REPUBLIKA SLOVENIJA
MINISTRSTVO ZA KULTURO
ARHIV REPUBLIKE SLOVENIJE
1127 Ljubljana, Zvezdarska 1, Slovenija, p.p. 21
Tel.: +386(1)2414200; fax: +386(1)2414269
e-mail: ars@gov.si; http://www.arhiv.gov.si

ENOTNE TEHNOLOŠKE ZAHTEVE

Verzija 1.0

Ljubljana, 01.12.2006

Nadzor dokumenta

Organizacija:	Arhiv Republike Slovenije
Naslov dokumenta:	Enotne Tehnološke Zahteve
Oznaka dokumenta:	ETZ
Šifra dokumenta:	382-17/2006/1
Status dokumenta:	končna
Verzija dokumenta:	1.0
Lastnik dokumenta:	Arhiv Republike Slovenije
Avtor dokumenta:	Arhiv Republike Slovenije

Zgodovina sprememb:

Različica dokumenta	Datum spremembe	Izvedene spremembe
1.0 – končna	01.12.2006	objava

KAZALO VSEBINE

1 UVOD 5
1.1 NAPOTKI ZA UPORABO 5
1.2 PRAVNA PODLAGA 5
1.3 POSTOPEK SPREJEMANJA 6
1.4 UVOD V ELEKTRONSKO HRAMBO 7
1.5 DEFINICIJE 12
2 ORGANIZACIJA IN NOTRANJA PRAVILA 22
2.1 NOTRANJA ORGANIZACIJA 22
2.2 INFORMACIJSKA INFRASTRUKTURA 23
2.2.1 Politika varovanja informacij 24
2.2.2 Organiziranost varovanja informacij 24
2.2.3 Upravljanje informacijskih sredstev 25
2.2.4 Varnost in človeški viri 26
2.2.5 Fizično in tehnično varovanje opreme in prostorov 27
2.2.6 Upravljanje komunikacijske infrastrukture in operativno delovanje 28
2.2.7 Obvladovanje dostopa do sistemov 30
2.2.8 Razvoj in vzdrževanje (aplikacijskih) informacijskih sistemov 31
2.2.9 Upravljanje varnostnih dogodkov 32
2.2.10 Zagotavljanje neprekinjenega delovanja 32
2.2.11 Zagotavljanje skladnosti na področju varovanja informacij 33
2.3 ZAJEM IN PRETVORBA 33
2.4 KRATKOROČNA HRAMBA 34
2.5 DOLGOROČNA HRAMBA IN NADZOR NAD IZVAJANJEM PRAVIL 34
2.6 UNIČEVANJE DOKUMENTARNEGA GRADIVA 35
2.7 ZAGOTAVLJANJE ZAPISOV O DELOVANJU SISTEMA 36
2.8 DELOVANJE V PREHODNEM OBDOBJU 36
2.9 SPREMLJANJE IN DOPOLNJEVANJE NOTRANJIH PRAVIL 37
2.10 HRAMBA ARHIVSKEGA GRADIVA 37
3 HRAMBA IN UPRAVLJANJE DOKUMENTARNEGA GRADIVA 39
3.1 RAZVRŠČANJE GRADIVA 39
3.1.1 Klasifikacijski načrt 39
3.2 NADZOR IN VARNOST 43
3.2.1 Dostop 44
3.2.2 Revizijske sledi 46
3.2.3 Rezervna kopija in obnova 48
3.2.4 Sledenje gibanju dokumentov 49
3.2.5 Avtentičnost in celovitost 50
3.2.6 Vrste in stopnje tajnosti 51
3.3 ROK HRAMBE IN IZLOČANJE 53
3.3.1 Roki hrambe 53
3.3.2 Pregled in odbiranje 56
3.3.3 Prenos, izvoz in uničevanje 58

3.4 ZAJEM IN PRETVORBA GRADIVA 60
3.4.1 Zajem in pretvorba gradiva 61
3.4.2 Masovni uvoz gradiva 64
3.4.3 Vrste zapisov 65
3.4.4 Upravljanje elektronske pošte 67

3.5 OZNAČEVANJE 68

3.6 ISKANJE, PRIKLIC IN PRIKAZOVANJE 69
3.6.1 Iskanje in priklic 70
3.6.2 Prikazovanje 73

3.7 SKRBNIŠTVO 75
3.7.1 Skrbništvo 75
3.7.2 Poročanje 77
3.7.3 Spreminjanje, brisanje in redakcija dokumentov 78

3.8 ZAHTEVE ZA METAPODATKE 80
3.8.1 Načela 81

3.9 HRAMBA IN PRETVORBA 84
3.9.1 Dolgoročna hramba in tehnološko zastaranje 85
3.9.2 Oblika zapisa 89
3.9.3 Pretvorba oblike zapisa 91
3.9.4 Nosilci zapisa 92
3.9.5 Izvoz in prenos gradiva 93
3.9.6 Hramba posebnih vsebin 94
3.9.7 Kombinirana hramba 97

3.10 ZAHTEVE GLEDE ARHIVSKEGA GRADIVA 100
3.10.1 Izročanje arhivskega gradiva pristojnemu arhivu 100
3.10.2 Hramba arhivskega gradiva v arhivu 101
3.10.3 Objava arhivskega gradiva na svetovnem spletu 101

4 ZAHTEVE ZA PONUDNIKE OPREME IN STORITEV *102*

4.1 SPLOŠNE ZAHTEVE ZA PONUDNIKE 102
4.1.1 Splošne zahteve 102
4.1.2 Zaposlovanje strokovnjakov pri ponudnikih opreme in storitev 102
4.1.3 Vrednotenje dodatnega strokovnega izobraževanja 102

4.2 ZAHTEVE ZA PONUDNIKE STROJNE OPREME 103

4.3 ZAHTEVE ZA PONUDNIKE STORITEV 104
4.3.1 Splošne zahteve za ponudnike storitev 104
4.3.2 Zahteve za ponudnike spremljevalnih storitev 105

5 ZAČETEK VELJAVNOSTI *107*

PRILOGE *108*

Priloga 1 – Seznam oblik zapisa za dolgoročno hrambo, ki ustrezajo zahtevam ETZ 108

Poleg mednarodnih standardov in priporočil so v seznamu navedeni tudi ustrezajoči slovenski standardi, če ti obstajajo. 108

Priloga 2 – Seznam mednarodnih standardov in priporočil 109

Poleg mednarodnih standardov in priporočil so v seznamu navedeni tudi ustrezajoči slovenski standardi, če ti obstajajo. 109

1 UVOD

1.1 NAPOTKI ZA UPORABO

V tem poglavju je opisana struktura in način uporabe enotnih tehnoloških zahtev.

Ta dokument vsebuje splošne enotne tehnološke zahteve. Poleg splošnih enotnih tehnoloških zahtev obstajajo tudi enotne tehnološke zahteve, ki se nanašajo zgolj na posamezno področje uporabe. Gre predvsem za hrambo gradiva v večjih javnih zbirkah in registrih, ki zaradi svojega specifičnega načina delovanja ter že vpeljanih ter preizkušenih tehnoloških in organizacijskih rešitev, ki niso primerne za splošnejšo uporabo, terjajo lastne, posebne enotne tehnološke zahteve pri izvajanju hrambe gradiva v elektronski obliki. Hramba dokumentarnega gradiva v vsaki izmed posameznih velikih javnih zbirk ali registrov bo zato urejena v posebnih enotnih tehnoloških zahtevah, ki bodo prilagojene drugačnim potrebam takšnih subjektov.

Splošne enotne tehnološke zahteve so celovit dokument, namenjen splošni uporabi pri zagotavljanju opreme in storitev povezanih s hrambo dokumentarnega gradiva v elektronski obliki. Sestavljene so iz posameznih poglavij, ki se nanašajo na zaokrožene vsebinske sklope oziroma poglavja, ki se nanašajo na različnima organizacijska in tehnološka vprašanja elektronske hrambe gradiva. Vsako poglavje vsebuje poleg uvodne razlage posamezne zahteve.

Posamezne tehnološke zahteve sledijo uvodu v posameznem podpoglavju. Zahtev je dvoje vrst:

- minimalne zahteve, ki morajo biti izpolnjene za samo registracijo ponudnika;
- dodatne zahteve, ki niso nujne, njihovo izpolnjevanje pa je zaželeno zaradi naprednejšega in uporabniku bolj prijaznega delovanja sistema ter večje združljivosti.

Posamezne zahteve so v dokumentu označene s številko, ki sledi oznaki ETZ (npr. ETZ 3.2.1.12, dodatne zahteve pa se od minimalnih ločijo po dodatku k številki v obliki črke, ki sledi poševnici (npr. ETZ 3.2.1.15/a).

Dodatne zahteve morajo izpolnjevati akreditirane storitve in oprema oziroma osebe, ki hranijo arhivsko gradivo.

1.2 PRAVNA PODLAGA

Temeljna pravna podlaga ne samo za sprejem enotnih tehnoloških zahtev, temveč tudi za pravno ureditev celotnega področja elektronske hrambe, predstavlja Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Ur.l. RS, št. 30/2006, v nadaljevanju: ZVDAGA).

Vendar ZVDAGA kot predpis ni pomemben le zato, ker ureja pravno veljavnost elektronsko hranjenega gradiva, temveč predvsem zato, ker postavlja pravno ogrodje za zagotovitev učinkovite infrastrukture, s pomočjo katere bo moč podpirati obsežno nalogo omogočanja elektronske hrambe vseh vrst gradiva – arhivskega in dokumentarnega, ne glede na njegov nastanek in rok hrambe.

Da bi ponudniki izpolnjevali vse zahteve in sledili temeljnim načelom ZVDAGA, morajo pri zagotavljanju naštetih storitev slediti podrobnejšim pogojem za opravljanje teh storitev. Ti pogoji so določeni v posebnem podzakonskem predpisu, Uredbi o varstvu dokumentarnega in arhivskega gradiva (Ur.l. RS, št. 86/2006) (v nadaljevanju: Uredba). Uredba vsebuje posamezne pogoje, ki jih morata izpolnjevati strojna in programska oprema za zajem in hrambo gradiva v elektronski obliki ali za spremljevalne storitve, splošne pogoje za hrambo gradiva v elektronski obliki ter posebne pogoje za hrambo specifičnega gradiva s posameznih področij (npr. javne evidence, prostorski podatki,…), splošne pogoje opravljanja spremljevalnih storitev ter posebne pogoje za specifične storitve v zvezi z gradivom s posameznih področij.
Še vedno pride v poštev tudi Zakon o elektronskem poslovanju in elektronskem podpisu, ki vsebuje temeljna določila za pravno veljavnost podatkov v elektronski obliki.

Potrebno je omeniti, da ZVDAGA in uredba ne vsebujeta določil glede rokov hrambe posameznih vrst dokumentarnega gradiva, temveč zgolj določila o načinu in organizaciji hrambe. Roki hrambe in morebitne druga določila, ki so specifična glede na vsebino hranjenega gradiva, so določeni v področnih predpisih.

Ne smemo pozabiti tudi na zakonodajo, ki ureja postopke in poslovanje. Tako npr. Zakon o splošnem upravnem postopku vsebuje mnoga določila, ki se nanašajo na delovanje upravnih organov pri izvajanju njihovih nalog in pooblastil. Poleg tega je zelo pomembna tudi Uredba o upravnem poslovanju, ki vsebuje določila o upravnem poslovanju, ki veljajo za organe državne uprave, uprave samoupravnih lokalnih skupnosti ter druge pravne in fizične osebe, kadar na podlagi javnih pooblastil opravljajo upravne naloge. V sodstvu imajo takšno vlogo drugi predpisi, med njimi najdemo Zakon o kazenskem postopku, Zakon o pravdnem postopku, Zakon o nepravdnem postopku ter Sodni red.

Ob veljavni zakonodaji je potrebno omeniti še standarde, ki urejajo pisarniško poslovanje, organizacijo arhivske službe, varno poslovanje z elektronskimi dokumenti, popisovanje arhivskega gradiva, smernice in tehnične specifikacije, ki so veljavne v okviru EU ter strokovna spoznanja in izkušnje, ki so dostopne v okviru dokumentov, priporočil, dogovorov in standardov Mednarodnega arhivskega sveta, Sveta Evrope in drugih mednarodnih in nacionalnih združenj, katerih delo in aktivnosti se nanašajo na obravnavanje dokumentacije v njenem celotnem življenjskem ciklu. V tem kontekstu naj izpostavimo le Model zahtev za upravljanje elektronskih dokumentov (MoReq), ISO standard 14721 - za izdelavo arhivskih sistemov elektronskih virov, ISO standard 15489 – sistemi upravljanja z dokumenti, ISO standard 23081 – principi metapodatkov za dokumente, ISO standard 17799 in ISO standard 27001– varnost informacijskih sistemov, ameriški standard US DoD 5015.2 – kriteriji za oblikovanje programske opreme namenjene upravljanju elektronskih dokumentov in norveški standard za obravnavanje elektronskih dokumentov NOARK-4. Te pa dopolnjujeta še oba arhivska strokovna standarda Splošni mednarodni standard za arhivsko popisovanje ISAD(g)2 in Mednarodni standard za arhivski normativni opis ustvarjalcev arhivskega gradiva - pravnih in fizičnih oseb ter družin ISAAR(CPF)2.

Enotnim tehnološkim zahtevam je zaradi preglednosti in lažje uporabnosti v prilogi dodan izčrpen informativni seznam različnih standardov, ki so na takšen ali drugačen način pomembni pri elektronski hrambi gradiva.

1.3 POSTOPEK SPREJEMANJA

Za sprejemanje enotnih tehnoloških zahtev je po ZVDAGA pristojen Arhiv Republike Slovenije.

Potrebno je omeniti, da pripravljanje in sprejemanje enotnih tehnoloških zahtev ni mišljeno kot enostransko in enkratno dejanje Arhiva RS, temveč kot stalna dejavnost in prizadevanje, pri katerem se bodo enotne tehnološke zahtev nenehno dopolnjevale in nadgrajevale. Postopek sprejemanja ETZ ne vključuje le strokovnjakov s področja arhivistike in hrambe arhivskega in dokumentarnega gradiva, ki delujejo v okviru državnega arhiva, temveč predvideva tudi sodelovanje drugih zainteresiranih oseb z različnih področij.

Elektronska hramba gradiva je področje, ki je močno odvisno od razvoja informacijske tehnologije. S spreminjanjem tehnoloških možnosti in opreme se spreminjajo tudi postopki in način izpolnjevanja zahtev, ki jih predpisuje ZVDAGA in njemu podrejeni podzakonski predpisi. Ker enotne tehnološke zahteve predstavljajo dokument, ki se problematike elektronske hrambe loteva na praktičen način, je najbrž upravičeno pričakovati, da se bodo hkrati s spreminjajočo se tehnologijo morale spreminjati tudi enotne tehnološke zahteve. Zato je tudi vloga enotnih tehnoloških zahtev predvidena kot vloga povezovalnega elementa med stalnimi zahtevami zakonodaje, katerih izhodišča so temeljna načela ZVDAGA (načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine, načelo trajnosti, načelo celovitosti, načelo dostopnosti in načelo varstva kulturnega spomenika), in spreminjajočimi se potrebami prakse.

Enotne tehnološke zahteve so torej dinamičen dokument, ki se spreminja glede na napredek stroke in tehnologije, pri nastajanju katerega sodelujejo strokovnjaki z relevantnih področij hrambe in drugi zainteresirani deležniki. Pomenijo tudi instrument, s katerim se zagotovi temeljna izhodišča uspešnega zagotavljanja celotne infrastrukture za elektronsko hrambo.

Bistvo enotnih tehnoloških zahtev je predvsem v poenotenju praks in tehnoloških postopkov za upravljanje dokumentarnega gradiva in njegovo hrambo v elektronski obliki, ter za hrambo arhivskega gradiva v elektronski obliki. Za doseganje tega cilja je potrebno sodelovanje tako arhivistične stroke kot tudi drugih oseb iz javnega ter zasebnega sektorja, ki takšno gradivo pri svojem delu ustvarjajo in uporabljajo.

Poleg splošnih ETZ je predviden tudi sprejem posebnih ETZ za posamezne velike zbirke ali registre javnopravnih oseb. Te vrste ETZ bodo vsebovale nekatera splošna določila, posebne določbe pa se bodo navezovale na specifične potrebe velikih registrov ali evidenc.

1.4 UVOD V ELEKTRONSKO HRAMBO

Elektronsko gradivo je izvorno ustvarjeno s pomočjo informacijske tehnologije ali pa z njeno pomočjo ustvarjeno iz drugih oblik dokumentarnega gradiva. Če je elektronsko gradivo sprva vsebovalo predvsem besedilo, so danes vanj lahko vključeni tudi avdio posnetki, mirujoče in gibljive slike, izvedljivi programi, numerični in drugi podatki.

Najpomembnejši lastnosti dobrega sistema hrambe sta njegova dostopnost in varnost. Dostopnost in varnost zagotavljamo na več načinov in na več ravneh. Prvo raven predstavlja že organizacijska postavitev, druga raven je omogočanje dostopa na ravni operacijskega sistema, na katerem arhivski sistem deluje. Tretja raven je omogočanje dostopa v aplikativnem arhivskem sistemu, zadnja raven pa predstavlja zaščito na nivoju posameznih dokumentov.

Katerikoli način hrambi, ki bi se omejil samo na ohranjanje besedila, bo kmalu postal neuporaben. Resnično dolgoročna rešitev mora biti nevtralna, kar se tiče vsebine in oblike elektronskega dokumenta, ki ga želimo shraniti.

Med ključnimi vprašanji je tudi informacijska varnost pri hrambi trajnega ali arhivskega gradiva ter hramba dinamičnega (npr spletne strani) in časovno občutljivega gradiva (npr. elektronski podpis)?

Nekateri vidiki hrambe elektronsko podpisanih podatkov in spletnih strani so določeni v Uredbi. V poglavju o zajemu, pretvorbi in hrambi gradiva v elektronski obliki določa in opisno našteva posamezne elemente zajetih, pretvorjenih ali hranjenih vsebin, ter postopek njihovega zajema. Še posebej določna je Uredba v primeru hrambe elektronskih podpisov – za reševanje te problematike ubira pristop, za katerega je značilna delitev subjektov na bolj ali manj zanesljive, z vidika javnega zaupanja in dejanske stopnje organizacijske urejenosti subjekta.

Ko so dokumenti zbrani, problem dolgoročne hrambe dokumentov v arhivu zahteva skrben premislek. S sedanjimi hitrimi tehnološkimi spremembami nosilci zapisa hrambe podatkov postajajo zastareli vsakih nekaj let, s tem pa tudi tehnologija, ki je potrebna za uporabo elektronskega arhiviranega materiala. To zahteva pripravo ustrezne strategije migracije (prenosa) podatkov iz enega sistema hrambe podatkov v novejši sistem. Podobni koraki se zahtevajo, ko je dosežena doba koristnosti nosilca zapisa skladiščenja, hrambe, neodvisno od dobe koristnosti same tehnologije.

Osnovna načela

Osnovna strokovna načela varovanja in ohranjanja elektronskega gradiva lahko sistemiziramo v dve ravni. Prvo raven tvorijo tista načela, ki se nanašajo na samo obravnavanje dolgoročnega varovanja in ohranjanja dokumentacije v elektronski obliki s poudarkom na njihovi dolgoročni hrambi. Ta načela so pomembna predvsem zaradi zagotavljanja pravnega varstva in v določeni meri tudi za zagotavljanje integritete arhivske vrednosti posameznih dokumentov ali njihovih zaokroženih celot. Druga raven načel, ki morajo biti upoštevana predvsem v pasivnem delu življenjskega cikla, pa sestavljajo obstoječa arhivska strokovna načela, katerih prvenstvena naloga je zagotavljati arhivsko vrednost ovrednotenim vsebinam v elektronski obliki in njihovo integracijo v sistem integralnega arhiviranja ne glede na pojavno obliko, vsebino ali berljivost dokumentov.

ZVDAGA vsebuje sledeča načela:

»Načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine« pomeni, da hramba dokumentarnega gradiva zagotavlja ohranjanje izvirnega dokumentarnega gradiva ali uporabnosti njegove vsebine. Hrambi izvirnega dokumentarnega gradiva je zato enaka hramba zajetega gradiva, če zagotavlja zajetemu gradivu vse učinke izvirnega gradiva (uporabnost vsebine gradiva).

»Načelo trajnosti« pomeni tako hrambo dokumentarnega gradiva, da ta zagotavlja trajnost tega gradiva oziroma trajnost reprodukcije njegove vsebine.

»Načelo celovitosti« pomeni zahtevo po taki hrambi dokumentarnega gradiva, ki zagotavlja njegovo nespremenljivost in integralnost dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenost dokumentarnega gradiva oziroma njegove vsebine ter dokazljivost izvora dokumentarnega gradiva (provenience).

»Načelo dostopnosti« pomeni, da mora biti dokumentarno gradivo oziroma reprodukcija njegove vsebine ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom.

»Načelo varstva kulturnega spomenika« izhaja iz dejstva, da je arhivsko gradivo kulturni spomenik in mora biti varovano kot takšno. Ob navedenih normativno postavljenih načelih se pojavljajo še druga načela, ki so povezana z dolgoročno hrambo dokumentacije v elektronski obliki. Nekatera izmed njih so že uveljavljena, druga pa je potrebno omeniti saj je znano, da bodo postala zaradi svoje narave aktualna v prihodnosti.

Poleg zakonskih načel bi lahko omenili tudi nekaj ostalih, manj pomembnih načel, ki so prav tako pomembna za zagotavljanje varstva arhivskega in dokumentarnega gradiva. Sledeča načela bi lahko izpeljali iz posameznih naštetih zakonskih načel.

- »Načelo proaktivnosti« predstavlja izhodiščno načelo normativne ureditve na področju obravnavanja dokumentacije v elektronski obliki. Tega definiramo kot permanentni strokovni nadzor slovenske javne arhivske službe pri valoriziranih ustvarjalcih nad celotnim življenjskim ciklom arhivskega in dokumentarnega gradiva v elektronski obliki vključno z možnostjo zgodnjega arhivskega strokovnega ukrepanja.

- »Načelo vzpostavljanja in ohranjanja verodostojnih metapodatkovnih struktur« se nanaša na obravnavanje metapodatkov. Za nje je potrebno v procesu pretvorbe v obliko za dolgoročno hrambo gradiva oz. pri migracijah gradiva iz enega sistema za dolgoročno hrambo v drugega, ohranjati potrebne sledi za logično rekonstrukcijo posameznih dogodkov v zvezi obravnavanjem gradiva v elektronski obliki skozi čas in prostor.

- »Načelo celovitega zajemanja stanja podatkov za hrambo« se nanaša na načine in oblike zajemanja elektronskih oblik gradiva. Na podlagi tega načela je potrebno zajemati podatke za potrebe hrambe bodisi kot celote stanj gradiva v elektronski obliki določenega zaključenega obdobja, njihove preseke, celote podatkov sledenja dokumentov v njihovem življenjskem ciklu in podobno.

- »Načelo celovite normalizacije tehničnih in vsebinskih specifikacij« pomeni, da bo za zagotavljanje javne vere elektronskega gradiva potrebno sprotno usklajevanje sprememb različnih specifikacij. S tem bodo skrbniki elektronskega gradiva omejevali možnosti manipulacij, ki bi temeljile na splošnem tehnološkem razvoju ter na spremembah in dopolnitvah specifikacij.

Ob izpostavljenih načelih, ki se nanašajo predvsem na obravnavanje elektronskega gradiva, je potrebno s stališča arhivske teorije in prakse s potrebnimi prilagoditvami upoštevati že obstoječa načela »klasične« arhivske teorije in prakse kot sta načeli provenience in prvotne ureditve.

Dolgoročna hramba

V arhivski stroki je do pred nekaj leti prevladovalo mnenje, da je mogoče uspešno vzpostavljati sisteme za dolgoročno hrambo elektronskega gradiva z različnimi postopki varnostnih in drugih oblik kopiranja na ravni operacijskih sistemov. To mnenje je bilo

regularno, saj je izhajalo iz izkušenj s fizičnim arhivskim gradivom. Vendar je ameriška stroka že pred leti opozarjala, da je potrebno v okviru obdelav in manipulacij z datotekami dosledno razlikovati med kopiranjem in preseljevanjem datotek, oboje skupaj pa razločevati od izvedenih migracij podatkov iz enega v drugi sistem. Danes je v okviru arhivske teorije in prakse popolnoma jasno, da zgolj običajne procedure varnostnega kopiranja s pomočjo ustvarjanja običajnih rezervnih kopij dolgoročno niso primerne.

Na podlagi praktičnih izkušenj so arhivski strokovni delavci kmalu ugotovili, da je na sistem za izvajanje dolgoročne hrambe gradiva potrebno gledati kot na poseben (pod)sistem, ki ga je ni mogoče realizirati samo na tehnično-tehnološki ravni ampak predvsem z ustreznimi programsko–organizacijskimi nadgradnjami, ustrezno izobraženimi zaposlenimi, množico uveljavljenih standardov in priporočil in seveda ustrezno zakonodajo, ki določa potrebne okvire tovrstnih aktivnosti.

Osnovne pravne norme vzpostavitve sistemov za dolgoročno hrambo gradiva v elektronski obliki (ang. recordkeeping systems) najdemo v ZVDAGA, Uredbi o upravnem poslovanju, Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje in v drugih sorodnih predpisih ter v različnih standardih (npr. ISO 15489-2, ISO 17799, ISO 27001, in drugi) Pri vzpostavitvi sistema za dolgoročno hrambo elektronskega gradiva je potrebno upoštevati mnoga določila, ki se nanašajo predvsem na:

- infrastrukturo, njeno varnost in zanesljivost;
- prostore in osebje, predvsem na pristojnosti in naloge posameznih članov osebja;
- morebitne zunanje sodelavce;
- fizično varovanja infrastrukture - predvsem glede dostopa v prostore (vstopne pravice, avtentikacijski sistem,...);
- ravnanja s strojno in programsko opremo;
- elektronsko oziroma programsko varovanje (varnostne nastavitve strežnikov, uporaba telekomunikacijskih sredstev in opreme ter prijave v sistem, varnostne kopije in podobno);
- notranji nadzor (operativna izvedba in spremljanje dogodkov: kontrola fizičnega dostopa, kontrola pooblastil, poročanje o varnostnih problemih itd.);
- ukrepe ob nepredvidenih dogodkih ter vodenje dnevnikov in sestave zapisnikov;
- aktivnosti v zvezi s tehnološkim staranjem strojne in programske opreme, propadanjem za dolgoročno hrambo elektronskega gradiva uporabljenih nosilcev zapisa in zastarevanjem oblik zapisov.

Pogoje sistema za dolgoročno hrambo elektronskega gradiva morajo izpolnjevati naslednja okolja:

- v prvotnem okolju informacijskega sistema za upravljanje z dokumenti,
- v zunanjem okolju za dolgoročno hrambo elektronskega gradiva,
- v arhivskem okolju za arhiviranje elektronskega gradiva.

Pravni učinki

Pri zagotavljanju hrambe dokumentarnega in arhivskega gradiva v elektronski obliki je potrebno nekaj pozornosti nameniti najprej pravni veljavnosti dokumentarnega gradiva, kot jo določa ZVDAGA.

Temeljni problem pri priznanju pravne veljave in dokazne vrednosti kakršnekoli elektronske vsebine leži v problemu, da podatki v elektronski obliki sami po sebi niso odporni na posege kot je spreminjanje ali uničenje. Če se gradivo, ki je hranjeno v elektronski obliki, spremeni, je takšna sprememba neizsledljiva, če ni posebej poskrbljeno za sledljivost. Zato je potrebno pri hrambi in zajemu elektronskih podatkov in delektronskega gradiva za takšno funkcionalnost poskrbeti na drugačne načine, z uporabo ustrezne varnostne tehnologije ter z ustreznimi organizacijskimi ukrepi.

ZVDAGA pravno veljavnost dokumentarnega gradiva pogojuje z načinom njegovega zajema in hrambe, saj ravno v času zajema in hrambe dokumentarnega gradiva namreč obstaja možnost, da je avtentičnost in celovitost vsebine gradiva okrnjena. Zakon zato določa tri različne scenarije, po katerih se pravna veljava takšnega gradiva presoja.

Na podlagi zakona se tistemu dokumentarnemu gradivu, ki je bilo zajeto in varno hranjeno v skladu s strani državnega arhiva potrjenimi notranjimi pravili subjekta, ki je hrambo in zajem gradiva izvajal, prizna enakost izvirnemu gradivu, posledica tega pa je, da je tudi pravna veljavnost takšnega elektronskega gradiva enaka pravni veljavnosti izvirnika. Takšno gradivo torej deli usodo izvirnika že po samem zakonu, kar pomeni, da njegove pravne veljavnosti ni potrebno posebej dokazovati.

Druga možnost je, da je bilo gradivo varno hranjeno in zajeto pri subjektu, ki sicer deluje po nekih zapisanih notranjih pravilih, vendar takšna pravila niso bila potrjena s strani državnega arhiva. V takšnem primeru je dokumentarnemu gradivu lahko priznana enakost z izvirnikom, vendar je potrebno pred tem dokazati, da so notranja pravila subjekta skladna z zakonom, podzakonskimi predpisi ter enotnimi tehnološkimi zahtevami, za katere bo poskrbel državni arhiv.

Tretja možnost pa je, da je bilo določeno gradivo hranjeno ali zajeto pri subjektu, ki tega nima urejenega z notranjimi pravili ali ki pravila sicer ima, vendar se jih v konkretnem primeru ni držala, ali pa gre za primer, ki ga potrjena pravila ne urejajo. V vseh teh primerih se enakost elektronskega gradiva z izvirnim presoja v vsakem posameznem primeru, kar pomeni, da mora izpolnjevati enake pogoje varne hrambe kot izvirno gradivo.

Trg opreme in storitev

Vsaka oseba, ki izvaja hrambo dokumentarnega gradiva, mora najprej sprejeti notranja pravila, ki vsebujejo podrobnosti o njihovem delovanju. Notranja pravila morajo biti v skladu z zakonom, podzakonskimi predpisi, s pričujočimi enotnimi tehnološkimi zahtevami ter drugimi pravili stroke. Oseba se mora priprave na izvajanje te dejavnosti lotiti na vnaprej določen način. Ta je sestavljen iz priprave na zajem in hrambo, priprave in sprejem notranjih pravil, spremljanja njihovega izvajanja in ukrepanja v primerih odstopanja ter dopolnjevanje pravil v primeru sprejema nove zakonodaje ali novih tehnoloških standardov. Sprejem notranjih pravil je pomemben predvsem za zagotavljanje pravne veljavnosti elektronsko hranjenih dokumentov. ZVDAGA namreč pravno veljavnost le-teh veže na obstoj (in izvajanje) potrjenih notranjih pravil. Posamezni subjekti lahko svoja notranja pravila pošljejo tudi v potrditev državnemu arhivu. Državni arhiv preveri skladnost pravil z zakonodajo in enotnimi tehnološkimi zahtevami - če skladnost ugotovi, ta pravila potrdi, s čemer se gradivu, katerega oseba hrani, zagotovi pravna veljavnost že na podlagi zakona.

ZVDAGA za vse osebe, ki bodo svoje dokumentarno gradivo ali dokumentarno gradivo svojih strank hranile v elektronski obliki, predvideva tudi zanimivo alternativo. Če bodo prevzele vnaprej pripravljena vzorčna notranja pravila drugih oseb, ki so taka pravila

pripravila za širšo uporabo, in če bodo ta prevzeta pravila že potrjena s strani državnega arhiva, jim posebej ne bo treba pridobivati dodatne potrditve, seveda pod pogojem, da jih bodo sprejele v celoti in brez sprememb. Takšna rešitev je prikladna predvsem zato, ker se bo na trgu bržkone pojavilo kar nekaj subjektov, ki bodo želeli opravljati različne storitve, zato jim bo na tak način izvajanje hrambe v skladu z zahtevami precej olajšano, poleg tega pa se bo na takšen način dosegla tudi precej bolj enotna praksa pri zagotavljanju hrambe. Ker je pričakovati, da bo hrambo v elektronski obliki uporabljalo več istovrstnih subjektov, bodo vzorčna notranja pravila lahko pripravljala tudi različna branžna združenja ter sorodni subjekti in tako omogočila različnim subjektom s svojega področja relativno enostavno vpeljavo elektronske hrambe.

Za opravljanje storitev zajema in hrambe gradiva v elektronski obliki, opravljanje spremljevalnih storitev ali za ponujanje programske ali strojne opreme, s katero se takšne storitve izvaja, ZVDAGA ne predvideva potrebe po predhodnem dovoljenju s strani državnega organa, temveč vpeljuje zgolj koncept registracije, ki je v enaki obliki že nekaj časa uveljavljen na področju elektronskega podpisovanja, kjer je vpeljan za delovanje overiteljev elektronskih podpisov. Osebe, ki na trgu ponujajo storitve hrambe ali opreme za zajemanje in hrambo gradiva ali opremo za te storitve, se morajo 8 dni pred začetkom izvajanja te dejavnosti prijaviti državnemu arhivu, kjer so na podlagi prijave vpisane v register ponudnikov.

Za zagotovitev še nekoliko višje ravni varnosti in zanesljivosti delovanja uvaja ZVDAGA še en nov institut – akreditacijo strojne in programske opreme ali akreditacijo storitev hrambe oziroma spremljevalnih storitev. Ponudniki, ki želijo pridobiti še nekoliko več zaupanja pri potencialnih odjemalcih, lahko storitve in opremo, katere ponujajo, poleg same registracije tudi dodatno akreditirajo pri državnem arhivu.

Seveda morajo za akreditacijo izpolnjevati dodatne pogoje in zahteve. Državni arhiv sprejme le splošne pogoje za izvajanje akreditacije, katerih se morajo ponudniki, ki bodo svojo opremo ali storitve želeli akreditirati, držati. Z državnim arhivom ti ponudniki sklenejo posebno akreditacijsko pogodbo, v kateri se določijo medsebojna razmerja, prav tako pa morajo slediti posebnim priporočilom državnega arhiva. Državni arhiv pri izvajanju akreditacije deluje tudi kot nadzorni organ, ki nadzoruje izvajanje akreditacije pri akreditiranih ponudnikih, njegova pooblastila pa so enakovredna inšpekcijskim, seveda le glede nadzora izvajanja podzakonskih predpisov, enotnih tehnoloških zahtev in svojih priporočil za akreditirano opremo in storitve.

Akreditacija ima za ponudnike storitev in opreme za hrambo in zajem dokumentarnega in arhivskega gradiva v elektronski obliki poleg višje ravni zaupanja, ki ga z uporabo naziva akreditiranega ponudnika lahko pridobi pri potencialnih odjemalcih, še eno odločilno prednost - storitve hrambe arhivskega gradiva in spremljevalnih storitev v elektronski obliki za javnopravne osebe lahko izvajajo zgolj akreditirani ponudniki. Akreditacija ima torej odločilno vlogo na celotnem področju javnega sektorja.

1.5 DEFINICIJE

Sledeče definicije so povzete predvsem po veljavnih predpisih, specifikaciji Moreq in po mednarodnih standardih.

dokument

je izviren ali reproduciran (pisan, risan, tiskan, fotografiran, fotokopiran, fonografski, v elektronski obliki ali kako drugače zapisan) zapis, ki je bil prejet ali je nastal pri delu organa in je pomemben za njegovo poslovanje.

dokumentarno gradivo

je izvirno in reproducirano (pisano, risano, tiskano, fotografirano, filmano, fonografirano, magnetno, optično ali kako drugače zapisano) gradivo, ki je bilo prejeto ali je nastalo pri delu pravnih oziroma fizičnih oseb;

dokumentarno gradivo v fizični obliki

je dokumentarno gradivo na fizičnem nosilcu zapisa, ki omogoča reprodukcijo vsebine brez uporabe informacijsko komunikacijskih ali sorodnih tehnologij (npr. na papirju, filmu itd.);

dokumentarno gradivo v elektronski obliki

je dokumentarno gradivo v elektronski ali analogni obliki;

dokumentarno gradivo v elektronski obliki

je dokumentarno gradivo v elektronski obliki zapisa in shranjeno na elektronskem nosilcu zapisa;

dokumentarno gradivo v analogni obliki

(npr. analogni avdio/video zapis) je dokumentarno gradivo v analogni obliki zapisa in shranjeno na elektronskem nosilcu zapisa;

dokumentarno gradivo v elektronski obliki za dolgoročno hrambo

pomeni gradivo, katerega vsebina je zapisana v elektronski obliki in shranjena na elektronskem nosilcu zapisa, pri čemer tako elektronska oblika kot tudi nosilec zapisa zagotavljata učinkovito dolgoročno hrambo in upoštevanje tehnološkega napredka v skladu s tem zakonom;

izvirno dokumentarno gradivo

je dokumentarno gradivo, ki je nastalo, bilo prejeto ali bilo poslano osebi, ki hrani to gradivo;

zajeto dokumentarno gradivo

je dokumentarno gradivo, ki je nastalo ob zajemu izvirnega dokumentarnega gradiva v hrambo s pretvorbo izvirnega dokumentarnega gradiva v novo elektronsko obliko zapisa ali na mikrofilm;

arhivsko gradivo

je dokumentarno gradivo, ki ima trajen pomen za znanost in kulturo ali trajen pomen za pravno varnost oseb v skladu s strokovnimi navodili pristojnih arhivov;

javno arhivsko gradivo«

je arhivsko gradivo, ki se odbere iz dokumentarnega gradiva javnopravnih oseb po strokovnih navodilih pristojnega arhiva;

zasebno arhivsko gradivo

je dokumentarno gradivo drugih pravnih in fizičnih oseb, ki ima lastnosti arhivskega gradiva in je kot arhivsko gradivo določeno na podlagi tega zakona ali odločbe državnega arhiva;

trajno gradivo

je lastno gradivo, ki je bilo prejeto ali je nastalo pri delu organa in je določeno z veljavnimi predpisi ali z aktom ministra ali predstojnika organa kot gradivo, ki je trajno pomembno za organ in ga je zato potrebno trajno hraniti pri organu, kadar nima značaja arhivskega gradiva in ga ni potrebno izročiti pristojnemu arhivu;

informacijski sistem za upravljanje

je informacijski sistem za upravljanje dokumentarnega gradiva v elektronski ali fizični obliki;

informacijski sistem za hrambo

je informacijski sistem za skladiščenje in iskanje dokumentarnega gradiva, ki nadzoruje posebne funkcije nastajanja, hrambe in dostopa do gradiva zato, da ohranja njegovo uporabnost, celovitost in dostopnost;

SUVI

je sistem upravljanja varovanja informacij.

hramba gradiva

je tista hramba izvirnega ali zajetega dokumentarnega gradiva, ki izpolnjuje pogoje po tem zakonu in zagotavlja uporabnost vsebine hranjenega gradiva;

dolgoročna hramba gradiva

je hramba gradiva za časovno obdobje, daljše od pet let;

storitve hrambe gradiva v elektronski obliki

so storitve, ki so neločljivo povezane z ohranjanjem vsebine gradiva v elektronski obliki, vendar ne gre za ponudbo opreme za takšno hrambo;

spremljevalne storitve

so storitve, ki so povezane s hrambo gradiva v elektronski obliki, vendar ne gre za storitve hrambe gradiva v elektronski obliki ali ponudbo opreme za tako hrambo (uničenje, poizvedovanje in analiziranje gradiva itd.);

notranja pravila zajema in hrambe gradiva v elektronski obliki

so pravila, ki jih kot svoj interni pravni akt sprejme oseba glede hrambe svojega gradiva;

strojna oziroma programska oprema za zajem oziroma hrambo gradiva v elektronski obliki

je vsaka strojna oziroma programska oprema, katere namen je v celoti ali delno omogočiti zajem ali hrambo gradiva v elektronski obliki ter s tem povezana opravila;

ponudnik strojne in programske opreme za hrambo gradiva v elektronski obliki

je vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči uporabo strojne ali programske opreme za zajem oziroma hrambo gradiva v elektronski obliki;

ponudnik storitve hrambe dokumentarnega gradiva v elektronski obliki

je vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči hrambo dokumentarnega gradiva v elektronski obliki na svoji infrastrukturi;

spremljevalne storitve

so storitve, ki so povezane z zajemom ali hrambo gradiva v elektronski obliki, vendar ne predstavljajo ponudbe opreme za zajem ali hrambo in tudi ne storitev hrambe;

ponudnik spremljevalnih storitev glede zajema ali hrambe gradiva v elektronski obliki

je vsaka oseba, ki za druge osebe odplačno ali neodplačno opravlja takšne storitve.

javni arhivi

so Arhiv Republike Slovenije, regionalni arhivi in arhivi lokalnih samoupravnih skupnosti;

javnopravne osebe

so državni organi, organi samoupravnih lokalnih skupnosti ter nosilci javnih pooblastil in izvajalci javnih služb ter druge osebe, ki izpolnjujejo večino od teh pogojev:

- so osebe javnega prava;
- njihov ustanovitelj je država ali samoupravna lokalna skupnost oziroma ima država ali samoupravna lokalna skupnost v njih odločujoč delež ali vpliv;
- so ustanovljene z javnopravnim aktom;
- so zavezanci po predpisih za dostop do informacij javnega značaja.

javnopravni organi

so državni organi, organi samoupravnih lokalnih skupnosti in nosilci javnih pooblastil;

informacijski varnostni dogodek

je vsak dogodek, ki ima ali bi lahko imel za posledico nerazpoložljivost opreme, razkritje varovanih podatkov ali izgubo oziroma nezaželeno spremembo podatkov, poškodovanje ali izgubo opreme in sredstev;

oblika zapisa

so tiste organizacijske in tehnološke značilnosti zapisa, ki določajo, kako je vsebina zapisana, hranjena in prikazana v procesu hrambe;

nosilec zapisa

je klasičen ali elektronski nosilec zapisa, na katerega se zapiše vsebina v skladu z obliko zapisa;

elektronsko sporočilo

je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto;

elektronski podpis

je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;

varen elektronski podpis

je elektronski podpis, ki izpolnjuje naslednje zahteve:
– da je povezan izključno s podpisnikom;
– da je iz njega mogoče zanesljivo ugotoviti podpisnika;
– da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
– da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi;

časovni žig

je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času; varni časovni žig pa elektronsko podpisano potrdilo overitelja, ki izpolnjuje pogoje iz prejšnje točke;

podatki za elektronsko podpisovanje

so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;

podatki za preverjanje elektronskega podpisa

so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;

sredstvo za preverjanje elektronskega podpisa

je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;

oprema za elektronsko podpisovanje

je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov;

podatki v elektronski obliki

so podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način;

tajni podatek

je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov zavarovati pred nepoklicanimi osebami, in ki je določeno in označeno kot tajno;

uradna evidenca

je evidenca, ki je vzpostavljena na podlagi zakona, podzakonskega predpisa ali splošnega akta, izdanega za izvrševanje javnih pooblastil;

varnostni dogodek

je vsak dogodek, ob katerem bi lahko bilo ogroženo življenje ali osebna varnost ljudi, varnost premoženja ali če gre za prekršek ali kaznivo dejanje ali drugo dejanje, ki krši pravila zagotavljanja varnosti;

skrbnik (angl. administrator)

Vloga, odgovorna za vsakodnevno funkcioniranje politike upravljanja dokumentov znotraj organizacije.
Opomba: To je poenostavljeno. Naloge, v tej specifikaciji, dodeljene skrbnikom, so posebno v velikih organizacijah lahko razdeljene med več vlog; nazivi teh so: vodja glavne pisarne, pisarniški uslužbenec, arhivist itd.

avtentičnost (angl. authenticity)

(samo v kontekstu poslovanja z dokumentarnim gradivom) Lastnost tistega, kar je izvorno.

Opomba: V kontekstu dokumenta ta lastnost pomeni, da je dokument tisto, kar naj bi bil. Ne govori pa o zanesljivosti vsebine dokumenta kot navedbe dejstva.
Opomba: Avtentičnost dajejo zadevi njena oblika, izgled, in/ali stanje prenosa in/ali način zaščite in hrambe. Za nadaljnje podrobnosti glejte pojmovnik UBC-MAS (kot zgoraj).

čas nastavitve (angl. configuration time)

Trenutek v življenjskem ciklu ISUD-a, v katerem se ta namesti in so vzpostavljeni njegovi parametri.

enota dokumentarnega gradiva (angl. record)

Vsebinsko zaokroženi zapis(i), ki so med poslovanjem nastali ali bili prejeti pri osebi ali organizaciji in se pri njej ohranili.

Opomba: Lahko se uporabljajo tudi lokalne nacionalne definicije.

Enota lahko obsega enega ali več zapisov (npr. če ima zapis priloge) in lahko je na kateremkoli nosilcu zapisa ter v katerikoli obliki zapisa. Poleg vsebine zapisa(-ov) bi

moral dokument vključevati še podatke o kontekstu in po potrebi tudi podatke o strukturi (tj. podatke, ki opisujejo komponente dokumenta). Bistvena lastnost dokumenta je, da ga ni mogoče spremeniti.

elektronska zadeva (angl. electronic file)

Celota povezanih elektronskih dokumentov oziroma druge enote dokumentarnega gradiva.

elektronski (angl. electronic)

Opomba: Analogni posnetki, četudi jih lahko razumemo kot elektronske, niso za potrebe te specifikacije upoštevani kot »elektronski«, ker kljub temu, da so lahko hranjeni na elektronskem nosilcu, nimajo lastnosti zapisov v elektronski obliki.

elektronski dokument (angl. electronic record)

Dokument, ki je običajno v elektronski obliki.

Opomba: Lahko je v elektronski obliki, ker je nastal z aplikacijo ali kot rezultat digitalizacije, npr. s skeniranjem papirja ali mikrooblike.

evidentiranje (angl. registration)

Dejanje, s katerim je dokumentu pri njegovem vstopu v sistem dodeljen edinstveni identifikator in zabeleženi drugi pomembni metapodatki.

izvleček (angl. extract) (dokumenta)

Kopija dokumenta, na katerem so bile narejene nekatere spremembe, s katerimi je bila odstranjena ali prekrita obstoječa vsebina, vendar ni nič dodano ali smiselno spremenjeno.

izvoz (angl. export)

Postopek izdelave kopije celovitih elektronskih zadev za drug sistem.
Opomba: Po izvozu ostaja zadeva v ISUD-u; v nasprotju s prenosom.

klasifikacija/razvrščanje (angl. classification)

Sistematična identifikacija in urejanje poslovnih aktivnosti in/ali dokumentov v kategorije v skladu z logično strukturiranimi konvencijami, metodami in proceduralnimi pravili, vdelanimi v klasifikacijski načrt.

klasifikacijski načrt (angl. classification scheme)

Klasifikacijski načrt je osnovni in najpomembnejši šifrant za razporejanje dokumentarnega gradiva. Glej tudi pod »klasifikacija«.

Opomba: Klasifikacijski načrt je pogosto prikazan hierarhično.

kombinirana zadeva (angl. hybrid file)

Celota med seboj povezanih elektronskih dokumentov in/ali fizičnih dokumentov, delno shranjenih v elektronski zadevi znotraj ISUD-a in delno v povezani zadevi na papirju ali v drugi fizični obliki zunaj ISUD-a.

revizijska sled (angl. audit trail)

Podatki o transakcijah ali drugih aktivnostih, ki so vplivale na posamezne enote ali so jih spremenile (npr. elemente metapodatkov), ki zajemajo zadostne podrobnosti, da omogočajo rekonstrukcijo prejšnje aktivnosti.
Opomba: Revizijska sled je po navadi sestavljena iz enega ali več seznamov ali baze podatkov; pregledovati jo je mogoče v tej obliki. Seznami so lahko kreirani z računalniškim sistemom (za transakcije znotraj računalniškega sistema) ali ročno (po navadi za ročne aktivnosti)**.**

metapodatki (angl. metadata)

so podatki o podatkih, ki opisujejo kontekst, vsebino in strukturo dokumentarnega gradiva, njegovo upravljane tekom časa in drugo;

Opomba: Razlika med podatki in metapodatki je lahko nejasna. Na primer, po navadi je jasno, da so nujni indeksni podatki za dokument (naziv, datum itd.) del njegovih metapodatkov. Vendar revizijsko sled za dokument ali podatek o njegovem roku hrambe lahko utemeljeno razumemo tako kot podatek kot tudi metapodatek, odvisno od konteksta. Različne vrste metapodatkov lahko definiramo, na primer za indeksiranje, zaščito, prikazovanje itd. Take podrobnosti uporabe metapodatkov presegajo okvir enotnih tehnoloških zahtev.

prenos (angl. transfer)

Postopek prenašanja celovitih elektronskih zadev v drug sistem.

Opomba: Zadeve pogosto prenašamo skupaj z vsemi drugimi zadevami v razredu klasifikacijskega načrta, če je namen prenosa zadev v arhiv zaradi trajne hrambe.
Glejte tudi izvoz, ki se od prenosa nekoliko razlikuje, saj pri izvozu zadeve še naprej ostanejo v ISUD.

razred (angl. class)

(samo v tej specifikaciji) Del hierarhije, predstavljen s črto, ki spaja katerokoli točko klasifikacijskega načrta z vsemi zadevami na nižjih ravneh.
Opomba: V klasični terminologiji lahko to ustreza »glavnemu razredu«, »skupini« ali »seriji« (ali podrazredu, podskupini, podseriji, itd.), na kateremkoli ravni kasifikacijskega načrta.

roki hrambe (angl. retention schedule)
Niz navodil, ki se nanašajo na razred ali zadevo za določanje časovne dobe, v kateri naj bi organizacije hranile dokumente za poslovne namene, ter končna usoda dokumentov ob izteku te časovne dobe.

seznam zadev (angl. repertory)

Seznam obstoječih nazivov zadev znotraj vsake od najnižjih ravni v klasifikacijskem načrtu.

vrsta in stopnja tajnosti (angl. security category).

Eden ali več pojmov, povezanih z dokumentom, ki določajo pravila za urejanje dostopa do dokumenta.
Opomba: Stopnje in vrste tajnosti so navadno določene na organizacijski ali državni ravni. Primeri stopenj in vrst tajnosti, ki se uporabljajo v Republiki Sloveniji so: strogo tajno, tajno, zaupno, interno.

uničenje (angl. destruction/disposal)
Postopek odstranitve ali brisanja dokumentov, tako da rekonstrukcija potem ni več mogoča.

uporabnik (angl. user)
Katerakoli oseba, ki uporablja ISUD.

Opomba: To lahko vključuje (med drugim) skrbnike, zaposlene, člane splošne javnosti in osebje drugih ustanov, kot so revizorji.

varnostno dovoljenje (angl. security clearance)

Eden ali več pojmov, povezanih z uporabnikom, ki določajo stopnje in vrste tajnosti, s katerimi je uporabniku omogočen dostop.

različica (angl. version) (zapisa)

Stanje zapisa na določeni točki njegovega razvoja.

Opomba: Različica je po navadi eden od osnutkov zapisa ali končni zapis. Vendar pa v nekaterih primerih obstajajo končni zapisi v več različicah, npr. tehnični priročniki. Opozarjamo tudi, da dokumenti ne morejo obstajati v več kot eni različici; glejte tudi izvleček.

vloga (angl. role)

Skupina funkcionalnih dovoljenj, dodeljenih vnaprej določeni podskupini uporabnikov.

zadeva (angl. file)

Zadeva je celota vseh dokumentov in prilog, ki se nanašajo na isto vsebinsko vprašanje ali nalogo,

(1) Če se ta pojem uporablja samostojno, se nanaša na oboje, tako na elektronske zadeve kot na zadeve v papirni obliki.
(2) Če se pojem uporabi s prilastkom, tj. elektronska zadeva ali zadeva na papirju, se uporablja ustrezna definicija.

zajem (angl. capture)

Evidentiranje, klasifikacija, dodajanje metapodatkov in shranjevanje dokumenta v sistem, ki upravlja dokumente.

zaključek (angl. close)

Postopek spremembe atributov elektronske zadeve, tako da ne more več sprejemati dodajanja dokumentov.

zaključena zadeva (angl. closed)

Opisuje elektronsko zadevo, ki je bila zaključena in zato ne more sprejeti dodajanja dokumentov.

zapis (angl. document)

Zapisana informacija ali predmet, ki se lahko obravnava kot enota.

Opomba: Zapis je lahko na papirju, v mikroobliki obliki, na magnetnem ali drugem elektronskem nosilcu. Lahko vsebuje vse kombinacije besedila, podatkov, grafik, zvoka, filma ali druge oblike informacij. Posamezen zapis je lahko sestavljen iz enega ali več podatkovnih objektov.

Opomba: Zapisi se razlikujejo od dokumentarnega gradiva v več pomembnih elementih.

2 ORGANIZACIJA IN NOTRANJA PRAVILA

Zajem in hramba gradiv v elektronski obliki se prične z ustrezno organizacijo dela, podprto z notranjimi pravili. Elektronska oblika ima drugačne značilnosti od fizične, drugačne ranljivosti in zahteva bolj sistematičen pristop k organizaciji dela.

Ustrezna organizacija na podlagi notranjih pravil mora zagotoviti:

- visoko stopnjo urejenosti v organizaciji (postavljene usmeritve, pravila, postopki),
- kompetentnost in dodatno usposobljenost zaposlenih za delo z informacijsko opremo,
- splošno zavedanje vseh zaposlenih o pomenu varovanja informacij in dosledno izvajanje varnostnih pravil,
- kakovostno IT podporo (skrben in strokoven izbor programske in strojne opreme, implementacija in vzdrževanje v skladu z dobrimi navadami in pravili stroke),,
- redni nadzor nad izvajanjem, ki ga dnevno opravljajo operativni vodje, periodično in po potrebi pa za to vzpostavljene kontrolne službe (notranja revizija) ali zunanji revizorji.

Predpisana vsebina notranjih pravil, ki opredeljujejo organizacijo in postopke je v nadaljevanju dodatno pojasnjena in dopolnjena z zahtevami.

2.1 NOTRANJA ORGANIZACIJA

Notranja pravila povzemajo ali določajo splošno organizacijsko oz. procesno strukturo osebe, ki izvaja zajem ali hrambo, s poudarkom na organizacijskih delih, procesih in vlogah zaposlenih, ki so vključeni v zajem in hrambo gradiv.

ETZ 2.1.1

Notranja organizacija osebe, ki izvaja zajem ali hrambo gradiv, mora biti v skladu s splošnim poslanstvom osebe (izvaja storitve le zase, ali je ponudnik storitev in katerih) in upoštevati obseg in vrednost gradiva v hrambi. Podlaga za to so ugotovitve iz postopka priprave na zajem in hrambo.

ETZ 2.1.2

Notranja pravila morajo celovito pokrivati hrambo gradiva v vseh oblikah (fizični in elektronski).

ETZ 2.1.3

Notranja pravila morajo opredeliti vse pomembne vloge v procesu zajema, hrambe, uporabe in uničenja dokumentarnega gradiva, njihove odgovornosti, število in potrebno strokovno usposobljenost.

ETZ 2.1.4

Dokumenti, ki sestavljajo notranja pravila (politike, pravilniki, postopki za delo,…) morajo biti obvladovani in vsem uporabnikom na voljo vedno, kadar jih ti potrebujejo. Vzpostavljen mora biti postopek, ki zagotavlja:

- da so dokumenti, ki so del notranjih pravil odobreni pred izdajo,

- da so preprečene nepooblaščene spremembe v dokumentih,
- da so dokumenti na mestu uporabe in na voljo vsem, ki so jim namenjeni (dostopni),
- da so dokumenti berljivi (uporabni),
- da je preprečena uporaba zastarelih dokumentov,
- da so zastareli dokumenti arhivirani,
- da so notranja pravila oz. dokumenti, ki jih sestavljajo, vzdrževana, da se redno pregledujejo in posodabljajo (najmanj enkrat letno in ob spremembah, ki vplivajo na njihovo vsebino).

ETZ 2.1.5

Oseba, ki izvaja zajem ali hrambo mora določiti odgovorno osebo za upravljanje notranjih pravil, v skladu z ETZ 2.1.4.

2.2 INFORMACIJSKA INFRASTRUKTURA

Ključni elementi pri zajemu ali hrambi gradiv v elektronski obliki so uporaba ustrezne informacijske infrastrukture, njeno strokovno upravljanje in dosledno upoštevanje uveljavljenih pravil s področja varovanje informacij (zagotavljanje zaupnosti, integritete in dosegljivosti).

Za zagotovitev ustrezne stopnje informacijske varnosti in tudi upravljanja z informacijsko tehnologijo se je priporočljivo nasloniti na mednarodni standard ISO/IEC 27001 »Information technology -- Security techniques -- Information security management systems – Requirements« in povezane standarde - ISO/IEC 17799 »Information technology -- Security techniques -- Code of practice for information security management« in BS 7799-3 »Information security management systems. Guidelines for information security risk management«. Ta par standardov celovito pokriva zahteve iz 5. točke zakona, zato bodo v nadaljevanju poglavje 2.2 in njegove zahteve obravnavane v skladu s tem standardom. Za dosego ustrezne informacijske varnosti in upravljanja informacijske tehnologije se lahko oseba drži tudi drugih standardov ali priporočil (npr.: ITIL, COBIT), ki pokrivajo postavljene zahteve.

ETZ 2.2.1

Ponudnik storitev mora vzpostaviti in voditi sistem upravljanja varovanja informacij (SUVI).

ETZ 2.2.2

Delovanje SUVI mora temeljiti na izvedeni oceni tveganj, ki je podlaga za izbor ustreznih nadzorstev oz. kontrol (organizacijske strukture, postopkov, ukrepov, razdelitve nalog,…) za zagotavljanje nemotenega delovanja osebe, ki izvaja zajem ali hrambo in varnosti gradiv.

ETZ 2.2.3

Ocena tveganj mora biti redno (najmanj enkrat letno in ob spremembah, ki vplivajo na tveganja) revidirana in usklajena z novimi zahtevami in pogoji delovanja. Enako velja za izbrana nadzorstva (kontrole), ki izhajajo iz ocene tveganj.

ETZ 2.2.4

SUVI mora imeti zagotovljeno ustrezno dokumentacijsko podporo sistemu upravljanja varovanja informacij, ki je lahko del splošnih pravil organizacije ali notranjih pravil v zvezi z izvajanjem zajema in hrambe. Za upravljanje teh pravil veljajo enake zahteve kot splošno za notranja pravila (glej ETZ 2.1.4, ETZ 2.1.5).

2.2.1 Politika varovanja informacij

ETZ 2.2.1.1

Najvišje vodstvo osebe, ki izvaja zajem ali hrambo dokumentarnega gradiva, mora zagotoviti vidno podporo varovanju informacij in se zavezati, da bo zagotavljalo potrebne vire (tehnologijo, ljudi in njihov čas) za zagotavljanje varnosti (zaupnost, celovitost in dostopnost informacij (dokumentarnega gradiva) in podporne tehnologije.

ETZ 2.2.1.2

Oseba, ki izvaja zajem ali hrambo oz. njeno najvišje vodstvo mora sprejeti in objaviti politiko varovanja informacij.

ETZ 2.2.1.3

Politika varovanja informacij mora najmanj:

- opredeliti cilje varovanja informacij,
- vsebovati izjavo vodstva o zavezanosti, da bo zagotavljalo potrebne vire za dosego ciljev in
- opredeliti obseg delovanja SUVI tako, da pokriva najmanj vse subjekte in dejavnosti v zvezi s hrambo dokumentarnega gradiva (lastnega in tujega)
- opredeliti (dokumentirati in implementirati) ukrepe in postopke varovanja informacij.

ETZ 2.1.1.4

Politika varovanja informacij je del dokumentacijske podpore SUVI in za upravljanje s tem dokumentom veljajo pravila opredeljena z ETZ 2.1.4 in ETZ 2.1.5.

2.2.2 Organiziranost varovanja informacij

Organizacija varovanja informacij mora biti integralni del notranje organizacije osebe, ki izvaja zajem ali hrambo gradiv. Varovanje informacij obsega splošna pravila, postopke, naloge in odgovornosti, ki so pomembne za zagotavljanje zaupnosti, celovitost in dostopnost informacij (dokumentarnega gradiva).

ETZ 2.2.2.1

Oseba, ki izvaja zajem ali hrambo dokumentarnega gradiva v elektronski obliki mora imeti odgovorno osebo za varovanje informacij, ki je neposredno odgovorna najvišjemu vodstvu.

ETZ 2.2.2.2

V opisu del in nalog ter opredelitvi odgovornosti zaposlenih, morajo biti določene tudi naloge s področja varovanja informacij. Varnostne vloge in naloge, od katerih je odvisna varnost delovanja ponudnika storitev hrambe, morajo biti natančno opredeljene.

ETZ 2.2.2.3

Delovna mesta in naloge zaposlenih morajo biti določeni na tak način, da se zagotavlja ustrezna ločenost nalog, ki bi v povezavi omogočale zlorabo ali kompromitacijo informacij. Z nalogami mora biti zaposlenim dodeljeno le toliko pravic, kolikor jih potrebujejo za opravljanje svojih nalog.

ETZ 2.2.2.4

Če oseba pri zajemu ali hrambi gradiv najame zunanje izvajalce ali storitve, mora pred tem pripraviti ustrezno oceno varnostnih tveganj.

ETZ 2.2.2.5

Vse fizične osebe, ki so vključene v procese zajema in hrambe gradiv, morajo imeti podpisano ustrezno izjavo o varovanju informacij. To velja za vse osebje, ki lahko pride v stik z gradivom v hrambi (redno in začasno zaposleni, zunanji sodelavci in tretje osebe).

ETZ 2.2.2.6

Pogodbe, ki jih oseba, ki izvaja zajem ali hrambo, sklene z zunanjimi izvajalci, morajo opredeliti najmanj naslednje:

- natančen obseg storitve,
- raven storitev – kakovostna in časovna opredelitev storitev (spremljajoča dokumentacija, odzivni časi, dostopnost…),
- opredelitev in razdelitev odgovornosti za izvajanje posameznih postopkov v skladu z obsegom storitve (npr.: zajem, kontrola kakovosti, administracija sistema, izvajanje sprememb, spremljanje zakonodaje, izvajanje varnostne hrambe, spremljanje sistema, prenosi med sistemi…),
- varovanje podatkov (opredelitev pravil in odgovornosti izvajalca v zvezi z ravnanjem z gradivi in povezanimi informacijami glede zagotavljanja zaupnosti celovitosti in dostopnosti,
- določila glede zagotovitve neprekinjenega delovanja,
- izrecno opredeljena pravica do redne revizije. Področja pregleda so lahko naslednja: splošna organizacija in notranja pravila, pregled upravljanja informacijskega sistema, varnostni pregled).

ETZ 2.2.2.7

Oseba, ki izvaja zajem ali hrambo mora imeti opredeljen postopek nabave informacijske tehnologije za podporo hrambi dokumentarnega gradiva, ki zagotavlja izbor ustrezne opreme v skladu z zakonom, uredbo in ETZ.

2.2.3 Upravljanje informacijskih sredstev

Organizacija in postopki hrambe in varovanje gradiv temeljijo na značilnosti samih gradiv (občutljivost, kritičnost, zaupnost, zahtevan rok hrambe). Temeljni mehanizem za ustrezno upravljanje in varovanje so jasno opredeljene odgovornosti za varovanje

posameznih informacijskih virov in njihova varnostna klasifikacija (opredelitev občutljivosti in zaupnosti).

V ta namen je potrebno popisati in vzdrževati seznam vseh pomembnih informacijskih virov. Vrste informacijskih virov so naslednje:

- informacije: dokumentarno gradivo, baze podatkov, datoteke, pogodbe, opisi postopkov, sistemska dokumentacija, uporabniška dokumentacija, zapisi o izvajanju;
- programska oprema: aplikacijska, sistemska, razvojna orodja in pripomočki;
- fizična sredstva: računalniška oprema, komunikacijska oprema, nosilci zapisa za hrambo;
- storitve: v zvezi z računalniško in telekomunikacijsko infrastrukturo in splošne storitve - elektrika, gretje, hlajenje, fizično varovanje;
- osebje in energija;
- ne-opredmetena sredstva kot so ugled organizacije, blagovne znamke ipd.

ETZ 2.2.3.1

Oseba, ki zajema ali hrani dokumentarno gradivo, mora opraviti inventurni popis vseh pomembnih informacijskih virov, ki so vključeni v izvajanje storitev in popis tekoče vzdrževati.

ETZ 2.2.3.2

Oseba, ki zajema in hrani dokumentarno gradivo, mora opredeliti odgovorne osebe za upravljanje in varovanje posameznih informacijskih virov (oz. skupin virov) na podlagi popisa.

ETZ 2.2.3.3

Oseba, ki zajema in hrani dokumentarno gradivo, mora vzpostaviti varnostno klasifikacijo informacijskih virov v skladu z analizo tveganj in kritičnostjo oz. občutljivostjo gradiv, za katere izvaja zajem in hrambo.

ETZ 2.2.3.4

Oseba, ki izvaja zajem ali hrambo, mora imeti postavljena pravila za ravnanje (hrambo, prenos, uporabo, uničenje) s posameznimi informacijskimi viri glede na varnostno klasifikacijo.

2.2.4 Varnost in človeški viri

Ustrezno ravnanje z informacijami v elektronski obliki temelji na odgovornih, zavednih in kompetentnih zaposlenih. Osebje, ki ravna z dokumentarnim gradivom in upravlja s podporno tehnologijo, ima bistven vpliv na varnost gradiv in ga je najtežje nadzorovati. Zato je potrebna velika skrbnost pri izboru in upravljanju lastnega in pogodbenega osebja.

ETZ 2.2.4.1

Oseba, ki izvaja zajem ali hrambo, mora imeti jasno opredeljene naslednje postopke:

- postopek izbora kadrov, ki mora temeljiti na preverjanju ustreznosti kadrov in njihovih dokazil v skladu z bodočimi nalogami;
- postopek zaposlovanja, ki mora vključevati ustrezno izobraževanje in dodelitev pooblastil in uporabniških pravic za delo v skladu z delovnimi nalogami;
- redno usposabljanje za delo in varovanje informacij;
- opredelitev disciplinskega postopka v primeru kršitev varnostnih pravil;
- postopek ob zamenjavi dela v okviru organizacije, ki mora pokrivati ustrezno spremembo pooblastil za delo in uporabniških pravic ter
- postopek ob prekinitvi delovnega razmerja (rednega ali pogodbenega), ki mora zagotoviti preklic uporabniških pravic v informacijskih sistemih in vračilo delovnih sredstev.

2.2.5 Fizično in tehnično varovanje opreme in prostorov

Fizično varovanje prostorov in opreme je eden od osnovnih kontrolnih mehanizmov pri zagotavljanju varnosti gradiv v hrambi.

ETZ 2.2.5.1

Oseba, ki izvaja hrambo, mora za ustrezno fizično varovanje opredeliti varovana območja v skladu s pomembnostjo in ranljivostjo informacijskih virov, ki se v teh območjih nahajajo. Fizični dostop v posamezna varovana območja mora biti omejen v skladu z nalogami zaposlenih in nadzorovan. Uporabljena tehnologija mora biti nameščena v skladu z navodili za namestitev ter redno pregledovana in vzdrževana.

ETZ 2.2.5.2

Oseba, ki izvaja zajem ali hrambo, mora opredeliti varovana območja v skladu s pomembnostjo informacijskih sredstev, ki se v območju nahajajo.

ETZ 2.2.5.3

Oseba, ki izvaja zajem ali hrambo, mora postaviti pravila za dostop do posameznih varovanih področij in implementirati ustrezne varovalne postopke (od enostavnih identifikacijskih priponk do zapletenih tehnologij za identifikacijo, dovoljevanje dostopa in nadzor nad vsemi poskusi dostopa, protivlomne zaščite…).

ETZ 2.2.5.4

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti zapise o vstopih v varovana območja in njihov reden pregled. Pogostost in podrobnost kontrol mora biti določena v skladu z oceno tveganj za posamezno varovano območje.

ETZ 2.2.5.5

Električna in telekomunikacijska napeljava mora biti izvedena tako, da je ni možno nenamerno prekiniti ali brez večjih težav uničiti ali zlorabiti.

ETZ 2.2.5.6

Oseba, ki izvaja zajem ali hrambo mora, imeti podporno komunikacijsko in računalniško opremo nameščeno v pogojih, ki so predpisani v specifikacijah uporabljene opreme.

ETZ 2.2.5.7

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti reden pregled in vzdrževanje podporne opreme ter voditi o tem ustrezne zapise. Pogostost pregledov mora biti v skladu z naravo opreme oz. z oceno tveganj.

ETZ 2.2.5.8

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti postopke za varno odstranitev ali uničenje nosilcev informacij, ki niso več v uporabi. Po odstranitvi mora biti onemogočen dostop do informacij, ki so se na nosilcih nahajale, ko so bili ti še v uporabi.

ETZ 2.2.5.9

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti ustrezne varnostne ukrepe in postopke zaradi zaščite pred okoljskimi nevarnostmi (požar, izlitje ali vdor vode, nenadne spremembe temperature ali vlage, itd.) kot npr.:

- namestitev protipožarnih vrat,
- samodejni izklop elektrike,
- namestitev javljalnikov požara in vzpostavitev postopkov rednega preverjanja njihovega delovanja ter vodenje dnevnikov preizkusov,
- na najbolj občutljivih varnih območjih je smiselna namestitev samodejnega protipožarnega sistema.
- namestitev javljalnikov vode in samodejnih črpalk,

Vsi varnostni postopki morajo delovati v vsakem trenutku (tudi izven delovnega časa).

2.2.6 Upravljanje komunikacijske infrastrukture in operativno delovanje

Področje upravljanja z informacijsko tehnologijo obsega redne in izredne postopke v zvezi z operativnim delovanjem informacijskega sistema za hrambo dokumentarnega in arhivskega gradiva.

ETZ 2.2.6.1

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti in vzdrževati opise postopkov za izvajanje vseh pomembnih operacij v skladu z oceno tveganj.

ETZ 2.2.6.2

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti takšno razdelitev nalog, ki zagotavlja, da posameznik nima takšnih pooblastil, da bi lahko neopaženo kompromitiral ali zlorabil informacije oz. gradiva, do katerih ima dostop.

ETZ 2.2.6.3

Ponudnik storitev mora zagotoviti ustrezne kontrolne mehanizme za ločevanje gradiv posameznih oseb, za katere izvaja hrambo.

ETZ 2.2.6.4

Oseba, ki izvaja zajem ali hrambo, mora imeti formalno opredeljen postopek za varnostno hrambo podatkov (dokumentarnega gradiva), sistemskih podatkov in uporabljene programske opreme. Pogostost izdelave kopij, število kopij in število ter oddaljenost lokacij za hrambo varnostnih kopij mora biti postavljena na podlagi ocene tveganj. Ocena tveganj mora upoštevati obseg, občutljivost in kritičnost gradiv v hrambi in značilnosti uporabljene tehnologije.

ETZ 2.2.6.5

Celoten postopek za varnostno kopiranje mora biti ustrezno preverjen (testiran) pred začetkom uporabe in ob morebitnih spremembah.

ETZ 2.2.6.6

Nosilci zapisa, ki se uporabljajo za hrambo varnostnih kopij, morajo biti ustrezno preverjeni pred prvo uporabo. Periodično, v skladu z zanesljivostjo uporabljenih nosilcev zapisa, najmanj pa enkrat letno, je potrebno izvesti preverjanje uporabnosti obstoječih varnostnih kopij.

ETZ 2.2.6.7

Vsi nosilci zapisa, na katerih se nahaja gradivo ali drugi pomembni podatki v zvezi z zajemom in hrambo, morajo biti hranjeni tako, da so zavarovani pred škodljivimi vplivi okolja, krajo ali nepooblaščenim dostopom.

ETZ 2.2.6.8

Oseba, ki izvaja zajem ali hrambo, mora imeti formalno opredeljen postopek za upravljanje sprememb. Potrebne spremembe v postopkih in podporni tehnologiji (strojna in programska oprema) morajo biti uvedene kontrolirano, po vnaprej opredeljenem postopku, ki vključuje zahtevek za spremembo, analizo vplivov, odobritev, testiranje in implementacijo.

ETZ 2.2.6.9

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti strogo ločitev operativnega okolja od okolja namenjenega za razvoj ali testiranje.

ETZ 2.2.6.10

Informacijski sistemi za hrambo gradiv morajo biti ustrezno zaščiteni proti virusom ter drugo škodljivo, nezaželeno in tudi nepotrebno programsko opremo, v skladu z oceno tveganj. Zaščita pred virusi in podobno zlonamerno programsko opremo se doseže z namestitvijo in uporabo ustreznega, certificiranega in registriranega protivirusnega programa, ki mora biti redno dopolnjen z zbirko virusov oziroma protivurusnimi dejavnostmi. Pred načrtovanimi napadi in vdori (DoS- Denial of Service) ni splošne zaščite, potrebno je odpraviti varnostne luknje, preko katerih so napadalci prišli v sistem. Popolna onemogočitev tovrstnih napadov je možna z zmanjšanjem števila »ranljivih« sistemov, ki omogočajo napadalcem namestitev in izvajanje tovrstnih procesov.

ETZ 2.2.6.11

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti postopke in zapise o rednem spremljanju in nadzoru delovanja računalniškega sistema.

ETZ 2.2.6.12

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti, da uporabljeni računalniški sistem samodejno izdeluje revizijske sledi oz. beleži vse pomembne dogodke na sistemu (kdaj in kdo je vstopil v posamezni informacijski podsistem in kakšne postopke je izvajal). Hkrati mora oseba, ki izvaja zajem ali hrambo, zagotoviti tudi redno pregledovanje izdelanih revizijskih sledi.

ETZ 2.2.6.13

Na ravni celotnega podpornega sistema mora biti ves čas delovanja zagotovljena uskladitev sistemskih ur oz. merjenja časa.

2.2.7 Obvladovanje dostopa do sistemov

ETZ 2.2.7.1

Dostop do podatkov mora biti urejen tako, da izpolnjuje vse zahteve veljavnih predpisov (npr. Zakona o varstvu osebnih podatkov, Zakona o tajnih podatkih, in drugih predpisov).

ETZ 2.2.7.2

Dostop do sistemov za hrambo dokumentarnega in arhivskega gradiva in povezanih sistemov smejo imeti samo kompetentni posamezniki z ustreznimi pooblastili za dostop in uporabo.

ETZ 2.2.7.3

Računalniški sistemi so večnivojski in tudi dostop do gradiv v sistemu poteka preko več ravni: dostop v računalniške mreže, dostop v operacijski sistem in dostop v aplikacijski sistem. Kontrole dostopa do posameznih ravni morajo biti med seboj ustrezno usklajene, da zagotavljajo zanesljivo kontrolo.

ETZ 2.2.7.4

Oseba, ki izvaja zajem ali hrambo, mora imeti opredeljen postopek in odgovornosti za dodeljevanje in odvzem uporabniških pravic v skladu z nalogami uporabnikov.

ETZ 2.2.7.5

Oseba, ki izvaja zajem ali hrambo, mora imeti postavljena pravila za dodeljevanje uporabniških imen in upravljanje identitet uporabnikov tako, da je zagotovljena enotna identifikacija vseh uporabnikov.

ETZ 2.2.7.6

Oseba, ki izvaja zajem ali hrambo, mora imeti postavljena pravila za upravljanje z gesli, ki minimalno obsegajo obvezno sestavo gesel, časovno opredelitev in postopek za redno spreminjanje gesel in postopek za prvo in po potrebi nadaljnjo dostavo gesel uporabnikom.

ETZ 2.2.7.7

Implementirani postopki za dostop do sistemov in identifikacijo uporabnikov morajo biti v skladu z oceno tveganj glede na kritičnost in pomembnost posameznih sistemov oz. gradiv v hrambi, ki jih ti sistemi podpirajo.

2.2.8 Razvoj in vzdrževanje (aplikacijskih) informacijskih sistemov

Razvoj in vzdrževanje informacijskih sistemov za podporo hrambi dokumentarnega in arhivskega gradiva mora temeljiti na formalnih postopkih za razvoj in vzdrževanje računalniških sistemov v skladu z uveljavljenimi pravili in dobrimi navadami stroke.

ETZ 2.2.8.1

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti, da je osebje, ki sodeluje pri razvoju novih sistemov, ustrezno strokovno usposobljeno.

ETZ 2.2.8.2

Oseba, ki izvaja zajem ali hrambo, mora pri razvoju zagotoviti posebno razvojno in testno okolje, ločeno od operativnega okolja na način, da operativno okolje ni ogroženo.

ETZ 2.2.8.3

Oseba, ki izvaja zajem ali hrambo, mora imeti sprejeto formalno metodologija oz. postopek razvoja informacijskih sistemov.

ETZ 2.2.8.4

Postopek razvoja mora zagotoviti, da so pri razvoju poleg funkcionalnih zahtev upoštevane tudi zahteve glede varovanja podatkov in usklajenostjo z zakonodajo in zahteve glede zanesljivosti ter ustrezne kakovosti sistemov.

ETZ 2.2.8.5

Postopek razvoja mora zagotavljati, da so vsi informacijski sistemi, ki se uporabljajo pri hrambi dokumentarnega in arhivskega gradiva pred uporabo overjeni oz. stestirani na podlagi dokumentiranega postopka. Testiranje mora poleg funkcionalnih testov obsegati tudi testiranje varnostnih elementov in obremenitev.

ETZ 2.2.8.6

Oseba, ki izvaja zajem ali hrambo, mora imeti v okviru razvoja opredeljen postopek za upravljanje sprememb, ki zagotavlja da so vse spremembe (dograditve, vzdrževanja) na obstoječi programski opremi nadzorovano izvedene in overjene pred uporabo.

ETZ 2.2.8.7

V kolikor oseba pri razvoju in testiranju uporablja podatke iz operativnega okolja, mora glede zaupnosti z njimi ravnati enako skrbno kot v operativnem okolju. Po uporabi je potrebno podatke ustrezno uničiti.

ETZ 2.2.8.8

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti tehnično in uporabniško dokumentacijo za vse sisteme v uporabi.

ETZ 2.2.8.9

Oseba, ki izvaja zajem ali hrambo, mora pred redno uporabo zagotoviti ustrezno izobraževanje uporabnikov in skrbnikov novih sistemov.

2.2.9 Upravljanje varnostnih dogodkov

Za zagotovitev varnosti in verodostojnosti hranjenih gradiv je pomembno, da je vzpostavljen sistem, ki zagotavlja redno beleženje in obravnavo vseh dogodkov v informacijskem sistemu, ki vplivajo ali bi lahko vplivali na varnost (zaupnost, celovitost, dostopnost) gradiv v hrambi.

ETZ 2.2.9.1

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti postopek upravljanja varnostnih dogodkov, ki obsega:

- obveznost poročanja o zaznanih varnostnih dogodkih s strani zaposlenih,
- obveznost avtomatskega spremljanja dogodkov v okviru računalniških sistemov,
- opredelitev načina poročanja o varnostnih dogodkih,
- zagotovitev postopkov za zavarovanje in hrambo dokazov,
- evidentiranje varnostnih dogodkov (sporočenih in avtomatsko zaznanih),
- ukrepanje ob dogodkih v skladu z naravo dogodka in možnimi vplivi na varnost sistemov in gradiv v hrambi,
- postopek beleženja izvedenih ukrepov in
- reden pregled in analizo evidentiranih varnostnih dogodkov.

ETZ 2.2.9.2

Evidence morajo biti vzpostavljene na takšen način, da služijo kot baza znanja za hitro ukrepanje ob že zabeleženih varnostnih dogodkih.

2.2.10 Zagotavljanje neprekinjenega delovanja

Pri hrambi dokumentarnega in arhivskega gradiva je bistven poudarek na ohranjanju gradiv, njihove celovitosti in dostopnosti in praviloma manj na potrebnem časovnem okviru za restavracijo gradiv. Postopek za restavracijo gradiv in vzpostavitev stanja mora biti postavljen tako, da zagotavlja celovitost in potrebno zaupnost gradiv tudi v posebnih razmerah. Skladno s temi zahtevami in oceno poslovnih vplivov mora biti pripravljen celovit načrt za zagotavljanje neprekinjenega delovanja (načrt).

Postopki za ponovno vzpostavitev stanja, ki so del načrta temeljijo na pripravi ustreznih varnostnih kopijah zato glej tudi ETZ 2.2.6.4, ETZ 2.2.6.5, ETZ 2.2.6.6. in ETZ 2.2.6.7.

ETZ 2.2.10.1

Oseba, ki zajema ali hrani gradivo, mora imeti pripravljen načrt v skladu s poslanstvom organizacije (izvaja hrambo le zase ali tudi za druge) ter obsegom in kritičnostjo gradiv v hrambi.

ETZ 2.2.10.2

Vse osebje, ki je vključeno v izvedbo načrta, mora dobro poznati načrt in svojo vlogo. V ta namen morajo biti primerno izobraženi in usposobljeni.

ETZ 2.2.10.3

Načrt mora biti ažuriran ob vsaki organizacijski spremembi, zamenjavi osebja ali spremembi v informacijski strukturi, ki vpliva na načrt. V tem primeru mora biti načrt ponovno testiran v primernem obsegu.

ETZ 2.2.10.4

Načrt obnove (ponovna vzpostavitev stanja) mora biti najmanj enkrat letno celovito testiran.

ETZ 2.2.10.5

Kadar je predpisana ali poslovno potrebna hramba na rezervni lokaciji, mora biti zagotovljena hramba gradiva in potrebnih podatkov in podpornih sistemov za obnovo sistema na rezervni lokaciji, ki mora biti oddaljena od osnovne najmanj 50 km zračne razdalje.

ETZ 2.2.10.6

V primeru potrebe izvajanja načrta za obnovo in restavracijo morajo biti vsi izvedeni postopki obnove natančno dokumentirani in shranjeni.

2.2.11 Zagotavljanje skladnosti na področju varovanja informacij

Varnostni in drugi pogoji ter roki hrambe dokumentarnega gradiva so opredeljeni v okviru splošne in področne zakonodaje ter s poslovnimi pravili organizacije. Redno spremljanje zakonodaje in kontrola skladnosti je instrument za zagotavljanje ustrezne skladnosti in dokaz o profesionalni skrbnosti osebe, ki izvaja zajem ali hrambo.

ETZ 2.2.11.1

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti postopek in odgovorno osebo za spremljanje zakonodaje.

ETZ 2.2.11.2

Oseba, ki izvaja zajem ali hrambo, mora zagotoviti redno izvajanje varnostnih pregledov in to dokumentirati.

2.3 ZAJEM IN PRETVORBA

Predpogoj za ustrezno hrambo gradiv v elektronski obliki je popoln zajem in zanesljiva pretvorba gradiv v elektronsko obliko za hrambo. Pravilno izvajanje postopkov pri zajemu in pretvorbi in predvsem zajem in pretvorba pravih elementov dokumentarnega gradiva in dodajanje ter ustvarjanji pravilnih vrst dodatnih podatkov in metapodatkov sta poglavitnega pomena za zagotavljanje varne in zanesljive dolgoročne hrambe dokumentarnega gradiva, pri kateri so upoštevana vsa temeljna načela hrambe.

ETZ 2.3.1

Oseba, ki izvaja zajem in hrambo, mora v okviru notranjih pravil predpisati ustrezen postopek in odgovornosti za zajem in pretvorbo dokumentarnega gradiva za vsako posamezno obliko (fizično, elektronsko), ki obsega najmanj:

- zahteve za ureditev oz. strukturo gradiv pred zajemom in/ali pretvorbo;
- evidenco gradiv pred in po zajemu oz. pretvorbi;
- evidenco napak v postopku;
- kontrole za zagotavljanje popolnosti zajema in pretvorbe (celotno gradivo v potrebnem kontekstu z vsemi potrebnimi metapodatki) in
- kontrole za preverjanje kakovosti (uporabnosti) zajetega gradiva.

ETZ 2.3.2

Oseba, ki hrani elektronsko podpisane dokumente, mora zagotoviti ustrezne postopke za preverbo veljavnosti elektronsko podpisov ob zajemu.

2.4 KRATKOROČNA HRAMBA

Naloga osebe, ki izvaja hrambo, je ohranitev gradiva in njegove uporabnosti za opredeljen čas, v skladu z zahtevami glede hrambe in na način, ki zagotavlja uporabnost, dostopnost, celovitost in avtentičnost shranjenih gradiv

Za ustrezno izvajanje hrambe gradiv je poleg organizacijskih postopkov in upravljanja z infrastrukturo (glej poglavje 2.2) pomembna uporaba ustrezne aplikacijske programske opreme (ISUD). Ustrezne zahteve v zvezi z uporabljeno podporno programsko opremo so opisane v poglavju 3.

ETZ 2.4.1

Oseba, ki izvaja zajem ali hrambo, mora z notranjimi pravili opredeliti veljavne oblike in nosilce zapisa za hrambo.

2.5 DOLGOROČNA HRAMBA IN NADZOR NAD IZVAJANJEM PRAVIL

Redno spremljanje delovanja v skladu z notranjimi pravili zagotavlja pravočasno odkrivanje morebitnih pomanjkljivosti in napak, je orodje za redno izboljševanje kakovosti storitev in dokaz, da se postopki izvajajo s profesionalno skrbnostjo.

ETZ 2.5.1

Oseba, ki izvaja zajem ali hrambo, mora z notranjimi pravili opredeliti veljavne oblike in nosilce zapisa, ki jih uporablja za dolgoročno hrambo.

ETZ 2.5.2

Zaradi zastaranja tehnologij za hrambo in prikaz dokumentov mora imeti oseba, ki izvaja zajem ali hrambo, vzpostavljene naslednje postopke:

- prenos dokumentov v novo obliko zapisa,

- prenos dokumentov na nove nosilce zapisa in
- zamenjava programske opreme za predstavitev.

ETZ 2.5.3

Oseba, ki izvaja zajem ali hrambo, mora imeti v sistemu za hrambo vzpostavljen mehanizem za obnovo dodatnih vsebin, ki zagotavljajo avtentičnost in nespremenljivost arhiviranih dokumentov. To so digitalni podpisi, časovni žigi in drugi mehanizmi, ki s časom izgubljajo svojo moč.

ETZ 2.5.4

Oseba, ki izvaja zajem ali hrambo, mora imeti v okviru notranjih pravil opredeljene odgovornosti in način izvajanja notranjega nadzora.

ETZ 2.5.5

Oseba, ki izvaja zajem ali hrambo, mora na letni ravni načrtovati izvajanje rednega notranjega in po potrebi zunanjega nadzora.

ETZ 2.5.6

Ponudnik storitev hrambe mora najmanj enkrat letno celovito preveriti izvajanje notranjih pravil s strani preizkušenega revizorja informacijskih sistemov.

2.6 UNIČEVANJE DOKUMENTARNEGA GRADIVA

ETZ 2.6.1

Postopek uničevanja dokumentarnega gradiva mora biti formalno predpisan z notranjimi pravili. Uniči se lahko le gradivo, evidence o gradivu, ki je šlo v uničenje, pa se trajno hranijo.

ETZ 2.6.2

Postopek uničenja mora biti usklajen z obliko gradiva in z varnostno klasifikacijo gradiva (stopnjo tajnosti). Pri uničenju je potrebno poskrbeti, da se uničijo tudi vse kopije (redne varnostne kopije, kopije na lokacijah za ponovno vzpostavitev sistema (disaster recovery), kopije zaradi hitrejše uporabe,....), kar je posebej pomembno pri tajnih gradivih.

ETZ 2.6.3

Notranja pravila osebe, ki izvaja zajem ali hrambo, morajo obsegati opis postopka uničenja, ki mora minimalno opredeljevati:

- pogostost izvajanja oz. opis pogojev za izvedbo postopkov,
- kriterije za izbor gradiv za brisanje,
- izvedben postopek za posamezne vrste gradiv,
- opredelitev potrebnih zapisov v postopku,
- specifikacijo obveznih podatkov o uničenju in

- odgovorne osebe v postopku.

ETZ 2.6.4

Postopek uničenja mora biti v skladu s tajnostjo gradiv in mora obsegati uničenje vseh kopij: fizične oblike, elektronske oblike in varnostnih kopij.

2.7 ZAGOTAVLJANJE ZAPISOV O DELOVANJU SISTEMA

Zakon in uredba posebej predpisujeta izdelavo nekaterih pomembnejših zapisov (npr.: notranja pravila, dnevnik nadzorov, zapisnik o začetnih avtorizacijah informacijskega sistema za hrambo in spremembah, zapisnik o uničenju gradiva,...).

ETZ 2.7.1

Delovanje sistema mora biti podprto z ustreznimi zapisi o delovanju sistema in izvajanju postopkov, ki dokazujejo, da je hramba izvajana v skladu s postavljenimi zahtevami. Zapisi o izvajanju so dokazi o neoporečnosti hranjenega gradiva in hkrati tudi sami po sebi dokumentarno gradivo. Zapisi o delovanju sistema obsegajo zapise o pripravi pravil in različnih postopkov (operativnih, nadzornih, testnih), zapise o izvajanju teh postopkov, zapise o namestitvi infrastrukture in podporne tehnologije.

ETZ 2.7.2

Zapisi o delovanju sistema se morajo hraniti enako dolgo kot osnovna gradiva ali do ustreznega pregleda s strani strokovne osebe, na podlagi katerega je pripravljen nov zapis o opravljenem pregledu in ustreznosti pregledanega sistema.

ETZ 2.7.3

Oseba, ki izvaja zajem ali hrambo, mora redno pripravljati in hraniti zapise o delovanju sistema in izvajanju postopkov v skladu z zahtevami zakona in internimi predpisi.

2.8 DELOVANJE V PREHODNEM OBDOBJU

Ko se spreminjajo pravila in postopki dela, je potrebno zagotoviti kontinuiteto dela. V prehodnem obdobju se pojavljajo zahteve po izvedbi izrednih, enkratnih postopkov, kot je masovni zajem gradiv v nove oblike in/ali nove sisteme. Tudi v okviru izrednih postopkov je potrebno z enako mero skrbnosti kot pri rednih postopkih zagotoviti celovitost in zaupnost gradiva. Notranja pravila morajo zagotoviti nadzorovano izvajanje potrebnih postopkov tudi v prehodnem obdobju.

ETZ 2.8.1

Notranja pravila morajo vsebovati določbe o delovanju v prehodnem obdobju. V kolikor nova pravila spreminjajo stara, je potrebno opredeliti čas prenehanja starih pravil in opredeliti morebitne izjeme. Stara pravila je potrebno varno shraniti.

ETZ 2.8.2

V primeru potrebe izvajanja posebnih postopkov pri vzpostavitvi novega sistema, kot so masovni zajem (skeniranje, uvoz) morajo biti vnaprej opredeljeni in dokumentirani pogoji in roki za izvedbo aktivnosti ter odgovornosti.

ETZ 2.8.3

Notranja pravila morajo vsebovati določbe o korektivnih ukrepih, ki se izvajajo po vzpostavitvi novega sistema in s katerimi se odpravljajo morebitne napake, ki bi lahko nastale pri izvedbi izrednih postopkov.

2.9 SPREMLJANJE IN DOPOLNJEVANJE NOTRANJIH PRAVIL

Notranja pravila morajo biti odraz zakonskih in regulatornih zahtev, interne organizacije osebe, ki izvaja zajem ali hrambo in uporabljene tehnologije. Zaradi nenehnih sprememb je potrebno pravila redno spremljati in usklajevati z obstoječim stanjem.

ETZ 2.9.1

Notranja pravila morajo opredeljevati postopek in odgovorne osebe za izvajanje rednega pregleda skladnosti obstoječih pravil z zakonodajo in uporabljano tehnologijo ter postopek za dopolnitev oz. spremembo teh pravil v skladu z zahtevami iz zakona in uredbe (glej ETZ 2.1.4 in 2.1.5).

2.10 HRAMBA ARHIVSKEGA GRADIVA

Po definiciji je »arhivsko gradivo« dokumentarno gradivo, ki ima trajen pomen za znanost in kulturo ali trajen pomen za pravno varnost oseb v skladu s strokovnimi navodili pristojnih arhivov. Ker je arhivsko gradivo podvrsta dokumentarnega gradiva, mora oseba, ki zajema ali hrani arhivsko gradivo, upoštevati vse zahteve glede dokumentarnega gradiva.

ETZ 2.10.1

Arhivsko gradivo mora biti ustrezno označeno.

ETZ 2.10.2

Oseba mora arhivsko gradivo skrbno hraniti v skladu s postopki za dolgoročno hrambo.

ETZ 2.10.3

V okviru notranjih pravil mora imeti oseba, ki hrani tudi arhivsko gradivo, predviden postopek in odgovornosti za sodelovanje s pristojnim arhivom glede pogojev hrambe, odbiranja arhivskega gradiva iz dokumentarnega gradiva in prenosa v pristojni arhiv.

ETZ 2.10.4

Oseba, ki hrani arhivsko gradivo, mora z ustrezno organizacijo in vsebino notranjih pravil zagotoviti izpolnjevati ustreznih zahtev iz poglavja 3.10.

ETZ 2.10.5

Oseba, ki hrani arhivsko gradivo, mora poleg na glavni lokaciji zagotoviti tudi varno hrambo najmanj dveh dodatnih kopij arhivskega gradiva na dveh geografsko oddaljenih lokacijah (lokacije morajo biti oddaljene najmanj 50 km zračne linije) tako, da se prepreči izguba podatkov ali da bi jih uporabile nepooblaščene osebe. Ponudnik mora evidentirati podatke o hrambi kopij.

3 HRAMBA IN UPRAVLJANJE DOKUMENTARNEGA GRADIVA

3.1 RAZVRŠČANJE GRADIVA

3.1.1 Klasifikacijski načrt

Klasifikacijski načrt leži v središču vsakega ISUD-a. Definira način, na katerega bomo elektronske dokumente organizirali v elektronske zadeve in povezave med zadevami.

To poglavje najprej v podpoglavju našteva zahteve po oblikovanju klasifikacijskega načrta. Nato našteva zahteve, ki se nanašajo na zadeve. Zadnje podpoglavje našteva zahteve, povezane z vzdrževanjem klasifikacijskega načrta.

Posebna pravila, ki se nanašajo na dokumentarno poslovanje, veljajo za državne organe, uprave samoupravnih lokalnih skupnosti ter druge pravne in fizične osebe, kadar na podlagi javnih pooblastil opravljajo upravne naloge, in se nahajajo v Uredbi o upravnem poslovanju (Ur.l. RS, št. 20/2005, 106/2005, 30/2006). Podrobna pravila vsebujejo tudi drugi sorodni predpisi (npr. Sodni red).

Oblikovanje načrta

ETZ 3.1.1.1

ISUD mora podpirati klasifikacijski načrt organizacije in biti združljiv z njim.

ETZ 3.1.1.2

ISUD mora biti sposoben podpirati klasifikacijski načrt, ta pa lahko predstavlja zadeve, kakor so hierarhično organizirane na najmanj treh ravneh. Tri ravni predlagamo kot minimum; v nekaterih okoljih jih bo potrebnih več.

ETZ 3.1.1.3/a

ISUD ne sme omejevati števila ravni v hierarhiji klasifikacijskega načrta, razen če je to predpisano.

ETZ 3.1.1.4

ISUD mora dovoljevati definiranje mehanizmov poimenovanja ob nastavitvi programa.

ETZ 3.1.1.5

ISUD mora podpirati obliko klasifikacijskega načrta, kakršen je bil ob nastavitvi programa, tako da je pripravljen za zajem ali uvoz elektronskih dokumentov.

ETZ 3.1.1.6

ISUD mora dovoliti skrbnik dodajanje novih razredov na katerikoli točki znotraj kateregakoli razreda, dokler na tej točki niso shranjene zadeve. Upoštevajte, da je to mogoče na vseh ravneh.

ETZ 3.1.1.7

Kjer je ISUD načrtovan za uporabo grafičnega uporabniškega vmesnika, mora podpirati pregledovanje in grafično navigacijo po zadevah in klasifikacijskem načrtu ter izbiranje, priklic in prikaz elektronskih zadev ter njihove vsebine s tem mehanizmom.

ETZ 3.1.1.8/a

ISUD mora podpirati definiranje in hkratno uporabo več klasifikacijskih načrtov. To bi se lahko zahtevalo npr. ob združitvi dveh organizacij, ni pa mišljeno za vsakodnevno uporabo. ISUD naj bi podpiral tudi gostovanje več organizacij v istem sistemu.

ETZ 3.1.1.9/a

ISUD mora podpirati porazdeljen klasifikacijski načrt, ki se lahko vzdržuje preko omrežja skladišč elektronskih dokumentov.

Zadeve

ETZ 3.1.1.10

ISUD mora podpirati metapodatke za zadeve v klasifikacijskem načrtu. Ko so dokumenti zajeti, mora ISUD omejiti možnost za dodajanje ali popravljanje metapodatkov na skrbnika.
Zahteve za metapodatke so opisane v Poglavju 3.8.

ETZ 3.1.1.11

ISUD mora ponujati najmanj dva mehanizma za poimenovanje elektronskih zadev v klasifikacijskem načrtu:

- mehanizem za dodelitev strukturiranih numeričnih in alfanumeričnih referenčnih oznak za vsako elektronsko zadevo;
- mehanizem za dodelitev tekstovnega naslova vsaki elektronski zadevi.

V isti aplikaciji mora biti mogoča ločena ali skupna uporaba obeh načinov.

ETZ 3.1.1.12

ISUD mora dovoljevati skrbnikom dodajanje (odpiranje) zadev na najnižji ravni v klasifikacijskem načrtu. Ni potrebno, da so vse najnižje ravni na isti ravni.

ETZ 3.1.1.13

ISUD mora v okviru metapodatkov zadeve zapisati datum odprtja nove zadeve.

ETZ 3.1.1.14

Kadarkoli odpremo novo zadevo, mora ISUD samodejno vključiti v njene metapodatke tiste lastnosti, ki izhajajo iz njene lege v klasifikacijskem načrtu (tj. ime, klasifikacijska oznaka). Npr. če je zadeva Dopisovanje v tej hierarhiji: Načrt regionalnega razvoja: javni posvet: dopisovanje in skrbnik na isti ravni, na kateri je zadeva Dopisovanje, doda novo zadevo, ki se imenuje Formalni zadržki, mora ta samodejno nasledi poglavje Načrt regionalnega razvoja: javni posvet.

ETZ 3.1.1.15/a

ISUD mora podpirati neobvezni mehanizem poimenovanja zadev, ki bi temeljil na nadzorovanih izrazih in odnosih, ki izhajajo iz tezavra, skladnega s standardoma ISO 2788 ali ISO 5964, in povezoval tezaver s klasifikacijskim načrtom.

ETZ 3.1.1.16/a

ISUD mora podpirati neobvezni mehanizem poimenovanja zadeve, ki vključuje tako imena (npr. osebna imena) in/ali datume (npr. datum rojstva) kot imena zadev, vključno s preverjanjem imen na seznamu. Zahteva je primerna za okolja transakcijskih procesov.

ETZ 3.1.1.17/a

Kot dodatek drugim zahtevam v tem podpoglavju mora ISUD podpirati dodelitev kontroliranih gesel v skladu s standardoma ISO 2788 ali ISO 5964 kot opisnih stvarnih gesel metapodatkov za razrede ali zadeve.

ETZ 3.1.1.18

ISUD ne sme vsiljevati nobenih praktičnih omejitev glede števila razredov ali zadev, ki jih lahko definiramo.

ETZ 3.1.1.19

ISUD mora dovoljevati samodejno izdelavo in ohranitev seznama ali podrobnega popisa zadev.

ETZ 3.1.1.20

ISUD mora dovoljevati skrbnikom dodajanje dokumentov v vsaki elektronski zadevi, ki ni zaključena.

ETZ 3.1.1.21

ISUD mora v njegovih metapodatkih zapisati datum odprtja nove zadeve.

ETZ 3.1.1.22

Kadarkoli odpremo novo zadevo, mora ISUD samodejno vključiti v njene metapodatke tiste lastnosti metapodatkov njene matične zadeve, ki so obema skupne (npr. ime, klasifikacijska oznaka).

ETZ 3.1.1.23

ISUD mora preprečiti uporabniku dodajanje elektronskih dokumentov v zaključeno zadevo (izjeme ETZ 3.1.1.25).

ETZ 3.1.1.24

ISUD mora dovoliti skrbniku, da za dodajanje dokumentov ponovno začasno odpre že zaključeno zadevo in jo nato ponovno zapre. Ta možnost je namenjena popravljanju uporabniških napak, če je bila zadeva npr. nenamerno zaključena.

Vzdrževanje načrta

ETZ 3.1.1.25

ISUD mora dovoljevati, da elektronsko zadevo ali celoten razred premestimo v hierarhiji na različna mesta v kvalifikacijskem načrtu in mora zagotavljati, da vsi že dodeljeni elektronski dokumenti ostanejo dodeljeni zadevam, ki smo jih premestili. Ta možnost je mišljena le v izjemnih okoliščinah, kot so združevanje organizacij in druge oblike reorganizacij ali popravljanje pisarniških napak. To zahtevo je treba razlagati skupaj z ETZ 3.1.1.27, 3.1.1.28, 3.1.1.29.

ETZ 3.1.1.26

ISUD mora dovoljevati preklasificiranje elektronskega dokumenta v drugo elektronsko zadevo. Ta možnost je namenjena za izjemne okoliščine, za popravljanje pisarniških napak. Te zahteve moramo razlagati skupaj z ETZ 3.1.1.27, 3.1.1.28 in 3.1.1.29.

ETZ 3.1.1.27

ISUD mora omejiti možnost za premikanje razredov klasifikacijskega načrta, zadev in dokumentov na skrbnika.

ETZ 3.1.1.28

Če katerikoli razred, zadevo ali dokument preklasificiramo, mora ISUD obdržati natančen pregled nad stanjem pred preklasifikacijo, tako da bo mogoče celotno zgodovino preprosto določiti. Najmanjša zahteva je, da se to ohrani v revizijski sledi. Morda je zaželeno, da se zapiše še kje drugje, npr. v metapodatkih premaknjenega objekta.

ETZ 3.1.1.29

Če so bili kakšni razredi, zadeve ali dokumenti preklasificirani, naj bi ISUD omogočal, da skrbnik vnese razlog za preklasifikacijo.

ETZ 3.1.1.30

ISUD mora preprečiti izbris elektronske zadeve ali kateregakoli dela njene vsebine, razen če gre za:
- uničenje v zvezi z roki hrambe;
- izbris, ki ga naredi skrbnik zaradi odprave uporabniških napak.

ETZ 3.1.1.31

ISUD mora dovoljevati, da skrbnik s posebnim postopkom zapre elektronsko zadevo, to možnost pa mora omejiti na skrbnika.

ETZ 3.1.1.32

ISUD naj bi bil sposoben samodejno zapreti elektronsko zadevo, ko so izpolnjeni določeni kriteriji, ki so bili definirani ob vzpostavitvi programa, pri tem pa mora obsegati najmanj:

- zadeve, določene za letno uničenje; npr. konec koledarskega leta, finančnega leta ali drugega definiranega letnega cikla;
- pretek časa od določenega dogodka; npr. zadnjega dodajanja dokumenta v zadevo;
- število elektronskih dokumentov, ki jih zadeva vsebuje.

V določenih okoliščinah so zaželeni drugačni kriteriji, ko npr. velikost zadeve doseže zmogljivost hrambe na prenosnem disku.

ETZ 3.1.1.33

ISUD mora zapisati datum zaprtja zadeve v njene metapodatke.

ETZ 3.1.1.34

ISUD ne sme dovoliti, da zadeva, ki jo začasno ponovno odpremo, ostane odprta, ko se skrbnik, ki jo je odprl, odjavi.

ETZ 3.1.1.35/a

ISUD mora dovoljevati uporabniku ustvarjati navzkrižne reference (tj. povezave tipa »glej tudi«) med povezanimi zadevami.

ETZ 3.1.1.36

ISUD mora ves čas vzdrževati notranjo celovitost (celovitost povezav ali drugega) ne glede na:

- aktivnosti vzdrževanja;
- aktivnosti drugih uporabnikov;
- napake komponent sistema.

Z drugimi besedami: ne sme se zgoditi, da bi bila posledica kakršnegakoli uporabniškega dejanja ali programske napake neskladnost v ISUD-u ali njegovi bazi podatkov.

ETZ 3.1.1.37/a

ISUD mora podpirati možnost večkratnega vnosa elektronskega dokumenta v različne elektronske zadeve, ne da bi se ta dokument fizično podvojil. Z drugimi besedami, za zajetje več kot enega dokumenta na osnovi istega zapisa naj bi uporabljal kazalce.

ETZ 3.1.1.38/a

ISUD mora ponujati orodja za obveščanje skrbnika o statistiki postopkov v okviru klasifikacijskega načrta ter oskrbo z njo, vključujoč število elektronskih zadev ali dokumentov, ki so nastali, bili zaključeni ali izbrisani v določenem obdobju.

3.2 NADZOR IN VARNOST

To poglavje prinaša zahteve za širok obseg kontrol, ki se nanašajo na varnost dokumentov.

Organizacije morajo biti sposobne nadzirati, kdo ima dovoljenje za dostop do dokumentov ter v kakšnih okoliščinah, ker lahko dokumenti vsebujejo osebno, poslovno ali operativno občutljive podatke. Morda je potrebno omejiti dostop tudi zunanjim uporabnikom. Npr. v nekaterih državah, v katerih je svoboda informacij zakonsko omogočena le za določen obseg javnih dokumentov, se lahko zgodi, da jih stranke želijo videti. Zahteve za dostop so navedene v podpoglavju 3.2.1

Dostop do dokumentov in vse druge dejavnosti, ki so povezane z njim in povezanimi zapisi ali podatki, bo prav tako potrebno shraniti v revizijski sledi, da bi zagotovili pravno dopustnost in bi lahko pomagali pri ponovnem pridobivanju podatkov. Zahteve za nadzor s revizijsko sledjo so navedene v podpoglavju 3.2.2

Varnost dokumentov vključuje tudi možnost varovanja pred sistemskimi napakami s pomočjo rezervne kopije in možnost obnovitve dokumenta na podlagi rezervne kopije. Te zahteve so navedene v podpoglavju 3.2.3

Zaradi različnih razlogov lahko dokumente premikamo med sistemi in lokacijami. Zahteve za nadzor takšnih prenosov so navedene v podpoglavju 3.2.4.

Zahteve za nadzor avtentičnosti dokumentov so navedene v podpoglavju 3.2.5.

In nazadnje, zahteve za varnost zaupnih zapisov so navedene v podpoglavju 3.2.6.

3.2.1 Dostop

Organizacije na splošno potrebujejo nadzor nad dostopom do njihovih dokumentov. Potrebujejo omejevanje ali dovoljevanje dostopa do specifičnih dokumentov in zadev posameznikom in/ali skupinam uporabnikov. Kjer gre za nacionalno varnost, lahko upoštevajo varnostno dovoljenje uporabnikov.

Dodeljevanje dostopnih pravic mora biti omejeno na določene vloge, npr. na vlogo skrbnika. Kljub temu upoštevajte, da je ta vloga s stališča sistema le izvršilna in da odločitve sprejemajo na višji ravni. Takšne odločitve navadno temeljijo na zakonih in uredbah, kakršne so zakonodaja o informacijah, zakonodaja o varstvu podatkov, arhivska zakonodaja in sektorski predpisi, ki urejajo določeno panogo.

ETZ 3.2.1.1

ISUD mora dovoljevati skrbniku omejevanje dostopa do dokumentov, zadev in metapodatkov na določene uporabnike ali uporabniške skupine.

ETZ 3.2.1.2

ISUD mora dovoljevati skrbniku dodati atribute profilu uporabnika, ki bodo določali možnosti, polja metapodatkov, dokumente ali zadeve, do katerih ima uporabnik dostop. Atributi profila bodo:

- preprečili dostop do ISUD-a brez odobrenega mehanizma za avtentikacijo, pripisanega uporabniškemu profilu;
- omejili uporabniku dostop do določenih zadev ali dokumentov;
- omejili uporabniku dostop do posebnih razredov v klasifikacijskem načrtu;
- omejili uporabniku dostop v skladu z njegovim varnostnim dovoljenjem;
- omejili uporabniku dostop do posameznih funkcij (npr. branje, posodabljanje ali ničenje specifičnih polj metapodatkov);

- zavrnili uporabniku dostop po določenem datumu;
- dodelili uporabnika določeni skupini ali skupinam.

Primer priznanega mehanizma za določanje avtentikacije je geslo.

ETZ 3.2.1.3

ISUD mora biti sposoben ponuditi enake kontrolne funkcije za nosilce vlog in za uporabnike. Ta funkcija dovoljuje skrbnikom, da namesto večjega števila posameznih uporabnikov skrbijo za določeno vrsto vlog glede pravic do dostopa in le-te upravljajo. Vloge lahko vključujejo predstojnika, odgovornega za pritožbe, varnostnega analitika, skrbnika baze podatkov itd.

ETZ 3.2.1.4

ISUD mora biti sposoben vzpostaviti skupino uporabnikov, ki je povezana z naborom zadev ali dokumentov. Primer skupine je lahko osebje, prodajna skupina.

ETZ 3.2.1.5

ISUD mora dovoliti uporabniku, da je član več kot ene skupine.

ETZ 3.2.1.6

ISUD mora dovoliti, da samo skrbniki vzpostavljajo uporabniške profile in uporabnike dodelijo skupinam.

ETZ 3.2.1.7

ISUD naj bi dovolil uporabniku določiti, kateri drugi uporabniki ali skupine lahko dostopajo do dokumentov, za katere so odgovorni. To možnost naj bi jim zagotovil skrbnik v skladu s politiko organizacije.

ETZ 3.2.1.8

ISUD mora dovoljevati spremembe varnostnih atributov za skupine ali uporabnike (kot so pravice dostopa, raven zaščite, privilegiji, dodelitev gesla in upravljanje), vendar pa jih lahko izvedejo le skrbniki.

ETZ 3.2.1.9

Če uporabnik zahteva dostop ali išče dokument, mapo ali zadevo, do katere nima pravice dostopa, mora ISUD ponuditi katerega od teh odgovorov (izbranega v času nastavitve programa):

- prikazati naslov in metapodatke;
- prikazati obstoj podatkov, zadeve ali dokumenta (tj. izpis številke zadeve ali dokumenta), ne pa tudi izpisati naslova in drugih metapodatkov;
- ne prikazati nikakršnih informacij o dokumentih ali na kakršenkoli način namigovati na njihov obstoj.

Te opcije so predstavljene po vrstnem redu povečevanja varnosti. Tretja zahteva (tj. najbolj brezpogojna) pomeni, da ISUD ne sme vključiti takih dokumentov v noben

rezultat iskanja; ta raven zaupnosti je navadno primerna za dokumente, ki vsebujejo teme, kot je npr. nacionalna varnost.

ETZ 3.2.1.10

Če uporabnik išče po celotnem tekstu, ne sme ISUD nikoli vključiti v seznam rezultatov iskanja nobenih dokumentov, do katerih uporabnik nima pravic dostopa. Če je izbrana prva možnost (v ETZ 3.2.1.9), je to lahko videti kot nasprotje. To navidezno nasprotje je namerno; če te zahteve namreč ni, uporabnik lahko uporabi iskanje po tekstu za pregledovanje vsebin zapisov, do katerih nima dostopa. Posledica tega je, da mora ta zahteva imeti prednost pred zahtevo ETZ 3.2.1.9.

ETZ 3.2.1.11

Če ISUD dovoljuje uporabniku poskuse nepooblaščenih dostopov do zadev, map ali dokumentov, mora to zabeležiti v revizijski sledi. Za to funkcijo bo sprejemljivo, da jo je možno nadzorovati, tako da bo uporabna samo za vrste in stopnje tajnosti, ki jih določi skrbnik (kot je definirano v zahtevi ETZ 3.2.6).

ETZ 3.2.1.12

Če ISUD hrani podroben popis zadeve (glejte zahtevo 3.1.2.10), mora biti možno uporabnikom omejiti dostop do delov popisa, ki so določeni v času vzpostavitve programa.

3.2.2 Revizijske sledi

Revizijska sled je zapis opravljenih dejanj, ki se nanašajo na ISUD. To vključuje dejanja, ki jih storijo uporabniki ali skrbniki ali dejanja, ki se izvajajo samodejno preko ISUD, kot rezultat sistemskih parametrov. Za uradno definicijo glejte Definicije v podpoglavju 1.5. Na revizijsko sled dokumentov lahko gledamo kot na metapodatke dokumentov (ker vsebuje informacije, ki opisujejo nekatere vidike zgodovine dokumentov), čeprav to ni bistveno.

ISUD mora biti sposoben upravljati in nadzorovati elektronske dokumente skladno s standardi, potrebnimi za usklajenost z zahtevami za pravno dopustnost in varnost ter mora biti sposoben to skladnost prikazati. Revizijska sled je ključni faktor pri zadostitvi tem zahtevam, ker na vsakem dokumentu ohranja celovit zapis o vseh dejanjih. Obseg podatkov v revizijski sledi lahko postane velik, če opazujemo vsa dejanja. Posledica je, da se lahko v nekaterih izvedbah uprava odloči, da določena dejanja ne bodo zabeležena. V večini primerov se revizijska sled, ki jo vodimo na periferni enoti, povezani z računalnikom, periodično prenaša v hrambo na enote, ki nimajo neposredne povezave in postane predmet uničenja, kolikor in kadar so posamezni ustrezni dokumenti uničeni. To je stvar politike uprave in/ali zahtev posameznih predpisov. Zato ta ETZ vključuje sistemske zahteve, da so omogočena ta dejanja, ne vključuje pa obsega, v katerem se uporabljajo.

ETZ 3.2.2.1

ISUD mora vzdrževati nespremenljivo revizijsko sled, ki je sposobna samodejno zajemati in shranjevati informacije o:

- vseh dejanjih, ki so potekala na elektronskih dokumentih, zadevah ali klasifikacijskem načrtu;

- uporabnikih, ki so začeli in/ali izvedli dejanja;
- datumu in času dogodka.

Beseda nespremenljivo pomeni, da revizijske sledi uporabnik nikakor ne more spreminjati ali uničiti. Lahko je predmet reorganizacije in kopiranja na prenosne nosilce zapisa, če to zahteva npr. program baze podatkov, vse dokler njegova vsebina ostaja nespremenjena.

ETZ 3.2.2.2

Ko se enkrat funkcionalnost revizijske sledi aktivira, mora ISUD slediti dogodkom brez ročnih posegov in shranjevati informacije o njih v revizijski sledi.

ETZ 3.2.2.3

ISUD mora vzdrževati revizijsko sled tako dolgo, dokler je potrebno, to pa je najmanj, dokler obstajajo elektronski dokumenti ali elektronske zadeve, na katere se nanaša.

ETZ 3.2.2.4

ISUD mora omogočati revizijsko sled o vseh narejenih spremembah v:

- skupinah elektronskih zadev;
- posameznih elektronskih zadevah;
- elektronskih mapah;
- elektronskih dokumentih;
- elektronskih zapisih;
- metapodatkih, povezanih s katerokoli našteto zadevo.

ETZ 3.2.2.5

ISUD mora zagotoviti revizijsko sled o vseh spremembah administrativnih parametrov. Npr. če skrbnik uporabniku spremeni dostopne pravice.

ETZ 3.2.2.6

ISUD mora biti sposoben zajemati in hraniti informacije revizijske sledi o teh dejanjih:

- datumu in času zajema vseh elektronskih dokumentov;
- preklasifikaciji kakega elektronskega dokumenta v drugo elektronsko mapo (glejte
- zahtevo 3.1.4.2);
- preklasifikaciji kake elektronske zadeve v okviru klasifikacijskega načrta (glejte zahtevo 3.1.4.1);
- spremembi rokov hrambe elektronske zadeve;
- kakršnikoli spremembi metapodatkov v povezavi z razredi, elektronskimi zadevami ali elektronskimi dokumenti;
- datumu in času kreiranja, spremembe in uničenja metapodatkov;
- spremembi pravic dostopa, ki se nanašajo na elektronsko zadevo, dokument ali uporabnika;
- postopkih izvoza ali prenosa, ki smo jih izvajali na elektronski zadevi;
- datumu in času prikaza (glejte Definicije, podpoglavje 1.5);
- postopkih brisanja elektronskih zadev ali dokumentov.

ETZ 3.2.2.7

ISUD mora skrbniku dovoljevati oblikovati pripomočke za revizijsko sled, da lahko izbere dejanja, o katerih se informacije samodejno shranjujejo; ISUD mora zagotavljati, da so izbira in vse spremembe shranjene v revizijski sledi.

ETZ 3.2.2.8

ISUD mora zagotavljati, da so podatki v revizijski sledi na voljo za pregled na zahtevo, tako da je posamezne dogodke mogoče identificirati, da so dostopni vsi podatki, ki se nanašajo nanje in da to lahko dosežemo s pooblaščenim zunanjim osebjem, ki sistem slabo pozna oziroma ga sploh ne pozna.

ETZ 3.2.2.9

ISUD mora biti sposoben izvoziti revizijsko sled za določene elektronske dokumente, elektronske zadeve in skupine zadev (brez vpliva na revizijsko sled, ki jo hrani ISUD). To funkcijo lahko uporabljajo zunanji nadzorniki, ki želijo preiskati ali analizirati sistemske aktivnosti.

ETZ 3.2.2.10

ISUD mora biti sposoben zajeti in shraniti kršitve (tj. poskuse uporabnika, da bi prišel do dokumenta, mape ali zadeve, do katerih nima dostopa) in (kjer so dovoljeni poskusi kršitev) poskuse kršitve kontrolnega mehanizma dostopa.

Za ilustracijo okoliščin, ki lahko dovolijo poskuse kršitve, glejte zahteve opisane pri 3.2.1.9.

ETZ 3.2.2.11

ISUD mora biti sposoben zagotoviti poročila najmanj za dejanja na razredih, zadevah in dokumentih, urejena po:

- dokumentu, zadevi ali razredu;
- uporabniku;
- kronološkem zaporedju.

ETZ 3.2.2.12

ISUD mora biti sposoben zagotoviti poročila o dejanjih na zadevah in dokumentih, urejena po delovnih postajah in (kjer je tehnično primerno) omrežnih naslovih.

3.2.3 Rezervna kopija in obnova

Tako poslovne kot določbe veljavnih predpisov zahtevajo, da mora imeti ISUD zagotovljen vsestranski nadzor, da zagotovi vsakodnevno izdelovanje rezervnih kopij dokumentov in metapodatkov in da je sposoben hitro obnoviti dokumente, če se kateri izgubi zaradi napak v sistemu, nesreč, kršitev varnosti itd.

Redno samodejno izdelovanje rezervnih kopij in obnavljanje lahko omogoči ISUD sam ali v povezavi s podporo in pripomočki sistema za upravljanje z elektronskimi zapisi (ISUZ) ali sistemom za upravljanje baze podatkov, ki dela z ISUD-om. V praksi so funkcije izdelave rezervne kopije in obnavljanja lahko razdeljene med skrbnike ISUD-a in osebje, zadolženo za informacijsko tehnologijo v organizaciji.

ETZ 3.2.3.1

ISUD mora omogočati avtomatsko izdelavo rezervnih kopij in postopek obnove, ki omogoča redno izdelovanje rezervnih kopij vseh ali izbranih razredov, zadev, dokumentov, metapodatkov in administrativnih atributov podatkovnega skladišča ISUD.

ETZ 3.2.3.2

ISUD mora omogočati skrbniku narediti razpored postopkov izdelave rezervnih kopij z:

- določitvijo pogostosti izdelave rezervnih kopij;
- izbiro razredov, zadev ali dokumentov, ki naj bodo rezervno hranjeni;
- določanjem nosilcev zapisa za hrambo, sistema ali lokacije za rezervno kopijo (npr. enota brez neposredne povezave z računalnikom, ločen sistem, oddaljen prostor).

ETZ 3.2.3.3

ISUD mora samo skrbniku dovoliti vzpostavitev prejšnjega stanja na osnovi rezervne kopije. Po obnovi mora biti zagotovljena popolna neokrnjenost podatkov.

ETZ 3.2.3.4

ISUD mora dovoljevati le skrbniku, da zavrti ISUD z rezervne kopije naprej v novejše stanje, tako da ohrani popolnoma neokrnjene podatke.

ETZ 3.2.3.5

ISUD mora biti, če bi bili podatki nepopolno obnovljeni, sposoben na to opozoriti uporabnike, ko ti ponovno uporabljajo sistem.

ETZ 3.2.3.6

ISUD mora omogočati uporabnikom navesti, da izbrani dokumenti veljajo za »vitalne dokumente«.
Vitalni dokumenti so tisti, ki so absolutno potrebni za to, da je organizacija sposobna nadaljevati poslovanje; to razumemo bodisi kot zmožnosti za obvladovanje nujnih/ katastrofalnih razmer bodisi kot varovanje svojih finančnih in pravnih interesov. Identifikacija in varstvo takih dokumentov sta zato zelo pomembna za vsako organizacijo.

ETZ 3.2.3.7

ISUD mora omogočati, da so vitalni dokumenti in drugi dokumenti obnovljivi s posebnimi postopki.

3.2.4 Sledenje gibanju dokumentov

Dokler zadeve in njihovi metapodatki obstajajo, jih lahko prenašamo iz enega nosilca zapisa za hrambo ali lokacije do druge, kot se njihova dejavnost zmanjšuje in/ali uporaba spreminja. Prenos je lahko lokalen do priročnega skladišča (npr. prenosni nosilec zapisa, kot je zgoščenka v magnetno-optični knjižnici), ločene enote (npr. do lokalnega ali

oddaljenega prostora za hrambo) ali do drugega skladišča dokumentov (npr. državni ali nacionalni arhiv). Potrebna je sposobnost sledenja, da bi zabeležili spremembe lokacije in tako olajšali dostop ter izpolnili normativne zahteve.

ETZ 3.2.4.1

ISUD mora zagotoviti možnost sledenja za nadzor in zapis informacij o lokaciji in gibanju zadev, in sicer tako elektronskih kot fizičnih.

ETZ 3.2.4.2

Funkcija sledenja mora zapisati informacije o gibanju, te pa vključujejo:

- enolični identifikator zadeve ali dokumentov;
- trenutno lokacijo kot tudi število prejšnjih lokacij, ki jih je določil uporabnik (lokacije naj bi določal uporabnik);
- datum pošiljanja/premikanja zadeve z lokacije;
- datum sprejema zadeve na lokacijo (za prenose);
- uporabnika, odgovornega za premikanje (kjer je potrebno).

ETZ 3.2.4.3

ISUD mora ohranjati dostop do vsebine elektronskega dokumenta, vključno z možnostjo za prikaz le-te ter ohranitve njene strukture in oblike zapisa v času in tekom generacij programov za poslovanje z dokumentarnim gradivom. To je možno, ni pa nujno, izvesti z uporabo programa za pregledovanje večjega števila oblik zapisa.

3.2.5 Avtentičnost in celovitost

Politika podjetja in zahteve poslovnih procesov za hrambo dokumentov določajo, katere dokumente naj zajamemo in kdaj. Bistveno je, da se od takrat, ko je dokument zajet, vsi njegovi deli, struktura in metapodatki, potrebni za zagotovitev avtentičnosti in celovitosti dokumenta, ne spreminjajo več. Da bi ohranili svojo avtentičnost, moramo zajete dokumente ohraniti v nespremenljivi obliki in jih v celotnem življenjskem ciklusu zavarovati pred namernimi ali naključnimi spremembami vsebine, konteksta, strukture in izgleda.

ETZ 3.2.5.1

ISUD mora omejiti dostop do sistemskih funkcij v skladu z vlogo uporabnika in strogim administrativnim nadzorom sistema. To je potrebno za zavarovanje avtentičnosti in celovitosti elektronskih dokumentov.

ETZ 3.2.5.2

Kjer je mogoče in potrebno, mora biti ISUD sposoben opozoriti na poskus zajetja dokumentov, ki so nepopolni in neskladni (nekonsistentni) na način, ki bi kasneje ogrozil njihovo navidezno avtentičnost ali celovitost. Npr. naročilo za nakup brez veljavnega elektronskega podpisa ali račun nepriznanega dobavitelja.

ETZ 3.2.5.3

Kjer je možno in potrebno, mora biti ISUD sposoben opozoriti na poskus zajema dokumenta, pri katerem bodoče preverjanje njegove avtentičnosti in celovitosti ni možno.

ETZ 3.2.5.4

ISUD mora preprečiti, da bi uporabniki in skrbniki kakorkoli spreminjali vsebino elektronskih dokumentov (razen če je sprememba del poslovnega in/ali dokumentarnega procesa, kot je navedeno drugje v tej specifikaciji).

3.2.6 Vrste in stopnje tajnosti

Podpoglavje 3.2.1 opisuje zahteve za nadzorovanje dostopa uporabnikov ali skupin. V nekaterih okoljih, še posebej tistih, ki so vpletena v nacionalno varnost, je treba z uporabo sistema stopenj in vrst tajnosti in varnostnih dovoljenj še bolj omejiti dostop. Ta dovoljenja so nad vsemi pravicami dostopa, ki bi bile morda dodeljene z uporabo funkcij, opisanih v podpoglavju 3.2.1. Zahteve v tem podpoglavju se nanašajo le na okolja, ki imajo takšne potrebe. To dosežemo z dodeljevanjem ene ali več »stopenj tajnosti« razredom, zadevam ali dokumentom.

Pojem »stopnja tajnosti« v tej specifikaciji uporabljamo v pomenu »enega ali več pojmov, povezanih z dokumentom, ki definirajo pravila za dostop do dokumenta«. Upoštevajte, da ta pojem uporabljamo izrecno v tej specifikaciji in ni splošno uporaben. Uporabnikom je lahko dodeljeno eno ali več varnostnih dovoljenj, ki preprečujejo dostop do vseh zadev/dokumentov, ki imajo višjo stopnjo tajnosti. Stopnje tajnosti so lahko sestavljene iz podstopenj. Nekatere podstopnje so po naravi hierarhične. Druge podstopnje so lahko urejene različno, po navadi na način, ki je v organizaciji ali sektorju enkraten. Ta specifikacija podrobno opisuje le zahteve za hierarhično organizirane podstopnje.

ETZ 3.2.6.1

ISUD mora dovoliti, da dokumentu dodelimo stopnjo in vrsto tajnosti.

ETZ 3.2.6.2

ISUD mora v času vzpostavitve programa dovoliti izbiro teh možnosti:

- dodelitev stopnje in vrste tajnosti razredom, zadevam ali mapam;
- elektronski razredi, zadeve ali mape nimajo oznake stopnje in vrste tajnosti.

To je zaželeno, ker nekatere organizacije raje dodeljujejo stopnje in vrste tajnosti elektronskim zadevam, s tem da posnemajo funkcionalnost dokumentov v papirni obliki in fizičnih zadev, druge organizacije pa zavarujejo le pomembnejše dokumente.

ETZ 3.2.6.3

Varnostni podsistem ISUD-a naj bi bil zmožen učinkovite uporabe skupaj z uveljavljenimi proizvodi (rešitvami) za varnost.

ETZ 3.2.6.4

ISUD mora dovoliti, ni pa izrecno zahtevano, da so stopnje tajnosti sestavljene iz ene ali več podstopenj. Npr. Stopnja tajnosti je lahko sestavljena iz treh podstopenj. Poglejmo primer s stopnjami tajnosti, ki so v uporabi v upravi:

Podstopnja	**Dovoljene vrednosti**
Razred	strogo tajno tajno zaupno interno brez omejitev

Pri tem izmišljenem primeru je podstopnja »razred« hierarhična (glejte zahtevo 3.2.6.6), druge podstopnje pa niso. Zahteve za hierarhične podstopnje so splošne in so navedene spodaj. Vendar pa so zahteve za hierarhične podstopnje lahko zapletene; razen zahteve 3.2.6.5 tukaj niso podrobneje obravnavane.

ETZ 3.2.6.5

ISUD mora dovoljevati specifično izvedbo zapletenih ali posebnih varnostnih pravil. To bi bilo možno s primernimi programskimi uporabniškimi vmesniki. To je potrebno tam, kjer je potrebno upravljati dokumente z uporabo dogovorov za označevanje, ki tu niso navedeni, kot npr. IDO = International Defence Organization (Mednarodna obrambna organizacija) ali omejitve dostopa do medicinskih dokumentov.

ETZ 3.2.6.6

Za najmanj eno podstopnjo mora ISUD podpirati hierarhijo najmanj petih ravni, od neomejenega dostopa na najnižji ravni do strožje prepovedi na najvišji. Podstopnja razred v zahtevi 3.2.6.4 je primer za to.

ETZ 3.2.6.7

ISUD mora omogočati dodelitev varnostnega dovoljenja uporabnikom, ki se ujema s podstopnjami.

Za nadaljevanje primera pri zahtevi 3.2.6.4 bo uporabniku dodeljeno eno od teh varnostnih dovoljenj:

- strogo tajno
- tajno
- zaupno
- interno
- brez omejitev.

ETZ 3.2.6.8

ISUD mora uporabniku zavrniti dostop do elektronskih dokumentov (in razredov ter elektronskih zadev v skladu z izbiro, narejeno pri 3.2.6.2), ki imajo dodeljeno višjo stopnjo tajnosti kot pa je varnostno dovoljenje.
Opozarjamo, da prava raven odobritve dostopnosti morda še ne zadošča za dostop. Dostop do elektronskih dokumentov je dodatno lahko omejen na določene uporabnike, vloge ali skupine, ki uporabljajo funkcije, opisane v podpoglavju 3.2.1.

ETZ 3.2.6.9

ISUD mora podpirati samodejno dodelitev najnižje izbrane stopnje tajnosti v podstopnji posameznega razreda, elektronske zadeve ali dokumenta, ki mu ni dodeljena druga vrsta tajnosti.

Glede na primer iz ETZ 3.2.6.4 bi bila npr. avtomatska dodelitev stopnje »brez omejitev«.

ETZ 3.2.6.10

ISUD mora biti sposoben preprečiti, da bi imela neka elektronska zadeva določeno nižjo stopnjo tajnosti kot katerikoli elektronski dokument v okviru te zadeve (glede na izbor, narejen v zvezi z zahtevo ETZ 3.2.6.2).

ETZ 3.2.6.11

Skrbnik mora biti sposoben z enostavno poizvedbo ugotoviti najvišjo stopnjo tajnosti vsakega dokumenta v vsakem razredu ali zadevi. V nekaterih okoljih bo to pomembna funkcija za pomoč pri upravljanju.

ETZ 3.2.6.12

ISUD mora podpirati rutiniran, časovno načrtovan pregled stopenj in vrst tajnosti.

3.3 ROK HRAMBE IN IZLOČANJE

Roki hrambe in odbiranje in izločanje dokumentov so eden izmed pomembnejših vidikov elektronske hrambe dokumentarnega ter arhivskega gradiva. Določajo, kako dolgo mora sistem hraniti dokumente ter način njihovega odstranjevanja in izbire za odstranjevanje iz sistema.

3.3.1 Roki hrambe

Roki hrambe za posamezno vrsto dokumentarnega gradiva so določeni s posameznimi področnimi zakoni. Tudi ZVDAGA ne vsebuje podrobnejših določil glede rokov hrambe za posamezno vrsto gradiva. Loči le dve vrsti hrambe dokumentarnega gradiva: dolgoročno hrambo ter »običajno« hrambo, za katero ne uporablja posebnega izraza. Meja med obema vrstama hrambe je trajanje hrambe petih let, ZVDAGA pa določa le, da mora biti oblika elektronskega zapisa za dolgoročno hrambo takšna, da po več kot petih letih omogoča pretvorbo v novo obliko zapisa, ki bo tudi potem izpolnjevala pogoje za varno hrambo.

Pomembno se je zavedati razlike med roki hrambe ter med dejanskim časom hrambe posamezne enote dokumentarnega gradiva. Če je s področnim zakonom za posamezno vrsto dokumentarnega gradiva določen rok hrambe, ki je krajši od 5 let, to še ne pomeni, da se takšno gradivo dejansko ne bo hranilo več od petih let. Rok hrambe pet let namreč začne teči šele takrat, ko je zadeva, katero sestavlja dokumentarno gradivo, zaključena, lahko pa se zgodi, da je takšno gradivo nastalo že precej prej, zato se bo tudi hranilo precej dalj, kot določa posamezen rok hrambe. Torej, večina gradiva, za katerega področni zakon določa hrambo krajšo od petih let, se bo dejansko hranilo dalj, zato v večini primerov pri hrambi pride v poštev predvsem dolgoročna hramba.

ETZ 3.3.1.1

ISUD mora ponujati funkcijo, ki podrobno navaja roke hrambe, avtomatizira obveščanje in dejanja uničevanja ter zagotavlja enotne pripomočke za izvoz dokumentov in metapodatkov.

ETZ 3.3.1.2

ISUD mora biti sposoben omejiti določanje in spreminjanje rokov hrambe na skrbnika.

ETZ 3.3.1.3

ISUD mora dovoljevati skrbniku, da definira in shrani standardni nabor prilagojenih standardnih rokov hrambe.

ETZ 3.3.1.4

ISUD mora biti sposoben povezati roke hrambe s katerimkoli dokumentom, zadevo ali razredom klasifikacijskega načrta. Roke hrambe lahko izberemo iz standardnega nabora ali pa jih vpišemo ročno, ko odpremo zadevo.

ETZ 3.3.1.5/a

ISUD mora biti sposoben združiti več kot en rok hrambe s katerokoli zadevo ali razredom klasifikacijskega načrta.

Sledijo primeri:

- zadeva ima lahko en rok hrambe, standarden za organizacijo, ki ji pripada, in drugi posebni rok, ki je povezan s procesom in se nanaša na zadevo;
- razred ima lahko rok hrambe, ki ga predpisuje zakon, toda razred znotraj tega ima tudi drug rok z drugimi pravili, ki izhajajo iz predpisov hrambe za druge dokumente.

ETZ 3.3.1.6

Vsak dokument v zadevi ali razredu je treba samodejno voditi po roku hrambe, vezanem na zadevo ali razred.

ETZ 3.3.1.7

Vsak rok hrambe mora vsebovati odločitev o odbiranju in izločanju (zahteva ETZ 3.3.1.10), čas hrambe (zahteva ETZ 3.3.1.11), vzrok in vir za odločitev.

ETZ 3.3.1.8

Za vsako zadevo mora ISUD:

- samodejno slediti rokom hrambe, ki so dodeljeni zadevi ali razredu, v katerega spada;

- začeti proces odbiranja in izločanja, ko se izteče končni rok hrambe.

ETZ 3.3.1.9

Če ima zadeva ali razred določenih več rokov hrambe, mora ISUD samodejno slediti vsem rokom, ki so določeni v teh seznamih rokov hrambe, in začeti proces odbiranja in izločanja, ko se izteče skrajni izmed rokov hrambe.

ETZ 3.3.1.10

ISUD mora omogočati najmanj te odločitve za vsak rok hrambe:

- trajna hramba;
- pripraviti za pregled na prihodnji datum, ki je definiran v zahtevi ETZ 3.3.1.11;
- uničiti na bodoči datum, ki je definiran v zahtevi ETZ 3.3.1.11;
- prenesti na prihodnji datum, ki je definiran v zahtevi ETZ 3.3.1.11.

ETZ 3.3.1.11

Vsak seznam rokov hrambe mora omogočati določanje prihodnjih rokov hrambe (kot je definirano v ETZ 3.3.1.10) z datumi, ki so določeni na ta način:

- po preteku določenega obdobja od odprtja zadeve;
- po preteku določenega obdobja po zaključku zadeve;
- po preteku določenega obdobja, ko je zadevi dodan zadnji dokument;
- po preteku določenega obdobja, ko je dokument iz zadeve zadnjič uporabljen;
- po preteku določenega obdobja, po določenem dogodku (ki je opisan v seznamu in ga ISUD ne bo samodejno prepoznal, ampak mu ga bo javil skrbnik; npr. »po podpisu pogodbe«);
- označeno kot »neomejeno« za pojasnitev dolgoročne hrambe dokumentov.

Ker zgornje navedbe vključujejo splošne možnosti, je možno, da bodo imeli nekateri dokumenti takšne zahteve za hrambo, ki tukaj niso naštete.

ETZ 3.3.1.12

ISUD mora podpirati roke hrambe, ki trajajo od enega meseca do 100 let (za zahteve pod ETZ 3.3.1.11

Ta spodnja in zgornja meja sta predlagani kot poljubni periodi, da bi se v praksi izognili omejitvam. Ker ni verjetno, da bi kakšen ISUD obstajal 100 let, bo zahteva s tem v zvezi dovoljevala izvoz dokumentov v prihodnje sisteme, ne da bi bilo potrebno popravljati sezname rokov hrambe.

ETZ 3.3.1.13

ISUD mora samodejno zapisati in poročati skrbniku o vseh dejavnostih odbiranja in izločanja.

ETZ 3.3.1.14

ISUD mora omogočiti dodeljevanje roka hrambe zadevi, ki ima lahko prednost pred rokom hrambe, določenem razredu, ki mu zadeva pripada.

ETZ 3.3.1.15

ISUD mora dovoljevati skrbniku dopolniti katerikoli rok hrambe, dodeljen katerikoli zadevi na katerikoli točki njenega življenjskega ciklusa.

ETZ 3.3.1.16

ISUD mora dovoljevati skrbniku spremeniti katerikoli rok(e), priključen(e) zadevi, na katerikoli točki njenega življenjskega ciklusa.

ETZ 3.3.1.17/a

ISUD mora dovoljevati definiranje zbirke procesnih pravil, ki naj bi jih uporabljali kot pripomoček za opozarjanje pred začetkom odbiranja in izločanja določenih zadev in razredov. Npr.:

- pregled zadev in vsebin, ki ga izvaja določen upravnik ali skrbnik;
- obvestilo skrbniku, če ima zadeva določeno raven varnosti.

3.3.2 Pregled in odbiranje

Pregled je proces preverjanja zadev, ki se uvede s časom, ko pride datum ali se zgodi dogodek, ki je bil določen z rokom hrambe, da se odločimo, ali jih bomo ohranili, prenesli v drug sistem ali uničili. Pregledovalec lahko ocenjuje metapodatke, vsebino ali oboje. V nekaterih okoljih se roki hrambe uporabljajo za odbiranje in izločanje brez pregleda.

Tako kot roki hrambe, sta tudi potrebnost in način izvajanja pregleda in odbiranja zadev in gradiva za različne vrste dokumentarnega gradiva posebej določena v posameznih predpisih. Pri pregledu in odbiranju gradiva oseb javnega prava je zato potrebno upoštevati predvsem Uredbo o upravnem poslovanju, ki vsebuje določila glede rokov hrambe in druga.

ETZ 3.3.2.1/a

ISUD mora biti sposoben redno opozarjati skrbnika na vse roke hrambe, ki bodo začeli veljati v posameznih časovnih obdobjih in ponuditi kvantitativna poročila o obsegu in vrstah dokumentov.

ETZ 3.3.2.2/a

Skrbnik mora biti sposoben določiti pogostost poročil o rokih hrambe, vrsto sporočenih podatkov in poudariti izjeme, kot so prekoračitve odbiranja in izločanja.

ETZ 3.3.2.3

ISUD mora podpirati postopek pregledovanja s prikazom elektronskih zadev, ki naj bi bile pregledane, z njihovimi metapodatki in informacijami o rokih hrambe (razlog) na način, ki dovoljuje pregledovalcu učinkovito pregledovanje (tj. navigacijo in preučevanje) vsebine zadev in/ali metapodatkov. V praksi pomeni to zmožnost za usmerjanje naprej, nazaj itd. v zadevi in med njimi ter iz/do metapodatkov zadev in dokumentov.

ETZ 3.3.2.4/a

ISUD mora opozoriti skrbnika, če je na zadevo, ki je namenjena za uničenje, narejena povezava iz neke druge zadeve in mora zadržati proces uničevanja, da omogoči ta dva ukrepa:

- potrditev skrbnika, da se proces nadaljuje ali prekine;
- izdelavo poročila s podrobnostmi o teh zadevah ali dokumentu(ih) in vse reference ali povezave, ki kažejo nanje.

ETZ 3.3.2.5

ISUD mora dovoliti pregledovalcu, da lahko med pregledom vsake zadeve izvede najmanj eno od teh dejanj:

- označi zadevo za brisanje;
- označi zadevo za prenos (glejte zahteve pri ETZ 3.3.3.7);
- spremeni roke hrambe (ali določi drug rok) tako, da se zadeva ohrani in kasneje ponovno pregleda, pri čemer se datum določi kot v zahtevi ETZ 3.3.1.11.

ETZ 3.3.2.6

ISUD mora dovoljevati pregledovalcu vnesti komentarje v metapodatke zadeve, da se zapišejo razlogi odločitev, sprejetih pri pregledu.

ETZ 3.3.2.7

ISUD mora opozoriti skrbnika na zadeve, ki jim je potekel rok in so namenjene odbiranju in izločanju, pred izvedbo. Na skrbnikovo potrditev mora biti ISUD sposoben začeti odbirati in izločati, kot je podrobno navedeno pri zahtevi ETZ 3.3.1.10.

ETZ 3.3.2.8/a

ISUD mora podpirati orodja za poročanje in analizo za upravljanje hrambe in rokov hrambe prek skrbnika, vključno z možnostjo za:

- navedbo vseh rokov hrambe;
- navedbo vseh elektronskih zadev, ki jim je dodeljen določen rok hrambe;
- navedbo roka(ov) hrambe, ki se nanaša(jo) na vse zadeve na določeni točki hierarhije klasifikacijskega načrta;
- identificiranje, primerjanje in pregled rokov hrambe (vključno z njihovo vsebino) v klasifikacijskem načrtu;
- identificiranje formalnih protislovij pri rokih hrambe v klasifikacijskem načrtu.

ETZ 3.3.2.9

ISUD mora shraniti v revizijski sledi vse odločitve, ki jih je sprejel pregledovalec med pregledovanjem.

ETZ 3.3.2.10/a

ISUD mora ponujati ali podpirati možnost povezave s pripomočkom za delovni tok, za podporo načrtovanju, pregledovanju in postopku izvoza ali prenosa s sledenjem:

- stanja/poteka pregledovanja, kot npr. ali zadeva čaka ali je v postopku, podatki o pregledovalcu in datumu;
- dokumentom, ki kot rezultat odločitev ob pregledovanju čakajo na odbiranje in izločanje;
- nadaljevanju postopka prenosa.

ETZ 3.3.2.11/a

ISUD mora biti sposoben zbirati podatke o odločitvah pri pregledovanju za določeno časovno obdobje in zagotavljati tabelarna in grafična poročila o dejavnostih.

3.3.3 Prenos, izvoz in uničevanje

Organizacije lahko potrebujejo premestitev dokumentov iz njihovega ISUD-a na druge lokacije ali sisteme. To je tukaj omenjeno kot »prenos«. Izraz prenos se uporablja tudi, če je na drugo lokacijo ali sistem poslana samo kopija. Vzroki za prenos lahko obsegajo:

- stalno hrambo zapisov zaradi pravnih, upravnih ali raziskovalnih razlogov;
- uporabo zunanjih storitev za srednje- ali dolgoročno upravljanje dokumentov.

Posledica teh dejanj je pogosto ta, da so dokumenti preneseni v drugo okolje ISUD. Upoštevajte, da bodo v nekaterih primerih dokumenti, ki so bili izvorno v ISUD-u, po prenosu zbrisani iz njega, v drugih primerih pa ohranjeni.

V drugačnih okoliščinah bo morala organizacija izvoziti dokumente, tj. premakniti kopijo na drugo lokacijo ali v drug sistem, ob tem pa bo dokumente ohranila. V povsem drugačnih okoliščinah pa bo morala dokumente uničiti.

Prenos, izvoz ali uničenje je vedno treba izvesti na nadzorovan način. V vseh primerih je treba istočasno kot dokumente upoštevati tudi metapodatke in revizijsko sled, ki se nanašajo na te dokumente.

Upoštevajte, da se v tem kontekstu izraz »uničevanje« razlikuje od izraza »brisanje«.

ETZ 3.3.3.1

ISUD mora zagotoviti dobro voden proces za prenos dokumentov v drug sistem ali organizacijo.

ETZ 3.3.3.2

Kadarkoli ISUD prenaša razred ali zadevo, mora ta vsebovati:
- (za razrede): vse zadeve v razredu;
- (za zadeve): vse hierarhično razvrščene zadeve;
- vse dokumente v vseh teh zadevah;
- vse metapodatke, ki so povezani s temi zadevami in dokumenti.

ETZ 3.3.3.3

ISUD mora biti sposoben prenesti ali izvoziti zadevo ali razred z nepretrganim zaporedjem operacij, tako da:
- vsebina in struktura elektronskih dokumentov zadeve oz. razreda nista okrnjeni;

- se vse komponente elektronskega dokumenta (če dokument vsebuje več kot eno komponento) izvozijo kot celovita enota; npr. eno sporočilo po elektronski pošti z vsemi priponkami;
- ostanejo ohranjene vse povezave med dokumentom in njegovimi metapodatki;
- ostanejo ohranjene vse povezave med elektronskimi dokumenti in zadevami.

ETZ 3.3.3.4

Kadarkoli ISUD prenaša ali izvaža dokumente, mora biti sposoben vključiti kopijo vseh podatkov iz revizijske sledi, ki so povezani z dokumenti in zadevami, ki jih prenašamo.

ETZ 3.3.3.5/a

ISUD mora zagotavljati pripomoček ali orodje za pretvorbo in podporo pri prikazu dokumentov, označenih za prenos ali izvoz v določeno(e) odobreno(e) obliko(e) zapisa(e) prenosa.

ETZ 3.3.3.6

ISUD mora izdelati poročilo z razlago kakršnegakoli neuspeha med prenosom, izvozom ali brisanjem. Poročilo mora navesti vse dokumente, namenjene za prenos, ki so povzročili procesne napake, in vse dokumente, katerih prenos, izvoz ali brisanje ni bilo uspešno.

ETZ 3.3.3.7

ISUD mora ohraniti vse elektronske zadeve, ki so bile prenesene, vsaj dokler ni potrjeno, da je bil prenos uspešno izveden. To je predlagano kot proceduralna varovalka za zagotovitev, da dokumentov ne bomo zbrisali, dokler ne bo prejemnik sporočil, da je bil prenos uspešen.

ETZ 3.3.3.8/a

ISUD mora biti sposoben izvoziti celotni razred klasifikacijskega načrta z enkratnim zaporedjem operacij z zagotavljanjem, da se:

- ohrani relativni položaj vsake zadeve v klasifikacijskem načrtu, da je možno rekonstruirati strukturo zadeve;
- ohranijo vsi metapodatki na višjih ravneh v hierarhiji in se premikajo skupaj z razredom.

ETZ 3.3.3.9/a

Če je treba prenesti, izvoziti ali uničiti kombinirane zadeve, mora ISUD zahtevati, da skrbnik potrdi, da je bil papirni del zadeve prenesen, izvožen ali zbrisan pred prenosom, izvozom ali brisanjem elektronskega dela.

ETZ 3.3.3.10/a

ISUD mora omogočati elektronskim zadevam, ki so izbrane za prenos, dodati elemente metapodatkov, ki jih določi uporabnik in so zahtevani za arhivsko upravljanje.

ETZ 3.3.3.11/a

ISUD mora omogočati razvrščanje elektronskih zadev, izbranih za prenos, v urejene sezname glede na elemente podatkov, ki jih izbere uporabnik.

ETZ 3.3.3.12/a

ISUD mora za opis elektronskih zadev, ki se izvažajo ali prenašajo, omogočati izdelavo obrazcev, kakršne določi uporabnik.

ETZ 3.3.3.13/a

ISUD mora omogočati popolno uničenje razredov in posameznih zadev, ki so shranjene na nosilcih zapisa za večkratno zapisovanje, tako da z uporabo specialnih pripomočkov za obnavljanje podatkov ponovna obnova ni več mogoča. V nekaterih okoljih to lahko zahteva večkratno prepisovanje podatkov glede na določene standarde.

Kjer je zahtevana zagotovitev uničenja, se lahko zgodi, da je potrebno upoštevati kopije na nosilcih za varnostne kopije.

ETZ 3.3.3.14

Če so dokumenti shranjeni na nosilcu zapisa za enkratno zapisovanje, mora ISUD zagotavljati pripomočke za preprečitev dostopa do njih, tako da ne morejo biti obnovljeni z normalno uporabo ISUD-a ali s standardnimi sistemskimi pripomočki. To navadno pomeni uničenje indeksnih podatkov (ki so shranjeni na nosilcih za večkratno zapisovanje), ki hranijo lokacije podatkov na nosilcih za enkratno zapisovanje.

Če je zahtevana zagotovitev uničenja, je potrebno upoštevati obstoj kopij na nosilcih za varnostne kopije.

ETZ 3.3.3.15

ISUD mora imeti možnost ohraniti metapodatke za zadeve in dokumente, ki so bili uničeni ali preneseni. V nekaterih okoljih je zaželeno ohraniti podrobne informacije o uničenih dokumentih. Prav tako lahko dovoljuje enostavno identifikacijo uničenih ali prenesenih dokumentov. To je tesno povezano z zahtevo ETZ 3.3.3.16.

ETZ 3.3.3.16

ISUD mora dovoliti skrbniku za tiste zadeve, ki jih bomo uničili, prenesli ali umaknili iz neposrednega dostopa, natančno določiti podmnožico metapodatkov, ki jih bomo ohranili. To je zaželeno zato, da lahko organizacija še vedno ve, katere dokumente je hranila, in pozna datume, ko so bili odbrani ali izločeni in uničeni, ne da bi si nujno naprtila režijske stroške za hrambo vseh metapodatkov te zadeve.

ETZ 3.3.3.17

ISUD mora dovoliti prenos ali izvoz dokumentov več kot enkrat.

3.4 ZAJEM IN PRETVORBA GRADIVA

V to poglavje so vključene zahteve, ki se nanašajo na vključevanje gradiva v sistem (ISUD). Vključevanje gradiva je lahko izvedeno na različne načine (običajni postopek

zajema, masovni uvoz gradiva), med postopkom pa je potrebno prepoznati tudi potrebe po pretvorbi in hrambi gradiva v različnih oblikah zapisa (formatih) in posebnosti pri evidentiranju in sledenju elektronske pošte.

3.4.1 Zajem in pretvorba gradiva

Pojem »zajem« uporabljamo tako, da obsega postopke evidentiranja dokumenta z odločitvami, v kateri razred bo razvrščen, z dodajanjem še drugih metapodatkov in shranitvijo v ISUD. V kontekstu ISUD-a so evidentiranje in drugi postopki lahko ločeni ali povezani.

Elektronski zapisi, ustvarjeni ali prejeti med poslovnimi procesi, izhajajo tako iz notranjih kot zunanjih virov. Elektronski zapisi so lahko v različnih oblikah zapisa, ustvarjajo pa jih lahko različni avtorji. Lahko jih prejmemo kot posamezne zapise ali kot zadeve z več zapisi. Prispejo lahko po različnih komunikacijskih kanalih, npr. po lokalni mreži (LAN), prostranih omrežjih (WAN), z elektronsko pošto, s faksimilnim sporočilom, s pošto (pismo, ki se skenira) ter z razlikami v pogostosti prispetja in obsega. Da bi zapise zajemali in imeli hkrati dober nadzor upravljanja, je potreben prilagodljiv sistem vnosa, da lahko zadostimo tako raznolikim zahtevam.

Pri zajemu gradiva, ki je izvirno nastalo v fizični obliki ali v elektronski, vendar ne v elektronski obliki, je potrebno poskrbeti, da se zajeto gradivo pri tem postopku zanesljivo pretvori v elektronsko obliko, pri čemer je potrebno poskrbeti, da se ohranijo vse značilnosti izvirne oblike gradiva.

Postopek zajema gradiva mora izpolnjevati temeljne zahteve ZVDAGA. Temeljno načelo ohranjanja dokumentarnega gradiva oziroma ohranjanja njegove vsebine je vsebovano v 3. členu zakona, po katerem je hramba dokumentarnega gradiva definirana tako, da pomeni *»ohranjanje izvirnega dokumentarnega gradiva ali uporabnosti vsebine tega gradiva«*. Če naj bo hramba zajetega gradiva enakovredna hrambi izvirnega gradiva, mora zajeto gradivo zagotavljati in ohranjevati vse učinke izvirnega gradiva.

ETZ 3.4.1.1

ISUD-ov proces zajema dokumenta mora zagotavljati kontrole in funkcionalnosti, ki:

- evidentirajo in upravljajo vse elektronske dokumente ne glede na metodo kodiranja in druge tehnološke značilnosti;
- zagotavljajo, da so dokumenti povezani s klasifikacijskim načrtom ter z eno ali več zadevami;
- povezujejo z aplikacijo, s katero se dokumenti ustvarjajo;
- preverjajo in nadzirajo vnos metapodatkov v ISUD.

ETZ 3.4.1.2

ISUD mora biti sposoben v okolje upravljanja elektronskih dokumentov vključiti:

- vsebino elektronskega dokumenta, vključno s podatki, ki definirajo njegovo obliko in prikaz, ter podatke, ki definirajo strukturo in obnašanje elektronskega dokumenta ob ohranjanju celovitosti njegove strukture (npr. vse komponente sporočila elektronske pošte s prilogami oz. spletne strani s povezavami);
- informacije o elektronskem zapisu, na primer ime zadeve;
- datum nastanka in druge metapodatke zapisa o elementih dokumenta;

- informacije o kontekstu, iz katerega izvira elektronski dokument, v katerem je nastal in bil objavljen, na primer o poslovnem procesu in tvorcu(cih) oz. avtorju(jih);
- podatke o aplikaciji, v kateri je bil dokument ustvarjen, vključno s podatki o njegovi različici.

ETZ 3.4.1.3

ISUD mora pri zajemu dopuščati pridobitev vseh metapodatkovnih elementov, določenih pri konfiguraciji sistemov in jih trajno ohraniti v tesni povezavi z elektronskim dokumentom.

ETZ 3.4.1.4

ISUD mora zagotavljati, da lahko vsebino izbranih elementov metapodatkov elektronskega dokumenta spremenijo samo pooblaščeni uporabniki in skrbniki.

ETZ 3.4.1.5/a

ISUD mora podpirati sposobnost, da isti elektronski dokument dodelimo različnim elektronskim zadevam iz enega elektronskega zapisa, ne da bi elektronski dokument fizično podvajali.

Na primer, račun lahko en uporabnik dodeli zadevi dobavitelja, drugi pa zadevi proizvoda. V drugem primeru se lahko nek uporabnik odloči, da zapis, ki se nanaša na dve zadevi, doda obema odgovarjajočima zadevama. To navadno dosežemo z uporabo kazalcev.

ETZ 3.4.1.6

ISUD mora podpirati samodejno pomoč pri evidentiranju elektronskih zapisov z samodejnim prevzemanjem metapodatkov za vsaj te zvrsti zapisov:

- pisarniške zapise (npr. dopisi v običajni obliki zapisa, narejeni z urejevalnikom besedil);
- prejeta in odposlana sporočila elektronske pošte brez prilog;
- prejeta in odposlana sporočila elektronske pošte s prilogami;
- prejeta in odposlana faksimilna sporočila.

ETZ 3.4.1.7

ISUD mora zabeležiti datum in čas evidentiranja kot metapodatek. Če sta datum in čas del enoličnega identifikatorja in dokler ju lahko eksplicitno razberemo iz te številke, datuma in časa ni potrebno hraniti ločeno. Časovna natančnost bo odvisna od aplikacije.

ETZ 3.4.1.8

ISUD mora zagotavljati, da ima vsak evidentiran dokument pregleden evidenčni vnos, vključno z metapodatki, ki sledijo in so določeni v času konfiguriranja. Nekateri od zahtevanih metepodatkov so lahko že vpisani v sistem ali pa se jih lahko samodejno povzema iz dokumenta. ISUD mora zahtevati vnos preostalih metapodatkov.

ETZ 3.4.1.9

ISUD mora dovoliti vnos dodatnih opisnih in preostalih metapodatkov:

- ob času evidentiranja, in/ali
- na poznejši stopnji obdelave.

ETZ 3.4.1.10

Ko ima zapis več kot eno različico, mora ISUD dovoliti porabniku, da izbere vsaj eno od naštetega:
- evidentirati vse različice zapisa kot en dokument;
- evidentirati eno različico zapisa kot dokument;
- evidentirati vsako različico zapisa kot dokument.

ETZ 3.4.1.11/a

ISUD mora zagotoviti samodejno podporo za odločitve o klasificiranju elektronskih dokumentov v elektronske zadeve, z nekaterimi ali vsemi temi sredstvi:
- omogočanje dostopa posameznemu uporabniku ali vlogi le do podskupine klasifikacijskega načrta;
- shranjevanje seznama nazadnje uporabljenih zadev za vsakega uporabnika ali vlogo;
- predlaganje zadev, ki jih je uporabnik uporabljal nazadnje;
- predlaganje zadev, ki vsebujejo povezane elektronske dokumente;
- predlaganje zadev na osnovi povzemanja iz metapodatkovnih elementov dokumenta: npr. pomembne besede, ki so uporabljene v naslovu zapisa;
- predlaganje zadev na osnovi povzemanja iz vsebin dokumenta.

ETZ 3.4.1.12/a

Zaradi kompletiranja procesa zajema mora ISUD uporabniku omogočiti, da posreduje elektronske dokumente drugemu uporabniku.

ETZ 3.4.1.13

Če so elektronski dokumenti sestavljeni iz več kot enega dela, mora ISUD:

- ravnati z dokumentom kot z enim nedeljivim dokumentom ob ohranjanju povezave s sestavnimi deli;
- ohraniti celovitost strukture dokumenta;
- podpirati kasnejše integrirano iskanje, prikaz in upravljanje;
- upravljati odbiranje in izločanje vseh komponent elektronskega dokumenta kot celote (tj. v eni operaciji).

Primeri takih dokumentov so spletne strani z vstavljenimi grafikami.

ETZ 3.4.1.14

ISUD mora podpirati samodejno pomoč pri evidentiranju elektronskih zapisov z samodejnim povzemanjem čim večjega števila metapodatkov za čim več vrst zapisov. Osnovno načelo te zahteve je zmanjšati količino vnosa podatkov, ki ga izvaja uporabnik in povečati natančnost metapodatkov. Od okolja bo odvisno, koliko elementov metapodatkov bo v to vključenih ter za katere vrste zapisov je to izvedljivo. Na primer: v pisarni, v kateri delajo z nestrukturiranimi in polstrukturiranimi tekstovnimi zapisi, bi bilo smiselno vključiti:

- dopise, zaznamke (memorandume) in druge zapise, ki nastanejo z urejevalnikom besedil z uporabo standardiziranih vzorcev (vnaprej pripravljenih obrazcev), oblikovanih za določeno organizacijo, to omogoča samodejno identifikacijo metapodatkovnih elementov;
- vhodno in izhodno elektronsko pošto s prilogami ali brez njih;
- izhodna faksimilna sporočila.

ETZ 3.4.1.15

ISUD mora opozoriti, če poskuša uporabnik evidentirati zapis, ki je že bil evidentiran v isti zadevi.

ETZ 3.4.1.16

Sistem ISUD mora podpirati zanesljivo pretvorbo gradiva v fizični obliki ali elektronski obliki, ki ni digitalna oblika (npr. analogni magnetni nosilci, itd.) v digitalno obliko.

ETZ 3.4.1.17/a (dolgoročna hramba)

Sistem ISUD mora podpirati zanesljivo pretvorbo gradiva v fizični obliki ali elektronski obliki, ki ni digitalna oblika (npr. analogni magnetni nosilci zapisa, itd.) v digitalno obliko, ki je primerna za dolgoročno hrambo. Za izpolnjevanje te zahteve mora sistem podpirati predvsem:

- elektronski podpis in ponovni elektronski podpis posamezne zajete enote gradiva;
- elektronski podpis in ponovni elektronski podpis posameznih skupin enot zajetega gradiva;
- elektronski podpis in ponovni elektronski podpis celotnega zajetega gradiva.

3.4.2 Masovni uvoz gradiva

Dokumente lahko masovno vključimo v ISUD na različne načine. Na primer iz drugega ISUD-a kot elektronsko zadevo, sestavljeno iz večjega števila istovrstnih dokumentov (npr. dnevne račune) ali kot masovni prenos iz ISUZ-a. ISUD jih mora biti sposoben sprejeti in mora biti zmožen upravljati proces zajema.

ETZ 3.4.2.1

ISUD mora zagotoviti sposobnost za zajemanje transakcijskih zapisov, ki nastajajo v drugih sistemih. To mora zajemati:

- podporo vnaprej definiranih uvozov transakcijskih paketov;
- zagotavljanje pravil za prilagajanje samodejnega evidentiranja zadev;
- vzdrževanje celovitosti podatkov.

ETZ 3.4.2.2

Sitem ISUD mora zagotavljati mehanizme za upravljanje vhodnih nizov.

ETZ 3.4.2.3/a

ISUD mora biti sposoben vzpostaviti več sočasnih vhodnih nizov za različne vrste zapisov.

ETZ 3.4.2.4/a

Sistem ISUD mora podpirati masovni uvoz gradiva, ki je bilo izvoženo iz drugih sistemov za upravljanje z dokumenti ali zapisi, predvsem pa masovno zajemanje:

- elektronskih zapisov v njihovi izvirni obliki zapisa, brez da bi se pri tem spremenila njihova vsebina ali struktura, ohraniti pa se morajo povezave med različnimi deli posameznega dokumenta;
- elektronskih zapisov s pripadajočimi metapodatki, brez da bi se pri tem izgubile povezave in razmerja med posameznimi dokumenti in metapodatki;
- celotne strukture elektronskih zadev, s katerimi so povezani posamezni zapisi, ter vseh povezanih metapodatkov, pri čemer morajo biti ohranjene povezave med posameznimi dokumenti ter zadevami.

ETZ 3.4.2.5/a

Sistem ISUD mora podpirati direkten masovni uvoz elektronskih zapisov v njihovi izvirni obliki zapisa, povezanih z metapodatki, ki so zapisani v vnaprej določeni strukturirani obliki (npr. XML) ali v nestandardni obliki.

ETZ 3.4.2.6/a

Sistem ISUD mora podpirati uvoz revizijskih podatkov, ki so neposredno povezani z dokumentom ali zadevo.

3.4.3 Vrste zapisov

Pri zajemu gradiva v sistem ISUD je potrebno upoštevati različne vrste zapisov, v katerih se gradivo v elektronski obliki lahko pojavlja, saj lahko takšne raznolikosti v postopku zajema pripeljejo do napak, ki lahko odločilno vplivajo na enakost vsebine izvirnega in zajetega gradiva.

Organizacije bodo morale zajemati širok spekter raznih vrst zapisov različnih oblik in struktur. Tehnične zahteve za zajem se bodo spreminjale glede na kompleksnost zapisov. V nekaterih okoljih ni mogoče vnaprej identificirati vseh vrst zapisov, ker nekatere prejemamo od zunanjih virov.

Občasno se pojavlja zahteva po zajemu zapisov, za katere se zdi, da se sami spreminjajo ali so dejansko »samospreminjajoči se«. Posledica so lahko kompleksne zahteve, ki jih tukaj preučujemo v bistvenih potezah, ne pa natančno.

Zdi se, da se nekateri zapisi sami spreminjajo, tj. spreminjajo svojo vsebino brez posredovanja uporabnika. Splošen primer so zapisi, oblikovani z urejevalnikom besedil ali preglednic, ki vsebujejo polje ali kodo, ki samodejno prikazuje tekoči datum. Prikaz zapisa se spreminja v skladu z datumom, ko je prikazan. V skrajnih primerih se lahko polje ali koda spreminja v takšni meri, da radikalno spremeni videz zapisa (na primer koda, ki prikazuje celotno drevo direktorija zapisov: v nekaterih primerih spremembe na poti zaradi dolgega imena poti v velikem hierarhčnem ISUD-u lahko povzročijo večje spremembe številčenja). Kljub temu pa zapis ni resnično spremenjen, spremeni se samo njegov prikaz, in to v skladu s programsko opremo, ki jo uporabljamo za njegovo

pregledovanje. Čeprav takšni zapisi, ki se na videz spreminjajo, niso v nasprotju z zahtevo, da morajo biti vsebine dokumenta nespremenljive, pa je lahko videti, kot da so. Zato se jim je dobro izogibati.

V drugih primerih lahko zapisi vsebujejo kodo, ki resnično spreminja zapis, kot so preglednice s sofisticiranim »makro programom«, ki spremeni preglednico (z uporabo iste aplikacije za njegovo pregledovanje) in jo potem samodejno shrani. V takih primerih obstaja nevarnost, da se bo zapis sam spremenil med postopkom zajema, odvisno od podrobnosti procesa in kontrol ISUD-a. To je povsem nesprejemljivo.

Večinoma naj bi se izogibali zapisov, ki se na tak način sami spreminjajo. Hranili naj bi jih v obliki zapisa, ki onesposobi kodo za »samospreminjanje« oziroma pregledovali naj bi jih samo s programsko opremo, ki ne povzroča sprememb. Če je »samospreminjajoča se« koda poglavitni del dokumenta, se je treba odločiti za primerne korake za vsak primer posebej.

ETZ 3.4.3.1

ISUD mora biti sposoben kot dokumente zajeti zapise iz širokega spektra različnih vrst oblik zapisa in struktur elektronskih zapisov.

ETZ 3.4.3.2

Sistem ISUD mora omogočati zajem dokumentarnega gradiva v njegovi izvirni obliki.

ETZ 3.4.3.3/a

Sistem ISUD mora pri zajemu zapisa v izvirni obliki zapisa podpirati tudi pretvorbo zapisa v standardne oblike zapisa in shranjevanje obeh oblik zapisa tako, da sta medsebojno povezana.

ETZ 3.4.3.4

ISUD mora podpirati zajem najsplošnejše uporabljenih pisarniških zapisov. To vključuje enostavne in kompleksne vrste zapisov. Vrste podpiranih oblik zapisa morajo obsegati:

- enostavne: faksimilna sporočila, pisarniške zapise, predstavitve, besedila, slike, sporočila elektronske pošte, zvok;
- sestavljene: elektronska sporočila s prilogami, namizno založništvo, spletne strani, grafike.

ETZ 3.4.3.5

Oblike zapisov, ki podpirajo zahtevo ETZ 3.4.3.2, morajo biti razširljive, tako, da jim je mogoče dodajati nove oblike zapisa.

ETZ 3.4.3.6/a

ISUD mora biti sposoben zajeti te vrste zapisov:

- elektronske koledarje;
- informacije iz drugih računalniških aplikacij, npr. računovodstvo, plačilne liste, računalniško podprto oblikovanje (CAD);

- skenirane zapise v papirni obliki;
- zvočne datoteke;
- video izseke;
- digitalne sheme in zemljevide;
- strukturirane podatke (npr. transakcije z računalniško izmenjavo podatkov – EDI);
- podatkovne baze;
- multimedijske zapise.

ETZ 3.4.3.7

ISUD ne sme vsiljevati nobene praktične omejitve za število dokumentov, ki so lahko zajeti v določeni zadevi ali za število dokumentov, ki se lahko shranijo v ISUD-u.

ETZ 3.4.3.8/a

ISUD mora omogočati, da je sestavljeni zapis zajet na katerega od teh načinov:

- kot posamezen sestavljeni dokument;
- kot serija povezanih enostavnih dokumentov po eden na komponento sestavljenega zapisa.

ETZ 3.4.3.9/a

Pri zajemu sestavljenih zapisov mora sistem ISUD omogočati:

- zajem in označevanje zapisa na tak način, da se ohrani povezave med različnimi deli sestavljenega zapisa;
- ohranitev strukturne integritete zapisa;
- podporo kasnejšega prikaza, upravljanje s sestavljenim zapisom ali dostopa do tega zapisa tako, da zapis obravnava kot celovit del;
- razpolaganje z zapisom kot s celotno enoto, za kar naj potrebuje le eno delovno operacijo.

3.4.4 Upravljanje elektronske pošte

Pri zajemu gradiva v elektronski obliki ima posebno mesto zajem sporočil elektronske pošte, saj ta zaradi svoje specifične oblike in načina prejemanja in pošiljanja lahko prinaša težave pri sledenju in evidentiranju.

ETZ 3.4.4.1

ISUD mora omogočati, da pri konfiguriranju izberemo enega izmed teh načinov delovanja:

- ISUD dopušča uporabnikom zajem elektronskih sporočil (tj. po morebitnem izboru sporočila se izvede njegovo evidentiranje), ali
- ISUD ponuja avtomatiziran postopek zajema vseh vhodnih in izhodnih sporočil elektronske pošte.

ETZ 3.4.4.2/a

ISUD mora omogočati uporabniku, da pri zajemu elektronskega sporočila izbere zajem:

- samo elektronskega sporočila;

- elektronsko sporočilo s priponkami;
- samo priponke;
- kakršnokoli zaporedje zgornjih kombinacij.

ETZ 3.4.4.3/a

ISUD mora omogočati individualnim uporabnikom obdelavo in zajem prejetih sporočil elektronske pošte iz njihovega sistema elektronske pošte. Uporabnik naj bi bil sposoben obdelati vsako sporočilo v svojem poštnem nabiralniku znotraj njihovega sistema elektronske pošte po tem postopku:

- pregledati vsako sporočilo in oznake za njegove priloge (če jih ima);
- pregledati vsebine prilog z uporabo pregledovalnika zapisov, ki podpira različne oblike zapisa;
- evidentirati sporočilo in njegove priloge kot nov dokument v ISUD-u;
- povezati sporočilo in njegove priloge z obstoječim dokumentom v ISUD-u.

ETZ 3.4.4.4/a

ISUD mora zagotavljati zajem elektronskega naslova iz sporočila elektronske pošte v berljivi obliki, kadar je ta povezan z izvornim sporočilom. Na primer: Jan Novak, ne pa 'jsa97@xyz.int'.

3.5 OZNAČEVANJE

Razne entitete ISUD-a (razredi, zadeve, dokumenti) potrebujejo identifikatorje. Ti identifikatorji morajo biti enolični za vsak pojav katerekoli entitete. Enoličnost se mora nanašati na celotni ISUD ali na ustrezno raven v hierarhiji. Ker so zahteve za označevanje skupne, so tukaj skupno predstavljene za razrede, zadeve in dokumente.

ETZ 3.5.1.1

Kadarkoli se v ISUD-u na novo pojavi katerakoli od naštetih kategorij, ji mora ISUD prirediti enolični identifikator (kot je določeno spodaj):

- zadeva;
- dokument;
- izvleček dokumenta.

ETZ 3.5.1.2

Vsi enolični identifikatorji ISUD-a morajo biti:

- enolični znotraj ISUD-a, ali
- enolični znotraj višje ravni ustrezne veje v hierarhiji, znotraj katere se pojavljajo.

Kot primer druge opcije je pot Pogodbe: ime podjetja: korespondenca enolična, vendar se lahko njen zadnji segment ponavlja tudi v kaki drugi poti, npr. Regionalni razvojni načrt: javna razprava: korespondenca

ETZ 3.5.1.3

ISUD mora biti sposoben shraniti enolične identifikatorje kot metapodatkovne elemente entitet, na katere se nanašajo.

ETZ 3.5.1.4

ISUD mora pri konfiguriranju dopustiti določiti format enoličnega identifikatorja. Identifikator je lahko številčen ali alfanumeričen ali pa lahko vključuje verigo identifikatorjev mape in elektronske zadeve nad ravnjo dokumenta v klasifikacijskem načrtu.

ETZ 3.5.1.5

ISUD mora:

- samodejno kreirati enolične identifikatorje in preprečiti, da bi jih uporabniki ročno vnašali ter jih naknadno spreminjali (na primer zaporedno številko), ali
- dopustiti uporabniku vnos enoličnega identifikatorja, vendar še pred sprejemom tudi preveriti, ali je res enoličen (na primer številka računa).

Možno je tudi avtomatsko kreiranje enoličnega identifikatorja, ki je uporabniku skrit, dopušča pa mu vnašanje neenoličnih znakovnih nizov (npr. priimek) za identifikatorje. Uporabnik bo uporabljal ta znakovni zapis kot identifikator, ISUD pa ga bo imel za metapodatek, ki ga je vnesel in ga lahko preiskuje uporabnik.

ETZ 3.5.1.6

Ko ISUD avtomatsko oblikuje enolične identifikatorje, mora skrbniku dopustiti, da pri konfiguraciji določi začetno število (npr. 0, 00, 100) in prirastek (npr. 1, 10); ta se nato uporablja v vseh primerih.

3.6 ISKANJE, PRIKLIC IN PRIKAZOVANJE

Integralni del ISUD-a je sposobnost, da uporabnik lahko prikliče zadeve in dokumente. To obsega njihovo iskanje, kadar ne poznamo podrobnosti ter njihovo prikazovanje. Prikazovanje je produciranje predstavitve na zaslonu (prikaz) ali izpisovanje (tiskanje). Lahko pa s tem pojmom razumemo tudi izvajanje avdio- in video vsebin.

Dostopanje k zadevam in dokumentom ter zatem njihovo pregledovanje bo zahtevalo prilagodljiv in širok spekter funkcij iskanja, priklica in prikazovanja, da bi zadostili zahtevam različnih vrst uporabnikov. Četudi lahko razumemo, da to ni klasična funkcija poslovanja z dokumentarnim gradivom, pa tukajšnji opis zahtevane funkcionalnosti temelji na tem, da ima ISUD brez dobrega pripomočka za preiskovanje in priklic omejeno vrednost.

Zakon posameznih določil o tej vrsti funkcionalnosti ne vsebuje, zagotovo pa potrebo po takšnih funkcionalnostih lahko najdemo že v načelu dostopnost, po katerem mora biti vse

gradivo dostopno uporabnikom (6. člen). V primeru hrambe gradiva v elektronski obliki bi o dostopnosti težko govorili, če sistem za elektronsko hrambo ne bi omogočal nekaterih možnosti za iskanje, priklic in prikazovanje različnih elementov in delov gradiva.

Vse značilnosti in funkcionalnosti, opisane v tem poglavju, morajo biti podrejene nadzoru dostopa; to je opisano na drugem mestu v teh tehnoloških zahtevah, vključno z varnostnimi kontrolami. Z drugimi besedami: ISUD nikoli ne sme uporabniku prikazati informacij, ki jih ni upravičen sprejeti. Zaradi poenostavitve je to predvideno povsod in tega ne ponavljamo pri vsaki podrobni zahtevi.

3.6.1 Iskanje in priklic

Iskanje je proces identifikacije dokumentov ali zadev z uporabniško določljivimi parametri, katerega namen so potrditev, lociranje, dostopanje in priklic dokumentov, zadev in/ali metapodatkov. Iskalna in navigacijska orodja ISUD-a za lociranje metapodatkov, dokumentov ali zadev zahtevajo številne preiskovalne tehnike, namenjene zahtevnemu uporabniku »preiskovalcu« in za podporo občasnemu in manj »računalniško pismenemu« operaterju.

ETZ 3.6.1.1

ISUD mora zagotavljati prilagodljiv niz funkcij, ki se izvajajo tako na metapodatkih, povezanih z vsako ravnjo združevanja dokumentov (zadeva, klasifikacijska skupina), kot na vsebinah dokumentov prek uporabniško določenih parametrov z namenom lociranja, dostopanja in priklica dokumentov in/ali metapodatkov, in to bodisi posameznih ali združenih.

ETZ 3.6.1.2/a

V primeru zadev mora ISUD omogočati enako funkcionalnost iskalnih orodij za elektronske, kombinirane in fizične zadeve.

ETZ 3.6.1.3

ISUD mora omogočati preiskovanje metapodatkov vseh dokumentov in zadev.

ETZ 3.6.1.4

ISUD mora omogočati preiskovanje tekstovnega dela dokumentov.

ETZ 3.6.1.5

ISUD mora uporabniku omogočati oblikovanje posameznih zahtev za iskanje s kombiniranjem metapodatkov in/ali vsebine dokumenta.

ETZ 3.6.1.6

ISUD mora skrbnikom omogočati konfiguriranje in spremembo iskalnih polj vključno z:

- navedbo kateregakoli metapodatkovnega elementa dokumenta ali zadeve ter po potrebi tudi celotne vsebine dokumenta kot iskalnega polja;
- spremembo konfiguracije iskalnega polja.

ETZ 3.6.1.7

ISUD mora zagotoviti iskalna orodja, ki obsegajo te tehnike:

- prosto iskanje po besedilu s kombinacijami metapodatkovnih elementov dokumenta in zadeve, pa tudi vsebine dokumenta;
- Booleovo iskanje metapodatkovnih elementov.

ETZ 3.6.1.8/a

ISUD mora zagotoviti prosto iskanje po besedilu in metapodatkih na integriran in dosleden način.

ETZ 3.6.1.9/a

ISUD mora omogočati koncept iskanja z uporabo tezavra, vključenega kot indeks z neposrednim dostopom (on-line). Tako bo mogoče najti zapise, ki imajo v vsebini ali metapodatkih širši, ožji ali povezan pojem. Na primer iskanje okulističnih storitev bi lahko našlo zdravstvene storitve, očesni pregled ali okulistiko.

ETZ 3.6.1.10

ISUD mora zagotoviti preiskovanje metapodatkov z znaki zamenjave, ki omogočajo razširitev na začetku, koncu ali na sredini. Na primer, preiskovanje besede proj* bi lahko našlo projekt ali proja; beseda K*a pa bi našla besedo Komisija.

ETZ 3.6.1.11/a

ISUD mora zagotoviti iskanje sorodnih besed na tak način, da se mora neka beseda pojaviti znotraj danega intervala druge besede v dokumentu in ga opredelil kot zadetek.

ETZ 3.6.1.12

Če uporabljamo grafični uporabniški vmesnik, mora ISUD zagotoviti tak mehanizem pregledovanja, ki zagotovi grafično ali neko drugo pregledovalno-prikazovalno tehniko na obeh ravneh, razredu in zadevi. To bi uporabljali skupaj z opisanimi preiskovalnimi tehnikami, da bi zagotovili pregled prve ravni metapodatkov za skupino dokumentov ali zadev, ki so ustrezali določenim iskalnim kriterijem.

ETZ 3.6.1.13

ISUD mora omogočati preiskovanje znotraj posamezne elektronske zadeve (na katerikoli ravni hierarhije klasifikacijskega načrta) ali po več zadevah.

ETZ 3.6.1.14

ISUD mora biti sposoben preiskati in najti celotne elektronske zadeve s popolno vsebino in metapodatki o kontekstu ter mora prikazati vse te in samo te vnose v kontekstu te zadeve kot ločeno skupino, in sicer v enem samem postopku priklica. To je potrebno, na primer, kadar želi uporabnik izpisati celotno zadevo, da jo vzame s sabo na sestanek, si začasno olajša delo s papirji ali pa zaradi kakega drugega razloga.

ETZ 3.6.1.15

ISUD mora biti sposoben iskati, najti in prikazati elektronsko zadevo z vsemi privzetimi načeli imenovanja, vključno z:

- nazivom zadeve;
- identifikatorjem zadeve (klasifikacijski znak).

ETZ 3.6.1.16

ISUD mora na uporabnikovem zaslonu prikazati skupno število rezultatov iskanja in mu omogočiti prikaz rezultatov iskanja (»seznam zadetkov«) ali pa mu omogočiti dopolnitev iskalnih kriterijev ter vnosa drugega zahtevka.

ETZ 3.6.1.17

ISUD mora omogočati izbor dokumentov, zadev itd., navedenih med rezultati iskanja, in nato (v skladu z nadzorom dostopa) njihovo odprtje z enim samim pritiskom na tipko miške ali tipkovnice.

ETZ 3.6.1.18/a

ISUD mora omogočati preiskovanje metapodatkov kateregakoli objekta (kot so dokument, zadeva ali razred) z uporabo tehnik, opisanih v tem poglavju, ne glede na to, ali je sam objekt v elektronski obliki ali ne in neodvisno od tega ali je shranjen z neposrednim ali posrednim mrežnim dostopom ali brez njega (on-line, near-line ali off-line).

ETZ 3.6.1.19/a

ISUD mora uporabnikom omogočati shraniti in ponovno uporabiti poizvedbe.

ETZ 3.6.1.20

ISUD mora uporabnikom omogočati dopolniti (tj. zožiti) iskanja. Uporabnik, bi na primer, lahko začel iskanje s seznama zadetkov, nato pa naj bi imel možnost znotraj tega seznama sprožiti nadaljnje iskanje.

ETZ 3.6.1.21/a

ISUD mora v iskalnih zahtevkih omogočati uporabo z besedo opisanih časovnih intervalov, na primer »prejšnji teden«, »ta mesec«. To pa se razlikuje od specifikacije intervalov s koledarskimi dnevi ali številom dni.

ETZ 3.6.1.22

ISUD mora uporabnikom omogočati poiskati zadeve in dokumente neposredno prek enoličnega identifikatorja. Če enolični identifikator uporabniku ni dostopen, to ni pomembno.

ETZ 3.6.1.23

ISUD mora zagotoviti oblike prikaza rezultatov iskanja, ki jih lahko oblikujejo uporabniki ali skrbniki, vključno s takimi značilnostmi in funkcijami, kot so:

- izbira ureditve, v kateri so rezultati iskanja predstavljeni;
- določitev števila hkrati prikazanih rezultatov iskanja na zaslonu;
- določitev maksimalnega števila prikazanih rezultatov za posamezno iskanje;

- shranitev rezultatov iskanja;
- izbira metapodatkovnih polj, ki se prikažejo na seznamu rezultatov iskanja.

ETZ 3.6.1.24/a

ISUD mora omogočati razvrščanje rezultatov iskanja po pomembnosti.

ETZ 3.6.1.25/a

ISUD mora biti sposoben povezati 'izvleček' elektronskega dokumenta (glejte podpoglavje 3.7.3) z izvornim dokumentom tako, da bi najdba enega omogočila najdbo drugega, pri tem pa za oba ohraniti ločene metapodatke in nadzor nad dostopom.

ETZ 3.6.1.26/a

Pri pregledovanju ali delu z dokumentom ali skupino dokumentov (na primer zadevo ali razredom), ne glede na to, ali gre za rezultat iskanja ali ne, mora biti uporabniku omogočeno uporabljati sposobnost ISUD-a, da najde podatke o naslednji višji ravni združevanja dokumentov, in to na lahek način in ne da bi bilo treba zapustiti ali zapreti dokument. Ko uporabnik na primer bere dokument, naj bi imel možnost ugotoviti, v kateri zadevi in zadevi je ta dokument. Če pregleduje metapodatke zadeve, mora biti uporabniku omogočeno ugotoviti, v katerem razredu se le-ta nahaja.

ETZ 3.6.1.27

Nobena funkcija iskanja ali priklica v ISUD-u ne sme uporabniku odkriti podatkov (metapodatkov ali vsebine dokumenta), ki mu jih želimo s kontrolami dostopa in varnosti prikriti.

ETZ 3.6.1.28/a

ISUD mora vključevati možnost za nadzor dostopa do dokumentov upoštevaje omejitve, vezane na intelektualno lastnino in tudi možnost za oblikovanje potrebnih podatkov v zvezi s stroški za tovrstni dostop. Ta kratka izjava obsega širok spekter funkcionalnosti, ki presega namen te specifikacije. To zahtevo lahko izpolnimo na ta način, da omogočimo povezavo z ločenim aplikacijskim sistemom.

3.6.2 Prikazovanje

Prikaz na zaslonu

ISUD lahko vsebuje dokumente različnih oblik zapisa in struktur. Uporabnik potrebuje splošna orodja za pregledovanje, ki olajšajo prikaz na zaslonu, predstavitev in izpis niza oblik zapisa.

ETZ 3.6.2.1

ISUD mora prikazati dokumente, ki jih je našel z iskanjem. Če ISUD hrani dokumente v lastniškem aplikacijskem obliki zapisa, je lahko sprejemljivo prikazovanje s pomočjo aplikacije zunaj ISUD-a.

ETZ 3.6.2.2/a

ISUD mora prikazati rezultate iskanje, ki jih je našel z iskanjem, brez zagona povezane aplikacije. To navadno zagotovimo z integriranjem programskega paketa za pregledovanje v ISUD-u. To je pogosto zaželeno zaradi povečanja hitrosti prikazovanja.

ETZ 3.6.2.3/a

ISUD mora biti sposoben prikazati vse vrste elektronskih dokumentov, ki jih določi organizacija na tak način, da se ohranijo podatki o dokumentih (npr. vse značilnosti vizualne predstavitve in izgleda, ki ga izvede aplikacijski paket, v katerem je dokument ustvarjen), pri tem morajo biti vse komponente elektronskega dokumenta prikazane skupaj. Organizacija mora določiti, kateri aplikacijski paketi in oblike zapisa so potrebni.

Izpis

To podpoglavje se nanaša tako na dokumente, ki jih lahko smiselno izpišemo, kot tudi na informacije o nadzoru znotraj ISUD-a. ISUD mora zagotoviti tak način izpisa, da lahko vsi uporabniki prejmejo izpisano kopijo dokumenta in njegovih metapodatkov, kot tudi drugih podatkov. V vseh primerih s pojmom »izpis« razumemo izpis na aplikacijski ravni z vsemi kontrolami in značilnostmi, ki jih navadno posredujemo (kot so poročila na več straneh, poglavja, uporaba kateregakoli primerno nastavljenega tiskalnika). Pri tej zahtevi pošiljanja vsebine zaslona tiskalniku ne razumemo kot normalno sprejemljivega.

ETZ 3.6.2.4

ISUD mora uporabniku ponujati prilagodljive načine izpisa dokumentov in njihovih ustreznih metapodatkov, vključno z možnostjo izpisa dokumenta(ov) z metapodatki, ki jih določi uporabnik.

ETZ 3.6.2.5

ISUD mora omogočati izpis metapodatkov za posamezno zadevo.

ETZ 3.6.2.6

ISUD mora omogočati izpis vseh dokumentov v eni zadevi, v zaporedju, ki ga določi uporabnik.

ETZ 3.6.2.7

ISUD mora uporabniku omogočati izpis zbirnega seznama izbranih dokumentov (npr. vsebin neke zadeve), ki je sestavljen iz podskupine metapodatkovnih elementov, ki jo uporabnik določi za vsak dokument (npr. naslov, avtor, datum nastanka).

ETZ 3.6.2.8/a

ISUD mora skrbniku omogočati določitev, da se vsem izpisom ali dokumentom dodajo izbrani metapodatkovni elementi, npr. naslov, evidenčna številka, datum, stopnja tajnosti.

ETZ 3.6.2.9

ISUD mora uporabnikom omogočati izpis seznama rezultatov iskanja.

ETZ 3.6.2.10

ISUD mora skrbniku omogočati izpis vsakega oziroma vseh administrativnih parametrov.

ETZ 3.6.2.11

ISUD mora skrbniku omogočati izpis rokov hrambe.

ETZ 3.6.2.12/a

ISUD mora skrbniku omogočati izpis tezavra.

ETZ 3.6.2.13

ISUD mora skrbniku omogočati izpis klasifikacijskega načrta.

ETZ 3.6.2.14

ISUD mora skrbniku omogočati izpis seznama zadev.

ETZ 3.6.2.15

ISUD mora skrbniku omogočati izpis revizijske sledi.

ETZ 3.6.2.16

ISUD mora biti sposoben izpisati vse vrste elektronskih dokumentov, ki jih določi organizacija. Izpis mora:

- ohraniti izgled, narejen z aplikacijskim(i) paketom(i), s katerim(i) je dokument ustvarjen;
- vključiti vse sestavne dele elektronskega dokumenta (ki jih je mogoče izpisati).

Organizacija mora določiti, kateri aplikacijski paketi in oblike zapisa so potrebne.

3.7 SKRBNIŠTVO

Določena stopnja sprememb v organizacijah je normalna in jo je treba upoštevati pri vzdrževanju ISUD-a in pri pripomočkih za podporo sistema. ISUD mora skrbniku zagotavljati tudi pripomočke za podporo dogodkov, kakršni so spreminjanje števila uporabnikov, povečane zahteve po zmogljivosti hrambe, obnavljanje po izpadu sistema in nadzorovanje sistemskih napak. Nekatere od teh pripomočkov lahko zagotavlja pridruženi ESUZ ali sistem za upravljanje baze podatkov.

V tem poglavju so naštete zahteve za skrbništvo poročanje o sistemu in redakcijo dokumentov.

3.7.1 Skrbništvo

To podpoglavje vključuje zahteve za upravljanje parametrov sistema, izdelavo rezervnih kopij in obnavljanje, upravljanje sistema ter administracijo uporabnika.

ETZ 3.7.1.1

ISUD mora dovoljevati skrbnikom, da na nadzorovan način in brez nepotrebnega napora pridobijo, prikazujejo in preoblikujejo sistemske parametre in izbire, ki so bile nastavljene ob vzpostavitvi programa – npr. na elementih, ki jih je treba indeksirati – ter ponovno dodeljevanje uporabnikov in funkcij uporabniškim vlogam.

ETZ 3.7.1.2

ISUD mora zagotoviti pripomočke za izdelavo rezervnih kopij in zmožnost za nadaljnje preoblikovanje z uporabo obnovljenih rezervnih kopij in revizijske sledi, tako da se ohrani celovitost sistema.
Z drugimi besedami, ISUD mora vključevati funkcionalnost za povrnitev dokumentov in metapodatkov v znano stanje z uporabo obojega: tako rezervne kopije kot revizijske sledi.

ETZ 3.7.1.3

ISUD mora zagotoviti pripomočke za obnovitev in povrnitev stanja ob morebitnem izpadu sistema ali napak, ki nastanejo pri posodobitvi (ažuriranju) in mora skrbnike obvestiti o rezultatih.
Z drugimi besedami, ISUD mora dovoljevati skrbnikom razveljaviti zaporedje transakcij, dokler ni dosežena zagotovljena celovitost baze podatkov. To je zahtevano samo, ko se pojavijo pogoji za napake.

ETZ 3.7.1.4

ISUD mora nadzorovati prostor za hrambo, ki je na voljo, in opozoriti skrbnike, ko je zaradi pomanjkanja prostora potrebno ukrepanje ali je potrebna drugačna pozornost skrbnika.

ETZ 3.7.1.5

ISUD mora dovoliti skrbnikom izvesti obsežne spremembe klasifikacijskega načrta, ki zagotavljajo, da bodo vsi metapodatki in revizijske sledi obdelani pravilno in v celoti, da bi naredili te organizacijske spremembe:

- razdelitev ene organizacijske enote na dve;
- povezavo dveh organizacijskih enot v eno;
- premik ali preimenovanje organizacijske enote;
- razdelitev celotne organizacije na dve organizaciji.

Ko izvedemo tako spremembo, morajo zaključene zadeve ostati zaključene in ohraniti povezave s klasifikacijskim načrtom pred spremembo, odprte zadeve pa morajo bodisi:

- biti zaključene in ohraniti svoje povezave s klasifikacijskim načrtom pred spremembo ter biti navzkrižno povezane z novo zadevo v spremenjenem načrtu, bodisi
- biti povezane s spremenjenim načrtom, vendar jasno ohraniti vse prejšnje povezave s klasifikacijskim načrtom pred spremembo.

Opisane spremembe organizacijskih enot lahko pomenijo vzporedne spremembe v klasifikacijskih načrtih enot in pri njihovih uporabniških populacijah. Izraz »masovne spremembe« pomeni, da se vsi razredi, zadeve in dokumenti, ki jih zadevajo, obdelujejo z majhnim številom transakcij, in da ni treba obdelati vsakega posebej.

ETZ 3.7.1.6

ISUD mora podpirati prehajanje uporabnikov med organizacijskimi enotami.

ETZ 3.7.1.7

ISUD mora dovoljevati definiranje vlog uporabnikov in dovoljevati, da so lahko z vsako vlogo povezani različni uporabniki.

3.7.2 Poročanje

To podpoglavje podaja le okvirne zahteve. Tu ni smiselno poskušati navajati zahteve za nek vsestranski podsistem pisanja poročil. Pri vsaki izvedbi bodo zahteve za obseg in kompleksnost poročanja določene z velikostjo, kompleksnostjo in ravnjo sprememb klasifikacijskega načrta, števila in narave dokumentov ter baze uporabnikov.

ETZ 3.7.2.1

ISUD mora zagotavljati skrbniku prilagodljive pripomočke za poročanje. Najmanj, kar morajo vključevati, je sposobnost za poročanje o:

- številu zadev in dokumentov;
- statistiki transakcij za zadeve in dokumente;
- poročila o dejanjih za vsakega uporabnika posebej.

ETZ 3.7.2.2

ISUD mora dovoliti skrbnikom raziskati in izdelati poročila o revizijski sledi. Ta poročila morajo vključevati najmanj poročanje, ki temelji na izbranih:

- razredih;
- zadevah;
- dokumentih;
- uporabnikih;
- časovnih obdobjih.

ETZ 3.7.2.3/a

ISUD mora dovoljevati skrbnikom, da poizvedo in izdelajo poročila o revizijski sledi, temelječa na izbranih:

- stopnjah tajnosti in vrsti tajnosti;
- skupinah uporabnikov;
- drugih metapodatkih.

ETZ 3.7.2.4

ISUD mora biti sposoben izdelati poročilo z naštevanjem zadev, strukturiranih tako, da odražajo celotni klasifikacijski načrt ali pa le del.

ETZ 3.7.2.5/a

ISUD mora vključevati možnosti za razvrščanje in izbiranje informacij poročila.

ETZ 3.7.2.6/a

ISUD mora vključevati funkcije za zaokroževanje in združevanje informacij poročila.

ETZ 3.7.2.7

ISUD mora dovoljevati skrbnikom, da zahtevajo redna periodična in posamezna poročila.

ETZ 3.7.2.8/a

ISUD mora dovoljevati skrbnikom, da uporabnikom omejijo dostop do izbranih poročil.

3.7.3 Spreminjanje, brisanje in redakcija dokumentov

Osnovno načelo je, da dokumentov navadno ne smemo spreminjati (razen na koncu življenjskega cikla v ISUD-u) ter da zadev in dokumentov navadno ne smemo brisati. Lahko pa so izjeme, npr. zaradi uporabniške napake. To podpoglavje definira te zahteve. skrbniki včasih morda morajo »brisati« dokumente, da bi popravili uporabniške napake (tj. odkrivanje dokumentov v napačnih zadevah) ali da bi zadostili zakonskim zahtevam za varstvo podatkov. Dejanje brisanja lahko pomeni eno od dveh stvari:

- uničevanje;
- ohranitev, pospremljeno z zapisom v metapodatkih dokumenta, da imamo dokument za odstranjenega in ne več pod nadzorom upravljanja dokumentov.

Možnost brisanja mora biti strogo nadzorovana, da bi zavarovali splošno celovitost dokumentov. V revizijski sledi je treba predvsem hraniti informacije o brisanju podatkov, sled o izbrisanem(ih) dokumentu(ih) pa mora ostati v ovojih, ki jih to zadeva. Skrbniki morajo včasih objaviti ali narediti dostopne dokumente, ki še vedno vsebujejo občutljive informacije. To lahko izvira iz predpisov za varovanje podatkov, varnostnih razlogov, komercialnega tveganja itd. Zato morajo biti skrbniki sposobni odstraniti občutljive informacije, ne da bi to vplivalo na osnovni dokument. Proces se tukaj imenuje redakcija in ISUD hrani tako originalni dokument kot redigirano kopijo; ta se tukaj imenuje »izvleček« dokumenta.

ETZ 3.7.3.1

ISUD mora dovoljevati obveznost ali opcijo, ki preprečuje, da bi katerikoli skrbnik ali uporabnik zbrisal ali premestil katerikoli dokument, ki je bil enkrat zajet. To pomeni, da katerakoli zahteva za skrbnika, da upošteva dokument kot »zbrisan « ali »prestavljen«, pomeni, da je dokument primerno označen in je, če je bil prestavljen na novo lokacijo, tam vstavljena kopija ali kazalec.

Zahteva ne vpliva na premeščanje ali uničenje dokumentov v skladu z roki hrambe.

ETZ 3.7.3.2/a

ISUD mora ob vzpostavitvi programa kot alternativo zahtevi ETZ 3.7.3.1 omogočati, da »brisanje« dokumenta izvedemo kot uničenje dokumenta.

ETZ 3.7.3.3

Skrbnik mora biti sposoben spremeniti vrsto in stopnjo tajnosti posameznih dokumentov. Navadno se to zahteva, da dokumentom zmanjšamo dodeljeno raven zaščite, ko se sčasoma njihova občutljivost zmanjša.

ETZ 3.7.3.4

Skrbnik mora biti sposoben spremeniti vrsto in stopnjo tajnosti vseh dokumentov v zadevi ali razredu z eno operacijo. ISUD mora zagotoviti opozorilo, če ima katerikoli dokument znižano stopnjo tajnosti, in pred izpeljavo operacije počakati na potrditev. Navadno se to zahteva, da dokumentom zmanjšamo dodeljeno raven zaščite, ko se sčasoma njihova občutljivost zmanjša.

ETZ 3.7.3.5

V zvezi s podporo zahtevami 3.2.6.2 mora biti skrbnik sposoben spremeniti vrsto in stopnjo tajnosti zadeve.

ETZ 3.7.3.6

ISUD mora zapisati vse podrobnosti kakršnekoli spremembe vrste in stopnje tajnosti v metapodatkih dokumenta ali zadeve, na katero se nanaša.

ETZ 3.7.3.7

skrbniku mora biti dovoljeno brisanje razredov, zadev in dokumentov (glede na opcijo izbrano v ETZ 3.7.3.1). Ob vsakem takem brisanju mora ISUD:

- izčrpno zabeležiti brisanje v revizijski sledi;
- izdelati posebno poročilo za skrbnika;
- zbrisati celotno vsebino zadeve, ko je ta zbrisana.
- zagotavljati, da ne bo izbrisan noben zapis, če bi to povzročilo spremembo drugega dokumenta (npr. če je zapis del dveh dokumentov – glejte zahtevo ETZ 3.4.1.5/a – in je eden od obeh zbrisan);
- posebej opozoriti skrbnika na katerokoli povezavo iz druge zadeve ali dokumenta z zadevo, ki je namenjena brisanju, in zahtevati potrditev pred koncem brisanja;
- ob vsakem času ohranjati celovitost metapodatkov.

Ta funkcionalnost je mišljena samo za izjemne okoliščine.

ETZ 3.7.3.8

Skrbnik mora biti sposoben spremeniti katerikoli element, ki ga v metapodatke vnese uporabnik. Informacije o vsaki taki spremembi moramo shraniti v revizijski sledi. Ta funkcionalnost omogoča skrbniku popravljati napake uporabnikov, kot so napake pri vnosu podatkov, ter vzdrževati dostope uporabnikov in skupin.

ETZ 3.7.3.9

ISUD mora dovoljevati skrbniku dokumenta ali zadeve izdelati kopijo dokumenta za potrebe redakcije. Ta kopija se bo v tej specifikaciji imenovala izvleček dokumenta.

ETZ 3.7.3.10/a

ISUD mora omogočati funkcionalnost za odstranitev ali skrivanje občutljivih informacij v izvlečku; to vključuje najmanj:

- odstranitev posameznih strani iz večstranske slike dokumenta;
- dodajanje zatemnjenih pravokotnikov za prekritje občutljivih imen ali besed;
- kakršnekoli druge funkcije, zahtevane za video- oz. avdiooblike zapisa, če obstajajo.

Če ISUD ne ponuja teh pripomočkov neposredno, mora to dovoljevati drugim programskim paketom. Bistveno je, da če uporabljamo to ali katerokoli drugo funkcijo za redakcijo, da nobene odstranjene ali skrite informacije nikoli ni mogoče videti v izvlečku, bodisi na ekranu, na izpisu ali pa na traku ter ne glede na uporabo katerekoli funkcije, kot je rotacija, zoomiranje ali kakšne druge manipulacije.

ETZ 3.7.3.11

Če je narejen izvleček, mora ISUD zapisati to dejanje v metapodatke dokumenta, ti obsegajo najmanj datum, čas, razlog nastanka in izvajalca.

ETZ 3.7.3.12/a

ISUD mora opomniti ustvarjalca izvlečka, da ga dodeli zadevi, če ta dodelitev ni samodejna.

ETZ 3.7.3.13/a

ISUD mora shraniti navzkrižno povezavo k izvlečku v isti zadevi kot originalen dokument, tudi če je ta zadeva zaključena.

ETZ 3.7.3.14

ISUD mora v revizijski sledi shraniti vsako spremembo, narejeno kot odgovor na zahteve v tem podpoglavju.

3.8 ZAHTEVE ZA METAPODATKE

Če skušamo metapodatke definirati dobesedno, so to »podatki o podatkih«. Na področju upravljanja z informacijami se naziv uporablja predvsem za informacije, ki so bile v preteklosti pogosto povezane z različnimi bibliografskimi podatki, kot so npr. avtor, predmet, mesto v vnaprej definirani klasifikacijski shemi, ipd. Danes se metapodatke uporablja predvsem kot podporo za naprednejše načine razvrščanja in upravljanja z dokumenti, pri katerih lahko že govorimo o upravljanju z znanjem ali upravljanjem z informacijskimi viri.

Glavna značilnost vseh elektronskih dokumentov je njihova zmožnost enostavnega dodajanja, brisanja ali spreminjanja njihove vsebine. Pri elektronski hrambi je gradivu potrebno zagotoviti določeno stopnjo avtentičnosti in nespremenljivosti – preprečiti

spreminjanje elektronskih dokumentov, kjer naj bi ti ostali nespremenjeni, ali zagotavljanje pregleda sprememb, kjer je do njih prišlo.

Če so metapodatki pravilno uporabljeni, to zagotovijo na naslednje načine:

- omogočanje funkcionalnejšega priklica;
- podpora širokega spektra procesov upravljanja z dokumenti;
- vzpostavljanje provenience dokumentov - okoliščine v katerih je dokument nastal, bil uporabljen ali sprejet;
- zagotavljanje integritete dokumenta;
- prikazovanje povezav med dokumenti, ki skupaj tvorijo vpis ali zadevo;
- zagotavljanje podatkov, ki so nujno potrebni za omogočanje združljivosti dokumentov z različnimi obstoječimi tehnološkimi platformami in morebitnimi novimi.

Sistemi za upravljanje in hrambo z elektronskim dokumentarnim gradivom lahko podpirajo širok spekter različnih metapodatkov, odvisno od potreb in namenov posameznega sistema. Predvsem so to indeksirani podatki, vključujejo pa lahko tudi druge informacije, kot so npr. omejitve dostopa do posameznih dokumentov, ključne besede, povezave z drugimi dokumenti, podatki o času in pogostosti dostopa, itd.

Ker so potrebe posameznih sistemov za hrambo dokumentarnega ali arhivskega gradiva različne, je vse vrste zahtev za posamezno vrsto sistema težko določiti na enoten način, saj bodo nekateri podatki pri določeni organizaciji lahko nujni, pri drugi pa nepomembni.

3.8.1 Načela

Ta del zahtev predlaga le minimalne zahteve, ki so določene kot splošne, vendar so odprte za prilagoditve. Skoraj vsak bodoči ISUD je lahko konfiguriran z zadostnimi polji za podporo metapodatkovnih elementov, vendar pa samo to ne zadostuje. Pomembno je, da:

- mora ISUD uporabljati elemente metapodatkov, da bi omogočal in podprl funkcionalnost, definirano v nadaljevanju te specifikacije (glejte zahtevo ETZ 3.8.1.2);
- mora ISUD vključevati funkcije, ki podpirajo pravila potrditve veljavnosti podatkov, dedovanja in privzetih vrednosti, ko zajemamo elemente metapodatkov.

Za vrsto in način hrambe metapodatkov se uporabljajo uveljavljeni in priznani mednarodni standardi in priporočila (npr. MoReq in drugi) ter veljavni predpisi.

ETZ 3.8.1.1

ISUD aplikacija ne sme postaviti nobene praktične omejitve pri številu metapodatkovnih elementov, dovoljenih za vsako enoto (npr. zadevo, dokument). Definicija praktične omejitve' bo odvisna od aplikacije. Na primer, majhne organizacije s skromnim klasifikacijskim načrtom verjetno ne bodo potrebovale toliko metapodatkovnih elementov kot velike organizacije z obsežnim klasifikacijskim načrtom.

ETZ 3.8.1.2

Kjer se vsebine elementov metapodatkov lahko nanašajo na funkcionalno obnašanje ISUD-a, mora ISUD uporabljati vsebine teh elementov za določanje funkcionalnosti. Na primer, če ISUD hrani stopnje tajnosti dokumentov in tudi varnostna dovoljenja za

uporabnike, mora ISUD ta uporabiti, da določi, ali uporabnik sme ali ne sme dostopati do dokumenta. Če ISUD hrani dovoljenja in stopnje samo kot tekstovna polja, ki jih ne uporabljamo pri kontroli dostopa, potem zahteva ni izpolnjena.

Upoštevajte, da je to splošna zahteva, ki se razteza skozi mnogo metapodatkovnih elementov. Ta specifikacija ne poskuša opredeliti vseh primerov, pri katerih je to pomembno.

ETZ 3.8.1.3

ISUD mora dopustiti, da se med konfiguracijo definirajo različne skupine metapodatkovnih elementov za različne vrste elektronskih dokumentov.

Na primer, dokumenti, ki so skenirane slike, bodo potrebovali metapodatke, ki se nanašajo na postopke skeniranja in indeksiranja, fakture bodo potrebovale metapodatke o številki računa, korespondenca pa večvrednostna polja metapodatkov prejemnika (naslovnika).

ETZ 3.8.1.4

ISUD mora skrbniku dopustiti, da med konfiguracijo določi za vsak metapodatkovni element, ali je obvezen ali ne in ali je mogoče po njem iskati.

ETZ 3.8.1.5

ISUD mora podpirati vsaj te formate elementov metapodatkov:
- tekstualne;
- alfanumerične;
- numerične;
- datumske;
- logične (tj. da/ne, pravilno/napačno).

ETZ 3.8.1.6/a

ISUD mora podpirati formate metapodatkovnih elementov, ki jih določi skrbnik, sestavljeni pa so iz kombinacij formatov, navedenih v zahtevi ETZ 3.8.1.5.

Na primer, aplikacija ima lahko identifikacijsko številko v obliki nnnnn/aa-n.

ETZ 3.8.1.7

ISUD mora med konfiguracijo omogočiti definiranje izvora podatkov za vsak metapodatkovni element.

Možni viri so opisani v zahtevah ETZ 3.8.1.9, 3.8.1.10, 3.8.1.11, 3.8.1.12.

ETZ 3.8.1.8

ISUD mora podpirati sposobnost za samodejne izvlečke elementov metapodatkov iz dokumentov, ko so zajeti. Obstaja nekaj aplikacij, pri katerih to ni obvezno. Zahtevo tu razumemo za obvezno, ker je v mnogih primerih zelo pomembna. Primeri tega so

samodejni izvlečki datumov, naslovov, imen prejemnikov in identifikacijskih oznak iz tekstualno oblikovanih zapisov ali strukturiranih transakcijskih zapisov, kot so fakture.

ETZ 3.8.1.9

ISUD mora dopustiti skrbniku določiti, kateri metapodatkovni elementi morajo biti vneseni in vzdrževani (spremembe) z vnosom prek tipkovnice ali izbrani iz spustnega seznama.

ETZ 3.8.1.10/a

ISUD mora dopuščati, da se vrednosti metapodatkov samodejno pridobijo iz naslednje višje ravni v hierarhiji klasifikacijskega načrta. Za zadevo mora biti na primer vrednost nekaterih metapodatkovnih elementov podedovana od njegove predhodne zadeve. Za dokument je vrednost nekaterih metapodatkov lahko podedovana iz tiste zadeve, v kateri je shranjen.

ETZ 3.8.1.11/a

ISUD mora omogočati vrednosti metapodatkov pridobiti iz vpoglednih tabel ali klicev v druge aplikacije. Na primer ISUD lahko zagotovi ime in poštno številko aplikaciji za naslavljanje, ta potem vrne ime ulice, ki se jo uporabi kot metapodatek.

ETZ 3.8.1.12

ISUD mora podpirati potrjevanje veljavnosti metapodatkov, ko uporabnik vnese metapodatek ali ko je ta uvožen. Potrjevanje veljavnosti mora uporabljati vsaj te mehanizme:

- oblika zapisa vsebin elementa;
- razpon vrednosti;
- potrditev veljavnosti s primerjavo seznama vrednosti, ki ga vzdržuje skrbnik;
- veljavno napotilo na klasifikacijski načrt.

Primer potrditve veljavnosti formata je, da so vse vsebine numerične ali v obliki datuma (skladno z zahtevo 3.8.1.14). Primer potrditve veljavnosti razpona formata je, da vsebine padejo v obdobje med 1. januarjem 1999 in 31. decembrom 2001. Primer potrditve veljavnosti s primerjavo seznama vrednosti je potrditev, da je določena izvozna destinacija na tem seznamu.

ETZ 3.8.1.13

Kadar je potrebno, mora ISUD podpirati potrditev veljavnosti metapodatkov z uporabo klica v drugo aplikacijo (na primer klic v kadrovski sistem, da preveri, ali je bila osebna številka dodeljena, ali klic v sistem podatkovne baze poštnih številk).

ETZ 3.8.1.14

Kjer vrednosti metapodatkovnega elementa vnašamo ročno, mora ISUD podpirati trajne privzete vrednosti, ki jih lahko določi uporabnik. Trajna privzeta vrednost se pojavlja kot privzeta v polju za vnos podatkov za vsako naslednjo enoto v zaporedju, dokler je uporabnik ne spremeni. Ko je ta enkrat spremenjena, ostane kot nova vrednost, tj. postane trajna.

ETZ 3.8.1.15/a

Kjer je element metapodatka shranjen v datumskem obliki zapisa, mora ISUD omogočati iskanja, ki prepoznavajo datumske vrednosti. ISUD mora na primer podpirati iskanje v razponu datumov. Za datum ni dovolj, da je shranjen kot tekstualno polje.

ETZ 3.8.1.16/a

Kjer je element metapodatka shranjen v numeričnem obliki zapisa, mora ISUD dopuščati iskanja, ki prepoznavajo številčno vrednost.

ETZ 3.8.1.17

ISUD mora omejiti možnost za spreminjanje vrednosti metapodatkov zgolj na skrbnika

ETZ 3.8.1.18

ISUD mora dopuščati, da skrbnik prekonfigurira nabore metapodatkov, to pa mora zabeležiti v revizijski sledi. Nekaterim vrstam zapisov bi bilo lahko na primer treba dodati nov podatkovni element, kot je 'identifikator oddelka'; to sledi iz organizacijske spremembe.

ETZ 3.8.1.19/a

ISUD mora biti sposoben prevzemati metapodatke od:

- aplikacijskega paketa za ustvarjanje zapisov, operacijskega sistema ali mrežne programske opreme;
- uporabnika v trenutku zajema ali objave;
- pravil, določenih v času nastavljanja, za ustvarjanje metapodatkov (ki jih ustvarja ISUD), v trenutku objave.

ETZ 3.8.1.20

ISUD mora biti sposoben preprečiti kakršenkoli popravek metapodatkov, zbranih neposredno iz drugih aplikacij, operacijskega sistema ali ISUD-a, na primer podatkov o prenosu elektronske pošte.

ETZ 3.8.1.21

ISUD mora preprečiti spremembo namena metapodatkovnih polj, določenih v času konfiguriranja.

3.9 HRAMBA IN PRETVORBA

V tem poglavju bodo natančneje obrazložene in določene zahteve glede tistih vidikov hrambe gradiva, ki se nanašajo na obliko zapisa podatkov ter na specifične vrste nosilcev, na katerih je gradivo shranjeno.

Čeprav ima elektronska hramba dokumentarnega in arhivskega gradiva mnoge prednosti pred klasično (papirno) hrambo, se pri elektronski hrambi pojavljajo tudi nekateri problemi in izzivi, s katerimi se je potrebno soočiti, če naj elektronska hramba zagotovi

avtentičnost gradiva, uporabljivost njegove vsebine, nespremenljivost gradiva ter njegovo kasnejšo uporabnost.

Prvi izziv je zagotoviti, da bodo vsi hranjeni dokumenti lahko prebrani in dosegljivi tudi v prihodnosti. Ker se področje informacijske tehnologije razvija s precej hitrim tempom, se pojavlja vprašanje zastaranja strojne ali programske opreme, na kateri in s pomočjo katere so elektronski dokumenti shranjeni. To vprašanje je še posebej pomembno pri gradivu za katerega zakonski predpisi predpisujejo dolgoročno hrambo, kar pomeni, da bodo ti dokumenti hranjeni še mnogo let po njihovem zajemu. Ker se s hitrim razvojem različnih oblik zapisov podatkov pojavljajo nove oblike zapisov podatkov ali pa se nadgrajujejo stare, obstaja možnost, da programska oprema v prihodnosti ne bo sposobna prebrati starejših oblik zapisov.

Naslednje vprašanje se nanaša na fizične nosilce podatkov, pri katerih sta opazna dva temeljna problema. Prvi se nanaša na nezdružljivost današnjih nosilcev podatkov s strojno opremo za branje podatkov z nosilcev v prihodnosti, drugi pa na samo fizično obstojnost takšnih nosilcev podatkov. Pri hrambi gradiva (predvsem pri dolgoročni hrambi) je potrebno zagotoviti tako možnost kasnejšega branja nosilcev, kot tudi učinkovite mehanizme za izogibanje fizičnemu propadanju nosilcev.

Zaradi specifičnih lastnosti elektronske oblike podatkov, ki sami po sebi ne nudijo nobene »zaščite« pred spreminjanjem njihove vsebine (brez dodatnih ukrepov ne moremo govoriti o sledljivosti sprememb), je potrebno zagotoviti celovitost hranjenega gradiva. Pri tem je potrebno upoštevati tehnološke značilnosti oblik zapisa podatkov. Poleg tega je potrebno zagotoviti tudi hrambo dodatnih metapodatkov o spremembah hranjenega gradiva.

Hranjeno gradivo bo potrebno v nekaterih primerih (še posebej v primeru arhivskega gradiva) tudi izvoziti in pretvoriti v drugo obliko zapisa, pri čemer je zopet potrebno zagotoviti nespremenljivost in avtentičnost vsebine gradiva.

3.9.1 Dolgoročna hramba in tehnološko zastaranje

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih se s tehnološkimi podrobnostmi tehnološkega zastaranja natančno ne ukvarja, vseeno pa je zavedanje zakonodajalca o tem problemu v njem prisotno, saj so temeljna načela zakona povezana tudi s tem vprašanjem.

V 3. členu zakon postavlja načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine. Zakon določa, da je *»hrambi izvirnega gradiva (…) zato enaka hramba zajetega gradiva, če zagotavlja zajetemu gradivu vse učinke izvirnega gradiva«.* Ta določba se prvenstveno nanaša na sam zajem in pretvorbo gradiva pri zajemu, ki mora zagotavljati določenim pogojem, s katerimi se ohranijo učinki izvirnega gradiva, ima pa tudi pomen za prihodnost. Če naj zajeto gradivo takšne učinke tudi ohrani, se je potrebno izogniti morebitnim težavam, ki bi lahko zaradi zastaranja opreme, oblike zapisa ali propadanja samega nosilca zapisa, na katerem se gradivo hrani, onemogočile gradivu enake učinke, kot jih je imelo izvirno gradivo. Na to se navezuje tudi 4. člen zakona (Načelo trajnosti), ki določa, da mora hramba zagotavljati trajnost gradiva ter trajnost reprodukcije njegove vsebine. Načelo celovitosti (5. člen) govori o nespremenljivosti in integralnosti dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenosti in dokazljivosti vsebine tega gradiva. Nekoliko pomembnejše je načelo dostopnosti (6. člen), po katerem mora biti hranjeno gradivo ves čas zavarovano pred izgubo ali okrnitvijo celovitosti, ob tem pa mora biti ves čas dostopno uporabnikom.

Tehnološko zastaranje lahko prepreči tako dostopnost do hranjenega gradiva kot tudi povzroči okrnitev celovitosti, zato je preprečevanje učinkov tega procesa zelo pomembno in kot tako posredno umeščeno v načela zakona.

To podpoglavje se ukvarja z dolgoročno hrambo, ki je po ZVDAGA tista hramba gradiva, pri kateri se gradivo hrani za časovno obdobje, ki je daljše od petih let.

V katerikoli organizaciji naj bi bil rok hrambe določen z zakonodajo in poslovnimi potrebami. V nekaterih okoljih bo to pomenilo več desetletij. V nekaterih arhivih se lahko čas podaljša na stoletja. V obeh primerih je časovno obdobje dovolj dolgo, da pristopov, ki jih rutinsko uporabljamo za krajša obdobja, ne moremo imeti za primerne.

Elektronski dokumenti, ki se hranijo dolgotrajno, so izpostavljeni tveganju zaradi:
- propadanja nosilca zapisa;
- zastarevanja tehnične opreme;
- zastarevanja oblike zapisa.

O tem razpravlja nadaljnje besedilo. Razpravam sledijo specifične zahteve. Vendar pa naj bi bralci upoštevali, da ta specifikacija ne navaja podrobnih zahtev za vse vidike tega vprašanja. Vsaka organizacija naj bi razvila in implementirala strategijo za dolgoročno hrambo svojih elektronskih dokumentov, tako kot je večinoma v zvezi z dokumenti na papirju.

V razpravi, ki sledi, hramba dokumentov pomeni ohranitev metapodatkov in informacij iz revizijskih sledi, ki jih spremljajo.

Propadanje nosilca zapisa

Tveganje zaradi propadanja nosilca zapisa nastaja zato, ker imajo vsi nosilci zapisa za elektronsko hrambo, omejeno življenjsko dobo. Življenjska doba se razlikuje od enega do drugega nosilca zapisa, razlikuje pa se tudi v odvisnosti od pogojev hrambe (temperatura, vlažnost in stopnje spremembe). Ko nosilec zapisa doseže ali preseže svojo pričakovano življenjsko dobo, se verjetnost napak pri branju (oziroma napačno prebranih bitov) začne dramatično povečevati. Večina strojne opreme za hrambo ima vgrajeno samodejno popravljanje napak; to lahko obvlada določeno raven bitnih napak z učinkovitim kompenziranjem. Vendar končno postanejo prebrane napake tako številne, da jim samodejno popravljanje ni več kos. Na tej stopnji postanejo dokumenti nepopravljivo popačeni. Učinek te popačenosti je odvisen od mnogih dejavnikov, lahko pa se zgodi, da postanejo posamezni dokumenti ali celotni diski, trakovi itd. neberljivi.

Da bi se izognili izgubi informacij zaradi propadanja nosilcev zapisa, lahko sprejmemo te preventivne ukrepe:

- zagotovimo, da so vsi nosilci zapisa shranjeni, da jih uporabljamo in z njimi ravnamo v pogojih stabilnega okolja. Na splošno velja: čistejše, hladnejše, stabilnejše in bolj suho kot je okolje, daljša je pričakovana doba trajanja. Vendar pa je treba za specifične nosilce zapisa upoštevati specifikacije proizvajalca (npr. okolje ne sme biti hladnejše od določene temperature. Nosilce zapisa moramo ali pa jih ne smemo periodično čistiti);
- rutinsko menjamo nosilce zapisa (s kopiranjem informacij na nove nosilce zapisa) pred pričakovanim iztekom dobe trajanja;
- hranimo več kopij vsakega dokumenta in jih primerjamo sistematično po razporedu. Potem zamenjamo vsako kopijo dokumenta in vsak del nosilca zapisa, ki pokaže nepopravljivo napako. Tak pristop po navadi uporabljamo v specializiranih arhivih trajnih podatkov. To zahteva avtomatizirane sisteme in

strojno opremo za preiskovanje; njihov podrobnejši opis pa presega namen te specifikacije.

Zastarevanje strojne opreme

Periferne enote za hrambo – pogonske enote za trakove in diske – imajo omejeno dobo trajanja na tržišču. Ko ta čas presežejo, po navadi zahtevajo več vzdrževanja, sčasoma pa postajajo vzdrževanje in popravila vse dražje in končno postanejo nepopravljivi za praktično uporabo. V nekaterih primerih z drugimi uporabniki lahko dosežemo sporazum o skupni uporabi podobne ali kompatibilne opreme. Vendar tega ni mogoče neskončno vzdrževati. V določenem trenutku se lahko informacije, shranjene na zastarelih napravah, ki niso prekopirane na drug nosilce zapisa, za vselej izgubijo, če naprava zataji.

Enak problem se pojavi pri računalnikih, ki upravljajo aplikacije in hrambo. Nedvomno je strategija za izogibanje temu tveganju spremljanje statusa strojne opreme in migracija podatkov na nov, sodoben nosilec zapisa, še preden zastaranje izpostavi informacije tveganju. Vsekakor naj bi izbrali nosilce zapisa in strojno opremo, ki imajo daljšo pričakovano dobo trajanja. Z drugimi besedami, popularen ali 'vodilni na tržišču' je lahko boljša izbira kot nov in zadnji krik tehnike.

Zastarevanje oblik zapisa

Zastarevanje oblik zapisa predstavlja najtežavnejši problem za vsako obdobje, daljše od nekaj desetletij. Problem se pojavlja zato, ker se mnoge komponente programske opreme, vključene v procesno »verigo« med nosilcem zapisa in prikazanimi informacijami, nenehno razvijajo. Komponente obsegajo:

- standarde programiranja;
- oblike zapisa datotek;
- aplikacije;
- baze podatkov in preostalo storitveno programsko opremo;
- operacijske sisteme.

Njihov razvoj je pospešen, različne komponente pa se razvijajo na različne načine in v različnih stopnjah. Nekatere razvite različice ostanejo kompatibilne s prejšnjimi oblikami zapisa. Vendar pa nekatere ne ohranjajo kompatibilnosti – in to še posebej drži za obdobja daljša od le nekaj desetletij. Kot je opisano zgoraj, se zaradi potrebe po migraciji na novejšo strojno opremo ni mogoče izogniti razvoju z 'zamrznitvijo' konfiguracije. Nova strojna oprema pogosto zahteva novo pogonsko programsko opremo, le-ta pa spet nov operacijski sistem in tako naprej.

Trenutno so priznane te tehnike **migracija** (konvertiranje informacij v nove oblike zapisa, do katerih je možno dostopati z obstoječo strojno in programsko opremo); **emulacija** (premeščanje informacij na novo strojno opremo, vendar z dodatno komponento programske opreme, ki posnema staro strojno opremo in tako omogoča izvajanje stare aplikativne programske opreme); opušča pa se **ohranitev tehnologije** (stalno vzdrževanje originalne strojne opreme; na daljši rok ni praktično).

Splošno prepričanje je, da sta migracija in/ali emulacija verjetno najvarnejši opciji. V praksi bosta obe zahtevali, da posebno pozornost posvetimo ohranitvi metapodatkov – glejte zgoraj. Vendar pa so obsežne migracije redko izvedljive brez težav. To se lahko kaže v izgubi posameznih enot, včasih pa tudi v izgubi funkcionalnosti, podrobnosti, ali drugih značilnosti.

Podobno velja, da obsežne dolgoročne emulacije ne poznamo dobro. Tudi pri tej obstaja tveganje izgube funkcionalnosti in drugih značilnosti.

Težave se kopičijo pri ponovljenih migracijah ali emulacijah. Nihče ne more predvideti narave migracij ali emulacij, ki bodo morda potrebne. Nihče tudi ne more predvideti posledic ponovljenih migracij ali več »slojev« emulacij.

Najprimernejša strategija je, da informacije hranimo samo v široko sprejetih, stabilnih, odprtih oblikah zapisa (tj. v oblikah zapisa, ki so vsestransko dokumentirane v javno dostopnih specifikacijah), ki imajo daljšo pričakovano dobo trajanja. Enako kot pri strojni opremi bolj priporočamo 'vodilne na trgu' kot pa neuveljavljene ali 'zadnji krik tehnike'. Predlagamo tudi izogibanje lastniškim oblikam zapisa, katerih specifikacije niso javno razpoložljive. Tu je tudi samoumevna posledica, da bo organizacija pri izbiranju oblik zapisa potrebovala strokovna znanja.

Zaradi nestanovitnosti multimedijskega tržišča in lastniških oblik zapisa, ki jih le-to uporablja, razmere na multimedijskem področju še posebej zbujajo skrb.

Ker ta problem zahteva poseben odgovor za vsako organizacijo, podrobna razprava na splošni ravni te specifikacije ne bi bila uporabna. Vendar pa je treba poudariti, da vsak pristop vključuje izdatek – za strojno in programsko opremo, pripravo in konverzijo podatkov ter za upravljanje – vendar nobeden ne bo zagotovil dostopanja, če ne bo praktično vpeljana strategija za dolgoročno hrambo, preden postane dostopnost problematična. Z drugimi besedami: dolgotrajna hramba zahteva preventivne izdatke, višina teh pa se lahko zelo poveča. V konceptu je to podobno hrambi arhivskega gradiva na papirju, le da bodo v nekaterih primerih stroški večji. Kjer se zahteva dolgoročna hramba, je bistveno, da je vodstvo naklonjeno nenehnim prizadevanjem in pripravljeno na izdatke, potrebne za zagotavljanje dostopa.

Metapodatki o hrambi

Kadar je potrebna dolgoročna hramba, je nujno, da metapodatke o hrambi hranimo skupaj z dokumenti. Ti metapodatki ponujajo informacije, ki presegajo okvir metapodatkov, določenih v tej specifikaciji, kot so informacije o tehničnem okolju, programski opremi, uporabljeni za kreiranje dokumentov, in programski opremi, potrebni za prikaz dokumenta ter vseh njegovih komponent.

Kjer je obdobje hrambe neomejeno, postane število zahtevanih metapodatkovnih elementov veliko.

Zahteve v tem podpoglavju so predlagane kot minimalna tehnična zahteva, pri kateri je načrtovana dolgoročna hramba.

ETZ 3.9.1.1

ISUD-ove nosilce zapisa za hrambo je treba uporabljati in hraniti v okoljih, ki so kompatibilna s pričakovano dobo trajanja in so znotraj tolerance specifikacije proizvajalcev nosilcev zapisa. V nekaterih primerih lahko citiramo standard, kot je BS 4783.

ETZ 3.9.1.2/a

ISUD mora vključevati značilnosti za samodejno periodično primerjavo kopij informacij in zamenjavo katerekoli kopije, za katero ugotovimo, da je pomanjkljiva, zato da jo zavarujemo pred degradacijo nosilca zapisa.

ETZ 3.9.1.3/a

ISUD mora omogočati obsežno pretvorbo dokumentov (z njihovimi metapodatki in informacijami o revizijski sledi) na druge nosilce zapisa in/ali sisteme, skladno s standardi, ustreznimi za oblike zapisa, ki so v uporabi.

ETZ 3.9.1.4

Dobavitelji ISUD morajo imeti vzpostavljen razviden program za nadgraditve tehnološke osnove ISUD-a, ki omogoča, da še naprej dostopamo do obstoječih informacij, ne da bi spreminjali vsebino.

ETZ 3.9.1.5

ISUD mora uporabljati samo široko sprejete standarde, ki so predmet odprtih in javno dostopnih specifikacij za kodiranje, hrambo in strukture podatkovnih baz.

ETZ 3.9.1.6

Če ISUD uporablja katerokoli lastniško kodiranje, ali hrambo ali strukture podatkovnih baz, morajo biti ti popolno dokumentirani, dokumentacija pa na voljo skrbniku. Treba je upoštevati, da to pomeni, da za dobavitelja morda ne bo dovolj shraniti kopijo dokumentacije. V časovnem razponu, ki ga obravnavamo, stabilnost dobavitelja ni zanesljiva. Zato je lahko zaželeno, da obstaja kopija te dokumentacije pri organizaciji uporabnika ali nevtralni tretji osebi.

ETZ 3.9.1.7

ISUD mora biti za dokumente in njihove sestavne dele sposoben upravljati niz metapodatkovnih elementov o hrambi.
Glejte zahtevo ETZ 3.8.4.13.

3.9.2 Oblika zapisa

Dokumenti so lahko shranjeni v velikem številu različnih oblik zapisa, ki so odvisne tudi od vrste dokumenta oziroma vrste vsebine, ki jo vsebujejo (besedilo, slike, multimedijske vsebine ali kombinacija vseh). Oblika zapisa dokumenta določa, na kakšen način so znaki, strukture in njihova razvrstitev organizirani in zapisani. Oblike zapisov za zapis dokumentov lahko za potrebe teh zahtev ločimo na tri razrede:

- produkcijske oblike zapisa – so odvisne od izvirnega orodja, s pomočjo katerega je dokument nastal;
- oblike zapisa za hrambo – oblike zapisa, ki so primerni za hrambo in dolgoročno hrambo, ker pod določenimi pogoji zagotavljajo avtentičnost, nespremenljivost in ohranjanje vsebine dokumenta ter njegovo dostopnost tudi po daljšem časovnem obdobju
- izmenjevalne oblike zapisa – oblike zapisa, ki se uporabljajo pri izmenjavi dokumentov med različnimi aplikacijami ali okolji, preko fizičnih nosilcev ali preko komunikacijskih sredstev.

ZVDAGA je ubral odprt pristop k urejanju oblike zapisa dokumentov, zato ni natančno specificiral, v kakšni obliki in v kakšnem obliki zapisa morajo biti hranjeni dokumenti zapisani. Zakon tako vsebuje zgolj splošne določbe, ki zahtevajo, da je pri hrambi

izvirnega ali zajetega dokumentarnega gradiva v elektronski obliki potrebno zagotoviti dostopnost, uporabnost, celovitost in avtentičnost tega gradiva (26. in 27. člen).

Produkcijske oblike zapisa

Produkcijske oblike zapisa se delijo v različne kategorije, med katerimi so najpomembnejši naslednji:

- znakovne oblike zapisa – shranjujejo se samo znaki in števila;
- tekstovne oblike zapisa – poleg znakov in števil se shrani tudi struktura in izgled dokumenta;
- grafične oblike zapisa – namenjene hrambi slik in grafičnih prikazov;
- video oblike zapisa – namenjene hrambi video-vsebin;
- audio oblike zapisa – namenjeni hrambi zvoka;
- multimedijske oblike zapisa – namenjene hrambi skupka teksta, slik, grafičnih vsebin, strukture in izgleda dokumenta, video vsebin ter zvoka.

Ker so produkcijske oblike zapisa odvisne od specifičnih aplikacij in orodij, s katerimi so bili dokumenti v teh oblike zapisa ohranjeni, ne predstavljajo zadovoljive rešitve za varno hrambo in dolgoročno hrambo dokumentov, s katero bi bilo zadoščeno vsem zakonskim in podzakonskim zahtevam. Dodatne težave se lahko pojavijo predvsem pri lastniških oblikah zapisa, katerih uporaba ni prosta in je pogosto odvisna od licenc. Poleg tega obstaja veliko število različnih oblik zapisa, ki se sproti in pogosto nadgrajujejo ter niso vzvratno-združljivi s starejšimi različicami programske opreme namenjene prikazu in pretvorbi teh oblik zapisa. Za izvajanje hrambe dokumentov je zato potrebno določiti le nekaj oblik zapisa, ki so univerzalne, nelastniške in primerne za hrambo različnih vsebin

Oblike zapisa za hrambo

Za zagotovitev predpisanih zakonskih zahtev za dolgoročno hrambo (dostopnost, uporabnost, celovitost, avtentičnost) je bolj kot uporaba produkcijskih oblik zapisa ustrezna uporaba takšnih oblik zapisa, ki so za takšne vrste hrambe primernejši – oblike zapisa za hrambo. Te oblike zapisa morajo zagotavljati dolgoročno dostopnost, kar je najlažje doseči s sledečimi zahtevami:

- oblika zapisa mora biti dokumentirana, dokumentacija pa mora biti odprtega tipa;
- zaželeno je, da je oblika zapisa ISO standard;
- oblika zapisa mora biti podprta s celovitimi in uveljavljenimi produkti na trgu;
- pretvorba dokumentov v obliko zapisa za hrambo mora biti razmeroma netežavna;
- v obliko zapisa za hrambo mora biti možno pretvoriti dokumente iz najpogosteje uporabljenih produkcijskih oblik zapisa, vključno z grafičnimi oblikami zapisa;
- omogočena mora biti kasnejša pretvorba oblik zapisa za hrambo v nove oblike zapisa za hrambo.

Takšne oblike zapisa so standardizirane, zato omogočajo uporabo na različnih platformah in operacijskih sistemih, večinoma pa so bile razvite tudi kot oblike zapisa za izmenjavo.

ETZ 3.9.2.1

ISUD mora omogočati uporabo najmanj ene od oblik zapisa, ki omogočajo dolgoročno hrambo elektronskih dokumentov (oblike zapisa, ki omogočajo dolgoročno hrambo elektronskih dokumentov, so našteti v Prilogi 1).

ETZ 3.9.2.2

Med izvozom ali prenosom dokumentov v obliki zapisa po standardu SGML, morajo biti priloženi dodatni podatki, potrebni za prikaz dokumenta (npr. definicija tipa dokumenta (DTD) in DSSSL (Document Style Semantics and Specification Language))

ETZ 3.9.2.3

Grafične datoteke so lahko enostranske ali večstranske. Če so enostranske, mora biti vsaka stran dokumenta shranjena v svoji datoteki v isti mapi.

ETZ 3.9.2.4

Za kompresiranje datotek smejo biti uporabljeni le splošno priznani in praviloma odprti standardi, ki so podprti s celovitimi in uveljavljenimi produkti na trgu in omogočajo kompresijo brez izgub podatkov. Primeri takšnih standardov so našteti v Prilogi 1.

ETZ 3.9.2.5/a

Datoteke, ki vsebujejo tekstovno vsebino, morajo biti, kjer je to mogoče, shranjene v obliki, ki temelji na tekstovnem zapisu, in ne v obliki, ki temelji na binarnem zapisu.

ETZ 3.9.2.6/a

Pri hrambi dokumentov morajo biti uporabljene pisave, priložene ali vgrajene dokumentom.

3.9.3 Pretvorba oblike zapisa

Poleg same oblike zapisa, je pri hrambi in dolgoročni hrambi velikega pomena tudi zmožnost pretvorbe teh oblik zapisa v druge oblike zapisa. Čeprav oblike zapisa za hrambo omogočajo izpolnjevanje določenih zakonskih zahtev, ki se nanašajo na dolgoročno hrambo, še vseeno niso popolnoma »odporne« na proces tehnološkega zastaranja, saj nikjer ni zagotovljeno, da se bo določena oblika zapisa obdržala v uporabi za nedoločen čas.

ISUD mora zato omogočati pretvorbo hranjenih dokumentov iz teh oblik zapisa v morebitne druge oblike zapisa, poleg tega pa tudi pretvorbo iz produkcijskih oblik zapisa v oblike zapisa za hrambo in obratno, pri čemer je potrebno zagotoviti, da se ohranja celovitost, avtentičnost in uporabnost vsebine dokumentov.

Uredba o varstvu arhivskega in dokumentarnega gradiva vsebuje zahteve, ki morajo biti izpolnjene pri pretvorbi gradiva v elektronski obliki iz ene oblike zapisa v drugo obliko zapisa. Pri pretvorbi je potrebno zagotoviti
ETZ 3.9.3.1

ISUD mora omogočati pravilno pretvorbo reprodukcije vsebine posamezne enote dokumentarnega gradiva. Pri tem mora pretvoriti vse ključne vsebinske podatke in obstoječe metapodatke, ustvariti vse potrebne metapodatke glede pretvorbe (dodatni odatki, ki potrjujejo enako avtentičnost zajetega gradiva, kot jo je imelo izvirno gradivo, datum pretvorbe, podatki o postopku pretvorbe, podatki o strojni in programski opremi, s katero je bila opravljena pretvorba, itd.) ter omogočiti strogo kontrolirano in dokumentirano dodajanje teh podatkov, in zagotavljati uporabnost vsebine izvirnega dokumentarnega gradiva.

ETZ 3.9.3.2

ISUD mora omogočati samodejno in ročno kontrolo pravilnosti pretvorbe reprodukcije vsebine in metapodatkov, varnost in nespremenljivost pretvorjenega dokumentarnega gradiva po pravilnem zajemu in možnost kasnejše poprave napak in upravičenega dopolnjevanja metapodatkov samo s strani pooblaščenih oseb.

ETZ 3.9.3.3

ISUD mora omogočati pretvorbo dokumentov iz produkcijskih oblik zapisa v standardiziran oblika zapisa za hrambo, ki je dokumentiran in čigar dokumentacija je odprta in dostopna.

ETZ 3.9.3.4/a

Funkcionalnost sistema, ki omogoča pretvorbo, mora biti enostavna za uporabo.

ETZ 3.9.3.5

Pretvorba mora ohraniti celovitost, avtentičnost in uporabnost vsebine dokumenta, poleg tega pa naj bi ohranila tudi vizualno avtentičnost dokumenta (način prikaza).

ETZ 3.9.3.6

Omogočena mora biti zaščita dokumentov, ki so shranjeni v obliki zapisa za hrambo, pred kasnejšim spreminjanjem ali urejanjem.

3.9.4 Nosilci zapisa

Posebno pozornost pri organiziranju hrambe ali dolgoročne hrambe dokumentarnega ali arhivskega gradiva v elektronski obliki terja izbira nosilca zapisa. Zagotavljanje celovitosti, dostopnosti in uporabnosti hranjenega gradiva je v veliki meri odvisno tudi od fizičnega elektronskega nosilca, na katerem je gradivo v elektronski obliki shranjeno, ne glede na obliko zapisa, ki je izbrana za primerno.

Pri nosilcih zapisa obstaja nevarnost tehnološkega zastaranja, zaradi katerega bi bila vsebina gradiva lahko ogrožena, še posebej tistega gradiva, za katerega je predpisana dolgoročna ali trajna hramba. Vprašanja glede nosilcev lahko razdelimo na dve vrsti. Prvi sklop potencialnih težav se lahko pojavi v povezavi z zastaranjem samega nosilca. Naprave, ki jih informacijski sistemi uporabljajo danes, bodo lahko v prihodnosti nadomeščene z drugimi, naprednejšimi in kvalitetnejšimi napravami, v katerih pa današnjih nosilcev ne bo več možno prebrati. Drug sklop potencialnih težav pa je povezan s staranjem nosilcev, kateri po poteku časa lahko začnejo izgubljati kakovost, posledica česar je izguba podatkov, ki so na njih zapisani.

En izmed možnih načinov izogibanja zastaranju nosilcev zapisa in izgubi podatkov je migracija. Z njo se zagotovi prepis gradiva na nove nosilce zapisa, če se ti pojavijo in izkažejo za dovolj zmogljive, varne in primerne za elektronsko hrambo gradiva, ali na istovrstne nosilce, s čemer se izogne propadanju nosilcev zaradi poteka časa.

ETZ 3.9.4.1

Nosilec zapisa mora temeljiti na mednarodnih uveljavljenih in splošno sprejetih standardih, ki so široko priznani oziroma uveljavljeni, njihova uporaba pa je podprta z na trgu uveljavljeno strojno in programsko opremo.

ETZ 3.9.4.2

Nosilec zapisa mora omogočati ohranitev zapisa podatkov tudi ob spremembi okoljskih pogojev ali ob prekinitvi dobave električne energije, za čas, ki je potreben za prenos podatkov na drug nosilec zapisa.

ETZ 3.9.4.3

Nosilec zapisa mora omogočati sledeče pogoje varne dolgoročne hrambe:
- dostopnost hranjenih podatkov in metapodatkov z zagotavljanjem varovanja pred izgubo;
- uporabnost hranjenih podatkov z zagotavljanjem možnosti in primernosti reprodukcije vsebine hranjenih podatkov;
- avtentičnost hranjenih podatkov tako, da omogoča dokazljivost povezanosti reproducirane vsebine z vsebino izvirnih podatkov;
- celovitost hranjenih podatkov tako, da je zagotovljena nespremenljivost in neokrnjenost ter urejenost reprodukcije vsebine hranjenih podatkov glede na vsebino izvirnih podatkov.

3.9.5 Izvoz in prenos gradiva

Ker je za preprečevanje tehnološkega zastaranja potrebno zagotoviti zmožnost prenosa celotnega hranjenega gradiva na morebitni nov sistem hrambe, mora sistem že sedaj omogočati enostaven izvoz vseh vrst elektronskih dokumentov v obliko zapisa, ki je neodvisna od kakršnegakoli sistema. S tem bo zelo olajšan prehod na nov sistem za hrambo gradiva.

ETZ 3.9.5.1

ISUD mora zagotavljati izvoz dokumentov iz oblike zapisa za hrambo v posamezne datoteke.

ETZ 3.9.5.2

Če je dokument sestavljen iz več datotek, morajo biti vse datoteke shranjene v isti mapi.

ETZ 3.9.5.3

Omogočeno mora biti povezovanje izvoženih dokumentov z drugimi podatki, ki so izvoženi iz ISUD.

ETZ 3.9.5.4/a

ISUD mora omogočati sledljivost vseh nekontroliranih kopij elektronskega dokumenta, ki so bili dodani v eno ali več zadev, ki niso zadeva njihovega izvora.

ETZ 3.9.5.5/a

ISUD mora omogočati samodejno shranjevanje povezav med več izvoženimi dokumenti in izvirno-hranjenim dokumentom.

ETZ 3.9.5.6

Pri izvozu dokumenta izven ISUD mora biti omogočen hkraten izvoz obstoječih metapodatkov, ki se na dokument nanašajo, hkrati pa mora biti omogočeno tudi odvzemanje določenih delov metapodatkov iz izvoženega dokumenta.

ETZ 3.9.5.7

ISUD mora pri dostopu in prikazu posameznega dokumenta omogočati prikaz podatkov o vseh izvoženih različicah tega dokumenta in omogočiti njihov priklic.

3.9.6 Hramba posebnih vsebin

Elektronski podpisi in časovni žigi

Elektronski podpisi in časovni žigi so pri hrambi ali dolgoročni hrambi elektronskega gradiva poglavitnega pomena, predvsem v povezavi z zagotavljanjem avtentičnosti in celovitosti hranjenega gradiva. Elektronski podpis je kontrolirana vsebina, ki je dodana shranjenemu gradivu (lahko je to posamičen dokument, lahko pa tudi celotna zadeva ali celo celotna zbirka dokumentarnega gradiva), zaradi svojih specifičnih matematičnih značilnosti pa ob pravilni uporabi omogoča preverjanje nespremenljivosti (avtentičnosti) in celovitosti vsebine gradiva.

Elektronski podpis za svoje delovanje združuje principe asimetrične kriptografije ter algoritmov za izračunavanje zgostitvene vrednosti katerihkoli podatkov v elektronski obliki. Pri elektronskem podpisovanju se vnaprej zbranim podatkom tako doda kriptirano sporočilo, ki vključujejo t.i. povzetek vsebine teh podatkov. S preprosto primerjavo dodanega elektronskega podpisa ter povzetka vsebine je možno zagotovo ugotoviti, ali so bili izbrani podatki spremenjeni v času od podpisa do preverjanja podpisa, poleg tega pa je zaradi uporabe para ključev možno preveriti tudi identiteto podpisnika. Časovni žigi delujejo na istem matematičnem principu, le da namesto osebe (podpisnika) povežejo vnaprej izbran skupek podatkov s točnim datumom in časom podpisa. Oba načina podpisovanja oziroma žigosanja vsebin sta lahko zaradi tega učinkovito uporabljena tudi pri hrambi dokumentarnega gradiva v elektronski obliki.

Pri uporabi elektronskih podpisov in časovnih žigov v organih državne uprave, uprave samoupravnih lokalnih skupnosti ter s strani drugih pravnih in fizičnih oseb, kadar na podlagi javnih pooblastil opravljajo upravne naloge, je potrebno upoštevati tudi določbe Uredbe o upravnem poslovanju, ki vsebuje posebne zahteve glede uporabe elektronskih podpisov ter časovnih žigov.

ETZ 3.9.6.1

ISUD mora biti sposoben ohraniti informacijo, ki se nanaša na elektronske podpise, šifriranje in podrobnosti overitelja.

ETZ 3.9.6.2/a

ISUD mora podpirati uporabo elektronskih podpisov in časovnih žigov, ki temeljijo na infrastrukturi javnih ključev.

ETZ 3.9.6.3/a

ISUD mora vsebovati funkcionalnost, da vsakemu dokumentu dodaja enega ali več elektronskih podpisov, s čemer se odobri (avtorizira) vsebino dokumenta. Ta funkcionalnost mora biti omogočena vsakemu, ki ima pravico do takšnega podpisovanja dokumentov.

ETZ 3.9.6.4

ISUD mora biti sposoben zaščititi dokument pred spreminjanjem takoj po tem, ko je dokumentu dodan elektronski podpis.

ETZ 3.9.6.5/a

ISUD mora imeti strukturo, ki dovoljuje enostavno uvajanje različnih tehnologij elektronskega podpisa.

ETZ 3.9.6.6/a

ISUD mora biti sposoben preveriti veljavnost elektronskega podpisa ali časovnega žiga. Postopek verifikacije elektronskega podpisa mora vsebovati najmanj:

- veljavnost podpisnikovega digitalnega potrdila (ni potekel, ni v CRL, overil ga je ustrezni izdajatelj);
- veljavnost izdajateljevega potrdila;
- veljavnost podpisa na podatkih;
- veljavnost časovnega žiga ali oznake, kjer je potrebno zagotoviti varno beleženje vrednosti in digitalnih podpisov;
- uporabniku morajo biti prikazani v berljivi obliki vsi ključni podatki o opravljeni verifikaciji podpisa.

ETZ 3.9.6.7

ISUD mora biti sposoben obdržati in shraniti kot metapodatke podrobnosti o postopku preverjanja elektronskega podpisa, vključujoč:

- dejstvo, da je bila preverjena veljavnost nekega elektronskega podpisa;
- overitelja potrdil, pri katerem je bil podpis overjen;
- datum in čas preverjanja.

ISUD mora podpirati zanesljivo dodajanje teh metapodatkov samemu gradivu.

ETZ 3.9.6.8/a

ISUD mora biti sposoben preveriti veljavnost elektronskega podpisa in časovnega žiga v trenutku zajetja dokumenta.

ETZ 3.9.6.9/a

ISUD mora vključevati funkcije, ki omogočajo vzdrževanje celovitosti dokumentov, ki imajo elektronske podpise (in dokazati, da je bila celovitost ohranjena), čeprav skrbnik spremeni nekaj metapodatkov, toda ne vsebine dokumenta, potem ko je dokument elektronsko podpisan.

ETZ 3.9.6.10/a

ISUD mora biti z elektronskim dokumentom sposoben shraniti:

- elektronske podpise, povezane s tem dokumentom;
- časovne žige, povezane s tem dokumentom;
- digitalna potrdila, ki overjajo podpis;
- katerekoli potrjujoče sopodpise, ki jih doda overitelj na tak način, da jih je mogoče najti v povezavi z dokumentom in brez škode za integriteto podatkov za elektronsko podpisovanje kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
- druge elektronsko podpisane ali časovno žigosane varnostne vsebine, potrebne za dolgoročno preverjanje veljavnosti hranjenega gradiva, kot npr.:
    - podatki iz registra preklicanih potrdil;
    - celotna veriga kvalificiranih potrdil ali časovnih žigov, ki izhajajo iz dokumenta.

ETZ 3.9.6.11/a

ISUD mora za potrebe verifikacije elektronskega podpisa upoštevati zahteve, ki so podane v splošno priznanih in uveljavljenih standardih s tega področja, ki so našteti v prilogi 2 enotnih tehnoloških zahtev.

Varnostno šifriranje

Varnostno šifriranje je pomembno pri hrambi podatkov z občutljivo vsebino, kjer je potrebno zagotoviti dodatne varnostne ukrepe, da bi vsebino zaščitili pred nepooblaščenim dostopom ali vpogledom. Pri šifriranju se elektronski dokument s pomočjo posebnega algoritma spremeni v nerazpoznavno obliko, katero je možno spremeniti nazaj v berljivo ali razumljivo obliko le z uporabo šifrirnega ključa.

ETZ 3.9.6.12

Kjer je bil elektronski dokument poslan ali prejet v šifrirani obliki z aplikacijo, ki je povezana z ISUD-om, mora biti ISUD sposoben omejiti dostop do tega dokumenta na uporabnike, ki so navedeni kot nosilci pripadajočega (odgovarjajočega) ključa za dešifriranje in poleg tega še v povezavi s katerimkoli drugim nadzorom dostopa, ki je dodeljen temu dokumentu.

ETZ 3.9.6.13

Kjer je bil elektronski dokument prenesen v šifrirani obliki s programsko aplikacijo, ki je povezana z ISUD-om, mora biti ISUD sposoben skupaj z dokumentom obdržati kot metapodatke:

- dejstvo, da je bil izveden šifriran prenos;
- vrsto algoritma;
- raven uporabljenega šifriranja.

ETZ 3.9.6.14/a

ISUD mora biti sposoben zagotoviti zajem šifriranih dokumentov neposredno iz aplikacije, ki ima sposobnost za šifriranje, in omejiti dostop na tiste uporabnike, ki so navedeni kot nosilci pripadajočega (odgovarjajočega) ključa za dešifriranje.

ETZ 3.9.6.15/a

ISUD mora pri uvozu ali zajetju dokumenta dovoliti odstranitev šifriranja. Ta funkcija je lahko zaželena v nekaterih zelo obsežnih arhivih dokumentov, za katere je zahtevan dolgoročen dostop (ker šifriranje lahko dolgoročno zmanjša možnost za branje dokumentov). V tem primeru se organizacija lahko opre na revizijsko sled ali podobno informacijo za dokaz, da je bilo šifriranje prisotno, vendar odstranjeno.

ETZ 3.9.6.16/a

ISUD mora imeti strukturo, ki dovoljuje enostavno uvajanje različnih tehnologij šifriranja.

Elektronski vodni znaki in drugo

Pri hrambi dokumentov, ki vsebujejo slikovni, avdio ali video material, za označevanje izvora ali lastništva elektronski podpisi ne pridejo v poštev, temveč je potrebno uporabiti nekoliko drugačno tehnološko rešitev. Elektronski vodni znaki in druge podobne tehnologije so največkrat uporabni za zaščito intelektualne lastnine. Z njimi se na bitno sliko naloži kompleksen viden ali neviden vzorec, katerega je moč odstraniti le z uporabo pravega algoritma in varnostnega ključa. Podobne tehnologije so v uporabi tudi za zaščito video ali avdio vsebine.

ETZ 3.9.6.17

ISUD mora biti sposoben hraniti dokumente, ki nosijo elektronske vodne znake in jih shranjevati skupaj z informacijami o vodnem znaku.

ETZ 3.9.6.18

ISUD mora biti sposoben spet priklicati informacije, shranjene v elektronskih vodnih znakih.

ETZ 3.9.6.19

ISUD mora imeti strukturo, ki dovoljuje enostavno vpeljavo različnih tehnologij za vodne znake.

3.9.7 Kombinirana hramba

Kljub infrastrukturi in sistemom, ki omogočajo hrambo gradiva v elektronski obliki, še vedno obstaja gradivo, ki obstaja le v fizični obliki, njegova pretvorba v elektronsko obliko pa zaradi takšnih ali drugačnih razlogov še ni bila izvedena. Sistemi za upravljanje in hrambo gradiva morajo zaradi dejstva, da so dokumenti, ki obstajajo v neelektronski, fizični obliki, in dokumenti v elektronski obliki, lahko vsebinsko ali na drug način povezani, podpirati tudi hrambo neelektronskih dokumentov ter hrambo kombiniranih zadev.

Upravljanje neelektronskih dokumentov

Skladišče dokumentov organizacije lahko vsebuje dokumente na papirju in drugih nosilcih zapisa, kot so video-, avdio kasete, ter tudi elektronske dokumente. ISUD naj bi bil sposoben evidentirati fizične zadeve po istem klasifikacijskem načrtu kot elektronske

dokumente in zagotoviti upravljanje »kombiniranih zadev« elektronskih in fizičnih dokumentov.

ETZ 3.9.7.1

ISUD mora biti sposoben definirati fizične zadeve v klasifikacijskem načrtu in dovoliti, da fizične dokumente v teh zadevah prikazujemo in upravljamo na enak način kot elektronske.

ETZ 3.9.7.2

ISUD mora definirati v klasifikacijskem načrtu zadeve, ki (logično) vsebujejo tako elektronske kot tudi fizične dokumente in mora dovoliti, da obe vrsti dokumentov upravljamo na povezan način. Te zadeve se v tej specifikaciji imenujejo 'kombinirane zadeve'. V praksi bodo kombinirane zadeve vsebovale tako elektronske kot fizične zadeve.

ETZ 3.9.7.3

ISUD mora dovoljevati fizični zadevi, ki je kot kombinirana povezana z elektronsko, uporabo istega naslova datoteke in številčne referenčne kode, toda z dodano navedbo, da gre za kombinirano zadevo.

ETZ 3.9.7.4

ISUD mora dovoljevati oblikovanje različnih naborov metapodatkovnih elementov za fizične in elektronske zadeve. Metapodatki za fizične zadeve morajo vključevati informacijo o fizični lokaciji fizične zadeve.

ETZ 3.9.7.5/a

ISUD mora podpirati sledenje fizičnih zadev z uporabo pripomočkov za odjavo, prijavo in posredovanje naprej, ki odražajo trenutno lokacijo zadeve.

ETZ 3.9.7.6

ISUD mora zagotoviti, da priklic kombinirane zadeve prikliče tudi metapodatke za elektronske in fizične dokumente, ki so povezani z njo.

ETZ 3.9.7.7/a

Kjer imajo zadeve stopnjo in vrsto tajnosti, mora ISUD zagotavljati, da kombinirani fizični zadevi dodelimo enako stopnjo in vrsto tajnosti kot povezani kombinirani elektronski zadevi.

ETZ 3.9.7.8

ISUD mora vključevati sposobnosti za nadzor in zabeležiti dostop do fizičnih zadev, vključno z nadzorom, ki temelji na stopnjah tajnosti. Le-te pa so primerljive s funkcijami za elektronske zadeve.

ETZ 3.9.7.9/a

ISUD mora podpirati tiskanje in prepoznavanje črtnih kod ali druge sisteme sledenja z samodejnim vnosom podatkov za sledenje gibanju fizične zadeve.

Upravljanje s kombiniranimi zadevami

ETZ 3.9.7.10

ISUD mora podpirati dodeljevanje rokov hrambe vsaki fizični zadevi v klasifikacijskem načrtu. Roki morajo delovati skladno z roki hrambe za elektronske dokumente. Opozoriti morajo skrbnika, ko pride datum za odbiranje in izločanje, toda z upoštevanjem, da so procesi uničevanja ali arhiviranja pri papirnih dokumentih drugačni kot pri elektronskih.

ETZ 3.9.7.11

ISUD mora podpirati uporabo enakih rokov hrambe tako za fizične kot elektronske zadeve, ki sestavljajo kombinirano zadevo.

ETZ 3.9.7.12

ISUD mora biti sposoben upoštevati vsako revizijo odločitve, ki je bila narejena na kombinirani elektronski zadevi, tudi na kombinirani fizični zadevi, ki ji je pridružena.

ETZ 3.9.7.13

ISUD mora opozoriti skrbnika na obstoj in lokacijo vsake kombinirane fizične zadeve, povezane s kombinirano elektronsko zadevo, ki naj bi jo izvozili ali prenesli.

ETZ 3.9.7.14

ISUD mora biti sposoben zapisati v revizijsko sled vse spremembe, narejene na metapodatkih, povezanih s fizičnimi ali kombiniranimi zadevami in dokumenti.

ETZ 3.9.7.15/a

ISUD mora podpirati izvedbo revizijskih odločitev, narejenih na skupini zadev, na katerikoli fizični zadevi te skupine, in opozarjati skrbnika na postopke, ki jih je treba izvesti na fizični zadevi.

ETZ 3.9.7.16/a

ISUD mora biti sposoben izvoziti in prenesti metapodatke fizičnih dokumentov in zadev.

ETZ 3.9.7.17/a

ISUD mora biti sposoben zagotoviti pripomočke za odjavo in prijavo fizičnih zahtev, vnesenih v sistem. Predvsem bi moral omogočiti zapis posameznega uporabnika ali lokacije, kjer je fizična zadeva odjavljena, ter prikaz teh informacij, če je fizično zadevo zahteval drug uporabnik.

ETZ 3.9.7.18/a

ISUD mora biti sposoben za fizične zadeve, vnesene v sistem, zagotoviti zmožnost za posredovanje naprej, tako da bi omogočil uporabniku vnesti datum posredovanja ali rezervni datum za fizično zadevo in izdelati dosledno poročilo ter ga posredovati trenutnemu skrbniku te zadeve ali skrbniku – odvisno od nastavitve programa.

3.10 ZAHTEVE GLEDE ARHIVSKEGA GRADIVA

ZVDAGA vsebuje nekatere določbe, ki urejajo izročanje hranjenega gradiva arhivu, ki je pristojen za hrambo arhivskega gradiva. Določeno dokumentarno gradivo, katerega hranijo javnopravne, fizične ali pravne osebe, je lahko ob izpolnjenih pogojih odbrano za arhivsko gradivo. Javnopravne osebe iz dokumentarnega gradiva odberejo arhivsko gradivo po strokovnih navodilih pristojnega arhiva, dokumentarno gradivo pravnih in fizičnih oseb pa državni arhiv določi za arhivsko gradivo z odločbo (34. člen ZVDAGA).

Ker ZVDAGA določa, da javno arhivsko gradivo hranijo le pristojni arhivi (36. člen), morajo vse osebe, čigar dokumentarno gradivo je odbrano za arhivskega, to gradivo pristojnim arhivom tudi izročiti. Oblika ali nosilec zapisa pri postopku izročitve nimata bistvenega pomena, saj dolžnost predaje obstaja ne glede nanju.

Nekoliko drugačne določbe veljajo za zasebno arhivsko gradivo. To je last fizičnih in pravnih oseb zasebnega prava, te pa ga ob izpolnjenih zakonskih pogojih (45. člen ZVDAGA) lahko hranijo sami, lahko pa ga predajo v hrambo tudi pristojnemu arhivu.

3.10.1 Izročanje arhivskega gradiva pristojnemu arhivu

ETZ 3.10.1.1

Pristojni arhiv določi obliko zapisa, nosilec zapisa in način izročitve arhivskega gradiva s strokovnimi navodili.

ETZ 3.10.1.2

Arhivsko gradivo se lahko izroča le v obliki za dolgoročno hrambo. Izročanje v kakršnikoli drugi obliki je možno le ob soglasju državnega arhiva.

ETZ 3.10.1.3

Filmsko arhivsko gradivo na analognem nosilcu se izroča v obliki končnega montiranega izdelka ter v obliki ogledne kopije, na sledečih nosilcih zapisa:

- Beta;
- Beta SP;
- VHS.

ETZ 3.10.1.4

Arhivsko gradivo na mikrofilmu se izroča v sledečih oblikah:

- arhivsko gradivo, čigar izvorna oblika je večja od formata A3, tehnična dokumentacija, časopisi karte, knjige in za vse drugo arhivsko gradivo se izroča na mikrofilmu v roli, širine 35 mm;
- s predhodno pridobljeno potrditvijo Arhiva RS se lahko arhivsko gradivo izroča tudi na mikrofilmu v roli, širine 16mm;
- mikrofiš formata A6 8148 X 105 mm.

3.10.2 Hramba arhivskega gradiva v arhivu

ETZ 3.10.2.1

Arhiv hrani arhivsko gradivo v obliki zapisa za dolgoročno hrambo v skladu z zakonom, uredbo in določbami tega dokumenta.

3.10.3 Objava arhivskega gradiva na svetovnem spletu

ETZ 3.10.3.1

Arhivi lahko brezplačno dostopnost arhivskega gradiva na svetovnem spletu v sledečih primerih zagotavljajo z uporabo vpoglednih različic gradiva:

- objava arhivskega gradiva, ki v elektronski obliki zaradi svoje velikosti ni primerno za objavo na spletu; za presojanje primernosti se upoštevajo uveljavljene prenosne zmogljivosti svetovnega spleta in pravila stroke;
- objava arhivskega gradiva, ki zaradi varstva avtorske in sorodnih pravic ali pravic industrijske lastnine ne more biti objavljena v izvirniku;
- objava arhivskega gradiva, ki ne obstaja v izvirni digitalni obliki za dolgoročno hrambo.

ETZ 3.10.3.2

Vpogledna različica gradiva je katerakoli oblika zapisa, ki ustreza mednarodno uveljavljenim priporočilom ali standardom za spletne objave.

ETZ 3.10.3.3

Arhivi lahko za zagotavljanje varstva avtorske in sorodnih pravic ali pravic industrijske lastnine pri zagotavljanju brezplačne dostopnosti arhivskega gradiva na svetovnem spletu uporabljajo tehnična sredstva, ki izpolnjujejo naslednje kriterije:

- omogočajo različne ravni dostopa do arhivskega gradiva;
- ne omejujejo dostopa do arhivskega gradiva, ki ni zaščiteno z avtorsko in sorodnimi pravicami ali pravicami industrijske lastnine;
- način in vrsto dostopa do zaščitenega arhivskega gradiva omogočajo v skladu z dovoljenji nosilca avtorske ali sorodne pravice ali nosilca pravice industrijske lastnine in ne onemogočajo ali kako drugače neupravičeno ne omejujejo dostopa do zaščitenega arhivskega gradiva strožje, kot je to potrebno za zaščito avtorskih in sorodnih pravic ter pravic industrijske lastnine.

4 ZAHTEVE ZA PONUDNIKE OPREME IN STORITEV

4.1 SPLOŠNE ZAHTEVE ZA PONUDNIKE

4.1.1 Splošne zahteve

ETZ 4.1.1.1

Ponudniki opreme in storitev morajo zagotoviti, da so ponujana oprema in storitve skladna z zakonom, uredbo, temi zahtevami in drugimi veljavnimi predpisi.

4.1.2 Zaposlovanje strokovnjakov pri ponudnikih opreme in storitev

ETZ 4.1.2.1

Ponudnik storitev hrambe mora zaposlovati dve osebi z opravljenim strokovnim izpitom iz arhivistike, ki je predpisan s posebnim pravilnikom, ter ki s strokovnim usposabljanjem iz zahteve ETZ 4.1.3.1 obnavljata strokovno znanje.

ETZ 4.1.2.2

Ponudnik spremljevalnih storitev in ponudnik programske opreme za zajem ali hrambo mora zaposlovati najmanj eno osebo z opravljenim strokovnim izpitom iz arhivistike, ki je predpisan s posebnim pravilnikom, ter ki s strokovnim usposabljanjem iz zahteve ETZ 4.1.3.1 obnavljata strokovno znanje.

ETZ 4.1.2.3

Osebe iz zahtev ETZ 4.1.2.1 in ETZ 4.1.2.2 morajo biti pri ponudniku bodisi redno zaposlene, bodisi pri njem delo v zvezi s hrambo dokumentarnega gradiva opravljati pogodbeno. Če ima oseba sklenjeno tovrstno pogodbo z več ponudniki, se šteje, da pogoje iz enotnih tehnoloških zahtev izpolnjuje le tisti ponudnik, ki je osebo pri Arhivu Republike Slovenije prvi prijavil kot zaposleno osebo, ki opravlja delo v zvezi s hrambo dokumentarnega gradiva.

ETZ 4.1.2.4

Osebe, ki so v zaposlene v javni arhivski službi, se ne štejejo za osebe, ki izpolnjujejo pogoje iz zahtev ETZ 4.1.2.1 in ETZ 4.1.2.2.

4.1.3 Vrednotenje dodatnega strokovnega izobraževanja

ETZ 4.1.3.1

Osebe, zaposlene pri ponudnikih storitev hrambe, spremljevalnih storitev ali programske opreme za zajem in hrambo, obnavljajo strokovno znanje na strokovnih usposabljanjih z naslednjih področij:

- arhivistike v najširšem smislu,
- informatike,

- pravnih predpisov,
- upravljanja z dokumentarnim gradivom.

ETZ 4.1.3.2

Arhiv Republike Slovenije najmanj enkrat letno določi, s katerimi strokovnimi usposabljanji je mogoče pridobiti kreditne točke in koliko kreditnih točk prinaša posamezno strokovno usposabljanje. Arhiv lahko odločitev sprejem tudi na predlog organizatorja ali udeležencev izobraževanja.

Arhiv RS svojo odločitev objavi na svetovnem spletu.

Arhiv Republike Slovenije oceni posamezno strokovno usposabljanje na podlagi predvidene tematike, ravni strokovnosti oziroma izčrpnosti podajanja tematike, strokovne priznanosti predavateljev, morebitnega zaključnega preverjanja znanja in podobnih meril. Vsako posamezno strokovno usposabljanje lahko oceni z najmanj 0,1 kreditne točke in največ 2 kreditnima točkama.

Strokovna usposabljanja, kjer ni obveznega preverjanja udeležbe, lahko oceni z največ 0.5 kreditnih točk.

ETZ 4.1.3.3

Vsaka od teh oseb mora v treh letih po opravljenem preizkusu strokovne usposobljenosti pridobiti 2 kreditni točki za vsako področje in 5 kreditnih točk na področju svojega delovanja. V kolikor oseba v treh letih ne pridobi zadostnega števila točk, mora ponovno opravljati preizkus strokovne usposobljenosti

Osebi, ki je pridobila strokovni naslov za katerega od naštetih področij se prizna 5 točk za obdobje 3 let iz področja iz katerega je pridobila strokovni ali znanstveni naziv.

4.2 ZAHTEVE ZA PONUDNIKE STROJNE OPREME

ETZ 4.2.1

Ponudniki, ki na trgu ponujajo strojno opremo za zagotavljanje hrambe gradiva v elektronski obliki ali za zagotavljanje spremljevalnih storitev, morajo zagotoviti, da je strojna oprema skladna s temi zahtevami.

ETZ 4.2.2

Strojna oprema za zajem gradiva, hrambo gradiva in spremljevalne storitve mora biti skladna z mednarodnimi, državnimi in drugimi splošno priznanimi standardi.

Skladnost strojne opreme z mednarodnimi, državnimi in drugimi splošno priznanimi standardi ponudnik dokazuje s certifikati, veljavnimi v Evropski uniji ali drugimi svetovno poznanimi certifikati. Če takšni ne obstajajo, pa s certifikati, ki so uveljavljeni v drugih državah.

ETZ 4.2.3

Strojna oprema za zajem gradiva, hrambo gradiva in spremljevalne storitve mora biti mednarodno uveljavljena. Za mednarodno uveljavljenost se šteje, da je strojna oprema uveljavljena v najmanj treh državah Evropske unije, v katerih proizvajalec strojne opreme izvaja prodajo ter vzdrževalne storitve za strojno opremo.

Ponudnik strojne opreme dokazuje mednarodno uveljavljenost z izjavo proizvajalca.

ETZ 4.2.4

Ponudnik strojne opreme za zajem gradiva, hrambo gradiva in spremljevalne storitve mora zagotoviti podporo in vzdrževalne storitve za strojno opremo v Republiki Sloveniji.

ETZ 4.2.5

Ponudniki strojne opreme za zajem gradiva, hrambo gradiva in spremljevalne storitve mora zagotoviti primeren odzivni čas pri zagotavljanju podpore strojne opreme. Odzivni čas mora biti dokazan z ustreznim dokazilom (pogodba, splošni pogoji).

Za primeren odzivni čas se šteje odzivni čas začetka reševanja, ki ne presega enega delovnega dne.

ETZ 4.2.6/a

Strojna oprema mora biti glede na zahteve veljavnih predpisov in poslovne zahteve ter pravila stroke primerna za predvidene obremenitve in upravljanje s predvideno občutljivostjo in obsežnostjo gradiva. V skladu s tem Arhiv Republike Slovenije v primeru akreditacije posamezno strojno opremo glede na dokazila in priporočila proizvajalca in pravila stroke razvrsti v enega od naslednjih razredov z navedbo posamezne vrste nalog:

- strojna oprema za manj zahtevne naloge (manjše obremenitve oziroma manjša občutljivost ali obsežnost gradiva);
- strojna oprema za srednje zahtevne naloge (srednje obremenitve oziroma srednja občutljivost ali obsežnost gradiva);
- strojna oprema za zelo zahtevne naloge (velike obremenitve oziroma velika občutljivost ali obsežnost gradiva).

4.3 ZAHTEVE ZA PONUDNIKE STORITEV

4.3.1 Splošne zahteve za ponudnike storitev

ETZ 4.3.1.1

Ponudnik spremljevalnih storitev, mora izpolnjevati vse pogoje, ki jih določajo zakon, uredba in enotne tehnološke zahteve ter drugi veljavni predpisi. Poleg tega mora ponudnik spremljevalnih storitev upoštevati tudi predpise, ki zavezujejo osebo, za katero izvaja storitve.

Akreditacija za izvajanje storitev se lahko podeli na podlagi že akreditirane strojne in programske opreme ali pa se akreditacija za strojno in programsko opremo podeli v okviru storitev. V slednjem primeru akreditacija strojne in programske opreme velja le v okviru akreditiranih storitev.

ETZ 4.3.1.2

Ponudnik storitev mora sprejeti notranja pravila, v katerih določi organizacijo, način in postopke zagotavljanja posamezne spremljevalne storitve v skladu z zakonom, uredbo, temi zahtevami in drugimi veljavnimi predpisi ter jih potrditi pri Arhivu RS.

ETZ 4.3.1.3/a

Ponudnik storitev hrambe mora v notranjih pravilih predvideti sistem neodvisnega reševanja sporov pred od ponudnika neodvisno organizacijo.

ETZ 4.3.1.4

Pri zagotavljanju storitev mora ponudnik poskrbeti za glede na občutljivost in obsežnost gradiva primerno število notranjih in zunanjih revizij.

ETZ 4.3.1.5

Ponudnik storitve in naročnik storitve morata pred začetkom izvajanja storitve poskrbeti za pripravo skupne ocene tveganja za posamezno storitev v obliki pisnega dokumenta, ki mora vsebovati najmanj:

- vrste in stopnjo tveganja pri zagotavljanju posamezne storitve,
- opis posameznih postopkov ali elementov storitve glede na vrsto in stopnjo tveganja,
- porazdelitev odgovornosti med ponudnikom in naročnikom glede na postopke ali elemente storitve.

4.3.2 Zahteve za ponudnike spremljevalnih storitev

ZVDAGA poleg storitev hrambe gradiva in strojne ter programske opreme, s pomočjo katere se hramba dokumentarnega ali arhivskega gradiva lahko izvaja, predvideva tudi zagotavljanje spremljevalnih storitev. Spremljevalne storitve so eksemplifikativno naštete tudi v Uredbi o varstvu dokumentarnega in arhivskega gradiva (23. člen):

- zajem dokumentarnega gradiva v elektronski obliki,
- zajem dokumentarnega gradiva v fizični obliki,
- pretvorba dokumentarnega gradiva iz fizične v elektronsko obliko,
- pretvorba dokumentarnega gradiva iz elektronske oblike v obliko za dolgoročno hrambo,
- urejanje ali odbiranje dokumentarnega gradiva v elektronski obliki,
- urejanje ali odbiranje dokumentarnega gradiva v fizični obliki,
- uničevanje dokumentarnega gradiva v elektronski obliki,
- uničevanje dokumentarnega gradiva v fizični obliki,
- zagotavljanje varnih prostorov za hrambo gradiva v elektronski obliki,
- druge storitve, ki kakor koli posegajo v celovitost, varnost ali avtentičnost dokumentarnega gradiva.

ETZ 4.3.2.1

Vsaka posamezna spremljevalna storitev mora izpolnjevati ustrezne zahteve iz enotnih tehnoloških zahtev, ki se nanašajo na izvajanje te spremljevalne storitve.

ETZ 4.3.2.2

Ponudnik spremljevalnih storitev mora naročniku v notranjih pravilih predvideti in omogočiti dostop in pregled statistike ali zapisov napak, ki se pojavljajo pri zagotavljanju posamezne spremljevalne storitve.

ETZ 4.3.2.3/a

Notranja pravila ponudnika spremljevalne storitve urejanja, odbiranja oziroma uničevanja morajo poleg splošnih določil iz podpoglavja 4.3.1 vsebovati tudi določila glede izvajanja postopkov na način, ki ga predvidevajo veljavni predpisi s področja varstva arhivskega gradiva.

ETZ 4.3.2.4

Notranja pravila ponudnika spremljevalne storitve zagotavljanja varnostnih prostorov morajo poleg splošnih določil iz podpoglavja 4.3.1. vsebovati tudi natančna določila o obsegu posamezne storitve (npr. zgolj varni prostor, varni prostor z zagotovljenimi energenti in okoljskimi pogoji, varni prostor in informacijsko komunikacijska infrastruktura ter podobno).

5 ZAČETEK VELJAVNOSTI

Te enotne tehnološke zahteve začnejo veljati 01.12.2006

Ljubljana, 01. December 2006

Dr. Matevž Košir
Direktor

PRILOGE

Priloga 1 – Seznam oblik zapisa za dolgoročno hrambo, ki ustrezajo zahtevam ETZ

Poleg mednarodnih standardov in priporočil so v seznamu navedeni tudi ustrezajoči slovenski standardi, če ti obstajajo.

- Tekstovni in mešani dokumenti:
  - ISO Latin-1 – ISO 8859-1
  - PDF/A - ISO 19005-1
  - XML - SGML – ISO 8879
  - ODF – ISO/IEC 26300
- Grafični dokumenti:
  - TIFF – ISO 12639
  - SVG – v1.1 – W3C Specification
- Kompresija:
  - LZW – barvni dokumenti
  - CCIT group 4 – č/b dokumenti
- Film/Video/Audio:
  - ANSI/SMPTE 268M
  - MPEG-2 - ISO/IEC 13818
  - MPEG-4 - ISO/IEC 14496

Priloga 2 – Seznam mednarodnih standardov in priporočil

Poleg mednarodnih standardov in priporočil so v seznamu navedeni tudi ustrezajoči slovenski standardi, če ti obstajajo.

- Informacijska varnost:
  - ISO/IEC 27001, Information security management systems
  - ISO/IEC 17799, Code of practice for information security management
  - ISO/IEC TR 18044, Information technology. Security techniques. Information Security incident management
  - ISO/IEC 12207, Software lifecycle processes

- Elektronski podpisi:
  - ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES)
  - ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI)
    - SIST-TS ETSI/TS 101 733 V1.5.1:2005, Elektronski podpisi in infrastruktura (ESI) – Formati elektronskega podpisa
  - CWA 14171, General guidelines for Electronic Signature Verification

- Upravljanje z dokumenti, hramba dokumentarnega in arhivskega gradiva in sorodni standardi:
  - BS 5454, Recommendations for the storage and exhibition of archival documents
  - ISO 14721, Space data and information transfer systems - Open archival information system - Reference model
  - ISO 15489, Information and documentation - Records management, vsi deli
    - SIST ISO 15489-1:2005, Informatika in dokumentacija – Upravljanje zapisov – 1. del: Splošno
    - SIST-TP ISO/TR 15489-2:2005, Informatika in dokumentacija – Upravljanje zapisov – 2. del: Smernice
  - ISO 23081, Information and documentation - Records management processes - Metadata for records, vsi deli
  - ISO 8601 - Data elements and interchange formats - Information interchange - Representation of dates and times
    - SIST EN 28601:2004, Podatkovni elementi in izmenjevalni formati – Izmenjava informacij – Prikaz datuma in časa (ISO 8601:1988 in tehnični popravek 1:1991)
  - ISO 2788 - Documentation -- Guidelines for the establishment and development of monolingual thesauri

        - SIST ISO 2788:1996, Dokumentacija - Smernice za zasnovo in razvoj enojezičnih tezavrov
    - ISO 5964 - Documentation -- Guidelines for the establishment and development of multilingual thesauri
        - SIST ISO 5964:1996, Dokumentacija - Smernice za zasnovo in razvoj večjezičnih tezavrov

- Oblike zapisa in nosilci zapisa:
    - ISO/IEC 8859, 8-bit single-byte coded graphic character sets, vsi deli
        - SIST ISO 8859-1:1995, Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1, osnova ISO 8895-1:1987
        - SIST ISO 8859-2:1995, Information processing - 8-bit single byte coded graphic character sets - Part 2: Latin alphabet No. 2, osnova ISO 8895-2:1987
    - ISO 8879 - Information processing - Text and office systems - Standard Generalized Markup Language (SGML)
    - ISO 19005 - Document management - Electronic document file format for long-term preservation, vsi deli
    - ISO 12639 - Graphic technology - Prepress digital data exchange - Tag image file format for image technology (TIFF/IT)
        - SIST ISO 12639:2004 - Graphic technology - Prepress digital data exchange - Tag image file format for image technology (TIFF/IT)
    - ISO/IEC 13818 - Information technology - Generic coding of moving pictures and associated audio information, vsi deli
        - SIST ISO/IEC 13818-1:2005 - Informacijska tehnologija – Splošno kodiranje premikajočih slik in pripadajočih avdio informacij: Sistemi
        - SIST ISO/IEC 13818-2:2005 - Informacijska tehnologija – Splošno kodiranje premikajočih slik in pripadajočih avdio informacij: Video
    - ISO/IEC 14496 – Information technology - Coding of audio-visual objects, vsi deli
        - SIST ISO/IEC 14496-10:2005, Informacijska tehnologija – Kodiranje avdio-vizualnih objektov – 10. del: Napredno video kodiranje za splošne avdiovizualne storitve, osnova: ISO/IEC 14496-10:2004
    - ANSI/SMPTE 268 - File Format for Digital Moving-Picture Exchange
    - NIST Special Publication 500-252 - Care and Handling of CDs & DVDs -- A Guide for Librarians and Archivists
    - BS 4783, Storage, transportation and maintenance of media for use in data processing and information storage
    - ISO 18921, Imaging materials -- Compact discs (CD-ROM) -- Method for estimating the life expectancy based on the effects of temperature and relative humidity

- ISO 18923, Imaging materials - Polyester-base magnetic tape - Storage practicesISO 18925 Imaging materials - Optical disc media - Storage practices
- ISO 18926 Imaging materials - Information stored on magneto-optical (MO) discs - Method for estimating the life expentancy based on the effects Of temperature and relative humidity)
- ISO 18927 Imaging materials - Recordable compact disc systems - Method for estimating the life expentancy based on the effects of temperature and relative humidity
- ISO/IEC 11172, Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s, vsi deli

- Standardi za film in mikrofilm:

  - ISO 18928, Imaging materials - Unprocessed photographic films and papers - Storage practices
  - ISO 10356, Cinematography - Storage and handling of nitrate-base motion-picture films
  - ISO 18915, Imaging materials - Methods for the evaluation of the effectiveness of chemical conversion of silver images against oxidation
  - ISO 14523, Photography - Processed photographic materials - Photographic activity test for enclosure materials
  - ISO 18901, Imaging materials - Processed silver-gelatin type black-and-white films - Specifications for stability
  - ISO 18902, Imaging materials - Processed photographic films, plates and papers - Filing enclosures and storage containers
  - ISO 18906, Imaging materials - Photographic films - Specifications for safety film
  - ISO 18911, Imaging materials - Processed safety photographic films - Storage practices
  - ISO 18918, Imaging materials - Processed photographic plates - Storage practices
  - ISO 18912, Imaging materials - Processed vesicular photographic film - Specifications for stability
  - ISO 18916, Imaging materials - Processed imaging materials - Photographic activity test for enclosure materials
  - ISO 18917, Photography - Determination of residual thiosulfate and other related chemicals in processed photographic materials - Methods using iodine-amylose, methylene blue and silver sulfide
  - ISO 18919, Imaging materials -- Thermally processed silver microfilm -- Specifications for stability
  - ISO 18920, Imaging materials - Processed photographic reflection prints - Storage practices

- ISO 18924, Imaging materials - Test method for Arrhenius-type predictions
- ISO 18909, Photography - Processed photographic colour films and paper prints - Methods for measuring image stability
- ISO 6199, Micrographics - Microfilming of documents on 16 mm and 35 mm silver-gelatin type microfilm - Operating procedures
- ISO 18905, Imaging materials - Ammonia-processed diazo photographic film - Specifications for stability
- ANSI/AIIM MS111, Micrographics -- Standard Recommended Practice for Microfilming Printed Newspapers on 35mm Roll Microfilm
- ANSI/AIIM MS14, Specifications for 16 & 35mm Roll Microfilm
- ANSI/AIIM MS18, Micrographics - Splices for Imaged Film - Dimensions and Operational Constraints
- ANSI/AIIM MS19, Recommended Practice For Identification of Microforms
- ANSI/AIIM MS23, Practice for Operational Procedures/Inspection and Quality Control of First-Generation Silver-Gelatin Microfilm of Documents
- ANSI/AIIM MS26, 35mm Planetary Cameras (Top-Light) - Procedures for Determining Illumination Uniformity of Microfilming Engineering Drawings
- ANSI/AIIM MS29, Micrographics - Cores and Spools for Microfilm Recording Equipment – Dimensions
- ANSI/AIIM MS34, Dimensions for Reels Used for Conventionally Threaded Processed 16mm and 35mm Microfilm
- ANSI/AIIM MS35, Requirements and Characteristics of Original Black-and-White Documents that May Be Microfilmed
- ANSI/AIIM MS43, Recommended Practice for Operational Procedures/Inspection and Quality Control of Duplicate Microforms of Documents and from COM
- ANSI/AIIM MS45, Information and Image Management - Recommended Practice for the Inspection of Stored Silver-Gelatin Microforms for Evidence of Deterioration
- ISO 3334, Micrographics - ISO Resolution Test Chart No. 2 - Description and Use
- ANSI/AIIM TR26, Resolution as it Relates to Photographic and Electronic Imaging.
- ANSI/AIIM TR09, Color Microforms
- ANSI/AIIM TR13, Preservation of Microforms in an Active Environment – Guidelines
- ANSI/AIIM TR20, Environmental and Work Place Safety Regulations Affecting Microfilm Processors
- ANSI/AIIM TR04, Silver Recovery Techniques
- ISO 18917, Photography - Determination of residual thiosulfate and other related chemicals in processed photographic materials - Methods using iodine-amylose, methylene blue and silver sulfide
- ANSI/AIIM MS5, Micrographic Microfiche

- ANSI/NISO Z39.62, Eye-Legible Information on Microfilm Leaders and Trailers and on Containers of Processed Microfilm on Open Reels

- Standardi za ravnanje s storitvami IT:
  - ISO 20000, Information technology - Service management, vsi deli
- Drugi standardi:
  - ISO 9075 - Information technology -- Database languages – SQL, vsi deli