Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

e-Dokument ve veřejné správě

Iva Prouzová

Bakalářská práce
2012

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Iva PROUZOVÁ**
Osobní číslo:	**E090271**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Regionální a informační management**
Název tématu:	**eDokument ve veřejné správě**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je stanovení kritérií pro vymezení kvality eDokumentu ve veřejné správě s důrazem na problematiku jeho správné manipulace a uchování. Práce bude zaměřena na vybrané organizace veřejné správy.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 40 stran**

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

Seznam odborné literatury:

BIITNER, Ivan, et al. *Spisová a archivní služba ve státní správě, samosprávě a v podnikatelské sféře*. **Praha: Linde, 2005. ISBN 80-7201-549-4.**

Česko. Zákon č.499/2004 Sb., o archivnictví a spisové službě. In Sbírka zákonů ČR, 2004. 173 s.

Česko. Strategie realizace Smart Administration v období 2007-2015. In Usnesení vlády č. 757, ze dne 11.7. 2007. 757 s.

Šimonová

Vedoucí bakalářské práce: **Ing. Stanislava Šimonová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. října 2011**

Termín odevzdání bakalářské práce: **30. dubna 2012**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. října 2011

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 31. 07. 2012 Iva Prouzová

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala své vedoucí práce Ing. Stanislavě Šimonové, Ph.D. za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Také bych chtěla poděkovat panu M. Bulíčkovi, správci počítačových aplikací Úřadu Královehradeckého kraje, za poskytnutí množství informací potřebných pro zpracování této práce

ANOTACE

Tato bakalářská práce pojednává o digitalizaci dokumentů ve veřejné správě. Úvodní část se zaměřuje na vlastní životní cyklus elektronického dokumentu. Další část této práce je věnována problematice uchování digitálního dokumentu. Závěrečná část této práce definuje kritéria kvality při manipulaci digitálních dokumentů.

KLÍČOVÁ SLOVA

Digitální dokument, autenticita, integrita, zaručené časové razítko, dlouhodobé ukládání dokumentu, migrace, neshoda, nápravné opatření

TITLE

eDocument in Public Administration

ANNOTATION

This bachelor´s paper deals with digitalization of documents in public administration. The introductory part is focused on its own life cycle of electronical document. Another part of this work is dedicated to the preservation of digital document. The final part of this work defines the quality criteria in the handling of digital documents

KEYWORDS

Digital dokument, autenticity, integrity, guaranteed time stamp, long-term storage of documents, migration, difference, corrective action

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH ZKRATEK

AIP	Archival Information Package
CAF	Common Assessment Framework= Společný hodnotící rámec
CMS	Systém pro správu datového obsahu
DIP	Dissemination Information Package
HSM	Hierarchical Storage Management
ISDS	Informační Systém datových schránek
ISO	International Organization for Standardization
IT	Informační technologie
KDR	Krajský digitální depozitář
KDS	Krajská digitální spisovna
KDÚ	Krajská digitální úložiště
KIVS	Komunikační infrastruktura veřejné správy
NAS	Networked Attached Storage
NDA	Národní digitální archív
NDK	Národní digitální knihovna
OAIS	Open Archival Information Systém
ORP	Obec s rozšířenou působností
SAN	Storage Area Network
SIP.	Submission Information Package
SSL	Elektronická spisová služba
TCK	Technologické centrum kraje

SEZNAM POUŽITÝCH POJMŮ

AGENDOVÝ INFORMAČNÍ SYSTÉM jedná se o elektronický systém spisové služby určený ke správě dokumentů v samostatných evidencích podle vyhlášky č. 191/2009 Sb., o podrobnostech výkonu spisové služby

AUTENTICITA vlastnost dokumentů vyjadřující jejich originální původ a hodnověrnost

BEZPEČNOST DOKUMENTU soubor opatření, které zajišťuje zachování dokumentu

CERTIFIKAČNÍ AUTORITA organizace, která vydává certifikáty, má vlastní certifikát a revokuje (zneplatnění) vydané certifikáty

CZECHPOINT Český Ověřovací a Informační Národní Terminál-kontaktní místo veřejné správy, poskytující občanům zejména ověřené údaje vedené v centrálních registrech. Zároveň zajišťuje konverzi dokumentů z moci úřední z listinné do elektronické formy a naopak

ČÍSLO JEDNACÍ evidenční znak dokumentu v rámci evidence dokumentu, jehož tvar vychází z požadavků právních předpisů

DATOVÝ FORMÁT způsob kódování komponenty, který zajišťuje uložení dokumentu nebo jeho části pro účely zpracování výpočetní technikou a jeho znázornění

DATOVÁ SCHRÁNKA elektronické uložiště určené ke vzájemné komunikaci občanů i firem se státem, ke komunikaci občanů i firem mezi sebou a mezi orgány veřejné moci

DOKUMENT každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, v podobě analogové nebo digitální, která byla vytvořena původcem nebo byla původci doručena. Klíčovou vlastností dokumentu je jeho neměnnost a trvalost jeho informačního obsahu. Dokument tvoří jeden nebo více záznamů.

ELEKTRONICKÁ SPISOVNA funkční složka elektronického systému spisové služby určená k uložení, vyhledávání a předkládání dokumentů pro potřebu původce a k provádění skartačního řízení v rámci informačních činností zajišťovaných tímto systémem

ELEKTRONICKÝ SYSTÉM SPISOVÉ SLUŽBY („ERMS“) informační systém určený ke správě dokumentů

EVIDENCE DOKUMENTŮ („ED“) nástroj umožňující přehledné odborné vedení spisové služby

ISO 14721	Space data and informatik transfer systems- Open archival informatik systém-Reference model
ISO 15489-1	Information and documentation – Record management – Part 1: General
ISO 15489-2	Information and documentation – Record management – Part 1: Guidelines
ISO/TR 15801	Document management – Elektronicky uložené informace – Doporučení pro důvěryhodnost a spolehlivost
JEDNOZNAČNÝ IDENTIFIKÁTOR	znak spojený s entitou zajišťující jeho nezaměnitelnost a jedinečnost. Každá entita v ERMS je označena jedinečným identifikátorem, kterým je údaj v metadatech. Obsahuje zejména označení původce, popřípadě zkratku označení původce, a to ve formě alfanumerického kódu.
KONVERZE	proces transformace jedné nebo více komponent do jiného formátu, výsledkem konverze je ztvárnění.
METADATA	data popisující souvislosti, obsah a strukturu dokumentů a jejich správu v průběhu času (§ 1 písm. n) zákona)
NÁPRAVNÉ OPATŘENÍ	přijaté opatření po zjištění neshody k tomu, aby byla tato neshoda odstraněna nebo , je-li to možné, aby byla odstraněna příčina vzniku této neshody
NESHODA	situace, služba nebo činnost, která neodpovídá stanoveným požadavkům
NEZBYTNÝ DOKUMENT	zásadního významu, který je nezbytný pro schopnost organizace pokračovat v pracovní činnosti, a to s přihlédnutím k zachování její připravenosti pro plnění svých úkolů a s přihlédnutím k vytvořeným předpokladům vypořádat se s následky mimořádných událostí nebo krizových stavů, anebo ochránit své dlouhodobé ekonomické a právní zájmy. Nezbytný dokument musí být po mimořádném ukončení funkci ERMS přednostně obnoven.
NORMA	Výsledek činnosti normalizačních organizací.
OPRÁVNĚNÝ UŽIVATEL	ERMS uživatel, který je pověřen k provedení operace náležející k výkonu spisové služby na základě pravidel organizace, popisovaných v kontextu spisové služby. Různí uživatelé mají rozdílná oprávnění.

POSUZOVATEL SKARTAČNÍ OPERACE správcovská role, jejíž nositel je zodpovědný za provedení procesu výběru archiválií vůči vedení organizace. Je určen vnitřním předpisem organizace.

ROLE je souhrn funkčních oprávnění udělených předem stanovenému uživateli nebo skupině uživatelů ERMS.

SCHVALOVATEL osoba nebo role v ERMS odpovědná v rámci svých oprávnění udělených organizací za obsah dokumentu nebo seskupení. Jedná se o osobu, která podepisuje podle vnitřního předpisu organizace.

SKARTAČNÍ OPERACE je úkon odborné správy dokumentů, při kterém je ve skartačním řízení uplatněn skartační režim.

SKARTAČNÍ REŽIM organizací stanovený systém vyřazování entit, který vymezuje dobu jejich ukládání (skartační lhůta) a určuje typ skartační operace (trvalé uložení, předložení k přezkumu, automatické zničení, zničení po jeho schválení uděleného správcem nebo export do archívu. Při posouzení se v rámci odborné prohlídky vyhodnocují metadata, obsah dokumentu nebo metadata a obsah dokumentu.

SKARTAČNÍ LHŮTA stanová dobu (vyjádřenou v letech), po kterou musí být vyřízený dokument uložen ve spisovně. Je vyjádřena číslicí za skartačním znakem. Skartační lhůta počíná běžet dnem 1. ledna kalendářního roku následujícího po vyřízení dokumentu nebo uzavření spisu. Skartační lhůty nesmí být zkracovány.

SKARTAČNÍ ZNAKY skartační znaky „A“, „S“ a „V“ určují, jak má být po uplynutí skartační lhůty s dokumentem naloženo:

Znak „A“ do této skupiny se zařazují dokumenty trvalé hodnoty, určené ve skartačním řízení jako archiválie k trvalému uložení v příslušném archívu.

Znak „S“ do této skupiny se zařazují dokumenty bez trvalé hodnoty, které po uplynutí skartační lhůty mohou být poté, kdy archiv vydá skartační povolení skartovány, tj. zničeny.

Znak „V“ do této skupiny jsou zařazovány dokumenty, jejichž dokumentární hodnotu nelze v okamžiku určit a u nichž ve skartačním řízení úřad navrhuje a archiv posuzuje, které z nich mají být předány do archivu a které z nich mohou být zničeny.

SPIS je entita, v níž jsou organizovány dokumenty vztahující se ke stejnému předmětu (věci). Spisy se vyskytují pouze ve věcných skupinách, které neobsahují jiné věcné skupiny.

SPISOVÝ A SKARTAČNÍ PLÁN hierarchické uspořádání věcných skupin, spisů, součástí, dílů, dokumentů a komponent, rozdělených podle věcných hledisek se spisovými znaky, skartačními znaky a skartačními lhůtami.

SKARTAČNÍ ŘÁD stanoví postup při vyřazování dokumentů z centrální spisovny v procesu skartačního řízení

SPISOVÁ ZNAČKA je evidenčním znakem spisu (identifikace), pokud tak stanoví jiný právní předpis nebo interní předpis původce. Spisovou značkou je zejména číslo jednací sběrného archu, iniciačního nebo jiného, původcem určeného dokumentu vloženého ve spisu, popřípadě jiné označení, které organizace pro své účely obvykle užívá nebo z jiných důvodu považuje za účelné.

SPISOVÝ ZNAK je označení, které zařazuje dokumenty do věcných skupin pro účely jejich budoucího vyhledávání, ukládání a vyřazování.

SYSTÉM SPRÁVY ELEKTRONICKÝCH ZÁZNAMŮ systém správy elektronických záznamů („EDMS) je počítačovou aplikací zabývající se správou záznamů. EDMS je často úzce integrován se systémem elektronické spisové služby (ERMS) Zatímco EDMS vede pouze záznamy, které nejsou dokumenty, ERMS spravuje dokumenty.

STANDARD Směrnice vydávaných různými konsorcii uživatelů a výrobců IT

TRANSAKČNÍ PROTOKOL soubor informací o operacích provedených v ERMS, které ovlivnily nebo změnily entity. Tyto informace umožňují rekonstrukci historie těchto operací. Transakční protokol umožňuje kontrolu provedených operací.

TŘÍDĚNÍ se rozumí systematická klasifikace dokumentů do seskupení v souladu se spisovým řádem a spisovým plánem, prováděná při výkonu spisové služby.

UZAVŘENÍ se rozumí proces změny atributů spisu, součásti nebo dílu, který se projeví v metadatech, v jehož důsledku je znemožněno vkládání dalších dokumentů neb vyjímání dokumentů stávajících. Současně se dokumenty spisu, součásti nebo dílu převedou do výstupního formátu.

UŽIVATEL	je každá fyzická osoba používající ERMS. Uživatel má v rámci svého uživatelského profilu přiděleny role a může být členem skupin uživatelů se stejnou uživatelskou rolí
ZÁZNAM	se rozumí informace, se kterou lze nakládat jako s jednotkou. Může být v listinné podobě, v mikroformě, na magnetickém nebo na jiném hmotném nosiči dat. Záznamy se svými znaky liší od dokumentů, především nejsou deklarovány jako dokumenty v ERMS. Při výkonu spisové služby se záznamy stávají dokumenty.
ZNÁZORNĚNÍ	je uživatelsky srozumitelná interpretace dokumentu v digitální podobě.
ZNIČENÍ	je proces likvidace záznamu a dokumentu, který znemožňuje jejich rekonstrukci a identifikaci jejich obsahu

ÚVOD

V minulých letech vznikl jeden z koncepčních úkolů vlády České republiky, kterým je zefektivnění veřejné správy a veřejných služeb. Pro tento úkol byly a jsou použity finanční prostředky strukturálních fondů Evropské Unie. Cílem koncepce je snaha o lepší vzájemnou spolupráci orgánů veřejné správy. Komunikace mezi nimi by měla probíhat pouze elektronicky. Cílem je také zlepšení komunikace občanů a správy.

Díky nárůstu využívání moderních informačních technologií a stále častějšímu používání elektronických forem dokumentů vzniká tlak na efektivní správu, ukládání a manipulaci s elektronickými dokumenty. V současné době je prováděna digitalizace již existujících listinných dokumentů a zároveň vznikají dokumenty v digitální formě.

Kraje jsou zapojeny do systému sdílení dat na národní úrovni, což znamená připojení k základním registrům veřejné správy. Mezi základní registry patří Registr osob, Registr obyvatel, Registr územní identifikace adres a nemovitostí a Registr práv a povinností.

Kraje mají být ústředním místem pro zpřístupnění všech zveřejňovaných a veřejně přístupných informací. Zároveň musí zajistit služby elektronické veřejné správy pomocí informačních a komunikačních technologií, digitalizaci datových zdrojů, jejich zpřístupnění a zároveň jejich ochranu. Podílí se na vzniku jednotné platformy pro důvěryhodné ukládání dokumentů, eliminaci rizik ze ztráty dokumentu či únik citlivých informací. Neposledním významným úkolem digitalizace je záchrana dokumentů ve špatném fyzickém stavu.

Cílem práce je stanovení kritérií pro vymezení kvality e-Dokumentu ve veřejné správě s důrazem na problematiku jeho správné manipulace a uchování. Práce je zaměřena na vybrané organizace veřejné správy.

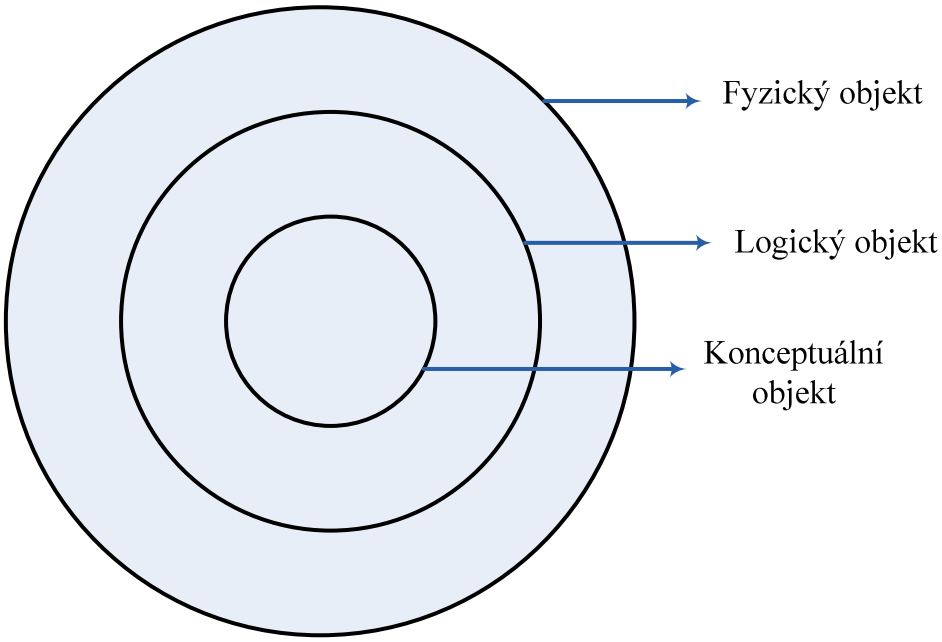
1 VYMEZENÍ E-DOKUMENTU

Digitální dokument se od analogového dokumentu neliší obsahovými, ale formálními vlastnostmi. Jedná se zejména o digitální způsob záznamu informací a z něho vyplývající větší nezávislosti a oddělitelnosti obsahu dokumentu od nosiče dat. Digitální informace jsou informace, které jsou vyjádřené v diskrétní (nespojité) číselné formě. Mohou být uloženy na různých datových nosičích. V dnešní době nejčastěji jsou používány magnetické a optické nosiče.

Podle normy OAIS [4] jsou informace definovány jako jakýkoliv typ znalostí, které mohou být předmětem výměny, přičemž informace jsou vždy vyjádřeny určitým typem dat. Podmínkou komunikace takto reprezentovaných informací je znalostní základna. To znamená, že pro komunikaci jsou nutná nejen data, ale i potřebné znalosti na straně příjemců těchto dat. Norma OAIS definuje data jako reprezentace informací, které lze komunikovat, interpretovat a zpracovávat. Data jsou abstraktní entita. V reálu konkrétní entita je nazývána datovým objektem. Norma OAIS rozlišuje dva typy datových objektů- fyzický objekt a digitální objekt. Fyzický objekt je objekt s fyzicky pozorovatelnými vlastnostmi, který reprezentuje to, co lze zdokumentovat pro účely ochrany, šíření nebo nezávislého využití. Digitální objekt podle normy OAIS je množina bitových posloupností.

1.1.1 Technický model digitálního objektu

Technický model digitálního objektu Kennetha Thibodeaua [4] definuje pro každý digitální objekt tři přístupové vrstvy, jak je znázorněno na obrázku 1:



Obrázek 1: Přístupové vrstvy digitálního objektu

Zdroj: upraveno podle[4]

Fyzický objekt představuje první přístupovou vrstvu. Jedná se o zápis znaků na konkrétním elektronickém nosiči. Rozdílné datové nosiče představují rozdílné technické konvence. Způsob zápisu bitů na datový nosič je nezávislý na významu, které tyto bity reprezentují. Přístup k fyzickému objektu vyžaduje čtecí zařízení. Ochránit možnosti tohoto přístupu odpovídá cíli uchovávání. Logický objekt je rozpoznán a zpracován softwarem. Určuje pravidla pro kódování bitů a jejich převodu z nosiče do paměti systému a datových typů. Přístup k logickému digitálnímu objektu je možný pouze prostřednictvím příslušných softwarových aplikací. Ochránit tento přístup odpovídá cíli zpřístupnění. Konceptuální objekt je smysluplná jednotka informace, kterou uživatel dokáže rozpoznat a rozumět ji. Přístup do všech třech vrstev vytváří úplný digitální objekt.

.

1.2 Charakteristika e-Dokumentu

Digitální podoba zaznamenání informace je chápáno jako převedení původní analogové informace vyjádřené například písmeny, u informace zaznamenané obrazově, zvukově nebo jinak do podoby číselné, nejčastěji do binární číselné soustavy.

Za nejvýznamnější vlastnosti dokumentů jsou chápány tyto dvě vlastnosti:

- kvalita zaznamenané informace se kopírováním nemění, tzn. není rozdíl mezi zdrojem a cílem duplikování těchto dokumentů. Nejsou kopie, ale další originály;
- dokument digitálně zaznamenaný není závislý na jednom konkrétním nosiči.

Z výše uvedených vlastností vyplývá i rozdílný přístup v péči o dokumenty zaznamenané v analogové podobě a o dokumenty zaznamenané v digitální podobě. Analogový dokument je pevně svázán s nosičem. Se zánikem nosiče zaniká i dokument. Mohou být zachovány pouze kopie původního dokumentu. Dokument v digitální podobě nezaniká se zánikem nosiče za předpokladu, že dokument bude dříve převeden na nosič nový, než skončí morální a fyzická životnost nosiče.

Zjednodušené lze říci, že dokumenty podle těchto vlastností se mohou rozdělit na dokumenty v materiálové podobě- ty jsou pevně svázány s materiálním nosičem a dokumenty v nemateriální podobě, které nejsou pevně svázány s jedním materiálním nosičem.

1.2.1 Autenticita dokumentů

Autenticita = pravost dokumentů v případě dokumentu v materiálové podobě je jednoznačná. Jakákoliv změna informace znamená vždy poškození nosiče.

V případě dokumentu v nemateriálové podobě je tato otázka složitější, avšak není neřešitelná. Z pohledu řešení autenticity mají dokumenty v nemateriálové podobě dvě důležité vlastnosti:

- zanechávají digitální stopy, po celou dobu svého životního cyklu;
- lze u nich aplikovat takzvaný systém veřejné kontroly. Typickou ukázkou zavedení systému veřejné kontroly do procesů elektronického úřadování je Informační systém datových schránek i Centrální registr konverzí.

Stěžejní legislativní změny (zákon č.300/2008 Sb. a novela zákona č.499/2009 Sb.) týkající se nakládání s dokumenty v nemateriální digitální podobě vymezují základní prvky:

- zavedení bezpečného, důvěryhodného a právně průkazného přenosového kanálu [1],
- konverze a převod dokumentů[2] ,
- sjednocení požadavků na IS pracující s dokumenty [3],

[1] Zákon č.300/2008 Sb.
[2] Zákon č. 300/2008 Sb.

- právní domněnka pravosti dokumentů v digitální podobě [4],
- sjednocení výstupních datových formátů [5].

Jak je definováno dokument se v digitální podobě považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu měla v době podepsání oprávnění nebo osoby, která byla zodpovědná za převedení z dokumentu v analogové podobě nebo osoby oprávněné provádět autorizovanou konverzi dokumentů, a opatřen kvalifikovaným časovým razítkem. Neprokáže-li se opak[6].

1.2.2 Vyvratitelná domněnka pravosti dokumentu

K 01. 07. 2012 nabyl účinnosti zákon č.167/2012 Sb., který novelizuje zákon č.227/2000 Sb. o elektronickém podpisu a zákon č.499/2004 Sb., o archivnictví a spisové službě. Účinnost také nabyla vyhláška č.212/ 2012 Sb., o postupech pro ověřování platnosti zaručeného elektronického podpisu, a také o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobou. Ani nová vyhláška neřeší největší problém, kterým je existence tzv. vyvratitelné domněnky pravosti. Jedná se o zásadní koncepční rozpor ohledně otázky, jak nakládat s elektronickými dokumenty v dlouhodobém časovém horizontu.

Na jedné straně v důsledku existence vyvratitelné domněnky pravosti postačuje elektronické dokumenty opatřit jednorázově elektronickým podpisem a časovým razítkem na libovolně dlouhou dobu, dokud někdo neprokáže opak.

Na druhé straně je požadována aktivní starost o elektronické dokumenty. Nestačí jednorázové opatření elektronickým podpisem a časovým razítkem. Je nutné elektronické dokumenty pravidelně opatřit dalším časovým razítkem z důvodu zachování možnosti ověření platnosti původního podpisu. Služba ISDS, soubor ZFO- systém zjistí, zda je potřeba časové razítko a přidá jej.

1.2.3 Kvalifikované časové razítko

Časové razítko je typ elektronického podpisu, který obsahuje údaj o čase, na který je možné se spolehnout. Kvalifikované časové razítko je časové razítko, kdy poskytovatel ručí za správnost tohoto časového údaje. Znázorněno na obrázku č. 2. Přítomnost kvalifikovaného

[3] Zákon č. 499/2004 Sb., ve znění pozdějších předpisů
[4] Zákon č. 499/2004 Sb., ve znění pozdějších předpisů
[5] Zákon č.499/2004 Sb., ve znění pozdějších předpisů
[6] §69 a, odstavec 8) zákona 499/2004 Sb., ve znění pozdějších předpisů

časového razítka na dokumentu obsaženého v datové zprávě je nezbytným předpokladem možnosti aplikace domněnky pravosti po celou dobu existence dokumentu. Jejím účelem je právně eliminovat omezenou platnost kvalifikovaného systémového certifikátu vydaného akreditovaným poskytovatelem certifikačních služeb. Na něm je založen zaručený elektronický podpis, respektive elektronická značka. Pravostí je míněno, že dokument se nezměnil od okamžiku, kdy byl opatřen elektronickým podpisem nebo značkou oprávněné osoby a kvalifikovaným časovým razítkem. Není-li tento dokument opatřen těmito náležitostmi, neznamená to, že dokument není pravý. Pouze na něj nelze aplikovat vyvratitelnost domněnky pravosti, tj. je nutno prokazovat jeho pravost, nikoliv nepravost.

Obrázek 2: Podepsání dokumentu poskytovatelem

Zdroj: vlastní zpracování

1.2.4 Kvalifikovaný certifikát

Na kvalifikovaném certifikátu je založen zaručený elektronický podpis, jímž je podepsán dokument obsažený v datové zprávě, pozbude časem platnost. Nemá vliv na platnost zaručeného elektronického podpisu, a tím pádem ani na pravost dokumentu. Totéž platí pro elektronické značky a kvalifikované časové razítko. Z hlediska dlouhodobého ukládání dokumentů v digitální podobě je však nutné opatřovat všechny vlastní dokumenty zaručeným elektronickým podpisem (event. elektronickou značkou), doručené dokumenty kvalifikovaným časovým razítkem. V případě, že došlý dokument, obsažený v datové zprávě není podepsán zaručeným elektronickým podpisem založeným na kvalifikovaném, systémovým certifikátu nebo nemá elektronickou značku založenou na kvalifikovaném, systémovém certifikátu anebo není opatřen kvalifikovaným časovým razítkem musí jej původce označit kvalifikovaným časovým razítkem.

Z výše uvedeného vyplývá, že pro prokazování pravosti dokumentů v digitální podobě po celou dobu jeho existence je důležité opatřovat tyto dokumenty kvalifikovaným časovým razítkem.

U elektronických podpisů je časově omezena možnost ověřit platnost podpisu, což má za důsledek, že elektronický podpis platí stále, i když nejsme schopni ověřit jeho platnost. Časové omezení možnosti ověření a prokázání platnosti podpisu je zcela záměrná a to, kvůli hrozbě kolizních dokumentů. (nahrazením původního dokumentu kolizním dokumentem).

Způsob obrany výše zmiňovaného nebezpečí je postupným přepodepisováním nebo přerazítkováním. Jeho výhody jsou znázorněny v tabulce č. 1. Nové další razítko je potřeba přidat v době, kdy existuje možnost ověření platnosti předchozího časového razítka. Nemalou výhodou je přerazítkování více dokumentů současně.

Tabulka 1: Výhody použití časového razítka

Časové razítko	Elektronický podpis
Nevyjadřuje žádné stanovisko k obsahu a fixuje v čase	Podpis vyjadřuje určité stanovisko, souhlas Nese v sobě údaj o okamžiku svého vzniku. Ten je převzat ze systémových hodin na PC, což samo o sobě není spolehlivé.

Zdroj: vlastní zpracování

1.2.5 Transakční protokol

Jedná se o nástroj pro zaručení záznamů o všech operacích prováděných s dokumenty. V tomto protokolu nesmí být prováděny změny. Je schopen automaticky ukládat údaje o všech operacích učiněných s dokumentem, o uživatelích provádějící operace a zaznamenávat datum a čas operace. Pomocí transakčního protokolu lze zabezpečit neporušitelnost obsahu dokumentu, resp. ihned zjistit jejich porušení. Je-li software pro zabezpečení spisové služby, vedené v elektronické podobě v elektronických systémech spisové služby, schopno zabezpečit funkci transakčního protokolu, pak používání dalších prostředků, jako např. opatřování dokumentů v digitální podobě zaručeným elektronických podpisem nebo časovým razítkem opakovaně vždy poté, kdy ztrácí platnost. Jedná se o double úkony. Z hlediska provozního a finančního je to náročný proces.

1.2.6 Prokazování pravosti a autenticity dat

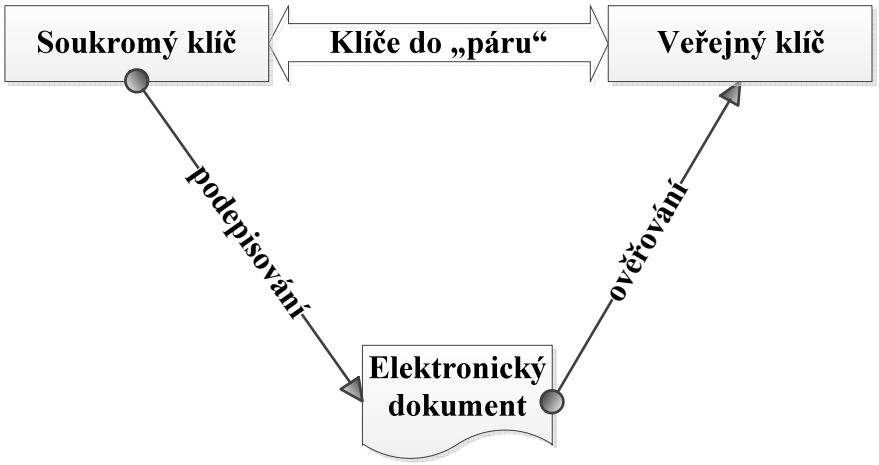
Pravost a autenticita jsou vlastnostmi dokumentu. Nosičem těchto vlastností jsou jiná metadata jednoznačně spojená s původním dokumentem (zaručený elektronický podpis, zaručená elektronická značka, případně časové razítko). Tato metadata mají své vlastnosti, které způsobují, že jejich prokazatelnost v čase zaniká. Hlavním problémem je omezení

platnosti těchto dat (atributů) a prokazování jejich existence zpět v čase. Nabízí se dvě následující řešení:

- řešení založené na organizačních a právních náležitostech. Řešení se opírá o zákonem garantovaný čas a certifikáty. Pro jednotlivce je relativně náročné na technologii, organizaci a finance. Momentální nevýhodou je nízká znalost tohoto řešení mezi uživateli;
- řešení formou centralizace archivační autority. Subjekt, který formou služby poskytuje technologickou platformu, je důvěryhodný. Jeho služby jsou zákonem garantované. Finanční náklady jsou rozprostřeny do jednotlivých cen poskytovaných služeb. Lze řešit odděleně ukládání dat (v rámci organizace) a formou archivační autority pouze prokazování jejich pravosti a autenticity. Návrh infrastruktury pro dlouhodobou archivaci elektronických dokumentů znázorňuje obrázek č. 7 [2.3.4].

1.2.7 Integrita

Základní podmínkou autenticity digitálního dokumentu je zachování jeho integrity. Integrita dokumentu znamená, že dokument je úplný, stálý, neporušený. Pro ověření pravosti je nezbytným úkonem ověření integrity toho, co je podepsán. Elektronický podpis vzniká výpočtem, včetně soukromého klíče. Ověření probíhá komplementárním výpočtem, do kterého je místo soukromého klíče zahrnut naopak odpovídající veřejný klíč, jak je zjednodušeně znázorněno na obrázku č. 3.



Obrázek 3: Ověření integrity

Zdroj: vlastní zpracování, podle [19]

Zachování integrity elektronického dokumentu je podmínka nezbytně nutná. Jestliže je integrita dokumentu narušena, znamená to, že dokument se od podpisu změnil, tudíž se jedná o jiný dokument.

Dalšími nezbytnými úkony pro ověření pravosti je ověření důvěryhodnosti certifikátu a jeho platnosti.

1.2.8 Základní výstupní formáty

Výstupní datové formáty z elektronické spisové služby jsou vymezeny a sjednoceny ve Vyhlášce o podrobnostech výkonu spisové služby §20 191/2009 Sb.

Výstupním datovým formátem metadat, jimiž jsou podle vyhlášky opatřovány dokumenty, se rozumí formát XML podle schématu XML, které je přílohou Národního standardu pro elektronické systémy spisové služby.

1.2.9 Konverze, převod a jiná konverze.

Je-li původci, vykonávajícímu spisovou službu v elektronickém systému spisové služby, doručen dokument v analogové podobě, naloží s ním podle svého spisového řádu nebo jiného vnitřního předpisu, nevydává-li spisový řád. Dokument v analogové podobě, jehož povaha umožňuje převod, zpravidla ho převede do digitální podoby. Pro převod vybere některý z níže uvedených způsobů.

1.2.10 Autorizovaná konverze dokumentů z moci úřední

Autorizovaná konverze dokumentů z moci úřední[7] je provedena v případě, že původce požaduje, aby převedený dokument měl právní náležitosti shodné s prvopisem a je-li možné ji provést. Výsledkem konverze je elektronická kopie s právními účinky prvopisu. Výsledný dokument- elektronická kopie- se použije buďto pro potřeby původce nebo pro komunikaci s dalšími původci nebo jinými fyzickými či právnickými osobami. Zároveň jsou definovány případy, kdy autorizovanou konverzi nelze provést[8].

[7] §22 až §26 zákona č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
[8] §24 odst. (5) zákona 300/2008

1.2.11 Převod dokumentu z analogové podoby do podoby digitální

Převod dokumentu z analogové podoby do podoby digitální bude proveden tehdy, požaduje-li původce, aby převedený dokument měl obdobné právní náležitosti jako prvopis[9]. Výsledkem převodu je ověřená elektronická kopie bez právních účinků prvopisu, zaručující pouhou shodu s prvopisem. Převedený dokument musí obsahovat autentizační prostředky.

1.2.12 Jiná konverze dokumentu

Výsledkem této konverze je neověřená kopie prvopisu a je prováděna zejména pro vnitřní potřebu původce. V předcházejících případech původce označí převedený dokument jednoznačným identifikátorem, jestliže nebyl již označen v analogové podobě. Pouze v případě, že výstup vzniklý jinou konverzí bude zaveden do systému spisové služby, bude dokument vzniklý jinou konverzí opatřen jednoznačným identifikátorem.

V záznamu o dokumentu v evidenci dokumentů se uvede, že dokument vznikl autorizovanou konverzí, převodem nebo jinou konverzí. A to z důvodu ošetření způsobu vzniku dokumentu a jeho právní povahy.

1.2.13 Riziko zneužití - kolizní dokument

Největší riziko spočívá v existenci kolizního dokumentu, cíleně zfalšovaného dokumentu. Je důsledkem způsobu vzniku elektronického podpisu, kdy jím nejsou podepisovány přímo dokumenty, ale pouze jejich otisky (haš). Vstupní digitální dokumenty mají různé velikosti, ale pomocí tzv. hašovací funkce vytvoří otisk pevné délky (128,160x190bitů). Jedná se o normalizaci délky, což usnadňuje návrh celého podpisového schématu. Nejdůležitějším požadavkem na hašovací funkci je bezkoliznost. Najít dvě různé zprávy se stejnými haš kódy musí být výpočetně neschůdné. V případě, kdyby se tak stalo, mohl by útočník tvrdit, že podpis patří zcela jinému dokumentu. Z důvodu neustálého vývoje výpočetní techniky je nutné nepřetržitě zvyšovat složitost výpočtu (hledání kolizních dokumentů) v podobě silnějších hašovacích funkcí.

1.2.14 Technické řešení

Technickým řešením je zabránění, aby původní dokument mohl být nahrazen kolizním dokumentem [19]. Ve skutečnosti se jedná o rozpoznání záměny kolizním dokumentem. Toto rozpoznání probíhá postupným přerazítkováním. Výhoda přerazítkování oproti

[9] § 69a odst. (4) až (7) zákona č.499/2004 Sb.

přepodepisování je viditelná v tabulce č.2 [2.2]. Časová razítka mají možnost jejich ověření záměrně omezená časem (omezená platnost certifikátů) z důvodu hrozby kolizních dokumentů. Časová razítka se musí přizpůsobit vývoji a používat silnější hašovací funkce. Omezení časem má za důsledek, že nové (další) časové razítko se musí použít dříve, než skončí možnost ověření platnosti stávajícího razítka.

K možnosti ověření je potřeba následující:

- otisk (haš) dokumentu- nesmí k němu existovat kolizní dokument,
- elektronický podpis/značku/razítko,
- certifikát, na kterém je podpis založen (obsahuje veřejný klíč, který je nutný k ověření podpisu, musí být platný v daném okamžiku (k posuzovanému okamžiku nesmí končit jeho platnost a k posuzovanému okamžiku nesmí být revokovaný)),
- všechny nadřazené a k danému okamžiku platné certifikáty,
- revokační informace (revokace- předčasné zrušení platnosti certifikátu).

Vyvratitelná domněnka pravosti vede k chybnému postoji, že není nutné se aktivně starat o své elektronické dokumenty. Platnost podpisu v čase nekončí a tato domněnka nechrání před kolizními dokumenty.

2 NAKLÁDÁNÍ S E-DOKUMENTY

e-Dokumenty, dokumenty v elektronické (digitální) podobě řeší přístup k informacím, jejich oběh, nakládání, archivování či dokonce jejich ztrátu. Dokumenty se evidují po celou dobu životního cyklu. Od příjmu až po zničení, nebo předání do archívu, jak je zachyceno v příloze 1.

2.1 Manipulace s e-Dokumenty

Elektronické dokumenty se zrovnoprávňují s papírovými a to ve všech fázích jejich životního cyklu. Elektronická spisová služba zajišťuje příjem dokumentů, přípravu a vyřízení, uložení do negarantovaného úložiště, odesílání a spojování do spisů. Elektronická spisová služba (SSL) hraje významnou roli v e-Governmentu .

Základní funkce systému elektronické spisové služby odpovídají požadavkům legislativy.

Minimální funkce jsou následující:

Příjem a evidence doručených i vlastních dokumentů

- evidence doručených i vlastních listinných dokumentů,
- zobrazení a uschování zpráv doručených do datové schránky a elektronické podatelny,
- označení dokumentů evidenčním číslem a číslem jednacím,
- vedení podacího deníku.

Oběh a vyřizování dokumentů- evidence předání a převzetí

- sledování stavu vyřízení a uzavření dokumentů,
- práce se spisy a uzavírání spisů.

Práce s elektronickými dokumenty- vložení, zobrazení a editace

- ukládání elektronických dokumentů způsobem zaručujícím věrohodnost původu dokumentu, neporušitelnost jeho obsahu a čitelnost dokumentu,
- automatická kontrola a doplňování časových razítek a elektronických značek dle požadavku zákona,
- elektronické podpisy- podepsání souboru, ověření podpisu,

- převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak (neautorizovaná konverze dokumentů),
- integrovaná konverze dokumentů do ukládacího nebo výstupního datového formátu.

Odesílání listinných i elektronických dokumentů

- odesílání dokumentů v listinné podobě (pošta, aj..),
- odesílání dokumentů v elektronické formě elektronickou podatelnou a do datové schránky,
- evidence doručení dokumentu v listinné podobě,
- evidence doručení a data dodání datovou schránkou.

Vyřízení a uzavření spisů a dokumentů

Ukládání a skartace- evidence skartačních znaků a lhůt

Předávání spisů a uzavřených dokumentů do krajské digitální spisovny

2.1.1 Národní standard pro elektronické systémy spisové služby

Evropský standard MOREQ 2 výrazně usnadňuje implementaci e-Governmentu v České republice a usnadňuje komunikaci v rámci zemí EU. Přináší výčet standardizovaných metadat důležitých pro předávání dokumentů v digitální podobě a jejich následnou archivaci. Tento standard má zaručit, že systémy, které jsou s ním v souladu, jsou v celé EU na stejné úrovni. Z evropského standardu vychází Národní standard pro elektronické systémy spisové služby. Vydává ho Ministerstvo vnitra ve svém věstníku [24]. Jeho přílohou je též metadatový model, který stanovuje potřebná metadata pro dlouhodobé a důvěryhodné ukládání dokumentů v digitální podobě. Národní standard pro elektronické systémy spisové služby je určen pro veřejnoprávní původce. Zároveň je určen pro obchodní společnosti, které se zabývají vývojem a aplikací příslušných programových a technologických prostředků, zajišťujících podmínky výkonu spisové služby v elektronické podobě.

K úvodním kapitolám patří hierarchicky strukturovaný spisový plán a organizace spisů. Dokument je zatříděn přímo do věcné skupiny, spisu, součásti nebo dílu.

Z hlediska přístupu k funkcím ERMS jsou definovány 2 hlavní role- uživatelská a správcovská. Potřeba role je proměnná v čase. Správcovské role se člení na 3 úrovně a záleží na velikosti organizace, zda všechny úrovně zvládne jedna osoba:

- ústřední správce- zajišťuje kontrolu nad konfigurací celého ERMS,
- místní správce- má správcovské oprávnění nad části ERMS nebo jeho spisovým plánem,
- posuzovatel skartačních operací je specialista, který odpovídá za provedení procesu výběru archiválií (export a zničení),
- koncový uživatel je standardní rolí v ERMS a jedná se o osoby, které nakládají s dokumenty v ERMS.

O funkčním oprávnění správců rozhodují příslušní vedoucí zaměstnanci.

Další významnou kapitolou je kontrola a bezpečnost. Organizace musí mít zajištěné takové programové vybavení ERMS, které umožní kontrolu povolení přístupu k dokumentům. Dokumenty mohou obsahovat důvěrné informace, obchodní tajemství, osobní údaje. Zároveň musí umět zajistit omezení přístupu pro externí uživatele a sdílení části úložiště ERMS. Pro zajištění přístupu v ERMS může správce nastavit v transakčním protokolu ukládání informací o každém nahlédnutí do dokumentů a jiných činnostech týkajících se těchto dokumentů. Transakční protokol je zápis provedených operací týkajících ERMS. Jedná se o uživatelské operace, operace správců anebo operace automaticky iniciované ERMS na základě parametrů systémů. Transakční protokol umožňuje dohledat, identifikovat, event. rekonstruovat činnost ERMS.

Po kapitole kontrola a bezpečnost následuje kapitola o záloze a obnově. ERMS musí pravidelně zálohovat dokumenty a metadata tak, aby byly neprodleně obnovitelné při jejich ztrátě, při poruše systému nebo narušení bezpečnosti systému.

Tématem kapitoly ukládání a vyřazování dokumentů jsou skartační režimy. Ukládání a vyřazování každého dokumentu se řídí skartačním režimem, přiřazeným k věcné skupině, spisu, součásti, dílu nebo typu dokumentu, do kterých dokument patří, popřípadě platným pozastavením skartační operace. V rámci každého skartačního režimu umožňuje ERMS následující typy skartačních operací:

- trvalé uložení pro dokumenty trvalé hodnoty,
- předložení k přezkumu,
- automatické zničení na základě vydaného trvalého skartačního souhlasu,
- přenos do správního archívu nebo jiného úložiště.

ERMS zajišťuje přesně definovaný proces přenosu dokumentů a jejich metadat a informací transakčního protokolu do jiného systému nebo do jiné organizace. Dokumenty a jejich metadata stanovená metadatovým modelem, který je přílohou národního standardu.

Nedílnou součástí ERMS je funkce vyhledávání a znázorňování spisů a dokumentů. Národní standard definuje požadavky na tyto funkce.

Kapitola Účelové dokumenty řeší dokumenty v analogové podobě.

Organizace vykonávající spisovou službu v ERMS musí vést dokumentaci po dobu svého životního cyklu v analogové podobě.

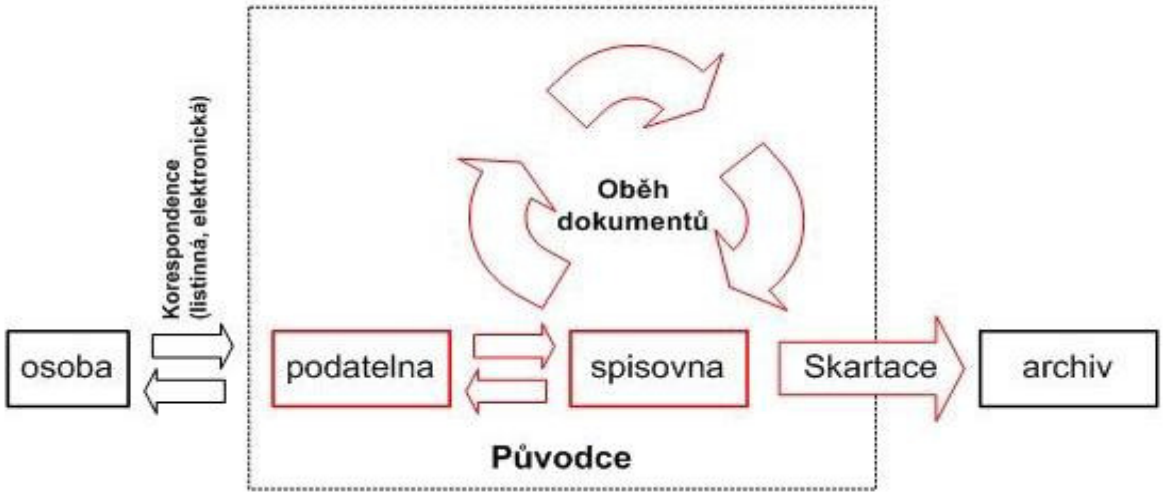
Samostatná kapitola je věnovaná funkčním požadavkům na metadata. Popis metadat stanoví metadatový model, který je přílohou.

Metadatové modely	Metadatový model pro výměnu dokumentů a jejich metadat mezi ERMS.
	Metadatový model pro předávání dokumentů a jejich metadat do archívu.
Schémata XML	Schéma XML pro výměnu dokumentů a jejich metadat mezi ERMS.
	Schéma XML pro předávání dokumentů a je jich metadat do archívu.

2.2 Ukládání dokumentů

Archivaci a dlouhodobé ukládání listinných a elektronických dokumentů musejí zajistit určení původci podle vyhlášky č.191/2009 Sb.

Z pohledu původce je ukládání dokumentů znázorněno na obrázku č. 4.



Obrázek 4: Ukládání dokumentů z pohledu původce

Zdroj: upraveno podle [5]

Ochrana digitálních dokumentů na rozdíl od listinných má jinou, novou podobu. Nosič digitálního dokumentu nemá žádnou nenahraditelnou hodnotu z hlediska informací. Z toho důvodu je možné bez ztráty autenticity oddělit nosič od obsahu a přenést jej na jiný elektronický nosič. Jedná se o uchovávání pouze informací.

Na rozdíl od klasických dokumentů, digitální informace nejsou pro uživatele přístupné přímo. Jsou závislé na informačním prostředí- hardware, software. Adekvátní počítačové konfigurace jsou schopné převést digitální informace do srozumitelné podoby pro uživatele. Problém nastává, že díky rychlému vývoji technologie dochází k zastarávání hardwarových a softwarových systémů. Původní nosiči mohou být v nepoškozeném, zachovalém stavu, ale data na něm uložená nebude možné otevřít v žádném existujícím softwaru. Ukládání dokumentů z pohledu předmětu znázorňuje tabulka č. 2.

Tabulka 2: Ukládání dokumentů z pohledu předmětu

Listinné	Elektronické
Obsah je svázaný s nosičem	Informace, která je předmětem archivace, je nezávislá na nosiči a formátu dat
Existuje originál a kopie	Není možné rozlišit kopii a originál

Vlastnosti dokumentu dokladující jeho pravost a autenticitu mizí s fyzikálními vlastnostmi dokumentu	Pravost a autenticita dokumentu je dána metadaty a jejich virtuálními vlastnostmi
Technologie archivace je technologií uchovávání fyzikálních a chemických vlastností dokumentu	Technologie archivace je technologií zachování čitelnosti dat a schopnosti dokladování virtuálních vlastností dokumentu
Interpretace obsahu archivovaného dokumentu je věcí znalosti lidí o prostředí, ve kterém dokument vznikl	
Archivace listinných dokumentů je obor, který se utváří již stovky let	Archivace elektronických dokumentů není starší než několik desítek let, ale je mnohem dynamičtější a neustálená

Zdroj. [18]

2.2.1 Obecné cíle dlouhodobé ochrany digitálních informací

Dlouhodobá ochrana digitálních informací zahrnuje hledisko ochrany samotného digitálního objektu, tak hledisko ochrany jeho zpřístupnění. Tyto dvě hlediska nelze od sebe oddělit.

Problémy dlouhodobé ochrany digitálních dokumentů se zabývá digitální archivace. Digitální archivace má čtyři obecně definované cíle, které však v reálu nelze vnímat izolovaně.

- uchovávání - jedná se o soustavné zálohování a údržba nejen digitálních dokumentů, ale také přidružených počítačových technologií a datových nosičů;
- zpřístupnění - ochrana zpřístupnění digitálních dokumentů znamená zachování jejich adekvátní reprodukce příslušným softwarem. Každý digitální dokument musí být nejprve zpracován určitou softwarovou aplikací, a až pak je zpřístupněn uživateli;
- srozumitelnost - požadavek srozumitelnosti je stejný jako u analogových dokumentů. Norma OAIS vyžaduje, aby archivované dokumenty byly opatřeny dostatečnou dokumentací [2.2.3]. Ta umožňuje uživatelům, aby jim rozuměli a nemuseli vyhledávat dodatečné informace, které nejsou dostupné. Z dlouhodobého hlediska je náročné stanovit, co by měla taková dokumentace obsahovat;
- dlouhodobý horizont ochrany - dlouhodobý horizont ochrany je parametrem výše uvedených cílů. Časově vymezuje dobu, během níž se technologie nutná pro trvalou ochranu digitálních objektů stane zastaralou. Intervaly zastarávání se mohou nejen

prodlužovat, ale i zkracovat. Proto není vhodné vymezovat dlouhodobou ochranu nějakými konkrétními časovými údaji. Dlouhodobá ochrana musí trvat tak dlouho, jak dlouho je nutné řešit dopady relevantních změn na archivované dokumenty. Relevantní změny jsou nejen technologické změny (nové datové nosiče, nové formáty souborů, atd.), ale i uživatelské změny (vyšší požadavky).

Digitální repozitář je definován jako organizace (lidé a technické systémy), která přebírá zodpovědnost za dlouhodobou ochranu a dostupnost digitálních dat. Na rozdíl od digitálního repozitáře hlavním úkolem digitální knihovny je střednědobá ochrana dokumentů. Teoreticky digitální repozitář funguje jako subsystém digitální knihovny

2.2.2 Problémy dlouhodobé ochrany

Při plnění cílů dlouhodobé ochrany digitálních dokumentů vznikají překážky, které členíme do čtyř rovin.

- **technologická rovina**

  Hlavní problémy vznikají při zachování digitálních informací uložených na elektronických nosičích, zastarávání hardwarových technologií, degradace nosičů, technologická selhání Jedná se o přístup k fyzické vrstvě digitálního objektu.

- **informační rovina**

  Rizika informační roviny se týkají logické a konceptuální vrstvy datového objektu. Jedná se o ochranu reprodukce softwarových aplikací, aby digitální objekty na datových nosičích byly čitelné i později. Jedná se o problematiku formátování-zastaralost, specifikace, vlastnictví formátu, podpora vývoje formátu a robustnost formátu. Z hlediska srozumitelnosti je nutné archivovat všechny informace k datovému objektu, obsah, původ, jeho vztahy s okolím, technické informace, atd.

- **systémová rovina**

  Na systémové rovině se řeší dlouhodobá ochrana fyzické, logické a konceptuální vrstvy digitálních objektů, které jsou soustředěny do strukturovaných celků v digitálních repozitářích. Problém nastává při správě stále rostoucího počtu souborů.

  Datový objekt, který je označen jedinečným identifikátorem se někdy nazývá referentem. Identifikátor je jedinečný v národním, v mnoha případech i v globálním měřítku a zároveň musí být trvalý, bez časového omezení. Identifikátor nejen

jedinečně odkazuje k datovému objektu, ale může plnit i funkci datového lokátoru, což znamená, že zprostředkuje zpřístupnění digitálního dokumentu.

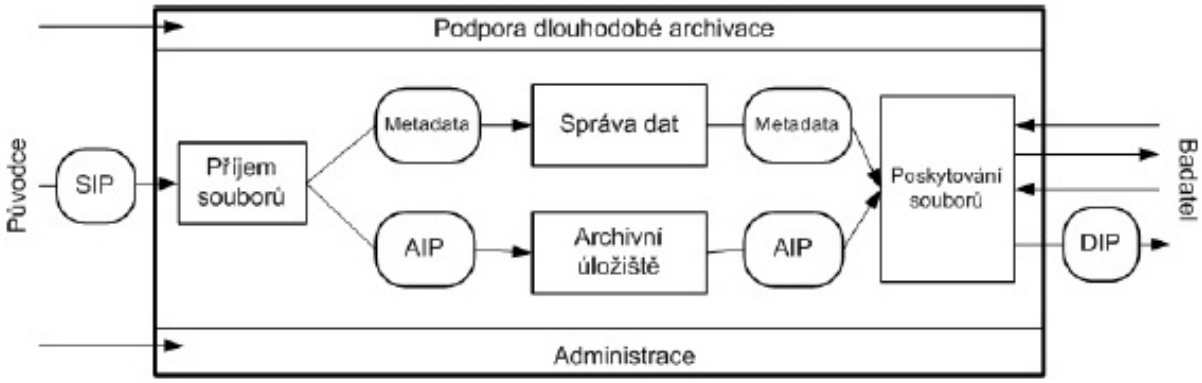
Digitální repozitář zajišťuje nejen ochranu všech vrstev datových objektů, ale také ochranu vztahu mezi digitálními objekty a vlastníky originálů, které digitální objekty reprezentují. Veškerá ochranná opatření prováděna na digitálních dokumentech, jako například kopírování dat, se dotýkají digitálních práv. V digitálních repozitářích jsou prováděny v rámci ochranných opatření změny digitálních objektů, jako například změna konverze souboru z jednoho formátu do druhého. Tyto změny nejsou považovány za narušení integrity.

- **institucionální rovina**

  Institucionální rovina se nezabývá přímo digitálními objekty, ale širším kontextem, ve kterém se digitální repozitář nachází. Příkladem jsou ekonomické faktory, právní otázky, řízení lidských zdrojů., atd. Digitální repozitáře musejí být schopny v širším kontextu svého působení dokázat, že jsou schopni zajistit dlouhodobou ochranu vlastních digitálních objektů.

2.2.3 Uplatnění normy OAIS

Vzhledem k neustálému vývoji technologií se při budování digitálních úložišť zaměřených na dlouhodobé uchovávání digitálních dokumentů vychází ze standardu OAIS (ISO 14721:2003 - Open Archival Information Systém). Tento standard specifikuje základní funkční část otevřeného archivu, komunikaci s okolím, procesy a informační model ve formě informačních balíčků přijímaných, poskytovaných a uložených v repozitáři. Standard definuje hlavní funkce, které má archiv zajišťovat. Jedná se o příjem, správu dat, archivní uložení, přístup, administraci a plánování uchovávání. Referenční model OAIS je na obrázku 5.



Obrázek 5: Referenční model OAIS

Zdroj: [17]

Podle standardu OAIS je elektronický dokument a jeho metadata zabalena do informačních balíčků s jednotnou strukturou a jsou nazývány:

- SIP (Submission Information Package) - balíčky přijímané od původců, vstupní informace předávané do archívu,
- AIP (Archival Information Package) - archivní balíčky zahrnující ukládaný obsah a jeho příslušné popisné informace pro uchovávání – metadata, informace uložené v digitálním archívu,
- DIP (Dissemination Information Package) - balíčky vytvořené na základě badatelského dotazu, pro využívání, informace poskytované z digitálního archívu.

Aby systém zůstal životaschopný, je nezbytné provádět pravidelný dohled nad morálním zastaráváním technického řešení. Je nutné mít připravené takové postupy, aby bylo možné včas obnovit systém. V modelu OAIS se tato služba nazývá „Preservation planning“. Monitoruje vnější prostředí, které může mít dopad na ochranu archívu. Následně služba vytvoří doporučení pro aktualizaci politik a procedur a přizpůsobení změnám.

Původce připraví elektronický dokument vhodný pro předání do archívu, tj. je vytvořen balíček SIP pomocí elektronického systému spisové služby. Balíček obsahuje nejen vlastní dokument, ale i metadata, která se k němu váží. Mezi základní metadata patří původce, identifikátor, datum vzniku, název, spisový plán, obsah, informace na základě čeho je ukládán. Zaslaný SIP balíček je v archivu zkontrolován, zda soubory neobsahují škodlivý kód, formát souborů a rozsah vyplnění metadat. Jestliže balíček obsahuje škodlivý kód, nevhodný formát souborů či neobsahuje požadovaná metadata, je odmítnut a původce je o této skutečnosti informován.

Přijatý balíček je nadále zpracován. V rámci digitálního archivu dokumentu je přidělen jednoznačný identifikátor. Metadata jsou doplněna o podporující procesy řízení uchovávání a zpřístupňování. Výsledkem je archivní informační balíček – AIP (všechna metadata a vlastní digitální soubory). Tento balíček je následně uložen do archivního úložiště s řízeným přístupem.

Nedílnou součástí digitálního archivu je zpřístupnění uložených dokumentů. To probíhá pomocí webového portálu archivu. Uživatel, badatel si pošle požadavek. Ten je následně zpracován - vytvořením DIP balíčku, který bude badateli zobrazen prostřednictvím webového portálu. V závislosti na uživatelském požadavku DIP balíček může v závislosti na uživatelském požadavku obsahovat seznam přístupných dokumentů a jejich náhledy, konkrétní dokument a jeho metadata, informaci o eventuálním omezení přístupnosti dokumentu apod.

Modely normy OAIS nabízí základní rámce pro vytváření konkrétních ochranných opatření digitálních dokumentů. Informační model poskytuje konceptuální základ pro ochranná opatření informační roviny (archivační metadata, formátové strategie). Funkční model poskytuje rámec pro konkrétní implementaci digitálních repozitářů.

2.2.4 Migrace/Emulace

Migrace

Migrace, zjednodušeně řečeno, je metoda přizpůsobení dat prostředí. Nejedná se o pouhé kopírování dat. Migrace se zaměřuje na ochranu kompletního informačního obsahu. Nová archivní implementace informací nahrazuje původní.

Migrace je rozlišována na následující typy:

- renovační migrace - zkopírování archivního balíčku z jednoho datového nosiče na jiný datový nosič stejného typu;
- duplikační migrace - přesunutí je provedeno na stejný nebo nový typ datového nosiče, ale v tomto případě dochází ke změně deskriptivních informací;
- balíčkovací migrace - dochází ke změně balíčkové informace. Cílem balíčkovací migrace je systémová rovina dlouhodobé ochrany;
- transformační migrace - při této migraci dochází ke změně strukturální interpretační informace potřebné k adekvátní reprodukci digitálního objektu.

Výstupem je nový archivní balíček. Transformační migrace může být reverzibilní (př. zabalení souborů do zipového archívu) nebo ireverzibilní (př. formátová migrace).

Tato metoda je použitelná u dat, u kterých není nutné zachovat vlastnosti dokládající pravost a autenticitu dat.

Emulace

Emulace je metoda, která se zabývá obnovováním původního počítačového prostředí, které je již na nových platformách nedostupné. Největším významem emulace je uchování dat na dobu neurčitou a jejich zpětná a bezchybná interpretace. Tato interpretace dat není závislá na žádném konkrétním hardwaru, který také zastarává. Metoda je používána v případě, že spolu s daty jsou ukládány informace nutné pro přizpůsobení prostředí, tzv. metadata.

2.3 Technologická centra

Technologická centra jsou určena k provozu systémů:

- spisových služeb včetně potřebných úložišť,
- projektů Digitalizace a ukládání dokumentů, Digitální mapa veřejné správy a další,
- systémových služeb a dalších aplikací provozovaných pro potřeby samosprávy měst a obcí

Technologická centra mají složku administrativní, technologickou, vzdělávací a jsou nositelem a šiřitelem konceptu e-Governmentu. Z pohledu hierarchie veřejné správy, se eGON centra rozdělují na eGON centra na úrovni obecních úřadů obcí s rozšířenou působností (ORP) a na krajských úřadech.

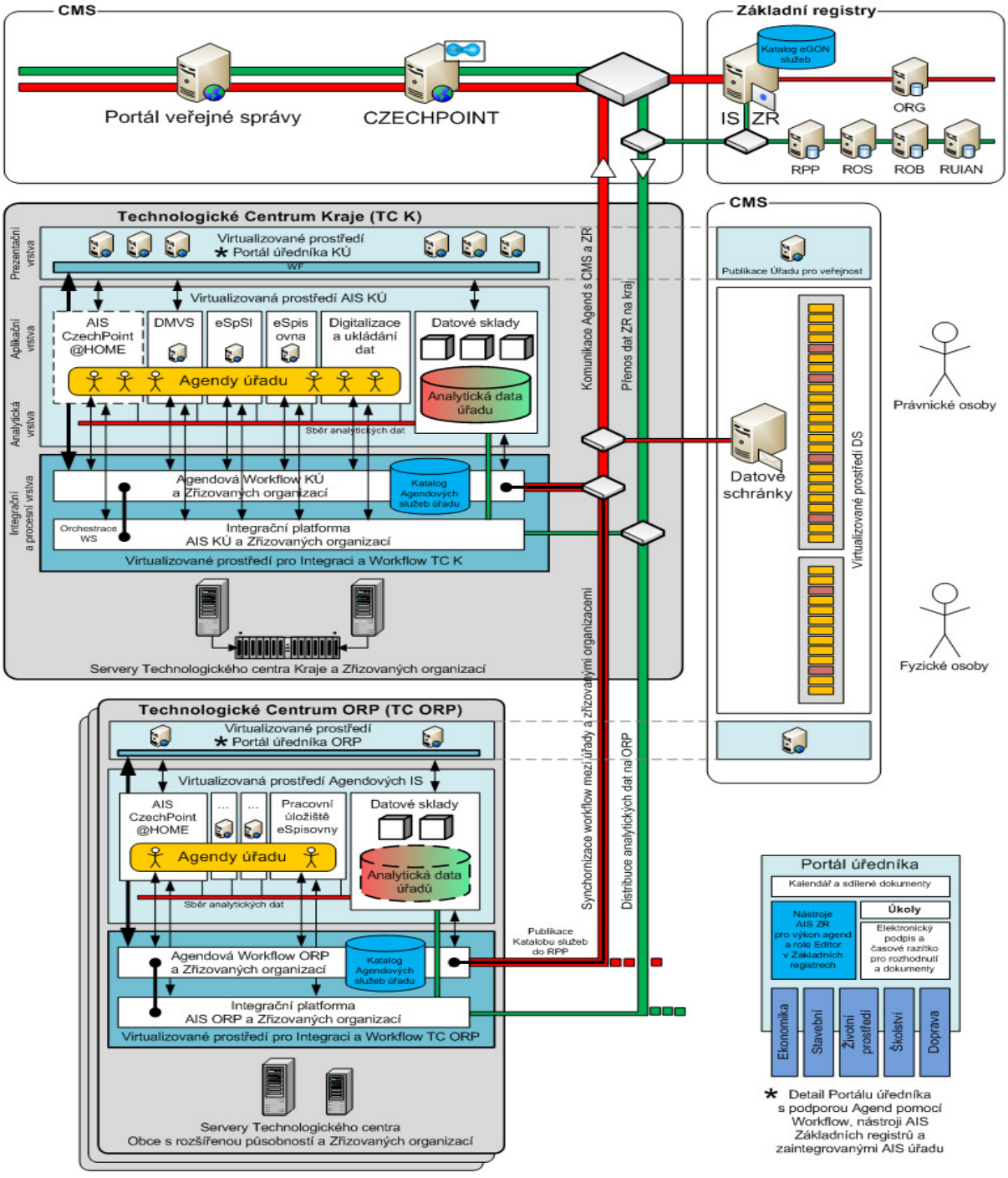
2.3.1 Služby a technologické části TCK

Technologické centra krajů jsou realizovány jako vícevrstvá centra nabízející služby, které jsou podporovány následujícími aktivitami: elektronickou spisovou službou, digitální technickou mapou, účelovou katastrální mapou, nástroji pro tvorbu a údržbu územně analytických podkladů, datovými sklady a nástroji business inteligence, integrací krajského úřadu, digitalizací a ukládáním.

Informační systémy mají obecnou třívrstvou architekturu: datovou (uchovávání dat), aplikační vrstvu (obsahuje aplikační logiky hostujících aplikací) poskytující služby okolí

a klientskou vrstvu (uživatelské rozhraní). Technologické centrum zahrnuje vrstvu datovou a aplikační.

Postavení Technologického centra v systému eGovernment, propojeno s infrastrukturou KIVS zachycuje obrázek 6.



Obrázek 6 Propojení postavení Technologického centra v systému eGovernmentu s infrastrukturou KIVS

Zdroj: převzato [16]

2.3.2 Garantované/ negarantované úložiště

Negarantované úložiště je určeno pro ukládání nevyřízených a neuzavřených spisů a dokumentů elektronické spisové služby. Velikost negarantovaného úložiště je závislá na typu spisové služby, počtu organizací kraje a množství zpracovávaných dokumentů. Jeho odhadovaná velikost je 3 TB. Po uzavření jsou spisy přesouvány ve formě datového balíčku (SIP) do garantovaného úložiště, do krajské digitální spisovny. Uzavřený dokument se již nesmí měnit. Dokumenty v listinné podobě se ukládají v listinných spisovnách. Po uplynutí skartační lhůty jsou digitální archiválie předávány do digitálního archivu (NDA).

2.3.3 Digitalizace a ukládání dokumentů na úrovni kraje

Proces digitalizace a ukládání dokumentů je zajišťován hw komponentami Technologického centra kraje. Cílem procesu je zabezpečení digitalizovaných dokumentů historického významu pro neomezenou dobu, usnadnění přístupu k nim a nahrazení fyzických podkladů.

Nástroji digitalizace a ukládání dat na území kraje jsou zejména:

- krajská digitalizační jednotka- technologie- skenery, další hw, sw pro řízení pro historické a úřední dokumenty,
- krajská elektronická spisovna (KDS) – uložení úředních dokumentů a spisů vzniklých jako produkt činnosti původců,
- krajský digitální repozitář (KDR)- uložení dokumentů z oblasti kulturního dědictví regionu a které nevznikly jako produkt činnosti původců,
- krajské digitální úložiště (KDU)- uložení dokumentů a dat vycházející z činnosti informačních systémů veřejné správy. Tyto dokumenty je třeba střednědobě až dlouhodobě uchovávat (zdravotní dokumentace, geodata, apod.).

V současnosti vzniká častěji řada dokumentů v elektronické podobě u původců (evidence, obrazové a zvukové záznamy, a zároveň je prováděna digitalizace stávajících fyzických dokumentů z důvodu zpřístupnění věrné podoby uložených archiválií uživatelům a z důvodu, že původní dokumenty dožívají.

Je-li dokument hotový, tzn. jakékoliv jeho další změny jsou nežádoucí, je zafixován jako neměnný. Problematika střednědobého a dlouhodobého ukládání se zabývá právě touto fází.

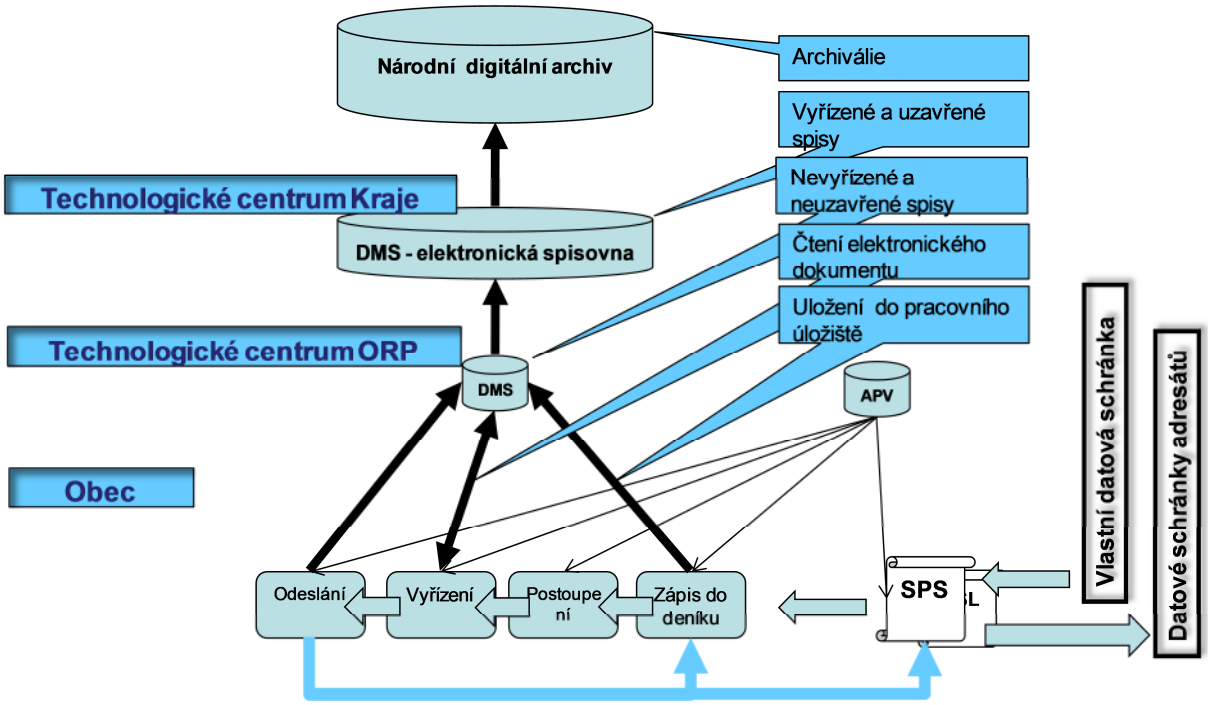
V případě jiných dat je tento moment při vyexportování z jejich provozního systému I v tomto případě je třeba, aby ukládaný obsah zůstal neměnný.

Dokumenty celonárodního významu jsou ukládány v Národní digitální knihovně, popř. NDA- Národním digitálním archívu. Digitalizace dokumentů regionálního charakteru se týká zpracování dat pro potřeby správného fungování úřadů, záchrana, ochrana a zpřístupnění dokumentů z oblasti knižních fondů, stavebních spisoven, zdravotnických spisoven nebo dokumentů významných svým obsahem či původem. Dokumenty regionálního významu se archivují do Krajského digitálního repozitáře.

2.3.4 Ukládání úředních dokumentů na úrovni kraje

Krajská digitální spisovna (KDS) zajišťuje správu úředních dokumentů na úrovni kraje. Z právního hlediska je správa úředních dokumentů stanovena především podle zákona č.499/2004 Sb. ve znění pozdějších předpis a, Národního standardu pro elektronické systémy spisové služby. KDS zajišťuje správu úředních dokumentů od uzavření dokumentů do skartace či vyřazení do Národního digitálního archívu. Uzavřený dokument se nesmí již měnit. Má již přiřazena metadata- věcnou skupinu a skartační režim dle spisového plánu ERMS původce.

Propojení elektronických spisových služeb, Krajské digitální spisovny a Národního digitálního archívu vyjadřuje následující obrázek 7.



Obrázek 7: Návrh infrastruktury pro dlouhodobou archivaci elektronických dokumentů

Zdroj: zpracováno podle [17]

2.3.5 Ukládání dokumentů kulturního dědictví na úrovni kraje

Kromě dokumentů úředního významu[10] je řada dokumentů, které nemají úřední charakter. Jedná se o kulturní památky, cenné písemnosti a umělecká díla, fotografie, historické mapy, audio, video, časopisy a ostatní publikace týkající se určitého regionu. Na úrovni kraje jsou výše zmiňované dokumenty ukládány v Krajském digitálním repozitáři (KDR). Přesněji se jedná o následující dokumenty- dokumenty, cenné písemnosti, umělecká díla a vybrané knihovní fondy spravované Krajskou knihovnou a dalšími krajem nebo obcemi, zřizovanými paměťovými institucemi- knihovnami, muzei, archivy:

- historické dokumenty a cenné písemnosti vzniklé činnosti nebo spravované školami a vědeckými institucemi,
- 3D digitalizované vybrané kulturní památky,
- historické dokumenty a cenné písemnosti vzniklé z činností náboženských obcí a kongregací,
- dokumenty vytvořené soukromými osobami,
- webové stránky regionálního významu vytvořené libovolnými původci,

[10] Zákon č.499/2004 Sb., ve znění pozdějších předpisů

- data uložená na pevných nosičích.

Do KDR se dostávají elektronické dokumenty spolu se svými metadaty v podobě SIP balíčků. Tyto balíčky vytvářejí z dodaných datových souborů archiváři KDR nebo původci, které mají uživatelské rozhraní KDR, které jim umožňuje tvorbu těchto balíčků. Krajská knihovna příslušného kraje je jeden z nejvýznamnějších původců KDR, který digitalizuje kulturní dědictví regionálního významu z knihoven v regionu kraje. Má také vzdálený přístup do KDR . Může vytvářet fondy či sbírky a dle potřeby upravovat metadata.

Po vstupním zpracování dokumentů je pro jeho jednoznačnou identifikaci přiřazen jednoznačný identifikátor vygenerovaný systémem správy dat KDR. Tento identifikátor spolu s ostatními metadaty a samotným dokumentem je uložen do archivního informačního balíčku AIP. Pro vyhledávání dokumentů uživateli se používají metadata, která jsou koncipována dle následujících standardů:

- standard metadat stanovený Národní knihovnou pro knihovní systémy,
- možné vazby na číselníky stanovené Národní knihovnou,
- základní archivní metadata používaná při budování archivních fondů a sbírek,
- standardy používaných v muzejnictví.

Povolené formáty elektronických dokumentů pro uložení v KDR jsou obdobné jako formáty pro KDS.

2.3.6 Ukládání obecně nespecifikovaných dat

Předem nespecifikována data jsou ukládána v Krajském digitálním úložišti (KDU). Zdrojem těchto dat jsou různé informační systémy různých původců. Úložiště neslouží pro přímé ukládání provozních dat původců, ale pro dlouhodobé uložení výstupních dat Vnitřní struktura uložených dat a manipulace s nimi se týká uživatele/původce. Provozovatel KDU řeší vlastní uložení dat, jejich dostupnost a zálohování sjednané s uživatelem.

Mezi KDS a KDR existují rozdíly ve funkčnosti:

V systému KDR se používají standardy a metadata stanovena Národní knihovnou, event. další sjednané s původci. V systému KDS je aplikován Národní standard pro elektronické systémy spisové služby, který je definován MV ČR. V rámci tohoto standardu je použito schéma pro předávání dokumentů a jejich metadat do archivu. Souborové formáty jsou definované ve vyhlášce č.191/2009 Sb. MV. V KDR mohou být formáty navíc dohodnuty

s původci. Liší se také v použití archivního úložiště (CAS/NAS). V některých případech s krátkou skartační lhůtou v systému KDS je používáno úložiště typu NAS.

V KDR je prováděno pouze interní skartační řízení, v KDS zákonné skartační řízení. V KDS musí probíhat opakovaná obnova časových razítek. Rozdíl je také v odlišném nastavení přístupových oprávnění. V KDS je správa obsahu uložených dat delegována na pověřené správce původce. V KDR tuto správu neprovádí přímo pracovník původce. Pro přístup k dokumentům v KD je třeba mít nastavené politiky (obecně přístupné, autorizované). Datové balíčky v KDS jsou přístupné pouze omezené množině autorizovaných uživatelů, datové balíčky v KDR jsou přístupné větší množině uživatelů.

Systém KDÚ slouží k rychlému, přímému ukládání dat po dohodě s původci. Data jsou uložena ve formě souborů a neobsahují popisná metadata v jednotném formátu. Tento systém zajišťuje spolehlivé uložení a zálohování obsahu datových souborů. Systém KDÚ je rozdělen na jednotlivé logické segmenty úložiště. Tyto segmenty jsou definovány v katalogu KDÚ a na jejich základě je vytvořena logická (adresářová) struktura úložiště. Každý segment má definován typ ukládaných dat, formát datových souborů, ukládací politika, původce datových souborů a přístupová pravidla.

3 NORMY

3.1 ISO 15489

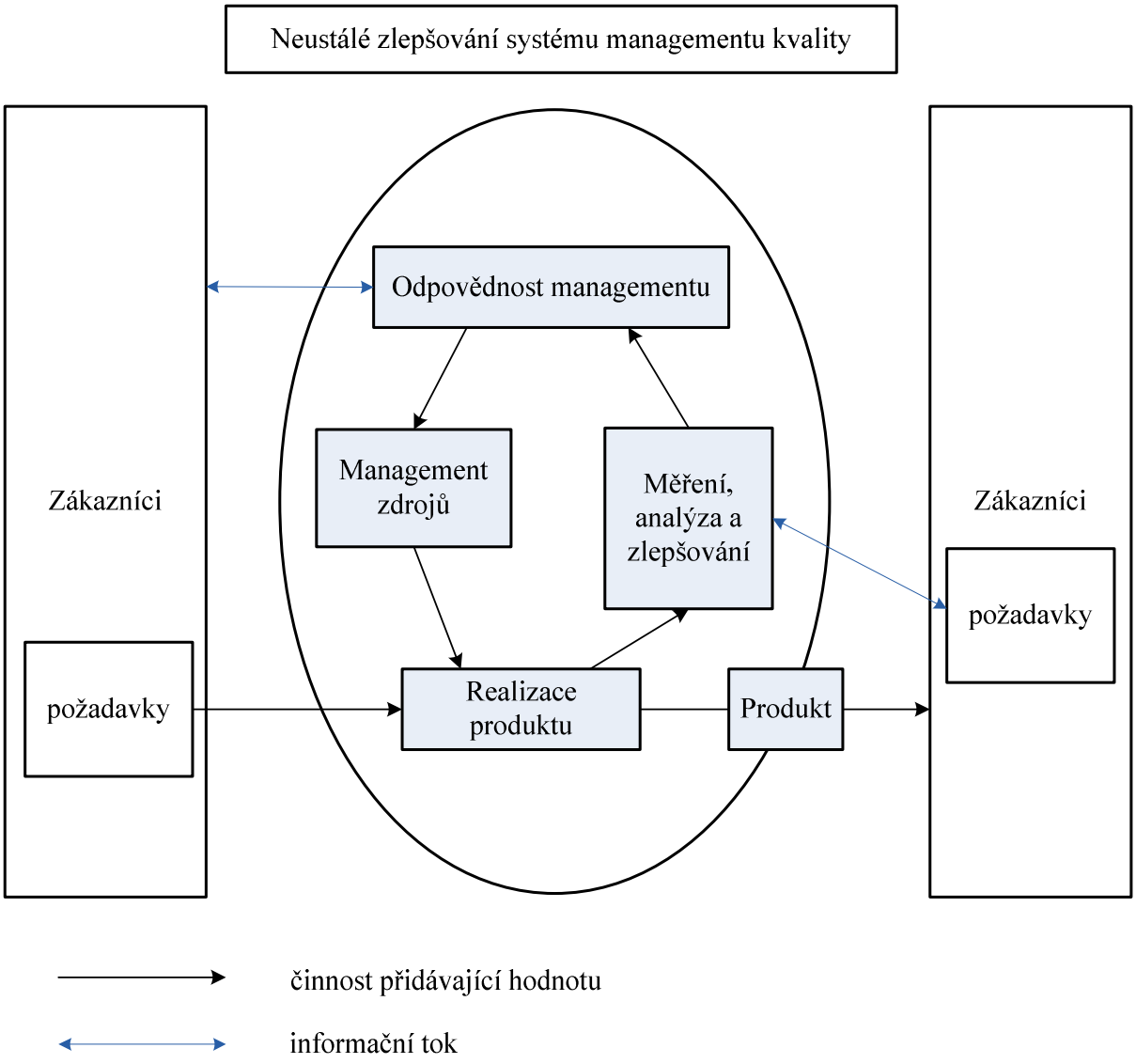
Mezinárodním standardem pro správu informací a dokumentů je ISO 15489:2001 Information and Documentation- Records Management (Správa informací a dokumentů- spisová služba). Norma se zabývá nastavením metodiky řešení spisové služby, řízení procesů, ukládání výstupů a využívání systémů řízení spisové služby. Norma má dvě části- mezinárodní normu ISO 15489-1:2001 Information and Documentation – Records management Part 1: General a technickou zprávu ISO/TR 15489-2 Information and Documentation- Records management- Part 2: Guidelines. Aplikace této normy napomáhá organizaci s nastavením vhodné struktury řízení dokumentů, záznamů a jejich obsahu.

ISO 15489 se vztahuje na správu dokumentů, ve všech formátech a prostředích, vytvořených veřejnou nebo soukromou organizací. Norma zdůrazňuje spisový plán, stanovení odpovědností a doložitelnosti činnosti subjektu. Platí jak pro analogové, tak digitální dokumenty. Nevztahuje se na správu archiválii v archivních institucích. Požadavky normy platí pro dokumenty do dovršení skartační lhůty výběru k trvalému uložení.

Z normy ISO15489 vychází doporučení MoReq (modelové požadavky na správu elektronických dokumentů spisové služby [2.1.1]. Cílem normy je standardizace postupu a procedur při správě dokumentů a zároveň efektivnější získávání informací z těchto dokumentů.

3.2 ISO 9001:2008

Norma ISO 9001 vydaná v ČR jako ČSN EN ISO 9001:2009 řeší systém managementu kvality procesním přístupem. Mezi základní požadavky patří i neustálé zlepšování a spokojenost zákazníka Pomáhá organizaci identifikovat a uspořádat všechny činnosti v organizaci, stanovit jasné pravomoci a odpovědnosti za řízení těchto činností a přispívá k celkovému zprůhlednění fungování organizace. Tato norma podporuje používání procesního přístupu při vytváření, implementaci a zvyšování efektivnosti systému managementu kvality s cílem zvyšování spokojenosti zákazníka prostřednictvím plnění jeho požadavků. Koloběh zlepšování kvality znázorňuje obrázek č. 8.



Obrázek 8: Koloběh neustálého zlepšování systému kvality

Zdroj: upraveno podle [14]

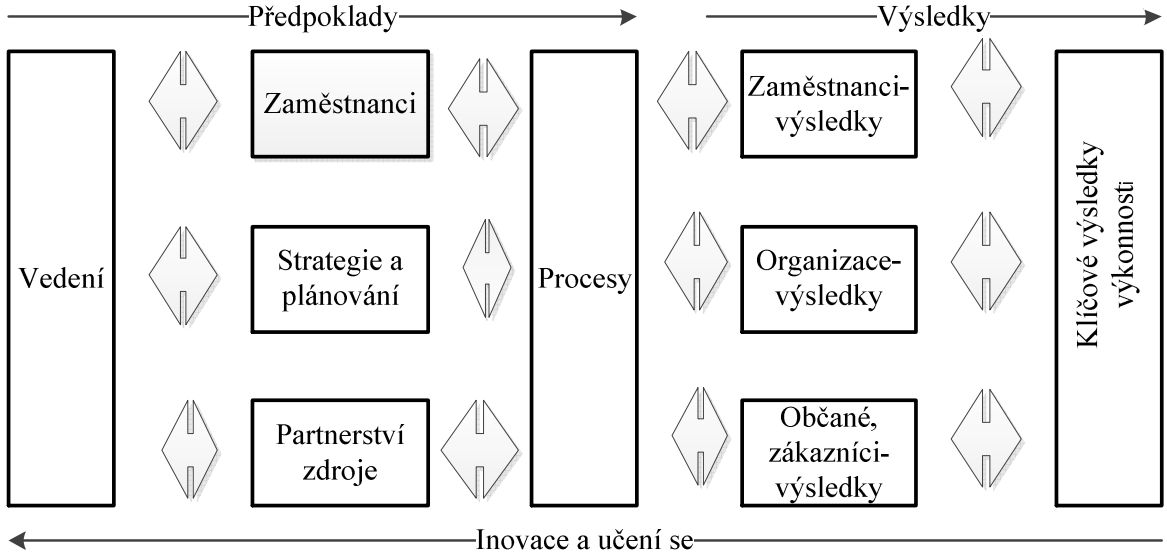
Návrh a implementace systému managementu kvality organizace jsou ovlivňovány prostředím, ve kterém organizace pracuje, jejími konkrétními cíli, poskytovanými produkty, používanými procesy, velikostí a strukturou organice. Organizace musí v souladu s požadavky této mezinárodní normy určovat kritéria a metody potřebné pro zajištění efektivního fungování s řízení těchto procesů. Má-li každá činnost vstup a výstup a využívá zdroje, jedná se o proces. Správa dokumentů lze chápat jako pomocný proces.

Tato norma je aplikována především v komerčních firmách. Činnost veřejné správy je podchycena legislativou.

3.3 Společný hodnotící rámec (Model CAF) ve veřejné správě

Společný hodnotící rámec je univerzální metodickou příručkou pro zlepšování organizací veřejného sektoru pomocí sebehodnocení. Jedná se o uznávaný a respektovaný model zvyšování kvality ve veřejném sektoru v České republice. Vychází z předpokladu, že výkonnost organizace, ve vztahu ke společnostem, občanům, ale i ke svým zaměstnancům jsou dosahovány na základě řízené strategie a plánování s pomocí zaměstnanců, využíváním partnerství, zdrojů a procesů.

Model CAF je znázorněn na následujícím obrázku č. 9.



Obrázek 9 Struktura modelu CAF

Zdroj: vlastní zpracování podle [2]

Struktura modelu CAF má devět kritérii identifikující hlavní aspekty při tvorbě analýzy organizace. Prvních pět kritérií se zabývá charakteristikami předpokladů organizace. Ty určují činnost organizace, jakým způsobem je dosaženo požadovaných výsledků. U kritérií 6-9 se měří výsledky dosažené v oblasti občané- zákazníci, zaměstnanci vůči společnosti a výsledky klíčových činností organizaci. Jedním nejdůležitějším výstupem sebehodnocení je identifikace silných stránek a oblastí pro zlepšení. Cílem použití modelu CAF v organizaci je získání informací, správné nasměrování zlepšení, měření dosaženého pokroku, získávání spolehlivých partnerů- forma benchmarking (učení se dané organizace od jiné navzájem). Na základě sebehodnotící zprávy a zprávy nezávislého hodnotitele je vhodné ze skupiny oblastí

ke zlepšení vybrat takové priority, kterými se organizace bude zabývat. Platí, že 20% faktorů jsou příčinou 80% následků. Právě řešením těchto příčin vede k nejlepšímu zlepšení.

V roce 2005 vznikl Mezikrajský benchlearningový (CAF) projekt, jehož cílem je zefektivnění procesů uvnitř úřadu a poskytování kvalitnějších služeb veřejnosti formou spolupráce mezi krajskými úřady.

Model CAF úzce souvisí s principy mezinárodní kriteriální normy stanovující požadavky na systém řízení kvality, zejména se zaměřením na efektivnost systému řízení kvality při plnění požadavků zákazníka, ISO 9001.

4 NÁVRH KRITÉRIÍ KVALITY E-DOKUMENTU

4.1 Kategorizace e-Dokumentu

4.1.1 Životní cyklus e-dokumentu

Původci zajišťují příjem dokumentu, opatří jej jednoznačným identifikátorem, čímž je zajištěna jeho nezaměnitelnost. Zároveň se tyto dokumenty s jednoznačným identifikátorem zaevidují. Při vyřizování dokumentů se všechny dokumenty týkající se stejné věci zkompletují ve spis. Dokumenty v analogové podobě se spojí fyzicky, v digitální podobě se vzájemně spojí pomocí metadat a při vzájemném spojení analogového a digitálního dokumentu se použijí odkazy. Po vyřízení věci se spis uzavře, dokumenty v digitální podobě se převedou do výstupního datového formátu, provede se kontrola a následně jsou uloženy do spisovny. Dokumenty jsou označeny spisovými znaky, skartačními znaky a skartačními lhůtami podle spisového a skartačního plánu. Po dobu skartační lhůty jsou vyřízené spisy uloženy ve spisovně

Doručený dokument v digitální podobě musí být opatřen uznávaným elektronickým podpisem, elektronickou značkou nebo kvalifikovaným časovým razítkem. Musí být vždy zkontrolován, neobsahuje-li chybný datový formát nebo počítačový program způsobilý přivodit škodu na programovém vybavení původce nebo není-li způsobilý poškodit původce zneužitím informací (dále jen„ škodlivý kód“). Pokud je škodlivý kód zjištěn, dokument v digitální podobě, který obsahuje chybný datový formát nebo který obsahuje informaci, kterou původce může bezpečně využít ve vztahu k dalšímu zpracování dokumentu a lze jej bezpečně uložit mimo elektronickou podatelnu, původce uloží dokument na zvláštní úložiště. Ostatní dokumenty se škodlivým kódem jsou původcem zničeny. V takovém případě je dokument v digitální podobě považován za nedoručený. Při uchovávaní dokumentu v digitální podobě musí být zaručena věrohodnost původu dokumentu, neporušitelnost jeho obsahu a čitelnost dokumentu, a to včetně údajů prokazujících existenci dokumentu v digitální podobě čase. Uvedené vlastnosti musí být zachovány po dobu skartační lhůty dokumentu. V rámci životního cyklu e-dokumentu ve veřejné správě lze definovat několik kategorií e-dokumentů [2.1]:

4.1.2 Kategorizace e-dokumentů v rámci životního cyklu

Podle původu se rozdělují digitální dokumenty do tří skupin:

- digitalizované dokumenty vznikly digitalizací analogových dokumentů. Z dlouhodobého hlediska mají výhodu, že mají analogový protějšek;
- výhradně digitální dokumenty nemají žádný analogový ekvivalent;
- elektronické archiválie digitální dokumenty, které vzniky v rámci každodenního chodu organizací, mají formální status a jsou stanoveny legislativou.

Z hlediska zdrojů se rozlišují digitální dokumenty na dvě kategorie

- dokumenty vzniklé z externích zdrojů jsou doručeny různými komunikačními kanály:

  elektronickou poštou,

  datovou schránkou,

  faxem,

  poštou,

  osobně,

- dokumenty vzniklé z interních zdrojů vznikají v rámci pracovní činnosti organizace,

Dokumenty jsou vytvořeny různými autory, které je možné rozdělit následovně:

- fyzické osoby,
- podnikající fyzické osoby,
- právnické osoby,
- orgány veřejné moci, tím se rozumí státní orgány, orgány územních samosprávných celků, Pozemkový fond České republiky i jiné státní fondy, zdravotní pojišťovny, Český rozhlas, Česká televize, samosprávné komory zřízené zákonem, notáři a soudní exekutoři.

Odesílatel dokumentu může, ale nemusí znát konkrétního adresáta, jmenovitě zaměstnance organizace, který jeho dokument bude vyřizovat. Z tohoto důvodu rozlišíme digitální dokumenty podle adresáta:

- univerzální dokument je zaslán příjemci, organizaci na centrální adresu,
- individuální dokument je nasměrován přímo ke konkrétnímu zaměstnanci organizace.

Na digitální dokumenty jsou kladeny různé požadavky na uchovávání:

- krátkodobé uložení,
- střednědobé uložení,
- dlouhodobé uložení v přípravě digitálních dokumentů pro dlouhodobé uložení je třeba počítat s vyššími náklady. Minimálně je třeba k dokumentům připojit příslušná metadata (popisná, technická a administrativní). Vše zabalit do balíčků vhodných archivaci. Pro některá data mohou být náklady na jejich převedení do podoby vhodné pro dlouhodobé uložení natolik vysoké, že doposud neexistují vhodné metody pro tento převod. Jedná se například uložení složitých databázových aplikací, které vyžaduje uložení vlastních dat i dlouhodobé uložení aplikačního software. Z tohoto důvodu je problematika ukládání dat rozdělena na dvě části:
- dlouhodobé ukládání dokumentů,
- bezpečné dlouhodobé ukládání dat.

Druh záznamů určí typ dokumentu smlouvy, životopisy, námitky, stížnosti, atd.

Hledisko významu dokumentu vytvoří čtyři kategorie dokumentů [2.3.3]:

- úřední dokumenty vytvořené původci,
- dokumenty kulturního dědictví celonárodního významu,
- dokumenty kulturního dědictví regionálního významu,
- ostatní data z provozních informačních systémů.

4.1.3 Životní cyklus digitálních dokumentů na krajském úřadu

Mezi orgány veřejné správy patří krajské úřady. Kraje jsou vyšší územní samosprávní celky. Krajské úřady plní úkoly v samostatné působnosti a v rámci přenesené působnosti stanovenou státní správu.

Na základě § 69 odst. 2 písm. f) zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů byl vydán Spisový a skartační řád Krajského úřadu Královehradeckého kraje[13], který řeší:

- chod spisové služby a postup při vyřazování dokumentů u Krajského úřadu Královehradeckého kraje. Podle tohoto spisového a skartačního řádu postupují přiměřeným způsobem i ostatní orgány kraje,
- účelem spisového a skartačního řádu je zajistit vedení spisové služby jednotně, racionálně a tak, aby zabezpečovala potřebnou evidenci o dokumentech, které byly úřadu doručeny nebo vzešly z jeho činnosti, zajistit správnou manipulaci s nimi, uchování a vyřazování nepotřebných dokumentů,
- manipulaci s dokumenty u úřadu provádějí podatelna a zaměstnanci jednotlivých oborů úřadu.

Příjem a evidence dokumentů

Veškeré dokumenty došlé, ale i vzniklé z vlastní činnosti úřadu, jsou evidovány v elektronickém podacím deníku. Ten obsahuje základní údaje (evidenční číslo, číslo jednací, věc, druh zásilky, datum odeslání, .., způsob vypravení, čas, spisový znak, skartační znak a skartační lhůtu.). Dokumenty se přijímají na podatelně úřadu, která zajišťuje i úkoly výpravny. Podatelna se nachází v budově úřadu, Pivovarské náměstí 12445, 500 03 Hradec Králové, č. dv. P1.1013. Za příjem dokumentů doručených mimo podatelnu je zodpovědný příjemce. Ten je zároveň povinen dokument předat k evidenci na podatelně.

Doručené datové zprávy se ukládají do uložiště doručených zpráv a ve tvaru, ve kterém byla přijata. Je-li k datové zprávě připojen kvalifikovaný certifikát a zaručený elektronický podpis nebo kvalifikovaný systémový certifikát a uznávaná elektronická značka ukládají se spolu se zprávou. Doručená datová zpráva určená k zaevidování se v elektronické podatelně zaeviduje, zároveň se označí identifikátorem elektronické podatelny, který má charakter podacího razítka. Spisový a skartační řád Krajského úřadu Královehradeckého kraje rozlišuje také, zda se jedná dokumenty prezidiální (tj. dokumenty adresované hejtmanovi, náměstkům

hejtmana, radním, řediteli krajského úřadu) nebo dokumenty označené stupněm utajení, podléhají zvláštnímu režimu, samostatné evidenci.

Elektronická podatelna Krajského úřadu Královehradeckého kraje

Adresa elektronické podatelny je posta@kr-kralovehradecky.cz. Adresa pro osobní a poštovní přijímání datových zpráv na technických nosičích je Krajský úřad Královehradeckého kraje, podatelna, Pivovarské náměstí 1245, 500 03 Hradec Králové.

Technické parametry přijímaných datových zpráv jsou následující: datové zprávy ve formátech HTML, PDF, DOC, JPG, RTF, případně dalších běžně používaných formátech datových zpráv. Technické parametry fyzických nosičů, na nichž lze předávat datové zprávy jsou disketa 1.44 MB se souborovým systémem FAT 16 (3,5 palce) a CD se souborovým systémem ISO9660. Datová zpráva, u které byl zjištěn škodlivý software nebo chybný formát, případně nevyžádané obchodní sdělení (spam), není zpracovávána.

Spisový a skartační řád Krajského úřadu Královehradeckého kraje řeší právní předpisy, podle kterých je možné vůči úřadu činit právní úkony v elektronické podobě a náležitosti těchto úkonů. Jedná se o žádost o poskytnutí informace[11], podání učiněné v elektronické podobě[12], návrhy, připomínky, podněty, stížnosti[13], atd.

Rozdělování a oběh dokumentů

Pověřený zaměstnanec útvaru si vyzvedne dokumenty na podatelně. Zároveň provede kontrolu. Nepřevzaté dokumenty přidělí vedoucí útvaru.

Vyřizování dokumentů

Každý útvar úřadu si vede samostatný podací deník. Každý zaměstnanec si odpovídá za jemu přidělené dokumenty a za jejich řádnou evidenci v elektronickém podacím deníku. K dokumentu v digitální podobě připojuje pověřený zaměstnanec zaručený elektronický podpis.

[11] Zákon č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
[12] Zákon č.500/2004 Sb., správní řád, ve znění zákona č.413/2005 Sb.
[13] Zákon č.129/2000 Sb., o krajích (krajské zařízení), ve znění pozdějších předpisů

Odesílání dokumentů

Dokumenty jsou odesílány podle své závažnosti podatelnou nebo přímo z konkrétního útvaru: poštou obyčejnou/doporučenou/do vlastních rukou, kurýrní službou, telekomunikačními prostředky, elektronickou poštou

Ukládání dokumentů

Vyřízené dokumenty jsou ve stanoveném termínu předávány do centrální spisovny. V centrální spisovně jsou všechny vyřízené dokumenty uloženy do doby uplynutí jejich skartačních lhůt a provedení skartačního řízení.

Skartace archiválie

Krajský úřad královehradeckého kraje spadá územně pod Státní oblastní archiv v Zámrsku. Tento archiv provádí kontrolu plnění povinností na úseku spisové služby, provádí výběr archiválií ve skartačním řízení. Za provádění skartačního řízení odpovídá oddělení vnitřní správy. Na základě předloženého skartačního návrhu provede pověřený zaměstnanec příslušného archivu odbornou archivní prohlídku dokumentů a v dojednaném termínu dokumenty, vybrané jako archiválie k trvalému uložení, převezme.

Další část této práce se zaměří na kategorii e-dokumentů digitální dokumenty z externích zdrojů, které jsou doručené elektronickou poštou.

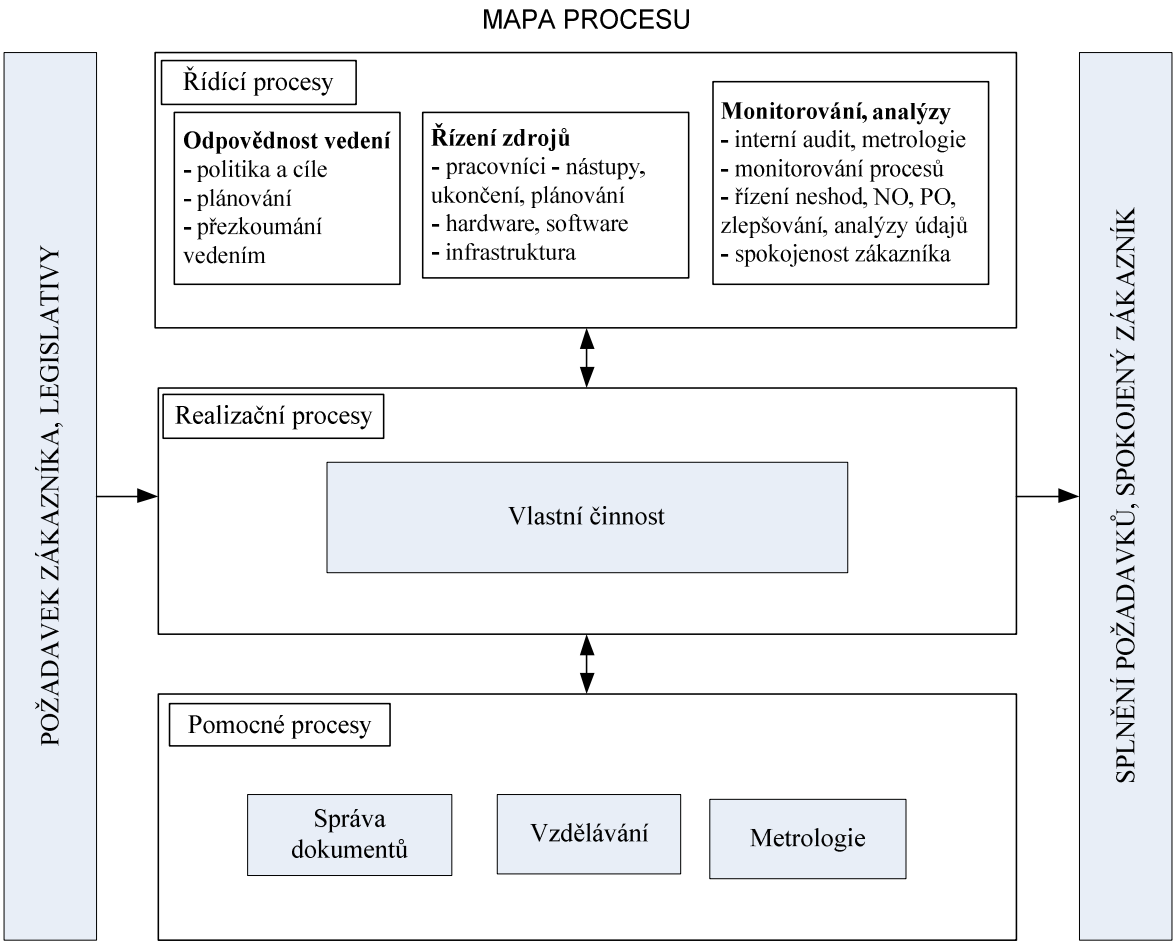
4.2 Předpoklady pro kvalitu e-Dokumentu

Předpoklady pro kvalitu e-dokumentů jsou stanoveny pro digitální dokumenty z externích zdrojů přijatých elektronickou podatelnou

4.2.1 Inspirace v Systému managementu kvality ISO 9001 komerční sféry

V každé organizaci lze definovat a rozlišit řídící, realizační a pomocné procesy. Manipulace a uchovávání dokumentů lze považovat za pomocný proces, jak je znázorněno na obrázku č.10.

Kvalita procesů je ovlivňována konkrétními cíli organizace, kdy jedním měřítkem kvality je nárůst či pokles výkonnosti organizace nebo nákladovost jednotlivých procesů [3.2].



Obrázek 10: Mapa procesů

Zdroj: vlastní zpracování podle[14]

4.2.2 Šetření na krajském úřadu

Rizikem elektronického systému spisové služby je lidský aspekt. V důsledku toho může být jedním problematickým místem příjem digitálních dokumentů doručených na elektronickou podatelnu a následné přiřazení jednotlivým složkám úřadu k vyřízení.

4.2.3 Návrh měřitelných ukazatelů pro stanovení kvality e-Dokumentu

U kategorie e-dokumentů přijatých elektronickou podatelnou lze určit měřitelné ukazatele pro stanovení jeho kvality:

- produktivita vyřizování dokumentů v digitální podobě,
- ,správné přiřazení a rozdělování dokumentů, z hlediska adresáta,
- nákladovostt při zpracování digitálního dokumentu

5 UKAZATELÉ PRO STANOVENÍ KVALITY E-DOKUMENTU

Politika kvality musí vycházet z vize a strategie organizace. Zohledňuje nejen zaměření na zákazníky- ostatní orgány veřejné správy, fyzické osoby a právnické osoby, ale také na rozvoj vlastní organizace v souladu s principy neustálého zlepšování [3]. S politikou kvality musejí být seznámeni všichni pracovníci krajského úřadu a musí se ztotožnit s tímto prohlášením. Plnění cílů kvality bude sledováno v rámci porad vedení konkrétních útvarů krajského úřadu za použití plánu kontroly kvality, jak je uvedeno v příloze č.2.

5.1 Produktivita útvarů krajského úřadu

Produktivita útvarů krajského úřadu v oblasti vyřizování dokumentů v elektronické podobě. Každý útvar vzhledem k oblasti, kterou má na starosti, si stanoví své koeficienty, které se mohou od sebe výrazně lišit. Produktivita je následně stanovena jako poměr počtu vyřízených digitálních dokumentů a spotřebovaného času Výsledný podíl by měl být násoben váhovým koeficientem. Tento váhový koeficient určuje náročnost zpracování dokumentu z hlediska obsahu a významu.

Obecný vzorec produktivity práce je:

$$P = \frac{Q}{t}$$

P produktivita práce

Q objem produkce

t strávený čas (maximální časová délka je stanovena zákonem [13])

V případě činnosti útvarů krajského úřadu by produktivita práce byla stanovena následovně:

$$P = \frac{Q}{t} \times \varphi,$$

kde φ je váhovým koeficient a pohybuje se v rozmezí 0-100%

Tento ukazatel může být pro vedoucí jednotlivých útvarů krajského úřadu nástrojem pro motivaci jejich podřízených. Určení akceptovatelné hranice produktivity se stává kritériem kvality manipulace s digitálními dokumenty. Při tvorbě plánu cíle kvality by měl být jeden

z cílů překročení stanovené produktivity vyřizování digitálních dokumentů. V rámci hodnocení kvality může vedoucí útvaru použít následující tabulku č. 3.

Tabulka 3: Hodnocení plánu produktivity vyřizování digitálních dokumentů

Plnění stanovení cíle	Odůvodnění
Pokles pod stanovenou produktivitu P	Špatně zvolený ukazatel, Nízká odbornost, nízká znalost správy digitálních dokumentů, Negativní postoj zaměstnanců
Udržení požadované produktivity P	Zpracování významnějších dokumentů, Nízká motivace zaměstnanců, Vnější okolnosti
P +nárůst o 15%	Vysoká motivace pracovníků Vysoká odbornost, dobrá znalost správy digitálních dokumentů
Více než 15%	Špatně zvolený ukazatel

Zdroj: vlastní zpracování

5.2 Správné přiřazení a rozdělování dokumentů

Správné přiřazení a rozdělování dokumentů přísluší pracovníkům elektronické podatelny. Již při příjmu a evidence dokumentů obsluha elektronické podatelny vede podací deník, který obsahuje následující údaje: evidenční číslo, číslo jednací, věc, druh zásilky, datum odeslání, číslo jednací odesílatele, typ dokumentu, počet listů, počet listů příloh nebo počet svazků příloh, datum a čas vzniku dokumentu, termín vyřízení, odesílatel, vyřizující pracovník, způsob vyřízení, způsob vypravení, čas, spisový znak, skartační znak a skartační lhůta.

Znamená to tedy, že obsluha vyplní vždy kolonku vyřizujícího pracovníka i v případě, kdy není jednoznačně jasné, že konkrétní dokument patří přiřazenému útvaru. Zjistí-li útvar, jemuž byl dokument doručen, že není příslušný k jeho vyřízení, bezodkladně jej vrátí na podatelnu nebo ho postoupí příslušnému útvaru. V tomto případě současně informuje podatelnu telefonicky.

S ohledem na požadavek termínu vyřízení je nutné tyto případy evidovat formou neshody jak je uvedeno v příloze č.3.

Kritériem kvality rozdělování přijatých dokumentů je poměr vzniklých neshod oproti celkovému počtu přijetí dokumentů v daném měsíci.

$$kriterium\ kvality = \frac{\sum NESHODY}{\sum DOKUMENTY}$$

Zdroj: vlastní zpracování

Jelikož se jedná o jistý způsob reklamace, i když uvnitř organizace, standardním koeficientem kritéria na trhu komerčních organizací jsou 3% neshod na počet přijatých dokumentů.

Je-li koeficient kritéria kvality rozdělování dokumentů nižší než 3% jsou tato pochybení akceptovatelná.

Přesáhne-li koeficient kritéria kvality rozdělování dokumentů 3%, nadřízený útvaru ve spolupráci s obsluhou musí následně navrhnout nápravné opatření. Jedním z nich může být lepší a srozumitelnější prezentace krajského úřadu vůči veřejnosti. Ve vztahu k obsluze se opatření bude týkat vzdělávání v oblasti organizačního řádu a vlastní činnosti krajského úřadu.

Přesáhne-li koeficient kritéria kvality rozdělování dokumentů více než 6% a nápravná opatření se minula účinkem, je nutné pracovníka obsluhy přeřadit na jiné pracovní místo, event. ukončit s ním pracovní poměr.

5.3 Nákladovost zpracování digitálního dokumentu

Práce s klasickou papírovou podobou dokumentů vystřídala práce s jeho digitální podobou. Přesto většina lidí více důvěřuje tištěnému dokumentu. Tento ukazatel poskytuje informaci o ekonomičnosti zpracování digitálního dokumentu. Nepřímo ukazuje na stupeň setrvačnosti jednotlivých úředníků ve vztahu k tištěnému dokumentu. Podoba výpočtu ukazatele je následující:

$$\boldsymbol{N = \frac{TI}{D}\mathrm{t}}$$

Zdroj. vlastní zpracování

N koeficient nákladovosti zpracování digitálního dokumentu,

t časový úsek, min. 1 měsíc,

D počet stránek přijatých dokumentů, včetně počtu stránek jejich příloh,

TI počet vytisknutých stran,

Návrh tabulky č.4 vystihuje vlastní hodnocení výpočtu koeficientu ekonomičnosti.

Tabulka 4: Hodnocení koeficientu nákladovosti

Výše koeficientu N	Vysvětlení
Pod 0,5	Zaměstnanci plně pracují digitálně
0,5-1	Neutrální informace-potřeba tištěné podoby dokumentu ze strany zaměstnanců je vyšší, přesto jejich snahou je dodržovat standardy digitalizace-
Více než 1	Zaměstnanci jednotlivých útvarů jsou silně konzervativní a nevyužívají možnosti digitálního zpracování. Je nutné se zaměřit na častější kontroly těchto útvarů a zároveň zajistit školení zaměstnanců v této tématice

Zdroj. vlastní zpracování

Tento ukazatel může být pro vedoucí jednotlivých útvarů krajského úřadu nástrojem pro motivaci jejich podřízených v práci s digitálními dokumenty. V důsledku sledování tisku dokumentů útvar získá mimo jiné i důležité informace ohledně spotřeby kancelářského papíru a tonerů tiskových zařízení.

Krajský úřad Královehradeckého kraje zaznamenal za loňský rok pokles spotřeby kancelářského papíru o 20% a tonerů tiskáren o 30%.

ZÁVĚR

Úspěšný byznys dneška se neobejde bez kvalitních lidských zdrojů. Kvalitní lidi a týmy se na trhu nekoupí. Ty si musí firma vychovat k obrazu svému. Totéž ale platí pro veřejnou správu, která si dala za dlouhodobý cíl zlepšení komunikace mezi orgány veřejné správy, a zároveň s občany. Vzájemná komunikace mezi orgány veřejné správy musí probíhat pouze elektronicky. Důvod elektronické komunikace je zcela jasný Jedná se o úspěšnost doručení digitálních dokumentů, která činí více než 97% a zároveň dochází k výraznému snížení finančních nákladů. I přes tyto pozitivní výsledky je nedůvěra v elektronické dokumenty vysoká. Listinný dokument potvrzený fyzickým podpisem je vnímán odlišně než zaručený digitální dokument opatřený zaručeným elektronickým podpisem.

Krajský úřad Královehradeckého kraje si je vědom svého významu a zároveň potenciálu svých zaměstnanců. Z tohoto důvodu zjišťuje jejich školení již od prvopočátku vzniku strategie e-Governmentu. Pracovníci úřadu jsou povinni přejímat odpovědnost, neklást bariéry v komunikaci a nevytvářet atmosféru osobní nepostradatelnosti.

Jedním významným úkolem krajských úřadů je digitalizaci dokumentů, jejich zpřístupnění a zároveň jejich ochrana. Řeší společně otázku důvěryhodného ukládání dokumentů. Se spuštěním Informačního Systému datových schránek vznikl problém určení způsobu dlouhodobého ukládání dokumentů v elektronické podobě. Ministerstvo vnitra České republiky vydalo doporučení používat zaručené časové razítko. Podle průzkumu ani jeden krajský úřad, včetně Královehradeckého z důvodu velkých finančních nákladů se tímto doporučením neřídil. Náklady na provoz a využití časového razítka jsou v prvním roce nízké. Následný nárůst finančních nákladů je velmi výrazný, přesto budou krajské úřady nuceni využít předplacených balíčků u certifikačních autorit a opatřit již stávající dokumenty časovými razítky.

POUŽITÁ LITERATURA

[1] BITTNER, Ivan. Spisová a archivní služba ve státní správě, samosprávě a v podnikatelské sféře. 3. aktualiz. a přeprac. vyd. Praha: Linde, 2005, 305 s. ISBN 80-720-1549-4.

[2] CAF. Společný hodnotící rámec (model CAF): Zlepšování organizace pomocí sebehodnocení. Praha: Národní informační středisko pro podporu jakosti, 2007. Dostupné z: http://npj.cz/narodni-politika-kvality/dokumenty/narodni-politika-kvality/

[3] COGAN, Rudolf. Krajské zřízení. Vyd. 1. Praha: ASPI, 2004, 440 s. ISBN 80-735-7041-6

[4] CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. 1. vyd. Praha: Národní knihovna České republiky, 2010, 154 s. ISBN 978-80-7050-588-5

[5] Česká republika. Vyhláška č.191/2009: o podrobnostech spisové služby. In: Sbírka zákonů. Ministerstvo vnitra, 2009, 57/2009, 2773. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68872&fulltext=&nr=191~2F2009&part=&name=&rpp=15#local-conten.

[6] Česká republika. Vyhláška č.193/2009: o stanovení podrobností provádění autorizované konverze dokumentů. In: Sbírka zákonů. Ministerstvo vnitra, 2009, 57/2009, 2796. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68874&fulltext=&nr=193~2F2009&part=&name=&rpp=15#local-content.

[7] Česká republika. Vyhláška č.194/2009: o stanovení podrobností užívání a provozování informačního systému datových schránek. In: Sbírka zákonů. Ministerstvo vnitra, 2009, 57/2009, 2799. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68875&fulltext=&nr=194~2F2009&part=&name=&rpp=15#local-content.

[8] Česká republika. Vyhláška č.212/2012: o ověřování platnosti zaručeného elektronického podpisu. In: Sbírka zákonů. Ministerstvo vnitra, 2012, 75/2012, 3020. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68875&fulltext=&nr=194~2F2009&part=&name=&rpp=15#local-content

[9] Česká republika. Zákon č.227/2000: o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: Sbírka zákonů. Ministerstvo vnitra, 2000, 68/2000, 3290. Dostupné z: http://portal.gov.cz/app/zakony/zakonInfo.jsp?idBiblio=49532&fulltext=&nr=227~2F2000&part=&name=&rpp=15#local-content

[10] Česká republika. Zákon č.300/2008: o elektronických úkonech a autorizované konverzi dokumentů. In: Sbírka zákonů. Ministerstvo vnitra, 2008, 98/2008, 4491. Dostupné z: http://portal.gov.cz/app/zakony/zakonInfo.jsp?idBiblio=67315&fulltext=&nr=300~2F2008&part=&name=&rpp=15#local-content.

[11] Česká republika. Zákon č.365/2000 Sb.: O informačních systémech veřejné správy a o změně některých dalších zákonů. In: *Sbírky zákonů*. Parlament České republiky, 2000, 365/2000 Sb., 99/2000. Dostupné z: http://portal.gov.cz/app/zakony/zakonInfo.jsp?idBiblio=49763&fulltext=&nr=365~2F2000&part=&name=&rpp=15#local-content

[12] Česká republika. Zákon č.499/2004: o archivnictví a spisové službě a o změně některých zákonů. In: Sbírka zákonů. Ministerstvo vnitra, 2004, 173/2004, 9742. Dostupné z: http://portal.gov.cz/app/zakony/zakonInfo.jsp?idBiblio=58364&fulltext=&nr=499~2F2004&part=&name=&rpp=15#local-content

[13] Česká republika. Zákon č.500/2004 Sb.: správní řád. In: *Sbírky zákonů*. Parlament České republiky, 2004, 174/2004. Dostupné z: http://portal.gov.cz/app/zakony/zakonInfo.jsp?idBiblio=58370&fulltext=&nr=500~2F2004&part=&name=&rpp=15#local-content

[14] ČSN EN ISO 9001. Systémy managementu kvality-Požadavky. ed. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[15] Digitální dokument. [online]. 2010 [cit. 2012-07-23]. Dostupné z: http://www.pd.nolimit.cz/digitalni-dokument.

[16] HŮRKA, Ondřej. Technologická centra krajů. [online]. 2010, s. 19 [cit. 2012-07-23]. Dostupné z: www.mvcr.cz/soubor/technologicka-centra-kraju-ondrej-hurka-pdf.aspx

[17] MINISTERSTVO VNITRA ČR. *Datové schránky* [online]. 2011. vyd. Praha: Česká pošta s.p., 2011 [cit. 2012-07-29]. Dostupné z: http://www.datoveschranky.info/

[18] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Digitalizace a ukládání: Typizovaný projektový záměr. verze 2.7. Praha, 2009, 34 s. Dostupné z: www.mvcr.cz/soubor/vyzva-08-ppzp-p14a-projekt-da-v2-7-pdf.aspx

[19] PETERKA, Jiří. Elektronické podpisy: z bláta do louže? [online]. s. 1 [cit. 2012-07-03]. Dostupné z: WWW: < http://www.lupa.cz/clanky/elektronicke-podpisy-z-blata-do-louze/ >

[20] PETERKA, Jiří. Elektronický nebo digitální dokument?. Bezpapiru.cz [online]. 2009-04-27 [cit. 2011-04-21]. Dostupný z WWW: <http://www.bezpapiru.cz/elektronicky-digitalni-dokument>

[21] PSOHLAVEC, Stanislav. Přednost a rizika digitálních dokumentů. Ikaros [online]. 2005, roč. 9, č. 12 [cit. 2011-04-15]. Dostupný z WWW: <http://www.ikaros.cz/node/2064>

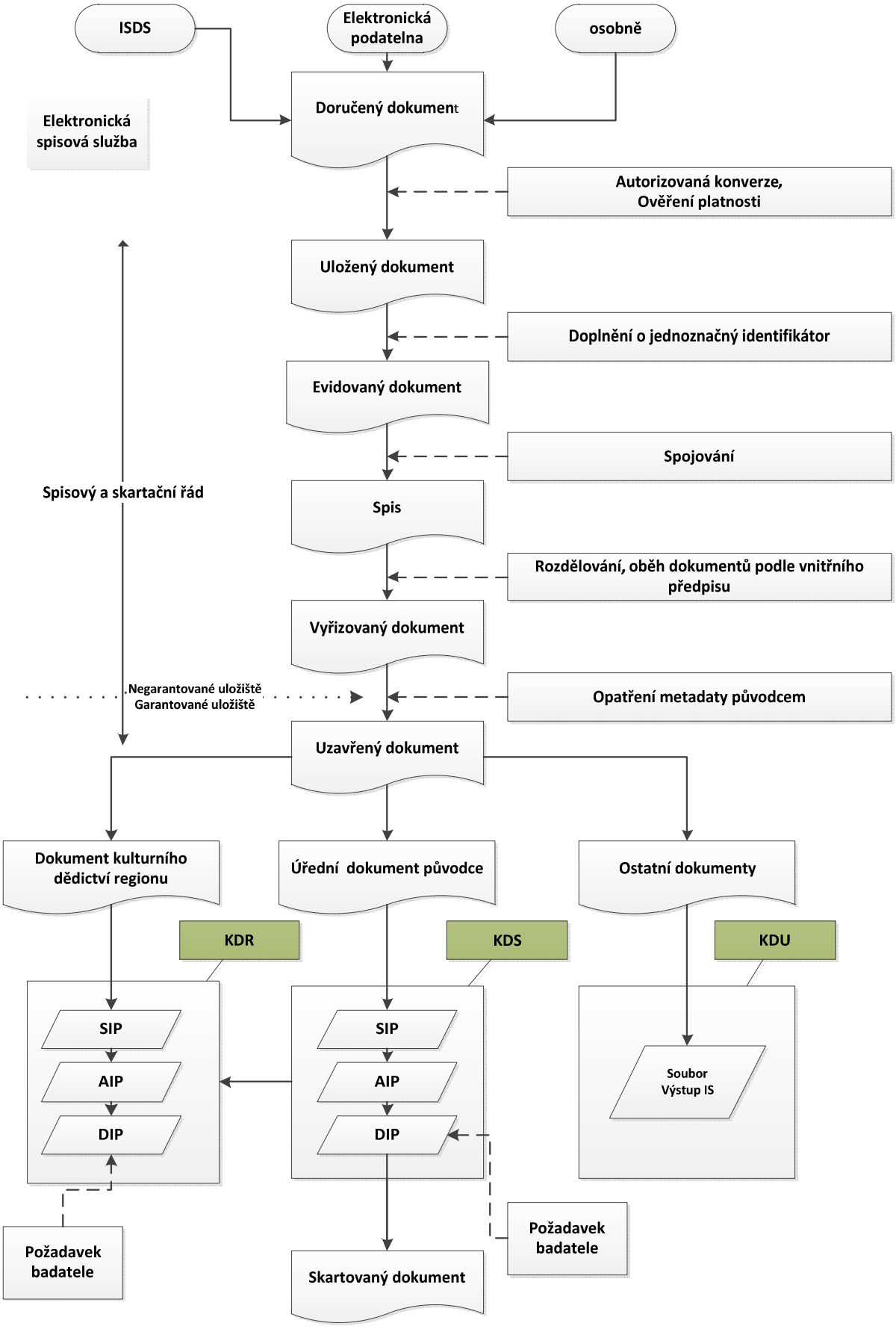
[22] ROSA, Tomáš. Nepopíratelnost digitálních podpisů. [online]. s. 5 [cit. 2012-07-01]. Dostupné z: WWW: <http://crypto.hyperlink.cz/files/rosa_ZMVS04.pdf >

[23] TESAŘ, Pavel. Provozní řád ISDS: Datové schránky. In: *Datové schránky* [online]. Praha: Ministerstvo vnitra ČR, 2012 [cit. 2012-07-29]. Dostupné z: http://www.datoveschranky.info/assets/ke-stazeni/provozni_rad_isds.pdf

[24] VMV čá. 101/2010. In: Národní standard pro elektronické systémy spisové služby [online]. Praha: Ministerstvo vnitra, 2010 [cit. 2012-07-23]. Dostupné z: http://www.mvcr.cz/clanek/vestnik-ministerstva-vnitra-vestnik-ministerstva-vnitra.aspx

SEZNAM PŘÍLOH

PŘÍLOHA 1 Životní cyklus digitálního dokumentu



Zdroj: vlastní zpracování

PŘÍLOHA 2 Program interní kontroly na období

Program interní kontroly na období:	
Zpracoval: *jméno a podpis manažera kvality*	**Dne:**
Schválil: *jméno a podpis nadřízeného*	**Dne:**
Platnost: *od - do*	

Proces	**Termín**	**Místo prověření**	**Tým auditorů**	**Záznam/protokol (označení)**	**Počet zjištěných neshod**	**Záznam o ověření účinnosti NO - datum**

PŘÍLOHA 3 Záznam o neshodě a nápravném opatření

Záznam o neshodě a nápravného opatření	
1. Popis neshody *(vyplní nadřízený)*	
2. Analýza příčiny *(vyplní nadřízený ve spolupráci s osobou odpovědnou za danou činnost)*	
3. Vypořádání neshody – přijaté NO *(vyplní osoba odpovědná za danou činnost)*	
Termín vypořádání:	Odpovídá: –
4. Ověření účinnosti	
Zjištění: Datum, podpis:	
Kontrola Komentář:	**Datum, podpis:**