VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

DLOUHODOBÁ ARCHIVACE DIGITALNÍCH DOKUMENTŮ
LONG-TERM ARCHIVING OF DIGITAL DOCUMENTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Klára Zatloukalová

VEDOUCÍ PRÁCE
SUPERVISOR
prof. Ing. Vladimír Smejkal, CSc.

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zatloukalová Klára

Manažerská informatika (6209R021)

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

Dlouhodobá archivace digitalních dokumentů

v anglickém jazyce:

Long-term Archiving of Digital Documents

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Podle § 60 zákona č. 121/2000 Sb. (autorský zákon) v platném znění, je tato práce "Školním dílem". Využití této práce se řídí právním režimem autorského zákona. Citace povoluje Fakulta podnikatelská Vysokého učení technického v Brně.

Seznam odborné literatury:

LECHNER, T. Elektronické dokumenty v právní praxi. Praha: Leges, 2013. ISBN 978-80-87576-41-0.
MATES, P. a V. SMEJKAL. E-government v České republice. Právní a technologické aspekty. 2. podstatně přepracované a rozšířené vydání. Praha: Leges, 2012. 456 str. ISBN 978-80-87576-36-6.
SMEJKAL, V. a M. A. VALÁŠEK. Jak na datové schránky: Praktický manuál pro každého. Praha: LINDE, 2012. 200 str. ISBN 978-80-86131-80-1.
SMEJKAL, V. a M. A. VALÁŠEK. TEOTWAWKI elektronicky podepsaných dokumentů. Jak dlouhodobě zajistit důvěryhodnost elektronických dokumentů? Archivní časopis, ročník 61., 2011. č. 4. ISSN 0004-0398.

Vedoucí bakalářské práce: prof. Ing. Vladimír Smejkal, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Obsahem této práce jsou jednak teoretické poznatky z oblasti archivace digitálních dokumentů, vysvětlení některých pojmů a náhled do platné legislativy. Dále pak analýza současného stavu vývoje archivace digitálních dat v prostředí veřejné správy České republiky. Na základě všech teoretických znalostí bude navrženo, co je potřeba pro zajištění dlouhodobého úložiště digitálních dat, aby vyhovovalo z hlediska právních předpisů, dokazování obsahu a ochrany obsahu v rámci orgánu veřejné správy České republiky.

Abstract

The content of this thesis are theoretical knowledge from section long-term archiving of digital documents, explanation of terms and view for applicable legislation. Next point will be analysis of current state of archiving digital data in public administration of The Czech republic. Based on theoretical knowledge will be proposal what is needed for secure long-term archiving digital data to be able to meet in terms of legislation, proving content and content protection within the public administration of The Czech republic.

Klíčová slova

dokumenty; archiv; dlouhodobá archivace; datové schránky

Keywords

documents; archives; long term archiving; data boxes

Bibliografická citace

ZATLOUKALOVÁ, K. *Dlouhodobá archivace digitálních dokumentů.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 75 s. Vedoucí bakalářské práce prof. Ing. Vladimír Smejkal, CSc..

Čestné prohlášení

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

V Brně dne 25. 5. 2016 ……..……

podpis

Poděkování

Tímto bych ráda poděkovala vedoucímu této práce prof. Ing. Vladimíru Smejkalovi, CSc. za pomoc při tvorbě této bakalářské práce. Za všechny materiály a čas, který mi věnoval. Dále bych chtěla poděkovat Městskému úřadu Šumperk, konkrétně vedoucímu informačního oddělení Ing. Pavlovi Kouřilovi a zaměstnankyni spisové a archivační služby Bc. Ivaně Semrádové. V poslední řadě chci vyjádřit vděk společnosti Gordic spol. s.r.o. za trpělivou a přínosnou komunikaci.

OBSAH

ÚVOD 12

1 TEORETICKÁ VÝCHODISKA 13

1.1 Dokument 13

1.2 Digitální dokument 14

1.2.1 Základní rozdělení digitálních dokumentů 15

1.2.2 Digitální dokumenty prosté a rozšířené 15

1.3 Archivace 16

1.3.1 Archivace digitálních dokumentů 16

1.4 Národní archiv 18

1.4.1 Národní digitální archiv 18

1.4.2 Model OAIS (Open Archival Information Systém) 19

1.5 Nástroje pro autentizaci digitálních dokumentů 20

1.5.1 Elektronický podpis 20

1.5.2 Úrovně elektronického podpisu 21

1.5.3 Ověření elektronického podpisu 22

1.5.4 Kvalifikovaný certifikát 24

1.5.5 Poskytovatel certifikačních služeb 25

1.5.6 Uznávaná elektronická značka 26

1.5.7 Kvalifikované časové razítko 26

1.5.8 Nařízení eIDAS 28
1.6 Konverze dokumentů 29
1.7 Datová schránka 30
1.7.1 Komunikace prostřednictvím datové schránky 31
1.7.2 Datová zpráva 31
1.8 Zákon o archivnictví spisové službě 33
1.9 Spisová služba 34
1.9.1 Příjem dokumentů 35
1.9.2 Příjem dokumentů v elektronické podobě 36
1.9.3 Evidence dokumentů 37
1.9.4 Evidence dokumentů podle národního standardu pro elektronické systémy spisové služby 37
1.9.5 Vyřizování a podepisování dokumentů 39
1.9.6 Ukládání dokumentů 39
1.9.7 Spisový a skartační plán 39
1.9.8 Skartační režim 40
1.9.9 Skartační lhůta 40
1.9.10 Metadata spisů 41
1.10 Datové formáty PDF a PDF/A 41
2 ANALÝZA SOUČASNÉHO STAVU 43
2.1 Spisová služba 43
2.1.1 Specifika zavádění ERMS 44
2.2 Normy PAdES, CAdES, XAdES 44

2.3 Příprava archivace 46
2.3.1 Vyřízení dokumentu a spisu 46
2.3.2 Výstupní formáty dokumentů v digitální podobě 46
2.3.3 Příprava spisů a dokumentů k uložení do spisovny 47
2.3.4 Výběr archiválií 48
2.3.5 Výběr archiválií mimo skartační řízení 49
2.3.6 Postup při vybírání archiválií archivem 50
2.3.7 Předání dokumentů archivu 50
2.4 Ukládání digitálních dokumentů 52
2.4.1 Kategorie archivace podle doby uložení dokumentů 52
2.4.2 Krátkodobé uložení dokumentů 52
2.4.3 Střednědobé uložení dokumentů 53
2.4.4 Dlouhodobé uložení digitálních dokumentů 54
2.4.5 Trvalé uložení 55
3 NÁVRH VLASTNÍHO ŘEŠENÍ 56
3.1 Životní cyklus dokumentu 56
3.2 Udržení autenticity dokumentu 58
3.2.1 Archivní kvalifikovaná časová razítka 59
3.3 Zajištění důvěryhodného úložiště 60
3.3.1 Informační systémy veřejné správy (ISVS) 60
3.3.2 Možnosti implementace 61
3.4 Přehled potenciálních dodavatelů 62

4 ZÁVĚR 67

SEZNAM ZDROJŮ 69

SEZNAM POUŽITÝCH ZKRATEK 73

SEZNAM OBRÁZKŮ 74

SEZNAM TABULEK 75

ÚVOD

Archivace neboli uchovávání cenných historických písemností nebo předmětů sahá již do dávné minulosti. Nejstarším českým státním archivem byl rodový archiv Přemyslovců. V dnešní době na území České republiky se archivy dělí na veřejné a soukromé, kdy mezi veřejné řadíme Národní archiv, Archiv bezpečnostních služeb, státní oblastní archivy s organizačními jednotkami, kterými jsou státní okresní archivy, dále pak specializované archivy, bezpečnostní archivy a archivy územních samosprávných celků (6). Nejvýznamnějším archivem je Národní archiv. Ukládá a pečuje o dokumenty, které vznikly v rámci činnosti státních, městských nebo obecních orgánů veřejné moci.

I tyto orgány prošly v posledních letech neúprosnou modernizací a spoustu dokumentů, které bývaly například v listinné podobě, dnes nalezneme pouze v podobě elektronické. S tímto technologickým postupem nastal i problém v oblasti archivace. S uložením listinného dokumentu si v současné době poradit dokážeme. Zajistíme jeho ochranu, důkazy o tom, že se jedná o originál a také to, že z něj budeme schopni informace přečíst i za několik let. Postup archivace v případě digitálních dokumentů je o něco složitější. V systému digitalizace a následné archivace v České republice je stále spoustu mezer. Samotný projekt Národní digitální archiv se po 10 letech plánování a realizací pustil do zkušebního provozu teprve v roce 2014 a stále v něm přetrvává (7).

Tato práce se bude zaměřovat především na archivaci digitálních dokumentů v rámci orgánů veřejné správy. Konkrétně na uložení dokumentů, zachování jejich autenticity a neporušitelnosti v době, nežli bude dokument vybrán za archiválii a odeslán do Národního digitálního archivu.

Veřejnou správu můžeme popsat jako správu veřejných záležitostí, která sleduje naplňování veřejných cílů a je vykonávána ve veřejném zájmu, tedy opak správy soukromé, kterou vykonává každá fyzická nebo právnická osoba a sleduje tak soukromé cíle ve svém soukromém zájmu (20).

1 TEORETICKÁ VÝCHODISKA

Tato kapitola se bude týkat teoretických poznatků z oblasti dlouhodobé archivace digitálních dokumentů. Celá problematika bude zobrazena od úplného základu. Co je to dokument, jeho druhy, a co je potřeba k dokázání pravosti jeho obsahu a také co je samotná archivace a proč je za potřebí ji provádět. Z velké části tuto kapitolu budou tvořit citace ze zákonů, protože obsahují nejpřesnější definice těchto pojmů. Dále zde bude popsáno vše co je potřeba znát k vytvoření dlouhodobého úložiště digitálních dat, tak aby vše korespondovalo z právního hlediska.

1.1 Dokument

Přímá definice slova dokumentu je obsažena v zákoně č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů (dále jen ArSSZ) § 2 písm. e) kde je stanoveno, že *„dokumentem se rozumí každá písemná, obrazová, zvuková nebo jiná záznamová informace, ať již v podobě analogové či digitální, která byla vytvořena původcem*[1] *nebo byla původci doručena.“* Ještě obecněji lze definovat dokument jako *každý pramen informaci na nějakém nosiči, který je uchovatelný v čase“* (28, s. 34).

Způsoby ztvárnění dokumentu

Rozlišujeme dva způsoby ztvárnění dokumentu – analogovou a digitální. Za analogový záznam se obecně považuje každý záznam prováděný signálem se spojitě proměnlivým průběhem; v archivnictví se za analogový záznam označuje i záznam zapsaný na nějakém nosiči, který je vnímatelný zrakem (2). Pojmem analogový dokument si spoustu lidí spojuje s listinnou podobou dokumentu, což není zcela správně. Analogový dokument může mít i jiné podoby, např. text vytesaný do kamene, 3D objekt, filmový pás, kresba na dřevěnou destičku aj (1).

Digitální dokument je oproti tomu reprezentován posloupností znaků bitů (stavy 0 a 1 ve dvojkové soustavě). Digitální dokument je principiálně nezávislý na konkrétním nosiči, který tak přestává plnit svou původní roli prostředku k časoprostorovému

[1] Podle § 2 písm. d) ArSSZ je původcem každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán.

transferu informací, a informace takto zachycené jako by z pohledu uživatele ztratily „hmotnou“ podobu (2).

Z výše uvedeného vyplývá, že digitální dokument nelze vnímat přímo, ale prostřednictvím určitého technického zařízení – počítače, mobilního telefonu apod.

1.2 Digitální dokument

Jedna z vlastností, kterou se digitální dokument výrazně liší od analogového dokumentu, je originalita. Zatímco analogový, konkrétně listinný dokument, má originál jen jeden, a nelze vytvořit jeho duplikát (kopii), aniž by byl bez viditelného rozdílu, duplikát digitálního dokumentu je sám o sobě originálem (1).

Další ze specifických vlastností může být nezávislost na konkrétním nosiči, převoditelnost. Máme-li dokument v analogové podobě a zanikne jeho nosič, zanikne i dokument sám o sobě, kdežto digitální dokument můžeme před zánikem nosiče převést na jiný nosič nebo jej zálohovat a stále se bude jednat o originál (1).

V následující tabulce je srovnání některých dalších vlastností digitálního dokumentu s vlastnostmi analogového – listinného dokumentu.

Atribut	Listinný dokument	Elektronický dokument
Tvorba	Lze přímo napsat na hmotný nosič	Vytváření pomocí technických nástrojů
Čtení	Pouze pomocí vlastních smyslů	Zprostředkovaně pomocí technických nástrojů
Ochranné prvky	Podpis Úředně potvrzený podpis Pečeť Další ochranné prvky použité např. na bankovkách	Uznávaný elektronický podpis Kvalifikovaná elektronická značka Elektronické časové razítko Další ochranné prvky budoucnosti
Přístup k originálu	Jeden originál	Nekonečně mnoho originálů
Přístup k ochraně	Když chráním originál,	Když chráním originál,

	chráním nosič Když zničím originál, jiný už nemůže být	chráním data Když zničím originál, nikdy nevím, byl-li poslední nebo jich jsou ještě tisíce kdekoliv uloženy

Tab. 1Rozdíl mezi listinným a digitálním dokumentem. (1, s. 43)

1.2.1 Základní rozdělení digitálních dokumentů

Rozlišujeme dva druhy digitálních dokumentů. Ty, které přímo v digitální podobě vznikly a ty, které do ní byly převedeny z podoby analogové pomocí scanneru nebo fotoaparátu (1).

V dnešní době je již možné využít metody OCR (Optical Character Recognation), které dokáže pomocí scanneru digitalizovat tištěné texty tak, aby se s nimi nadále dalo pracovat a upravovat je, a zároveň dokáže zachovat potřebné atributy dokumentu, např. razítka, loga, podpisy a jiné v obrazové podobě (1).

1.2.2 Digitální dokumenty prosté a rozšířené

Digitální dokumenty jsou v zásadě ve dvou variantách:

1. Prosté dokumenty, tj. bez použití jakýchkoliv nástrojů, umožňujících identifikaci a autentizaci podepsané osoby a/nebo jiných atributů (bez elektronického podpisu, značky a bez časových razítek). Archiv, systém spisové služby atd. sice může tyto dokumenty doplnit elektronickým podpisem, značkou nebo časovým razítkem jako indicii jejich existence v konkrétním čase, ale tím nezískáme žádné další informace, natož jistotu, kdo a kdy dokument vytvořil či jej podepsal.

2. Dokumenty s rozšířenými vlastnostmi, umožňující je pomocí různých, převážně kryptografických nástrojů opatřit atributem (-y) určujícím (-i) některé charakteristiky související se vznikem, případně modifikací dokumentu (elektronicky podepsané nebo označené dokumenty včetně dokumentů opatřených časovým razítkem) (2). Tyto dokumenty jsou tedy těmito nástroji a postupy autentizovány a ukotveny v čase, což umožní ověřit jejich pravost i se značným časovým odstupem.

1.3 Archivace

„Archivace zajišťuje dlouhodobé uložení vybraných dat až do okamžiku, kdy se musí archivní systém postarat o jejich certifikované a doložitelné odstranění“ (9). Dle § 2 písm. f) ArSSZ se archiváliı rozumí *„takový dokument, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiváliı; archiváliemi jsou i pečetidla, razítka a jiné hmotné předměty související s archivním fondem či s archivní sbírkou, které byly vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrány a vzaty do evidence.“* Místo, kam se archiválie ukládají a pečuje se o ně, je archiv (9).

1.3.1 Archivace digitálních dokumentů

Součástí ArSSZ je možnost převodu dokumentů z analogové podoby do digitální. Archivaci je tedy díky tomu možno provádět v jakékoli formě.

Podle § 13 odst. 5 původce, který nevykonává spisovou službu v elektronické podobě v elektronických systémech spisové služby, musí převést dokument v digitální podobě určený k výběru archiváliı mimo skartační řízení do výstupního datového formátu stanoveného prováděcím právním předpisem a opatřit ho metadaty stanovenými prováděcím právním předpisem podle § 19 písm. g)[2], a to nejpozději při přípravě výběru archiváliı mimo skartační řízení. Pokud dokument nelze převést do stanoveného datového formátu a opatřit ho metadaty (ani ve spolupráci s příslušným archivem) dokument jeho původce převede do analogové, tedy papírové podoby.

Zvláštní ustanovení o dokumentech v digitální podobě popisuje v pěti odstavcích § 69a.

V prvním odstavci uvádí, že převádění dokumentu v analogové podobě na dokument v digitální podobě nebo naopak a změnu datového formátu dokumentu v digitální podobě

[2]§ 19 písm. g)rozsah metadat dokumentů v digitální podobě vybraných jako archiválie mimo skartační řízení u původců, kteří nevykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby

provádí původce tak, aby zaručil věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu.

V druhém odstavci stanoví, že připojení údajů, které vznikly při přípravě dokumentu k uchování podle § 3 odst. 5 (tj. metadata a údaje prokazující existenci dokumentu v čase) nebo při převedení či změně datového formátu dokumentu podle prvního odstavce a které jsou pro uchování dokumentu nebo převedení nebo změnu datového formátu dokumentu nezbytné, se nepovažuje za nezajištění neporušitelnosti obsahu dokumentu.

Dále pak před převedením dokumentu v digitální podobě na dokument v analogové podobě nebo změnou datového formátu dokumentu v digitální podobě ověří původce platnost uznávaného elektronického podpisu, uznávané elektronické značky nebo kvalifikovaného časového razítka, pokud je jimi dokument v digitální podobě opatřen, a platnost kvalifikovaných certifikátů, na kterých jsou založeny. Údaje o výsledku ověření a datum převedení dokumentu v digitální podobě na dokument v analogové podobě nebo datum změny datového formátu dokumentu v digitální podobě určený původce zaznamená a uchová je spolu s dokumentem vzniklým převedením nebo změnou datového formátu.

Dokument v digitální podobě vzniklý převedením z dokumentu v analogové podobě nebo změnou datového formátu dokumentu v digitální podobě opatří původce doložkou, která bude obsahovat údaje o převedení nebo změny datového formátu, podepsanou uznávaným elektronickým podpisem osoby odpovědné za převedení z dokumentu v analogové podobě anebo změnu datového formátu dokumentu v digitální podobě nebo označenou elektronickou značkou určeného původce, a dále opatřenou kvalifikovaným časovým razítkem. Údaje týkající se převedení nebo změny datového formátu stanoví prováděcí právní předpis.

V posledním, pátém odstavci říká že, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem.

1.4 Národní archiv

Národní archiv sídlící v Praze je od 1. ledna 2005 správním úřadem a ústředním archivem státu přímo řízeným Ministerstvem vnitra. Patří do organizačních složek státu a je účetní jednotkou; jeho rozpočet je součástí rozpočtové kapitoly ministerstva (10).

Národní archiv pečuje o archiválie, které vznikly především v rámci činnosti státních, městských a obecních orgánů veřejné moci. Archiválie v digitální podobě, které jsou uloženy v Národním archivu, jsou zpřístupňovány způsobem umožňující dálkový přístup prostřednictvím portálu pro zpřístupnění archiválií v digitální podobě, jehož správcem je Národní archiv; tento portál je v § 18b odst. 1 ArSSZ nazván legislativní zkratkou „národní portál. „*Národní portál je informační systém veřejné správy a jeho správcem je Národní archiv. Prostřednictvím národního portálu je způsobem umožňujícím dálkový přístup zajišťován:*

a) výběr a příjem archiválií v digitální podobě a jejich metadat,
b) vedení a zpřístupňování evidence Národního archivního dědictví,
c) příjem metadat popisů původců,
d) příjem metadat popisů archivů a kulturně vědeckých institucí,
e) příjem a prezentace archivních pomůcek v digitální podobě,
f) přístup k archiváliím v digitální podobě a dokumentům v digitální podobě vzniklým jako digitální reprodukce z archiválií v analogové podobě.“

1.4.1 Národní digitální archiv

Národní digitální archiv je součást Národního archivu, která řeší bezpečné, důvěryhodné a dlouhodobé uložení digitálních dokumentů vybraných veřejnými archivy za archiválie (11). Zahájení projektu Národní digitální archiv bylo provedeno dne 9. února 2011 (12). O tři roky později, roku 2014 se přešlo do zkušebního provozu a v něm doposud Národní digitální archiv přetrvává (7). „*Hlavním cílem bylo vybudovat servisní pracoviště zajišťující:*

- *dlouhodobé uchování digitálních archiválií vybraných veřejnými archivy,*
- *provoz archivního portálu,*

- *zpřístupnění dokumentů,*
- *podpora institucí (původců) a archivů při skartačním řízení,*
- *podpora při zpracování digitálních archiválií,*
- *bezpečné uložení digitálních reprodukcí tradičních archiválií"* (13).

Dva nejpodstatnější body projektu byly vybudování bezpečných prostor, včetně záložních, a vytvoření informačního systému, který dokáže přijímat dokumenty, bezpečně ukládat, zajišťovat kontrolu neměnnosti dokumentů, zajišťovat autenticitu a spravovat archivní portál (13).

Základem Národního digitálního archivu je model OAIS (ISO 14721:2003 - Open Archival Information System).

1.4.2 Model OAIS (Open Archival Information Systém)

Popisuje tři druhy balíčků, které mají specifický úkol v rámci úložiště.

SIP (Submission Information Package) - Balíček podávaných informací

AIP (Archival Information Package) - Balíček archivovaných informací

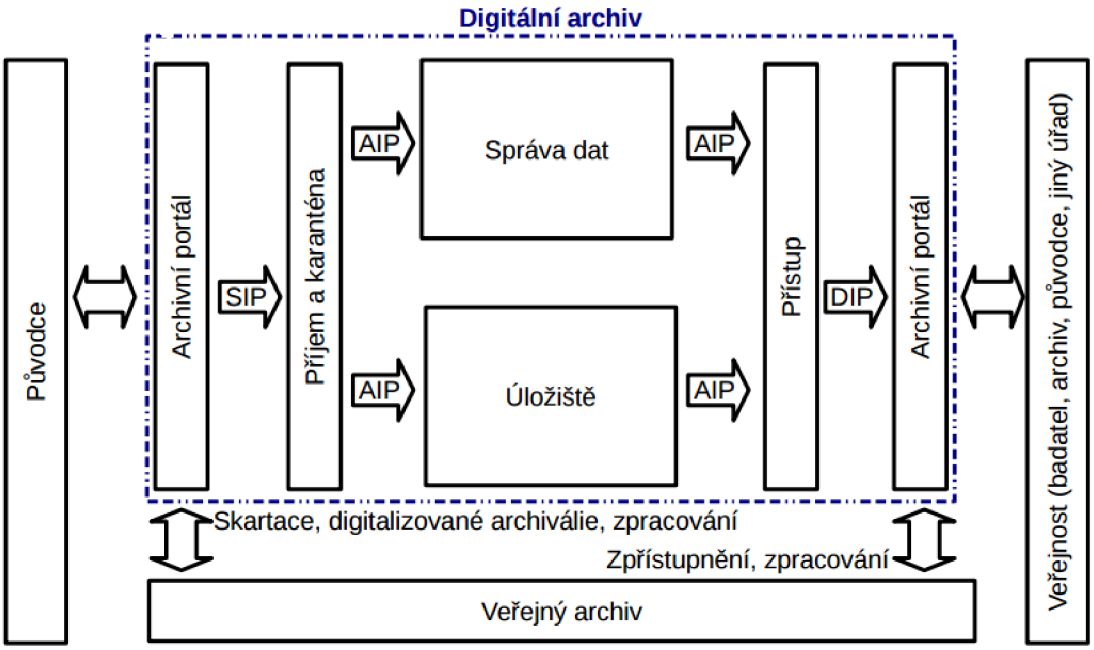
DIP (Dissemination Information Package) - Balíček informací k rozšiřování

Digitální dokument, který bude vybrán za archiválii, bude nejprve převeden do podoby vhodné pro předání do archivu – vznikne balíček SIP. Bude v něm zahrnut nejen samotný dokument, ale i metadata, která se k němu váží. Většinou je automaticky vygenerován informačním systémem spisové služby (2).

Přijatý balíček bude dále zpracováván. Zejména budou doplněna metadata podporující procesy řízení, uchováván a zpřístupňování a bude mu v rámci digitálního archivu přidělen jednoznačný identifikátor – vznikne balíček AIP. Následně bude balíček uložen do archivního úložiště s řízeným přístupem, aplikací uchovávacích metod apod. (2).

Pomocí národního portálu může uživatel zadat svůj požadavek pro zpřístupnění uložených dokumentů. Modul vytvoří balíček DIP, který bude uživateli prostřednictvím webového portálu zobrazen. DIP obsahuje seznam přístupných dokumentů, jejich náhledy, konkrétní dokument, jeho metadata a informace o případném omezení přístupu k dokumentu (2).

Následující obrázek zobrazuje celý proces vytváření balíčků.



Obr. 1Proces vytváření balíčků. (13)

1.5 Nástroje pro autentizaci digitálních dokumentů

Jak je uvedeno výše, elektronickými podpisy, značkami a časovými razítky můžeme k dokumentu připojit atributy, umožňující za určitých okolností i se značným časovým odstupem ověřit pravost dokumentu.

1.5.1 Elektronický podpis

„Elektronický podpis se dá využít všude tam, kde je dnes nutný vlastnoruční podpis“ (2, s. 270). Lze podepsat i to, co lze ručně opatřit podpisem velmi těžko – obsah datového souboru, fotografie, audiovizuální záznamy atd. (2). *„Podpis slouží k doložení skutečnosti, že určitá osoba projevila svoji vůli, případně že se v určitou dobu nacházela na určitém místě, popřípadě, že stvrzuje platnost určitého dokumentu“* (2, s. 271).

Stejně jako pro digitální dokument potřebuje prostředky, kterými jsme schopni jej přečíst, tak je tomu tak i u elektronického podpisu. Především, elektronický podpis není to stejné jako digitalizovaný podpis nebo oskenovaný podpis. Digitální podpis je číslo. Můžeme si představit číslo v desítkové tak i ve dvojkové soustavě. Je to jedno, protože

každý z těchto tvarů můžeme vzájemně převést na druhý. Toto číslo bývá velmi dlouhé a jeho výpočet nebo ověření je dosti složitý úkon, který nejsme schopni provádět ručně, ale pouze pomocí počítače (2).

Součástí elektronického podpisu je identifikace osoby, které podpis patří. Při ověřování pravosti podpisu je nutná komunikace s třetí stranou, tedy důvěryhodnou autoritou, která je tvůrcem podpisu. K tomu se využívají digitální certifikáty, které nám ověření zajistí, bez nutnosti vždy třetí stranu kontaktovat (1).

1.5.2 Úrovně elektronického podpisu

Zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (dále jen ElPZ) rozlišuje pro elektronický podpis tři úrovně.

Elektronický podpis

§ 2 písm. a) jsou „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*.“

Zaručený elektronický podpis

§ 2 písm. b) je *„elektronický podpis, který splňuje následující požadavky*

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.“

Uznávaný elektronický podpis

§ 11 odst. 3 písm. a) je „*zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby.*“

písm. b) „*zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie.*“

V rámci orgánu veřejné správy, tedy v oblasti, kterou se tato práce bude zabývat, se podle § 11 ElPZ musí používat uznávaný elektronický podpis nebo uznávaná elektronická značka, protože jak §11 praví, k podepisování nebo označování dokumentu v podobě datové zprávy lze použít pouze uznávaný elektronický podpis nebo uznávanou elektronickou značku, pokud jehož prostřednictvím činíme úkon vůči státu, územnímu samosprávnému celku, právnické osobě (zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem) nebo právnické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti a fyzické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti.

1.5.3 Ověření elektronického podpisu

Ověřování elektronického podpisu probíhá podobně jako u ověřování ručního podpisu. Při rukou psaném podpisu nám slouží podpisový vzor, při elektronickém veřejný klíč (2).

Stejně jako při vytváření ručního podpisu, kdy do něj promítáme naši jedinečnou schopnost, nějaký individuální stereotyp psaní, který známe jen my, tak i při vytváření elektronického podpisu se používá jedinečná soukromá informace. Je to číslo, kterému se říká privátní klíč. Náš dokument, který chceme opatřit elektronickým podpisem je prezentován také číslem (2). „*Určitým matematickým spojením, založeným na vlastnostech asymetrických kryptografických algoritmů, z těchto dvou čísel vzniká nové číslo, které je právě digitální podpis*“ (2, s. 290). Je tedy závislý na každém bitu daného dokumentu, tudíž i nepřevoditelný. Matematické operace musí provádět počítač, jejich výpočet je velmi složitý (2). “*Pokud podepisujeme - byť v jediném bitu - odlišné digitální dokumenty, jejich digitální podpisy budou naprosto odlišné - nikoliv jen v jediném bitu“* (2, s. 290).

„U digitálního podpisu probíhá ověřování podpisu podobně jako u ručních podpisů. Našim podpisovým vzorem pro ověření digitálního podpisu je opět číslo, které můžeme nazvat veřejným ověřovacím číslem (veřejným klíčem). Toto číslo je sice pevně svázáno s číslem podepisovacím, ale může být dáno veřejně k dispozici. Ověření digitálního podpisu pak probíhá opět určitým, přesně definovaným, spojením podpisu nacházejícího se pod podepsaným dokumentem a veřejného klíče. „Spojení" je složitá matematická operace, kterou opět musí provádět počítač. Výsledkem tohoto spojení je informace, zda dokument byl podepsán osobou, která se za podepisujícího vydává, a zda nebyl dokument po jeho podepsání jakkoli změněn" (2, s. 292).

1.5.3.1 Šifrovací algoritmy elektronického podpisu

"Šifrovací algoritmy pro digitální podepisování pracují na bázi asymetrické kryptografie" (2, s. 284). Aplikace těchto algoritmů převádí data na zašifrovaná a naopak pomocí šifrovacího klíče. Vždy jsou potřeba klíče dva. Jeden slouží pro zašifrování a druhý pro odšifrování. Jsou- li tyto klíče totožné, nazýváme tento jev symetrický šifrovací algoritmus, pokud se klíče od sebe navzájem liší, jedná se o asymetrický šifrovací algoritmus. U symetrického šifrování je potřeba k přístupu k zašifrovaným datům znát šifrovací klíč, naopak u asymetrického šifrování, je jeden z klíčů veřejně dostupný, tudíž se můžeme k datům bez problémů dostat, a nelze z něj odvodit klíč druhý. Čili není nutné předávat údaje o klíči a použitém algoritmu protistraně, což by znamenalo použít nějaký způsob zabezpečené komunikace (2).

1.5.3.2 Hash funkce

Jakýkoli digitální dokument je představen posloupností bitů, čísel. Protože práce s takovými čísly by byla časově náročná, je nutná redukce tohoto čísla, na číslo kratší s pevně danou délkou. To zajišťuje matematicko-kryptografická metoda, tzv. hashování (2).

„Pro použití hashovaní funkce je klíčová její odolnost, a to:

a) *vůči získání předlohy. Pro daný hash c je obtížné spočítat x takové, že h(x) = c (hashovaní funkce je jednosměrná),*
b) *vůči podvržení jiné předlohy. Pro daný vstup x je obtížné najít y takové, že h(x) = h(y),*
c) *odolnost proti kolizím. Je obtížné, resp. málo pravděpodobné najít rozdílnou dvojici vstupů (x,y), pro které h(x) = h(y)"* (2, s. 288).

Dříve používaní funkce MD5 a SHA-1 nejsou již považovány za dostatečně bezpečné. Následující je skupina hashovacích funkcí SHA-2 (Secure Hash Algorithm-2), pojmenovány podle délky SHA-224, SHA-256, SHA-384 a SHA-512 (8). Nyní již existuje neoficiální verze SHA-4. Verze SHA-3 samozřejmě nebyla vynechána, ale zjistilo se, že dosahuje stejné kvality bezpečnosti, jako předchozí verze SHA-2 (29). Nicméně byla americkým úřadem pro standardy a technologie (NITS) jmenována standardem (2. října 2012). Původní název funkce byl KECCAK (8).

1.5.4 Kvalifikovaný certifikát

Kvalifikovaný certifikát je digitální dokument, v kterém jsou kromě jiného uvedeny zejména údaje identifikující příslušnou osobu a její veřejný klíč. Tento digitální dokument je pak digitálně podepsán certifikační autoritou – CA (podle zákona i dle směrnic ES poskytovatelem certifikačních služeb, PCS), a to dohromady dává žádaný podepsaný certifikát (1).

Údaje o poskytovateli certifikačních služeb jsou zaznamenány přímo v kvalifikovaném certifikátu jim vydaným. Konkrétně kvalifikovaný certifikát musí dle ElPZ § 12 odst. 1 písm. f) obsahovat elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává, a podle písm. g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb.

„V praxi to znamená, že důvěryhodnost kvalifikovaného certifikátu je založena na důvěryhodnosti kvalifikovaného systémového certifikátu poskytovatele certifikačních služeb“ (1, s. 72).

Další nezbytný údaj je, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití, případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. Přičemž tato omezení musí být dle odst. 2 § 12 ElPZ zjevná třetím stranám, což v praxi znamená jejich standardizovaný popis (1).

Velmi podstatné kvůli důvěryhodnosti certifikátu je také vyznačení začátku a konce platnosti kvalifikovaného certifikátu. Kvalifikované certifikáty jsou obvykle vydávány s dobou platnosti jeden rok, kvalifikované systémové certifikáty s dobrou platnosti maximálně několik let (1).

„Na základě principu přenosu důvěry je možné důvěřovat neznámým certifikátům, které jsou podepsané důvěryhodnou certifikační autoritou. Jinými slovy důvěra ve vydavatele je přenesena na jím vydaný certifikát“ (2, s. 293).

1.5.5 Poskytovatel certifikačních služeb

V České republice existují tři akreditovaní poskytovatelé certifikačních služeb, kteří splňují podmínky stanovené v § 10 odst. 4 ElPZ, dále pak ve vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikované systémové certifikáty byly ověřeny Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (3).

Zmiňovanými poskytovateli jsou:

1. První certifikační autorita, a.s.,
   Identifikační číslo 26 43 93 95,
   Podvinný mlýn 2178/6,
   PSČ 190 00 Praha 9
   Akreditace udělena 15. 3. 2002,

2. Česká pošta, s. p.
   Identifikační číslo 47 11 49 83,
   Olšanská 38/9,
   PSČ 225 99 Praha 3
   Akreditace udělena 15. 7. 2005,

3. identity a. s.,
   Identifikační číslo: 27 11 24 89,
   Vinohradská 184/2396,
   PSČ 130 00 Praha 3
   Akreditace udělena: 13. 9. 2005 (3).

1.5.6 Uznávaná elektronická značka

ElPZ, byl změněn zákonem č. 440/2004 Sb., kde podle § 2 písm. c) se elektronickou značkou rozumí *„údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky*
1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.“

Elektronická značka nemá tři úrovně jak je tomu pro elektronický podpis, ale zahrnuje v sobě podmínky jako je to u úrovně uznávaného elektronického podpisu, a to je, že elektronická značka musí být založena na kvalifikovaném systémovém certifikátu (1).

Základní rozdíl mezi uznávaným elektronickým podpisem a uznávanou elektronickou značkou je specifikován ElPZ § 3 a 3a. Jestliže byl použit elektronický podpis, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila. Pokud je použita elektronická značka, má se za to, že osoba tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli. Technologický princip však je elektronický podpis a elektronická značka založen stejné bázi (1).

1.5.7 Kvalifikované časové razítko

Znovu zdůrazním odstavec 5 z ArSSZ § 69a který uvádí, že *„neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“*

ElPZ §2 písm. r) definuje, že „*kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.*“

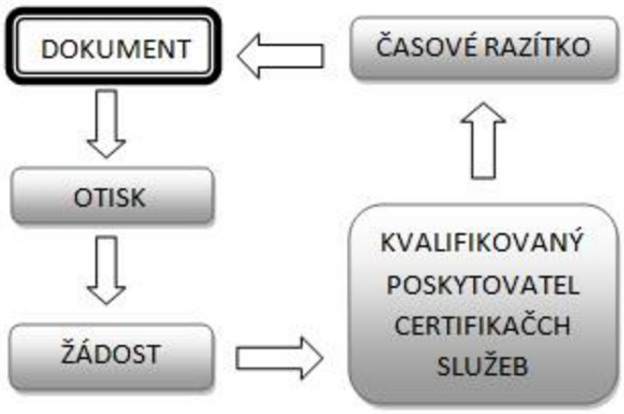
Vydavatelem kvalifikovaných časových razítek je opět kvalifikovaný poskytovatel certifikovaných služeb, který je povinen zajišťovat, aby razítko obsahovalo všechny potřebné náležitosti a splňoval tak § 6b ElPZ. Nutnou náležitostí podle zmiňovaného paragrafu je časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka, dále musí poskytovatel zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku. Poskytovatel také musí přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek a musí poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

Kvalifikovaný poskytovatel certifikačních služeb musí dle ElPZ vydat neprodleně kvalifikované časové razítko po přijetí žádosti o jeho vydání.
Další potřebné náležitosti časového razítka jsou uvedeny v již citovaném ElPZ § 12b. Jde především o unikátní číslo kvalifikovaného časového razítka, pravidla, podle kterých kvalifikovaný poskytovatel certifikačních služeb razítko vydal, v případě právnické osoby stát nebo firmu ve kterém je kvalifikovaný poskytovatel usazen, v případě fyzické osoby pak jméno, příjmení, stát kde je usazen. Hodnotu času, která odpovídá koordinovanému světovému času při vytváření razítka a data pro která bylo razítko vydáno. Na závěr elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

Důvod, proč časové razítko potvrzuje existenci dokumentu před daným časovým okamžikem, nikoli v daný časový okamžik, vyplývá ze samotného procesu vydávání časových razítek. Jednoduše řečeno to funguje tak, že se kvalifikovanému poskytovateli certifikačních služeb zašle otisk existujícího dokumentu, který je nutné orazítkovat a pokud žádost vyhovuje podmínkám, poskytovatel doplní otisk dokumentu o časový údaj

a další potřebné náležitosti a pošle tyto data zpět. Tyto údaje se pak připojí ke zdrojovému, prvotnímu dokumentu a vše se opatří podpisem kvalifikovaného poskytovatele certifikačních služeb a to potvrzuje, že celý dokument nebyl od časového okamžiku uvedeného v razítku změněn (1).

Postup je znázorněn pomocí následujícího schématu:



Obr. 2Proces opatření digitálního dokumentu časovým razítkem. (1)

1.5.8 Nařízení eIDAS

Dne 23. července 2014 bylo vydáno Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále také jen „Nařízení"), které je – s určitými výjimkami – účinné od 1. července 2016. Protože jde o přímo působící předpis, bude jeho důsledkem s největší pravděpodobností zrušení, nebo značná redukce zákona o elektronickém podpisu, jakož i další změny v české legislativě.

Jak uvádí publikovaný detailní rozbor tohoto Nařízení „*zásadní novou kvalitu Nařízení prakticky nepřináší, byť v detailech je lze považovat za lepší variantu oproti směrnici 1999/93/ES. Určitě pak ne v České republice, která některé velice pokročilé nástroje eGovernmentu, jako jsou např. elektronická značka, časové razítko a především systém důvěryhodného doručování pomocí datových schránek zakotvila ve své legislativě a prakticky jej realizovala již před několika lety*" (30, s. 189 - 235).

Nařízení eIDAS nemění zásadním způsobem výše popsané nástroje, pouze musíme počítat s tím, že jde o přímo působící právní předpis EU, který nahrazuje zákon o elektronickém podpisu. V ČR je nyní projednáván v Parlamentu návrh zákona o službách vytvářejících důvěru, který mj. ruší zákon o elektronickém podpisu tak, aby nedocházelo k duplicitní právní úpravě[3].

1.6 Konverze dokumentů

Konverze, tedy převod dokumentu může být dvojí. První je z listinné podoby do digitální, čili digitalizace, nebo z elektronické podoby do listinné (1).
Vzhledem k tématu této bakalářské práce se budu zabývat pouze digitalizací, čili přípravou analogových dokumentů k digitální archivaci.

Nejčastějším nástrojem digitalizace je skenování. Jak již bylo zmíněno v kapitole 1.2.1 o základním rozdělení digitálních dokumentů, nejpoužívanější metodou je OCR metoda (Optical Character Recognition), která nám umožňuje skenovaný text převést do podoby, s kterou je dále možné pracovat a upravovat ji. Doposud není vždy rozpoznání písmen stoprocentní, čili se doporučuje vždy provést korekturu skenovaného textu. Pokud je potřeba zachovat obrazovou podobu některé části dokumentu (razítka, podpisy, loga, aj.), je možnost použít kombinaci OCR s obrazovým skenováním. Výstupním formátem těchto dokumentů by měl být formát PDF verze 1.7 a vyšší (je tak stanoveno ve vyhlášce č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů), který nám umožňuje v jednom souboru uchovat jak naskenovanou obrazovou část dokumentu, tak i rozpoznaný text. Některé dokumenty však potřebujeme výhradně v obrazové podobě (např. formulář s ručně vyplněnými údaji, fotografie, doklady, aj.) (1).

V §5 vyhlášky č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů, platné od roku 2009 jsou zmíněny technické náležitosti snímacího zařízení následující:
„a) rozlišení snímání nejméně 300 x 300 dpi,

[3] Dostupné na: <http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx>

b) barevná hloubka nejméně 24 bitů nebo 256 stupňů šedi, jde-li výlučně o černobílé převádění,

c) velikost formátu snímací plochy nejméně A4.“

Zákonů, kde se zmiňuje konverze dokumentů je několik, každý v jiné oblasti. Například se o ni hovoří v prováděcí vyhlášce č. 383/2009 Sb. zákona č. 563/1991 Sb., o účetnictví nebo zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, nebo se s ní setkáme v oblasti notářské a advokátské.

1.7 Datová schránka

Významným nástrojem pro elektronickou komunikaci a tedy i doručování digitálních dokumentů je informační systém datových schránek. Jedna se vlastně o systém důvěryhodného doručování tak, jak se o něm hovoří v Nařízení eIDAS.

Dle § 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen ElÚAKDZ) je datová schránka *„elektronické úložiště, které je určeno k:*

a) *doručování orgány veřejné moci,*
b) *provádění úkonů vůči orgánům veřejné moci,*
c) *dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.*“

Nejedná se o nástroj nahrazující spisovou službu, úložiště dat dokonce ani archiv nebo zálohy informačního systému. Zprávy jsou v datové schránce uloženy nikoliv trvalým způsobem, ale pouze krátkodobě (90 dnů) pro účely zabezpečené komunikace. Dá se tvrdit, že datové schránky jako důvěryhodné krátkodobé úložiště datových zpráv poskytují možnost bezpečného činění úkonů způsobem, který vysoce přesahuje bezpečnost a důvěryhodnost současných doručovacích cest (2).

Zásadní rozdíl oproti nejběžnější komunikaci, tedy e-mailu je v používání šifrovaného spojení mezi uživateli informačního systému datových schránek. Pro bezpečnou komunikaci neexistuje vhodnější univerzálně použitelný nástroj, nežli jsou datové schránky (2).

Informační systém datových schránek je v České republice spuštěn od 1. listopadu 2009 (4).

1.7.1 Komunikace prostřednictvím datové schránky

Povinné použití datových schránek je dle zákona nastaveno tak, že povinně přes ni musí probíhat obousměrná komunikace orgánů veřejné moci mezi sebou a komunikace orgánů veřejné moci vůči právnickým osobám a podnikajícím osobám, kterým se zřizuje datová schránka ze zákona, a právnických nebo fyzickým osobám, kterým byla datová schránka zřízena na základě jejich žádosti. Nepovinně, tedy doporučuje se ji používat pro komunikaci právnických a fyzických osob vůči orgánům veřejné moci a ke vzájemné komunikaci mezi fyzickými a právnickými osobami (2).

Veškerá komunikace má probíhat elektronicky, pokud je to z povahy věci možné. V případě orgánů veřejné moci je za účelem snížení ekonomických nákladů nastaveno povinné použití elektronické formy komunikace. Pokud má fyzická či právnická osoba zřízenou datovou schránku, musí orgán veřejné moci doručovat v elektronické formě právě do datové schránky dané osoby. K jedné konkrétní datové schránce může mít přístup více osob, pokud je k tomu držitel datové schránky pověřil dle § 8 odst. 6 dle ElÚAKDZ, přičemž všechny osoby nemusí mít přístup ke všem datových zprávám, které jsou ve schránce – např. pokud je zpráva určena pouze do vlastních rukou adresáta a adresát nepověřil touto úrovní přístupu další osoby, není ostatním oprávněným osobám přístupná (2).

1.7.2 Datová zpráva

Datovou zprávou je dokument, který je doručován prostřednictvím datové schránky. Tvoří jej obálka a obsah zprávy. Strukturu obálky, zvané XML obálka, můžeme najít v technické příloze č. 1 Provozního řádu Informačních systémů datových schránek podle § 14 ElÚAKDZ. Obsahem zprávy může být nejméně jedna příloha v některém z přípustných počítačových formátů. Povolené formáty příloh jsou uvedeny v Příloze 3 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění vyhlášky č. 422/2010 Sb.:

a) pdf (Portable Document Format)
b) PDF/A (Portable Document Format for the Long-term Archiving)
c) xml (Extensible Markup Language Document)
d) fo/zfo (602XML Filler dokument)
e) html/htm (Hypertext Markup Language Document)

f) odt (Open Document Text)

g) ods (Open Document Spreadsheet)

h) odp (Open Document Presentation)

i) txt (prostý text)

j) rtf (Rich Text Format)

k) doc/docx (MS Word Document)

l) xls/xlsx (MS Excel Spreadsheet)

m) ppt/pptx (MS PowerPoint Presentation)

n) jpg/jpeg/jfif (Joint Photographic Experts Group File Interchange Format)

o) png (Portable Network Graphics)

p) tif/tiff (Tagged Image File Format)

q) gif (Graphics Interchange Format)

r) mpeg1/mpeg2 (Moving Picture Experts Group Phase 1/Phase 2)

s) wav (Waveform Audio Format)

t) mp2/mp3 (MPEG-1 Audio Layer 2/Layer 3)

u) isdoc/isdocx (Information System Document) verze 5.2 a vyšší

v) edi (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů - EDI)

w) dwg (AutoCAD DraWinG File Format) verze 2007 a vyšší

x) shp/dbf/shx/prj/qix/sbn/sbx (ESRI Shapefile)

y) dgn (Bentley MicroStation Format) verze V7 a V8

z) gml/gfs/xsd (Geography Markup Language Document)

Uvedené formáty jsou přípustnými formáty pro datové zprávy, které lze dodat do datové schránky. Musí obsahovat odpovídající příponu, čímž se rozumí vnější znak formátu datové zprávy, který umožňuje programového vybavení počítače určit typ datového souboru.

Formát XML (bod c) je přípustným formátem datové zprávy dodávané do datové schránky, odpovídá-li veřejně dostupnému XSD schématu publikovanému příjemcem datové zprávy.

Protože součástí mnoha dokumentů posílaných prostřednictvím datové schránky je i elektronický podpis a časové razítko vytvořené mimo datovou zprávu, oznámilo Ministerstvo vnitra, že je nezbytné, aby informační systém doručoval elektronické

podpisy a časová razítka v těchto formátech: CER, CRT, DER, PK7, P7B, P7C, P7F, P7M, P7S, TST (1).

1.8 Zákon o archivnictví spisové službě

Jak už bylo nesčetněkrát zmíněno, nejdůležitějším zákonem, o který se opírá tato bakalářská práce je ArSSZ. Byl vydán ve Sbírce zákonů dne 30. června 2004 a účinnosti nabyl 1. ledna následujícího roku. Tento zákon celkové upravuje

a) výběr archiválií,
b) ochranu archiválií,
c) práva a povinnosti vlastníků archiválií,
d) využívání archiválií,
e) práva a povinnosti držitelů a správců archiválií,
f) využívání archiválií,
g) zpracování osobních údajů pro účely archivnictví,
h) soustavu archivů,
i) práva a povinnosti zřizovatelů archivů,
j) spisovou službu,
k) působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisové služby,
l) správní delikty.

Aktuálně má zákon tři přílohy. Příloha č. 1 obsahuje seznam druhů dokumentů vzniklých z činnosti obchodních společností, družstev, s výjimkou bytových družstev, a notářů, které jsou tito za podmínek stanovených tímto zákonem povinni uchovávat a umožnit výběr archiválií. V příloze 2. je seznam druhů dokumentů, které budou podle obsahu vždy předloženy k výběru za archiválie. A příloha 3. obsahuje seznam státních oblastních archivů a jejich vnitřních organizačních jednotek – státních okresních archivů.

1.9 Spisová služba

Podstatnou otázkou je, kdo má povinnost vést spisovou službu. Pro tuto práci konkrétně – kdo má povinnost vést elektronickou spisovou službu. Současný ArSSZ uvádí, že vedou spisovou službu v elektronické podobě tito původci:

- organizační jednotky státu,
- ozbrojené síly,
- bezpečnostní sbory,
- státní příspěvkové organizace,
- zdravotní pojišťovny,
- právnické osoby zřízené zákonem,
- kraje a hlavní město Praha.

Možnost volby mezi elektronickou a listinnou variantou mají tito původci:

- státní podniky,
- školy,
- veřejné výzkumné instituce,
- obce,
- organizační složky územních samosprávných celků, vytvářejí dokumenty uvedené v přílohách č. 1 nebo 2 k ArSSZ, a
- právnické osoby zřízené nebo založené územními samosprávními celky, vytvářejí-li dokumenty uvedené v přílohách č. 1 a 2 k ArSSZ.

Je potřeba dostatečně rozlišit pojmy spisovna a archiv. Může se zdát, že oba zastávají stejnou funkci. V § 2 ArSZZ, písm. c) definuje archiv jako „*zařízení podle tohoto zákona, které slouží k ukládání archiválií a péči o ně*“ a spisovnu dle písm. m) jako„*místo určené k uložení, vyhledávání a předkládání dokumentů pro potřebu původce a k provádění skartačního řízení.*“

Dále podle § 2 písm. l) „*výkonem spisové služby zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování,*

podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností.“

Konečně je pak třeba pracovat s pojmem podle § 2 písm. n) správní archiv, což je „*součást původce určená k dohledu na spisovou službu původce a k uložení, vyhledávání a předkládání dokumentů se skartační lhůtou delší než 5 let.*“

Tyto pojmy spolu nicméně souvisí. Dokumenty jsou dočasně uložené ve spisovně, dokud nedojde na skartační řízení a nejsou posouzeny jako archiválie nebo vyřazeny. Dokumenty mohou být uloženy též ve správním archivu, pokud jej určený původce zřídil. (§ 68 odst. 1 věta druhá ArSZZ). V případě archiválie dokument dále putuje do Národního (digitálního) archivu. V této kapitole budou popsány podstatné aspekty spisové služby od přijetí dokumentu až k uložení do archivu.

1.9.1 Příjem dokumentů

Základním místem pro přijetí dokumentů je podatelna. Obecně zajišťuje příjem všech typů a forem dokumentů, v praxi však mohou být určená různá specializovaná podací místa, které mohou zajišťovat příjem specifických forem dokumentů. Kromě toho původce může mít i více než jednu podatelnu. Přestože je pro příjem dokumentů předurčena podatelna, nemůže veřejnoprávní původce odmítnout přijmout dokument i mimo podatelnu. Ovšem osoba, která dokument přijme mimo podatelnu je povinna jej na podatelnu doručit nebo může sama následně provést všechny kroky spojené s přijetím podání, což zjednodušuje elektronický systém spisových služeb, prostřednictvím kterého se může zpřístupnit funkce podatelny určeným uživatelům (14).

Podle § 64 odst. 1 ArSZZ „*v případě dokumentů v digitální podobě určení původci zajistí jejich příjem alespoň v datových formátech stanovených jako výstupní datové formáty nebo formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě. Pokud veřejnoprávní původci umožní příjem dokumentů v digitální podobě také v dalších datových formátech nebo pokud umožní příjem dokumentů v digitální podobě na přenosných technických nosičích dat, zveřejní jejich přehled na úřední desce nebo, nezřizují-li úřední desku, na svých internetových stránkách.*“

1.9.2 Příjem dokumentů v elektronické podobě

Nejčastějšími elektronickými komunikačními kanály, jimiž je činěno podání, jsou datové schránky nebo e-mailová komunikace. Obdobou zásilky je v tomto případě datová zpráva. Nejprve je nutná kontrola, zda je zpráva doručena správnému adresátovi. Pokud ne, adresát odmítne přijetí a uvědomí odesílatele (14).

Dále proběhne antivirová kontrola, tedy zda zpráva neobsahuje škodlivý kód. Pokud ano, adresát uvědomí odesílatele a stanoví další postup pro její odstranění. Je možné, že pokud zpráva obsahuje škodlivý kód, může být „zastavena" dříve, než je skutečně dostupná podatelně, např. specializovaným elektronickým zařízením chránícím připojení původce do internetu. Veřejnoprávní původce musí vystavit na své úřední desce způsob nakládání s datovými zprávami, u kterých byl zjištěn výskyt škodlivého kódu (14).

Další co je nutné zkontrolovat, je formát dokumentu. Formáty, které smí původce přijmout, jsou zmíněny v předcházejících kapitolách. Je nutné upozornit, že samotná přípona dokumentu formát nedefinuje. Mezi kontrolu formátu se také řadí kontrola velikosti dokumentu. Pokud jsou formát a velikost jiná, než připouští vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky č. 283/2014 Sb. (dále jen SSV), opět jde o vadu podání. Dalším krokem kontroly je zjištění, zda jednotlivé komponenty dokumenty lze zobrazit uživatelsky vnímatelným způsobem, tj. zda je počítačový program schopen dokument zobrazit čitelným způsobem (14).

Na rozdíl od příjmu a podání analogového, tedy listinného dokumentu, kde podpis či jinou identifikaci podatele řeší až osoba vyřizující danou věc, u příjmu digitálního dokumentu jsou hned v rámci příjmu (tedy podatelnou) prováděny kontroly případného připojeného elektronického podpisu, elektronické značky anebo časového razítka. Důvody jsou zde minimálně dva.

Prvním důvodem je omezená časová platnost kvalifikovaných a systémových kvalifikovaných certifikátů, na nichž jsou tyto autentizační prvky ve své uznávané a kvalifikované podobě založeny. Díky ní je třeba ověření provést co nejdříve po doručení datové zprávy. Ustanovení § 3 odst. 1 vyhlášky č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky,

kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (dále jen OvěřElPV) k tomu říká: „*Okamžikem, ke kterému je ověřována platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, je okamžik doručení datové zprávy*.“ Samozřejmě, že postup ověřování uznávaného elektronického podpisu a uznávané elektronické značky ještě závisí na tom, zda je k datové zprávě připojené také časové razítko, protože není-li kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát v okamžiku přijetí datové zprávy platný, a je-li k datové zprávě podepsané elektronickým podpisem nebo označené elektronickou značkou připojeno platné kvalifikované časové razítko, ověřuje se platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu k časovému údaji uvedenému v kvalifikovaném časovém razítku.

Druhým důvodem je nutnost provést ověření identity odesílatele (osoby činící podání).

Po ověření uznávaného elektronického podpisu, uznávané elektronické značky popřípadě kvalifikovaného časového razítka a ověření platnosti certifikátů, na nichž jsou tyto autentizační prvky založeny, se výsledky zaznamenají do příslušné evidence. Údaje, které mají být zaznamenány, jmenuje SSV v odst. 7§ 4.

1.9.3 Evidence dokumentů

Evidence dokumentů slouží k celkovému sledování životního cyklu dokumentu v rámci původce. V evidenci jsou sledovány dokumenty jak vzniklé z činnosti původce, tak dokumenty původci doručené. Pokud původce vede spisovou službu v listinné podobě, je základním evidenční pomůckou spisový deník, avšak pokud původce vede spisovou službu v elektronické podobě v elektronickém systému spisové služby (dále jen ERMS -*Electronic Record Management System*), je touto základní evidenční pomůckou přímo sám elektronický systém spisové služby (14).

1.9.4 Evidence dokumentů podle národního standardu pro elektronické systémy spisové služby

Pokud původce vede spisovou službu v elektronické podobě, je ERMS základní evidenční pomůckou. Evidence se vede přírůstkovým způsobem, kde základem je pořadové číslo. Platí, že ERMS nesmí nikdy jedno pořadové číslo v rámci určeného období přidělit dvakrát (14).

Podle požadavků č. 6.7.28 podle národního standardu pro elektronické systémy spisové služby (dále jen NS ESSS), který vydalo Ministerstvo vnitra na základě zmocnění v § 70 odst. 2 ArSSZ,[4] se údaje vedené v evidenci dokumentů po uplynutí lhůty jednoho roku od ukončení určeného časového období ztvární jako samostatný dokument, který se opatří zaručeným elektronickým podpisem nebo elektronickou značkou a následně kvalifikovaným časovým razítkem. Evidence v elektronické podobě musí obsahovat minimálně tytéž údaje jako listinné.

1. *„Příjem, kterým se dokument dostává do správy původce.*
2. *Kontrola a třídění, což jsou dvě prolínající s operace, které zároveň určují, zda daný dokument podléhá evidenci, popř. jaké, tj. zda podléhá evidenci ve spisové službě, nebo je evidován v samotné evidenci dokumentů.*
3. *Označení a zaevidování dokumentů, což jsou kroky, kterými se dokument dostává do evidence a zároveň je tato skutečnost na dokumentu vyznačena.*
4. *Dále následuje rozdělování dokumentů, sledování jejich oběhu a vyřizování a další kroky až po vyřazení dokumentu ve skartačním řízení nebo mimo ně.“*

K tomu ještě další údaje definované SSV § 10 odst. 2 jako jednoznačný identifikátor dokumentu, informace o tom, zda je dokument v digitální nebo v analogové podobě, zda byl dokument zařazen do výběru archiválií a zda byl dokument vybrán jako archiválie a identifikátor, který dokumentu vybranému jako archiválie přidělil Národní archiv nebo digitální archiv.

A v poslední řadě dle NS ESSS, plně určený spisový znak[5] dokumentu a údaje (případně poznámky) o dokumentech (stanovené kap. 6.7 NS ESSS). Součástí evidence dokumentů je také evidence spisů[6], a to včetně typových spisů[7]. Konkrétně evidované údaje udává č. 6. 7. 11 a č. 6. 7. 18 NS ESSS.

---

[4] NS ESSS byl zveřejněn ve Věstníku Ministerstva vnitra částka 64/2012 a také způsobem umožňujícím dálkový přístup.

[5] Dle NS ESSS je spisový znak označení, které zařazuje dokumenty do věcných skupin pro účely jejich budoucího vyhledávání, ukládání a vyřazování.

[6]Spojení dokumentů týkajících se stejné věci (14, s. 81)

1.9.5 Vyřizování a podepisování dokumentů

Podle ust. § 65 odst. 1 ArSZZ *„při vyřizování dokumentů se všechny dokumenty týkající se téže věci spojí ve spis. Dokumenty v analogové podobě se vzájemně spojí fyzicky, dokumenty v digitální podobě se vzájemně spojí prostřednictvím metadat, vzájemné spojení dokumentu v analogové podobě a dokumentu v digitální podobě se činí pomocí odkazů.“*

Podle odst. 2 *„vyřízením spisu se rozumí zpracování návrhu, jeho schválení, vyhotovení, podepsání a vypravení rozhodnutí nebo jiné formy vyřízení.“*

Z pohledu této práce je podstatný pak odst. 5, podle kterého *„po vyřízení věci se spis uzavře. Uzavřením spisu se rozumí kompletace všech dokumentů patřících do spisu, kontrola a doplnění údajů podle § 66 odst. 3 před uložením do spisovny a převedení dokumentů v digitální podobě do výstupního datového formátu a jejich opatření metadaty podle národního standardu.“*

1.9.6 Ukládání dokumentů

Podle § 68 odst. 1 zákona *„všechny vyřízené spisy a jiné dokumenty určeného původce jsou po dobu trvání skartační lhůty uloženy ve spisovně. Dokumenty mohou být uloženy též ve správním archivu, pokud jej určený původce zřídil. Dokumenty se ukládají podle spisového a skartačního plánu, a to zpravidla ihned po jejich vyřízení, pokud povaha věci nevyžaduje, aby zpracovatel měl vyřízený dokument déle.“*

1.9.7 Spisový a skartační plán

Spisový plán odráží agendu původce – seskupuje příbuzné dokumenty a takto vzniklé skupiny označuje spisovým znakem (ukládacím znakem). Spisový plán, doplněný o skartační režimy (skartační znak, skartační lhůta, popř. spouštěcí událost) se nazývá spisový a skartační plán. Povinnost vydat skartační plán zakotvuje ArSSZ (14).

---

[7] NS ESSS definuje typový spis jako soubor dokumentů s předem stanovenou strukturou, členěný na věcné, podle obsahu stanovené části (součásti), kterou jsou dále členěny na díly, do kterých se zatřiďují dokumenty nebo vkládají křížové odkazy na spisy.

1.9.8 Skartační režim

„Skartační režim je tvořen[8]

1. *typem skartační operace,*
2. *skartační lhůtou a*
3. *spouštěcí událostí "*

„Skartační znak vyjadřuje předpokládanou hodnotu dokumentu pro účely posouzení ve skartačním řízení:

- *Skartační znak „A" („archiv") znamená, že dokument bude ve skartačním řízení navržen k vybrání za archiválii, protože původce předpokládá, že má trvalou hodnotu,"*
- *„Skartační znak „S" („sběr") určuje, že původce považuje dokument po uplynutí skartační lhůty za bezcenný, a proto jej ve skartačním řízení, navrhuje ke zničení, protože nemá trvalou hodnotu z hlediska věcného, správního, hospodářského ani kulturního.„*
- *„Skartační znak „V" („výběr") znamená, že je dokument určený k dodatečnému posouzení ve skartačním řízení, protože jeho hodnota nelze předem ve spisovém a skartačním plánu předpovídat.„*

„V případě, že spis nebo typový spis obsahuje dokumenty různých skartačních znaků, je stanovena preference od závažnějšího k méně závažnému skartačnímu znaku „A" – „V" – „S".„[9].

1.9.9 Skartační lhůta

SSV definuje pojmy skartační lhůta a spouštěcí událost v § 15.

Skartační lhůta doba, po kterou ze správních, právních a zákonných důvodů musí zůstat dokument uložen ve spisovně a nelze ho navrhnout k výběru archiválií (k vyřazení). Vyjadřuje se počtem let (celým kladným číslem) uvedeným za skartačním znakem a počítá se od 1. ledna kalendářního roku následujícího po roce, ve kterém nastala

[8] požadavky dle NS ESSS

[9] § 15 odst. 3 SSV

spouštěcí událost. V některých případech je dána právními předpisy, ale ve většině případů si ji původce určuje sám.

Spouštěcí událost je doba, od které začíná běžet skartační lhůta. Obecně je definována jako vyřízení dokumentu nebo uzavření spisu. Jiné externí spouštěcí události musí být uvedeny ve spisovém a skartačním plánu.

1.9.10 Metadata spisů

Spis představuje množinu dokumentů, které se týkají vyřizování jedné věci. Tato množina je v analogové podobě ohraničena obalem spisu někdy nazývaným referátník, který obsahuje základní identifikaci spisu (označení, věc), případně údaje o oběhu a pokyny pro vyřizování. Povinně na něm musí být uveden stručný obsah spisu, spisový znak, skartační režim a údaje o uložení spisu včetně rozsahu (počtu stran atd.). V digitální podobě je obal spisu nahrazen metadaty a zatříděním dokumentů do spisu. Povinně musí být, kromě údajů zmíněných již pro analogový spis, uvedeny také jednoznačný identifikátor spisu, informace o přítomnosti dokumentů v analogové podobě a jejich fyzické umístění, informace o zařazení do výběru archiválií nebo o jeho provedení a identifikátor digitálního archivu (pokud byl vybrán za archiválii) (14).

1.10 Datové formáty PDF a PDF/A

Pro statické textové soubory a statické kombinované textové a obrazové dokumenty SSV přikazuje výstupní datový formát Portable Document Format/Archive (PDF/A), který patří mezi celkově nejrozšířenější formáty digitálních dokumentů vůbec. Mimo jiné také proto, že uvedené typy dokumentů jsou u většiny veřejnoprávních původců převládající. Nicméně se lze setkat i s obecnějšími variantami formátu PDF, který nemusí splňovat požadavky kladené normou PDF/A. Jde zejména o výstupy z autorizované konverze dokumentů. Datový formát PDF vytvořila společnost Adobe Systems v polovině 90. let 20. století (14).

Formát PDF existuje v různých verzích, přičemž platí, že PDF/A je technicky specifikovaná podmnožina formátu PDF libovolné verze. Norma PDF/A byla vytvořena právě pro účely dlouhodobé archivace elektronických dokumentů. Jinými slovy jde o veřejnou normu, která specifikuje takové datové objekty v rámci formátu PDF a taková

pravidla jejich popisu, které odpovídají potřebám dlouhodobého archivování a zachování nezávislosti na hardwaru, na operačním systémů a na konkrétní aplikaci. Dle platné legislativy, je tento formát využíván již na úrovni střednědobého uložení digitálních dokumentů (14). Nejnovější verze PDF/A vznikla v roce 2012 s názvem PDF/A-3, založena na specifikací PDF 1.7. Tato verze umožňuje vkládání libovolných formátů (např. XML, CSV, CAD, word dokumentů, tabulkových dokumentů a dalších) do formátu PDF/A a jejich archivování jako kompletního objektu (15).

PDF/A nemá v normě povolen audio a video obsah ani JavaScript nebo jiné spustitelné soubory. Fonty, které jsou v něm užity, musí být legálně vložené pro neomezené a univerzální zobrazení. V dokumentech je zakázáno šifrování a odkazy na externí objekty, ale je vyžadováno použití standardizovaných metadat. Přestože tomu tak v první verzi PDF/A nebylo, v těch následujících je povolená komprese JPEG 2000, transparentní objekty a vrstvy. Prostředky pro digitální podpisy v souladu s normou PAdES jsou podporovány taktéž až od druhé verze formátu PDF/A. Totéž platí i pro možnost připojit další PDF/A soubory a uložit je jako jeden. Třetí verze formátu dokonce podporuje připojit soubory s využitím jiných formátů, např. XML nebo CSV (15).

2 ANALÝZA SOUČASNÉHO STAVU

V této části bakalářské práce se budu zabývat současným stavem digitální archivace. Převážně z právního hlediska tedy popíši všechny zákony, vyhlášky a normy, které jsou pro tuto problematiku podstatné, a v současné době se právě jimi musíme řídit. Pro účely této práce je nutné si popsat, jak funguje spisová služba a všechny procesy, které jsou s ní spojené, protože se věnuji archivaci v rámci orgánu veřejné správy, kde střednědobá a následně dlouhodobá archivace digitálních dokumentů probíhá pomocí elektronického systému spisové služby, a také jak probíhá příprava na samotný výběr a předání digitálních dokumentů do archivu.

2.1 Spisová služba

Spisová služba je v současné době regulována mnoha různými právními předpisy. Nejdůležitějším zákonem pro tuto oblast, jak už název napovídá, je opět ArSSZ. Do výčtu zákonů, které v současné době nějakým způsobem ovlivňují výkon spisové služby, je třeba zahrnout ElPZ, zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Tento seznam stále není úplný. Existuje i řada zákonů, které upravují skartační lhůtu.

K výše uvedeným zákonům patří ve většině případů ještě prováděcí právní předpisy vydané na základě zákonných zmocnění zejména Ministerstvem vnitra. K ArSSZ jsou aktuálně platné dvě vyhlášky. SSV, ve znění vyhlášky 283/2014 a vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění vyhlášek č. 192/2009 Sb., a č. 213/2012 Sb. Z hlediska spisové služby je nejdůležitější ta prvně jmenovaná.

Kromě zákonů a vyhlášek je nutné k výčtu norem regulující spisovou službu přičíst také Národní standard pro elektronické systémy spisové služby (dále jen NS ESSS), který vydalo Ministerstvo vnitra na základě zmocnění v § 70 odst. 2 ArSSZ. NS ESSS byl zveřejněn ve Věstníku Ministerstva vnitra částka 64/2012 a také způsobem umožňujícím dálkový přístup.

2.1.1 Specifika zavádění ERMS

Systém ERMS by měl plně podporovat evidenci, ukládání a vyřazování jak elektronických, tak i tradičních listinných dokumentů. Klíčové jsou především evidence a správa doručených, vlastních a odesílaných dokumentů, jejich oběh (práva přístupu k nim), zatřídění do spisového plánu a podpora jeho doplňování, převod dokumentů (jejich komponent) do výstupního datového formátu, kvalitní metadata umožňující vyhledávání a třídění a možnost jejich exportu. Je také nezbytně nutné nastavit používání autentizacích prvků. Zvláště kvalitní spisový plán je nutnou podmínkou pro správu dokumentů v digitální podobě, full textové vyhledávání nepostačuje, protože velké množství dokumentů neobsahuje textovou (strojově čitelnou) vrstvu a jedná se např. o výstup ze skeneru v podobě rasterové grafiky. Podrobné požadavky na ERMS obsahuje NS ESSS (14).

2.2 Normy PAdES, CAdES, XAdES

Normy PAdES, CAdES, XAdES udávají postupy, které zajistí, že dokument bude nezpochybnitelný po neomezeně dlouhou dobu ve všech státech EU. Jedná se přímo o názvy referenčních formátů. Tyto formáty vznikly v Evropském institutu pro telekomunikační standardy (ETSI – European Telecommunications Standard Institute), což je autoritativní zdroj norem a standardů v oblasti informačních a komunikačních technologií. V dokumentu č. 102 778 je detailně uvedeno, jakým způsobem má být připojen elektronický podpis a časové razítko.

*„**PAdES** (PDF Advanced Electronic Signatures) – připojování podpisu k PDF dokumentům,*

***XAdES** (XML Advanced Electronic Signatures) – připojování podpisu k XML datům,*

***CAdES** (CMS Advanced Electronic Signatures) – podpis podle této normy je použitelný pro jakýkoliv elektronický dokument“* (5).

„V rámci každé výše uvedené skupiny je definována celá řada formátů – například XAdES Basic, XAdES-T (s připojením časového razítka), XAdES-X (extended) apod. Pro účely dlouhodobé archivace důležitých originálů jsou podstatné verze PAdES LTV (Long Term Validation), CAdES-A (Archival) a XAdES-A“(5).

Jejich požadavky vychází z následujících principů:

„VŠECHNO DŮLEŽITÉ UVNITŘ DOKUMENTU – k dokumentu jsou připojeny veškeré informace, které mohou být v budoucnu potřebné pro posouzení jeho pravosti, tedy pro posouzení, zda připojené elektronické podpisy byly v době prvního ověření platné.
NEZÁVISLOST NA ÚLOŽIŠTI – dokument může být vyňat z informačního systému, aniž by tím byla narušena jeho nezpochybnitelnost. Protože všechno důležité je uvnitř, nepotřebuje se odvolávat na žádná potvrzení vydaná informačním systémem.
ODOLNOST VŮČI VNĚJŠÍM UDÁLOSTEM – v současné době nikdo nedokáže předvídat další technologický vývoj, ať už ve smyslu nástupu nových přístrojů nebo prolomení šifer či třeba kompromitace certifikačních autorit. Princip, že všechno důležité je uvnitř, chrání také před jakoukoliv vnější událostí.
NEZPOCHYBNITELNOST PO NEOMEZENOU DOBU – u řady dokumentů dnes není možné říci, jak dlouho mají být uchovávány. Kupříkladu u dokumentů souvisejících s důchodovým zabezpečením vyžadují předpisy 30 let. Ale co když bude někdy v budoucnu tato lhůta prodloužena? Práce s elektronickým podpisem podle norem ETSI umožňuje dobu archivace neomezeně prodlužovat, a to tak, aby pravost zůstala „nade všechno pochybnost“ (5).

„Ze zmíněných norem také vyplývá, jak má proces dlouhodobé archivace dokumentu probíhat:

1. *Kontrola platnosti elektronických podpisů připojených k dokumentu. To zahrnuje záležitosti jako neporušenost kontrolního hashe či platnost certifikátu.*
2. *Připojení metadat: protokolu o ověření, aktuální verze CRL (seznam zneplatněných certifikátů) atd.*
3. *Připojení časového razítka tak, aby kontrolní hash chránil nejen samotný dokument, ale i metadata.*

Periodické připojování dalších časových razítek tak, aby každé další bylo připojeno před vypršením platnosti předchozího (princip digitální kontinuity)“ (5).

Do práva EU byly tyto technické normy začleněny Rozhodnutí Komise EU č. 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přes

hraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu.[10]

2.3 Příprava archivace

V této kapitole jsou popsány postupy, jak dokumenty, spisy nebo typové spisy putují ze samotného ERMS až do archivu. Jak se postupuje při výběru archiválií a podmínky je nutné dodržet.

2.3.1 Vyřízení dokumentu a spisu

Platné právní předpisy vycházejí z předpokladu, že každý spis musí být vyřízen. Také je dle SSV § 14 vyžadováno, aby byl vyznačen způsob vyřízení a případného adresáta vyřízení v evidenční pomůcce. Pokud je dokument vložen do spisu, je vyřízen v jeho rámci. Vyřízením spisu jsou pak vyřízeny všechny do něj vložené dokumenty i samotný spis. ArSSZ § 65 odst. 2 uvádí, že „*vyřízením spisu se rozumí zpracování návrhu, jeho schválení, vyhotovení, podepsání a vypravení rozhodnutí nebo jiné formy vyřízení*.“

2.3.2 Výstupní formáty dokumentů v digitální podobě

Dokumenty dle SSV § 23 musí být před odesláním převedeny do výstupního datového formátu, kterým se rozumí datový formát výstupu z ERMS, datový formát dokumentu ukládaného ve spisovně, která je součástí ERMS a datový formát pro předávání do digitálního archivu.

Datové formáty dané tímto zákonem pro různé druhy dokumentů jsou uvedeny v tabulce.

[10] Úřední věstník Evropské unie, OJ L 53, 26. 2. 2011, p. 66–72

Statické textové dokumenty	Statické kombinované textové a obrazové dokumenty	Statické obrazové dokumenty	Dynamické obrazové dokumenty	Zvukové dokumenty	Databáze
PDF/A (ISO 19005)		PNG (ISO/IEC 15948)	MPEG-2 (ISO/IEC 13818)	MP2	XML
		TIF/TIFF (rev. 6 – nekomprimovaný)	MPEG-1 (ISO/IEC 11172)	MP3	
		JPEG/JFIF (ISO/IEC 10918)	GIF	WAV (mod. PCM).	

Tab. 2 Výstupní datové formáty dokumentů z ERMS. (SSV §23)

Posledním podstatným výstupním datovým formátem je formát metadat, jimiž jsou opatřovány dokumenty v ERMS. Ty dle tohoto zákona musí mít formát Extensible Markup Language Document (XML) podle schématu XML pro výměnu dokumentů a jejich metadat mezi elektronickým systémem spisové služby stanoveného národním standardem nebo datový formát XML podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem, který obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem (viz kapitola 1.4.2 Model OAIS (Open Archival Information Systém)).

2.3.3 Příprava spisů a dokumentů k uložení do spisovny

Před podáním musí být zkontrolován každý vyřízený dokument i uzavřený spis. Kontrolu provádí předávající pracovník, jemuž musí být tato povinnost uložena spisovým řádem. U dokumentů v digitální podobě musí být zkontrolování, že se nachází ve výstupním datovém formátu (14).

Vlastní předání musí být prováděno prokazatelným způsobem. Pro práci spisovny je z pravidla v EMRS připraven modul, jehož prostřednictvím se celý proces provádí. Využije funkce předání/převzetí. Prostředky systému vedou dle SSV v seznamech stručný obsah (předmět, věc), označení dle příslušného spisového a skartačního plánu, spisové znaky a skartační režimy dokumentů a spisů (14).

2.3.4 Výběr archiválií

Výběr archiválií obnáší oddělování bezcenných dokumentů od těch, co mají trvalou hodnotu a jsou určeny k trvalému uložení do archivu. Vedle původce se na výběru archiválií podílí i příslušný archiv z důvodu nestrannosti. Aby se z dokumentu stala archiválie, musí být vedle výběru také zařazen do evidence národního archivního dědictví (NAD), kdy se stane předmětem péče archivu nebo vědecké instituce[11] (14).

Při výběru archiválií ve skartačním řízení u digitálních dokumentů nebo spisů vytvoří sám ERMS návrh pro vyřazení. Řízení výběru archiválií na straně původce je v podstatě na pracovníkovi spisovny. Seznam dokumentů evidovaných v ERMS pro skartační řízení je tvořen souborem balíčků SIP podle přílohy 2 a 3 NS ESSS, avšak bez komponent.

Každý spis, díl typového spisu nebo dokument je prezentován jedním SIP balíčkem. – „*Každý archiv má přístup k webové aplikaci „eSkartace“, součástí národního portálu, kde po vložení zmíněných balíčků SIP může archivář pracovat s klasickou podobou seznamu, kde jsou hierarchicky zobrazovány věcné skupiny, spisy, díly typových spisů a dokumenty*“ (14, s. 217, 218). U dokumentů a spisů se udává, zda jsou tvořeny také částmi v analogové podobě. Archivář si může zobrazit i podrobné údaje o dokumentu, např. odesílatele doručeného dokumentu, adresáty vyřízeného dokumentu apod. Jeho úkolem je vybrat a označit věcné skupiny, spisy, díly typových spisů nebo samostatné dokumenty, které vybírá za archiválie nebo určuje ke zničení. Z věcné skupiny se dědí rozhodnutí a všechny spisy, díly a dokumenty v ní, podobně ze spisu na jeho dokumenty. Existuje také možnost vyznačit spisy a dokumenty vyřazované ze skartačního řízení nebo (dočasně) ty, které nemůže vyhodnotit jen na základě údajů z evidence, ale musí je prohlédnout. Konečným výsledkem je seznam, kde jsou dokumenty a spisy vybrané za archiválie, popř. ty vyloučené ze skartačního řízení. Tento seznam existuje, resp. je ke stažení ve dvou podobách: v „lidsky čitelné“ v datovém souboru CSV (pro MS Excel nebo OpenCals) nebo PDF/A a ve „strojově čitelné“ dle přílohy č. 4 NS ESSS, kde jsou uvedeny vedle rozhodnutí archiváře příslušné identifikátory dokumentů a spisů. Tyto výstupy z aplikace „eSkartace“, tedy

[11] Podle § 11 odst. 5 ArSSZ je kulturně vědeckou institucí museum, knihovna, galerie, památník, veřejná výzkumná instituce a vysoká škola.

strojově čitelný kód a PDF/A, se stávají přílohou protokolu o provedeném skartačním řízení (zkráceně skartačního protokolu) (14).

Každý archiv má jinou strukturu skartačního protokolu, ale vždy podle § 10 odst. 2 ArSSZ musí obsahovat soupis dokumentů nebo souboru dokumentů, které byly vybrány za archiválie, soupis dokumentů, které lze zničit a určení archivu, do jehož péče budou dokumenty předány. Další obsah skartačního protokolu tvoří dle § 21 odst. 2 písm. c) SSV také doba a způsob předání archiválií pečujícímu archivu.

Pokud někdo s rozhodnutím archiváře nesouhlasí, může podat námitku proti skartačnímu protokolu (do 15 dnů od doručení). Teprve podáním námitky je zahájeno správní řízení, které v prvním stupni řeší správní úřad, kterým je z pravidla některý ze správních archivů nebo specializovaný archiv, jehož zřizovatelem je ústřední správní úřad; archiv provádějící skartační řízení je tak většinou totožný se správním úřadem. Druhostupňové rozhodování – po odvolání se – je vyhrazeno Ministerstvu vnitra.[12]

V případě, že skartační protokol nabude právní moci, je na původci, aby provedl předání dokumentů vybraných za archiválie po dohodě určenému archivu, popř. likvidaci dokumentů určených ke zničení. Po načtení zmíněného strojově čitelného kódu se vyznačí dokumenty a spisy k trvalému uložení do archivu nebo ke zničení. Rozhodnutí a datum provedení výběru archiválií se zaznamená do metadat příslušných entit, stejně jako důvody rozhodnutí (14).

2.3.5 Výběr archiválií mimo skartační řízení

Výběr mimo skartační řízení se u veřejnoprávních původců uplatní ve specifických případech např. neevidovaných dokumentů (publikace, mapy apod.) nebo v případě zániku původce, když nelze provést skartační řízení. Výběr zde provádí vždy příslušný archiv. Tento proces je administrativně jednodušší (14).

ArSSZ § 12 odst. 1 uvádí, že *„po ukončení výběru archiválií mimo skartační řízení vyhotoví příslušný archiv protokol o provedeném výběru archiválií mimo skartační řízení a určí, do čí péče budou dokumenty vybrané jako archiválie náležet. Byl-li výběr*

---

[12] Dostupné na: <http://www.mvcr.cz/clanek/metodicky-navod-odboru-archivni-spravy-k-vyberu-archivalii-mimo-skartacni-rizeni-podani-namitky-proti-protokolu-a-vyrazovani-dokumentu-s-utajovanymi-skutecnostmi.aspx>

archiválií mimo skartační řízení proveden na žádost vlastníka dokumentu vybraného jako archiválie, lze tento dokument svěřit do péče archivu pouze se souhlasem tohoto vlastníka a na základě jeho přivolení s určením, do čí péče bude dokument náležet.“

2.3.6 Postup při vybírání archiválií archivem

Postup je velmi individuální. Záleží na archiváři. Závazně se však za archiválie vybírají dle § 5 odst. 1 ArSSZ, který uvádí například dokumenty vzniklé do roku 1850, dokumenty z oborů průmyslové a zemědělské výroby, úvěrové soustavy a pojišťovnictví, finančního a důlního podnikání včetně patentů na významné vynálezy vzniklé do roku 1900, fotografické záznamy vzniklé do roku 1900, zvukové záznamy vzniklé do roku 1930, filmové záznamy vzniklé do roku 1930.

ArSSZ stanovuje ve své druhé příloze okruhy dokumentů, které je původce povinen vždy z pravidla předložit k výběru archiválií. Jejich seznam dobře ilustruje, co je zpravidla za archiválie vybíráno.

Archivář, pokud se nechce spoléhat na tyto rozdělení připravené původcem, by měl především znát dobře současnou i dřívější náplň činnosti původce, jeho organizační strukturu, historii, orientačně vazby na jiné subjekty a lehce i resortní legislativu. Z toho by měl usoudit, co je vhodné archivovat.

2.3.7 Předání dokumentů archivu

Při předávání dokumentů v digitální podobě se nejdříve kontroluje, zda je dokument čitelný, neobsahuje škodlivý kód a má všechny požadovaná metadata. Spolu s dokumentem se předávají metadata ve tvaru podle příloh 2 a 3 NS ESSS. Jedná se o SIP balíček, dle § 21 odst. 7 SSV. Národní digitální archiv bude předané SIP kontrolovat oproti seznamu ze skartačního řízení; při chybějících SIP nebude možné přejímku realizovat. Kontroluje se rovněž převod do výstupních datových formátů. Po uložení v digitálním archivu se potvrdí úspěšný přenos. Děje se tak prostřednictvím datového souboru sestaveného dle přílohy 4 NS ESSS. Jde o obdobný seznam jako v případě skartačního řízení v listinné podobě, pouze místo vyznačení výběru archiválií vrací digitální archiv své identifikátory, pod kterými archiválii uložil. Tyto identifikátory je žádoucí vložit do ERMS, protože umožňují v budoucnu digitální

archiválie přímo vyhledat a slouží i k potvrzení, že dokument byl do digitálního archivu předán.

Při přenosu a exportu dokumentů a metadat je nutné dodržení XML schématu dle přílohy 2 a 3 NS ESSS[13]. Systém musí zajistit i zachování vazeb mezi dokumenty a jejich komponentami, integritu dokumentů a správné vazby metadat. Křížové odkazy na spisy a dokumenty, které jsou mimo přenášený soubor nebo exportovaný celek, se pro přenos a export nahradí – přenášejí se celé odkazované spisy a dokumenty i s jejich metadaty (např. díl se všemi metadaty typového spisu a spisy vloženými křížovými odkazy)[14].„*Komponenty se přenášejí a exportují všechny. Pro uskutečnění přenosu a exportu musí být možné připojit zaručený elektronický podpis nebo elektronickou značku k exportované nebo přenášené entitě z důvodu ověření její integrity. Totéž platí pro zprávu o provedení exportu nebo přenosu, která by měla být elektronicky podepsána. Kvůli ověření je vhodné současně exportovat i certifikát s veřejným klíčem podepisujícího*[15]„.

ERMS určitou dobu uchovává všechna seskupení, dokumenty, metadata a transakční protokoly, které jsou přenášeny. Nejméně do doby potvrzení úspěšnosti ukončeného přenosu[16]. V případě přenosu dojde v ERMS k jeho potvrzení. Poté může dojít ke zničení dokumentů a jeho metadat s výjimkou jejich tzv. hlavičky nutné k identifikaci věcné skupiny, dokumentu, spisu, typového spisu, součásti nebo dílu. Vedle komponent dokumentu musí být zničena i jeho ztvárnění. Nelze však nijak zničit dokument nebo spis, na který je odkazováno křížovými odkazy ze spisu nebo dokumentu, který zničení podléhá. V takovém případě se spis ponechá a případně samostatný dokument přetřídí. (14).

[13] Požadavky č.5.3.1 a 5.3.4 NS ESSS

[14] Požadavky 5.3.2, 5.3.5 a 5.3.10 NS ESSS

[15] Požadavky č. 10.7.9. a 10.7.10 NS ESSS

[16] Požadavek č. 5.3.4 NS ESSS

2.4 Ukládání digitálních dokumentů

Základní rozdíl mezi uchováváním analogových a digitálních dat je zejména ve faktu, že pokud chráním listinný dokument, chráním nosič, když chráním elektronický dokument, chráním data. Je nutné si uvědomit, že vývoj metod pro ukládání digitálních dokumentů se stále velmi významně vyvíjí díky neustálému vývoji informačních a komunikačních technologií. Z hlediska ukládání digitálních dokumentů je podstatné, na jak dlouho jsou dokumenty ukládány a jak často se k nim přistupuje.

2.4.1 Kategorie archivace podle doby uložení dokumentů

Z pohledu délky archivace dokumentů můžeme obecně archivaci rozlišovat podle doby uložení dokumentů na:

• dočasnou – doba, po kterou nevyprší platnost certifikátu pro verifikaci podpisu,

• krátkodobou – doba archivace je řádově srovnatelná s délkou platnosti certifikátu pro verifikaci elektronického podpisu, tj. 1–3 roky v závislosti na archivačním řádu konkrétního archivu,

• střednědobou – 10–20 let,

• dlouhodobou – 20–50 let,

• trvalou – archivace dokumentů majících historickou hodnotu, nad50 let.

V průběhu archivace dokumentu může být dokument přesunut z jednoho archivu do druhého.

2.4.2 Krátkodobé uložení dokumentů

Jedná se o dobu, kdy je dokument v oběhu při vyřizování spisu.

V tomto případě je doba uložení tak krátká, že není nutné se zabývat otázkami trvanlivosti zvoleného úložiště a zastaráván datových formátů. Podstatná je zde zejména důvěryhodnost, tedy platnost vytváření a ověřování autentizacích prvků, jako uznávaných elektronického podpisu, uznávaných elektronických značek a kvalifikovaných časových razítek.

2.4.3 Střednědobé uložení dokumentů

Doba, po kterou jsou dokumenty uloženy v ERMS zajišťujícím činnost spisovny, resp. správního archivu s požadavkem vysoké dostupnosti, která je nutná pro vyřizování dokumentů. Protože doba může přesáhnout i několik let, je nutné se zde zabývat platností kvalifikovaných certifikátů, zastaráváním datových formátů a degradací technických nosičů. Dle ArSSZ § 3 odst. 5 *„v případě dokumentů v digitální podobě se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.“*

Zajištění věrohodnosti původu digitálních dokumentů souvisí jednak s procesními postupy identifikace původu dokumentů (u doručených dokumentů odesilatele, u vlastních dokumentů zpracovavatele a schvalovatele) a jednak s ověřováním elektronických zabezpečovacích prvků typu uznávaný elektronický podpis a uznávaná elektronická značka, které jak už je několikrát zmíněno, jsou jednoznačně spojeny s podepisující osobou a identifikují ji (14).

Zajištění neporušitelnosti obsahu digitálního dokumentu tvoří dvě realizační postupy, přičemž jeden z nich je procesní a druhý technický. Procesní postup souvisí s celkovým zajištěním úložiště, nastavením přístupových práv a povolených operací pro jednotlivé uživatele. Technický postup zajišťuje neporušitelnost obsahu zejména prostředky elektronické značky (v tomto případě nemusí jít o uznávanou elektronickou značku), nebo obdobným technickým způsobem, např. ukládáním otisku dokumentů. Avšak vlastní opatření dokumentu elektronickou značkou ještě neznamená, že k porušení obsahu dokumentu nemůže dojít, ale že je vždy zpětně prokazatelné, zda k němu došlo či nikoliv. V praxi je nejlepší oba postupy kombinovat (14).

Zajištění čitelnosti digitálních dokumentů souvisí s problematikou datových formátů (14). Protože § 64 odst. 1 ArSSZ stanoví, že *„určení původci zajistí příjem digitálních dokumentů alespoň v datových formátech stanovených jako výstupní datové formáty, nebo ve formátech, které jsou výstupem z autorizované konverze dokumentů,“* znamená to, že ERMS musí v rámci střednědobého uložení dokumentů minimálně tyto formáty

ukládat a vypořádat se se zachováním jejich čitelnosti. Z hlediska metod pro udržení čitelnosti datových formátů podléhajících zastarávání jsou zde zvoleny dvě základní strategie. První strategií je volba datových formátů s otevřenou dokumentací, jež je mnohdy podložena dokonce příslušnými ISO standardy. Díky tomu se ve střednědobém horizontu riziko zastarávání daného formátu zásadně snižuje. Ale konkrétní původce může povolit příjem digitálních dokumentů i v dalších datových formátech, a proto může přijít na řadu druhá strategie, kterou je v tomto případě migrace za pomoci změny datového formátu podle § 69a ArSSZ.

Odpovídající tvorba a správa metadat náležejících k digitálním dokumentům je často podceňovaným, avšak nezbytným opatřením. Během této části životního cyklu dokumentu, kdy je dokument vyřizován (tedy od začátku zaevidování dokumentu ve spisové službě až po okamžik vyřízení), metadata typicky vznikají a je třeba kontrolovat jejich korektnost. Další kontrola se provádí před předáním dokumentu do spisovny. Metadata jsou také klíčová při vyhledávání uložených dokumentů. Bez korektních metadat dokument není možné vytvoření SIP balíčku pro předání dokumentu do archivu (14).

Připojení údajů prokazující existenci digitálního dokumentu v čase je čistě technická záležitost. Je možné využít kvalifikovaného časového razítka nebo obdobného technického prostředku. V rámci požadavků kladených NS ESSS na ERMS byl pro snížení nákladů na používání kvalifikovaných časových razítek na každý digitální dokument vytvořen postup denních svorek transakčních protokolů obsahující otisky v daný den přijatých anebo vytvořených dokumentů. Prokázání existence dokumentu v čase je tak sice nepřímé, avšak s ohledem na zvolené technologie dostatečně průkazné. Na to je potřeba dbát hned při implementaci ERMS a i nadále, aby nedošlo k narušení digitální kontinuity, jejíž případné navázání je spojeno s vysokými finančními náklady nebo je dokonce nemožné. Pokud ERMS zajistí uvedené požadavky, stává se tak institucionálně důvěryhodným repozitářem (14).

2.4.4 Dlouhodobé uložení digitálních dokumentů

Dlouhodobým uložením digitálních dokumentů se rozumí jejich uložení v digitální spisovně. ArSSZ nerozlišuje střednědobé a dlouhodobé uložení digitálních dokumentů, takže aspekty problematiky pro dlouhodobé uložení jsou stejné jako pro střednědobé.

2.4.5 Trvalé uložení

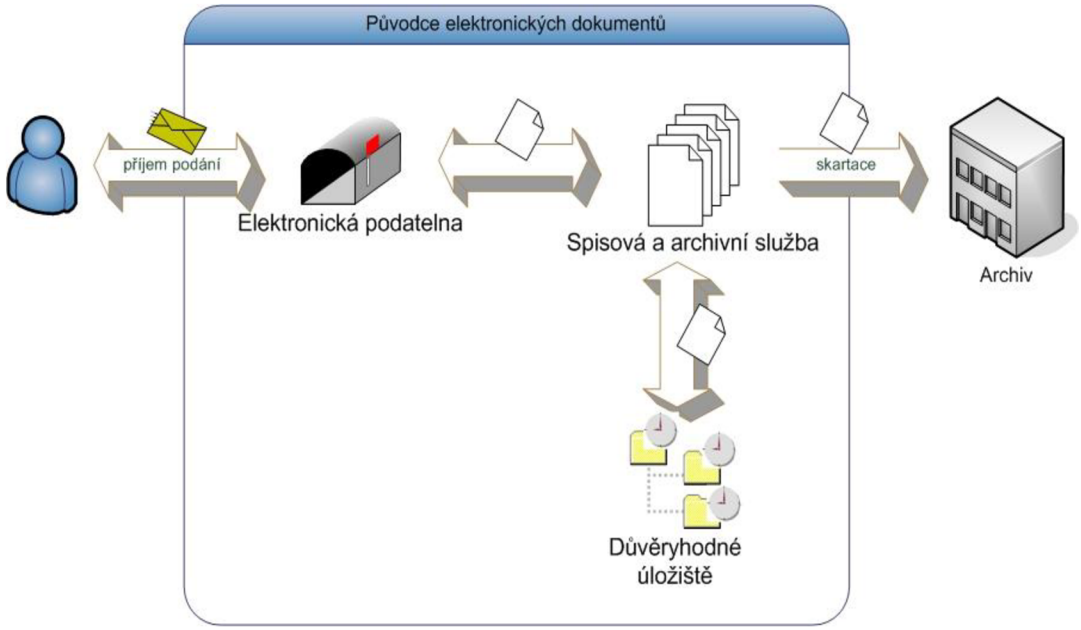
Jedná se o uložení, o které se stará Národní (digitální) archiv. Dokument by od tohoto okamžiku již neměl být součástí ERMS.

3 NÁVRH VLASTNÍHO ŘEŠENÍ

V této části bakalářské práce bude nastíněno, jaká je moje představa o bezproblémovém chodu dlouhodobé archivace v rámci orgánu veřejné správy. Na začátku je důležité si objasnit, jakým bodem životního cyklu dokumentu se budu zabývat a proč je to nutné. Dále se pokusit vysvětlit řešení největšího problému při dlouhodobém uložení digitálních dokumentů, a to zajištění jejich autenticity a důvěryhodnosti. Nebudu se zabývat technickým řešením problému, pouze navrhnu možné řešení.

3.1 Životní cyklus dokumentu

Na obrázku je znázorněný životní cyklus digitálního dokumentu. Oblast původce elektronických dokumentů pro tuto práci představuje orgán veřejné správy. Jak a proč se dokument dostane od elektronické podatelny do spisovny je popsáno v předcházejících kapitolách. Stěžejní bod je mezi elektronickou podatelnou a archivem, konkrétně důvěryhodné úložiště, které musí mít orgán veřejné správy zajištěné, protože dokumenty a spisy, které mohou na tomto místě zůstat i několik let.



Obr. 3Životní cyklus digitálního dokumentu. (16)

Prvním důvodem jsou skartační lhůty, které jsou uvedeny ve spisovém řádu, jehož součástí je i skartační plán, který jsou veřejnoprávní původci povinni vydat na základě § 66 ArSZZ. Podrobnosti jsou uvedeny ve SSV – viz kapitola 1.9.7 a 1.9.9 výše. Vzhledem k tomu, že tato vyhláška neobsahuje podrobnosti k provedení této povinnosti, vydal odbor archivní správy Ministerstva vnitra Vzorový spisový a skartační plán pro obce s rozšířenou působností. Dále Moravský zemský archiv v Brně vydal vzorové plány pro různé původce. Spisový plán vždy musí schválit příslušný archiv a poskytuje metodickou pomoc při jeho tvorbě. Čas od času vydávají jednotlivá ministerstva metodické pokyny, ve kterých stanovují přesné skartační lhůty pro určité dokumenty (např. Ministerstvo pro místní rozvoj vydalo Metodický pokyn pro archivaci dokumentů v rámci operačních programů) nebo jsou skartační lhůty dané zákonem – zákon č. 563/1991 Sb. O účetnictví – skartační lhůta pro účetní závěrky a výroční zprávy je 10 let (§ 31 a 32).

U skartační lhůty mohou nastat extrémy, které stanovuje například 2/2009 SIS Instrukce Ministerstva spravedlnosti ze dne 19. prosince 2008, č. j. 94/2007-OIS-ST, kterou se vydává skartační řád pro okresní, krajské a vrchní soudy ve znění instrukcí č. 10/2011 SIS a č. 9/2013 SIS. Tady některé spisy mají skartační lhůtu stanovenou až na 75 let.

Dalšími důvody mohou být např. běžící správní řízení, kterým se zpravidla pro tento účel zakládá spis, do kterého se vkládají dokumenty vztahující se k předmětné věci. Tyto dokumenty mohou být vyřízené, ale neběží jim skartační lhůta. Skartační lhůta začíná běžet v okamžiku uzavření spisu od 1. ledna následujícího kalendářního roku a řídí se nejdelší skartační lhůtou nejpozději vloženého dokumentu. Pokud je ale ve spise vložen dokument, který očekává zadání spouštěcí událost, která není dosud známa, nelze rok skartace určit. To znamená, že spis po svém uzavření bude čekat na zadání spouštěcí události a skartační lhůta nebude do té doby plynout.

Praktickým příkladem může být třeba u sociální právní ochrana dětí a mládeže – sociální odbor – vede spisy nezletilých dětí (z různých důvodů – pěstounská péče, problematické děti atp.), spis po vyřešení „problému“ uzavře, ale spouštěcí událost nastává teprve v okamžiku nabytí zletilosti dítěte a tudíž skartační lhůta začíná plynout 1. ledna následujícího roku po nabytí zletilosti dítěte.

Nebo z jiného oboru – výstavba – postaví se dům, po kolaudačním řízení se spis uzavře, ale pokud dům stojí, je spis tzv. „živý“ a spouštění událost nastává v okamžiku zbourání stavby. Ačkoliv je skartační lhůta u realizovaných staveb 20 let se znakem A, spis zůstává uložen ve spisovně úřadu a není možné jej předat do Národního (digitálního) archivu.

3.2 Udržení autenticity dokumentu

Dříve bylo považováno za největší překážku udržování platnosti elektronického podpisu nebo elektronické značky. Certifikáty k těmto atributům jsou vydávány na omezenou dobu a obnova certifikátu, většinou po uplynutí jednoho roku, je nutná z důvodu bezpečnosti. Postupem času vždy bezpečnost klíče klesá, protože čím déle se s nimi pracuje, tím více přibývá příležitostí, jak se jich zmocnit. Existují samozřejmě i další důvody, třeba vývoj stále novějších kryptosystémů (17).

Podle pana Ing. Miroslava Čejky, hlavního metodika DRMS (Document Record Management System) z Gordic spol. s.r.o. již tato problematika není tak složitá. (19) A Zajištění důvěryhodného úložiště nespočívá jen v péči o elektronický podpis, i když někteří dodavatelé celou tuto oblast redukují právě jen na starost o elektronický podpis. Důvěryhodnost je opřena o dvě věci – o důvěryhodnost systému, který dokument spravuje (tedy ERMS), a o prvky, které v sobě dokument sám nese. Pokud je dokument v důvěryhodném systému, tak je nezpochybnitelné, že dokument je stále tím dokumentem, za který se vydává a nebyl např. modifikován. Pokud ale takový dokument opustí tento důvěryhodný systém, bude např. odeslán jinam, tak musí nést atributy, které garantují jeho důvěryhodnost. Tedy např. elektronický podpis osoby archivu jako doklad, že dokument je stále autentický, a nezbytné časové razítko. Pokud by se dokument nenacházel v žádném důvěryhodném systému, je nutné se kontinuálně starat o jeho časové razítko, tedy před expirací tzv. přerazítkovat razítkem novým, aby byla zaručena kontinuální garance integrity dokumentu v čase (viz kapitola 3.2.1 Archivní kvalifikovaná časová razítka). Mohou nastat výjimečné případy, které je nutné také zohledňovat, např. prolomení algoritmu pro hash. Čas od času se z bezpečnostních důvodů přechází na složitější a tím i bezpečnější hashovací algoritmy, z důvodu kompromitace těch starších (SHA-1).

Hash je digitální otisk zprávy, který vzniká použitím hashovacího algoritmu, převádějícího jakýkoliv digitální dokument (obecně řečeno vstupní posloupnost libovolného počtu bitů) na normalizovaný otisk (výstupní posloupnost pevné délky n bitů); v současnosti se používají algoritmy skupiny SHA-2 (2).

V těchto případech je také nutné dokument orazit novým časovým razítkem s novým, vyšším zabezpečením.

Zajištění autenticity závisí také uchovávací strategii - tedy na datovém formátu dokumentů, na systémové bezpečnosti -která je úzce spojena s finančními nároky, dále musí být vždy monitorováno, dokumentováno a přezkoumáváno jak a kým byl dokument přijat, jak a kým zpracován, kdo k němu smí přistupovat a kdo k němu smí přistupovat, a kdy a kdo kontroluje a spravuje uložené dokumenty. Odborní pracovníci musí neustále kontrolovat a posuzovat platnou legislativu, právní předpisy a mezinárodní standardy (19).

3.2.1 Archivní kvalifikovaná časová razítka

„Časové razítko je nástroj, který důvěryhodným způsobem zajišťuje přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům nebo událostem, a to na základě důvěryhodného času odvozeného od UTC“ (18).

Pro archivní kvalifikovaná časová razítka platí to stejné jako pro klasická časová razítka, o kterých píši v kapitole 1.7, kromě délky platnosti. Zde je z pravidla mnohem delší, zhruba 10 let.

Archivní kvalifikovaná časová razítka se používají tam, kde klient potřebuje uložit digitální dokumenty na delší časové období (cca 10 i více let) a současně důvěryhodným způsobem po celou dobu uložení prokázat platnost dokumentu, čas jeho uložení, neměnnost obsahu (18).

Klient odebírá klasická časová razítka, interní aplikace certifikační autority hlídá platnost časového vydaného razítka. Před koncem platnosti certifikátu časové autority, nejdříve však po vydání nového certifikátu, aplikace časové razítko přerazítkuje a uloží v interních systémech certifikační autority. Na základě dotazu klienta vyhledá certifikační autorita konkrétní razítko a klientovi poskytne přerazítkované razítko/a, protokol o řetězených/přerazítkovaných razítkách podepsaný certifikační autoritou,

službu na vyhledání přerazítkovaného razítka, kompletní strukturu údajů pro potřeby např. soudního znalce (18).

3.3 Zajištění důvěryhodného úložiště

Nejjednodušší a nejefektivnější zajištění důvěryhodného úložiště je dle mého názoru pořízení systému, který poskytují různé společnosti, který nám zajistí jednak uložení elektronických dokumentů podle ArSSZ, NS ESSS, ElÚAKDZ, SSV a podle úrovně technického řešení problematiky obvyklého v Evropské unii (viz kapitola 1.9.4). Poslouží také v udržení autenticity dokumentu, kontrolu formátu samotného dokumentu a metadat, garanci čitelnosti uloženého obsahu v budoucnosti, vyřazování dokumentů podle skartačního plánu a možnost jejich vyhledávání za pomocí metadat.

Pořízení tohoto systému může být samozřejmě nákladné. Bohužel i jeho správa a údržba. Na trhu se vyskytuje větší množství společností, které tuto službu nabízejí a jejich ceníky jsou různé. Nejpohodlnějším řešením je implementace modulu důvěryhodného úložiště přímo do informačního systému veřejné správy (dále jen ISVS) pokud ovšem tuto variantu vydavatel konkrétního ISVS umožňuje. Nejdříve je nutné tedy objasnit, co je a co není ISVS, a následně posoudit možnosti implementace důvěryhodného úložiště.

3.3.1 Informační systémy veřejné správy (ISVS)

ISVS jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Aby mohl být určitý informační systém označován za ISVS, je nutné naplnění materiálních znaků ISVS, které stanovuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. Povaha informačního systému vyplývá přímo z § 3 odst. 1 zákona o ISVS (20).

Podle § 5a zákona o ISVS „*orgány veřejné správy si zajistí atestaci dlouhodobého řízení informačních systémů veřejné správy a prokáží splnění povinností podle odstavců 1 a 2 atestem dlouhodobého řízení informačních systémů veřejné správy. Rozsah provozní dokumentace předkládané při atestaci stanoví prováděcí právní předpis. Povinnost podle věty první se nevztahuje na obce, které vykonávají přenesenou působnost pouze v základním rozsahu).*“

Tyto podmínky avšak musí splnit sám orgán veřejné správy, nikoli dodavatel informačního systému. Ministerstvo vnitra vydalo doporučení, jak postupovat při plnění povinností vyplývající z tohoto zákona.[17] Správcem těchto ISVS jsou ministerstva, jiné správní úřady a územní samosprávné celky (orgány veřejné správy). Důležitý je také Komentář k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů: Co je a co není informační systém veřejné správy[18].

V České republice je v provozu 7006 ISVS. Pro tuto práci podstatné v oblasti Archivnictví – 131 ISVS a Spisová služby – 412 ISVS (21).

3.3.2 Možnosti implementace

Na trhu existují společnosti, které nabízejí produkt Archiv a Spisová služba. Můžeme se setkat s dodavateli, kteří o sobě tvrdí, že jsou poskytovateli informačních systémů pro veřejnou správu. V podstatě jde o firmy, které původci, ve své odbornosti a znalosti dodávají podklady pro atestaci (např. školení, bezpečnost) pro splnění podmínek stanovené v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Pro pohodlný a bezproblémový přenos dokumentů a informací z informačního systému konkrétního orgánu veřejné správy do jeho systému spisové služby je nejjednodušší mít programové vybavení od jedné společnosti. Pokud to není možné, existuje varianta napojení produktů od rozdílných poskytovatelů, ale podmínkou je rozhraní. Čili softwarové zařízení, které zajistí bezproblémovou komunikaci, aby si mohli oba systémy vyměňovat informace a dokumenty. V zásadě si potřebují systémy navzájem předávat pouze SIP balíčky. To bývá největší problém, protože není nijak standardizován, respektive existují některé pokusy, ale nejsou dostačující. Lze to řešit jedině součinností obou dodavatelů.

V praxi například existuje případ - který uvedl Ing. Miroslav Čejka, hlavní metodik DRMS (Document Record Management System) z Gordic spol. s.r.o. (19), - kooperace Krajské digitální spisovny (KDS), provozované na krajských úřadech. Ty slouží pro

---

[17] Dostupné na <http://www.mvcr.cz/clanek/jak-postupovat-pri-plneni-povinnosti-vyplyvajicich-ze-zakona-c-365-2000-sb.aspx>

[18] Dostupné na < http://www.mvcr.cz/clanek/co-je-a-co-neni-isvs.aspx>

ukládání dokumentů nejen daného krajským úřadem, ale i pro podřízené organizace a obce, které to chtějí využívat. Tedy opravdu velká směska nejrůznějších systémů pro spisovou službu, které se na tyto centralizované úložiště napojují. Zřejmě hlavním dodavatelem KDS jsou společnosti Gordic spol. s.r.o. a ICZ a.s., plus některé další, které zmiňuji dále. Je zde i spousta případů, kdy spisové služby GINIS od Gordic spol. s.r.o., třeba na obcích, se takto napojují na jiná úložiště, např. na produkty společnosti ICZ a.s.

3.4 Přehled potenciálních dodavatelů

V této kapitole jsou shrnuty výsledky po průzkumu trhu. Jak jsem již uvedla výše, společností nabízející tuto službu je veliké množství. Vybrala jsem osm, dle mého názoru nejzajímavějších z hlediska jejich referencí, možnosti implementace, let zkušeností, počtu klientů po České republice a plnění aktuálně platné legislativy. Společnosti a informace o nich jsem nalezla na jejich webových stránkách, případně u nich osobně ověřila. Loga firem jsou taktéž převzaty z oficiálních webových stránek firem. Cena této služby je vždy individuální. V tabulce je uveden souhrn společností a název jejich systému důvěryhodného dlouhodobého úložiště (DDÚ), pod tabulkou jsou společnosti představeny konkrétněji.

Pořadí	Název společnosti	Název systému DDÚ
1	AiP Safe s.r.o.	SAFE
2	Aplis.cz a.s.	absSuite
3	CCA Group a.s.	3D archiv
4	GEOVAP, spol. s r.o.	TomStorage
5	Gordic spol. s.r.o.	GINIS GDU
6	ICZ a.s.	ICZ DESA
7	Software602 a.s.	Dlouhodobý archiv
8	VUMS LEGEND, spol. s r.o.	FIDO

Tab. 3 Společnosti poskytující dlouhodobé důvěryhodné úložiště

AiP Safe s.r.o.

AiP Safe je česká společnost, která se zaměřuje na řešení a produkty pro správu dokumentů a řízení jejich oběhu. Působí v oblasti DMS (Document Management System) i ECM (Enterprise Content Management). Mezi jejich zákazníky patří z veřejného sektoru například Slovenské národní muzeum nebo Úřad průmyslového vlastnictví. Produkty společnosti splňují podmínky pro implementaci ve veřejné správě dle §6 zákona č. 365/2000 Sb. Jejich systém SAFE zajišťuje bezpečné dlouhodobé důvěryhodné uložení dat a metadat včetně jejich efektivní správy a logické ochrany. Splňuje s mezinárodními standardy a především normu OAIS (22).

Aplis.cz a.s

Aplis je poskytuje produkty a služby v oblasti informačních technologií. Na základě své produktové platformy abcSuite nabízí profesionální řešení jak pro oblast veřejné správy, tak i pro oblast komerční sféry. Mezi jejich zákazníky z oblasti veřejné správy patří například Český statistický úřad, Ministerstvo financí ČR a Ministerstvo životního prostředí ČR. Současně pokrývají tato řešení celý životní cyklus dokumentů, to znamená správu dokumentů od vstupu do organizace, přes evidenci, elektronické zpracování a řízený oběh až po jejich bezpečné uložení, archivaci a případně i skartaci.

V jejich nabídce můžeme najít produkt Důvěryhodné úložiště, který odpovídá standardu OAIS (Open Archival Information Systém – norma ISO 14721) (23).

CCA Group a.s.

CCA Group je předním poskytovatelem informačních systémů v České republice se zaměřením na obory systémová integrace, správa dokumentů a business intelligence. Mezi jejich zákazníky patří významné firmy z různých odvětví průmyslu a služeb či organizace státní a veřejné správy. Mezi jejich klienty patří Ministerstvo pro místní rozvoj, Státní úřad pro jadernou bezpečnost aj. Jejich řešení důvěryhodného úložiště se nazývá 3D archiv. Systém je postaven na technologii Java a je vyvinut jako technologicky nezávislé řešení, které lze úspěšně integrovat do stávajícího informačního systému (24).

GEOVAP, spol. s r.o.

Jedním z mnoha zaměření společnosti GEOVAP je na vývoj softwaru a poskytování služeb v oblastech agend veřejné správy. Implementace Spisové služby byla provedena na krajských úřadech, magistrátech, městských i obecních úřadech, příspěvkových a dalších organizacích v České republice. Nabízí hodně produktů a jedním z nich je Spisová služba. Spisová služba má vlastní úložiště elektronických dokumentů a je možné její napojení i na robustnější datová úložiště. Systém určený pro centralizovanou správu a krátkodobou až střednědobou archivaci digitálních dat se jmenuje TomStorage. Systém drží soulad s platnou legislativou (NSESSS, zákon 499/2004 Sb., 300/2008 Sb., 259/2012 Sb., 193/2009 Sb., 194/2009 Sb., a další.). Využívá standardizovaný implementační postup pro rychlé nasazení systému (25).

Gordic spol. s.r.o.

Nejrozšířenější poskytovatel informačních systémů pro veřejnou správu. Jejich systém GINIS s 20letou praxí v současné době používá více než 6000 klientů, mezi které patří organizace veřejné správy všech velikostí (od příspěvkových organizací až po ministerstva). K nejvýznamnějším uživatelům patří Ministerstvo obrany ČR, Ministerstvo vnitra ČR, Ministerstvo práce a sociálních věcí ČR, Ministerstvo zdravotnictví ČR, Ministerstvo kultury ČR, Kancelář prezidenta republiky aj. Mezi jeho funkční oblasti patří i digitální archivy, spisovny a úložiště. Ucelená sada modulů GINIS BASIC – ULTIMATE zahrnuje diagnostiku datových formátů, důvěryhodný archiv (GDA), elektronické skartační řízení (ESR), garantované dlouhodobé úložiště digitálních dokumentů (GDU), spisovnu (SPI) a správu uložených digitálních dokumentů (SUD). Řešení modulu GDU, který je významný pro tuto práci by měl být nezávislý na provozovaném systému spisové služby (26).

ICZ a.s.

ICZ je významným integrátorem a je schopna nabízet úřadům komplexní řešení pro podporu efektivního fungování jejich agend a usnadnění komunikace občanům s úřadem. Dodávky zahrnují potřebnou infrastrukturu a řešení jak pro samotný úřad, tak pro jím zřizované a zakládané organizace. Spolupracují například s Magistrátem hlavního města Prahy nebo Liberce, s Fakultní nemocnicí Brno nebo národním archivem (27).

Mimo jiné nabízejí i řešení ICZ DESA, čili důvěryhodnou elektronickou spisovnu a archiv. Dokumenty a spisy se do ICZ DESA ukládají primárně po jejich uzavření, přičemž jejich životnost je určena jednotným spisovým plánem. Po uplynutí skartační lhůty dojde ke skartaci dokumentů nebo jsou jako vybrané archiválie předány do Národního digitálního archivu. Přístup k uloženým dokumentům v elektronické spisovně mají uživatelé prostřednictvím uživatelského rozhraní spisovny nebo prostřednictvím spisové služby / agendových systémů, které jsou schopny vyžádat si potřebný dokument ze spisovny přes komunikační rozhraní (27).

Software602 a.s.

Společnost Software602 poskytuje komerčnímu a veřejnému sektoru řešení pro pořízení, zpracování a uchování důvěryhodných digitálních dokumentů, dokladů a dat. Mezi zákazníky této společnosti z veřejného sektoru patří například Česká pošta, CzechPoint, Poslanecká sněmovna Parlamentu České republiky nebo Ministerstvo průmyslu a obchodu (28).

Jejich produkt FormFlow, díky kterému probíhají veškeré podnikové procesy, poskytuje celkový přehled o toku informací a o tom, kde se zdržují klíčová rozhodnutí. Přináší rychlou a jednoduchou administrativní činností přehlednou správou veškeré agendy a jednoznačností sesbíraných údajů. Lze jej rozšířit o aplikační nadstavby Řízené dokumentace nebo Spisové služby, zejména ale o Dlouhodobý archiv. Dokumenty do dlouhodobého archivu mohou být automaticky přebírány z různých zdrojů, jako jsou výstupy schvalovacích procesů, výstupy informačních systémů, odeslané dokumenty (datové zprávy, e-maily, soubory určené pro tisk, dokumenty předané přes webové rozhraní apod.) či výstupy konverze. Mohou být také vkládány manuálně (28).

VUMS LEGEND, spol. s r.o.

VUMS LEGEND, spol. s r.o. poskytuje komplexní služby při výběru, zavádění a dalším rozvoji informačních systémů a technologií včetně sítí. Společnost VUMS LEGEND je dodavatel firemních informačních systémů. Spolupracují například s Ministerstvem vnitra ČR, Ministerstvem spravedlnosti ČR a Úřadem vlády ČR. Jedním z jejich produktů je správa dokumentů, která zahrnuje důvěryhodné úložiště FIDO, spisovou službu a SPI 8NS, správní řízení a elektronickou podatelnu. FIDO je řízen a designován dle obecně platné normy OAIS. K přednostem společnosti patří zejména schopnost

vytvářet a zavádět informační systémy ve všech běžně využívaných prostředích a řešit datové komunikace mezi různými systémy na různých platformách (29).

4 ZÁVĚR

Cílem práce bylo prozkoumat problematiku dlouhodobého ukládání (archivování) digitálních dokumentů v rámci orgánu veřejné správy. V poslední době ve veřejné správě radikálně narůstá počet dokumentů v digitální podobě a je bohužel nutné je ukládat, ať už na krátkou nebo dlouhou dobu, protože tak stanovuje legislativa. Důvodem mohou být skartační lhůty nebo běžící správní řízení. Důležitou součástí problematiky je zajištění autenticity dokumentů, čili abychom byli i s odstupem času schopni dokázat jeho pravost. Přestože mají úřady povinnost dle zákona dokumenty ukládat, toto téma nikdo příliš neřeší a raději se provádějí konverze do listinné podoby a uchovává se klasickým způsobem, což vede k zbytečným výdajům.

V této práci jsem vysvětlila pojmy, které s dlouhodobým ukládáním digitálních dokumentů souvisí a je nutné je znát. Popsala jsem funkcionalitu atributů, které jsou potřeba k potvrzení pravosti digitálních dokumentů a znázornila platnou legislativu, o kterou se archivace v současné době opírá. Dále jsem uvedla, jak funguje spisová služba, pojmy, které se v rámci spisové služby používají a jak probíhá skartační řízení včetně výběru dokumentů, které se budou ukládat.

Zjistila jsem, jaké jsou možnosti zajištění ukládání dokumentů. Uložení dokumentů lze zajistit informačním systémem důvěryhodného úložiště, které musí splňovat podmínky stanovené zákonem, aby mohl být použit v rámci veřejné správy. V části Návrh řešení jsem uvedla a podrobněji popsala osm společností, které jsou dodavateli důvěryhodného úložiště, a z hlediska zjištěných informací bych je doporučila.

Práce může sloužit jako podklad při zajišťování důvěryhodného úložiště v nějakém konkrétním orgánu veřejné správy. Ten, kdo bude chtít něco takového realizovat, se může v práci dozvědět, jaké aspekty jsou při zajišťování důležité, jak takové důvěryhodné úložiště funguje a jaké jsou možnosti řešení.

V práci bych popřípadě ráda pokračovala v navazujícím, magisterském studiu. Zajímal by mě fakt, zda se problematika někam posunula. Jestli většina úřadů stále převádí raději digitální dokumenty do listinné podoby nebo se smířila s moderní dobou a začala pracovat na digitalizaci. Ovšem s mými teď již získanými informacemi a zkušenostmi je pravděpodobnost nějakého pokroku za dva roky velmi malá. Je otázkou, zda nařízení

eIDAS, které nabývá účinnosti 1. července 206, a připravovaná zákon o službách vytvářejících důvěru změní situaci k lepšímu.

SEZNAM ZDROJŮ

(1) LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013, 256 str. ISBN: 978-80-87576-41-0.

(2) MATES, P., SMEJKAL, V. *E-government v České republice*. Právní a technologické aspekty. 2. podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, 456 str. ISBN 978-80-87576-36-6.

(3) MINISTERSTVO VNITRA ČESKÉ REPUBLIKY [online]. *Přehled udělených akreditací.* [cit. 20. 12. 2015]. Dostupné na: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>

(4) EPRAVO.CZ [online]. *58679. Ostrý start datových schránek – 1. listopadu 2009.* [cit. 23. 1. 2016]. Dostupné na: <*http*://www.epravo.cz/top/clanky/ostry-start-datovych-schranek-1-listopadu-2009-58679.html>

(5) BUSINESSIT [online]. *Proč je důležité archivovat významné dokumenty podle norem PAdES, CAdES či XAdES.* [cit. 2. 1. 2015]. Dostupné na: <http://www.businessit.cz/cz/archivace-vyznamne-dokumenty-normy-pades-cades-xades-platnost-elektronicky-podpis.php>

(6) MINISTERSTVO VNITRA ČESKÉ REPUBLIKY [online]. *Archivnictví.* [cit. 5. 2. 2016]. Dostupné na: <http://www.mvcr.cz/clanek/archivy-a-archivalie.aspx>

(7) NÁRODNÍ ARCHIV [online]. *Digitální archiv. Národní archiv po roce zkušebního provozu*. [cit. 2. 1. 2016] Dostupné na: <http://digi.nacr.cz/wp-content/uploads/2015/12/Stodulka.pdf>

(8) KLÍMA, Vlastimil. *Nový standard digitálního otisku SHA-3*. Sdělovací technika: Kryptografie pro praxi [online]. 2012 [cit. 5. 2. 2016]. Dostupné na: <http://cryptography.hyperlink.cz/2012/ST_2012_12_09_11.pdf>

(9) KYSELA, František. *Zálohování a archivace dat není totéž: Poznejte rozdíly.* OnBusiness [online]. 2013 [cit. 9. 2. 2016]. Dostupné na: <http://onbusiness.cz/zalohovani-a-archivace-dat-neni-totez-poznejte-rozdily-134>

(10) NÁRODNÍ ARCHIV [online]. *O nás. Historie archivu.* [cit. 9. 2. 2016]. Dostupné na: <http://www.nacr.cz/A-onas/D-hist.htm?type=s>

(11) BERNAS, Jiří. *Národní digitální archiv* [online]. 2010 [cit. 9. 2. 2016]. Dostupný na:<http://www.drms.cz/2010/down/10/J_Bernas_NDA.pdf>

(12) MINISTERSTVO VNITRA ČESKÉ REPUBLIKY [online]. *Ministerstvo vnitra zahájilo projekt Národní digitální archiv.* [cit. 9. 2. 2016]. Dostupné na: <http://www.mvcr.cz/clanek/ministerstvo-vnitra-zahajilo-projekt-narodni-digitalni-archiv.aspx>

(13) BERNAS, Jiří. *Národní digitální archiv* [online]. 2012 [cit. 9. 2. 2016]. Dostupný z: <http://www.isss.cz/archiv/2012/download/prezentace/bernas_nda.pdf>

(14) KUNT, M. LECHNER, T. *Spisová služba*. Praha: Leges, 2015, 400 str. ISBN 978-80-7502-083-3

(15) EARCHIVACE.CZ [online], *Archivní formát PDF/A*. [cit. 18. 3. 2016]. Dostupné na: <http://www.earchivace.cz/legislativa-a-normy/typy-dokumentu-k-archivaci>

(16) VOHNOUTOVÁ, Marta. *Řešení střednědobé archivace dokumentů ve státní správě* [online]. 2007 [cit. 29. 4. 2016]. Dostupný na: < https://www.isss.cz/archiv/2007/download/prezentace/vohnoutova_siemens.ppt.>

(17) SMEJKAL, V. a VALÁŠEK, M. A. *TEOTWAWKI elektronicky podepsaných dokumentů.* Jak dlouhodobě zajistit důvěryhodnost elektronických dokumentů? Archivní časopis, ročník 61., 2011. č. 4. ISSN 0004-0398.

(18) PRVNÍ CERTIFIKAČNÍ AUTORITA, A. S.. První certifikační autorita, a.s. (I.CA): *Kvalifikovaná časová razítka*. [online]. [cit. 2. 5. 2016]. Dostupné na: <http://www.ica.cz/Kvalifikovana-casova-razitka>

(19) ČEJKA, M. a FIALA, S. *GORDIC® spol. s r.o., Zajištění autenticity.* Sdělení emailem ze dne 10. 5. 2016

(20) MINISTERSTVO VNITRA ČESKÉ REPUBLIKY [online]. *Komentář k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy a o změně*

některých dalších zákonů:Co je a co není informační systém veřejné správy. [cit. 1. 5. 2016]. Dostupné na: <http://www.mvcr.cz/clanek/co-je-a-co-neni-isvs.aspx>

(21) ASD SOFTWARE, S.R.O. [online]. *Informační systém a informačních systémech veřejné správy.* 2015 [cit. 5. 5. 2016]. Dostupné na: <https://www.sluzby-isvs.cz/ISoISVS/Views/Public/Login.aspx?action=get>

(20) AIPSAFE, S.R.O. [online]. AipSafe s.r.o., 2009 [cit. 12. 5. 2016]. Dostupný na: <http://www.aipsafe.cz/cs>

(21) APLIS.CZ, A.S. [online]. Aplis.cz a.s., 2014 [cit. 12. 5. 2016]. Dostupný na: <http://www.aplis.cz/ >

(22) CCA GROUP, A.S. [online]. CCA Group a.s., [cit. 12. 5. 2016]. Dostupný na: <http://www.cca.cz/ >

(23) GEOVAP SPOL. S.R.O. [online]. GEOVAP spol. s.r.o., 2016 [cit. 12. 5. 2016]. Dostupný na: <http://www.geovap.cz/ >

(24) GORDIC SPOL. S.R.O. [online]. Gordic spol. s.r.o., 2016 [cit. 12. 5. 2016]. Dostupný na: <http://www.gordic.cz/ >

(25) ICZ A.S. [online]. ICZ a.s., 2016 [cit. 12. 5. 2016]. Dostupný na: <http://www.i.cz/ >

(26) SOFTWARE602, A.S. [online]. Software602 a.s., 2016 [cit. 12. 5. 2016]. Dostupný na: <http://www.602.cz/ >

(27) VUMS LEGEND SPOL. S.R.O. [online]. VUMS LEGEND spol. s.r.o., 2016 [cit. 12. 5. 2016]. Dostupný na: <http://www.i.cz/ >

(28) MATES, P. a SMEJKAL, V. Dokumenty budoucnosti. *Data Security Management*, 1998.

(29) KLÍMA, Vlastimil. Digitální otisk SHA-4 přeskočil SHA-3. *Sdělovací technika: Kryptologie pro praxi* [online]. 2012. [cit. 17. 5. 2016]. Dostupné na: <www.cryptography.hyperlink.cz/2012/ST_2012_05_18_19.pdf>

(30) SMEJKAL, V., KODL, J., UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*[online]. 2015. ISSN 1805-2797

SEZNAM POUŽITÝCH ZKRATEK

ArSSZ	zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
ElPZ	zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
ElÚAKDZ	zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
ERMS	Elekctronic Record Management Systém – elektronický systém spisové služby
NS ESSS	Národní standard pro elektronické systémy spisové služby
OvěřElPZ	vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověření platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka
SSV	vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky č. 283/2014 Sb.

SEZNAM OBRÁZKŮ

Obr. 1Proces vytváření balíčků. (13) 20

Obr. 2Proces opatření digitálního dokumentu časovým razítkem. (1) 28

Obr. 3Životní cyklus digitálního dokumentu. (16) 56

SEZNAM TABULEK

Tab. 1Rozdíl mezi listinným a digitálním dokumentem. (1, s. 43) 15

Tab. 2 Výstupní datové formáty dokumentů z ERMS. (SSV §23)..... 47

Tab. 3 Společnosti poskytující dlouhodobé důvěryhodné úložiště..... 62