

1 Životní cyklus elektronických dokumentů

1.1 Právní rozbor tuzemské legislativy

1.1.1 Pojem písemnosti, transformace dokumentů do elektronické formy

České právo upravuje písemnou formu v § 40(4) občanského zákoníku. Podle tohoto ustanovení je písemná forma zachována, „je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.“ Toto ustanovení kombinuje požadavky na písemnost s požadavky na zaručený elektronický podpis. Neobsahuje však požadavek na reprodukovatelnost a čitelnost, obsaženou v UNCITRAL Model Law a ve většině novějších evropských úprav včetně legislativy EU.

České právo v jednom případě upravuje možnost převodu původních písemných dokumentů do elektronické formy a jejich dlouhodobou archivaci v elektronické formě. Jedná se o zákon č. 235/2004 Sb. o DPH. V ustanovení § 27 (2) zákona o DPH je uvedeno, že: „Daňový doklad v písemné formě lze převést do elektronické podoby a uchovávat pouze v této podobě, pokud metoda použitá pro převod a uchování zaručuje věrohodnost původu, neporušitelnost obsahu daňového dokladu a jeho čitelnost a pokud je daňový doklad převedený do elektronické podoby opatřen zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo označen elektronickou značkou založenou na kvalifikovaném systémovém certifikátu osoby odpovědné za jeho převod.“

České právo s výše uvedenými výjimkami v současnosti vůbec neupravuje zásadní právní instituty (viz kapitola 2.1.3). Domníváme se, že celou tuto oblast českého práva, tedy úpravu základních institutů práva elektronické komunikace, je třeba systematicky a nově v českém právu upravit.

1.1.2 Elektronické podpisy

Vzhledem k tomu, že právo EU v oblasti elektronických podpisů je dostatečně rozvinuté, jsou evropské právní předpisy upravující elektronické podpisy založené na evropské legislativě a nikoliv na Modelovém zákonu UNCITRAL o elektronických podpisech, jako je tomu v případě USA. Český zákon č. 227/2000 Sb., ve znění pozdějších předpisů, je na úrovni srovnatelné s vyspělými evropskými státy.

Bohužel řada jiných zákonů není konsistentní se zákonem o elektronickém podpisu. Zákon o elektronickém podpisu v § 11 (1) upravuje požadavky na elektronické podpisy používané v oblasti orgánů veřejné moci takto: „V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis“).“ To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.

Jiné zákony však rozdílně upravují požadavky na elektronické podpisy, aplikovatelné při komunikaci ze strany soukromých osob vůči orgánům veřejné moci. Tak např. zákon č. 500/2004 Sb., nový správní řád, vyžaduje v § 37 (4) pouze použití zaručených elektronických podpisů. Zákon č. 137/2006 Sb., nový zákon o zadávání veřejných zakázek, vyžaduje v § 149(4) použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu.

Současně však zákon o elektronickém podpisu obsahuje v § 3 vyvratitelnou zákonnou domněnku autentičnosti podpisu pouze ve vztahu k zaručeným elektronickým podpisům založeným na kvalifikovaných certifikátech a vytvořeným pomocí prostředku pro bezpečné vytváření podpisu. Znamená to, že na elektronická podání podle stávajících právních předpisů by se vyvratitelná domněnka obsažená v § 3 zákona o elektronickém podpisu nevztahovala. To může mít velmi závažné důsledky v soudních sporech při dokazování, kdy bude jedna strana např. tvrdit, že neobdržela příslušný elektronický dokument, přestože správní orgán obdržel potvrzení o převzetí podepsané zaručeným elektronickým podpisem adresáta.

Je zvláštní, že při komunikaci v oblasti veřejné správy jsou kladeny jiné požadavky na správní orgány a jiné na soukromé osoby, komunikující s těmito orgány. Dále jsou tyto požadavky odlišné od vyvratitelných zákonných domněnek obsažených v zákoně o elektronickém podpisu. Rovněž požadavky na soukromé osoby pro účely komunikace s veřejnou správou by měly být shodné ve všech právních předpisech.

1.1.3 Elektronické doručování a podání

Je důležité, aby existovala jasná a konsistentní úprava elektronického doručování a podávání, bez něhož je elektronická komunikace s veřejným sektorem nemožná. Charakteristickým rysem současné tuzemské úpravy je však nesystematičnost a různorodost.

Doručování

Zákon o správě daní a poplatků (ZSDP), upravuje doručování na elektronickou adresu v § 17a. U běžného doručování ZSDP neupravuje okamžik doručení. U elektronického doručování do vlastních rukou považuje tento zákon písemnost za doručenou v okamžiku, kdy převzetí doručované písemnosti potvrdí adresát zprávou opatřenou zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu (tzv. elektronická doručenka). ZSDP neupravuje fikci doručení elektronickou cestou.

Podání

Stejně jako u doručování, české právo obsahuje řadu zvláštních přístupů k úpravě elektronických podání vůči správním orgánům. ZSDP obsahuje prakticky totožnou úpravu okamžiku přijetí podání jako okamžiku doručení; podání je přijato dnem, vyznačeným na potvrzení o přijetí generovaném technickým zařízením správce daně.

Nový správní řád v § 37 (6) uvádí, že podání je učiněno dnem, kdy příslušnému orgánu došlo. Co to však znamená pro elektronická podání? Ve světě existuje několik

výkladů toho, kdy elektronická zpráva "dojde" svému adresátovi – právě proto je třeba být v zákonné úpravě přesnější.

Významné rozhodnutí Ústavního soudu č. ÚS 319/05 potvrdilo, že české právo umožňuje provádět soudní podání pouze elektronicky, jestliže je k podání uznávaný elektronický podpis dle §11 odst. 1 zákona č. 227/2000 Sb. o elektronickém podpisu.

1.1.4 Uzavírání smluv elektronicky

UNCITRAL Model Law obsahuje základní úpravu elektronických závazkových vztahů. Tato úprava se podle těchto dokumentů má uplatnit pouze pokud se strany závazkového vztahu nedohodnou jinak, nejedná se tedy o ustanovení mandatorní povahy. Občanský zákoník nyní obsahuje poměrně komplexní úpravu spotřebitelských smluv uzavíraných na dálku, kromě jiného díky nedávno přijatému zákonu o některých službách informační společnosti č. 480/2004 Sb.. Nicméně, ustanovení ve výše uvedených dokumentech UNCITRAL jsou velmi podnětná hlavně z těchto důvodů: (1) pravidla obsažená v dokumentech UNCITRAL vznikla jako reflexe pravidel digitálního prostoru, zejména pravidel komunikace (kdy je datová zpráva odeslána a doručena, platnost datových zpráv, kdo je považován za adresáta, příjemce a odesilatele datových zpráv, kdo je odpovědný za obsah datové zprávy, aj.) a dále pravidel uzavírání smluv (místo a čas uzavření smlouvy elektronicky, uzavírání smluv prostřednictvím automatizovaných systémů, aj.). Proto tato pravidla zejména slouží jako vodítko pro podnikatele, kteří hodlají uzavírat své smluvní vztahy elektronicky. Proto tato pravidla postupně přejímá více a více vyspělých států světa. Domníváme se, že součástí systematického přístupu k legislativě elektronické komunikace by měla být také legislativní analýza a následné úprava těchto pravidel v rámci českého práva.

1.1.5 Elektronická fakturace a archivace

V českém právu je úprava elektronické fakturace obsažena zejména v zákoně č. 235/2004 Sb., v aktuálním znění, o DPH¹. Z ustanovení § 26 odst. (4) vyplývá, že daňové doklady mohou být se souhlasem osoby vystaveny pouze v elektronické formě, avšak musí pak být opatřeny zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo elektronickou značkou založenou na kvalifikovaném systémovém certifikátu nebo pokud je zaručena věrohodnost původu a neporušitelnost obsahu daňového dokladu elektronickou výměnou informací (EDI) ... Ustanovení § 27 odst. (3) a (4) pak upravuje možnost a podmínky uchování daňových dokladů v elektronické formě v zahraničí.

V případě použití EDI tedy není výslovně nutné opatřit daňový doklad elektronickým podpisem pokud by byla věrohodnost původu a neporušitelnost obsahu zaručena jinak (např. potvrzováním přijetí a obsahu zpráv, kontrolními součty, identifikačními nástroji aj.).

Dle českého práva je možné všechny typy daňových dokladů vystavovat elektronicky avšak se souhlasem osoby, pro kterou se plnění uskutečňuje, s výjimkou „dokladu o

¹ v § 26 a § 27

použití“, kdy souhlasu není třeba. V některých případech je nutná spolupráce s výstavcem dokladu v jiném členském státě za účelem splnění tamějších předpisů. Rovněž v případě daňových dokladů při dovozu a vývozu je třeba souhlasu celního orgánu. Je možné využít ale i tzv. „self-billing“, jde o případ, kdy plátce zplnomocní k vystavování daňových dokladů svým jménem třetí osobu.²

České právo upravuje rovněž povinnosti týkající se zaúčtování elektronických daňových dokladů zejména v zákoně č. 563/1991 Sb., v aktuálním znění, o účetnictví a ve výše uvedeném zákoně o DPH. Například, jednou z povinností v účetnictví je vést účetní doklady jako průkazné účetní záznamy. Každou skutečnost týkající se vedení účetnictví je nutno zaznamenávat výhradně jen účetními záznamy³. Průkaznost jako jeden z požadavků kladených na účetnictví jako celek (tedy včetně průkazných účetních záznamů a účetních dokladů) je tvořena řadou dílčích povinností upravených v zákoně o účetnictví (např. § 8 (1) a (4), § 33, § 33a, § 34). Součástí těchto povinností je také např. odsouhlasení obsahu účetního dokladu po věcné a formální stránce osobou odpovědnou za účetní případ a osobou odpovědnou za jeho zaúčtování⁴. Důkazem odsouhlasení je i tzv. podpisový záznam odpovědných osob⁵.

Podpisový záznam může mít rovněž formu elektronického podpisu nebo jiného technického záznamu⁶. Zákon o účetnictví sice nevyžaduje výslovně použití zaručených elektronických podpisů jako podpisových záznamů, nicméně z důvodu prokazatelnosti, že záznam příslušná osoba učinila, je aplikace zaručených elektronických podpisů, případně značek velice žádoucí pro splnění zákonných podmínek průkaznosti. Zde je velmi významná role účetní jednotky a jejího vnitřního kontrolního systému ve stanovení oprávněnosti, povinnosti a odpovědnosti jednotlivých osob za podpisový záznam ve vztahu k obsahu příslušného účetního záznamu. Jaký způsob zvolí je na uvážení účetní jednotky (písemná nebo technická forma). Podrobnosti aplikace podpisových záznamů nebo identifikačních záznamů musí stanovit vnitřní předpis⁷. Podpisovými záznamy lze označovat účetní doklady i hromadně např. jednou za určitou dobu nebo jednotlivě.

Další povinností je čitelnost účetních (daňových) dokladů⁸. Povinnost čitelnosti neznamená, že by účetní doklad musel být vždy v čitelné formě, ale že musí být ve formě, která příslušné účetní jednotce - držiteli dokladu umožňuje jej převést do čitelné formy. Účetní jednotky tedy musí disponovat prostředky, které toto převedení umožňují.

Úprava archivačních povinností, způsob a délka archivace účetních dokladů, je poměrně rozčleněna vzhledem k tomu, že účetní doklady slouží jako doklad k doložení rozličných povinností právnických a fyzických osob vyplývajících např. ze zákona o DPH, o dani z příjmu, o účetnictví či o pojistném na sociální zabezpečení.

² § 26(3) a) zákona o DPH

³ § 4 (10)

⁴ § 11(1)f) zákona o účetnictví

⁵ § 33a (1d)

⁶ § 33a (3)-(9) zákona o účetnictví

⁷ § 33a (9) zákona o účetnictví

⁸ § 33 (2) b), § 33 (6) zákona o účetnictví

Obecná úprava týkající se nakládání s účetními doklady je obsažena v zákoně o účetnictví⁹, který stanovuje, že účetní jednotky jsou povinny uschovávat účetní záznamy pro účely vedení účetnictví¹⁰. Za účetní záznam jsou přitom pokládána veškerá data, která jsou záznamem veškerých skutečností týkajících se vedení účetnictví¹¹, tedy účetní doklady. Účetní jednotky jsou navíc povinny zabezpečit jejich ochranu (včetně jejich obsahu, nosičů informací, technických prostředků a programového vybavení) před jejich zneužitím, poškozením apod.¹² a rovněž jsou povinny disponovat účetními záznamy, kterými dokládají formu vedení účetnictví.

Pojem dispozice s účetními záznamy není v zákoně o účetnictví blíže specifikován, je však možné k jej konkretizovat ustanoveními zákona o DPH¹³ a Směrnice 2001/115/ES (Směrnice). Vzhledem k úpravě v zákonu o DPH vycházejícího ze směrnice je možné, aby plátce DPH uchovával daňové doklady v elektronické podobě mimo Českou republiku¹⁴. Pojem disponovat proto není nutné vykládat restriktivně jako vlastnictví dat či jejich naprostá kontrola. Za těchto okolností ale plátce musí zajistit elektronicky správci daně právo volného přístupu v reálném čase k daňovým dokladům a datům, která zaručují věrohodnost jejich původu a neporušitelnost jejich obsahu. Tímto zákon o DPH nepřímou stanovuje rovněž povinnost archivovat i data zaručující věrohodnost původu účetního dokladu a neporušitelnost jeho obsahu. Právo volného přístupu v reálném čase lze vyložit jako zpřístupnění bez zbytečného prodlení po požádání správce daně¹⁵. Zde je třeba připomenout, že pro tyto účely je nutné, aby účetní jednotky měly potřebné prostředky umožňující převedení do čitelné formy (viz výše).

Směrnice přímo obsahuje oprávnění přístupu příslušných orgánů členských států elektronickými prostředky k fakturám uchovávaným v jiném členském státě. Ve vztahu ke státům, které nejsou členy EU Směrnice umožňuje, aby členské státy zvolili za určitých okolností přísnější režim, který by zakazoval nebo omezoval uchovávání faktur. Česká republika této možnosti nevyužila avšak stanovila v zákoně o DPH, že plátcí navíc k výše uvedeným povinnostem mají povinnost oznámit předem správci daně, že daňové doklady jsou uchovávány mimo Českou republiku¹⁶.

Zákon o účetnictví předpokládá, že účetní záznamy využívá účetní jednotka i pro jiné účely než-li vedení účetnictví a stanovuje, že účetní jednotky mají postupovat tak, aby po uplynutí lhůt stanovených v zákoně o účetnictví zajistily požadavky, které vyplývají z jejich použití např. pro účely soudního, správního řízení či opatření proti legalizaci výnosů z trestné činnosti¹⁷, tedy v obdobných případech dokumenty uchovávala v případě, že lhůta dle zákona o účetnictví uplynula.

⁹ č.563/1991 Sb., v aktuálním znění

¹⁰ § 31 (1)

¹¹ §4 (10)

¹² § 33 (8)

¹³ č. 235/2004 Sb., v aktuálním znění

¹⁴ §27 (2)

¹⁵ Směrnice čl. 2(1)d

¹⁶ §27 (4)

¹⁷ § 32 (1)

1.1.6 Archivace obecně

Archivační požadavky je vždy nutné provázat s dalšími zákony, zejména zákonem o archivnictví a spisové službě a vyhláškami¹⁸. Zákon o archivnictví a spisové službě definuje jako dokument každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální¹⁹. Tento zákon ukládá rovněž podnikatelům zapsaným v obchodním rejstříku²⁰ povinnost uchovávat takovéto dokumenty²¹ (např. včetně finančních dokumentů a účetních záznamů) a umožnit z nich výběr archiválií. K výběru archiválií dochází u podnikatelů zapsaných v obchodním rejstříku obvykle mimo skartační řízení, pokud se nestanou tzv. určenými původci, kteří vedou spisovou službu v souladu s tímto zákonem a prováděcím předpisem.²²

Za archiválie přitom budou vždy vybrány dokumenty dle Přílohy č. 2 k zákonu o archivnictví a spisové službě, např. dokumenty dle obsahu, které obsahují zásadní informace o rozvoji hospodářství včetně důležitých účetních přehledů či účetní závěrky. Pro tyto účely lze odkázat na typový skartační rejstřík Ministerstva vnitra. Je tedy nutné uchovávat dané dokumenty tak dlouho, než dojde k výběru archiválií. Podnikatel ale může požádat příslušný archiv, aby vydal trvalý skartační souhlas na jím stanovené dokumenty, které pak lze zničit i bez výběru archiválií mimo skartační řízení²³.

Chtěli bychom upozornit na pravděpodobné neplatné ustanovení prováděcí vyhlášky č. 646/2004 §5 odst. 1, požadující trvalé uložení dokumentů se skartačním znakem A do archivu na trvanlivém papíru. Toto ustanovení vyhlášky je v rozporu s ustanovením zákona o DPH, umožňujícím trvalou transformaci papírových daňových dokladů do elektronické formy a dlouhodobou archivaci pouze v tomto formátu.

1.2 Životního cyklus papírových dokumentů

Životní cyklus dokumentů je upraven v zákoně o archivnictví č. 499/2004 Sb., v aktuálním znění, ve vyhlášce o podrobnostech výkonu spisové služby č. 646/2004 Sb., vyhlášce, kterou se provádějí některá ustanovení zákona o archivnictví č. 645/2004 Sb. a ve vyhlášce 496/2004 o elektronických podatelkách. Životní cyklus dokumentů lze víceméně rozdělit do dvou fází – spisovou službu a archivnictví.

1.2.1 Spisová služba

¹⁸ č. 499/2004 Sb., v aktuálním znění, vyhláška č. 646/2004 Sb., vyhláška 645/2004 Sb.

¹⁹ §2d

²⁰ §3 (2)

²¹ Příloha č. 1 k zákonu o archivnictví a spisové službě

²² č. 646/2004 Sb., v aktuálním znění, kdy např. v případě dokumentů označených dle spisového a skartačního plánu skartačním znakem „A“, dokument musí být vyhotoven na trvanlivém papíru

²³ §15 zákona o archivnictví a spisové službě

Vyhláška o podrobnostech výkonu spisové služby č. 646/2004 Sb. obsahuje podrobnosti „document workflow“, tedy oběhu dokumentů ve spisové službě, jehož průběh je rámcově následující:

- Příjem dokumentů
opatření dokumentu razítkem či elektronickým identifikátorem a předání k vyřízení
- Evidence dokumentů
v podacím deníku nebo jednacím protokolu podatelny
- Rozdělování a oběh dokumentů
nutnost zabezpečení jeho průkazného předávání a přebírání
- Vyřizování dokumentů
určeným zaměstnancem, který poté připojí pokyn k založení a další údaje, např. skartační lhůtu a skartační znak
- Vyhотовování dokumentů
dle přidělených skartačních znaků, typ A např. na trvanlivém papíru, nebo dokumenty z úřední činnosti se musí specificky označovat
- Podepisování dokumentů
zaměstnancem pověřeným vnitřními předpisy, možnost el. podpisu u dokumentů v digitální podobě; ve zvláštních případech úřední razítko
- Odesílání dokumentů
přes výpravnu, která je součástí podatelny
- Ukládání dokumentů
dle spisového a skartačního řádu, včetně dokumentů v digitální podobě

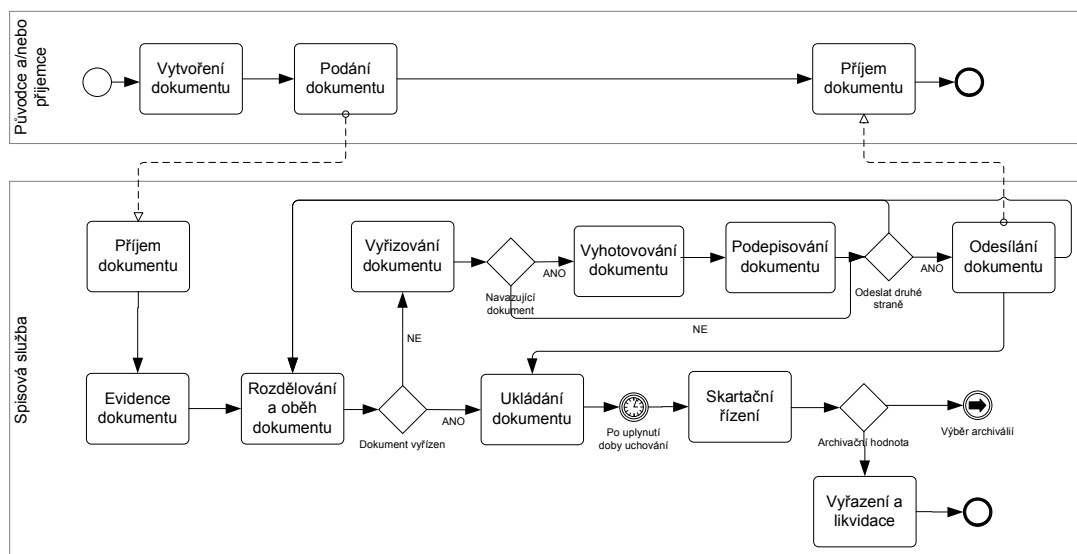
1.2.2 Archivnictví

Při ukládání dokumentů dle spisového a skartačního řádu dochází k vyznačení skartační lhůty. Z dokumentů, jímž uplynula skartační lhůta, jsou vybírány archiválie a to ve skartačním řízení či mimo něj. Archiválie jsou po té

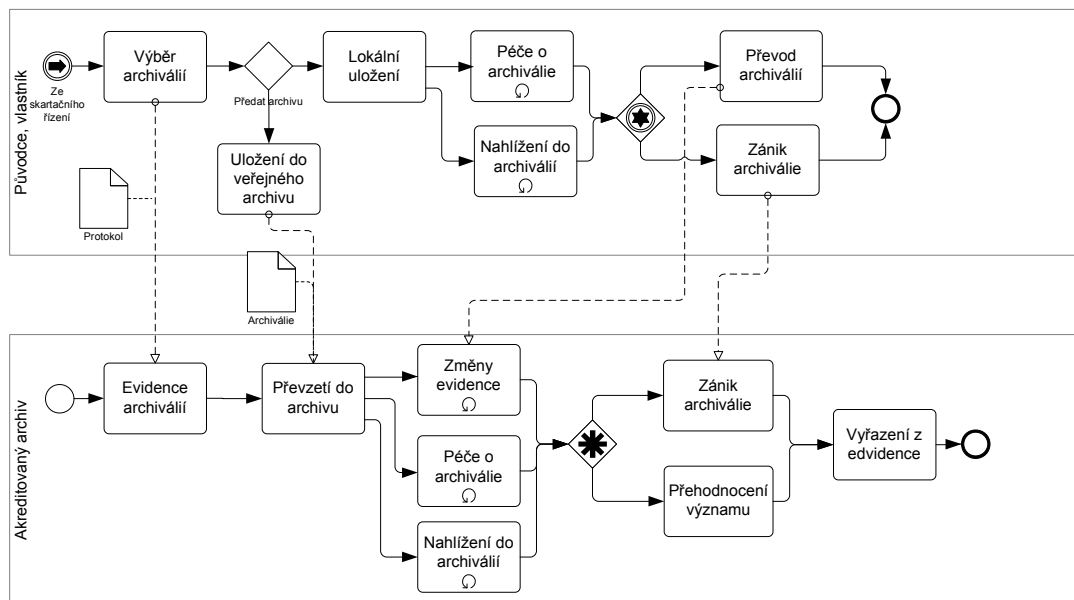
- kategorizovány
- evidovány
- uloženy ve veřejném archivu (nepovinné)
- je o ně pečováno
- lze do nich nahlížet a pořizovat výpisy, opisy a kopie.

Níže uvedené diagramy schématicky ukazují oběh dokumentů jak ve spisové službě, tak i následně v rámci jejich archivace:

Tok dokumentů ve spisové službě



Tok dokumentů v archivnictví



1.3 Taxonomie elektronických dokumentů

Pro lepší pochopení procesů spojených s životním cyklem elektronických dokumentů a především s jejich dlouhodobou archivací bude vhodné provést rozčlenění této široké kategorie do vhodné taxonomie (systému tříd/kategorií), která rozdělí ED do takových tříd, které budou mít podobné vlastnosti z hlediska především archivace. Jak vyplývá z provedených výzkumů v oblasti legislativní a procesní (viz kapitoly 1.1 a 1.2) mezi hlavní vlastnosti ovlivňující dlouhodobou uchovatelnost a použitelnost ED patří zejména:

- Plná reprodukovatelnost obsahu
(schopnost reprezentovat obsah ED ve formě srozumitelné lidskému uživateli, tak aby ji byl schopen mu porozumět a využít ho)
- Integrita obsahu
(schopnost prokázat, že obsah nebyl změněn a je dostupný v takové podobě, v jaké byl vytvořen a/nebo uložen)
- Autentičnost
(schopnost, prokázat, že ED byl vytvořen a/nebo uložen danou entitou, často je integrita vnímána jakou součástí autentičnosti v širším smyslu)

Vlastnosti ED jsou vyjádřeny metadaty - „data o datech“, proto právě existující metadata standardy jsou jedním z hlavních podkladů, která jsou použity pro návrh taxonomie.

Jedná se především o Dublin Core, rozšířený mezinárodní standard pro popis digitálních zdrojů, OAIS, který popisuje obecný informační model archivačního systému, a některé další standardy které definují specifické sady metadat pro účely dlouhodobé archivace digitálních objektů (PREMIS aj.).

Navržená taxonomie nejenže vychází z existujících výsledků na poli metadat pro dlouhodobé uchování digitálních objektů, ale bude zároveň tvořit rámcové východisko pro návrh systému metadat pro řešení navazující na naši studii.

Pro návrh taxonomie jsme vycházeli z následujících požadavků:

- Vycházet z existujících standardů a zkušeností, především v oblasti metadat, jak bylo uvedeno výše
- Vytvořit jednoduchý a obecný klasifikační systém
 - Není nutné zacházet do detailů, klasifikace by měla sloužit pro rámcové roztřídění ED
 - Minimalizovat počet tříd
- Klasifikovat ED v několika nezávislých směrech, tak aby byly podchyceny klíčové vlastnosti z hlediska životního cyklu ED

Vycházejíce z uvedených požadavků jako vhodné vlastnosti pro klasifikaci ED se ukazují:

- Typ ED
- Historická hodnota
- Formát
- Zajištění původu a integrity

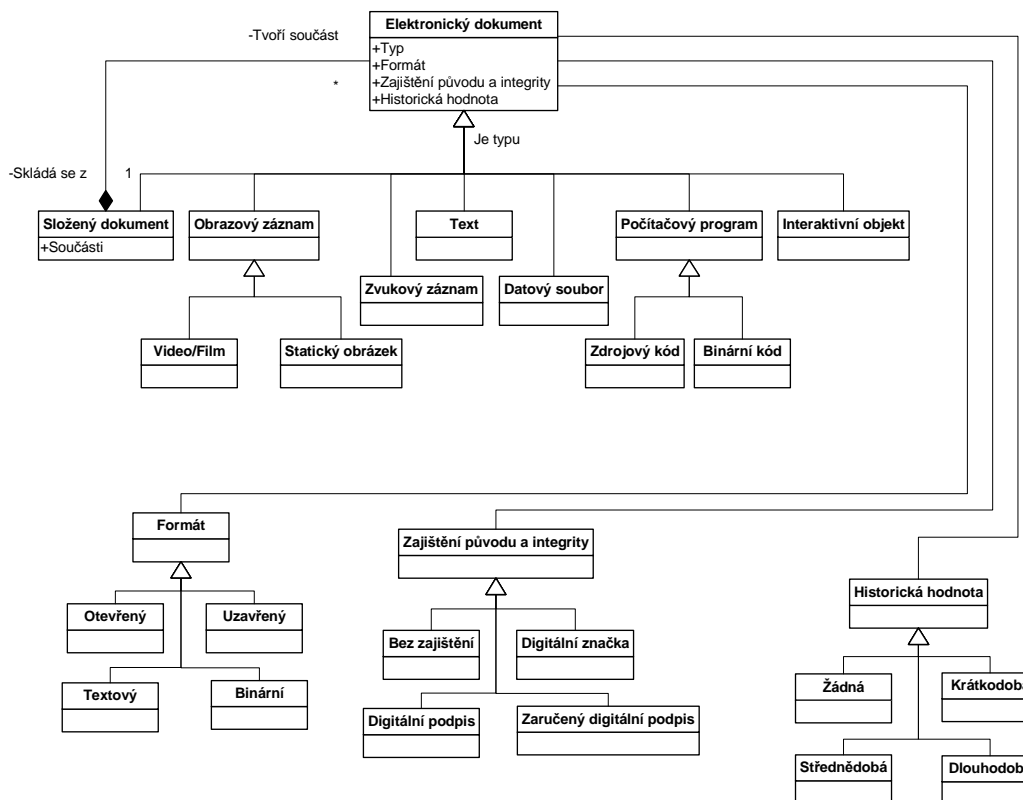
Typ ED je hlavním směrem klasifikace, odpovídá běžnému způsobu třídění fyzických objektů (nábytek -> skříň, židle, stůl ...), nicméně pro vhodné roztřídění je nutné

zavést ještě směry vedlejší. Historická hodnota vyplývá z kulturního, legislativního a sociálního kontextu dokumentu, její ekvivalent je možné též nalézt ve fyzickém světě. Další dva směry (formát a zajištění původu a integrity) jsou spíše specifické pro digitální svět a jejich ekvivalenty ve fyzickém světě jsou pouze přibližné.

Například formát (neboli reprezentace) hraje v digitálním světě velkou roli, určuje způsob jak bude daný koncept zapsán jako řetězec binárních symbolů. V digitálním světě je obvyklé že stejné koncepty jsou reprezentovány rozdílnými zápisy (např. obrázek kočky může být v několika formátech a při zobrazení na obrazovce se všechny reprezentace budou jevit jako shodné) ve fyzickém světě toto ale není obvyklé (neexistují dvě různé reprezentace kočky, které by byly z našeho pohledu zcela ekvivalentní). Pro formát digitálních objektů je také možné, že dva objekty budou shodné až po nejmenší možné rozlišovací detaily (tedy bity), což opět není obvyklé ve fyzickém světě (i když máme například dvě knihy ze stejného vydání v drobných detailech jako je kvalita papíru na jednotlivých stránkách se budou lišit).

Pokud se týká zajištění integrity a původu, ty u elektronických dokumentů fungují na zcela odlišných principech než u fyzických objektů, což se odráží nejenom v klasifikaci ED.

Následující obrázek ukazuje navrženou taxonomii ve formě UML diagramu:



Taxonomie vychází ze základního objektu **elektronický dokument**, který představuje prakticky libovolnou informaci, existující v digitální podobě.

Základním směrem rozlišení je **typ**, který klasifikuje elektronické dokumenty podle způsobu, jakým je informace prezentována uživateli:

- Složený (obsahuje v sobě několik typů)
- Zvukový záznam
- Obrazový záznam
 - Statický obrázek
 - Video záznam
- Text
- Datový soubor (jako je databáze, spreadsheet)
- Počítačový program
 - Zdrojový kód
 - Binární kód
- Interaktivní objekt (interaktivní prezentace, interaktivní webové stránky, aj.)

Data obsažená v elektronickém dokumentu mají určitý **formát**, který umožní je reprezentovat. Na nejvyšší úrovni můžeme rozdělit formáty na:

- Textový (kde bitový řetězec vždy představuje kódované znaky abecedy)
- Binární (libovolná posloupnost bitů)
- Otevřený (popis formátu je k dispozici jako norma, doporučení, aj.)
- Uzavřený (popis formátu není k dispozici, je proprietární)

Dokumenty také mohou mít různou úroveň **zajištění své autentičnosti**:

- Bez zajištění
- Digitální značka
- Digitální podpis
- Zaručený digitální podpis

A také se liší ve své **historické hodnotě**, která určuje potřebnou dobu jejich uchování:

- Žádná
- Krátkodobá (do 10 let)
- Střednědobá (do 30 let)
- Dlouhodobá (nad 30 let)

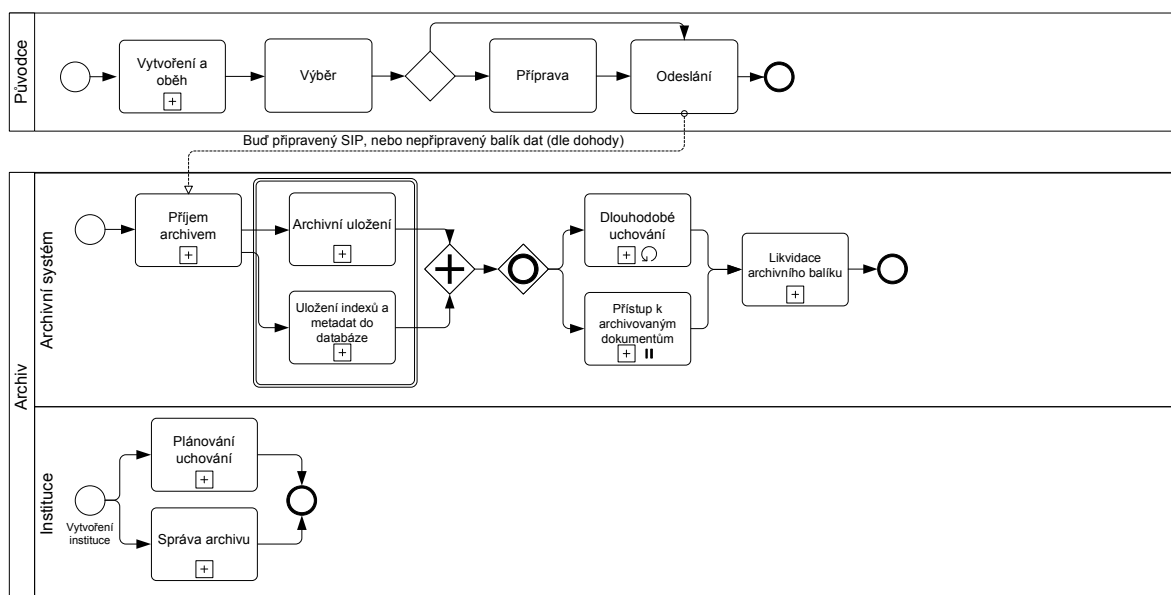
1.4 Životní cyklus elektronického dokumentu

V této kapitole rozebíráme životní cyklus elektronického dokumentu (též tok dokumentu, oběh dokumentu nebo workflow). Díky nutnosti zobecnění popisu pro zachycení celkového obrazu toku dokumentu je výsledný tok jakousi syntézou možných kroků v rámci životního cyklu elektronického dokumentu, kdy konkrétní instance životního cyklu mohou vynechat některé kroky, nebo naopak zahrnout jiné velmi specifické pro zpracovávaný typ dokumentů.

Životní cyklus se zaměřuje především na oběh dokumentu v rámci archivu v souladu s posláním celé studie.

Následující obrázek ukazuje procesy toku dokumentu na dvou úrovních – jednak pokud se týká vlastního toku dokumentu (dále sekce 1.4.1) a dále dlouhodobé

procesy, které běží v rámci archivu a které jsou nezbytné pro jeho chod a důvěryhodnost jeho služeb (dále sekce 1.4.2).



Následující kapitoly popíší detailně jednotlivé kroky životního cyklu.

1.4.1 Vlastní oběh elektronického dokumentu

1.4.1.1 Vytvoření, oběh, výběr, příprava a odeslání ED

Vytvoření a oběh

Probíhá v rámci organizace dle pravidel platných v dané organizaci a může jít o poměrně složitý proces, který se může lišit pro jednotlivé organizace i typy dokumentů. Proto je v tomto popisu celý proces pouze shrnut do obecného složeného procesu, který může být dále rozpracován pro konkrétní podmínky. Z hlediska archivace je důležitý především výstup z tohoto procesu, tedy elektronický dokument a případně metadata, která vhodně popíší proces vzniku a oběhu dokumentu na úrovni potřebné pro jeho uchování (např. pro záznamy je kontext vzniku velmi důležitý).

Detaily procesu ovlivňují také legislativní a normativní předpisy, kdy např. pro státní správu bude v ČR určující zákon o spisové službě, pro organizace vytvářející dokumenty jako záznamy budou relevantní normy jako ISO 15489 či Evropské doporučení MoReq.

Výběr

V rámci oběhu dokumentu u původce musí být implementován krok, kdy se rozhodne, zda daný dokument má být archivován a jakým způsobem. Rozhodnutí o archivaci probíhá typicky na konci oběhu dokumentu v organizaci, kdy dokument již nebude dále měněn, případně kdy existuje jeho významná verze kterou je vhodné archivovat. Rozhodnutí o archivaci se řídí :

- legislativou – např. pro podmínky ČR zákonem o archivnictví a zákonem o spisové službě
- Politikou a procedurami původce
- Požadavky a politikou archivu
- Nebo požadavky jiné třetí strany, která má zájem na dokumentech původce

Zde ukazuje, že archivace bude probíhat u třetí strany – tedy archivu. Je samozřejmě možná i archivace v rámci organizace původce, kdy „archiv“ je pak součástí organizace (jedná se tedy o obecnější vnímání archivace),.

Pro elektronické dokumenty, na rozdíl od papírových, se neuplatňují žádná omezení vyplývající z fyzické podstaty dokumentu a omezeného počtu instancí dokumentu, lze tedy např. absolutně stejný dokument uložit jak lokálně, tak v několika archivech.

Příprava

Vybrané elektronické dokumenty by původce měl připravit do formy vhodné pro předání do archivu. Tato forma je předepsána archivem a její detailní popis by měl být součástí dohody mezi původcem a archivem nebo je definována obecně politikou a standardy archivu.

Tato forma může být buď ve formě kompletního předávacího balíku (SIP - podrobněji viz kapitola 2.3.3), nebo v nějaké dočasné formě, kterou je původce schopen vytvořit a kdy další zpracování do formy standardního předávacího balíku může proběhnout až na straně archivu.

Vhodná příprava předávacího balíku je důležitá pro zajištění dlouhodobé uchovatelnosti a důvěryhodnosti elektronického dokumentu, kdy je potřeba zajistit především:

- Vhodné formáty dokumentu, které jsou přijatelné pro archiv
- Vhodná metadata, která definují potřebné informace týkající se kontextu vzniku, identifikace původce, popisu formátu atd.
- Vhodné zabezpečení dokumentu a metadat, které zajistí jejich autentičnost a integritu při převzetí archivem

Odeslání

Předávací balík nebo jinak dohodnutá forma dat jsou následně doručeny do archivu. Přenos dat může probíhat elektronicky nebo data mohou být doručena fyzicky do archivu na dohodnutém médiu. V případě elektronické komunikace, pokud vlastní zabezpečení předávacího balíku nezajistí dostatečnou autentičnost a integritu dokumentu, musí ji zaručit komunikační protokol.

1.4.1.2 Příjem archivem

Příprava příjmu

Archiv může provádět pro určité typy předání přípravné kroky, kdy jsou dokumenty a metadata upraveny tak, aby dále mohli být archivem přijaty standardním způsobem. Jedná se tedy spíše o výjimky, kdy původce z určitých důvodů nemůže předat data ve standardní formě a deleguje některé úkoly přípravy dat na archiv. Může se jednat například o:

- Skenování (v případě, že původce nemůže předat dokumenty v elektronické podobě)

- Normalizaci formátu (pokud původce není schopen dodat dokumenty v některém z požadovaných formátů)
- Doplnění metadat

Proces přípravy může ovlivnit autentičnost dokumentu, pokud je tedy proces přípravy potřebný, je nutné pomocí vhodné spolupráce archivu s původcem zajistit její zachování.

Ověření předávacího balíku

Po přijetí předávací balíku v digitální formě do archivu, musí být provedeno jeho plné ověření:

- Formáty dokumentů musí být v souladu s politikou archivu a musí být ověřena jejich správnost a shoda se standardem (pokud možno automatická kontrola²⁴ nebo alespoň manuální kontrola)
- Metadata musí obsahovat všechny potřebné údaje a jejich formální prezentace musí odpovídat požadavkům archivu
- Hodnoty polí metadat musí být ve shodě s požadavky a politikou archivu
 - Případně mohou být i ověřena proti obsahu dokumentu
- Prvky zabezpečující autentičnost a integritu předávacího balíku musí být ověřeny (musí být zřejmý původ z hlediska předání do archivu)
- Forma a způsob předání balíku musí odpovídat požadavkům archivu a podmínkám dohodnutým s původcem.

Záznam o převzetí balíku včetně výsledků ověření musí být pořízen archivem a udržován spolu s dokumentem jako součást jeho procesních metadat. Výsledky ověření tvoří základ pro důvěryhodné uchování dokumentu.

Odmítnutí předávacího balíku

Pokud předávací balík neodpovídá požadavkům a politikám archivu, tento jej musí odmítnout a informovat původce o důvodech. Původce pak může vytvořit nový předávací balík, který ale opět musí projít celým procesem.

Záznam o odmítnutí předávacího balíku musí být také uložen v záznamech archivu.

Vytvoření archivního balíku

Pokud je předávací balík v pořádku, je upraven a doplněn do formy archivního balíku (AIP – Archival Information Package), tedy do přesné digitální podoby, která bude uložena v archivu. Tato úprava musí probíhat takovým způsobem, který zachová autentičnost dokumentu. Lze tedy předpokládat, že půjde spíše o rozšíření předávacího balíku nebo případné zapouzdření než o jeho zásadní změny. Tyto úpravy zahrnují především:

- Doplnění metadat o jednoznačnou identifikaci balíku, časové značky, údaje potřebné pro dlouhodobé uchování (jako jsou odkazy na archivní balíky obsahující podrobný popis formátu nebo programy pro zobrazení dat v daném formátu), doplňující údaje o kontextu dokumentu (jako může být například odkaz na archivní balík obsahující smlouvu mezi původcem a archivem o předávání a uchování dokumentů)

²⁴ Existují nástroje které ověří shodu formátu dokumentu s daným standardem, jedním z takových nástrojů je např. JHOVE - JSTOR/Harvard Object Validation Environment (<http://hul.harvard.edu/jhove/>) nebo Global Digital Format Registry (<http://hul.harvard.edu/gdfr/>).

- Formátování metadat do vhodného schématu
- Opatření dat obálkou, která umožní identifikovat jednotlivé části balíku
- Opatření balíku bezpečnostními prvky, které zajistí integritu balíku po dobu jeho uchování.

1.4.1.3 Archivní uložení

Vytvořený archivní balík je uložen v archivu v několika kopiích tak, aby bylo zaručeno jeho zachování v případě narušení jedné kopie (nebo selhání systému, na kterém je daná kopie uložena).

1.4.1.4 Uložení indexů a metadat

Souběžně s uložením archivního balíku, je potřebné vytvořit indexy, které umožní jeho pozdější opětovné nalezení a použití.

Vytvoření indexů z metadat

Metadata archivního balíku budou použita pro vytvoření řady indexů ukazujících na tento balík dle různých kritérií, které archiv používá pro vyhledávání a identifikaci uložených dokumentů. Extrakce dat pro indexy by měla být automatická s případnými manuálními doplňky nebo opravami.

Uložení indexů v databázi

Vytvořená indexová data jsou uložena v databázích. Ochrana přístupu do těchto databází a zajištění dostupnosti indexů po celou dobu uložení dokumentů jsou stejně závažné jako ochrana a uchování vlastního dokumentu resp. archivačního balíku, který jej obsahuje, neboť při zničení nebo poškození indexů nelze daný dokument vyhledat a je tedy efektivně ztracen.

1.4.1.5 Dlouhodobé uchování

Kontrola stavu

Jedním z nejdůležitějších úkolů probíhajících během uchování dokumentů, jsou kontroly, které zjišťují, zda je dokument nadále čitelný a přístupný pro potenciální uživatele. Kontroly musí být prováděny kontinuálně podle vhodně stanovených plánů. Mezi hlavní kontroly patří:

- Kontrola medií, kde se kontrolují vlastnosti medií na kterých je uložen digitální obraz archivního balíku, zda nedochází k chybám při čtení dat. Podrobněji jsou popsány postupy v kapitole 2.3.4.3. Pro rozsáhlý archiv nebude možné samozřejmě testovat všechna média, plán kontroly bude tedy počítat spíše s namátkovým výběrem se zohledněním životnosti medií.
- Kontrola formátu – na základě vývoje v informačních technologiích bude nutné kontrolovat, zda všechny formáty uložené v archivu jsou a budou v blízké budoucnosti čitelné a použitelné. Pro identifikace přítomných formátů lze vycházet z metadat, ověření čitelnosti lze provést pro vybrané vzorky uložených dat (např. pro nové verze programů ověřit, že zobrazí bez problémů dokumenty vytvořené v předchozích verzích atd.). Pro formáty, kde hrozí ztráta čitelnosti, musí být naplánovány akce, které ji obnoví a zaručí do budoucna. Podrobnější popis ohledně kontroly formátu a možných přístupů k zachování čitelnosti je v kapitole 2.3.2.

- Kontrola zabezpečení – kontrola, zda použité metody zabezpečení uložených archivních balíků jsou stále účinné. Pokud např. díky vývoji v IT je nějaký mechanismus (jako je třeba hašovací funkce) zastaralý, je nutné naplánovat jeho nahrazení ekvivalentním novým mechanismem. Podrobnější rozbor k této tématice je v kapitole 2.3.5.
- Kontrola indexů a referencí – kontrola, že dokument je stále vyhledatelný podle indexů a že reference, které jsou součástí metadat, odkazují na existující objekty.

Kontrola systémů

Kromě kontroly vlastních dokumentů, musí probíhat také kontinuální kontrola všech systémů archivu na jejich spolehlivost, dostupnost, atd. a také kontrola jejich technické relevantnosti. Pro případné problémy v systému (zastaralé součásti atd.) je nutné plánovat jejich nahrazení.

Změna medií

Pokud kontrola média ukáže nějaké problémy, jsou data přenesena na nové médium. Tyto akce musí být podchyceny v záznamech archivu.

Změna formátu

Pokud kontrola formátu ukáže rizika, jednou z možných akcí je změna formátu na nový, který zaručí čitelnost do budoucna. Vzhledem k tomu, že změna formátu je typicky poměrně velkým zásahem do uloženého dokumentu, je vhodné:

- Vypracovat detailní popis změny (včetně např. zdrojových kódů transformačních programů), který bude také uložen v archivu a nadále referován z archivního balíku
- Zaznamenat průběh změny a připojit ho jako metadata k výslednému archivnímu balíku
- Zachovat dokument v původním formátu v archivním balíku (nový formát je tedy přidán „navíc“).

Rozšíření/prodloužení platnosti formátu

Další možné akce pro udržení čitelnosti formátu jsou zaměřeny na to, aby byl formát nadále použitelný tak, jak je uložen. Není tedy nutné měnit dokument uložený v archivním balíku, ale je nutné připravit jiné postupy a nástroje, jak jej zobrazit pomocí dostupných prostředků IT.

Mezi hlavní technologie v této oblasti patří tzv. emulace, kdy je vytvořen virtuální počítač, na kterém lze spustit programy potřebné pro zobrazení dokumentu.

Mezi další přístupy v této oblasti (které jsou vhodné spíše pro specifické případy) patří:

- Zpětná kompatibilita (nově dostupné programy přesně zobrazí starší verze formátů dokumentů)
- Vytvoření nového zobrazovacího programu pro nové platformy
- Uchování HW
- Tzv. „digitální archeologie“, kdy je zodpovědnost za interpretaci formátu přenesena na budoucí uživatele, archiv přispívá pouze uchováním co možná nejpresnějšího popisu formátu (akcí z jeho strany je tedy vhodné rozšiřování popisu formátu).

Prodloužení/zlepšení zabezpečení

Pokud kontrola zabezpečení ukáže nějaké problémy, musí archiv nahradit nedostatečné bezpečnostní prvky novými. Může se jednat o výměnu kryptografického algoritmu, změnu protokolu, přidání nového mechanismu aj.

Oprava/úprava indexů a odkazů

Pokud index, nebo reference mezi balíky odkazuje na neplatný nebo neexistující objekt, je třeba jej aktualizovat.

Migrace systému

Pokud některé části systému zastarají a nebudou dále moci spolehlivě plnit své funkce musí být vyměněny za nové. Změny by neměly významně omezit fungování archivu, proto musí být pečlivě naplánovány a vyzkoušeny. Také architektura systému archivu musí s těmito průběžnými změnami počítat (viz podrobnější diskuze v kapitole 2.3.6).

Obnova po mimořádné události

V případě rozsáhlé mimořádné události (přírodní katastrofa aj.), kdy je zničena nebo zneprístupněna nějaká část archivního systému, je nutné postupovat dle předem vypracovaného plánu obnovy tak, aby byla zajištěna opětovná funkce archivu a obnoveny všechny uložené dokumenty (nebo možné maximum).

1.4.1.6 Přístup k archivovaným dokumentům

Způsob a rozsah přístupu pro dané komunity uživatelů je součástí politiky archivu a tato zase vychází z platné legislativy.

Vyhledání dokumentu

Na základě kritérií uživatele musí být vyhledán daný archivní balík (nebo množina balíků) v indexech a následně i jeho uložení na určitých médiích.

Příprava výstupu

Vyhledaný archivní balík musí být upraven do tvaru vhodného pro uživatele (tzv. výstupního balíku – DIP), kdy bude vybrána potřebná podmnožina metadat a vybrány formáty dokumentu srozumitelné pro daného uživatele. Možné jsou i případné transformace formátů, pokud je archiv podporuje.

Součástí metadat mohou být informace podporující integritu a autentičnost výstupního balíku z archivu.

Předání výstupu

Výstupní balík je předán uživateli buď on-line pomocí vhodného protokolu, který zaručí spolehlivý a bezpečný přenos dat, nebo off-line (na médiu, vytištěné, ...).

1.4.1.7 Likvidace archivního balíku

Na základě politiky archivu mohou být po určité době některé archivní balíky označeny pro likvidaci a vymazány z archivu. Je zřejmé, že zde politika a příslušné procedury pro likvidaci archivních balíků musí být zcela v souladu s legislativou. Likvidace znamená vymazání všech kopií archivních balíků a úprava indexů, referencí a externě uložených metadat tak, aby byla zachována jejich integrita a aby

bylo prokazatelné, že dokument byl po určitou dobu uložen v archivu a následně vymazán podle platných předpisů a postupů.

1.4.2 Důležité dlouhodobé úkoly z hlediska instituce archivu

Kromě vlastního toku dokumentu v archivu je také velmi důležité, aby v archivu fungovaly dlouhodobější procesy, které řídí funkci archivu jako celku.

1.4.2.1 Plánování uchovávání

Na nejvyšší úrovni musí být provedeno plánování strategie uchovávání pro dané cílové komunity uživatelů a typy uchovávaných dokumentů. Strategie bude východiskem pro klíčové standardy archivu. Strategie i z ní vycházející standardy musí být pravidelně konfrontovány s vývojem jak technologií, tak i ostatních aspektů, které ovlivňují požadavky cílové komunity.

Hlavní úkoly v této oblasti jsou:

Vytvoření strategie dlouhodobého uchovávání

Identifikuje klíčové uživatele systému, jejich požadavky, ideální cílový stav a hlavní kroky jak jej dosáhnout.

Vytvoření standardů pro dlouhodobé uchovávání

Na základě strategie jsou definovány hlavní standardy pro digitální archiv, které budou zásadně ovlivňovat jeho funkce. Týkají se formátů uchovávaných dat, podporovaných aplikací, platformy archivu, využití dostupných národních a mezinárodních norem, atd.

Monitorování požadavků komunity uživatelů

Monitorování vývoje technologie

Strategické plánování není pouze jednorázové, je nutné průběžně sledovat jak vývoj komunity uživatelů a s ní spojených relevantních společensko-ekonomických faktorů, tak vývoj technologie a přizpůsobovat strategii novým podmínkám.

1.4.2.2 Správa archivu

Na základě definované strategie musí archiv vytvořit sadu provozních politik a postupů, které umožní správu archivu jako celku. Opět se nejedná o statickou záležitost, politiky a postupy se vyvíjí podle potřeby.

Správa zahrnuje především:

Vytvoření politik a postupů a jejich údržba

Jedná se o detailní rozpracování procesů potřebných pro funkce archivu, zejména:

- Archivační politika
- Provozní řád
- Bezpečnostní politika
- Plán obnovy a kontinuity (DRP)

Detailnější popis této organizační stránky archivu je uveden v kapitole 2.4.

Vytvoření smluvních podmínek s původci dokumentů a uživateli archivu

Vztahy s třetími stranami (hlavě s původci dokumentů a uživateli dokumentů) by měly být smluvně upraveny tak, aby byly definované poskytované služby, práva a povinnosti jednotlivých stran.

Správa informačního systému

Jako každý informační systém potřebuje i archiv průběžnou správu svého informačního systému, úkoly správy zahrnují:

- Příprava a provedení implementace systému
- Monitorování funkcí systému
- Podpora uživatelů
- Správa konfigurace systému
- Správa přístupu do systému
- Preventivní údržba
- Příprava a provedení migrace systému

Audit procesů, dat a systémů

Systém archivu by měl procházet pravidelným auditem, kde se ověří shoda stavu systému, postupů a organizace archivu s relevantními předpisy a normami, jejich dostatečná dokumentace a jejich dodržování.

Správa uživatelů/zákazníků

Tato oblast se týká správy vztahů s uživateli/zákazníky.

1.5 Rozdílová analýza workflow papírových a elektronických dokumentů

Rozdílová analýza workflow papírových a elektronických dokumentů je poměrně jednoduchou záležitostí. Po věcné stránce se workflow papírových a elektronických dokumentů neliší. Také pro workflow elektronických dokumentů platí všechna věcná stádia archivnictví a spisové služby, tak jak jsou popsána a graficky znázorněna v kapitole 1.2.

Rozdíly workflow papírových a elektronických dokumentů jsou výrazné ve formální rovině, a to vzhledem k tomu, že workflow dokumentů v elektronické, tedy nehmotné formě se řídí jinými bezpečnostními a organizačními a z toho vyplývajícími právními pravidly než workflow papírových, resp. hmotných dokumentů.

Lze říci, že formální rozdíly mezi workflow papírových a elektronických dokumentů jsou podrobně popsány v kapitole 1.4. Dle našeho názoru právě specifikace těchto speciálních nezbytných prvků, uvedených v kapitole 1.4 ve vztahu k elektronickým dokumentům, představuje současně rozdílovou analýzu workflow papírových a elektronických dokumentů.