UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

VLOGA ELEKTRONSKEGA ARHIVA V SODOBNEM PODJETJU

Ljubljana, maj 2005 **PRIMOŽ BERGER**

IZJAVA

Študent Primož Berger izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Aleša Groznika, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____.

Podpis:

_____

KAZALO

1. Uvod

Človek že stoletja dolgo zapisuje raznovrstne vsebine na različne nosilce. V začetku so bili to predvsem les, kamen, kasneje papir, danes pa, vsaj v poslovnem svetu, že prevladuje elektronski zapis dokumentov. Ena največjih težav, s katerimi se danes spopadajo v podjetjih, je nadzor vedno večjega števila dokumentov. Sistemi za elektronsko obvladovanje dokumentacije predstavljajo vitalni del organizacije in pomenijo povečanje produktivnosti, dodane vrednosti, izboljšajo komunikacijo s poslovnimi partnerji in hkrati tudi zmanjšujejo stroške celotnega poslovanja. Raziskava neke hiše, ki se ukvarja z tržnimi raziskavami, kaže na to, da zaposleni v določenih panogah v povprečju 80% delovnega časa porabijo za iskanje informacij. Ta podatek pa ni pomemben le stroškovno z vidika porabe mrtvega časa. Vpliva tudi na motiviranost zaposlenih, predvsem pa zmanjšuje nadzor nad procesi.

Vsi problemi klasičnega arhiviranje se pri digitalnem formatu še potencirajo in nekateri izmed njih so tudi podrobneje obdelani v diplomski nalogi. Za večino izpostavljenih težav sem ponudil tudi ustrezne praktične rešitve. Zavedati se je treba dejstva, da je na področju informatike razvoj tako hiter, da mu tudi strokovnjaki iz specializiranih podjetij le stežka sledijo. Novosti se v panogi pojavljajo tako rekoč dnevno. Izjema niso niti sistemi za upravljanje z dokumenti, ki so dobili sodobno podobo. Vedno bolj je prisotno vprašanje, kdaj je obstoječ sistem tako zastarel, da so spremembe nujne oz. katere novosti je smiselno uvesti. Vse skupaj je močno povezano z rentabilnostjo. Investicija se namreč mora povrniti, poleg tega pa je stalno spreminjanje in uvajanje novosti za uporabnika moteče in mu dela ne olajšuje. Elektronsko upravljanje z dokumenti se v slovenskem prostoru že precej uporablja. V veliki večini gre za povzemanje tujih rešitev, zlasti velika luknja pa zeva na področju zakonodaje, ki je mnogo pomembnih vprašanj slabo rešila.

Z rastjo uporabe elektronskih dokumentov in elektronsko podpisanih dokumentov postaja varno arhiviranje nastale dokumentacije v izključno elektronski obliki vedno bolj pomembno vprašanje. Pri poslovanju modernega podjetja so informacije namreč ključnega pomena. V primeru ogroženosti informacij je v nevarnosti obstoj podjetja kot celote. S pojmom varno je mišljeno tudi elektronsko arhiviranje na način, ki zagotavlja elektronskim dokumentom verodostojnost v upravnih ali poslovnih postopkih in legitimnost na sodišču.

Diplomsko delo sem si zamislil kot kratek pregled sistemov za elektronsko upravljanje z dokumenti, nato pa se bom v naslednjem poglavju osredotočil na končno fazo življenjskega cikla dokumentov, to je končno arhiviranje v elektronski obliki. V poglavju sem opredelil prednosti in slabosti digitalnega arhiviranja, opisal v svetu uveljavljen model elektronskega arhiva, tehnične in pravne zahteve… Naslednji dve poglavji obravnavata oddajanje storitev elektronskega arhiviranja zunanjemu ponudniku in uvajanje sistema za varovanje in zaščito informacij v podjetju. Praktični primer obravnava elektronsko storitev Pošte Slovenije moja.posta.si, ki ponuja tudi storitve elektronskega arhiviranja za fizične osebe.

2. Sistem za elektronsko upravljanje z dokumenti

2.1 Kaj je dokument?

Do nedavnega smo na dokument gledali kot na statičen objekt (tekst ali sliko), največkrat na papirju, ki ima s svojimi lastnostmi nepogrešljivo vrednost za določen subjekt. Danes je to za dokumente že zelo pomanjkljiva definicija.

Dokument se je skozi čas preoblikoval iz statične v dinamično kategorijo, ki se časovno spreminja in je lahko besedilo, zvočni ali video zapis, program, ki kroži po spletu, del CAD risbe… Dokument je tako objekt, je zbirka kazalcev in odnosov, je sočasna povezava različnih komponent in aktivnosti, je dinamičen, in je osnova in temelj poslovne integritete (Jakovljevič, 1998, str. I-63). Posamezen dokument je lahko sestavljen iz več delov. Med najobsežnejše oz. najzahtevnejše dokumente sodi dokumentacija, ki se hrani v arhivih. Dokument je lahko tudi sinonim za pismeno potrdilo ali dokazilo o nekem dejstvu, hkrati s tem pa tudi dokaz obstoja nekega upravno-opravnega ali drugega dokumentiranega dejanja ali stanja (Novak, 2002, str. III-60).

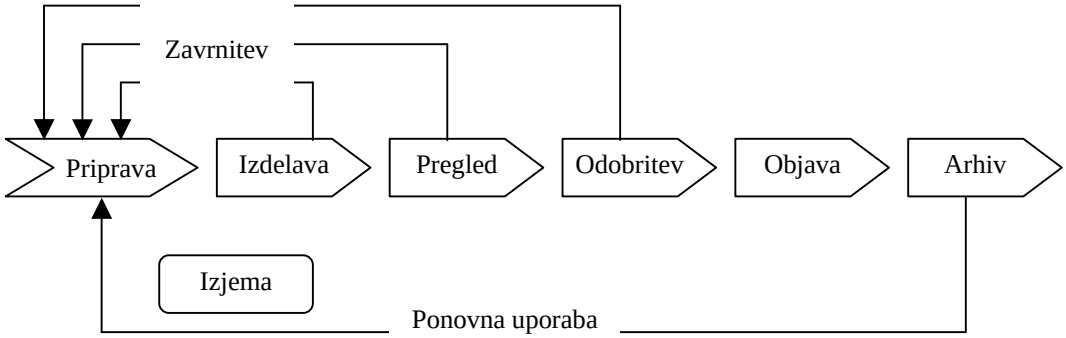
Dokumenti kot osnovni nosilci informacij vsebujejo zapise o preteklih transakcijah in lahko služijo kot medij za ponazarjanje odvijanja poslovnih dogodkov. Kritična narava dokumentov in njihove uporabe narekuje potrebo po orodjih, ki bi zagotavljala potrebno zanesljivost, varnost, integriteto in razpoložljivost informacij vsem uporabnikom ob vsakem času. S temi zahtevami pa se od samega začetka uporabe srečujejo uporabniki strukturiranih podatkov, ki so shranjeni npr. v relacijski bazi podatkov. Sistemi, ki so danes prisotni na tržišču, so načrtovani tako, da omogočajo enostavno integriteto informacij, tako dokumentov kot elektronske pošte, s poslovnimi procesi. Upravljanje z dokumenti običajno temelji na skupnem odlagališču oz. bazi in ki služi shranjevanju in upravljanju dokumentov. Takšno odlagališče zagotavlja organiziranje, preiskovanje, spremljanje verzij in upravljanje s skupnimi dokumenti (Bakan Toplak, 1999, str. I-13).

V zadnjem desetletju je prišlo do izredno hitrega razvoja inženirskih tehnologij, ki obvladujejo celoto delovnih procesov podjetja in so znani kot sistemi za upravljanje življenjskega cikla proizvoda (angl. Product Lifecycle Management). Po tej antologiji in ker je dokument dejansko tudi proizvod, lahko uporabljamo pojem upravljanja življenjskega cikla dokumenta (angl. Document Lifecycle Management). Ugotovimo lahko, da so dokumenti tako proizvodi, ki imajo svojo kakovost, ceno in življenjsko dobo (Čufer, 2004, str. IV-10).

Dokumenti imajo torej na svoji poti od nastanka do arhiva več različnih stanj. Pot prehajanja med temi stanji imenujemo življenjski cikel dokumenta. Vedno sta v proces vključena najmanj avtor oz. tvorec dokumenta in naslovnik oz. prejemnik dokumenta. V zahtevnejših okoljih je med nastankom in arhivom še mnogo drugih stanj in oseb, ki sodelujejo pri delovnem toku znotraj vsake faze življenjskega cikla. Z velikostjo organizacije, kjer se

dokument uporablja, se veča tudi zahtevnost postopkov, ki so povezani z njim. Za bolj učinkovito upravljanje delovnih procesov je potrebno uporabiti tudi nekatere avtomatizirane postopke, kot npr. časovna sprožitvena pravila, ki omogočajo delovanje sistema bolj neodvisno od človeških napak. Gre predvsem za reševanje težav zaradi nadomeščanja, odsotnosti ali poteklih rokov, v katerih se mora določena faza izvesti. Osnovni življenjski cikel dokumenta prikazuje Slika 1.

Slika 1: Osnovni življenjski cikel dokumenta



Vir: Kroflič, Jerman Blažič, 2004, str. VI-55.

2.2 Opredelitev sistemov za elektronsko upravljanje z dokumenti

Sistem za elektronsko upravljanje z dokumenti, s kratico SEUD (angl. Electronic Document Management System), lahko opredelimo kot informacijski sistem, katerega naloga je, da upravlja z dokumenti v elektronski obliki ter jih nadzira skozi njihov celoten življenjski cikel od nastanka do arhiviranja. Celoten spekter funkcij SEUD je usmerjen na nastajanje, ravnanje, distribucijo, pregledovanje verzije oz. različice, pretok, varnost in shranjevanje dokumentov (Kočevar, 2002, str. 16).

Raziskave svetovalnih in raziskovalnih inštitutov v ZDA kažejo (Žerko, 2000, str. III-8):

- 90% dokumentov, s katerimi imamo opravka vsak dan, je pomešanih,
- zbiranje, razvrščanje in razpošiljanje dokumentov predstavlja 90% tipičnih opravil v pisarni,
- 7,5 do 15% dokumentov se izgubi in za njihovo iskanje porabimo 30% svojega časa,
- stroški za hranjenje informacij na papirju znašajo $4,55/MB, na optičnem disku pa $0,06/MB,
- v podjetjih naredijo povprečno 19 kopij istega dokumenta,
- podjetja hranijo 90% svojega znanja na papirjih in s prehodom na elektronsko obravnavanje dokumentov lahko zmanjšajo obseg arhiva za 60 do 80%,
- 5% vseh stroškov z arhiviranjem dokumentov predstavlja oprema, 20% prostor in kar 70% odpade na stroške dela,
- stroški dela za arhiviranje vsakega dokumenta znašajo $20, za iskanje založenih $120 in kar $250 za »restavriranje« podatkov iz izgubljenega dokumenta.

Po uspešni implementaciji SEUD sistema se lahko nadejamo (Žerko, 2000, str. III-9):

- produktivnost (odzivni časi) se poveča za 25 do 50%,
- transakcijski časi se zmanjšajo celo do 75%,
- stroški arhiviranja (prostor) se zmanjšajo za 60 do 80%.

Problema upravljanja z dokumenti so se najprej pričeli zavedati v podjetjih, ki dejansko uporabljajo zelo velike dokumente, ki nastajajo na več lokacijah, so izdelani timsko, različnih formatov in se spreminjajo skozi čas. Podjetja dokumente in informacije razumejo kot ključ do kakovosti in poslovnega uspeha ter posledično večje konkurenčnosti samega podjetja.

Večji delež sistemov za upravljanje z dokumenti je integriranih in združujejo tako informacije zapisane na papirju kot v elektronski obliki. Zapis na papirju lahko hkrati uporablja le en človek, dokumenta ni vedno mogoče razmnožiti in razdeliti v kopije, če pa že, lahko to pripelje do številnih, pogosto neskladnih različic dokumenta. Razvoj je šel logično pot in tako se lahko elektronske informacije hkrati pojavijo na toliko mestih, kot je treba. Tehnologija podatkovnih baz spreminja pravilo enkratnega pojava originala dokumenta, ker omogoča uporabnikom hkraten dostop do informacije. Integracija v informacijski tehnologiji poleg tega omogoča, da en človek opravi vse korake procesa, od začetka do kraja življenjskega cikla dokumenta. Posamezne faze je poprej namesto generalista opravil specialist za določeno fazo. Ko odpravimo podajanje, zastoje in napake, ki so posledica implementacije SEUD, pride v podjetju do neverjetnih izboljšav glede časa, natančnosti in stroškov. Sodobne komunikacijske mreže omogočajo, da imajo središče in dislocirani oddelki enake dokumente in jih hkrati obdelujejo. Dokumenti so fleksibilni, pojavljajo se na različnih krajih hkrati. To pomeni prilagodljivo strukturo podjetja , ki optimalno izpolni zahteve poslovnih partnerjev (centralizacija, decentralizacija ali splet obeh).

Danes se še vedno mnogo podatkov v informacijski sistem vnese ročno. Avtomatski vnos pa mora vsebovati naslednje postopke (Nose, 2001, str. I-99):

- *Preverjanje podatkov*: točnost podatkov je odločilnega pomena v vsaki aplikaciji za zajem dokumentov. Napačni podatki ponavadi pomenijo izgubo informacije in tudi skeniranega dokumenta. Napačni podatki v bazi podatkov so lahko zelo nevarni.
- *Odprava napak*: odločujoči faktor pri izbiri aplikacije za razpoznavanje znakov ni točnost in hitrost prepoznavanja, ampak zmožnost in cena popravkov napak, ki so nastale pri tem procesu.
- *Obdelava obrazcev*: avtomatizacija pri obdelavi dokumentov v obliki znanih form zahteva napredno tehnologijo pri prepoznavanju znakov. Vsebovati mora:
  - prepoznavanje znakov na določenih poljih,
  - prepoznavanje nestandardnih podatkov,
  - možnost izbire polja skeniranja.

2.3 Pretvorba papirnih dokumentov v elektronsko obliko

Zajem dokumentov se v teoriji lahko opredeli kot proces pretvarjanja papirnih dokumentov v uporabno elektronsko obliko. Nakup strojne in programske opreme je z vidika stroškov enkratna investicija, medtem ko so stroški dela za podjetje stalna obremenitev. Prihranki pri stroških dela tako po določenem času močno presežejo začetno investicijo.

Zajem dokumentov zajema različne kompleksne korake in odločitve (Nose, 2001, str. I-102):
- sestavljanje in pretvorba papirnih dokumentov v digitalne slike,
- zagotavljanje, da so slike uporabne,
- izpis podatkov, potrebnih za indeksiranje slik ali celotnega besedila,
- izvoz slik in podatkov v delovni tok ali aplikacije,
- integracija razpoložljivih tehnologij v lastni sistem,
- upravljanje delujočega sistema.

Morda uvedba sistema za avtomatiziranje ročnega dela in optično prepoznavo dokumentov na prvi pogled deluje dokaj enostavno, a ni tako. Brez modulov prilagojenih različnim standardom je nemogoče vzpostaviti zanesljiv sistem. Takšna nadgradnja pogosto zahteva kompletno prestrukturiranje obstoječega sistema, kar poraja še dodatne probleme.

Po implementaciji rešitve se lahko nadejamo naslednjih izboljšav (Nose, 2001, str. I-102):
- potrebno je manj ročnega dela za povzetek podatkov in njihovo hrambo v podatkovni bazi,
- slike so bolj berljive,
- velikost datotek je manjša, kar poceni shranjevanje in izboljša prenos po mreži,
- zmanjšajo se stroški indeksiranja,
- sistemski viri so bolj produktivni in lažje upravljivi,
- nadgradnja sistema je enostavnejša.

Na kratko bom opredelil še vse štiri faze pri zajemu dokumentov (Nose, 2001, str. I-102):
- *Predskeniranje, priprava dokumentov*: je ključna faza pri pretvorbi v digitalno obliko. Pravilno izvršena priprava je pomembna, da se posamezni dokumenti ne izgubijo in da vse kritične vsebine resnično vnesemo v sistem. Pri kompleksnih dokumentih moramo paziti tudi na vrstni red skeniranja posameznih listov. Faze predskeniranja so:
  - prepoznavanje telesa dokumenta,
  - selekcija strani, ki se bodo skenirala,
  - sestavljanje vrstnega reda obdelave posameznih strani,
  - dokumentom določiti prioriteto in organizirati (odpreti kuverte, poravnati robove…),
  - določiti potrebno strukturo dokumenta,
  - dostaviti je potrebno vsebine operaterju skeniranja.

- *Pretvorba dokumenta v berljivo sliko*: vsebuje več faz, kot so:
  - Skeniranje: določimo velikost strani, vsebino strani (besedilo, tabele, slike, grafikoni), enostransko ali dvostransko popisanost, resolucijo skeniranja, format slik…
  - Obdelava slik skeniranega dokumenta: zajema rotacijo slike v pravilni položaj, filtriranje, izboljšanje kontrasta, odstranjevanje robov, ozadja… Kakovostna obdelava nam izboljša berljivost dokumentov, prepoznavanje znakov…
  - Kontrola kvalitete slike: preveri, če so resnično vsi zajeti dokumenti v elektronski obliki berljivi. Če kontrola ugotovi neberljivost, gre gradivo znova v skeniranje.
- *Zajem podatkov, indeksiranje in preverjanje*: obstajajo trije ključni koncepti:
  - Indeksiranje po ključnih besedah: ena ali več besed se uporablja za ključ do dokumenta. Pogosta je tudi uporaba identifikacijskih številk, na podlagi katerih aplikacija npr. dokument shrani v pravilno mapo.
  - Indeksiranje po celotnem tekstu: zajame vse besede v dokumentu. Ta način je uporaben, ko je potrebno shraniti celotno vsebino in kasneje lahko iščemo dokument po določenih besedah v dokumentu.
  - Vnos podatkov: uporablja se v aplikacijah, katerih osnovni namen je procesiranje obrazcev in je slika dokumenta pripomoček za končen ročni ali avtomatski vnos podatkov v sistem. Po zapisu v podatkovno bazo se slika dokumenta lahko preusmeri v arhivski sistem ali pa se v celoti izbriše.
- *Izvoz dokumentov v sistem za elektronsko upravljanje z dokumenti*

2.4 Pasti pri uvajanju dokumentarnega sistema

Uvedba elektronskega dokumentarnega sistema ima številne prednosti in postaja nepogrešljivo orodje pri vsakodnevnem poslovanju. Z napačnim pristopom pa se kaj hitro lahko sprevrže v nočno moro. Eden izmed ključnih dejavnikov uspešne implementacije sistema je zmožnost predvidevanja različnih vplivov, ki bi lahko na kakršenkoli način ogrozili zmožnost predvidevanja različnih vplivov, ki imajo potencialni vpliv na kakovost delovanja celotnega dokumentarnega sistema. Ti vplivi so opisani v nadaljevanju.

Definicija obsega dokumentarnega sistema: v začetni fazi je zelo pomembno pravilno načrtovanje obsega projekta in dinamika njegovega izvajanja. Preobsežno zastavljen projekt zlepa ne bo dal želenih pričakovanj v kratkem času. Tak projekt, ki vključuje večje število uporabnikov, potrebuje v osnovi jasno definirane vse cilje, poti, uporabnike, prioritete za delovanje v sistemu, varnostno shemo, vrsto dokumentov in procesov ter dinamike poslovanja. Zaradi prevelikih pričakovanj lahko pride do odpora oseb, ki takoj po uvedbi začnejo zavestno delovati proti dosegi cilja Po drugi strani pa je uvedba t.i. mini dokumentarnega sistema smiselna, če rešuje specifično težavo. Preozko usmerjen sistem ne posega na druga področja znotraj podjetja, večji del sistema je odvisen od manjše skupine uporabnikov, posveča se mu premalo pozornosti, kar lahko sproži zaustavitev…

Uporabniki - šolanje in uporaba: informacijska tehnologija je relativno lažje obvladljiva kot njeni uporabniki. Pričakovati je odpor do novosti, torej uporabe elektronskih dokumentov. Tako je prilagoditev uporabniških vmesnikov in navodil eden izmed ključnih dejavnikov, ki zagotovi uspešnost delovanja elektronskega sistema za delo z dokumenti.
Oprema: informacijska tehnologija je relativno draga. Ponavadi so želje eno, dejanske zmožnosti pa drugo. Varčevanje pri nakupu informacijske opreme se kaj kmalu pokaže na slabšem poslovanju podjetja. Zelo je kritična predvsem tehnologija za pretvorbo papirnatih dokumentov v elektronsko obliko. Zadostiti mora t.i. minimalnim pogojem vidljivosti vsebine. Slaba informacijska oprema povzroči še ostale stroške, kot npr. stroške ročnega dela in izgube delovnega časa.
Prevelika pričakovanja: osnovni namen takšnega sistema je elektronsko upravljanje in arhiviranje dokumentov. Moderni sistemi imajo poleg tega še druge funkcije, vendar to ni njihov osnovni namen. V dokumentarnih sistemih so prisotne le zato, da je upravljanje z dokumenti lažje in bolj dovršeno. Tak sistem npr. ne more nadomestiti osnovnih aplikacij za analiziranje podatkov, saj bi tako zgubil svoj osnovni namen.
Pričetek implementacije: prej ko se uvede sistem za elektronsko obvladovanje in arhiviranje dokumentov, prej se lahko pričakujejo učinki, tako poslovni kot finančni. V posameznih poslovnih procesih sodeluje več dokumentov, ki nastajajo v različnem času in prostoru. Za lažji vpogled v vse dokumente se lahko uporabi hiperlink (angl. Hyperlink), ki povezuje dokumente enega dogodka ali procesa v celoto. Vodenje projekta uvedbe sistema za elektronsko upravljanje z dokumenti se zaupa osebi, ki ima veliko opravka z dokumenti, je seznanjena z organizacijo in potekom poslovnih procesov v podjetju in ni nujno, da izhaja iz informacijskega oddelka. Ostali oddelki, npr. informatiki, pa znotraj projekta aktivno sodelujejo pri implementaciji sistema in integraciji z obstoječim informacijskim sistemom.
Varnostna politika in omejevanje vsebin: logično je, da je potrebno znotraj dokumentarnega sistema vzpostaviti določeno politiko dostopa do samega sistema in do dokumentov v njem. V primeru nepooblaščenega dostopa lahko pride do ogromne škode, bodisi za posameznika ali za podjetje. V praksi prevladuje omejevanje dostopa do skupine dokumentov. Uporabniki lahko dostopajo do dokumentov, ki jih potrebujejo pri vsakodnevnem delu. Globje omejevanje dostopa je teoretično možno, praktično pa ni izvedljivo v celoti. To pomeni, da je potrebno ročno selekcionirati, kateri del vsebine posameznega dokumenta je viden in kateri ne. Ta omejitev je odvisna od posameznika, ki določa te omejitve in pripeti se lahko, da kriterij omejevanja ni vedno popolnoma enak. Omejitev do skupine dokumentov se lahko izvaja avtomatično, glede na nastavljene atribute dokumenta.
Prilagajanje procesov obstoječi dokumentaciji: elektronska podpora dokumentom in procesom se uvaja za tiste procese, ki že potekajo znotraj podjetja. V večini primerov se ne ustvarja novih, razen če ni takšne potrebe. Uporaba novih tehnologij lahko korenito spremeni poslovne procese, saj je nadzor nad procesi v elektronski obliki precej bolj preprost, kot nad klasičnimi procesi. Pred implementacijo se je potrebno prepričati, ali je proces, s katerim želimo podpreti poslovanje, maksimalno optimiziran ali pa je samo elektronska kopija starega procesa. Največji učinek dosežemo, če se izvede tako modernizacija kot informacijska podpora poslovnega procesa.

3. Elektronski arhiv

Arhive lahko na splošno opredelimo kot zbirko listin in dokumentov, ki imajo poslovno, zgodovinsko, kulturno ali znanstveno vrednost oz. kot prostor (tudi ustanovo), kjer so shranjene te listine in dokumenti. Arhivirana pisna gradiva vsebujejo pomembna dejstva, podatke, informacije, risbe, slike… Te s splošnim izrazom imenujemo dokumenti. Arhiv jih prejme v trajno last, s čimer sprejme obvezo, da je vsebina teh dokumentov ustrezna in dostopna vsem skupinam uporabnikov. Hkrati mora zagotavljati tudi dolgoročno nespremenljivost in verodostojnost vseh hranjenih informacij (Kroflič, Jerman Blažič, 2004, str. VI-54). Dokumentarno gradivo arhiviramo zaradi različnih potreb in hranimo v arhivu ustanove, dokler ne potečejo roki hranjenja, ki jih narekujejo predpisi in potrebe poslovanja ali dokler dela dokumentarnega gradiva, ki ima značaj arhivskega gradiva (trajni pomen za zgodovino, znanost ali kulturo), ne izločimo pristojnemu arhivu (Žumer, 2001, str. 48).

S pojavom elektronskih dokumentov in s tem elektronskih arhivov se je spremenila tudi sama logika arhiviranja. Ta ne temelji več samo na vzdrževanju in ohranjanju nosilcev in na njih zapisanih sporočilih, ampak predvsem na vzpostavljanju, vzdrževanju in razumevanju kontekstov, v katerih so zapisi nastali ali bili uporabljeni. Brez njih digitalni dokumenti izgubijo veljavnost in pomen.

Življenjski krog dokumentov se vrti v krogu ustvarjanja, pridobitev, kategorizacije oz. identifikacije, hranjenja in dostopa. Arhiviranje elektronskih zapisov zaznamuje zaključno funkcijo življenjskega cikla. Operacije nad elektronskimi dokumenti v arhivu se nanašajo predvsem na vlaganje in prevzemanje iz arhiva, upravljanje, osveževanje berljivosti in veljavnosti samih dokumentov ter pripadajočih atributov (npr. digitalni podpis) in nenazadnje izbris iz arhiva (Kroflič, Jerman Blažič, 2004, str. VI-54).

Osrednja težava tradicionalnih arhivov je njihova okornost. Upravljanje s papirnimi in drugimi dokumenti v analogni obliki je v primerjavi z digitalnimi kompliciranо in nepregledno, še posebej, če razpolagamo z večjimi količinami podatkov, ki zahtevajo ogromne tehnične in prostorske kapacitete, kar je povezano z velikimi stroški. S pojavom elektronskih arhivov so glavne pomanjkljivosti klasičnega modela odpravljene, saj omogočajo preprosto iskanje željenih vsebin po raznih atributih dokumentov, prostorsko so ti neomejeni, dostopni časi do vsebin pa zanemarljivi…

Ne glede na tip arhiva je potrebno zagotoviti (Kroflič, Jerman Blažič, 2004, str. VI-54):

- *verodostojnost vsebine dokumenta,*
- *avtentičnost dokumenta in subjekta, ki je dokument ustvaril,*
- *celovitost oz. garancijo, da dokument ni bi spremenjen delno ali v celoti,*
- *uporabnost oz. berljivost dokumenta, ter v primeru podpisanih dokumentov tudi verifikacijo podpisa v daljšem ali trajnem časovnem obdobju,*
- *pravno veljavnost arhiviranega dokumenta.*

3.1 Prednosti in slabosti elektronskega arhiva

V primerjavi s klasičnimi arhivi imajo njihove elektronske izpeljanke številne prednosti in seveda tudi slabosti. Najpogosteje navajane prednosti so:

- *najnižji možni stroški hranjenja in transporta arhiviranih gradiv,*
- *varno in pregledno okolje arhiva,*
- *lažje upravljanje in vzdrževanje poenotene podatkovne baze dokumentov,*
- *prilagodljivost novim standardom na področju digitalnega arhiviranja,*
- *indeksiranje vsebin z možnostjo iskanja po različnih tipih datotek,*
- *pri rednem ustvarjanju rezervnih kopij zelo mala verjetnost izgube vsebin,*
- *razpoložljivost zajetih dokumentov kadarkoli in kjerkoli,*
- *zmanjšani stroški tiskanja, vsaka natisnjena kopija je maksimalno kvalitetna,*
- *izboljšana klima v podjetju, saj je odpravljeno zastarelo, neučinkovito poslovanje,*
- *večja kvaliteta storitev in posledično bolj zadovoljne stranke,*
- *boljše osredotočenje na osnovne cilje podjetja.*

Po drugi strani imajo elektronski arhivi tudi nekatere slabosti. Tovrstna tehnologija je sorazmerno nova in se še vedno hitro spreminja. Mnoga področja v celoti še niso urejena, a se stanje hitro izboljšuje, saj se z njimi ukvarjajo številne svetovne institucije.

Izpostavil bi sledeče temeljne probleme digitalnih arhivov:

- *spreminjanje in zastarelost tehnologije,*
- *problem dolgoročnega hranjenja elektronskih vsebin,*
- *problem migracije vsebin,*
- *tehnična in pravna vprašanja,*
- *pomanjkanje standardov s tega področja.*

Digitalne informacije nastajajo v okolju, ki je v veliki meri odvisno od strojne (angl Hardware) in programske (angl. Software) opreme. Proizvajalci take opreme so pred težavno dilemo, saj se morajo odločiti med skladnostjo s prvotnimi verzijami in konkurenčno borbo, ki zahteva stalno uvajanje novosti, ki spreminjajo obstoječe formate. V preteklosti so kot glavno težavo dolgotrajnega hranjenja vsebin navajali predvsem fizične nosilce, na katerih so se le te nahajale. Današnje raziskave pa kažejo, da se celoten cikel zamenjave strojne, programske opreme in procesov v podjetju zgodi vsakih 2 do 5 let. V primerjavi s takim tempom uvajanja novosti imajo celo najbolj občutljivi fizični nosilci dolgo življenjsko dobo. Zastaranju nosilcev se lahko izognemo s kopiranjem podatkov na nove oblike medijev. Bolj problematična je kompatibilnost prvotnih formatov podatkov z novimi strojnimi in programskimi rešitvami. Idealno bi bilo, če bi lahko zagotovili dolgoročno hranjenje vsebin v formatu, ki je neodvisen od tehnologije. Migracija je občasen prenos digitalnih vsebin iz ene kombinacije strojne in programske opreme na drugo, ponavadi tehnološko bolj izpopolnjeno. Namen migracije je ohraniti integriteto digitalnih objektov in zagotoviti, da uporabniki lahko iščejo, prikazujejo in drugače uporabljajo vsebine v primeru sprememb tehnologije. Pri

migraciji je zelo težko zagotoviti popolno sliko digitalnega objekta (npr. SQL relacijske baze) in njegovo skladnost z novo tehnologijo. Poleg množice tehničnih problemov se pri migraciji srečujemo še s pravnimi izzivi. Težavno je uskladiti zahteve lastnikov in uporabnikov avtorskih pravic, saj imajo različna pričakovanja in izkušnje. Stroški migracije in z njo povezana tehnična in pravna vprašanja predstavljajo največjo grožnjo za dolgoročen obstoj digitalnih informacij. V tako hitro spreminjajočem se in neurejenem okolju so zato natančni in globalno poenoteni standardi nuja.

Standardi naj bi zagotavljali (Lorist, 2001, str. 3):

- *berljivost dokumentov,*
- *poenotenje tehnik in procedur,*
- *neodvisnost od strojne platforme.*

Za dolgotrajno hranjenje je potrebno razlikovati vsaj sledeče standarde (Lorist, 2001, str. 3):

- *Standardi, ki služijo kot referenčni model* (opredelijo arhitekturo arhivskega sistema), navajajo delovanje in obnašanja elektronskega arhiva, njegove koncepte in procedure.
- *Dokumentarni standardi, ki opredeljujejo formate zapisa in prikaza hranjenih digitalnih vsebin*.
- *Metapodatkovni standardi* omogočajo dostop do shranjenih vsebin, saj shranijo npr. povezave, izvor, ključne besede za poznejšo ponovno interpretacijo digitalnega gradiva.

Na področju standardov so številne institucije so ponudile svoje rešitve. Vsaka ima svoje prednosti in slabosti, a njihova medsebojna primerjava presega okvire te diplomske naloge. Na kratko bom opisal le tri osnove splošne standarde, ki opredeljujejo osnovne pojme, koncepte in procedure elektronskega arhiviranja (Lorist, 2001, str. 4):

- *ISO/DIS 15489*: v modernem okolju je nemogoče, da bi bilo upravljanje celotne digitalne zbirke gradiv v pristojnosti le ene same organizacije. Za uspešno omrežno sodelovanje izdajateljev, elektronskih knjižnic in arhivov je nujno temeljito opredeliti osnovne pojme. Osnutek standarda obravnava področja kot so: izrazi, definicije, omejitve, pravila delovanja, potrebe, načrtovanje in implementacija sistema za upravljanje z dokumenti, delovni procesi, kontrola delovanja sistema, šolanje uporabnikov…
- *AS 4390*: avstralski standard, izpeljanka ISO/DIS 15489, ki je v osnovi prilagojen evropskemu in ameriškemu okolju. Uporaben je za vse vrste zapisov.
- *DoD 5015.2-STD*: ustvarjen je bil na ameriškem obrambnem ministrstvu, navaja smernice za uspešno implementacijo sistema za elektronsko upravljanje z dokumenti. Kljub svojemu ameriškemu izvoru ga priporoča tudi nizozemska vlada.

Na arhitekturi arhivskega sistema se zrcalijo vse zahteve, potrebne za uspešno delovanje sistema. Predstavljenih je bilo mnogo različnih arhitektur, v nadaljevanju je prikazan model OAIS (angl. Open Archival Information System*),* ki je med vsemi najbolj razširjen in priznan.

3.2 Model elektronskega arhiva

Elektronski arhiv razumemo kot celoto postopkov in aktivnosti za ohranjanje vseh vrst podatkov, dokumentov in informacij, ki so izvorno nastale bodisi v elektronski obliki ali pa so bile iz klasične pretvorjene v elektronsko, z zmožnostjo zagotavljanja ustreznih dostopov do teh virov (Kroflič, Jerman Blažič, 2004, str. VI-54).

V nadaljevanju bom predstavil referenčni model *odprtega arhivskega informacijskega sistema OAIS* (angl. Open Archival Information System), vse ugotovitve povzemam iz njegove spremljajoče dokumentacije. Pridevnik »odprt« se nanaša na način njegovega nastanka, saj je proizvod večjega števila organizacij in je javno dostopen vsem. Posebno pazljivost so namenili njegovi dolgoročni obstojnosti, saj je odporen na menjavo tehnologij, kar vključuje tudi nove oblike formatov podatkov in njihovih fizičnih nosilcev.

Referenčni model OAIS v svoji osnovi ponuja naslednje (Reference Model for an Open Archival Information System, 2002, str. I-14):

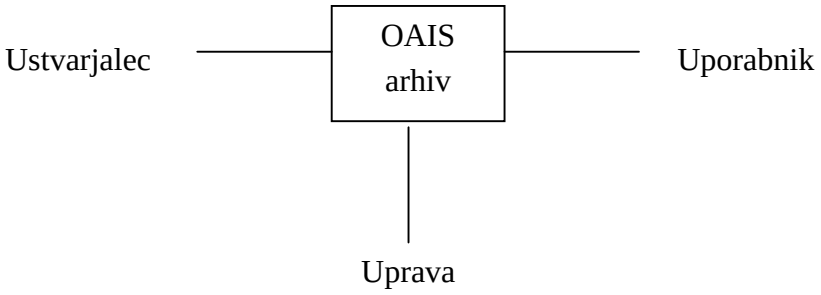
- ogrodje za razumevanje pomembnosti dolgoročne hrambe podatkov in dostopa do njih,
- koncepte, ki omogočajo učinkovito hrambo tudi podjetjem, katerim to ni osnovna dejavnost,
- ogrodje, ki vključuje terminologijo in koncepte za primerjavo arhitekture in delovanja obstoječih in bodočih arhivov,
- ogrodje za medsebojno primerjavo tehnik in strategij dolgoročnega hranjenja podatkov,
- osnovo za primerjavo podatkovnih modelov digitalnih informacij v arhivih in njihovih morebitnih sprememb v prihodnosti,
- načine za dolgoročno hrambo podatkov, ki niso v digitalni obliki,
- smernice za nastanek standardov, povezanih z OAIS.

Model obravnava celoten spekter funkcij manipuliranja s podatki v elektronskem arhivu kot so zajem, shranjevanje, upravljanje, dostop in razpošiljanje podatkov. Ukvarja se tudi z migracijo digitalnih informacij na nove nosilce in formate, podatkovnimi modeli za predstavitev informacij, vlogo programske opreme, izmenjavo digitalnih informacij med arhivi, notranjimi in zunanjimi vmesniki za dostop do funkcij arhiva… Nenazadnje opredeli še minimalne zahteve, katerim mora arhiv zadoščati, da si prisluži naziv »OAIS kompatibilen arhiv«.

3.2.1 Okolje modela

Slika 2 prikazuje okolje modela OAIS s tremi ključnimi zunanjimi subjekti.

Slika 2: Okolje modela OAIS



Vir: Reference Model for an Open Archival Information System, 2002, str. 2-2.

Trije ključni elementi v okolju modela so:

- *Ustvarjalec*: je oseba ali pa računalniški klient, ki zagotavlja informacije, katere se bodo shranjevale v arhivu.
- *Uprava*: določi pravila arhiviranja in kontrolira njihovo izvajanje. Poudariti je treba, da se uprava ne ukvarja z vsakodnevnimi operacijami v arhivu, saj je izdelava načel arhiviranja le ena izmed njenih nalog. Odgovornost uprave za delovanje arhiva je v kasnejšem podrobnejšem modelu predstavljena posredno preko entitete administracija.
- *Uporabnik*: je oseba oz. računalniški klient, ki preko arhivskega sistema pridobiva informacije. Delijo se v več razredov, glavno pa je, da nekateri poznajo ustroj arhivskega sistema in si lažje razložijo arhivirane informacije, nekateri pa ne. Potrebno je zagotoviti razumljivost hranjenih informacij za vse profile uporabnikov.

3.2.2 Definicija informacijskega paketa

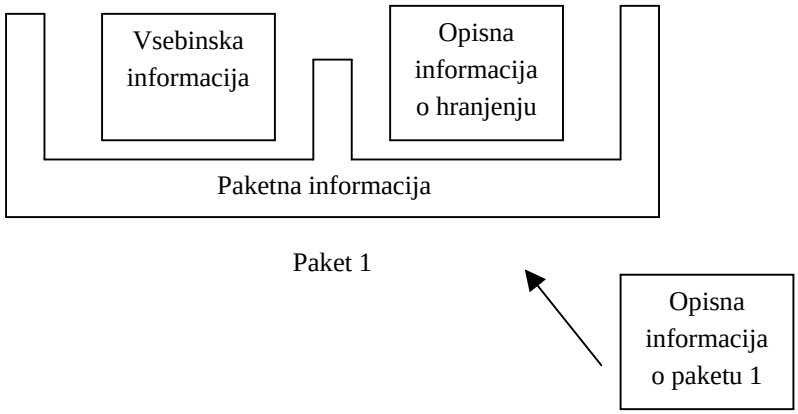
Vsak vnos informacij v arhivski sistem oz. razpošiljanje iz sistema povzroči enega ali več nepovezanih prenosov paketov informacij. Te pakete imenujemo *informacijski paketi*.

Vsak informacijski paket vsebuje dve vrsti informacij:

- *vsebinsko informacijo* (angl. Content Information),
- *opisno informacijo o hranjenju* (angl. Preservation Description Information).

Ti dve informaciji združeni v celoto imenujemo *paketna informacija* (angl. Packaging Information). *Opisna informacija* (angl. Descriptive Information) nam služi za iskanje tako nastalega informacijskega paketa, ki vsebuje željeno *vsebinsko informacijo*. Te relacije nam prikazuje Slika 3.

Slika 3: Koncept informacijskega paketa



Vir: Reference Model for an Open Archival Information System, 2002, str. 2-5.

V *vsebinski informaciji* se nahajajo informacije, katere so smisel samega arhiviranja. Vsebinska informacija vsebuje *vsebinski podatkovni objekt* (lahko fizičen ali pa digitalni) in z njim povezano *reprezentativno informacijo*, ki identificira in napravi vsebinski podatkovni objekt razumljiv v elektronskem okolju. Vsebinski podatkovni objekt je lahko npr. slika (angl. Image) CD-ROMa, katero skupaj z drugimi datotekami shranimo na drug CD-ROM, ki vsebuje tudi reprezentativne informacije za vse datoteke na tej zgoščenki.

Šele ko opredelimo vsebinsko informacijo lahko pridemo tudi do *opisne informacije o hranjenju*. Omogoča temeljito opredelitev vsebinske informacije, okolja v katerem je nastala… Vsebuje štiri tipe informacij:

- *Izvor*: navaja izvor vsebinske informacije, odgovornost za njeno hranjenje, zgodovino informacije…
- *Povezanost*: opredeli povezave z drugimi informacijami izven samega informacijskega paketa. Na primer, opredeli v kakšnih okoliščinah je vsebinska informacija nastala, lahko pa nas naveže tudi na druge vsebinske informacije, ki so na voljo.
- *Ključ*: navaja enolično identifikacijo za vsebinsko informacijo. Lahko gre tudi za skupino atributov, ki v zadostni meri označijo informacijo.
- *Nespremenljivost*: navaja zaščito pred nepooblaščenimi spremembami. Zaščiti se lahko npr. z uporabo zgoščevalne funkcije (angl. Hash Code), ki je podrobneje obravnavana v poglavju o elektronskem podpisovanju.

Paketna informacija vzpostavi povezavo med vsebinsko in opisno informacijo o hranjenju. Če se vrnemo k primeru z zgoščenko, nam lahko paketno informacijo predstavlja ISO 9660 datotečna struktura, ki jo uporabimo pri zapisu zgoščenke.

Opisna informacija je uporabna za določanje paketa, ki vsebuje določeno vsebinsko informacijo, katero iščemo. Pri tem lahko gre preprosto za ime paketa ali pa tudi kombinacijo atributov, po katerih lahko iščemo.

3.2.3 Vrste informacijskih paketov

Za razumevanje podrobnejšega modela elektronskega arhiva, ki ga bom predstavil v nadaljevanju, je nujno razlikovati med tremi tipi informacijskih paketov. Razločiti je potrebno med paketi, ki nastanejo in se shranjujejo v samem arhivu ter paketi, ki so bili poslani v arhiv ali pa iz njega zahtevani. Vse to nam omogoča, da razumemo, da nekateri predloženi paketi lahko imajo nezadostno reprezentativno oz. opisno informacijo o hranjenju, kar jim onemogoča, da bi zadostili pravilom modela OAIS o hranjenju. Vsakega od informacijskih paketov sistem obravnava posebej, tako da nekakšnega skupnega imenovalca, ki bi veljal za vse, ne moremo navesti. Klub temu pa lahko arhiv uporabniku postreže z informacijami, kjer vsebinska informacija ni v zadostni meri povezana z reprezentativno in opisno informacijo o hranjenju.

Ločimo tri tipe informacijskih paketov:
- *predložen informacijski paket* (angl. SIP-Submission Information Package),
- *arhivski informacijski paket* (angl. AIP- Archival Information Package),
- *razposlan informacijski paket* (angl. DIP- Dissemination Information Package).

Predložen informacijski paket pošlje v arhiv ustvarjalec. Njegova oblika in natančna vsebina sta glede na format vhodnih podatkov navedena v dokumentaciji o arhivu. Večina SIP vsebuje nekaj vsebinske in nekaj opisne informacije o hranjenju, tako, da je za formiranje AIP v praksi potrebnih več vhodnih SIP. En paket SIP lahko vsebuje informacije, ki se uporabijo v več različnih AIP. Paketna informacija je pri SIP zmeraj enaka.

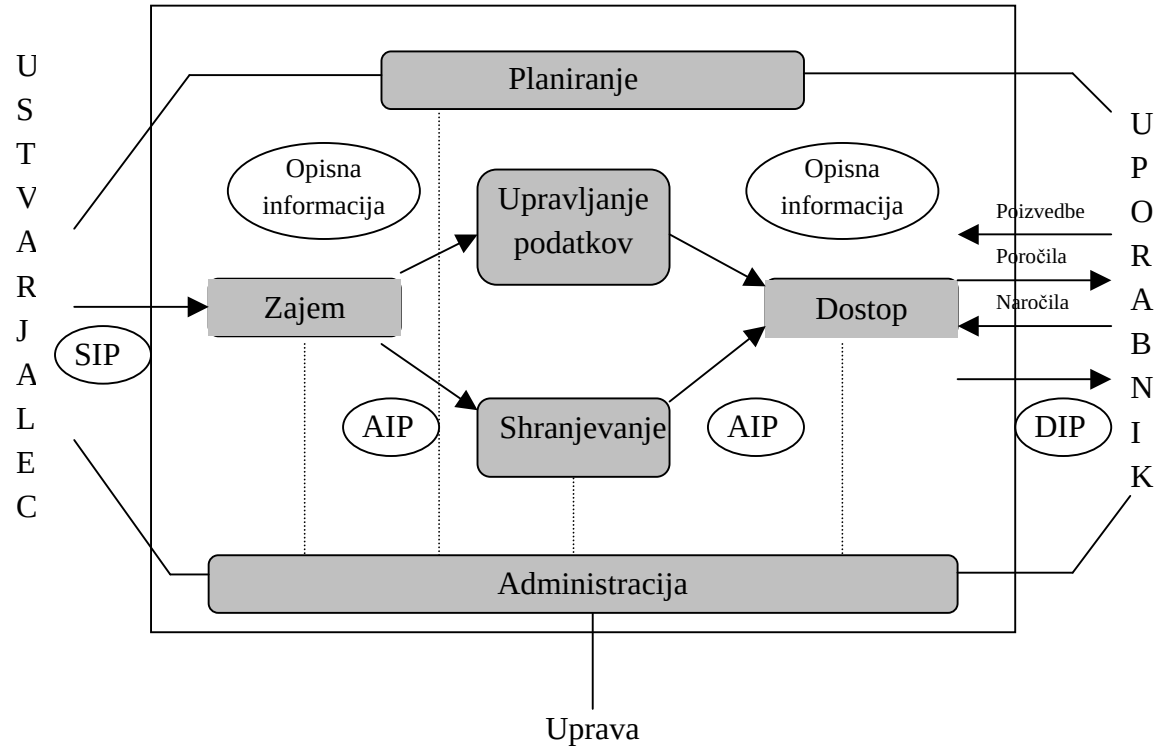
Arhivski informacijski paket nastane s pretvorbo enega ali več SIP. Vsebuje kompleten nabor opisne informacije o hranjenju, potreben za arhiviranje vsebinske informacije, ki jo predstavlja. AIP lahko vsebuje tudi druge AIP, vendar to presega okvire našega modela, zato je ta možnost navedena le kot zanimivost. Paketna informacija AIP je odvisna od internih standardov organizacije, ki upravlja arhiv in se lahko s časom spreminja.

Razposlan informacijski paket predloži arhiv na zahtevo, ki izvira iz okolja arhiva, bolj natančno od končnega uporabnika. DPI lahko vsebuje zbirko AIP in ne rabi nujno vsebovati celotne opisne informacije o hranjenju. Paketna informacija DIP mora biti zmeraj prisotna v obliki, ki uporabniku omogoča celovit prikaz zahtevane informacije. Zaradi zunanje uporabe informacije mora biti paketna informacija DPI prilagojena zunanjemu mediju in uporabnikovim željam.

3.2.4 Natančna opredelitev modela arhiva OAIS

Slika 4 prikazuje model arhiva OAIS s šestimi pripadajočimi entitetami in njihovimi medsebojnimi povezavami. Slika prikazuje le glavne tokove informacij, njihov pretok je možen v obe smeri. Povezave k entitetama administracija in planiranje sta prikazani črtkano, saj za sam model nista ključnega pomena, poleg tega pa je takšen prikaz bolj pregleden.

Slika 4: OAIS model s prikazanimi ključnimi entitetami



Vir: Reference Model for an Open Archival Information System, 2002, str. 4-1.

Na kratko bom predstavil še funkcije posameznih entitet, predstavljenih v modelu.

Zajem: entiteta zajem skrbi za pripravo dokumenta in preoblikovanje v ustrezno obliko za shranjevanje. Predloženi paketi (SIP) so opremljeni z ustreznimi atributi, namenjenimi upravljanju s paketi in zaščiti elektronskega zapisa. Pomembni sta predvsem indeksacija in integriteta, s pomočjo katerih v fazi dostopa lažje oz. hitreje iščemo dokument po določenih atributih in dokazujemo njegovo veljavnost oz. pravilnost hranjenega zapisa. Vstopni paketi se preoblikujejo v AIP, ki ustrezajo formatom in standardom arhiva.

Shranjevanje: arhiv od entitete zajem sprejme podatke in zahtevo po njihovi shranitvi na trajen medij. V sklopu te entitete se določi raven varnosti fizičnega zapisovanja (maksimalno dovoljeno število napak, procedure obnove podatkov) in spremljanja napak (angl. Error Logs) med prenosom podatkov. Pomembna funkcija, ki jo zagotavlja arhiv je zamenjava medija v arhivu, ki omogoča dolgoročno hranjenje podatkov (migracija). To pomeni, da se na dolgi rok

vsebina ne spreminja. Strategija migracije izbere nov medij, na katerega se bodo prenesli podatki. Nujno je zagotoviti tudi obnovitev stanja pred uničenjem (angl. Disaster Recovery). Arhiv glede na zahtevo uporabnika po določenem dokumentu posreduje arhivirana podatke entiteti dostop, kjer se izvaja dekapsulacija zapisa in predložitev uporabniku.

Upravljanje podatkov: zagotovi funkcije upravljanja z opisnimi informacijami, ki identificirajo dokument, ter administrativni podatki, ki so nujni za upravljanje arhiva. Upravljanje z opisnimi podatki kreira nabor metapodatkov namenjenih upravljanju in zaščiti elektronskih zapisov. Metapodatki opisujejo shranjeno vsebino v arhivu, nekatere administrativne funkcije povezane s tem in varnostne atribute (podpis, čas arhiviranja itd.). Ti podatki omogočajo zunanjim in notranjim uporabnikom lažje obvladovanje arhiva in zagotavljajo verodostojnost hranjenim zapisom.

Metapodatki so lahko (Kroflič, Jerman Blažič, 2004, str. VI-60):

- atributi, ki opisujejo arhivirano gradivo, namenjeni iskanju, pregledovanju in naročanju arhiviranega gradiva (naslov, avtor, datum arhiviranja, črtna koda…),
- atributi, ki ščitijo arhivirano gradivo, namenjeni zagotavljanju celovitosti arhiviranega gradiva (preprečevanju spreminjanja hranjene vsebine) in temeljijo na kriptografskih mehanizmih,
- informacije o politiki, ki lahko navajajo politiko zaračunavanja storitev, dostopnost arhiviranih vsebin,
- podatki o zahtevah in prenosu podatkov, ki vključujejo sledljivost vsake transakcije med arhivom in uporabnikom,
- statistične informacije v zvezi z arhivom (število prenosov, časi prenosa, zasedenost kapacitet), ki omogočajo lažjo pripravo politike,
- informacije o uporabnikih vključno z uporabniškimi imeni, gesli, ki zagotavljajo identifikacijo uporabnikov in njihove pravice pri dostopanju do gradiv.

Dostop: predstavlja v sistemu arhiva uporabniški vmesnik, preko katerega uporabniki iščejo in naročajo zapise. Na voljo so jim funkcije s katerimi izločijo in prejmejo ustrezen zapis iz arhiva. Pogoji dostopa za vsakega uporabnika so določeni z arhivsko politiko za vsak nivo posameznega dokumenta. Poizvedba ali naročilo uporabnika sproži prenos DIP informacijskega paketa ali poročila k uporabniku.

Administracija: namen entitete je bedenje nad funkcijami delovanja arhivskega sistema. Svetuje ustvarjalcem gradiva in pregleduje vložene dokumente, da se zagotovi skladnost s standardi. Entiteta vsebuje tudi funkcije, ki omogočajo inženirske posege v arhiv, s čemer se poveča kakovost in varnost hranjenih vsebin. V fazah uvajanja arhiva mora administracija pripraviti politiko hranjenja, omogočiti uporabnikom tehnično podporo…

Planiranje: ta entiteta omogoča učinkovitejše delovanje arhiva na podlagi ugotovitev, ki so nastale pri opazovanju arhivskega okolja. Njena priporočila in izboljšave omogočajo uporabnikom brezskrbno dolgoročno shranjevanje gradiv, neodvisno od tehnoloških sprememb. Večina dela je namenjenega pripravi planov migracij, izdelavi prototipov programskih rešitev in pripravam na testiranje na novo implementiranih rešitev.

3.3 Tehnična priporočila elektronskega arhiviranja

Elektronska izmenjava dokumentov je danes ustaljen način komunikacije, tako med fizičnimi kot pravnimi osebami. Papirnati dokumenti čedalje bolj izgubljajo veljavo, a na dolgi rok se bodo vseeno ohranili, če ne drugače, kot eden izmed izhodnih formatov sistemov za upravljanje elektronskih dokumentov. Papirnata oblika bo v veljavi predvsem za ključne in občutljive dokumente, saj ima digitalna tehnologija pri dolgoročnem hranjenju številne pomanjkljivosti. Problem je v izjemno hitrem napredku na področju tehnologije, njenega razvoja pa se ne da točno predvideti.

Tehnološki problem se kaže predvsem v slednjem (Žužek, Dobnikar, 2003, str. IV-31):

- formati zapisov se naglo spreminjajo, obstoječi hitro zastarajo,
- elektronski zapis je preprosto spremeniti, ne da bi se to dalo preprosto ugotoviti (rešitev je zaščita z elektronskim podpisom, ki je v tem poglavju podrobno obdelan),
- potrebno je zagotoviti zanesljivo povezavo zapisa na pripadajoče dokumente (angl. Context), saj se sled sicer lahko hitro izgubi,
- današnji sistemi, kjer se ustvarjajo elektronski zapisi, niso načrtovani za dolgoročno hrambo (primer elektronske pošte, Office programska oprema…).

Rešitvi za zagotavljanje berljivosti in legitimnosti današnjih dokumentov v prihodnosti sta dve (Žužek, Dobnikar, 2003, str. IV-31):

- institucije, ki skrbijo za arhivsko gradivo bodo zagotovile, da bodo skupaj z zapisi v originalnem formatu, hranile tudi programsko in strojno opremo, na kateri je izvorni dokument pred časom nastal (angl. Emulation),
- drugi način pa temelji na migraciji elektronskih dokumentov v modernejše formate in na drugo programsko in strojno opremo, ki bo takrat v uporabi.

Vsak od teh dveh način ima svoje prednosti in slabosti, idealna pa bi bila mešanica obeh. Eden izmed takih načinov je hranjenje dokumenta v izvorni obliki, zraven pa se hrani tudi podrobne metapodatke za njegovo kasnejšo interpretacijo.

Ohranjanje berljivosti dokumentov pa je le ena izmed težav, ki jih prinaša brezpapirno poslovanje. Za kakovostno elektronsko poslovanje je potrebno zagotoviti vsaj tak nivo zaupanja, kot pri klasičnem, papirnem poslovanju. Omogočeno mora biti (Žužek, Dobnikar, 2004, str. IV-31) brezpogojno ugotavljanje identitete, zaupnost pri izmenjavi zaupnih podatkov, zaščiten dostop do podatkovnih baz… Vse vidike varnosti in zaupnosti zagotovi

infrastruktura javnih ključev (angl. PKI-Public Key Infrastructure) oz. neposredno overitelj digitalnih potrdil javnih ključev (angl. CA-Certification Authority). Zahteve, ki jim mora zadostiti kvalificirano potrdilo, sem podrobneje predstavil v poglavju, ki zadeva zakonodajo oz. Zakon o elektronskem poslovanju in elektronskem podpisu. Pri nas izdaja kvalificirana digitalna potrdila Center Vlade RS za informatiko (CVI) in so skladna z vsemi pri nas veljavnimi zakoni in uredbami, kot tudi evropskimi direktivami. Potrdila CVI zagotavljajo najvišjo možno stopnjo varnosti in močno enkripcijo. Izdajajo dve, medsebojno priznani ter tehnološko in pravno enako veljavni potrdili, to sta SIGEN-CA za pravne in fizične osebe in SIGOV-CA za upravo Republike Slovenije. Eden izmed večjih problemov je zagotavljanje legitimnosti digitalnih potrdil na daljše časovno obdobje. Ker se ta tema navezuje na diplomsko nalogo, jo bom v nadaljevanju temeljiteje obdelal.

3.3.1 Varen elektronski podpis

Za zagotavljanje avtentičnosti informacij v elektronski obliki se uporabljajo elektronski podpisi, ki temeljijo na kriptografskih logaritmih. Digitalno potrdilo lahko smatramo kot nekakšno novejšo alternativo klasičnim identifikacijskim sredstvom, kot sta npr. osebna izkaznica in potni list. Kot vsak dokument v fizičnem svetu, ima tudi digitalni certifikat svojega izdajatelja, rok veljavnosti ter druge potrebne podatke. Vendar je med klasičnim in elektronskim identifikacijskim sredstvom pomembna razlika: k vsakemu digitalnemu potrdilu, ki vsebuje javni ključ, spada tudi ustrezen zasebni ključ. Javni in zasebni ključ sta med sabo matematično povezana, a je slednjega praktično nemogoče izračunati na osnovi drugega. Pri podpisovanju elektronskega dokumenta se tako uporabi zasebni ključ, naslovnik sporočila pa nato preveri s podpisnikovim javnim ključem, ali je bil za elektronsko podpisovanje uporabljen ustrezen zasebni ključ.

Osnovna oblika elektronskega podpisa, ki ustreza vsem pravnim zahtevam, pomeni uporabo asimetričnih algoritmov za šifriranje s podpisnikovim zasebnim ključem nad sledečimi podatki (Žužek, Dobnikar, 2003, str. IV-34):

1. *Zgoščena vsebina* (angl. hash code): predstavlja »seštevek« sporočila, ki povezuje digitalni podpis s podatki, ki se jih podpisuje. Nastane iz podatkov z uporabo zgoščevalne funkcije z naslednjimi lastnostmi:
   - rezultat zgoščene vsebine nad istimi podatki je vedno enak,
   - iz zgoščene vsebine je nemogoče restavrirati izvorno sporočilo,
   - vsaka sprememba v sporočilu povzroči spremembo zgoščene vsebine.
2. *Kvalificirano digitalno potrdilo*, ki nedvoumno in enolično pripada zasebnemu ključu podpisnika elektronskega sporočila.

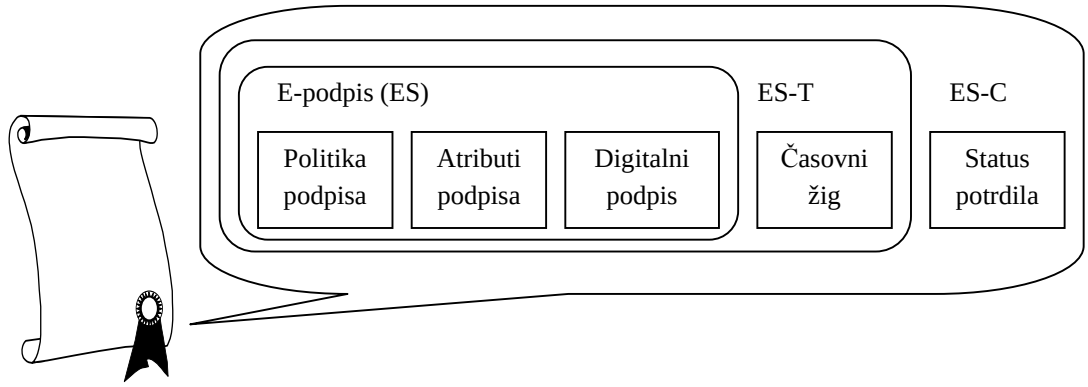
Omenjena oblika elektronskega podpisa zadošča za uporabo v kratkem časovnem obdobju, ko smo prepričani, da se dejstva, povezana s stanjem potrdila, niso spremenila. Za uspešno verifikacijo podpisa morajo biti na razpolago (Žužek, Dobnikar, 2003, str. IV-34):

1. *Vsa potrdila uporabljena za podpis*, se pravi podpisnikovo digitalno potrdilo in potrdilo izdajatelja,
2. *Statusi uporabljenih digitalnih potrdil*, pridobljeni na podlagi:
   - registra preklicanih potrdil (angl. CRL- Certificate Revovation List),
   - sprotnega odgovora o stanju potrdila (angl. OCSP- Online Certificate Status Protocol),
3. *Varen časovni žig*, ki potrjuje obstoj digitalnega podpisa ob določenem času, izda pa ga zaupanja vredna institucija TSA (angl. Time Stamp Authority) in vključuje:
   - zgoščeno vsebino digitalnega podpisa,
   - zaupanja vredno označbo časa,
   - identiteto TSA.

3.3.2 Elektronski podpis za krajše časovno obdobje

Slika 5 prikazuje shematski prikaz elektronskega podpisa (ES) z dodanim časovnim žigom (ES-T). Za izpolnjevanje pravnih zahtev je potrebno osnovni obliki dodati še nekatere atribute, kot so politika podpisa (določa tehnične zahteve in pravna razmerja med podpisnikom in tretjo osebo) in ostali potrebni atributi varnega elektronskega podpisa. V skrajnem primeru je potrebno e-podpisu dodati še statuse uporabljenih potrdil, uporabljenih za verifikacijo dokumenta (ES-C).

Slika 5: Elektronski podpis s časovnim žigom in statusom potrdila



Vir: Žužek, Dobnikar , 2003, str. IV-35.

3.3.3 Elektronski podpis za daljše časovno obdobje

Nekaj let po nastanku elektronskega dokumenta sama vsebina in digitalni podpis nista zadostno jamstvo za uspešno verifikacijo dokumenta. Nujno je imeti dostop do ustreznega digitalnega potrdila in dokazila o njegovi veljavnosti v času nastanka dokumenta. Ker je

možno, da je bilo sprva veljavno, kasneje pa preklicano, je posledično nujno hraniti tudi status digitalnega potrdila v času nastanka arhivskega gradiva. Te podatke je nujno zbrati čim hitreje po nastanku elektronskega podpisa.

Za eksplicitno pravno veljavnost dokumenta je ključna veljavnost digitalnega podpisa v času nastanka dokumenta, kar se dokazuje s časovnim žigom. Ko govorimo o hrambi dokumentacije na daljše časovno obdobje moramo predvideti različne spremembe v statusu digitalnega podpisa (Žužek, Dobnikar, 2003, str. IV-36):

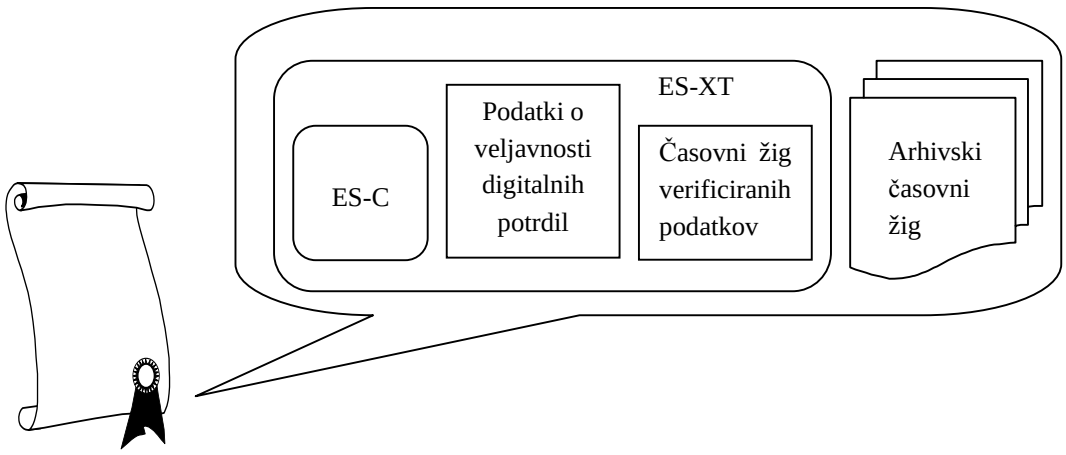
- da je bilo od nastanka podpisa podpisnikovo ali izdajateljevo digitalno potrdilo zlorabljeno, preklicano,
- da status digitalnih potrdil ni več na voljo (izdajatelj prenehal z delovanjem oz. je njegove aktivnosti prevzel drug ponudnik tovrstnih storitev),
- da so bili predhodno uporabljeni kriptografski algoritmi razbiti in tako niso več vredni zaupanja, to pa posledično povzroči tudi razbitje ključev, časovnih žigov.

Za zagotavljanje dolgotrajne veljavnosti e-podpisa je potrebno za zaščito legitimnosti dokumenta poskrbeti za podaljševanje veljavnosti z dodajanjem časovnih žigov, narejenih po novejših algoritmih, kot originalni časovni žig. Sekvenčno dodajanje časovnih žigov, zaščitenih z novejšo tehnologijo, je možno dokler (Žužek, Dobnikar, 2003, str. IV-36):

- ni mogoče iz javnega ključa ugotoviti zasebnega,
- zgoščevalna funkcija nima več zaupanja vrednih lastnosti.

Za zagotavljanje dolgotrajne veljavnosti elektronsko podpisanim dokumentom je potrebno osnovnemu formatu, predstavljenemu na Sliki 5, dodati še podatke o veljavnosti digitalnih potrdil, kar vključuje potrdila izdajateljev in njihove statuse (tudi te podatke se zaščiti s časovnim žigom). Razširjeni model e-podpisa prikazuje Slika 6. Digitalni podpis z razširjenimi podatki je potrebno na novo zaščititi, preden časovnemu žigu (ES-XT) poteče veljavnost oz. je le-ta ogrožena (arhivski časovni žig).

Slika 6: Arhivski format varnega elektronskega podpisa

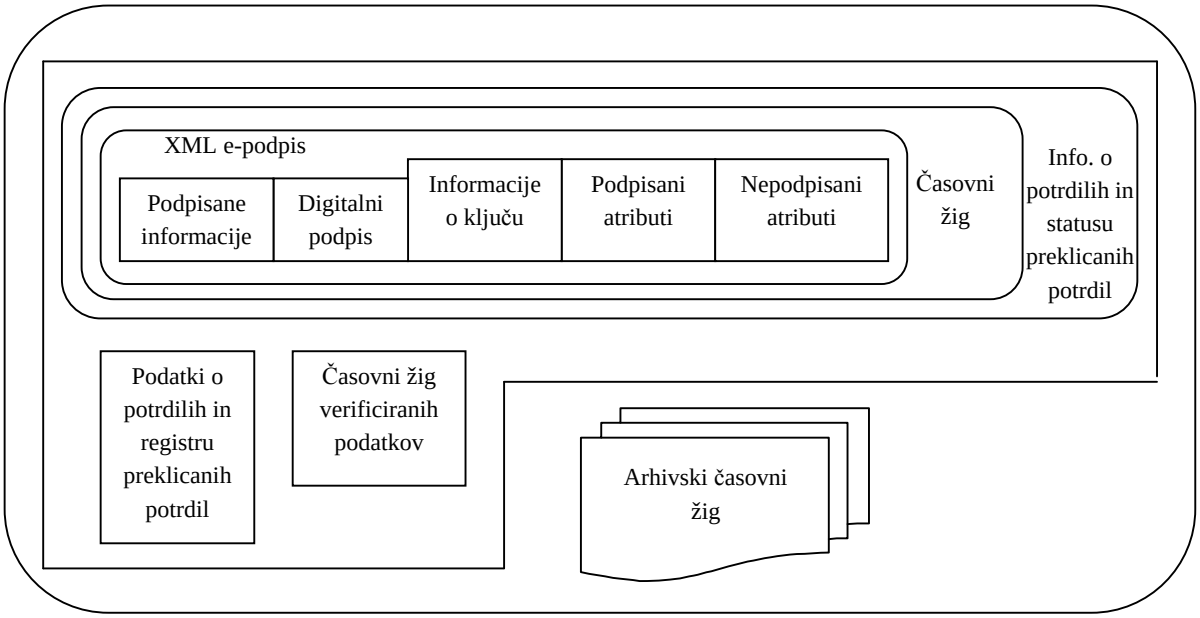


Vir: Žužek, Dobnikar , 2003, str. IV-36.

3.3.4 Format XML za dolgotrajno hranjenje

XML (angl. eXtensible Markup Language) postaja standardni format zapisa podatkov, uporaben v različnih aplikacijah. V zadnjih letih predstavlja tudi edino perspektivno obliko za dolgotrajno hranjenje dokumentov v elektronski obliki. Priporočila standarda XML navajajo tudi elemente za varen elektronski podpis, vključujejo pa tudi vse potrebno za zagotovitev dolgotrajnega in legitimnega hranjenja (Slika 7).

Slika 7: Arhivski format elektronskega podpisa v XML



Vir: Žužek, Dobnikar , 2003, str. IV-37.

3.4 Pravni vidik elektronskega arhiviranja

Na področju informacijskih tehnologij smo bili v zadnjih dveh desetletjih priča izjemno hitremu tehnološkemu razvoju, kar je v veliki meri spremenilo tudi nekatere zadeve v arhivistiki, predvsem pa odnos samih ustvarjalcev do dokumentarnega in arhivskega gradiva. To področje je bilo nujno urediti tudi s pravnega vidika. Tako je bil v Sloveniji leta 2000 sprejet Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), ki opredeljuje elektronsko poslovanje z uporabo informacijske in komunikacijske tehnologije, opredeli uporabo elektronskega podpisa v sodnih, upravnih in drugih postopkih. Največji pomen zakona je sicer v izenačitvi elektronskega podpisa s ročnim. Nesprejetje tega zakona bi pripeljalo do velikih ovir pri uvajanju elektronskega poslovanja v vse segmente gospodarstva.

Pravni vidik elektronskega podpisa

Kot vsi ostali informacijski sistemi, ki se uporabljajo pri elektronskem poslovanju, morajo biti tudi sistemi za upravljanje z dokumenti skladni z veljavnimi zakonskimi zahtevami, še posebej, če se pri tem uporablja enega izmed uveljavljenih načinov elektronskega podpisa.

Elektronski podpis ima naslednje značilnosti (Klasinc, 2001, str. I-71):

- podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena,
- podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotavljati iz podatkov za preverjanje elektronskega podpisa, sam podpis pa je učinkovito zaščiten pred ponarejanjem z uporabo trenutno dostopne tehnologije,
- podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom,
- sredstvo za varno elektronsko podpisovanje ne sme spremeniti podpisanih podatkov ali preprečiti prikaza podatkov podpisniku pred podpisom,
- Vlada RS predpiše s podzakonskim aktom podrobnejša merila za izpolnjevanje zahtev glede sredstev za varno elektronsko podpisovanje.

Sami podatki za preverjanje elektronskega podpisa so po tem zakonu edinstveni podatki, gre za razne šifre oz. javne šifrirne ključe, katerih izključen namen je preverjanje elektronskega podpisa.

Fizične in pravne osebe izdajajo tudi uradno overjena potrdila s področja elektronskega podpisa. Po ZEPEP je potrdilo v elektronski obliki narejeno tako, da povezuje podatke za preverjanje elektronskega podpisa z določeno osebo, torej imetnikom določenega potrdila, s čimer se izkaže njegova identiteta.

Kvalificirano potrdilo tako izpolnjuje naslednje zahteve (ZEPEP, 2003, 28. člen):

- navedba, da gre za kvalificirano potrdilo,
- ime ali firma in država stalnega prebivališča ali sedeža overitelja,
- ime oz. psevdonim imetnika potrdila ali naziv oz. psevdonim informacijskega sistema z navedbo imetnika potrdila, pod katerega nadzorom je, z obvezno navedbo, da gre za psevdonim,
- dodatni podatki o imetniku potrdila, ki so predpisani za namen uporabe,
- podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila,
- začetek in konec veljavnosti potrdila,
- identifikacijska oznaka potrdila,
- varen elektronski podpis overitelja, ki je potrdilo izdal,
- morebitne omejitve v zvezi z uporabo potrdila,
- morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja,
- če ni drugače dogovorjeno, potrdilo drugih podatkov ne sme vsebovati.

Pravilnik o arhiviranju

Arhiviranje dokumentov v podjetju je logična posledica poslovanja, s tem povezanih potreb po ohranjanju vsebin, ter zakonskih zahtev, ki določajo katere dokumente in koliko časa je potrebno hraniti. Poleg tega podjetje hrani določene dokumente tudi zaradi zasebnega pravnega interese (npr. razne pogodbe, dokazi…). Ne glede na to, kako gledamo na arhiviranje, zmeraj je opaziti pravni smoter. Zakoni poleg vprašanja, zakaj arhivirati, določajo tudi odgovore na vprašanji, kaj arhivirati in kako.

Vprašanje o tem, kaj arhivirati, se v pretežni meri nanaša na množico dokumentov in podatkov v podjetju, ki jih je smiselno hraniti. Vprašanje, kako arhivirati, pa je samo po sebi bolj kompleksno in se nanaša na samo določitev postopkov arhiviranja, izpolnjevanje zakonskih zahtev, izbiro tehnologije in ročnost arhiviranja. Vsi odgovori na ta vprašanja morajo biti v sodobnih podjetjih zapisana v splošni pravnih aktih, to je v pravilnikih oz. politikah arhiviranja. Politika hranjenja mora biti udejanjena tudi v praksi, kar pomeni, da so zaposleni zavezani k njenemu spoštovanju (pri tem mislim na pogodbo o zaposlitvi z navedenimi disciplinskimi ukrepi).

Zgoraj navedena vprašanja (zakaj, kaj in kako) se v pravilniku obdelajo v naslednjih konkretnih področjih (Berčič, 2004, str. V-2):

- *klasifikacija dokumentov in podatkov organizacije,*
- *razlogi za arhiviranje in zakonska podlaga,*
- *ročnost arhiviranja,*
- *zahteve arhiviranja,*
- *tehnologija arhiviranja,*
- *procesi arhiviranja in notranje poslovanje*.

Klasifikacija dokumentov in podatkov je praktično zmeraj možna po dveh kriterijih, vsebinskem in pravnem. V praksi se pogosto uporablja tudi navzkrižna klasifikacija - zakon zato za različne kombinacije zahteva različne načine hranjenja.

Po vsebinski klasifikaciji se pojavljajo naslednje kategorije (Berčič, 2004, str. V-3):

- računovodske listine,
- pravni dokumenti (pogodbe, ponudbe),
- poslovna komunikacija (dopisi, e-pošta),
- seznami (zaposlenih, poslovnih partnerjev, osnovnih sredstev, programske opreme…),
- različni načrti in politike (poslovni in strateški načrt, varnostna, trženjska politika…),
- informacijska intelektualna lastnina (izvorna koda programov, spletne strani, slike…),
- računalniški dokazi (vdori v sistem, dnevniški zapisi).

Klasifikacija po pravnih inštitutih izgleda tako (Berčič, 2004, str. V-3):

- Intelektualna lastnina
  - Avtorske pravice
  - Patenti
- Zaupni podatki
  - Interni
  - Zaupni
  - Tajni
  - Strogo tajni
- Osebni podatki

Dokumentom, ki so bili uspešno kvalificirani, se nato pripišejo zakonske podlage za njihovo hranjenje. Hranjenje je lahko obvezno, dopustno ali pa celo prepovedano.

Na podlagi klasifikacije in zakonskih podlag se dokumenti razvrstijo na tiste, ki se bodo hranili in tiste, ki se ne bodo. Razlogi za oz. proti so različni: zakonske zahteve, zasebni pravni interes, poslovni interes, reduciranje stroškov… Preobsežno shranjevanje dokumentov je lahko prav tako kaznivo kot premajhno arhiviranje. Primer tega je shranjevanje osebnih podatkov, kar je v praksi pogost prekršek. Za dokumente, ki gredo v arhiviranje, se iz zakonov razbere ročnost hranjenja. Kar se tiče gradiva v elektronski obliki, je potrebno poudariti, da v Sloveniji v tem trenutku ni veljavnega predpisa, ki bi zagotavljal odbiranje elektronskega gradiva, njegovo uničevanje, pretvorbo izvirnika v sodobnejši tehnološki format, ponovno zagotavljanje elektronskega podpisa zaradi poteka veljavnosti izvirnika…čeprav so roki shranjevanja v elektronski obliki določeni pravilno.

Iz vrste dokumentacije je prav tako nujno določiti same zahteve oz. načela shranjevanja za vsak posamezen tip dokumenta oz. dovoljene operacije med njimi (tukaj se gre predvsem za določitev dostopnosti do podatkov, kdaj je pomembna nespremenljivost podatkov, kdaj je nujno zagotoviti zaupnost, sledljivost operacij…). Bistvena je tudi določitev skupin podatkov in uporabniških pravic pri operacijah z dokumenti.

Iz teh, že konkretnih zahtev, se določi najustreznejšo tehnologijo shranjevanja. V preteklosti je bila to predvsem papirnata oblika in mikrofilm, za nas pa so bolj zanimive elektronske rešitve (relacijske podatkovne baze, XML, tekstovne, multimedijske zbirke podatkov). Sami zakoni podajajo konkretne zahteve za shranjevanje posameznih vrst podatkov, tem zahtevam pa tako zakoni posredno določajo izbor tehnologij.

Na koncu se na podlagi zgoraj navedenih korakov popišejo faze zajemanja, transformacije, evidentiranja, shranjevanja, branja, dodajanja, brisanja ter vzdrževanja podatkov in dokumentov. Ne sme se pozabiti niti na uničenje vsebin, ko potečejo zakonsko predpisani roki hranjenja.

3.5 Mobilnost podatkov v digitalnem arhivu

Zadnja faza pri obdelavi podatkov je priprava za njihov prenos v arhiv. Gre za zadnjo in v marsičem tudi najbolj kompleksno stopnjo življenjskega cikla dokumentov. Arhivsko gradivo je namreč potrebno ustrezno pripraviti, stabilizirati in ga vzdrževati skozi celotno življenjsko dobo. Tovrstne procedure so pri klasičnih arhivih že dodobra utečene, pri digitalnem okolju pa tega ne moremo trditi in je potrebno šele vzpostaviti podatkovne kontrole. Pojem mobilnosti podatkov dobi še dodatno težo pri javno dostopnih elektronskih podatkovnih virih.

Vprašanja povezana z mobilnostjo oz. bolje rečeno prenašanjem podatkov v času in prostoru, so bila na področju arhivistike venomer aktualna, danes pa zaradi kopice razlogov še pridobivajo na teži. Navedemo lahko materialno-tehnične in njim nasprotujoče uporabniške razloge, vidike zagotavljanja integritete in celovitosti podatkov arhivske vrednosti, zaščito integritete posameznikov in zahteve po neoviranem dostopu do npr. informacij javnega značaja. Medsebojni odnosi med temi zahtevami so diametralno si nasprotujoči, zato je potrebno sklepati kompromise.

Problem procedur, povezanih z mobilnostjo podatkov, se v digitalnem okolju le še potencira. Tako se je dandanes zaradi tehnoloških sprememb porušilo zgodovinsko razmerje med »mobilnostjo« in »stabilnostjo« močno v prid mobilnosti. Ko govorimo o mobilnosti podatkov, mislimo na njihovo obravnavanje v okviru strojne in komunikacijske opreme, operacijskih sistemov in drugih programskih rešitev, pa tudi o prenosih med različnimi tehnologijami itd. Mobilnost daje moč, zagon in smisel razširjenosti uporabe informacijske tehnologije. Začarani krog mobilnosti digitalnih podatkov se navadno pričenja s trženjsko pripravo uporabnikov, da uvidijo svoje potrebe. Tako oblikujejo potrebe po novi strojni in programski opremi, le te pa generirajo nove možnosti obravnavanja podatkov. Vedno več podatkov ustvarja potrebo po njihovi uporabi, uporaba pa znova sklene krog z novimi potrebami po tehnologiji. Razlika med klasično in elektronsko obliko arhiviranja pa ni samo v uporabljeni tehnologiji, temveč v časovnem razponu trajanja posameznega cikla. Če izpustimo uničenje gradiva (npr. poplave, požari, potresi, vojne), je časovni razpon cikla pri klasičnih arhivih merjen v stoletjih, v digitalnih okoljih pa je mnogo manjši.

Procesi mobilnosti podatkov v arhivski teoriji in praksi

Pri terminologiji procesov, ki omogočajo izvajanje mobilnosti podatkov, je potrebno izpostaviti 7 procesov in 2 nivoja sistemov (Novak, 2004, III-3):

- *Transformacija podatkov*: je pojem, ki se uporablja pri preoblikovanju podatkovnih struktur iz strukturiranih oblik v nestrukturirane in obratno. Uporablja se tudi pri označevanju preobrazb z dodajanjem ali pa odvzemanjem podatkovnih entitet. Transformacija je uporabna za redukcijo podatkovne strukture, kadar ne rabimo določenih entitet, seveda pa je možno tudi preoblikovanje v obratni smeri, ko z dodajanjem podatkovnih entitet izpopolnjujemo podatkovno strukturo.

- *Konverzija podatkov*: označuje zamenjavo ene vrste podatkovnega zapisa z drugo. Načini podatkovnega zapisa so odvisni tako od operacijskega sistema (kodne tabele), kot tudi od uporabljenih programskih rešitev, ki lahko uporabljajo standardiziran način zapisa ali pa tudi ne (interni standardi).
- *Migracija podatkov*: prenos iz enega podatkovnega okolja v drugo. Označuje tudi prenos iz zastarelega medija na novejši, bolj ustrezen nosilec.
- *Enkapsulacija*: je pojem, ki označuje kontroliranje oblike transformacije natančno določenih podatkovnih struktur arhiva. Omogoča jo dodajanje metapodatkovnih struktur. Izvajamo jo z namenom, da podatkovnim strukturam, ki morajo ostati nespremenjene, omogočimo obstoj samim po sebi, kot tudi v odnosu do digitalnega okolja v katerega so posredovane.
- *Agregacija*: združevanje, spojitev podatkov iz razdrobljene oblike v širši okvir.
- *Generalizacija*: posploševanje podatkov.
- *Asociacija*: vzročna povezava med logično povezanimi podatki.
- *Izvorni informacijski sistem*: je tisti, iz katerega jemljemo podatkovne strukture za izvajanje postopkov transformacije, konverzije, migracije ali njihove kombinacije. Generiramo standardne ali nestandardne podatkovne strukture, ki omogočajo nadaljnje postopke.
- *Ponorni informacijski sistem*: je tisti, kamor se po opravljenih procesih oz. njihovi kombinaciji stekajo podatki iz izvornega sistema preko standardne točke. Standardna točka je stanje vnaprej dogovorjene podatkovne oblike, forme ali strukture podatkov, ki je primerna za prenos podatkov med informacijskimi sistemi in to ne glede na tehnike izvedbe postopkov, ki smo jih uporabili.

Če podatki, ki so bili dodani v elektronski arhiv, niso pod posebnim varstvom (osebni podatki), so lahko z informacijsko-tehničnega vidika takoj na razpolago. Z arhivsko-strokovnega pa ne, saj je potrebno arhiv še urediti, to je vzpostaviti relacije med podatki.

Ugotovimo, da se pri prevzemanju digitalnega gradiva izvajajo procesi (Novak, 2004, III-9):
- *priprava podatkov izvornega sistema v elektronski obliki pri ustvarjalcu ali predajniku do standardne oblike,*
- *fizični prenos podatkov do izvornega sistema in instalacija v ponornem sistemu,*
- *deinstalacija metapodatkovnih struktur pri ustvarjalcu in njihova namestitev v ponornem informacijskem sistemu,*
- *instalacija spremljajoče dokumentacije v ponorni informacijski sistem*

Na elektronskih dokumentih se za razliko od klasičnega arhivskega gradiva lahko izvajajo procesi migracije, konverzije, enkapsulacije (časovni žig) in transformacije.

Do sprememb prihaja pri predaji elektronskega gradiva v klasični arhivski dejavnosti na naslednjih ravneh (Novak, 2004, III-10):

- *Raven dogovornih osnov procesov*: določa načine in oblike izvajanja prevzemanja podatkov arhivske vrednosti (npr. mednarodni standard MOREQ).
- *Tehnološko-tehnična raven*: služi kot podpora procesu, vsebuje naslednje ravni:
  - *Raven podatkovne berljivosti*: dosežemo jo s konverzijo podatkovnih struktur v elektronski oblik ali s celovitim razumevanjem podatkovnih struktur.
  - *Raven vsebine*: nujno je dokumente ovrednotiti kot arhivske, saj je dandanes med vhodnimi dokumenti mnogo smeti (koncepti istega dokumenta, »spam«…).
  - *Raven konteksta*: v digitalnem okolju igra ključno vlogo, je strokovno najpomembnejša aktivnost, saj daje potrebne geografske, časovne in druge okvire v elektronskem arhivu zapisanih dejstev.

Ključno spoznanje tega poglavja je, da so podatki v elektronski obliki v celoti mobilni le, če je v ponornem sistemu mogoče uspešno zagotoviti tudi ustrezne migracije metapodatkovnih vsebin. Vse faze postopka je potrebno dokumentirati in zapisati v ponornem sistemu.

4. Arhiviranje pri zunanjem ponudniku (angl. Outsourcing)

Trend v modernem podjetju je v zadnjem času izločanje vseh nebistvenih dejavnosti iz okvira samega podjetja. Nove tehnologije namreč zahtevajo velika vlaganja v strojno in programsko opremo podjetja, izobraževanje kadrov, ki imajo opravka s to tehnologijo, prenovo procesov v podjetju. Najlažjo rešitev tako predstavlja prenos teh aktivnosti k zunanjim ponudnikom, t.i. outsourcing. Tem podjetjem je arhiviranje dokumentov osnovna dejavnost, v njej so dosegli veliko specializiranost, sledijo najnovejšim tehnologijam in tako lahko ponudijo podjetjem, ki sodelujejo z njimi, bistveno višjo raven storitve z nižjimi stroški.

V Sloveniji začetki tovrstnih izločanj segajo v čase sanacije bank v začetku devetdesetih let. Zunanji ponudnik je bil prisiljen prevzeti delavce banke, tako da takrat problem zaupanja v zunanjega ponudnika ni bil posebej pereč. Naročniki se tako niso ukvarjali z vprašanji odgovornosti za dokumente oz. zaupnosti vsebin teh dokumentov. Vsa ta vprašanja so bila rešena na pogodbenem nivoju, ne pa na operativni ravni, ki omogoča naročniku dejanski nadzor nad izvajanjem pogodbenih določil. Kot v ostalih panogah, se je tudi v dejavnosti arhiviranja počasi zaostrila konkurenca, začela se je tehnološka borba. Nekateri ponudniki so svojo priložnost videli v nizki ceni, ki pa s seboj potegne tudi nižjo raven storitve, izpuščanje posameznih faz obdelave, kot na primer primopredaja in kontrola kvalitete. Za resne stranke taka storitev ni zanimiva, pri digitalnem arhiviranju je namreč ključno zagotavljanje verodostojnosti obdelav in sledljivost postopkov.

Zakon o elektronskem poslovanju in elektronskem podpisu ni rešil vseh težav glede pravne veljave skeniranih dokumentov in arhiviranja teh digitalnih podob dokumentov. Digitalni podpis in časovni žig omogočata širitev elektronskega poslovanja, a ne odpravljata ključnih težav. Ali digitalni podpis resnično zagotavlja, da je digitalna podoba, ustvarjena s

skeniranjem, istovetna izvirniku? Takšno istovetnost lahko potrdi primerjava z izvirnikom. Če pa izvirnikov po obdelavi ne smemo uničiti, je digitalizacija zelo vprašljiva, saj je zmanjšanje stroškov arhivskega prostora ena najpomembnejših prednosti elektronskih arhivov. Verodostojnost digitalnih dokumentov z izvirniki lahko sicer dokažemo tudi na osnovi primerjave vsebine podobe z npr. vsebino knjige računov, dnevnika knjiženja itd. Tega problema razen z državnimi koncesijami, ki bi izbrana podjetja verificirala za zaupanja vredna, ni mogoče rešiti. Eden ključnih načinov za povečanje dokazne vrednosti digitalnih dokumentov je tako le zagotavljanje celovite revizijske sledi obdelave za vsak posamezen dokument. Da bi bil zajem dokumentov v elektronsko obliko čimbolj verodostojen, je treba slediti proces zajema skozi vse postopke obdelave, takšno revizijsko sled obdelave pa arhivirati kot sestavni del dokumenta v elektronskem arhivu. Za vsako fazo postopka je potrebno ugotoviti kdo in kdaj jo je izvedel.

Pri zunanjem izvajanju storitev arhiviranja papirnih dokumentov v elektronsko obliko se postopek prične z odpremo dokumentov v obdelavo. Zato je treba pričeti z izvajanjem revizijske sledi obdelave dokumenta s postopkom odpreme.

Posamezne faze in odgovornosti so naslednje (Pauletič, 2004, str. IV-72):

- odprema na obdelavo (delavec naročnika),
- transport dokumentov na obdelavo (oznaka zabojnika),
- sprejem dokumentov na obdelavo (pred pričetkom obdelave),
- skladiščenje dokumentov (skladiščni prostor in regal),
- tehnična in vsebinska priprava pred skeniranjem (oznaka pladnja),
- skladiščenje pladnjev (skladiščni prostor in regal),
- skeniranje (oznaka naprave, paketa),
- skladiščenje skeniranih dokumentov (oznaka paketa, direktorija, strežnika),
- skladiščenje izvirnikov po obdelavi (skladiščni prostor in regal),
- komisijsko uničenje izvirnikov dokumentov ali pospravljanje v prvotno obliko,
- transport razrezanih dokumentov na razgradnjo ali vračilo izvirnikov nazaj stranki,
- preverjanje pravilnosti strojno zajetih podatkov,
- kontrola ustreznosti obdelav in kakovosti (digitalni podpis in časovni žig),
- uvoz dokumentov v elektronski arhiv naročnika ali ponudnika,
- zapis na medije in registracija medijev v elektronskem arhivu,
- transport in dobava medijev k naročniku.

V prihodnosti nameravajo iti podjetja, ki pogodbeno izvajajo digitalno arhiviranje za zunanje naročnike, v smeri prevzema t.i. »sprejemnih pisarn«. Tovrstna storitev pomeni prevzem dokumentov iz poštnega predala naročnika, njihova celovita obdelava ter distribucija v naročnikovo podatkovno bazo. Sprejemna pisarna naj bi v prihodnosti predstavljala vez med klasičnim in elektronskim poslovanjem. Namen tovrstne ponudbe je razbremeniti naročnika poslovanja s papirjem.

Nekatere dokumente je potrebno dolgoročno ohraniti tudi v izvirni, papirnati obliki. Za uspešno izvedbo te storitve je nujno izgraditi fizična skladišča, ki so dobro varovana in zaščitena pred morebitnimi nesrečami (požar, potres, poplava…). V prihodnje je nujno zagotoviti še celovitejšo preglednost procesov s strani naročnika. Zaželjen je vpogled preko spletnega brskalnika v proizvodni informacijski sistem zunanjega izvajalca. Če danes zadostuje kdo, kdaj in kje je dokument skeniral si bodo jutri naročniki želeli še informacijo, v katerem prostoru se je dokument nahajal v postopkih obdelave, kateri delavci so ga imeli možnost videti v katerikoli obliki, kje so bile opažene napake pri obdelavi…

V ZDA in Zahodni Evropi je pri tovrstnih ponudnikih opaziti trend izvajanja t.i. »Offshore Data Capture«. Gre za to, da se določene storitve, ki niso lokacijsko vezane na lokalno okolje, izvajajo v državah s cenejšo delovno silo. Poleg tega so opazni tudi ugodni poslovni učinki zaradi še večje specializacije opravil, poenostavitve opravil, zmanjšanja podpore ter zagotavljanja storitev z manj osnovnimi sredstvi. Tako se storitve ročnega vnosa podatkov selijo v države, kjer je strošek dela tudi 8-10 krat nižji, dodatna prednost pa je tudi krajši čas obdelav zaradi časovnih razlik. Nujno pa je, da si podjetje že pred globalno širitvijo zagotovi zadostno količino obdelav, saj je nakup opreme in upravljanje procesov na daljavo povezano s precejšnjimi stroški.

5. Varovanje in zaščita informacij

Pri poslovanju modernega podjetja so informacije ključnega pomena. V primeru ogroženosti informacij je v nevarnosti obstoj podjetja kot celote. Informacije bi lahko opredelili kot »življenjsko tekočino, ki, podobno kot kri pri človeku, omogoča obstoj organizacije.«

Naša družba prehaja v informacijsko dobo, ki je odvisna od pretoka informacij in s tem posledično uporabe omrežij, v pretežni meri interneta, za komunikacijo s strankami, dobavitelji, izvajalci, zastopniki, zaposlenimi… Tovrstna povezljivost prinaša podjetjem nešteto prednosti, hkrati pa jih sili v nove izzive, povezane z varovanjem informacij, ki so ključni faktor pri novem načinu poslovanja. Dejavniki, ki ogrožajo informacije prihajajo tako od zunaj (virusi, trojanski konji, napadi hekerjev…), kot iz podjetja samega (okvare strojne opreme, napake uporabnikov, neučinkovita uporaba opreme, zlonamerne akcije uporabnikov…).

Pri varovanju in zaščiti informacij gre v osnovi za (Šalej, 2004, str. VI-18):

- *Razpoložljivost informacij*: informacije in storitve so na voljo pooblaščenim uporabnikom takrat, ko jih potrebujejo.
- *Neoporečnost informacij*: informacije so takšne, kot so, in niso bile nepooblaščeno spremenjene.
- *Zaupnost informacij*: Dostop do informacij imajo le pooblaščeni, torej osebe katerim so v osnovi namenjene.

Za zagotavljanje zgoraj navedenih zahtev so v uporabi različni mehanizmi, kot so avtentikacija, avtorizacija, šifriranje, varnostne kopije, ločevanje funkcij… Samo varovanje informacij se izvede z implementacijo varnostnih kontrol na informacijskih virih. V uporabi je predvsem kodeks za varovanje informacij BS 7799 in njegova ISO izpeljanka ISO 17799.

Standarda BS 7799 in ISO 17799 navajata priporočene kontrole, ki so razdeljene v 10 poglavij, katera vsebujejo varnostno politiko, organizacijske kontrole, kontrole v zvezi z zaposlenimi, fizično varovanje, kontrole dostopa, upravljanje informacijskega sistema, razvoj programske opreme in zagotavljanje neprekinjenega poslovanja. Seveda to ne pomeni, da mora vsako podjetje uvesti vse priporočene kontrole. Vse je odvisno od podjetja samega, njegove ogroženosti, ki se izrazi z oceno tveganja.

5.1 Faze pri uvajanju sistema za varovanje in zaščito informacij

Današnje grožnje na informacijskem področju so preveč kompleksne, da bi se jih dalo zreducirati na primerno raven z nakupom npr. samo nove programske opreme. Rešitev je veliko bolj kompleksna in zahteva mnogo časa, angažiranja zaposlenih in predvsem finančnih sredstev. Vzpostaviti je treba sistem za varovanje in zaščito informacij, ki bo varoval tako pred današnjimi, kot tudi bodočimi grožnjami na informacijskem področju. Strategija obrambe mora ustrezati velikosti podjetja, načinu poslovanja, panogi, organizacijski kulturi, znanju…

Faze pri uvajanju sistema za varovanje informacij so naslednje (Šalej, 2004, str. VI-19):

- *analiza stanja,*
- *ocena tveganj,*
- *postopek zmanjševanja tveganj,*
- *politika varovanja in zaščite informacij*.

Analiza stanja

Namen te faze je ugotoviti dejanski trenutni nivo varovanja in zaščite informacij v organizaciji. Glede na izbrani standard (npr. ISO 17799) se izvede pregled uvedenih varnostnih kontrol, ki jih ta standard opredeljuje in priporoča. Končni izdelek te faze je poročilo o skladnosti, ki navaja, katere kontrole so v organizaciji implementirane in katere ne.

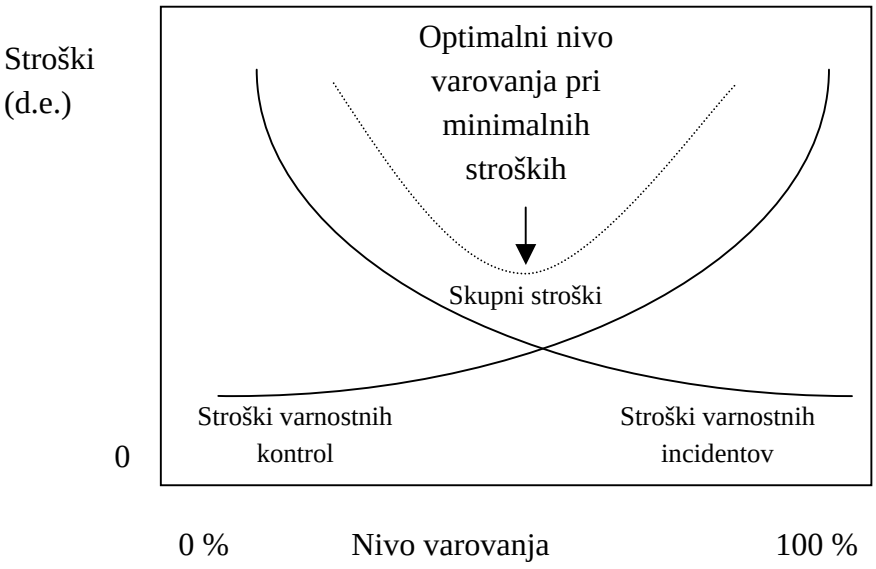
Ocena tveganj

Opredeli, ali trenutne uvedene kontrole zadoščajo, ali pa je potrebno varnost informacijskega sistema izboljšati. Potrebno je oceniti, koliko informacijske varnosti podjetje potrebuje in kakšni so še mogoči stroški za to področje. Stroški so lahko veliki, lahko pa veliko izboljšanje zaščite dosežemo že z uvedbo ali spremembo postopkov, kar zahteva le čas, energijo in strpnost.

Ocenjuje se torej tveganja, katerim so informacijski viri izpostavljeni. Za določitev tveganja je nujno za vsak informacijski vir določiti odnos med grožnjami, ki viru pretijo, ranljivostmi, ki so v viru navzoče, in vrednostjo vira za obstoj podjetja. Če grožnje ni oz. vir ni posebno ranljiv, potem so tveganja minimalna in obratno. Grožnje je praktično nemogoče odpraviti, tveganje lahko zmanjšamo le z zmanjšanjem ranljivosti. Večje kot je tveganje, večja je možnost, da se grožnja uresniči ter uniči ali poškoduje vir.

Slika 8 prikazuje optimalni nivo varovanja v podjetju. Stroški varovanja se s povečevanjem nivoja varovanja strmo povečujejo, hkrati pa padajo stroški morebitnih incidentov, povezanim z varnostjo informacijskih virov. Optimalni nivo varovanja je tisti, pri katerem funkcija skupnih stroškov varovanja doseže svoj minimum.

Slika 8: Optimalni nivo varovanja informacijskih virov

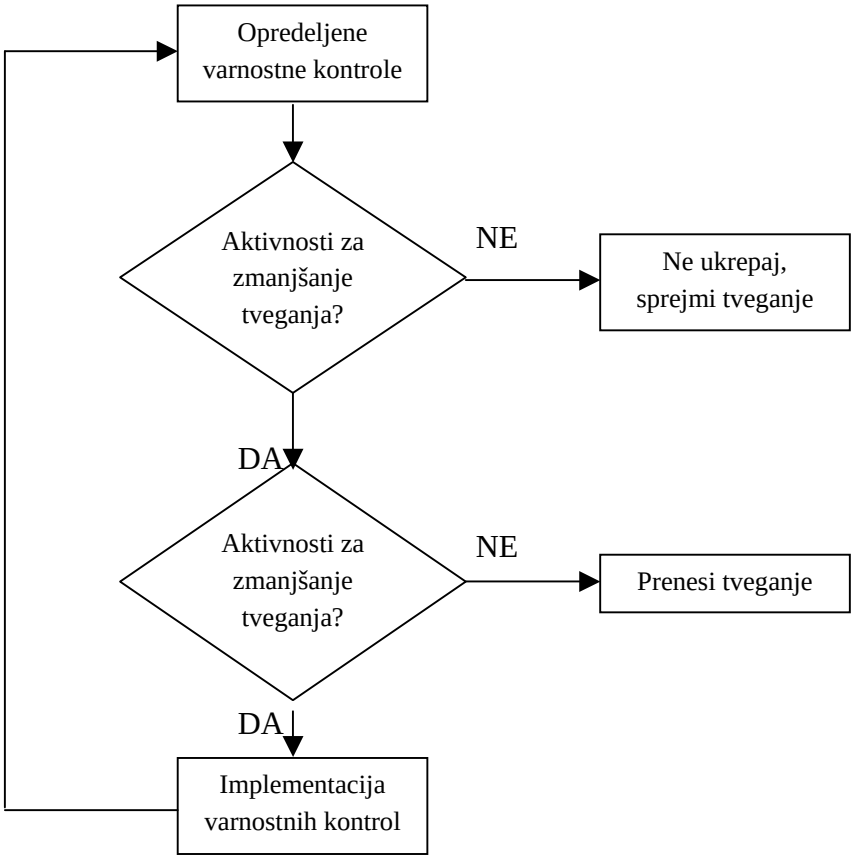


Vir: Šalej, 2004, str. VI-20.

Postopek zmanjševanja tveganj

Za ustrezno zavarovanje informacijskih virov je potrebno poleg same ogroženosti virov preučiti še druge zahteve kot so: zakonske in pogodbene obveznosti, standarde, organizacijske predpise… Namen vseh teh postopkov je zmanjševanje tveganja oz. prenos odgovornosti na tretjo osebo, kot je npr. zavarovalnica. Postopek je potrebno ponavljati toliko časa, da spravimo tveganje na sprejemljiv nivo. Ta cikličen postopek prikazuje Slika 9 na naslednji strani.

Slika 9: Postopek za zmanjševanje tveganj



Vir: Šalej, 2004, str. VI-21.

Rezultat tega postopka je seznam priporočenih kontrol z opredeljenim terminskim planom implementacije kontrol. O tem, katere kontrole se bo uvedlo in kdaj, odloča vodstvo podjetja, saj so le te velik finančni zalogaj. Če so stroški za uvedbo določene kontrole preveliki, je smiselno razmisliti vsaj o alternativnih možnostih, ki bodo tudi nekoliko zmanjšale tveganje. Po odobritvi vodstva informatiki izdelajo plan uvedbe. V njem je dosledno navedeno kdo in kdaj bo implementiral kontrole. To je tudi pravi trenutek za začetek izdelave spremljajoče dokumentacije, ki navaja politike varovanja in zaščite informacij.

Politika varovanja in zaščite informacij (PVZI)

Dokument z opredelitvijo PVZI zaokroži in dokumentira postopek implementacije sistema za varovanje in zaščito informacij. Opis je večnivojski, saj se postopoma prehaja od navedbe ciljev k opisu konkretnih postopkov in tehnologij, ki omogočajo njihovo izvršitev. Cilji so vezani na dolgo obdobje, uporabljena tehnologija pa je zastavljena bolj kratkoročno, saj se s časom hitro spreminja. Večnivojska struktura dokumenta je zato priporočljiva tudi zaradi tovrstnega časovnega okvira. Pojav nove tehnologije tako zahteva le majhne spremembe v določenih poglavjih. PVZI je dokument, ki se časovno nujno mora spreminjati, seveda le v delih, kjer je to potrebno.

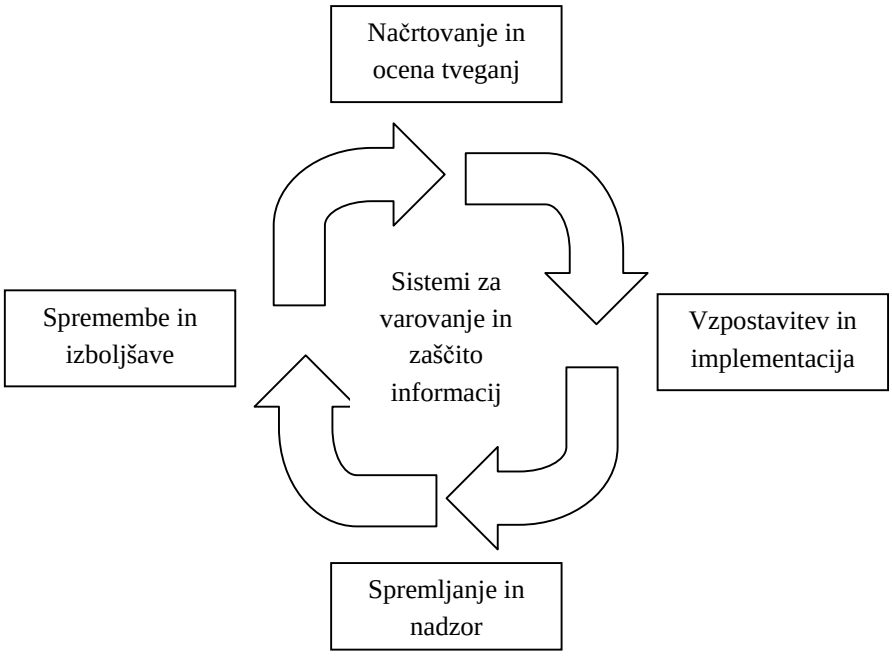
Takšna izvedba dokumentacije omogoča izdelavo priročnikov, ki so namenjeni določenim končnim uporabnikom. Celoten PVZI je zaupne narave in kot tak ni na razpolago komurkoli. Strukturna zasnova omogoča, da se vsebine razdelijo specifičnim skupinam, kot so uporabniki, vzdrževalci informacijskega sistema, revizorji… Nujno je, da politiko predpiše predsednik uprave podjetja, saj se tako še dodatno poudari, da velja za podjetje za celoto.

5.2 Uvedba varnostne politike na nivoju celotnega podjetja

Po dokumentiranju in uveljavljanju politike varovanja in zaščite informacij nas čaka še najkompleksnejši del celotne naloge - vzpostavitev delujočega sistema. Potrebno je vse vpletene seznaniti z vsebino, ki se nanaša na cilje, pravila, postopke in jih ustrezno izobraziti. Pozitiven zgled mora dati tudi uprava, ki s celovitim upoštevanjem pravil pokaže, da uvedena politika velja enako za vse, ne glede na hierarhijo v podjetju.

Klobčič potrebnih postopkov nam prikazuje Slika 10. Po uvedbi politike je, kot je prikazano, potrebno uvesti nadzor nad izvajanjem politike in uvesti učinkovit sistem uvajanja sprememb in izboljšav na delujočem sistemu. Tako se cikel začenja vedno znova. Spremembe se pojavljajo zaradi nenehnih sprememb v poslovnem okolju podjetja. Zaznavanje teh sprememb in učinkovito ukrepanje je ključnega pomena za celovito vzpostavitev sistema za varovanje in zaščito informacij v organizaciji.

Slika 10: Vzpostavitev sistema za varovanje in zaščito informacij



Vir: Šalej, 2004, str. VI-22.

6. E-storitev Pošte Slovenije moja.posta.si

Pošta Slovenije je bila v preteklosti bolj kot po visoki tehnologiji znana po uniformiranih možeh, ki na kolesu, mopedu ali peš polnijo pisemske nabiralnike. Ob besedi pošta najprej pomislimo na prenašanje sporočil, slovenska Pošta pa je po 500 letih delovanja ohranila vlogo prenašalca in jo kot eno največjih informacijskih podjetij razširja tudi na elektronske komunikacijske kanale ter elektronska sporočila.

Prehod na nov sodoben informacijski sistem Pošte Slovenije sovpada s časom, ko je leta 1995 Pošta izšla iz podjetja PTT. Takrat je bil informatiziran le čelni del Poštne banke ter nakateri procesi znotraj poštnih logističnih centrov, vse skupaj pa ni bilo povezano. Z ločitvijo od PTT se je pošta veliko bolj tržno usmerila, največja težava pa je bila, da informatika ni mogla pravočasno izpolnjevati naraščajočih zahtev uporabnikov glede novih storitev. Potrebovali so odprto in prilagodljivo informacijsko infrastrukturo, kateri bi lahko nove storitve hitro dodajali. Celoten informacijski sistem je Pošta postavila na novo, s stare osnove so prenesli le podatke. Največ pozornosti so namenili izvedbi *Univerzalnega poštnega okenca*, ki je podpiral standardne posle oz. procese na 1250 poštnih okencih.

Konec leta 2001 so na Pošti Slovenije sprejeli strategijo e-poslovanja in te aktivnosti z »e« predznakom so razdelili na tri obsežne sklope:

- *Notranje e-poslovanje*: namen je bil znižanje stroškov in pretočnih časov.
- *Selitev določenih klasičnih poštnih storitev v elektronsko obliko.*
- *Pošta na zvezi:* sklop projektov, med drugim agencija za izdajo digitalnih potrdil ter e-storitvi moja.posta.si in poslovna.posta.si.

6.1 Informacijski sistem Pošte Slovenije

Potrebe po novem informacijskem sistemu je še potenciral takrat obstoječi sistem na osnovi OS/2, ki je zašel v slepo ulico in problem letnice 2000. Analitiki Pošte Slovenije so temeljito preučili ponudbo na slovenskem trgu in postavili sledeče zahteve za nov informacijski sistem:

- *robustnost,*
- *zanesljivost,*
- *možnost širitve*
- *skupni stroški lastništva za 5 let.*

Za dobavitelje strojne opreme so izbrali HP, ponudnik programske osnove pa je bil Microsoft. Takšen prehod na povsem nov sistem je bil zelo pogumna poteza, saj tako veliki sistemi navadno nastajajo z evolucijo skozi daljše časovno obdobje.

Poštin IS zdaj podpira skupno 1900 delovnih mest na skoraj 600 lokacijah. Strežniška infrastruktura temelji na 650 HP-jevih strežnikih ProLiant, ki so nameščeni na 550 lokacijah in formirajo trinivojsko strukturo. Večina aplikacijskih, datotečnih in transakcijskih

strežnikov deluje na operacijskem sistemu Windows 2000 Server, za terminalski dostop do pisarniških orodij pa uporabljajo Windows Server 2003. Za različne poslovne aplikacije imajo nameščenih okrog 600 SQL podatkovnih baz. Zaradi svoje tradicionalne vloge prenašalca sporočil je Pošta Slovenije zgradila tudi moderen komunikacijski sistem. Obsega 5000 km komunikacijskih povezav in je formiran v obliki križa Kranj-Novo Mesto in Koper-Murska Sobota, pri čemer so vse povezave in ključni sestavni deli podvojene. Prepustnost omrežja presega 4 GB/s, v centralnem mariborskem informacijskem centru pa se nahaja več kot 200 1 GB vrat za povezavo strežnikov. Pri izgradnji komunikacijskega omrežja, ki temelji na Ciscovi tehnologiji, so upoštevali možnost nadaljnjega razvoja z minimalnimi stroški. Uvedli so izjemno učinkovit programski sistem obvladovanja omrežja imenovan Spectrum, saj za preko 15000 sestavnih delov skrbi le 35 zaposlenih informatikov.

Takšen sistem zagotavlja praktično 100 % razpoložljivost sistema, močno zniža stroške obratovanja in vzdrževanja, omogoča centralizirano upravljanje s celotnim sistemom, kar skupaj z drugimi dejavniki navsezadnje močno izboljša kvaliteto poštne storitve. Od začetka prenove je Pošta Slovenije v svoj informacijski sistem vložila 3,5 milijarde tolarjev, letno namenja za področje informatike 10 do 15 % naložbenih sredstev, kar je približno odstotek celotnih prihodkov (torej okoli 700 milijonov tolarjev).

6.2 Kaj je moja.posta.si?

E-storitev Pošte Slovenije moja.posta.si je nastala kot nadgradnja obstoječe informacijske infrastrukture, ki je bila ustvarjena za potrebe agencije za izdajanje digitalnih potrdil Pošta®ca. Pošta izdaja tri tipe kvalificiranih digitalnih potrdil:

- *Napredno*: dva para ključev, en namenjen digitalnemu podpisu, drugi šifriranju podatkov.
- *Standardno*: en par ključev, uporaben tako za podpisovanje, kot šifriranje.
- *Standardno z uporabo pametne kartice*: varnejša izpeljanka standardnega potrdila.

Digitalno potrdilo tako služi kot osnova, na kateri temeljijo napredne elektronske storitve. Moja.posta.si v osnovi ponuja storitve *posredovanja e-dokumentov*, kjer Pošta ponuja *predale*, kamor se shranjujejo prispeli dokumenti. Uporabnik do predalov dostopa preko spletnega brskalnika s pomočjo ustreznega digitalnega potrdila. Moja.posta.si omogoča, da si uporabnik dokumente, ki jih je prvotno prejemal po klasični poti, prenese preko spleta v elektronski obliki. Ti dokumenti so lahko računi in druga množična pošta, kakor tudi osebna pošta, pretvorjena v digitalno obliko. Sistem ponuja tudi storitev pooblaščanja imenovano *Naslovnikovo naročilo*, kjer prejemnik preusmeri prejeto pošto kamorkoli oz. zanjo pooblasti kogarkoli za določeno časovno obdobje ali za stalno. Dodali so tudi *funkcijo elektronskega arhiviranja dokumentov* za izdajatelje, ki jih je trenutno okoli 60 in prejemnike e-dokumentov. Prejemnikom je namenjen tudi *trezor*, ki izpolnjuje vse kriterije za varno hranjenje elektronskih dokumentov.

Pri prejetih računih sistem omogoča storitev *plačevanja*, saj se povezuje z bančnimi sistemi na ravni informacijskega sistema. Kvalificirano digitalno potrdilo Pošte Slovenije ustreza

zahtevam Banke Slovenije in Zakonu o bančništvu, saj ponuja časovno žigosanje, ki je pri plačevanju računov nujno potrebno. V teku so pogajanja glede priznavanja digitalnega potrdila Pošte Slovenije z večino slovenskih komercialnih bank, trenutno pa je dogovor o priznavanju kvalificiranega digitalnega potrdila Pošta®ca sklenjen s Poštno banko Slovenije. Plačevanje računov v sistemu moja.posta.si je izredno preprosto, saj je potrebno le določiti, pri kateri banki se račun poravna, vse ostalo pa sistem izvede avtomatsko. Računi so v formatu *e-Slog*, Pošta pa se lahko s formatom računa prilagodi izdajatelju. Podjetje tako lahko posreduje celoten nabor podatkov ali računov Pošti, ta pa poskrbi za elektronsko in tiskano distribucijo računov k naslovnikom.

V prihodnosti načrtujejo v okviru storitve moja.posta.si ponuditi tudi nekatere uporabne programe, kot so obveščanje o odstopanju računov od povprečja za določeno storitev, sporočanje sprememb stalnega bivališča naslovnika podjetjem… Na obzorju so tudi elektronske storitve za podjetja. Storitev poslovna.posta.si je usmerjena v racionalizacijo in pospešitev poslovanja podjetij s Pošto. Storitev bo obsegala predvsem prejemanje in oddajanje pošte (elektronska vročitev), pri čemer bo povezala uporabnikov informacijski sistem s pisemsko/paketnim modulom Poštinega informacijskega sistema. Pošiljanje elektronskih dokumentov bo v prihodnosti potekalo v obe smeri, saj bodo tako pri storitvi moja.posta.si, kot tudi poslovna.posta.si ponudili storitve optičnega branja (angl. Optical Character Recognition) oz. tiskanja dokumentov. Pošta kot član projekta e-Slog načrtuje oblikovanje vozlišča za posredovanje elektronskih dokumentov med podjetji (B2B), ponudila pa bo tudi storitev zunanjega elektronskega arhiviranja dokumentov za podjetja. Kljub ohranjanju klasičnih poštnih storitev je Pošta Slovenije v prihodnje eden glavnih oblikovalcev in pospeševalcev slovenskega trga e-storitev.

6.3 Razlogi za in proti e-storitvam

Po podatkih ameriškega urada za e-poslovanje omogočajo eksponentno rast elektronskega poslovanja podjetij predvsem nižji transakcijski stroški, zmanjšanje inventarja, krajši časi obračanja zalog, krajše dobavne poti, učinkovitejše poprodajne storitve, možnost globalnega poslovanja ter nove tržne priložnosti.

Kot najpomembnejše prednosti elektronskega poslovanja je 90 odstotkov anketirancev označilo: hitrost transakcije, boljše upravljanje s podatki, odpravo časovnih in krajevnih omejitev in dostop do globalnega tržišča. Sledijo naslednje prednosti: povečanje ravni storitev za kupca, dostop do konkurenčnega tržišča, zmanjšanje stroškov in zmožnost, da se celotni posel izvede elektronsko, kar je potrdilo več kot 80 odstotkov anketirancev.

Poleg dejstva, da internet uporablja skorajda polovica slovenskih gospodinjstev, gre na roko tudi dejstvo, da tehnologija, uporabljena za to storitev, predstavlja vsekakor nižji strošek, kakor pred nekaj leti. Pojavile so se standardizirane programske aplikacije, katerih zanesljivost in kakovost se je izoblikovala z leti uporabe in sprotnih izboljšav. Poleg tehničnih razlogov je v ospredju tudi pragmatični razlog. Tovrstne storitve pri nas enostavno še ni.

Glede na to, da je Pošta v tem sektorju monopolist, lahko del svojega poslovanja prenaša v e-obliko in s tem pridobi prednost pred potencialno konkurenco. Dejstvo je, da prvi konkurent na trgu pobere vso »smetano«.

Po raziskavah sodeč se, kljub vse večji razširjenosti uporabe interneta v Sloveniji, zaupanje do e-storitev ni povečalo. V Sloveniji je med uporabniki interneta še posebej nizka uporaba e-bančništva (SI 21% : EU 33%) in e-nakupovanja (SI 21% : EU 39%). V kolikor primerjamo to z zaupanjem in uporabo teh storitev v EU, ugotovimo, da je potrebno naše potrošnike za dokončen uspeh take storitve primerno ozavestiti. Le z ozaveščanjem in s primernim znanjem potrošnikov je lahko takšna storitev ekonomsko uspešna. Po mojem mnenju lahko v veliki meri nezaupanje potrošnikov do e-storitev pripišemo dvomom glede varnosti podatkov in zasebnosti transakcij.

To so splošni razlogi, zakaj se je Pošta Slovenije odločila uvesti e-storitve. Pošta Slovenije je na slovenskem trgu, kar se tiče osebne pošte, monopolist in tak vodilni položaj si seveda želi ohraniti tudi v prihodnje. To ji lahko uspe samo tako, da vlaga v moderne poslovne modele, ki bodo v prihodnosti zavzemali precejšen obseg poslovanja.

7. Sklep

Sistemi za celovito elektronsko obvladovanje dokumentacije bodo v prihodnosti predstavljali hrbtenico celotnega informacijskega sistema v podjetju. Managerji z izdelano vizijo bodo pravočasno zaznali vse možnosti, ki jim jih ponuja elektronsko arhiviranje, čeprav splošno veljavni standardi na tem področju še vedno niso sprejeti. V modernem poslovnem okolju primerjalne prednosti prinašajo že malenkosti, vpeljava učinkovitega informacijskega sistema pa je danes nujen pogoj za konkurenčnost v prihodnosti. Kljub velikim investicijam je vpeljava sistemov za elektronsko upravljanje dokumentov smiselna čimprej, saj bo podjetje lahko prednosti izkoristilo nemudoma in konkurenca ne bo imela možnosti, da bi se na tem področju oddaljila. Menim tudi, da kljub kritikam, naša vlada namenja zadosti pozornosti problematiki informatizacije. Sprejeti zakoni na tem področju so v skladu s svetovnimi trendi in zagotavljajo zadovoljivo infrastrukturo. Država bi lahko dala dober zgled podjetjem s čimprejšnjo izgradnjo delujočega sistema celotne elektronske uprave.

Sam menim, da bo razvoj na tem področju šel v smeri oddajanja tovrstnih storitev zunanjim ponudnikom. Le ti bodo izkoristili prednosti, ki jim jih nudi specializacija. Gre za ekonomije obsega, ki prinaša nižje stroške, boljše poznavanje predpisov in tehnologije, kar pomeni tudi višjo raven kakovosti storitve in večjo varnost hranjenih vsebin. Sodobna pisarna bo v prihodnosti delovala izključno elektronsko, brez papirja. Vhodno pošto bo prevzel zunanji izvajalec, jo digitaliziral in posredoval v podjetje. Komunikacija med podjetji bo tekla v elektronski obliki, morebitne izhodne dokumente v papirnati obliki bo prav tako obdelal zunanji sodelavec. Za uspešno dolgoročno hranjenje elektronskih vsebin bodo morali ponudniki storitev digitalnega arhiviranja redno analizirati spreminjajoče se tehnološko

okolje. Število institucij, ki se bodo ukvarjale s tovrstno dejavnostjo, se bo s časom zmanjšalo, preživele bodo le najboljše s certifikatom za zaupnost hranjenja. Najboljšo celovito rešitev na področju elektronskega arhiviranja je potrebno najti z različnimi pilotnimi projekti, spodbudami države in preizkusom rešitev v praksi.

Na koncu lahko izpostavim tudi sociološki problem elektronskega arhiviranja oz. življenja v t.i. digitalni dobi. Stvari, ki bodo hranjene na takšen način, nenadoma ne bodo več vidne, ne bodo imele oblike, vonja, zvoka, ne bo jih mogoče otipati. Komunikacija bo postala brezosebna, pogosto bo sogovornika zaznamoval le njegov elektronski naslov. Sčasoma bo tudi čedalje manj ljudi, ki bodo lahko obvladali razvijajočo se tehnologijo. Kje so sploh njene meje, bo nekoč tehnološki razvoj prišel do točke, ko ne bo več obvladljiv? Tehnologija namreč hkrati z novimi možnostmi prinaša mnoge nevarnosti in neznanke, saj je večja funkcionalnost tesno povezana s kompleksnostjo. Teoretično lahko vsak s pomočjo kompasa ali zvezd nastavi sončno uro, le redko kdo pa zna popraviti oz. razume delovanje digitalne ure, ki je hkrati bolj natančna in priročna.

Literatura

1. *Bakan Toplak Metka: Računalniško podprt pretok dokumentov v arhivu. DOK_SIS 1999. Ljubljana : Media.doc, 1999, str. I-12 – I-23.*

2. *Berčič Boštjan: Kako v skladu z zakonodajo določiti postopke arhiviranja v pravilniku o arhiviranju dokumentov. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. V-1 – V-7.*

3. *Chandler Doug, Young Jocelyn: The Business Benefits of Digital Archiving Solutions. [URL: http://www.ironmountain.com/File_Uploads/605_0_DA_Benefits.pdf], 2002.*

4. *Čufer Stanko: Sistemi za elektronsko upravljanje z dokumenti z vidika ekonomike podjetja. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. IV-10 – IV-15.*

5. *Gomboc Mateja: Zakaj in kako e-procesi v podjetjih. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. IV-16 – IV-20.*

6. *Jakovljevič Čedo: Upravljanje dokumentov – upravljanje znanja. DOK_SIS 1998. Ljubljana : Media.doc, 1998, str. I-63 – I-71.*

7. *Klasinc Peter Pavel: Slovenska arhivistika in zakon o elektronskem poslovanju in elektronskem podpisu. DOK_SIS 2001. Ljubljana : Media.doc, 2001, str. I-67 – I-73.*

8. *Kočevar Matija: Prednosti in slabosti pri upravljanju dokumentov. Gospodarski vestnik. Ljubljana : Gospodarski vestnik, 2002, 19, str. 16 – 17.*

9. *Kroflič Jernej, Jerman Blažič Aljoša: Varno arhiviranje elektronskih zapisov in storitve elektronskih notariatov. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. VI-54 – VI-65.*

10. *Lorist Jeroen: Standards for Digital Libraries and Archives. Delft University of Technology.*
[URL: http://www.betade.tudelft.nl/reports/Lorist_StandardsLongevity_20010307.pdf], marec 2001.

11. *Nose Boris: Potrebe po uvedbi sistemov za upravljanje z dokumenti v podjetju. DOK_SIS 2001. Ljubljana : Media.doc, 2001, str. I-97 – I-105.*

12. *Nose Boris: Pasti pri uvajanju dokumentarnega sistema. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. IV-51 – IV-54.*

13. *Novak Miroslav: Dokument kot izziv sodobnega poslovanja. DOK_SIS 2002. Ljubljana : Media.doc, 2002, str. III-56 – III-66.*

14. *Novak Miroslav: Problemi mobilnosti podatkov v arhivski teoriji in praksi. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. III-1 – III-12.*

15. *Pauletič Igor: Obdelava in arhiviranje dokumentov pri zunanjem ponudniku – zagotavljanje verodostojnosti obdelav in sledljivost postopkov. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. IV-68 – IV-73.*

16. *Preserving Digital Information.*
[URL: http://www.rlg.org/legacy/ftpd/pub/archtf/final-report.pdf], maj 1996.

17. *Reference Model for an Open Archival Information System (OAIS).*
[URL: http://www.ccsds.org/documents/650x0b1.pdf], januar 2002.

18. *Šalej Andrej: Vzpostavitev sistema za varovanje in zaščito informacij. DOK_SIS 2004. Ljubljana : Media.doc, 2004, str. VI-17 – VI-23.*

19. *Žerko Bine: IMiS® - Imaging, Made in Slovenia. DOK_SIS 2000. Ljubljana : Media.doc, 2000, str. III-8 – III-17.*

20. *Žorž Jaka: Od kolesa do e-storitev. Moj Mikro, Ljubljana, 2004, 4, str. 67 - 69.*

21. *Žumer Vladimir: Arhiviranje zapisov. Ljubljana : GV založba, 2001. 479 str.*

22. *Žužek Alenka, Dobnikar Aleš: Tehnična priporočila in pravni vidiki digitalnega arhiviranja. DOK_SIS 2003. Ljubljana : Media.doc, 2003, str. IV-31 – IV-37.*

Viri

1. *Cedars Guide to The Distributed Digital Archiving Prototype. [URL: http://www.leeds.ac.uk/cedars/guideto/cdap], marec 2002.*

2. *Hedstrom Margaret: Report and Recommendations of the NSF-DELOS Working Group on Digital Archiving and Preservation. [URL: http://delos-noe.iei.pi.cnr.it/digitalarchiving/Digitalarchiving.pdf], 2003.*

3. *MacTavish Susanne et al.: Electronic Digital Imaging Standards for Archiving Records. [URL: http://www.amibusiness.com/dcs/imagingstandards.pdf], junij 1999.*

4. *Model Requirements for the Management of Electronic Records. [URL: http://www.cornwell.co.uk/moreq], marec 2001.*

5. *Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000, 2/2001).*

6. *Zakon o arhivskem gradivu in arhivih (Uradni list RS, št. 20/97, 32/97).*

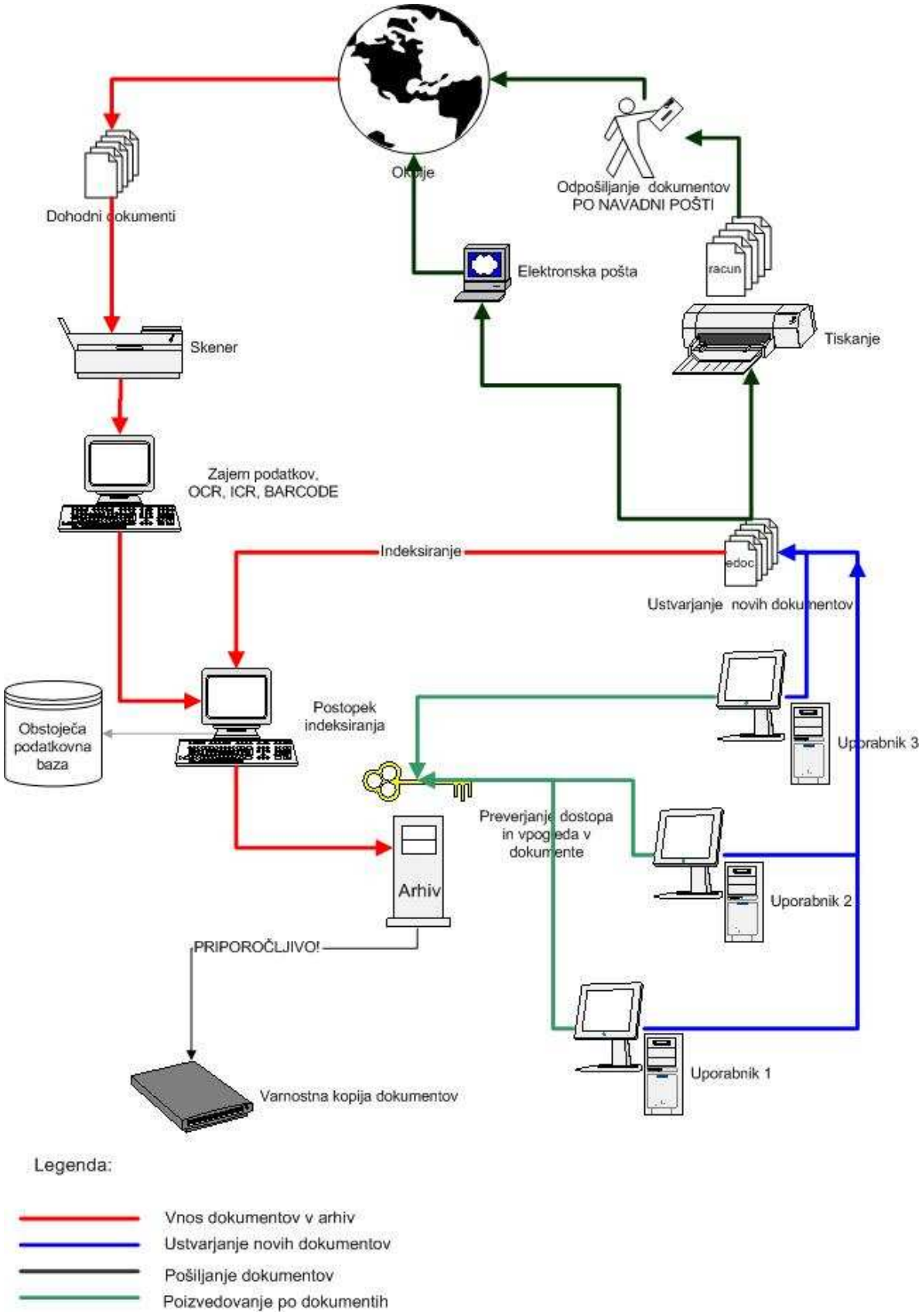
7. *Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000, 30/2001).*

Priloge

Slovarček slovenskih prevodov tujih izrazov:

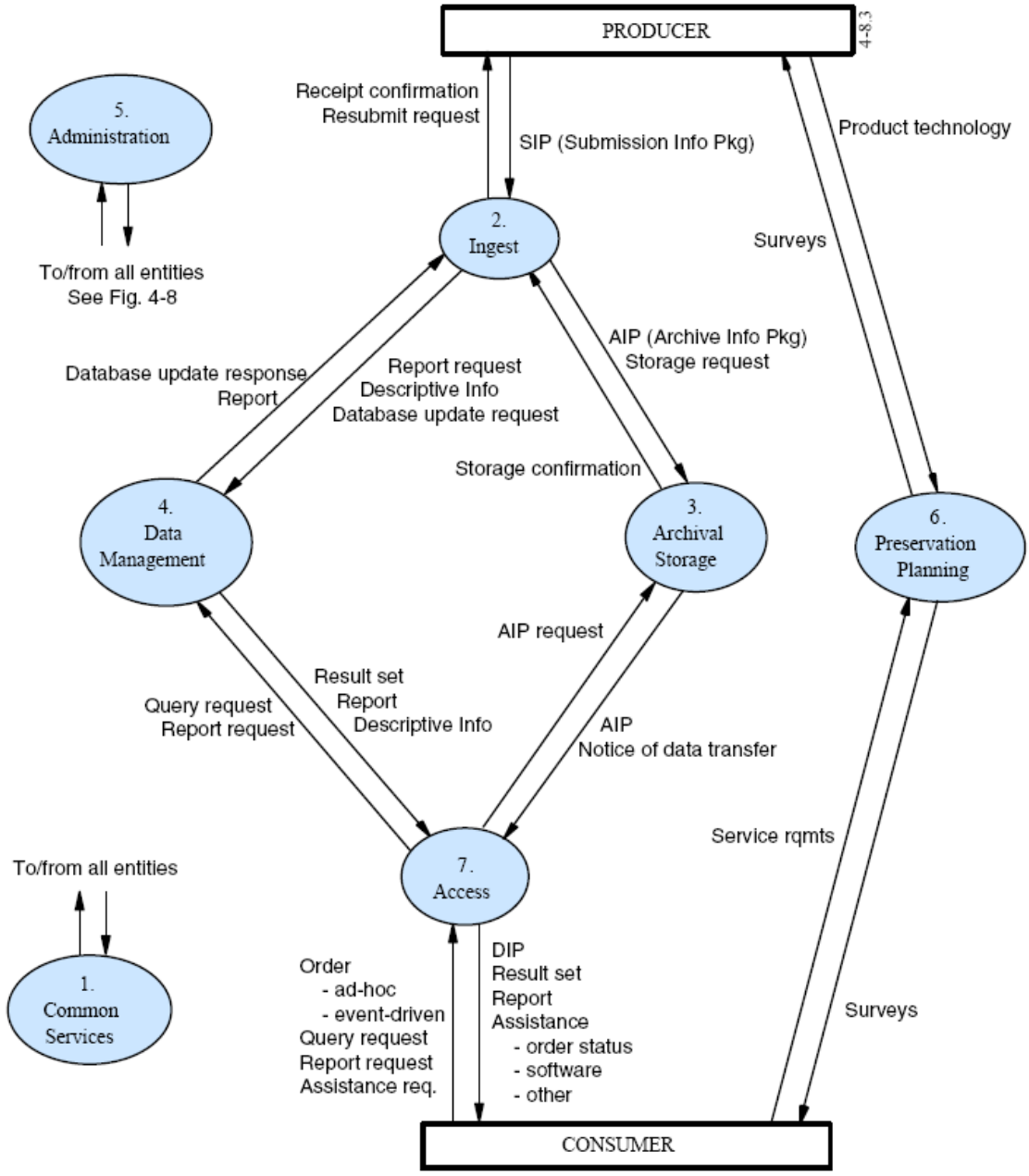
Archival Information Package (AIP) - arhivski informacijski paket
Backup – rezervna kopija
Certification Authority - overitelj digitalnih potrdil javnih ključev
Content Information - vsebinska informacija
Descriptive Information – opisna informacija
Digital Archiving – elektronsko arhiviranje
Disaster Recovery – obnovitev stanja pred uničenjem
Dissemination Information Package (DIP) - razposlan informacijski paket
Document Lifecycle Management – sistem za upravljanja življenjskega cikla dokumenta
Electronic Document Management System - sistem za elektronsko upravljanje z dokumenti
Hash Code – rezultat zgoščevalne funkcije
Open Archival Information System (OAIS) – odprti elektronski arhivski sistem
Optical Character Recognition – optična razpoznava znakov
Packaging Information – paketna informacija
Preservation Description Information - opisna informacija o hranjenju
Product Lifecycle Management - sistem za upravljanje življenjskega cikla proizvoda
Public Key Infrastructure - infrastruktura javnih ključev
Submission Information Package (SIP) - predložen informacijski paket
Time Stamp – časovni žig

Priloga 1: preprost prikaz procesov elektronskega arhiviranja



Vir: Comtech d.o.o., Ljubljana, 2004.

Priloga 2: diagram pretoka podatkov v modelu OAIS



Vir: Reference Model for an Open Archival Information System, 2002, str. 4-17.