování zneplatněných certifikátů v seznamu CRL.
- Správa klíčů po dobu jejich platnosti.

5.9. Standard X.509

Standard X.509 je jedním z nejpoužívanějších typů certifikátů. Formát certifikátu je popsán normou RFC 2459 a doporučením ITU X.509. Certifikát je datová struktura popsaná v jazyce ASN.1 a pro přenos je kódovaná podle specifikace DER (Distinguished Encoding Rules).

Certifikát obsahuje položky:

- Sériové číslo certifikátu.
- Identifikace algoritmu.
  - Název algoritmu asymetrického.
  - Název jednocestného algoritmu.
  - Délka klíče.
- Identifikace certifikační autority.
- Platnost certifikátu (od - do).
- Identifikace vlastníka certifikátu.
- Veřejný klíč, pro který je certifikát vydán.
- Digitální podpis certifikační autority.

5.10. Certifikační autorita

Certifikační autorita je subjekt, který vydává certifikáty. Svojí autoritou potvrzuje pravdivost údajů, které jsou uvedeny ve veřejném klíči držitele. Dochází k principu přenosu důvěry. Můžeme důvěřovat údajům uvedeným v certifikátu, pokud důvěřujeme certifikační autoritě. Při žádosti o vydání certifikátu u certifikační autority je potřeba u

fyzických osob prokázat se občanským průkazem a u právnických osob předložením výpisu z obchodního rejstříku. Seznam certifikačních autorit, které mohou vydávat certifikáty v České republice, zveřejňuje Ministerstvo vnitra.

5.11. Shrnutí

Pro zajištění integrity dokumentu je potřeba dokumenty opatřit elektronickým podpisem. Nevýhodou elektronického podpisu je, že se používá systémový čas stroje, na kterém je dokument podepisován. Je tedy možné uvádět nepřesný okamžik. Tomuto se snaží zabránit časové razítko. Tyto technologie společně s PKI umožňují elektronickou archivaci dokumentů, na základě platné legislativy, kterou zmiňuji v kapitole 6.

6. Legislativa

Legislativa byla zavedena z důvodu sjednocení pravidel mezi institucemi a firmami. Každý dokument, který bude určen k dlouhodobému archivování, musí mít zajištěno, že ho bude možné přečíst v nezměněné podobě za mnoho let. A to i s odlišných hardwarovým a programovým vybavením.

Nejdříve je zde uvedena česká legislativa a poté legislativa evropská, kterou Česká republika postupně na doporučení Evropská komise přijímá. V rámci evropských standardů jsou důležité normy od ETSI z rodiny AdES, které se zabývají zacházením s podpisy. V kapitole 12 jsem provedl analýzu současné směrnice 1999/93/EC a připravovaného nařízení o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu.

6.1. Česká legislativa

Oblast dlouhodobé archivace dokumentů je vytyčena několika českými zákony a vyhláškami. Zde zmiňuji ty nejdůležitější, celý přehled je uveden v Příloze A.

- Vyhláška č. č.118/1974 Sb., o podnikových archivech. Tato vyhláška mimo jiné v §7 určuje povinnost zřídit podnikový archiv nejpozději do pěti let od zahájení činnosti.

- Vyhláška č. 117/1974 Sb. Tato vyhláška stanovuje podmínky a pravidla posuzování dokumentů jako archiválie a definuje také podrobnosti skartačního řízení.

- Zákon č. 563/1991 Sb., o účetnictví, který definuje dobu a podmínky ukládání účetních záznamů.

- Zákon č. 499/2004 Sb., o archivnictví a spisové službě.

- Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě.

Tato potřebná legislativa byla zavedena z důvodu sjednocení pravidel mezi institucemi a firmami, aby každý dokument, který bude určen k dlouhodobému archivování, měl zajištěno, že ho bude možné přečíst v nezměněné podobě za mnoho let i s odlišných hardwarovým a programovým vybavením.

6.2. Evropské normy

Do poloviny roku 2012 byla v České republice problematika elektronické archivace poněkud komplikovaná. Právě v té době přijala novelu, která zavádí normy Evropského institutu pro telekomunikační standardy (ETSI - European Telecommunications Standards Institute).

Před přijetím těchto norem se často stávalo, že byly paralelně vedeny papírové záznamy pro případy, co kdyby náhodou se něco přihodilo. Dalším problémem bylo, že firmy používaly své vlastní archivační systémy, které se nedržely doporučených norem. Z právního a praktického hlediska mohl často vyvstat problém v důvěryhodnost těchto dat. Nemohla být jasně zaručena pravdivost dokumentu. Povinnost vytvářet a archivovat data dle norem ETSI mají pouze úřady. Pro komerční subjekty je to pouze doporučení, při jehož dodržení mají zaručenou akceptaci u úřadů v celé Evropské unii (EU). Výhodou ETSI norem je, že jsou celoevropské a členské státy EU je postupně začleňují do své legislativy.

6.3. Popis ETSI

Protože se oblast archivace dat týká i elektronických podpisů, byla zavedena určitá pravidla. ETSI definuje referenční standardy pro elektronické podpisy, které navazují na soustavu norem ISO. Konkrétně se jedná o:

- PAdES (PDF Advanced Electronic Signatures), pro podepisování PDF dokumentů.
- XAdES (XML Advanced Electronic Signatures), pro podepisování XML dokumentů.
- CAdES (Cryptographic Message Syntax Advanced Electronic Signatures), pro podepisování dokumentů v libovolném formátu.

Normy ETSI stanovují detaily připojení elektronického podpisu k dokumentu. U dlouhodobé archivace musejí být všechny tyto informace potřebné pro ověření autenticity k dokumentu přiloženy.

Společně s těmito údaji je připojeno časové razítko, které chrání data. Jakákoliv snaha o změnu dat by zapříčinila rozbití časového razítka. V rámci zachování validity dokumentu jsou připojována další časová razítka. Děje se tak před vypršením platnosti předchozího. Tím je zaručeno, že v dokumentu nedošlo k žádné změně.

V problematice dlouhodobého archivování se využívá standardu PAdES, konkrétně jeho podspecifikace PAdES/LTV (Long Term Validation). Ta kromě dlouhodobé čitelnosti dokumentu používá formátu PDF/A převzatého z ISO norem. Opatřuje dokument certifikáty a časovými razítky. Problémem certifikátu je, že má omezenou dobu platnosti a je tedy třeba po vypršení dané lhůty dokument znovu orazítkovat. U dlouhodobě platných dokumentů je nutné doložit, že daný certifikát byl v době použití platný a nebyl zneužit. Tato skutečnost se dokládá přiložením certifikačních revokačních listů.

Při dodržování ETSI norem je zajištěna nezávislost dokumentu na hardwaru i softwaru. Za podmínky připojení veškerých metadat k dokumentu je velice snadný přesun do jiného úložiště, přitom důvěryhodnost nebude narušena.

6.4. CAdES

CAdES byl vytvořen okolo protokolu CMS (Cryptographic Message Syntax [8]), který zabezpečuje zprávy. Je to základní stavební kámen pro digitální podpisy založené na infrastruktuře veřejných klíčů (PKI). Základní možnosti podepisování jsou definovány ve verzi CAdES-BES (kde BES označuje Basic Electronic Signature) a v CAdES-EPES (Explicit Policy Electronic Signature). Jsou to pokročilé formy, kterými CAdES podporuje dlouhodobou validaci, tzv. LTV podpisů.

6.5. XAdES

XAdES využívá standard XML-DSIG (XML Digital Signatures) pro digitální podpisy reprezentované v XML. Nejedná se o podepisování pouze XML dokumentů. Tyto podpisy mohou být použity na jakýkoliv typ dat. Norma, podobně jako výše uvedená CAdES, definuje verzi základního elektronického podpisu XAdES-BES a výslovná pravidla pro elektronické podpisy XAdES-EPES. A také definuje stejné LTV ověřování XML-DSIG, jako CAdES dělá s CMS.

6.6. PAdES

Tento standard funguje velice podobně jako výše uvedené standardy z AdES skupiny. ETSI standard PAdES obsahuje pět částí:

- Část 1 se zabývá přehledem standardu.
- Část 2 informuje o obsahu normy ISO 32000-1.
- Část 3 popisuje rozšíření o elektronický podpis.
- Část 4 obsahuje stejné LTV vlastnosti definované v CAdES a XAdES.
- Část 5 se zabývá XML obsahem, tedy XAdES podpisy XML obsahu v PDF dokumentech.

6.7. Shrnutí

V České republice legislativa určuje, jak dlouho je potřeba archivovat určité dokumenty. Dále definuje, jak nakládat s elektronickým podpisem. Evropské normy stanovují standardy pro dlouhodobou archivaci.

S vytvářením dokumentů souvisí i jejich skartace. V následující kapitole je skartování popsáno.

7. Skartování dokumentů

Legislativa určuje, jaké dokumenty je třeba uchovávat po určitou lhůtu, jak již bylo uvedeno v tabulce 1. Každý dokument má opatřen skartační znak. Po uplynutí vytyčených lhůt se podle skartačních znaků rozhoduje, co se s dokumentem dále stane. Proces není tak jednoduchý, protože Národní archiv podle zákona[1] může mít o archiválie zájem a musí mu být nejdříve nabídnuty. Příští podkapitoly jsou věnovány problematice skartačního znaku, vyznačené lhůtě a samotnému průběhu skartace.

7.1. Skartační znak

Skartační znak přiřazuje skartační komise dané společnosti. Na základě předloženého návrhu vykoná pracovník Národního archivu archivní prohlídku, kde posoudí, popř. změní rozdělení dokumentů do skupin. Skartační znak označuje soubory podle jejich obsahu, čímž určí jejich hodnotu a způsob likvidace při skartačním řízení.

- Skartační znak „A“ (archiv) značí dokument trvalé hodnoty, který bude při skartačním řízení vybrán jako archiválie[2] k trvalému uložení do archivu.

- Skartační znak „S“ (stoupa) značí dokument bez trvalé hodnoty z hlediska vědeckého, správního, hospodářského ani kulturního a ve skartačním řízení bude určen ke zničení.

- Skartační znak „V“ (výběr) značí dokument, jehož hodnotu nelze v době vzniku určit a v následném skartačním řízení bude znovu posouzen a bude mu přiřazen buď skartační znak „A“ nebo „S“.

7.2. Skartační lhůta

Skartační lhůta se udává číslicí za skartačním znakem a značí dobu, po kterou je nutné dokument uchovat. Dokumenty lze skartovat nejdříve po uplynutí skartační lhůty. Tuto lhůtu není možné zkrátit z žádného důvodu. Je ale možné ji prodloužit, pokud jej původce potřebuje pro svou další činnost. Pro ujasnění uvedu názorný příklad: V5 znamená po pěti letech rozhodnout, zda bude dokument archivován nebo skartován.

Speciálně účetní doklady a další důležité dokumenty mají zákonem danou skartační lhůtu. Ta se počítá od 1. dne roku následujícího po roce, kterého se dokumenty týkají. Případně od 1. dne po konci účetního období, kterého se dokumenty týkají.

[1] http://www.epravo.cz/_dataPublic/sbirky/archiv/sb18-74.pdf

[2] Archiválie je takový dokument, který byl vzhledem ke svému obsahu a trvalé hodnotě vybrán ve veřejném zájmu k trvalému zachování. Trvalou hodnotu posoudí příslušný archiv.

7.3. Průběh skartace

Po uplynutí skartační lhůty, či při zániku podnikatelského subjektu musí být nejdříve nabídnuty oblastnímu archivu dokumenty, které mají trvalou hodnotu. Poté je nutné vytvořit skartační návrh. Tvoří jej soupis dokumentů ke zničení, označení dokumentů skartačními znaky. K němu je potřeba připojit průvodní dopis a poslat vše příslušnému státnímu archivu. Ten vypracuje protokol, kde jsou schválené dokumenty ke zničení, kterým uplynula skartační lhůta, a nemají trvalou hodnotu.

7.4. Shrnutí

Dokumenty se označují skartačními znaky, které vyznačují, co se s nimi stane po uplynutí vyznačené lhůty. Skartační znaky rozlišujeme tři.

Protože jsem již popsal požadavky na data, která chceme ukládat, archivační formáty a legislativu, je potřeba zmínit digitální archiv. Digitální archiv má určitá pravidla při přijetí dokumentů. Vyznačuje, kdy a co se stane v které části archivu s dokumenty. Jednou z metod je OAIS.

8. Digitální archiv založený na OAIS modelu

Nyní již máme představu o tom, jak dokument určený k archivování má vypadat a jak by měl být zabezpečen. Nastal čas se zabývat otázkou, jak by mělo vypadat místo, ve kterém budu archiválie skladovat. Digitální archiv je speciální úložiště kam ukládat data určená k dlouhodobé archivaci. V archivu musí platit jasná pravidla, jak nakládat s daty, jaký přístup zajistit uživatelům apod. Původně si každý archiv určoval pravidla dle svého uvážení a situace byla roztříštěná. Následně začaly vznikat standardy. Metoda OAIS je mezinárodně uznávaný a doporučovaný standard.

8.1. Vznik OAIS

Model OAIS je zkratkou pro Open Archival Information System, často tento pojem může být zmiňován jako Referenční model pro otevřený archivní informační systém.

OAIS byl poprvé publikován v roce 1995 společností CCSDS (Consultative Committee for Space Data Systems). Ta si uvědomila, že velké objemy jejich dat jsou nepoužitelné kvůli změnám softwaru a hardwaru. Norma vznikala otevřeně a veřejně ve spolupráci s tradičními archivy. Následně se tato norma roku 2003 stala standardem ISO (označení ISO 14721:2003). Slouží k popisu systému pro dlouhodobou ochranu digitálních dat. Další vlastností tohoto standardu je vymezení pojmů a tedy definování zainteresovaným stranám slovník pojmů.

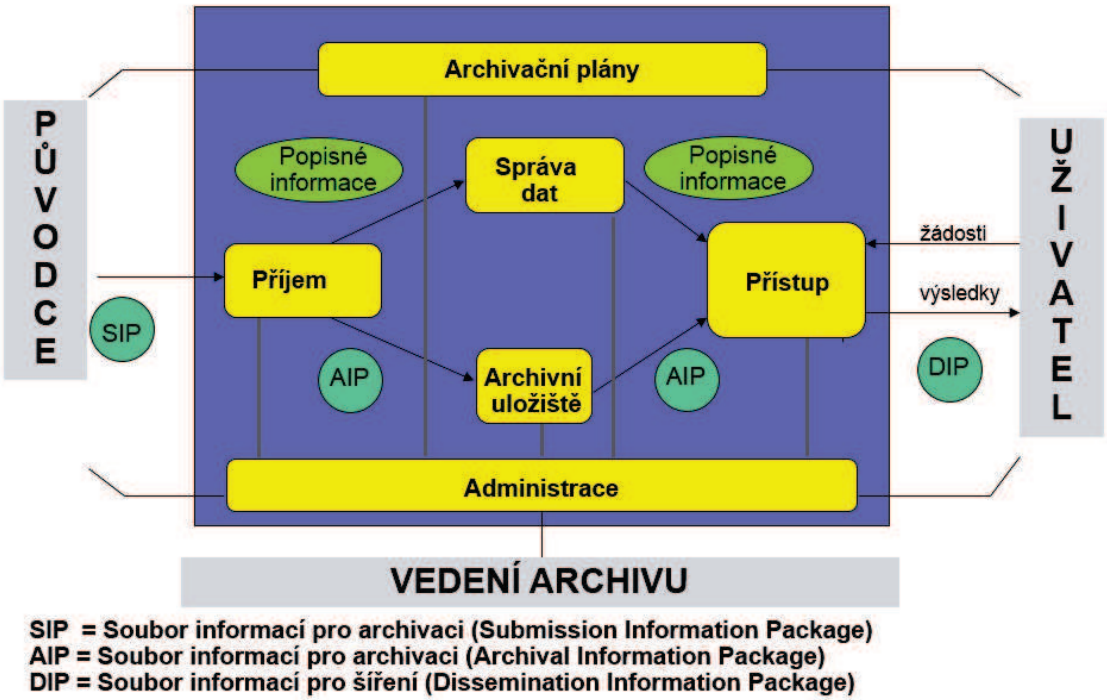
8.2. Popis normy OAIS

Tento referenční model velmi obecně zahrnuje hardwarové a softwarové komponenty. Dále typy zodpovědných osob za ochranu a zpřístupňování informací a archivní informační systém. Jelikož je to pouze doporučený standard, ve výsledné implementaci můžou některé části těchto rámců chybět.

8.3. Rozdělení OAIS modelu

Tento referenční model lze rozdělit na několik samostatných jednotek, viz Obrázek 9, které budu nazývat entity. Archiv, který je vystavěn podle normy OAIS, pracuje se třemi typy informačních balíčků, které mají definované konkrétní úkoly v rámci archivu.

Obrázek 9. Funkční celky modelu OAIS. [9]



8.3.1. Soubor informací pro dodávání

Soubor informací pro dodání (SIP) zajišťuje přijetí informačních balíčků od původce dat. Po jejich doručení získává OAIS systém kontrolu a právo nakládat s informacemi nad daným balíčkem za účelem zajištění dlouhodobé archivace. Další postup musí OAIS archiv dodržovat dle nastavených strategií a postupů a musí zajistit ochranu proti rizikům. Výsledný archivní balíček je přesunut na vstup archivační entity.

8.3.2. Soubor informací pro archivaci

Soubor informací pro archivaci (AIP) poskytuje služby a funkce pro skladování. Je to informační balíček, který se používá pro přenos archivačních objektů do digitálního archivu. Obsahuje metadata, která popisují obsah a strukturu archivovaného objektu.

8.3.3. Soubor informací pro šíření

Soubor informací pro šíření (DIP) je balíček, který je odeslán uživateli. Balíček je tvořen z jednotlivých AIP balíčků, kterých může být více, nebo to mohou být pouze jejich části.

8.3.4. Entita Příjem

Entita zajišťuje příjem dat od původce, která se dále zpracovávají v rámci SIP balíčku.

8.3.5. Entita Archivní úložiště

Entita archivního úložiště má na starosti ochranu dat. Tato entita má pro případy poruch a katastrof vytvořené mechanismy pro redundantní kopie AIP balíčků.

8.3.6. Entita Administrace

Entita se stará o poskytování podpory původci, dodržování a vytváření standardů, řízení a sledování archivu. Řídí celý provoz archivu, plánuje ochranu celého archivu. Tato entita je zodpovědná za audit AIP balíčků, při kterém musí prokázat, že kvalita uložených dat je v souladu s požadavky archivu.

8.3.7. Entita Správa dat

Entita zajišťuje správu všech dat a jim přidružených metadat u všech záznamů. Zpřístupňuje informace a na základě žádostí z entity Přistup, vypracovává odpověď na dotaz a odesílá ji zpět původci. Pokud jsou požadovaná data k dispozici, vygeneruje žádost o dodání příslušného archivního objektu entitě Přístup.

8.3.8. Entita Plánování ochrany

Entita Plánování ochrany musí sledovat aktuální trendy, kde má na starosti vyhledávat technologie a postupy, které by mohly zapříčinit zastarávání archivu. Dále se stará o požadavky původců týkající se volby formátu dat, typu nosičů vhodných pro archivaci. V popisu činností je rovněž zvolení strategie pro doručování dat a celkovou komunikaci s archivem. Mezi další úkoly patří tvorba plánů na migraci dat, které zahrnují transformaci AIP balíčků. Po vytvoření plánu migrace a jeho otestování je odeslán entitě Administrace AIP balíček. Zde bude podroben vlastní migraci.

8.3.9. Entita Přístup

Tato entita zajišťuje přístup koncových uživatelů do archivu pomocí vyhledávacích nástrojů. Tím dokáže poskytnout údaje o dostupnosti dat, jejich popis a lokaci. Dokáže sestavit požadavek na dodání DIP balíčku.

9. Národní archiv

Národní archiv je ústřední archiv České republiky. Sídlí v Praze na Chodovci. Stará se o cenné dokumenty, které zachovává budoucím generacím. Nejstarší písemností je privilegium krále Vladislava II. z roku 1158. Provádí výběr archiválií ve skartačním řízení a přejímá je. Stará se o jejich správné uložení a restaurování. Poskytuje také odborné a poradenské služby. V badatelnách umožňuje veřejnosti studium archiválií.

9.1. Národní digitální archiv

Protože má Národní archiv za úkol pečovat o archiválie pro příští generace, musí zajistit archivaci dokumentů z dnešní doby, která ve velké míře využívá digitální data. Česká republika proto podle usnesení vlády č. 11 ze 7. ledna 2004 potřebuje vlastní digitální archiv. Odpovědnost na jeho vybudování připadla podle zákona[1] na Národní archiv.

Proto byl na počátku roku 2011 zahájen projekt Národní digitální archiv (NDA), který měl být spuštěn na počátku roku 2014. Tento archiv má být založen za účelem vyřešení bezpečné problematiky dlouhodobé archivace elektronických dokumentů a její rychlé dohledatelnosti ve veřejné správě. Budou zde uloženy dokumenty, které již neslouží aktuální denní potřebě, ale pro budoucí využití kvůli jejich historické a právní hodnotě. Tento digitální archiv umožní jejich dlouhodobé a důvěryhodné uchování, jejich zpřístupnění a čitelnost. Celý návrh digitálního archivu vychází z OAIS standardu.

Aktuální stav projektu je takový, že instituce Národního digitálního archivu je založena a spadá pod Národní archiv. Ukládání do digitálního archivu od počátku roku 2014 nebylo umožněno. Toto bylo způsobeno problémy při zadávání výběrových řízeních a následných odvoláváních soutěžících k Úřadu pro ochranu hospodářské soutěže (ÚOHS). Úřad tato výběrová řízení zrušil. Nyní se čeká na vypsání nových výběrových řízení. Nevýhodou tohoto stavu je nejen zpoždění celého projektu, ale také zadávání výběrových řízení podle požadavků na technické vybavení. Tyto požadavky jsou ale staré již několik let a neodpovídají aktuálním potřebám.

9.2. Uchovávání dat v NDA

Pro uchovávání dat jsou zvolena dvě geografická místa vzdálená od sebe minimálně 100 km. Konkrétně se jedná o Prahu a záložní pracoviště v Hluboké nad Vltavou. Na těchto místech se dokumenty ukládají na disková pole a UDO disky (Ultra Density Optical - speciální optické disky s vysokou hustotou ukládání) a to vše je zálohováno na pásky. Zajištění čitelnosti dokumentu do budoucna má na starosti metoda migrace (převádění do nových formátů).

[1] Zákon č. 499/2004 Sb., o archivnictví a spisové službě

9.3. Ochrana archivu

Archiv je potřeba chránit před účinky virů a dalšími druhy nákazy. U Národního digitálního archivu je zřízená tzv. karanténní zóna, která převezme data a zkontroluje je. Následuje samotná fyzická ochrana, kde existují požadavky na ventilaci, protipožární dveře a zákaz kouření v prostoru archivu.

10. Poskytovatelé dlouhodobé archivace

V této části práce jsem se zaměřil na krátký přehled poskytovatelů dlouhodobé archivace v České republice. Vybral jsem 6 firem. Každá z nich nabízí své řešení, které prezentuje jako nejlepší možné. V rámci dotazování poskytovatelů jsem navštívil společnost Sefira na jejím semináři k archivaci. U firmy Software602 se mi věnoval zástupce společnosti, který velmi ochotně vše představil a vysvětlil. Nepříjemné překvapení mě čekalo u společnosti O_2, která poskytuje podrobnější informace pouze korporátní klientele a dotazy studentů se nezabývá. Dosud se mi nepodařilo zjistit, zda je řešení této společnosti funkční a v provozu.

10.1. O_2 Důvěryhodný archiv

Obrázek 10. Logo O_2 [10]

Společnost O_2 nabízí svou službu, která nese název O_2 Důvěryhodný archiv. Umožňuje uložit dokumenty, které budou zpřístupněny pouze pověřeným osobám. Důvěryhodný archiv spravuje především elektronické listiny z datových schránek, jako jsou faktury, daňová přiznání a další obchodně právní dokumenty. O_2 Důvěryhodný archiv prošel jako jediný v České republice certifikací Elektrotechnického zkušebního ústavu, a splňuje tak normu ISO 15288. Tato norma popisuje životní cyklus softwaru, zpracování dat a splňuje zákonné požadavky na validní archivaci elektronických dokumentů. Licence tohoto produktu je doživotní.

Společnost O_2 poskytuje podrobnější informace pouze korporátní klientele a dotazy studentů se zabývá pouze okrajově a zasílá obecné marketingové materiály.

10.2. Software602

Obrázek 11. Logo Software602 [11]

Firma Software602 na českém trhu nabízí své komplexní řešení pro dlouhodobou archivaci dat. Její program, který zajišťuje převod do PDF/A, se nazývá Software602 Print2PDF X. K převáděným datům doplní metadata. Společnost nabízí pouze softwarové řešení. Tedy produkty pro digitalizaci dat a jejich následnou konverzi do formátu

PDF/A podle PAdES LTV nebo CAdES-A. Vlastní úložiště pro data nenabízí. Firma velice rychle reaguje na změny v legislativě a nových standardech. Na většině z nich se sama podílí. Tato firma patří mezi největší na tuzemském trhu a snaží se o osvětu v oblasti archivování.

Společnost na počátku roku 2014 spustila službu s názvem Long-Term Docs. Služba je zajímavá tím, že neposkytuje službu celého úložiště včetně počítačového vybavení a vlastního uložení dokumentů a dat. Ale zajišťuje péči o dokumenty a uživatel může libovolně využívat úložiště, které má k dispozici, tak jak je zvyklý. Služba respektuje všechny referenční formáty rodiny AdES. Tím umožňuje zajištění dlouhodobé ověřitelnosti nejen PDF dokumentů, ale jakýchkoliv data. Vstupním kanálem pro zpracování dokumentů či dat může sloužit cloudové úložiště, e-mail, či nějaké interní úložiště, či Systém datových schránek ISDS pro archivaci Datových zpráv. V cloudových úložištích podporuje Google Drive, Office 365, OneDrive a SharePoint. Služba umí ověřit certifikáty kvalifikovaných autorit z EU, ověřit PDF/A formát, přidat kvalifikované časové razítko. Dále konvertovat do PDF/A formátu, opatřit dokument digitálním podpisem a zajistit časovou kontinuitu a ověřitelnost dat či dokumentů v souladu s českou i evropskou legislativou.

10.3. Sefira

Obrázek 12. Logo Sefira [12]

Společnost Sefira nabízí řešení pro ověřování platnosti dokumentů, zabezpečený elektronický archiv a zabezpečení dokumentů, které definuje rozdílná práva pro skupiny zaměstnanců. Tato ochrana je užitečná. Podle vyjádření této firmy je přes 60 % chyb způsobeno zaměstnanci. Její produkt se jmenuje OBELISK Archive.

10.4. Fujitsu

Obrázek 13. Logo SecDocs [13]

Společnost Fujitsu nabízí vlastní, kompletní řešení nazvané SecDocs pro dlouhodobou archivaci podle standardu OAIS. Firma se chlubí rychlou implementací do stávající IT infrastruktury díky modularitě a architektuře SOA. Výhodou této společnosti je její celosvětové působení.

10.5. Česká pošta

Obrázek 14. Logo Česká pošta [14]

Česká pošta nenabízí produkt, který by se zabýval všemi procesy dlouhodobé archivace. Specializuje se na zachování zpráv v datových schránkách i po 90 denní lhůtě, kdy se zprávy automaticky mažou. Tuto službu nazvala Datový trezor. Umožňuje archivovat 100, 200, 500, 1000, 2000 a 5000 zpráv. Aktivace datového trezoru je provedena do 60 dnů od objednání. Je možné si domluvit zřízení služby na zkoušku na 3 měsíce o kapacitě 50 zpráv. V rámci doplňkových služeb k datovým schránkám, nabízí Česká pošta SMS notifikace při příchodu zpráv a tzv. Bezpečný klíč. Je to nadstandardní úroveň zabezpečení přístupu k datové schránce.

Celkově je u Datového trezoru velice zajímavé prostudovat si v Obchodních podmínkách sekci věnovanou zárukám [8]. Zde jsou uvedeny smluvní pokuty, pokud poskytovatel, Česká pošta, poruší funkcionalitu Datového trezoru. Porušením se rozumí například poškození zpráv, či jejich úplná ztráta. Smluvní pokuty jsou vskutku mizivé:

- Pro Datový trezor o kapacitě do 250 zpráv je *sankce 1000 Kč, a to za každý případ poškození či ztráty datových zpráv v průběhu jednoho měsíce (bez ohledu na celkový počet současně poškozených či ztracených datových zpráv v průběhu tohoto měsíce).*

- Pro Datový trezor o kapacitě nad 250 a do 1000 zpráv je *sankce 3000 Kč, a to za každý případ poškození či ztráty datových zpráv v průběhu jednoho měsíce (bez ohledu na celkový počet současně poškozených či ztracených datových zpráv v průběhu tohoto měsíce).*

- Pro Datový trezor o kapacitě nad 1000 zpráv je *sankce 5000 Kč, a to za každý případ poškození či ztráty datových zpráv v průběhu jednoho měsíce (bez ohledu na celkový počet současně poškozených či ztracených datových zpráv v průběhu tohoto měsíce).*

Tyto sankce neřeší důležitost jednotlivých zpráv. Stačí tedy mít v Datovém trezoru uložený dokument, který bude například použit u soudního sporu, ve kterém půjde o miliony korun. Výpadek služby nás připraví o důkaz, tím prohrajeme soud a jako kompenzaci dostaneme pouhých 1000 Kč.

10.6. Gordic

Obrázek 15. Logo Gordic [15]

Firma Gordic patří mezi větší firmy na našem území. Zabývá se informačními systémy pro státní správu. Nabízí vlastní řešení pro konverzi dokumentů do digitální podoby a následné vložení do datové zprávy v datové schránce. Toto řešení je nazvané RAK – Registr autorizovaných konverzí. Firma dále nabízí řešení pro ukládání digitálních dokumentů. Pod názvem GINIS® DRMS se skrývají tři moduly: Elektronická spisovna (eSPI), Elektronické skartační řízení (ESR) a Správa uložených digitálních dokumentů (SUD). Takovéto řešení umožní kompletní správu digitálních dat, od konverze do formátu PDF/A, přes jeho uložení do spisovny, až po skartační řízení.

10.7. Shrnutí

Obecně se nedá říct, která firma nabízí nejlepší řešení. Cena řešení je velice individuální, vše záleží na konkrétních požadavcích zákazníka a pohybuje se řádově ve stovkách tisících za komplexní řešení. Zmapováním poskytovatelů dlouhodobé archivace jsem zjistil velké rozdíly ve vstřícnosti v poskytování informací. Nejuzavřenější společností je O_2. Ta má na webových stránkách pouze několik hesel připravených marketingovým oddělením. Odmítá sdělit podrobné informace, pokud nejste vážný zájemce o jejich služby. Úplným opakem je pak firma Software602, která se snaží o veřejnou osvětu. K dispozici dává mnoho informací a pořádá semináře pro širokou veřejnost. Tato společnost se navíc snaží neustále nabízet inovativní produkty. Kontroverzní společností je státní podnik Česká pošta. Provozuje Datový trezor, který slouží k archivaci zpráv z datových schránek. Kontroverznost spočívá v obchodním podmínkách společnosti. Při ztrátě dokumentů zaplatí pouze pokutu 1000 Kč a vůbec neřeší, že dokumenty pro nás mohou být existenčně důležité. Společnost Sefira také pořádá semináře jako Software602, ale již není tolik otevřená v poskytování informací. Zbylé dvě společnosti, Gordic a Fujitsu, jsou více uzavřené a spíše se zaměřují na velké firmy a státní správu.

V praktické části využiji znalostí z výše načerpaných teoretických kapitol. Jedná se o podepisování dokumentů a jejich ověřování. Abychom data měli ve správném formátu, poslouží informace o formátu PDF/A. Již víme, že dokumenty musí být někde uložené, proto využiji znalosti standardu OAIS pro ukládání dat do archivu.

11. Případová studie

Praktická část mé bakalářské práce na základě předchozí teorie navazuje na vhodné řešení archivace s ohledem na legislativní požadavky. Tato případová studie se týká zmapování aktuálního stavu archivace, popsání postupu v OAIS archivu a poté jsou zde vyhodnoceny nové legislativní požadavky Evropské unie a jejich dopady.

11.1. Ukládání dat

Data je potřeba někam ukládat. Převažují dvě možnosti způsobu ukládání dat.

První možností je zřídit vlastní infrastrukturu, na které bude umístěno řešení datového úložiště od poskytovatele dlouhodobé archivace. Toto řešení má své výhody a nevýhody:

+ Úložiště máme pod svou vlastní kontrolou.

+ Můžeme snadno modifikovat.

− Nutná údržba infrastruktury.

− Dodatečné náklady na ochranu infrastruktury proti přírodním a kriminálním živlům.

Druhou možností je umístit data do cloudu. Cloud je služba na Internetu, kterou poskytuje poskytovatel na své infrastruktuře. K těmto službám je možné přistupovat prakticky odkudkoliv. Obvykle se neplatí za samotný software, ale za jeho použití. Nemusíme se tedy starat o vlastní datové úložiště, pouze si jej u cloudového poskytovatele pronajmeme a od poskytovatele řešení dlouhodobé archivace si necháme nastavit ukládání dokumentů a jejich ověřování do tohoto úložiště v „oblaku“.

Také tato možnost má své kladné a záporné stránky:

+ Jednoduchá škálovatelnost. Platí se výkon, který potřebujeme.

+ Odpadají náklady na údržbu infrastruktury.

+ Vždy aktuální verze služeb.

+ Garance neustálého provozu.

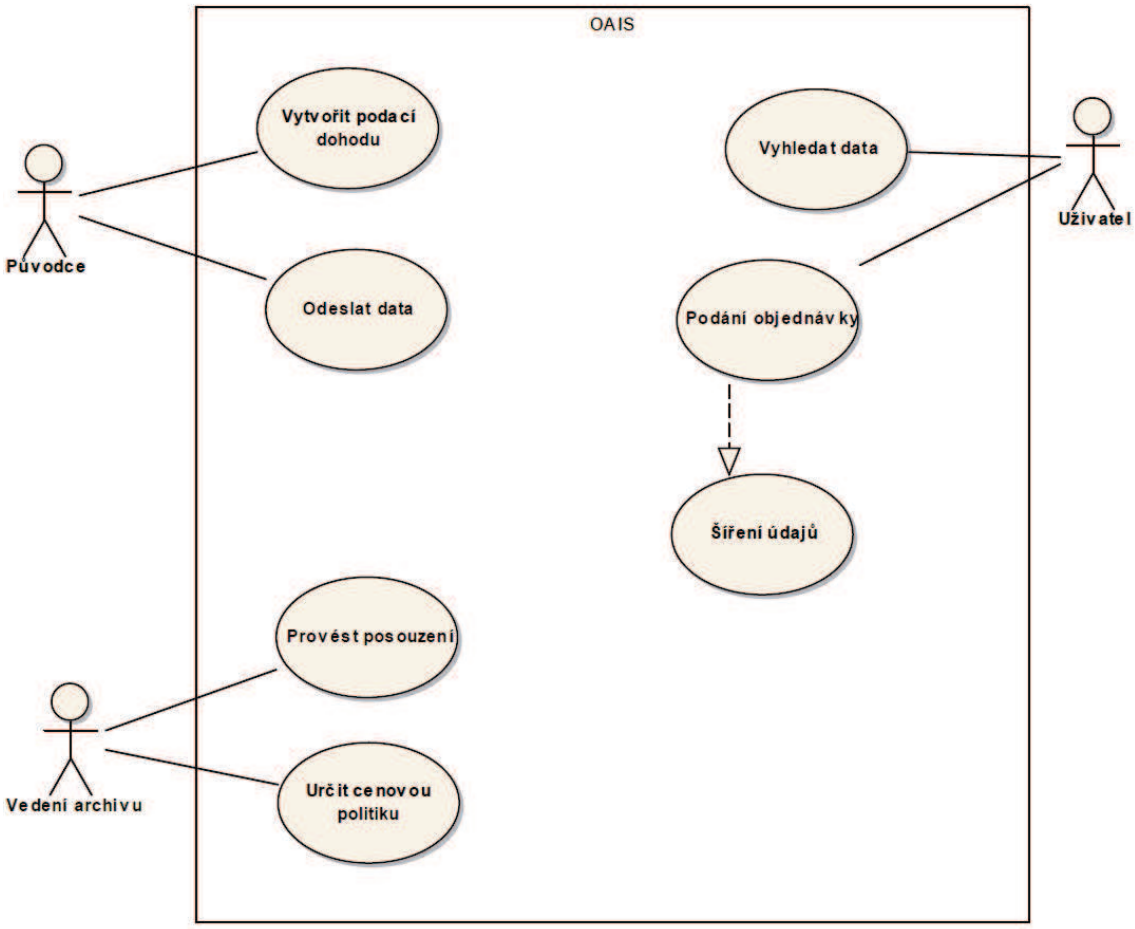
− Data nemáme pod naprostou vlastní kontrolou, jsou umístěna „někde“.

− Ochota umístit „někam“ svá citlivá data.

– Služba může trpět aktuálním výpadkem a nedostupností.

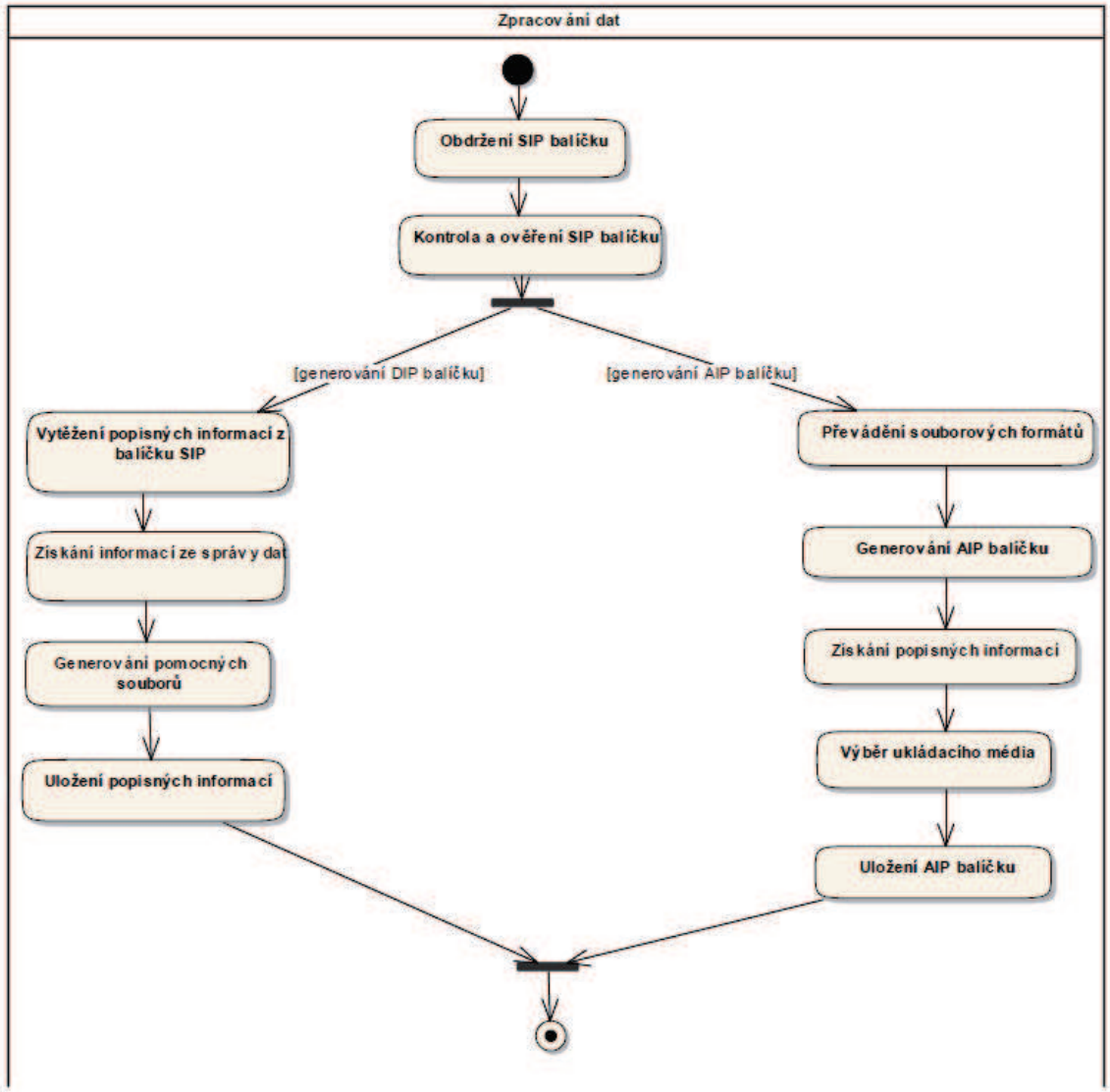
V OAIS archivu existují určité role, které k sytému přistupují. Ke znázornění jsem využil Use Case diagramu v UML jazyce. Diagram zachycuje jednotlivé aktéry, tedy ty, kteří pracují s daným systémem a jejich činnosti, které v něm mohou vykonávat. Mezi aktéry patří držitel dat, který vkládá data. Svou roli zde má i běžný uživatel, který si chce data vyhledat. Posledním aktérem je řízení, tedy systém, který posuzuje dokumenty z hlediska připravenosti dokumentů na vložení do archivu.

Obrázek 16. Use Case Diagram



Pro názornou ukázku, jak v OAIS funguje proces od obdržení SIP balíčku po jeho uložení, jsem vytvořil UML diagram aktivit. Tento diagram slouží k zachycení sekvence jednotlivých kroků, kde jsou zakresleny jednotlivé akce. Jak je vidět na obrázku 17, nejdříve je přijat samotný SIP balíček, který je následně zkontrolován. Poté se zpracování rozdělí na 2 činnosti, ve kterých se generuje DIP balíček a AIP balíček. Při generování DIP balíčku se vytěží data ze SIP balíčku. Následně se vygenerují se pomocné soubory a uloží popisné informace. Mezitím se generuje AIP balíček, který získá popisné informace a zvolí vhodné uložení.

Obrázek 17. Diagram aktivit zpracování dat



12. Analýza současné a připravované evropské legislativy

V případové studii budu navazovat na kapitolu 6 s legislativou. Provedu analýzu současné evropské normy 1999/93/EC a vyhodnotím dopady připravovaného nařízení. Dále budu vycházet ze znalosti elektronické značky, kterou využiji v modelovém příkladu.

Digitální archivaci formuje legislativa. Česká republika je členem Evropské unie a v rámci ní přejímá evropské předpisy a nařízení. Aktuální legislativa, která se v hojné míře zabývá elektronickým podpisem a přeshraničním uznáváním již nevyhovuje a je navržena legislativa nová. Oba dokumenty jsou zmíněny v následující části.

12.1. Současná směrnice 1999/93/EC

U digitálního podpisu aktuálně platí směrnice navržená roku 1999 s označením 1999/93/EC Evropského parlamentu a Rady o zásadách Společenství pro elektronické podpisy.

V této směrnici se uvádí, jaké jsou náležitosti elektronického podpisu, jak k němu přistupovat a jaká plynou práva a povinnosti. Důraz byl kladen na právní stránku. Bylo požadováno, aby elektronický podpis založený na kvalifikovaném certifikátu byl roven klasickému vlastnoručnímu podpisu a bylo jej možno použít u soudního řízení.

Dále jsou zde uvedeny požadavky na poskytovatele certifikačních služeb a k bezpečnému vytváření podpisů a jejich ověřování.

Ve směrnici bylo myšleno na jednotný evropský trh a zjednodušení použití podpisů napříč trhy. Hranice měly přestat být překážkou. Potíž nastala při požadavcích na poskytovatele služeb. Každý stát si zde může stanovit další požadavky. Tím se stěžují podmínky pro vzájemné uznávání elektronických podpisů.

12.1.1. Vyplývající nedostatky

Při následném sledování funkčnosti, zjistila Evropská komise tyto nedostatky:

- Státy začaly používat rozdílné úrovně ověřování certifikátů. A některé systémy ověřují pouze kvalifikované certifikáty, zatímco ostatní ověřují i komerční. Došlo k různému výkladu a vytvoření překážek.

- V jednotlivých členských státech jsou na poskytovatele služeb uplatňována rozdílná pravidla. Tato rozdílnost je způsobena odlišným výkladem směrnic, které jsou navíc zastaralé a tím způsobují narušení vnitřního trhu. Stejný problém se týká časových razítek a elektronických značek.

- Byl zjištěn rozdíl v dohledu nad poskytovateli certifikačních služeb.

- Směrnice měla usnadnit uznávání napříč trhy, ale stále volnému trhu překážejí různé regulace na národních úrovních.

- Poskytovatelé certifikačních služeb mají povinnost oznamovat ostatním členským státům veškeré informace. Ale neexistuje žádná aktualizovaná centrální databáze těchto poskytovatelů.

- U osobní identifikace jsou problémy způsobeny odlišnými technologickými řešením. Dále nejasnou odpovědností za správnou identifikaci a nedostatečnými právními jistotami při přeshraničním používání elektronických průkazů totožnosti.

- S narůstajícím počtem počítačů a jejich výpočetním výkonem, roste požadavek na rychlejší kontrolu vhodných kryptografických algoritmů.

- Na elektronický podpis není nahlíženo s důvěrou, jakou má běžný, vlastnoruční podpis. Stále existuje veliká nedůvěra v elektronické služby ze strany uživatelů, ale i z hlediska právních záruk. Uživatelé se při přeshraniční komunikaci necítí bezpečně kvůli rozdílným vnitrostátním předpisům.

- Dostatečně se nesleduje technologický vývoj a nevyužívají se jeho příležitosti.

12.1.2. Původ problémů

Výše jsem uvedl problémy, kterými vnitřní trh EU trpí. Ale jak tyto problémy vznikly? Pokusím se vysvětlit v následujících bodech.

- Nedostatečné nebo žádné vysvětlení vlastním občanům, kteří nemají tolik odborných znalostí. Občané nemají v novinky důvěru a nevěří třetím stranám, kterým svěřují údaje.

- V dřívějším vývoji pravidel byl kladen důraz především na elektronický podpis. Ale již nebyla řešena časová razítka, elektronické značky a jejich uznávání napříč státy. Každý stát si řešil tyto problémy svou vlastní cestou. Nyní tak vzniká nedůvěra k navrhovaným změnám o uznávání elektronických služeb napříč státy.

- Velkým problémem je bezpečnost, která se uživatelům nezdá dostatečná a neexistuje výměna informací mezi státy.

12.1.3. Zkoumání situace

Při zkoumání reálného používání směrnice 1999/93/EC a celého vnitřního trhu Evropské unie jsem kontaktoval certifikační autority napříč členskými státy. V rámci svého dotazu jsem se ptal na to, jak oni vidí celou situaci ze svého pohledu. Zda je přeshraniční uznávání bezproblémové a jaké další překážky oni identifikují. Samozřejmě, část dotazu týkající se uznávání, nemůže být plnohodnotně zodpovězena pouze ze strany certifikačních autorit, ale spíše ze strany poskytovatelů služeb využívající tyto certifikáty. Přesto je to zdroj informací vhodný, protože znají situaci na trhu a svěřují se jim klienti se svými zkušenostmi.

Jako samostatnou část přeshraničního uznávání vidím vztah mezi Českou a Slovenskou republikou. Tyto dvě země mají dlouholetou společnou historii, velmi podobný

jazyk a legislativu. Přes všechny tyto podobnosti si klienti certifikačních autorit stěžují na těžkosti při přeshraničním uznávání elektronických certifikátů.

Z odpovědí certifikačních autorit vyplynula shoda, že přeshraniční uznávání je sice napsáno na papíře, ale v praxi nefunguje. Další identifikované problémy u kvalifikovaných elektronických podpisů:

- Různé standardy pro podpisy.
- Rozdílné certifikační schéma.
- Získání potřebných informací o držiteli certifikátu z jiného členského státu, kde je původně vydán.

Zabezpečení kvalifikovaných elektronických certifikátů stále používá hashovací algoritmus SHA-1 a bezpečnějšího nástupce SHA-2. Algoritmus SHA-1 je často používán s RSA klíčem, ale dnes je již toto spojení považováno za zastaralé a postupně se přechází na SHA-2. Tento nový algoritmus je již jako jediný doporučený Ministerstvem vnitra ČR.

12.1.4. Shrnutí současné směrnice 1999/93/EC

Současná norma není plně dostatečná nejen z pohledu vývoje technologií, ale také z neuspokojivého popsání problematiky a přijetí veřejností. Proto byl vytvořen nový návrh, který může celou problematiku ovlivnit. V příštích podkapitolách jsem jej popsal.

12.2. Legislativní změny

V červnu roku 2012 vzniknul návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. Důvodem pro vytvoření tohoto návrhu bylo zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu. Dnešním problémem přeshraničních elektronických služeb jsou hranice, které je potřeba odstranit. *Je třeba, aby elektronická identifikace, autentizace, podpisy a související pomocné důvěryhodné služby (eIDAS) byly vzájemně uznávány a akceptovány v celé EU a namísto překážek se staly podpůrnými prvky. Pro služby eIDAS neexistuje ucelený přeshraniční a meziodvětvový rámec. Na úrovni EU byl vytvořen právní rámec pouze pro elektronické podpisy, avšak nikoli pro elektronickou identifikaci a autentizaci ani pro související pomocné důvěryhodné služby.*[16]

Následují změny a dopady tohoto nového nařízení.

12.3. Nová legislativa

V návrhu nového nařízení je zrušení stávající směrnice 1999/93/EC popsané výše. Cílem nového návrhu je eliminace výše uvedených nedostatků a rozšíření o nové předpisy.

Nařízení se nezapracovává do národních legislativ, ale platí přímo a stejně ve všech členských zemích.

Hlavním bodem je již několikrát zmíněné vzájemné uznávání elektronické identifikace a autentizace napříč EU. To má samozřejmě dopad na dlouhodobou archivaci. Dokumenty podepsané a opatřené časovým razítkem bude možné uznat členskými státy Evropské unie a tím budou moci podniky snáze působit v zahraničí.

Dosud nepanovala velká důvěra v elektronický podpis. Nové nařízení zavádí povinnost přiznávat kvalifikovaným elektronickým podpisům stejný právní účinek jako podpisům vlastnoručním. V případě přeshraničního přístupu nesmí být vyžadován elektronický podpis s vyšší zárukou bezpečnosti, než má kvalifikovaný elektronický podpis. V dokumentu jsou stanoveny podmínky pro dlouhodobé uchovávání kvalifikovaných elektronických podpisů.

V nařízení je pamatováno na elektronické značky. Návrh stanovuje požadavky na kvalifikované elektronické značky, podmínky pro jejich ověřování a uchovávání. Mají sloužit jako důkaz, že daný dokument vydala právnická osoba a poskytnout jistotu ohledně původu a integrity dokumentu. Elektronická značka nesmí být v soudním sporu odmítnuta jenom proto, že má elektronickou podobu.

U přijímání elektronických dokumentů podepsaných kvalifikovaným elektronickým podpisem nebo opatřených kvalifikovanou elektronickou značkou platí, že jsou v ostatních členských státech přijímány bez dodatečných požadavků. A to tehdy, pokud se podle vnitrostátních předpisů členského státu považují za originály nebo ověřené kopie.
Podobné požadavky, které platí pro elektronickou značku a elektronický podpis, platí i pro časové razítko. Požadavkem je, aby bylo spojeno s koordinovaným světovým časem (UTC).

V rámci rychlého technologického pokroku by toto nařízení mělo být otevřeno inovacím a neutrální, tedy nestanovuje žádné požadavky na vybavení.

V dokumentu se zavádí dohled nad poskytovateli důvěryhodných služeb. Jednou ročně se musí podrobit auditu nezávislého subjektu. Je to z důvodu, aby se ověřilo, zda oni sami i jejich služby, které poskytují, splňuje nařízení. Je stanoveno, že lze provést mimořádnou kontrolu kdykoliv i mimo tento každoroční audit. Každý členský stát vyhotoví a zveřejňuje seznamy s těmito poskytovateli důvěryhodných služeb.

Nařízení má nedostatek, protože není uvedeno, jakým způsobem bude ověřování probíhat. Neuvádí, zda bude zřízena například důvěryhodná centrální služba, která by toto prováděla. Společnost Software602 by mohla tuto centrální službu po celé EU zastoupit svým produktem SecuStamp.

Na závěr bych zmínil, že občas může docházet k rozporům mezi oficiálním českým překladem a originálem v anglickém jazyce. Anglický originál je vždy rozhodující.

12.4. Shrnutí

Nové nařízení znamená velkou změnu. Bude důležité sledovat, jak se ujme a případně zapracovat změny vypozorované používáním, aby celé snažení neskončilo pouze „na papíře“ a v praxi nebyl výklad mnohoznačný.

13. Modelový příklad

Nyní popíši modelový příklad týkající se archivace ve firmě. Příklad je rozdělen na 3 scénáře. Zvolím si fiktivní firmu s názvem Pokus, s.r.o. Na trhu není dlouho a postupně se rozvíjí a získává zakázky.

13.1. Všeobecné údaje

Firma by ráda archivovala dokumenty po dobu 20 let[1]. Očekávaný počet dokumentů rozdělila na čtyři pětiletá období a předpokládá u každého dokumentu průměrně 5 stran.

Počátečních 10 000 dokumentů za rok a počet stran jsem zvolil na základě oslovení 2 společností[2] s maximálně padesáti zaměstnanci s cílem zjistit objektivní počet. Veškeré ceny, které zde uvádím, jsou bez daní.

Firma u každého scénáře nakoupila[3] na každé období černobílé tiskárny, každou za cenu 15 000 Kč. Předpokládá, že po každém pětiletém období se zbaví starých. Dále musí započítat cenu tonerů, kde je výdrž 2 000 stran formátu A4 na toner, který stojí 3 000 Kč. Jejich počet byl u každého scénáře volen tak, aby byly dostupné zaměstnancům na více místech ve firmě a zátěž byla rozdělena rovnoměrně.

U každého dokumentu uvažuji 2[4] podpisy. Z celkového počtu dokumentů bude vždy potřeba desetinu nechat úředně ověřit. Současná směrnice 1999/93/EC nám totiž nezaručuje, že budou elektronické podpisy uznány i v zahraničí. Připravované nařízení si klade za cíl tuto skutečnost změnit. Podpisy mají být vzájemně uznatelné napříč státy EU a navíc by to zde zmíněné firmě přineslo výhodu, ve formě používání elektronické značky.

Ceny jsou aktuální k 31. březnu 2014 a všechny počty dokumentů a uváděné procentuální části jsou pouze orientační. Vše záleží na aktuálních potřebách dané firmy a odvětví její činnosti.

13.2. Podklady pro vícekriteriální analýzu

Pro celkové hodnocení nebude důležitá jen cena. Pro zachycení této skutečnosti použiji vícekriteriální analýzu. V analýze je dána konečná množina variant, které jsou hodnoceny podle kritérií. Cílem je určit, která varianta je podle daných parametrů hodnocena nejlépe. Varianty lze seřadit od nejlepší po nejhorší.

Nejdříve stanovím jednotlivá kritéria a jejich důležitost. U každého scénáře následně pomocí této analýzy vyplním údaje a doplním ji o krátký komentář se zdůvodněním

[1] Časový horizont vyplynul z konzultací u vedoucího této bakalářské práce ing. Pavla Náplavy.

[2] První firmou je BIOFERM CZ spol. s r.o., druhá společnost si nepřála uvést své jméno.

[3] Ceny za tiskárny, tonery a jejich výdrž je zvolena z údajů maloobchodních prodejců a výrobců těchto zařízení.

[4] Obvykle podpis zástupce firmy Pokus, s.r.o. a podpis obchodního partnera.

přidělených hodnot. V závěrečném shrnutí zvolím nejvhodnější řešení pomocí analýzy.

Názvy kritérií a odůvodnění jejich zvolení[5]:

- Dostupnost dat – jak rychle můžu mít archiváliі na monitoru nebo v ruce.
- Přehlednost v datech – jak se lze v datech vyznat, jak je jednoduché a rychlé v nich vyhledávat.
- Ekologický přístup – Evropská unie se snaží snížit všemožné plýtvání a navíc, pro mnoho uživatelů je přirozené šetřit přírodu.
- Jednoduchost řešení – jak jednoduše se pracuje s vybraným řešením, provádí údržba apod.
- Pohodlí – jak se dané řešení ovládá a pracuje s daty.
- Bezpečí dokumentů – jak moc jsou dokumenty zabezpečeny proti nechtěným chybám a výpadkům dokumentů.
- Nároky na skladovací prostor – každé řešení obsadí určitou kapacitu.
- Dlouhodobá čitelnost – jak je složité zajistit dlouhodobou čitelnost.

Důležitost kritérií je hodnocena stupnicí 1-8 (1 nejdůležitější, 8 nejméně důležité), viz. tabulka 2.

Tabulka 2. Vícekriteriální analýza

Kritérium	**Označení**	**Důležitost**
Dostupnost dat	K1	1-2
Přehlednost v datech	K2	4
Ekologický přístup	K3	8
Jednoduchost řešení	K4	6
Pohodlí	K5	5
Bezpečí dokumentů	K6	3
Nároky na skladovací prostor	K7	7
Dlouhodobá čitelnost	K8	1-2

Již tedy máme určena kritéria, která mají svojí důležitost. V závěru příkladů bude provedeno vyhodnocení na základě normalizované matice a váženého součtu.

[5]Kritéria vyplynula z konzultace u zástupce Software602 a u vedoucího této bakalářské práce ing. Pavla Náplavy.

13.2.1. Celkový počet dokumentů

V následující tabulce 3 je rozepsán počet dokumentů a stran za jednotlivá období. Tento počet je u každého scénáře stejný.

Tabulka 3. Počet dokumentů a stran za jednotlivá období

Období	**Přírůstek dokumentů za každý rok**	**Dohromady dokumentů za období**	**Dohromady stran za období**
Prvních 5 let	10 000	50 000	250 000
Druhých 5 let	13 000	65 000	325 000
Třetích 5 let	15 500	77 500	387 500
Čtvrtých 5 let	18 000	90 000	450 000
Souhrn	282 500	282 500	1 412 500

Celkem tedy firma za 20 let vyprodukuje 282 500 dokumentů. Všechny tyto dokumenty chce mít archivovány a úředně ověřeny. Protože se u každého dokumentu předpokládá 5 stran, za sledované období je to tedy 1 412 500 stran.

13.3. Scénáře

Firma Pokus, s.r.o. se rozhoduje nad třemi možnými scénáři.

1. Archivovat vše v papírové podobě a přijmout riziko placení pokut.

2. Archivovat digitálně a provozovat vlastní infrastrukturu a zároveň tisknout 30 %[6] celkového počtu dokumentů.

3. Archivovat digitálně s využitím cloudového úložiště a zároveň tisknout 30 % celkového počtu dokumentů.

V rámci poskytovatelů dlouhodobé archivace jsem vybral společnost Software602 a jejich službu Long Term Docs. Důvodem je jejich vstřícný přístup a velká dostupnost informací na jejich webovém portálu.

Následovat budou jednotlivé situace a na konci celkové shrnutí a porovnání celkových nákladů za všechny scénáře v přehledné tabulce i podle vícekriteriální analýzy.

13.4. Scénář první

První scénář obsahuje pouze archivaci v listinné podobě. Firma nakoupila v prvním období 4 černobílé tiskárny. Předpokládá, že po každém pětiletém období se zbaví starých tiskáren a nakoupí nové za stejnou cenu a každé toto období přikoupí jednu tiskárnu navíc. Dále musí započítat cenu tonerů.

[6] Vyplynulo z konzultace u zástupce Software602.

13.4.1. Celkový počet stran prvního scénáře

Předpokládám, že velkou část dokumentů je potřeba tisknout dvakrát, například smlouvy. Jako koeficient pro tyto případy jsem zvolil hodnotu 1,8[7], kterou vynásobím počet stran. Počty za jednotlivá období jsou uvedeny v tabulce níže.

Tabulka 4. Počet stran po vynásobení konstantou

Období 5 let	Počet stran	Počet stran s koeficientem 1,8
První	250 000,00	450 000,00
Druhé	325 000,00	585 000,00
Třetí	387 500,00	697 500,00
Čtvrté	450 000,00	810 000,00
Souhrn	1 412 500,00	2 542 500,00

13.4.2. Náklady na tisk prvního scénáře

Kalkulace nákladů je uvedena v tabulce 5:

Tabulka 5. Kalkulace tiskových nákladů za jednotlivá období

Období 5 let	Počet tiskáren	Cena za tiskárny	Počet stran na tiskárnu	Počet tonerů	Cena za tonery	Cena za stránky
První	4	60 000	112 500,00	56,25	168 750,00	180 000,00
Druhé	5	75 000	117 000,00	58,50	175 500,00	234 000,00
Třetí	6	90 000	116 250,00	58,13	174 375,00	279 000,00
Čtvrté	7	105 000	115 714,29	57,86	173 571,43	324 000,00
Souhrn	22	330 000	461 464,29	230,73	692 196,43	1 017 000,00

Náklady na tiskárny, tonery a stránky, vycházejí celkové náklady ve výši 2 039 196,43 Kč.

[7] Zvoleno na základě konzultace u zástupce Software602.

13.4.3. Celkové náklady prvního scénáře

Následně je zde kalkulace nákladů na úřední ověření stránek. Předpokládám, že v každém dokumentu jsou 2 podpisy, které je také nutné úředně ověřit. A dále předpokládám, že počet dokumentů nutný k ověření jsou 2 %[8] z celkového počtu všech dokumentů. Pro ověření stránek a podpisů počítám s původním počtem dokumentů, tedy bez násobení konstantou 1,8.

Tabulka 6. Kalkulace nákladů na ověření stránek a podpisů

Náklady	**Cena**
Celkové náklady na tisk	2 039 196,43
Náklady na ověření 1 stránky dokumentu	30,00
Náklady na ověření 1 podpisu	30,00
Počet dokumentů k ověření	5 650,00
Počet podpisů k ověření	11 300,00
Počet stran k ověření	28 250,00
Náklady na ověření všech stránek	847 500,00
Náklady na ověření podpisů	339 000,00
Náklady na tisk a ověření celkem	3 225 696,43

V prvním modelovém scénáři jsou celkové náklady podle tabulky výše vyčísleny na 3 225 696,43 Kč.

13.4.4. Další náklady prvního scénáře

K nákladům uvedeným v tabulce 6 je potřeba přičíst náklady na skladování. Existují 2 možnosti:

- Mít vlastní sklad, kde každý rok přiroste tisíce nových dokumentů. Jsou to tedy velké nároky na prostor. Dále je potřeba místo zajistit proti požáru, zajistit stálou teplotu, vlhkost a učinit opatření proti možnému vytopení.

- Využít služeb společností zabývajících se bezpečným uložení listinných dokumentů[9]. Zde se platí obvykle měsíční částka za uložení. Platí se za uložení krabice či boxu. Tuto částku označím konstantou „U“. Pokud chceme určitý dokument, který je uložen ve skladu, stojí jeho vyhledání 6*U, přivezení stojí 3*U a skartace přibližně 10*U. Je tedy jasně zřetelné, že vyhledání a dovezení je cenově diametrálně odlišné. Vyhledávání dokumentů probíhá obvykle jednou až dvakrát ročně v případě různých kontrol.

[8] Vyplynulo z konzultace u zástupce Software602.
[9] Aktuální ceny si firmy pečlivě střeží, ze starších materiálů jsou odvozeny násobky za konkrétní služby.

13.4.5. Vícekriteriální analýza prvního scénáře

Je potřeba vyplnit údaje vícekriteriální analýzu pro závěrečné shrnutí. K tomuto účelu slouží následující tabulka.

Tabulka 7. Vícekriteriální analýza první varianty

Kritérium	Označení	Hodnota	Komentář
Dostupnost dat	K1	3	Přivést dokument ze skladu je časově náročné.
Přehlednost v datech	K2	3	Najít konkrétní dokument v šanonech může být obtížné.
Ekologický přístup	K3	1	Obrovské množství tištěných dokumentů určitě není šetrné k přírodě.
Jednoduchost řešení	K4	3	Velké množství šanonů, špatný přehled, to není známka jednoduchosti.
Pohodlí	K5	3	Nošení dokumentů na úřady k ověření, množství šanonů.
Bezpečí dokumentů	K6	5	Dokumenty musí být v zabezpečeném archivu, pak je zajištěna relativní bezpečnost. Papír se lehce poškodí.
Nároky na skladovací prostor	K7	2	Velké nároky na skladovací prostory.
Dlouhodobá čitelnost	K8	3	Nutné použít kvalitní potřeby a zvolit dobré uložení.

Následuje společný úvod pro druhý a třetí scénář.

13.5. Společný úvod pro druhý a třetí scénář

Druhý a třetí scénář mají společnou část nákladů, kterou popíši nejdříve. Poté bude následovat pro každou situaci specifická část výpočtů nákladů na infrastrukturu a ukázání celkových nákladů.

Mezi další náklady firmy spadá pořízení kvalifikované elektronické značky, kde cena k 31. 3. 2014 činí 645 Kč na jeden rok. Do kalkulace tuto cenu započítávat nebudu, podobně jako u tisknutých a ručně podepisovaných dokumentů nezapočítávám cenu za propisky, razítka a jejich inkoust.

Samozřejmě, že společnost potřebuje uchovávat některé dokumenty i v listinné podobě z důvodu různých kontrol či podpisy nových smluv, které se následně digitalizují. V rámci případové studie byl objem takovýchto dokumentů stanoven na 30 % z celkového počtu.

13.5.1. Celkový počet stran

Předpokládám, že velká část dokumentů je potřeba tisknout dvakrát, například smlouvy. Jako koeficient pro tyto případy jsem zvolil hodnotu 1,8[10]. Výsledný počet stran je uveden pod tímto textem.

Tabulka 8. Počet stran

Období 5 let	**Počet stran**	**Počet stran s koeficientem 1,8**
První	75 000,00	135 000,00
Druhé	97 500,00	175 500,00
Třetí	116 250,00	209 250,00
Čtvrté	135 000,00	243 000,00
Souhrn	423 750,00	762 750,00

Objem tisknutých dokumentů je uveden v tabulce 9 níže:

Tabulka 9. Počet dokumentů a stran za jednotlivá období

Období	**Přírůstek dokumentů za rok**	**Dohromady dokumentů za období**	**Dohromady stran za období**
Prvních 5 let	3 000	15 000	135 000
Druhých 5 let	3 900	19 500	175 500
Třetích 5 let	4 650	23 250	209 250
Čtvrtých 5 let	5 400	27 000	243 000
Souhrn	84 750	84 750	762 750

Celkem tedy firma za 20 let vyprodukuje 84 750 dokumentů. Všechny tyto dokumenty chce archivovat a úředně ověřit. U každého dokumentu se předpokládá 5 stran. Dohromady to je 762 750 stran.

[10] Zvoleno na základě konzultace u zástupce Software602.

13.5.2. Náklady na tisk

Náklady na tisk, tonery a tiskárny jsou znázorněny v tabulce 10:

Tabulka 10. Kalkulace tiskových nákladů za jednotlivá období

Období 5 let	Počet tiskáren	Cena za tiskárny	Počet stran na tiskárnu	Počet tonerů	Cena za tonery	Cena za stránky
První	1	15 000	135 000,00	67,50	202 500,00	54 000,00
Druhé	2	30 000	87 750,00	43,88	131 625,00	70 200,00
Třetí	2	30 000	104 625,00	52,31	156 937,50	83 700,00
Čtvrté	2	30 000	121 500,00	60,75	182 250,00	97 200,00
Souhrn	7	105 000	448 875,00	224,44	673 312,50	305 100,00

Jak je vidět v tabulce 10 výše, náklady na tiskárny, tonery a stránky, činí 1 083 412,50 Kč.

13.5.3. Celkové náklady

Předpokládám, že v každém dokumentu jsou 2 podpisy, které je také nutné úředně ověřit. A dále předpokládám, že počet dokumentů nutný k ověření jsou 2 %[11] z celkového počtu všech dokumentů. Pro ověření stránek a podpisů počítám s původním počtem dokumentů, tedy bez násobení konstantou 1,8.

Tabulka 11. Kalkulace nákladů na ověření stránek a podpisů

Náklady	Cena
Celkové náklady na tisk	1 083 412,50
Náklady na ověření 1 stránky dokumentu	30,00
Náklady na ověření 1 podpisu	30,00
Počet dokumentů k ověření	1 695
Počet podpisů k ověření	3 390
Počet stran k ověření	8 475
Náklady na ověření všech stránek	254 250,00
Náklady na ověření podpisů	101 700,00
Náklady na tisk a ověření celkem	1 439 362,50

Celkové náklady ve společné části pro druhý a třetí scénář jsou podle tabulky 11 vyčísleny na 3 225 696,43 Kč.

Následuje druhý modelový scénář, kde je archivace prováděna na vlastní infrastruktuře.

[11] Zvoleno na základě konzultace u zástupce Software602.

13.6. Druhý scénář

Výše jsem vyčíslil náklady na tisk 30 % dokumentů. Následuje kalkulace druhého scénáře založeného na vlastní infrastruktuře.

13.6.1. Náklady na vlastní infrastrukturu

Společnost Pokus, s.r.o. si nakoupila vlastní infrastrukturu, kterou po pěti letech obměňuje[12].

- Server v ceně 10 000 Kč.
- 4 1TB disky, každý za 2 500 Kč. Disky budou zapojeny do pole RAID 10. Budou tedy zapojeny po dvojicích, kdy nejdříve zapisujeme na jeden disk a data se zároveň zrcadlí na druhý. Po jejich zaplnění obdobně postupujeme s druhou dvojicí. Výhodou jsou redundantní data, nevýhodou je využití pouze poloviční kapacity disků.

Předpokládám, že po každých pěti letech se cena komponent sníží na 70 %[13] ceny předchozích.

Do ceny řešení nezapočítávám cenu energií. Samotná kalkulace infrastruktury je uvedena níže v tabulce.

Tabulka 12. Kalkulace infrastruktury

Období 5 let	**Cena za server**	**Cena za disky**	**Počet dokumentů**	**Cena za dokumenty**
První	10 000	10 000	50 000	50 000
Druhé	7 000	7 000	65 000	65 000
Třetí	4 900	4 900	77 500	77 500
Čtvrté	3 430	3 430	90 000	90 000
Souhrn	25 330	25 330	282 500	282 500

[12] Ceny a doba vyplynula z konzultace u zástupce Software602.
[13] Vyplynulo z konzultace u zástupce Software602.

13.6.2. Celkové náklady druhého scénáře

Pro celkovou kalkulaci jsem sečetl v tabulce níže náklady na tisk s náklady na infrastrukturu.

Tabulka 13. Celková kalkulace druhého scénáře

Náklady	Cena
Náklady na tisk a ověření celkem	1 439 362,50
Celková cena za infrastrukturu	333 160
Souhrn	1 772 522,50

Kalkulace druhého scénáře je 1 772 522,50 Kč.

13.6.3. Vícekriteriální analýza druhého scénáře

Zhodnocení druhého scénáře vícekriteriální analýzou je znázorněno v tabulce 14.

Tabulka 14. Vícekriteriální analýza druhé varianty

Kritérium	Označení	Hodnota	Komentář
Dostupnost dat	K1	8	Rychlý server zajistí data v krátké době.
Přehlednost v datech	K2	8	Data jsou přehledně uložena discích.
Ekologický přístup	K3	5	Tisk dokumentů je menší, existují náklady na provoz infrastruktury.
Jednoduchost řešení	K4	7	Vše je uloženo na serveru, o který se musíme starat.
Pohodlí	K5	7	Zajištěné podepisování dokumentů a přidání časových razítek ušetří spoustu času.
Bezpečí dokumentů	K6	7	Data jsou redundantní, potřeba ochránit server.
Nároky na skladovací prostor	K7	8	Střední nároky na skladovací prostory.
Dlouhodobá čitelnost	K8	9	Čitelnost zajištěna použitím správných formátů a zajištěním integrity a autenticity dat.

V příští podkapitole je třetí, a zároveň poslední, modelový scénář založený na cloudové infrastruktuře.

13.7. Třetí scénář

Ve společném úvodu pro druhý a třetí scénář jsem kalkuloval náklady na tisk 30 % dokumentů. Velikost dokumentu, kterou zabírá v úložišti, předpokládám 250 kB[14]. Vybral jsem dva cloudové poskytovatele[15], firmu Google s produktem Drive a firmu Microsoft s úložištěm OneDrive. Pro oba jsem vypracoval kalkulaci zvlášť.

13.7.1. Náklady na cloudovou infrastrukturu

U Google Drive je 15 GB zdarma. Pro první období tedy není potřeba žádná investice do úložiště, pro další období je nutné zaplatit za využití 100 GB. Měsíční částka je 1,99 $, pro převod na českou korunu předpokládám 20 Kč za 1 americký dolar[16]

Služba společnosti Microsoft nazvaná OneDrive, nabízí 7 GB zdarma, to vystačí na první dva roky prvního období. Dále je nutné investovat po zbytek prvního období, celé druhé a třetí období 480 Kč ročně za využití 50 GB. Pro čtvrté období je nutné zaplatit 960 Kč za 100 GB. Všechny ceny Microsoft uvádí rovnou v českých korunách.

Následuje kalkulace cloudové infrastruktury.

Tabulka 15. Kalkulace nákladů na cloud a dokumenty

Období 5 let	**Google Drive**	**OneDrive**	**Počet dokumentů**	**Cena za dokumenty**
První	0	1 440	50 000	50 000
Druhé	2 388	2 400	65 000	65 000
Třetí	2 388	2 400	77 500	77 500
Čtvrté	2 388	4 800	90 000	90 000
Souhrn	7 164	11 040	282 500	282 500

13.7.2. Celkové náklady třetího scénáře

Celková kalkulace pro Google Drive a OneDrive:

Tabulka 16. Celková kalkulace s využitím Google Drive a OneDrive

Popis	**Google Drive**	**OneDrive**
Náklady na tisk a ověření celkem	1 439 362,50	1 439 362,50
Celková cena za infrastrukturu	7 164	11 040
Souhrn	1 446 526,50	1 450 402,50

[14] Vytvořil jsem 10 pětistránkových dokumentů s různým množstvím textu a velikost se pohybovala kolem této hodnoty.

[15] Službou Long-Term Docs podporuje zatím pouze produkty firem Google a Microsoft, z tohoto důvodu jsou vybrány jejich cloudové produkty.

[16] K 31. 3. 2013 byl kurz koruny vůči americkému dolaru 19,9 Kč, pro jednodušší výpočet jsem kurz zaokrouhlil.

13.7.3. Vícekriteriální analýza třetího scénáře

Pro oba poskytovatele cloudu postačí jedna společná vícekriteriální analýza. Liší se pouze cenou a detaily ve smluvních podmínkách. Hodnoty a komentáře jsou uvedeny v tabulce 17.

Tabulka 17. Vícekriteriální analýza třetího scénáře

Kritérium	Označení	Hodnota	Komentář
Dostupnost dat	K1	8	Cloudové služby mají malé riziko výpadků služeb, větší riziko hrozí od poskytovatelů připojení k Internetu. Riziko odchodu cloudového poskytovatele.
Přehlednost v datech	K2	8	Data jsou přehledně uložena v cloudu.
Ekologický přístup	K3	6	Tisk dokumentů je menší, existují náklady na cloud.
Jednoduchost řešení	K4	8	Vše je uloženo v cloudu, odpadá údržba serveru.
Pohodlí	K5	7	Zajištěné podepisování dokumentů a přidání časových razítek ušetří spoustu času.
Bezpečí dokumentů	K6	7	Data jsou redundantní.
Nároky na skladovací prostor	K7	9	Malé nároky na skladovací prostory.
Dlouhodobá čitelnost	K8	9	Čitelnost zajištěna použitím správných formátů a zajištěním integrity a autenticity dat.

13.8. Shrnutí nákladů za všechny scénáře

Na předchozích stránkách jsem ukázal tři modelové příklady archivování. Nejdříve byla nulová digitální archivace, následovala archivace na vlastní infrastruktuře a nakonec proběhla archivace na cloudové infrastruktuře.

V tabulce 18 jsou k porovnání celkové náklady za jednotlivé modelové scénáře.

Tabulka 18. Srovnání celkových nákladů za jednotlivé scénáře

Popis	Celkové náklady
První scénář	3 225 696,43 Kč
Druhý scénář	1 772 522,50 Kč
Třetí scénář, úložiště Google Drive	1 446 526,50 Kč
Třetí scénář, úložiště OneDrive	1 450 402,50 Kč

Z výše uvedených dat plyne cenová nevýhodnost papírové archivace. Využití digitální archivace na vlastní architektuře je již mnohem výhodnější, výhodou jsou data pod

vlastní kontrolou. Třetí scénář s využitím cloudového úložiště je cenově nejvýhodnější. Cenový rozdíl mezi cloudovými poskytovateli je minimální.

13.9. Vícekriteriální analýza

U této analýzy nejdříve podle důležitosti spočítám body za dané kritérium a váhu kritéria.

b_i... Body za dané kritérium, kde i je řádek.
v_i... Váha, spočítá se takto: $v = \frac{b_i}{\sum_{i=0}^{n} b_i}$, kde n je celkový počet kritérií a i je řádek.

Tabulka 19. Váhy pro jednotlivá kritéria

Kritérium	**Označení**	**Důležitost**	b_i	v_i
Dostupnost dat	K1	1-2	7,5	0,208333333
Přehlednost v datech	K2	4	5	0,138888889
Ekologický přístup	K3	8	1	0,027777778
Jednoduchost řešení	K4	6	3	0,083333333
Pohodlí	K5	5	4	0,111111111
Bezpečí dokumentů	K6	3	6	0,166666667
Nároky na skladovací prostor	K8	7	2	0,055555556
Dlouhodobá čitelnost	K9	1-2	7,5	0,208333333
Suma	X	X	36	1

Po spočtení bodů a vah za jednotlivá kritéria jsem v souhrnné tabulce 19 uvedl kritéria za jednotlivé scénáře, spočítal ideální hodnotu a bazální hodnotu. Tyto hodnoty použiji pro normalizovanou matici.

- Ideální hodnota H je veličina, která dosahuje ve všech kritériích nejlepší možné hodnoty.

- Bazální hodnota D je hodnota, jejíž ohodnocení je nejhorší podle všech kritérií.

Jako typ kritéria jsem zvolil maximalizační (Max), kde nejlepší hodnoty mají nejvyšší body.

Tabulka 20. Souhrn kritérií

	K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**
Typ kritéria	Max	Max	Max	Max	Max	Max	Max	Max
První scénář	3	3	1	3	3	5	2	3
Druhý scénář	8	8	5	7	7	7	8	9
Třetí scénář	8	8	6	8	7	7	9	9
Ideální hodnota Hj	8	8	6	8	7	7	9	9
Bazální hodnota Dj	3	3	1	3	3	5	2	3
Hj-Dj	5	5	5	5	4	2	7	6

Normalizovanou matici spočtu podle vzorce: $x_{i,j} = \frac{y_{i,j} - D_j}{H_j - D_j}$, kde i je index řádku a j je index sloupce.

Tabulka 21. Normalizovaná matice

První scénář	0	0	0	0	0	0	0	0
Druhý scénář	1	1	0,8	0,8	1	1	0,857143	1
Třetí scénář	1	1	1	1	1	1	1	1

13.9.1. Vyhodnocení vícekriteriální analýzy

Podle vážených součtů jsem sestavil takovéto pořadí:

Tabulka 22. Výsledná tabulka

scénář	**Vážený součet**	**Pořadí**	**Náklady**
První scénář	0	3	3 225 696,43 Kč
Druhý scénář	0,969841	2	1 772 522,50 Kč
Třetí scénář	1	1	1 446 526,50 Kč (Google Drive) 1 450 402,50 Kč (OneDrive)

Není žádné překvapení, že čistě listinná archivace vyšla nejhůře, oproti výhodám softwarového řešení nenabízí žádnou zásadní přednost. U druhého a třetího scénáře, tedy vlastní a cloudové infrastruktury, výsledek tak jednoznačný již není. Vítězí zde sice cloudové řešení, ale ne s žádným výrazným rozdílem. Pokud má někdo nedůvěru svěřit data „do mraku“, je pro něj vhodnou volbou vlastní server s diskovým polem, o které je nutné se starat.

13.9.2. Shrnutí modelového příkladu

Z pohledu vícekriteriální analýzy i cenové výhodnosti vyplývá, že archivace v cloudovém úložišti je nejvýhodnější. Pro společnost, která se nechce starat o vlastní infrastrukturu, je to jednoznačná volba.

A co konzervativní firmy, které se drží klasické papírové archivace? Z tabulky 22 vyplývá, že z pohledu nákladů je to nejhorší možnost a podle vícekriteriální analýzy bychom jednoznačně měli od této varianty upustit.

Závěr

Hlavním cílem teoretické části bylo seznámit čtenáře se všemi aspekty, které se týkají dlouhodobé digitální archivace. Tento cíl jsem obsáhl popsáním formátu PDF/A, zabezpečením dokumentu a jeho uchováním v archivu.

V praktické části byla prvním cílem analýza současné evropské směrnice a připravovaného nařízení. Analýzu jsem provedl a zjistil, že nedostatky současné směrnice v novém nařízení již nejsou. Zůstává ale otevřená otázka, jak se nařízení ujme v praxi a jaké se objeví nové nedostatky. Druhým cílem byl modelový příklad, na kterém jsem ukázal, že je jednoznačně výhodné mít digitální archiv. Konkrétně jej mít umístěný v cloudu.

Všechny stanovené cíle se podařilo splnit.

Přínosem pro čtenáře je seznámení se s problematikou dlouhodobé archivace. Při archivaci dokumentů je potřeba sledovat aktuální trendy, změny v národních a také evropských předpisech.

Nesmíme opomenout bezpečnost archivovaných dokumentů. Proto se k nim přikládá elektronický podpis a časové razítko, které dokládá existenci a nezměněnost dokumentu. Toto razítko má omezenou platnost a je nutné dokument před vypršením jeho platnosti, opatřit razítkem novým. Vývoj jde rychle dopředu a při ochraně integrity dokumentu by mohlo dojít k jejímu prolomení. Proto je třeba zjišťovat zprávy o prolomení šifer a postupně používat šifry výkonnější.

Při dlouhodobé archivaci dokumentů je musíme uložit do formátu, který budeme schopni přečíst i za mnoho let. V současné době je tímto formát PDF/A. Tento formát se neustále vyvíjí a již obsahuje 3. verzi, která přináší další vylepšení a možnosti ukládání.

Zabýval jsem se poskytovateli dlouhodobé archivace. Je mezi nimi velký rozdíl v ochotě sdělovat informace veřejnosti. Vítězem v otevřenosti je společnost Software602, která pořádá semináře pro veřejnost. Zároveň se snaží nabízet inovativní produkty. Za zmínku ještě stojí firma Sefira. Není již tolik inovativní, ale také se snaží být vstřícná k veřejnosti, ve které vidí své potenciální klienty. Obě tyto firmy jsem měl možnost navštívit a konzultovat s jejich odborníky danou problematiku i svoji práci. Na opačném konci tohoto pomyslného žebříčku je společnost O_2, která nemá ochotu sdělovat podrobnější informace o svých produktech.

Dle vyjádření poskytovatelů řešení archivace spousta firem nevyužívá jejich služeb a nearchivují data digitálně, protože se jim stále finančně vyplatí jednou za čas zaplatit pokutu.

Praktická část obsahuje analýzu současné a připravované legislativy. Dále je součástí kalkulace a vícekriteriální analýza tří modelových scénářů, na kterých jsem demonstroval jejich výhody a nevýhody a také cenu. Z výsledků jednoznačně vyplývá, že archivování pouze v papírové podobě je nejvíce finančně nákladné a přináší mnoho překážek. Scénář s archivací v cloudovém úložišti vyšel jako nejvýhodnější.

V rámci bakalářské práce jsem zjistil, že archivace dat je zajímavý a perspektivní obor. Považuji jej za důležitý, protože elektronická zařízení jsou všude kolem nás a je potřeba data uchovat a zajistit jim právní platnost. Zde vidím velký prostor pro další navázání na mé poznatky. V době psaní této práce ještě nebylo v platnosti nové nařízení Evropského parlamentu o elektronické identifikaci. Bude zajímavé sledovat jeho dopady na praxi.

Příloha A.

V této příloze jsou podrobněji zmíněny zákony týkající se dlouhodobé archivace dat.

A.1. Zákony týkající se archivní a spisové služby

A.1.1. Zákon č. 499/2004 Sb., o archivnictví a spisové službě

Zákon definuje záznamy pro trvalé uchování (archiválie), způsoby zacházení s nimi, jejich ochranu. Dále to jsou práva a povinnosti držitelů a správců archiválií a zřizovatelů archivů. Zákon také specifikuje konverzi dokumentů a působnost Ministerstva vnitra a další správní úřady.

A.1.2. Vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby

Tato vyhláška je o podrobnostech výkonu spisové služby. Nahradila vyhlášku 191/2009 Sb.

A.1.3. Věstník Ministerstva vnitra č. 64/2012

Národní standard pro elektronické systémy spisových služeb.

A.1.4. Zákon č. 563/2001 Sb., zákon o účetnictví

Zde je definována elektronická faktura pod pojmem „záznam v technické formě“.

A.1.5. Vyhláška č. 191/2009 Sb.

Vyhláška o podrobnostech výkonu spisové služby stanovuje konkrétní požadavky na archivaci, skartaci a příjem dokumentů, také jejich podepisování a označování.

A.1.6. Vyhláška č. 193/2009 Sb.

Vyhláška o stanovení podrobností elektronické konverze dokumentů definuje požadavky na dokument, např. formát a také konverzi dokumentů.

A.1.7. Vyhláška č. 194/2009 Sb.

Vyhláška o užívání a provozování informačního systému datových schránek upravuje náležitosti datových schránek. Jedná se o definování přihlašování, formát zpráv, maximální velikost zpráv, apod.

A.1.8. Vyhláška č. 496/2004 Sb.

Vyhláška o elektronických podatelnách definuje povinnosti úřadů při vedení elektronické podatelny, práci s elektronickým podpisem a archivaci příchozích a odchozích zpráv.

A.1.9. Zákon č. 263/2011 Sb.

Zákon, kterým se mění zákon o informačních systémech veřejné správy, umožňuje zřídit kontaktní místo Czech POINT v bankách. Dále umožňuje začlenit datovou schránku do internetového bankovnictví a mění pravidla pro předávání datových zpráv mezi fyzickými a právnickými osobami.

A.2. Zákony o elektronickém podpisu

A.2.1. Zákon č. 227/2000 Sb., o elektronickém podpisu

Zákon definuje náležitosti kvalifikovaných elektronických podpisů, dále povinnosti vlastníků podpisů a certifikačních autorit.

A.2.2. Vyhláška č. 212/2012 Sb.

Vyhláška o ověřování platnosti elektronického podpisu detailně řeší strukturu údajů, které umožňují identifikovat podepisující osobu. Je zde uveden postup při ověřování elektronického podpisu a časového razítka.

A.3. Zákony o autorizované konverzi

V těchto zákonech jsou definována pravidla pro konverzi elektronických dokumentů do listinné formy a také opačně. Dále pokrývá veškerou problematiku datových schránek, zacházení s nimi, definuje požadavky na informační systém datových schránek a zacházení s datovými zprávami.

A.3.1. Zákon č. 300/2008 Sb.

Zákon definuje elektronické úkony a autorizovanou konverzi dokumentů. Z tohoto zákona vychází Informační systém datových schránek.

Příloha B.

Obsah přiloženého CD

Zde je uveden seznam všech příloh přiloženého CD.

- *thesis* - složka se zdrojovými texty v LaTeX
- thesis.pdf - bakalářská práce ve formátu PDF

Literatura

[1] *Zálohování vs archivace*. URL: http://thedatarescuecenter.com/blog/wp-content/uploads/Untitled-1.jpg (cit. 26. 11. 2013).

[2] *Obecně o elektronickém archivačním systému*. 2009. URL: http://www.hsicom.cz/systemy-dms/e-arsys-elektronicky-archiv (cit. 26. 11. 2013).

[3] *PDF/A*. URL: http://www.pdfa.org/wp-content/uploads/2011/08/pdffileimages.jpg (cit. 26. 11. 2013).

[4] *Zákon o elektronickém podpisu*. 2000. URL: http://portal.gov.cz/app/zakony/download?idBiblio=49532&nr=227~2F2000~20Sb.&ft=pdf (cit. 07. 04. 2014).

[5] *Princip tvorby důvěryhodného dokumentu u*. URL: https://www.secustamp.eu/cs/secustamp-tsa-cartridge (cit. 26. 11. 2013).

[6] *Elektronický podpis — Wikipedie: Otevrená encyklopedie*. URL: http://cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg (cit. 27. 11. 2013).

[7] *PKI-E*. URL: http://www.cipher.risk.tsukuba.ac.jp/wordpress/wp-content/uploads/2012/02/pki_e.png (cit. 26. 11. 2013).

[8] *Cryptographic Message Syntax: RFC 2630*. 1999. URL: http://www.ietf.org/rfc/rfc2630.txt (cit. 07. 04. 2014).

[9] *6.1.8 The Open Archival Information System*. 2009. URL: http://www.iasa-web.org/tc04/open-archival-information-system-oais (cit. 26. 11. 2013).

[10] *Logo O2*. URL: https://www.telefonica.cz/_pub/a6/fb/2b/237540_504860_O2_RGB.jpg (cit. 27. 11. 2013).

[11] *Logo Fujitsu*. URL: http://www.fujitsu.com/fts/Images/Fujitsu_Logo_screen_tcm21-73457.jpg (cit. 27. 11. 2013).

[12] *Logo Software602 a.s.* URL: http://www.602.cz/sites/all/themes/602k/logo.png (cit. 27. 11. 2013).

[13] Pavel Novotný. *Úvod do kryptologie: Digitální podepisování pomocí asymetrické kryptografie*. 2010. URL: https://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/Digitalni_podpis.pdf (cit. 06. 03. 2014).

[14] *Logo Fujitsu - SecDocs*. URL: https://www.openlimit.com/assets/images/_grafiken/deutsch/Fujitsu-SecDocs-powered-by-OpenLimit.gif (cit. 27. 11. 2013).

[15] *Vícekriterální analýza variant*. 2005. URL: http://pef.czu.cz/~BROZOVA/CASESTUDY/VAV1.html (cit. 01. 04. 2014).

[16] *PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN POSOUZENÍ DOPADŮ: Průvodní dokument k návrhu nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu*. 2012. URL: www.mvcr.cz/soubor/003-pruvodni-dokument-k-navrhu-narizeni-ep-a-rady-docx.aspx (cit. 07. 04. 2014).

[17] Ladislav Cubr. *Dlouhodobá ochrana digitálních dokumentů*. Národní knihovna České republiky, 2010, s. 154. ISBN: 978-80-7050-588-5.

[18] Jiří Peterka. *Báječný svět elektronického podpisu*. CZ.NIC, 2011, s. 430. ISBN: 978-80-904248-3-8.

[19] *Národní archiv*. URL: http://www.nacr.cz/ (cit. 01. 10. 2013).

[20] *Rozdíl mezi archivací a zálohováním*. 2012. URL: http://www.zalohovani.net/rozdil-mezi-archivaci-a-zalohovanim (cit. 08. 10. 2012).

[21] *Archivace a zálohování*. URL: http://www.storage.cz/622-archivace-jak-a-cim (cit. 08. 10. 2013).

[22] Jakub Žemlička. *Legislativní požadavky archivace elektronických dokumentů*. 2012. URL: http://www.systemonline.cz/sprava-dokumentu/legislativni-pozadavky-archivace-elektronickych-dokumentu.htm (cit. 27. 11. 2013).

[23] *PDF/A - nový formát pro archivaci a publikování nastupuje*. URL: http://www.svettisku.cz/buxus/generate_page.php?page_id=2969&buxus_svettisku=678c62a399fee88739549e7085976fc7 (cit. 10. 10. 2013).

[24] *Průlom v elektronické archivaci dokumentů*. URL: http://cfoworld.cz/ostatni/prulom-v-elektronicke-archivaci-dokumentu-1785 (cit. 10. 10. 2013).

[25] *Legislativní požadavky archivace elektronických dokumentů*. URL: http://www.systemonline.cz/sprava-dokumentu/legislativni-pozadavky-archivace-elektronickych-dokumentu.htm (cit. 10. 10. 2013).

[26] *3 Key Differences Between Backup and Archive*. URL: http://blogs.ironmountain.com/2013/service-lines/data-backup-and-recovery/3-key-differences-between-backup-and-archive/ (cit. 10. 10. 2013).

[27] *Elektronické dokumenty - SEFIRA*. URL: http://www.sefira.cz/cs/elektronicke-dokumenty (cit. 15. 11. 2013).

[28] *SecDocs – Digitální dlouhodobá archivace*. URL: http://www.fujitsu.com/cz/products/computing/storage/software/backup-archiving/secdocs/ (cit. 15. 11. 2013).

[29] *Logo ETSI*. URL: http://m2m.gemalto.com/tl_files/cinterion/content/main/Partner/Logo%20etsi.jpg (cit. 26. 11. 2013).

[30] *Logo Sefira spol. s.r.o.* URL: http://www.sefira.cz/image/layout_set_logo?img_id=11461&t=1384469456819 (cit. 27. 11. 2013).

[31] *Logo Česká pošta, s.p.* URL: http://media0.webgarden.name/images/media0:4cc47fbada355.jpg/logo%20%C3%84%C2%8Desk%C3%83%C2%A1%20po%C3%85%C2%A1ta.jpg (cit. 27. 11. 2013).

[32] *Logo Gordic spol. s.r.o.* URL: http://www.auroton.cz/sites/auroton.local/files/Gordic%20logo.jpg (cit. 14. 12. 2013).

[33] *Ceník Kvalifikovaných časových razítek*. 2013. URL: http://www.postsignum.cz/kvalifikovana_casova_razitka.html (cit. 06. 04. 2014).

[34] Vladimíra Hloušková. *Pravidla elektronické komunikace v rámci Evropské unie*. 2012. URL: http://www.systemonline.cz/it-pravo/pravidla-elektronicke-komunikace-v-ramci-eu.htm (cit. 06. 04. 2014).

[35] *The AdES family of standards: CAdES, XAdES, and PAdES: Implementation guidance for using electronic signatures in the European Union*. 2009. URL: http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf (cit. 06. 04. 2014).

[36] *Je výhodné mít data v cloudu?* 2012. URL: http://computerworld.cz/technologie/je-vyhodne-mit-data-v-cloudu-48581 (cit. 06. 04. 2014).

[37] *Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu.* 2012. URL: htwww.mvcr.cz/soubor/001-navrh-narizeni-ep-a-rady-docx.aspx (cit. 06. 04. 2014).

[38] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market.* 2012. URL: www.mvcr.cz/soubor/002-proposal-for-regulation-of-the-ep-pdf.aspx (cit. 06. 04. 2014).

[39] *Průvodní dokument k návrhu nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu.* 2012. URL: www.mvcr.cz/soubor/003-pruvodni-dokument-k-navrhu-narizeni-ep-a-rady-docx.aspx (cit. 06. 04. 2014).

[40] *Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market.* 2012. URL: www.mvcr.cz/soubor/004-accompanying-the-proposal-for-a-regulation-of-the-european-pdf.aspx (cit. 06. 04. 2014).

[41] *ETSI SR 001 604 V1.1.1 (2012-07).* 2012. URL: www.mvcr.cz/soubor/005-etsi-sr-001604-pdf.aspx (cit. 06. 04. 2014).

[42] *Obchodní podmínky pro poskytování služby Datový trezor.* 2014. URL: http://www.ceskaposta.cz/assets/sluzby/datove-schranky/datovy-trezor/Obchodni-podminky-pro-poskytovani-sluzby-Datovy-trezor.pdf (cit. 06. 04. 2014).