UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA PONUDBE STORITEV OHRANJANJA ELEKTRONSKEGA DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA V SLOVENIJI IN IZBRANIH DRŽAVAH EU

Ljubljana, marec 2014 JUDITA MESARIČ

IZJAVA O AVTORSTVU

Spodaj podpisana Judita Mesarič, študentka Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtorica magistrskega dela z naslovom Analiza ponudbe storitev ohranjanja elektronskega dokumentarnega in arhivskega gradiva v Sloveniji in izbranih državah EU, pripravljenega v sodelovanju s svetovalko prof.dr. Mojco Indihar Štemberger.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisala;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 2.6.2014 Podpis avtorice:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Uporaba informacijske tehnologije na vseh področjih našega življenja povzroča tudi spremembe v načinu nastajanja, izmenjave in ohranjanja informacij. Informacijska revolucija ni povzročila samo hitrejšega iskanja in prenosa informacij, temveč tudi njihovega hitrejšega in količinsko večjega nastajanja. Posledično pa se vedno bolj srečujemo tudi s težavami pri ohranitvi takšnih informacij za naše zanamce. Vsesplošno navdušenje nad vedno novimi tehnologija in načini komuniciranja povzroča, da ljudje spreminjajo svoje navade proizvajanja in izmenjave informacij hitreje, kot v ozadju nastaja tehnologija, ki bi omogočala ohranjanje novonastalih informacij (Gladney, 2007, str. 8).

Nove pojavne oblike informacij (SMS sporočila, spletne interaktivne vsebine, multimedijske vsebine, socialna omrežja itd..) pa predstavljajo, poleg izziva ohranjanja takšnih vsebin, še dodaten izziv omogočanja ponovne uporabe takšnih vsebin na enak način in v enakem obsegu kot ob nastanku. V osebnem in poslovnem življenju se srečujemo s postopki, ki za seboj ne puščajo nobenih papirnih sledi, temveč se dogajajo od začetka do konca v digitalnem svetu. Nekateri, tako nastali dokumenti in podatki, so lahko del kulturne ali pravne dediščine naroda oz. posameznika, ki jo je treba v skladu z arhivsko stroko ohranjati za naše zanamce.

Žontar (2003, str. 23) ugotavlja, da varstvo arhivskega gradiva obsega vse postopke in ukrepe, katerih namen je zagotoviti trajen obstoj arhivskega gradiva in njegovo uporabo. Žumer (2007, str. 30-31) tudi navaja 5 temeljnih načel varstva dokumentarnega in arhivskega gradiva oz. uporabnosti njegove vsebine in sicer načelo varstva arhivskega gradiva kot kulturnega spomenika, načelo uporabnosti, načelo trajnosti, načelo celovitosti, ki vsebuje zahtevo po nespremenjenosti, avtentičnosti in integralnosti, ter načelo dostopnosti.

Digitalno gradivo, ki nastaja vsakodnevno, je lahko dokumentarno gradivo, ki ima z različnimi predpisi določene roke hrambe, ki so običajno časovno omejeni. Gradivo pa je lahko že ob nastanku ali kasneje, s spremembo predpisov ali z odločitvijo pristojnega arhiva, označeno za arhivsko. V tem primeru gre za ohranjanje gradiva brez časovnih omejitev hrambe. Za obe vrsti gradiva mora ustvarjalec ves čas hrambe – bodisi do uničenja gradiva ali do predaje gradiva pristojnemu arhivu, zagotoviti uporabnost tega gradiva in dokazljivost njegove avtentičnosti.

V primeru, da je rok hrambe omejen na krajše časovno obdobje, to za ustvarjalca ne predstavlja večjega problema, saj uporabnost običajno zagotavljajo višje verzije programske opreme, ki vključujejo module za uporabo dokumentov, ki so nastali v nižjih verzijah programske opreme. Seveda pa se ta povezljivost za nazaj ne more uporabljati v nedogled, saj se programska oprema ne spreminja samo po verzijah, ampak predvsem nastaja nova, ki ne zagotavlja vedno povezljivosti s podobnimi programskimi produkti v

preteklosti. Takšen primer je MS Excel 2010, ki ne podpira več formatov DBASE II, MS Excel 2003 pa jih še podpira (File formats that are supported in Excel, 2014).

V primeru arhivskega gradiva pa so postopki za ohranjanje gradiva v skladu z arhivsko stroko bolj zapleteni in za ohranjanje avtentičnosti, uporabnosti, celovitosti in dostopnosti nikakor ne zadoščajo več samo tehnološki ukrepi. Za preprečevanje tehnološke zastarelosti je najpomembnejše proaktivno delovanje v smislu spremljanja zastarevanja opreme in pravočasnega ukrepanja. Vendar s tem rešimo samo problema dostopnosti in uporabnosti, za zagotavljanje vsega ostalega pa so ključnega pomena ustrezni organizacijski ukrepi, tako na področju informacijske varnosti, kot tudi obvladovanja dokumentov.

Problematika dolgotrajnega ohranjanja digitalnega gradiva je širša, kot samo prenos iz enega datotečnega formata v drugega. Zadeva vse države, vse inštitucije, bodisi državne ali z državnimi pooblastili, na koncu pa se tiče tudi vsakega posameznika, ki kakorkoli sodeluje z državno in javno upravo. Arhivska stroka in inštitucije na tem področju se zavedajo težav že več kot dve desetletji, zato so na področju obvladovanja, hrambe, varovanja in upravljanja z dokumentarnim in arhivskim gradivom v digitalni obliki nastali številni standardi, predpisi in v posameznih državah tudi zakonodaja.

Storitve hrambe gradiva v digitalni obliki so storitve, ki so, po Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Ur.l. RS, št. 30/2006, v nadaljevanju ZVDAGA), neločljivo povezane z ohranjanjem vsebine gradiva v digitalni obliki. Hramba mora slediti temeljnim načelom varovanja arhivskega gradiva, ki so trajnost, celovitost in dostopnost (ZVDAGA, 3., 4. in 5 člen). Za vzpostavitev storitve elektronskega arhiva (skrbništva gradiva) pa moramo zagotoviti tudi trajno uporabnost tega gradiva. Ponudniki storitve zajema in hrambe torej lahko zagotavljajo samo hrambo, brez zagotavljanja dolgotrajne uporabnosti hranjenega gradiva. Zakonodaja v posameznih državah EU se tudi na tem področju zelo razlikuje. Problem ni samo v natančnem definiranju skrbništva gradiva, temveč tudi v zagotavljanju nadzora nad trgom ponudnikov – tako v izpolnjevanju zakonskih kot tudi strokovno arhivskih zahtev.

S pojavom digitalnih podatkov v najrazličnejših oblikah pa za ponudnike storitve zajema in hrambe in tudi državne arhive, ki so temeljna institucija za zagotavljanje skrbništva nad digitalnim arhivskim gradivom, prihaja obdobje, ko bo skrbništvo takšnega gradiva predvsem tehnološki problem zagotavljanja njegove nadaljnje uporabe vsaj na podoben način, kot je bilo gradivo v uporabi pred predajo skrbnikom v začasno ali pristojnim arhivom v trajno hrambo. Z zagotavljanjem ustrezne hrambe se ponudniki storitve srečujejo z organizacijskimi in predvsem z velikimi finančnimi bremeni, ki jih morajo skozi trženje storitve pokriti. Na drugi strani pa se srečujejo države, zakonodajalci, javni in državni arhivi s pripravo in izvajanjem zakonodaje, na koncu pa tudi z nadzorom izvajanja zakonodaje pri ponudnikih storitve.

Namen magistrskega dela je raziskati aktualno problematiko na področju ohranjanja in skrbništva digitalnega gradiva pri ponudnikih te storitve v Sloveniji in izbranih državah Evropske unije (v nadaljevanju EU). Raziskava bo obsegala pregled osnovnih teoretičnih načel in pristopov k reševanju problema, ki veljajo v arhivski stroki. Natančneje bom raziskala zakonodajo in standarde, ki urejajo to problematiko na področju EU. Zakonodajo bom primerjala z aktualno zakonodajo s področja ohranjanja digitalnega gradiva, ki velja v Sloveniji.

Cilj naloge je ugotoviti stanje na področju ponudbe storitve digitalne hrambe oz. digitalnega arhiva na območju raziskovanih držav članic EU. Osrednja točka raziskave bodo predvsem zakonska določila in zahteve, ki jih morajo v posameznih državah izpolniti pravne osebe, če želijo nastopati na trgu kot ponudniki storitve zajema in hrambe elektronskega gradiva oz. ponudniki elektronskega arhiva. Osredotočila se bom na tehnološke in organizacijske zahteve, ki jih morajo ponudniki izpolniti, in organizacijske in finančne posledice, ki nastanejo zaradi tega.

Poskusila bom definirati nekaj dejavnikov, ki so pomembni pri odločitvi ponudnikov, ali bodo pristopili k postopkom dokazovanja, da je njihova digitalna hramba zaupanja vredna. Izvedla bom tudi intervju med obstoječimi registriranimi ponudniki storitve zajema in hrambe digitalnega gradiva v Sloveniji in tistimi, ki so pridobili akreditacijo svoje storitve. Raziskala bom, kako ocenjujejo postopke pridobitve akreditacije, zakaj so se ali pa se niso odločili pristopiti k postopku pridobivanja akreditacije in ali storitev dosega svoj namen, glede na obseg vloženega dela in finančni vložek. S pomočjo analize odgovorov, pridobljenih z intervjujem, bom poskusila potrditi ali ovreči nekaj trditev:

- nabor ponudnikov akreditirane storitve v Sloveniji je majhen zaradi zahtevnih ter obsežnih postopkov in predpisov na tem področju, velikih organizacijskih sprememb, ki jih morajo izvesti ponudniki v svojem okolju, in velikih finančnih vložkov, ki so potrebni za vzpostavitev storitve;
- akreditirano storitev koristi v glavnem državni in javni sektor;
- ponudnik, ki nima akreditirane storitve, nima stroškov z letnimi podaljševanji akreditacij opreme in storitev, posledično ima nižje stroške in zato je uporaba takšne storitve za stranko cenejša.

Poleg slovenske zakonodaje bo predmet raziskav še zakonodaja in postopki na Danskem in v Estoniji. Razlog za izbor teh držav je dejstvo, da sta zakonodaja in praksa na tem področju v državah EU zelo raznoliki in zapleteni, zato ni dovolj samo branje zakonodaje, temveč je zelo pomembna ustrezna interpretacija in izkušnje iz prakse. V obeh arhivih gospod Jan Dalsten Sørensen (Danski državni arhiv) in gospod Kuldar Ass (Državni arhiv Estonije) delujeta kot izvajalca zakonodaje na področju dolgotrajnega ohranjanja digitalnega gradiva in tudi sodelujeta s ponudniki storitev na tem področju. Ker vsak v svoji državi delujemo na področju, ki je predmet raziskave v nalogi, sem lahko iz prve roke pridobila tako razlago zakonodaje, kot tudi oris dejanskega stanja na terenu.

1 OHRANJANJE DIGITALNEGA GRADIVA

Postopki ohranjanja papirnega dokumentarnega in arhivskega gradiva gredo predvsem v smeri materialnega varstva. Pri ohranjanju dokumentarnega in arhivskega gradiva v digitalni obliki pa se srečujemo s težavami, ki jih ni tako enostavno rešiti. Pri digitalnem gradivu ne govorimo več samo o njegovem ohranjanju, temveč je izraz ohranjanje (angl. *preservation*) nadomestil izraz skrbništvo (angl. *curation*) (Giaretta, 2011, str ix). Skrbništvo digitalnega dokumentarnega in arhivskega gradiva ne obsega samo ohranjanje temveč tudi vzdrževanje in dodajanje vrednosti podatkom v vsem njihovem življenjskem ciklu (Giaretta, 2011, str. ix) od nastanka do uničenja v primeru dokumentarnega oz. predaje pristojnim državnim arhivom, če gre za arhivsko gradivo. Le-ti so po prevzemu takšnega gradiva še vedno dolžni skrbeti zanj po načelih ohranjanja arhivskega gradiva.

Obdobje od nastanka arhivskega gradiva do predaje gradiva pristojnim arhivom pa je lahko zelo dolgo. Roki hrambe dokumentarnega gradivo so določeni v zakonih, ki urejajo področja, na katerih gradivo nastaja. Za arhivsko gradivo pa je že ob nastanku določen neskončen rok hrambe, kar pomeni ne samo, da se ga ne sme nikoli uničiti, temveč je treba zanj skrbeti po načelih arhivske stroke že od nastanka pri ustvarjalcih. Skrbništvo digitalnega gradiva torej obsega v prvi fazi vse postopke, ki preprečijo propad oz. tehnološko zastaranje medija, na katerem se nahaja digitalno gradivo.

Glavni način dolgotrajnega ohranjanja gradiva je migracija – nabor organiziranih nalog, s katerimi periodično zagotavljamo prenos digitalnih podatkov iz ene strojne in programske konfiguracije v drugo, iz ene računalniške generacije v drugo (Gladney, 2007, str. 274). V drugi fazi pa gre tudi za ohranjanje berljivosti, ki jo lahko zagotovimo s kopiranjem vsebine iz zastarelega v sodobnejši format. Ohranjanje digitalnega gradiva se lahko obravnava kot poseben način asinhronega komuniciranja, ko neka informacija nastane, se le-ta ne posreduje takoj uporabniku, temveč se shrani v repozitoriju (Gladney, 2007, str. 15).

Repozitorij je način ohranjevanja digitalnih informacij, ki velikokrat ne omogoča preverjanje verodostojnosti informacije pri njenem izvoru. Tukaj se pojavi tudi razlika med digitalnim arhivom in digitalnim repozitorijem. Naloga repozitorija je torej predvsem zagotavljanje dolgoročne hrambe in dostopnosti do gradiva v času, ko je izvor gradiva še dostopen. Naloga pristojnih državnih arhivov pa je v zagotavljanju avtentičnosti, celovitosti, dostopnosti, trajne hrambe in uporabnosti gradiva predvsem v obdobju, ko izvor gradiva ni več dostopen za takšno preverjanje.

Ker je že samo odpravljanje tehnoloških ovir za zagotavljanje dostopnosti digitalnega gradiva velik zalogaj v finančnem in organizacijskem smislu, so države na področju EU pristopile k reševanju teh težav na različne načine. Evropska zakonodaja in standardi na tem področju uvajajo smernice in določila predvsem v obliki formatov dokumentov, ki so primerni za dolgoročno hrambo, in v obliki zahtev, ki jih mora izpolnjevati programska

oprema, ki se ukvarja z dolgotrajnim ohranjanjem digitalnih dokumentov. Zakonodaja posameznih držav EU pa določa, katere zahteve morajo izpolnjevati pravne osebe, če želijo izvajati skrbništvo nad digitalnimi podatki bodisi zase ali v obliki ponudnika storitve elektronske hrambe ali elektronskega arhiva.

Na področju ohranjanja digitalnega gradiva pa je še vedno ločnica med javnim/državnim in zasebnim sektorjem. Zasebni sektor v večini ni ustvarjalec arhivskega gradiva, zato so zahteve za vzpostavitev skrbništva v obliki digitalne hrambe ali digitalnega arhiva manjše, kot za osebe javnega prava. V Sloveniji so javnopravne osebe s strani Arhiva Republike Slovenije (v nadaljevanju Arhiv RS) lahko označene tudi kot ustvarjalci arhivskega gradiva in vpisane v Register ustvarjalcev javnega arhivskega gradiva (v nadaljevanju RegUst), dostopen na spletnem naslovu http://www.arhiv.gov.si/si/javne_evidence/ . V tem primeru pa so podvrženi zakonom in podzakonskim aktom, s katerimi so postavljeni okvirji in določila varovanja dokumentarnega in arhivskega gradiva v skladu z načeli arhivske stroke. V Sloveniji je trenutno v RegUst vpisanih okoli 4000 ustvarjalcev arhivskega gradiva (Arhiv Republike Slovenije, b.l.-b).

1.1 Problematika ohranjanja digitalnega gradiva

Glavni cilj ohranjanja digitalnega gradiva je optimizacija upravljanja z gradivom tekom njegovega življenjskega cikla od nastanka do diseminacije in njegove dolgoročne uporabe (Barateiro, Antunes, Freitas, Borbinha, 2010, str.5). Proces ohranjanja digitalnega gradiva, po definiciji American library association (2007, v nadaljevanju ALA), združuje politike, strategije in ukrepe, ki zagotavljajo natančno upodabljanje verodostojne vsebine skozi čas, ne glede na izzive, ki so povezani z napakami na medijih ali tehnološkimi spremembami. Proces poteka enako, ne glede na to, ali gre za izvorno digitalno ali za digitalizirano gradivo.

Proces ohranjanja digitalnega gradiva obsega vse postopke od zajema ali nastanka gradiva, zagotavljanja njegove celovitosti, do njegovega vzdrževanja in ohranjanja. V postopku zajema ali nastanka gradiva morajo biti podane natančne tehnične specifikacije gradiva, izvedene kontrole kvalitete gradiva, gradivo mora biti ustrezno opisano in opremljeno z metapodatki, ki bodo omogočali njegovo nadaljnjo uporabo. Proces zagotavljanja celovitosti gradiva obsega dokumentiranje vseh postopkov in procesov, ki se izvajajo nad gradivom v procesih ohranjanja, ter nadzorne in varnostne mehanizme, ki upravljajo dostope in posege v gradivo.

Proces vzdrževanja in ohranjanja gradiva obsega vzdrževanje robustne informacijske infrastrukture, zagotavljanje varnostnih kopij gradiva, nadzor nad datotekami z gradivom in programe osvežitve, migracija ali emulacije. Poleg tega pa so ključnega pomena še načrti za preprečevanje nesreč, obnovitveni plani po nesreči, upravljanje s tveganji in konstanten pregled ter prenova politik in procesov, udeleženih pri ohranjanju gradiva. Upravljanje s tveganji pri ohranjanju digitalnega gradiva obsega nadzor nad gradivom in

tudi nad okoljem v katerem se gradivo nahaja. (ALA, 2007).Vsebinski in strateški cilji ohranjanja digitalnega gradiva v nekem okolju so odvisni predvsem od tipa, velikosti in količine gradiva, pa tudi od zahtev po ponovni uporabi podatkov (angl. *re-use*).

Ne glede na specifične zahteve, pa obstaja nekaj generičnih zahtev, ki veljajo za vsa okolja, ki se ukvarjajo z dolgotrajnim ohranjanjem digitalnega gradiva. Barateiro et al. (2010, str.7-8) so definirali generične zahteve kot zahteve po zagotavljanju:

- zanesljivosti: digitalni repozitorij mora biti zasnova tako, da bo ohranjal podatke v neskončno prihodnost z minimalnimi možnimi izgubami;
- avtentičnosti: uporabnik mora imeti možnost preverjanja ali je informacija verodostojna;
- dokazil o izvoru (provinenca): informacija mora vsebovati podatke o izvoru – predvsem o ustvarjalcu oz. viru, ki je odgovoren za njen nastanek;
- celovitosti: obstajati morajo dokazila, da vsebina digitalnega objekta ni bila spremenjena;
- reševanja težav z zastarelostjo strojne in programske opreme: zagotavljanje ustrezne strojne in programske opreme, ki bo omogočala dostop do informacij na tak način, kot je predvidel ustvarjalec;
- tehnične nadgradljivosti in raznolikosti: zaradi zastaranja opreme in potreb po povečanju zmogljivosti obstoječe opreme morajo biti repozitoriji zasnovani tako, da omogočajo nadgradnjo oz. posodobitev strojne in programske opreme ne da bi s tem bila povzročena škoda gradivu ali uporabnikom;
- obvladovanju tveganj in sprememb okolja: vzpostavitev nadzornih in obnovitvenih planov ter zagotovitev skladnosti delovanje repozitorija z veljavno zakonodajo.

1.2 Tehnike ohranjanja digitalnega gradiva

Pri ohranjanju digitalnega gradiva se srečujemo z zastarelostjo formatov, v katerih je digitalno gradivo hranjeno, in z zastarelostjo strojne in programske opreme, ki sestavljata informacijski sistem za hrambo in dostop do gradiva. Posodobitev strojne opreme je projekt zase, ki se izvaja na daljše časovno obdobje, posodobitev programske opreme pa se izvaja pogosteje. Kljub temu, da večina novih verzij programske opreme lahko bere datoteke narejene s prejšnjo ali še starejšimi verzijami, pa ni tako redko, da se ob nadgradnji ta funkcionalnost zgubi. Datoteke, ki niso migrirane v novejšo verzijo programske opreme, lahko postanejo neberljive. Barateiro et al. (2010, str.10-13) navajajo nekaj dobrih praks in tehnik za zmanjševanje nevarnosti, ki jo prinaša zastarelost formatov in opreme, in sicer:

- redundanca oz. replikacija datotek: glavna težava tega pristopa je vzdrževanje skladnosti med kopijami;
- migracija oz. prenos ali prepis datotek na sodobnejši medij ali sodobnejši format: v obeh primerih se lahko srečamo z izgubami oblike ali vsebine dokumenta;

- emulacija oz. simulacija strojnega in programskega okolja, v katerem je gradivo nastalo, na sodobni opremi;
- osveževanje oz. vzdrževanje obstoječe infrastrukture na način, da imamo vedno najsodobnejše okolje, v katerem dokumenti nastajajo in se hranijo.
- raznolikost:
  - fizičnih lokacij: z geografsko oddaljenimi fizičnimi lokacijami zmanjšamo tveganje hkratnih odpovedi sistema v primeru nesreč;
  - programske in strojne opreme: zmanjšamo občutljivost in ranljivost programske in strojne opreme ter znižamo tveganje odpovedi vzdrževanja v primeru, da proizvajalec propade;
  - administracije sistema: upravljanje sistema razdeljeno na več oseb zmanjša tveganje, da bi ena oseba hote ali nehote povzročila izpad celotnega sistema;
  - medijev za hrambo: s tem zmanjšamo vpliv na delovanje sistema zaradi odpovedi posamezne vrste medijev zaradi tehničnih napak;
  - virov financiranja: zmanjša tveganje ekonomske nestabilnosti digitalnega repozitorija;
- uporaba metapodatkov: podatki o podatkih so ne samo dodana vrednost podatkom, temveč so nujni ob implementaciji ostalih tehnik za ohranjanje podatkov. Pri emulaciji in migraciji so ključnega pomena za zagotovitev celovitosti in avtentičnosti digitalnega gradiva;
- nadzor: njegov namen je pravočasno odkrivanje napak v sistemu in s tem hitrejšo obnovo in manjše tveganje za izgubo podatkov.

1.3 Zanesljiv digitalni repozitorij

Leta 1996 je Skupina za ohranjanje in dostop in skupina raziskovalnih knjižnic ustanovila Skupino na področju arhiviranja digitalne informacije (angl. *Task Force on Archiving of Digital Information*), ki je v svojem poročilu pozvala k vzpostavitvi programov certificiranja repozitorijev za dolgotrajno ohranjanje digitalnega gradiva, saj »morajo repozitoriji, ki trdijo, da izvajajo funkcijo arhiviranja, to tudi dokazati z doseganjem ali preseganjem standardov in kriterije neodvisnega programa za certificiranje arhivov« (Garrett & Waters, 1996, str.9). Vsak digitalni repozitorij ima svoj namen in značilnosti, vendar pa morajo, kot ugotavlja Klump (2011), biti kriteriji za dokazovanje zanesljivosti splošni in na visokem abstraktnem nivoju, pri uporabi pa pretvorjeni v skladu s kontekstom in potrebami okolja, ki jih uporablja.

Dobratz, Rödig, Borghoff, Rätzke in Schoger (2010, str.48-50) definirajo zanesljivost digitalnega repozitorija kot skladno delovanje s cilji in specifikacijami, z vidika informacijske varnosti pa to pomeni varovanje celovitosti, avtentičnosti, zaupnosti in zagotavljanje razpoložljivosti. Poleg tehnične ustreznosti pa je pokazatelj zanesljivosti tudi urejena dokumentacija z opisanimi postopki in procesi, ki zagotavlja transparentno upravljanje in poslovanje repozitorija. Za izkazovanje zanesljivosti je pomembno tudi, ali

je digitalni repozitorij kot institucija pridobil katerega od certifikatov, ki dokazujejo urejenost in skladnost poslovanja, saj jih lahko uporabi kot dokaz v postopkih certificiranja po standardih s področja ohranjanja digitalnih podatkov (The Consultative Committee for Space Data Systems, 2009, poglavje 2 str.2).

2 MEDNARODNI STANDARDI NA PODROČJU OHRANJANJA DIGITALNEGA GRADIVA

Zaradi vedno večje količine izvorno digitalnega gradiva, ki ga je enostavno kopirati, spreminjati in prenašati po digitalnih poteh, je tveganje, da se gradivo od izvora do cilja spremeni, pa to ne bo opazno, vedno večje. Posledica tega dejstva je vedno večji poudarek na zanesljivem in varnem upravljanju z njim. Namen standardov in zakonodaje, ki so jo uveljavile posamezne države, je ravno v vzpostavitvi okolja, procesov in postopkov ohranjanja digitalnega gradiva, ki bodo upoštevali tudi, kaj bi lahko nekdo v prihodnosti zahteval od danes shranjenih podatkov (Barateiro et al., 2010, str.7). Področje ohranjanja digitalnih vsebin ureja več standardov, ki opredeljujejo infrastrukturne zahteve za informacijsko okolje, kjer bo gradivo hranjeno, zahteve informacijske varnosti in upravljanja z dokumenti. Barateiro et al. (2010) ugotavljajo, da so generične zahteve standardov in zakonodaje enake osnovnim zahtevam arhivske stroke in so opredeljene kot:

- zanesljivost: pomeni, da kopija ali primerek kateregakoli digitalnega objekta preživi življenjsko dobo sistema, na katerem se nahaja, kar je lahko v primeru arhivskega gradiva neskončno dolgo. V praksi to pomeni, da mora biti sistem hrambe zasnovan tako, da lahko hrani podatke neskončno dolgo brez izgub;
- avtentičnost: pomeni, da se lahko bodoči uporabnik gradiva odloči ali je pridobljena informacija zanesljiva. V tem delu se naslonimo tudi na provenienco (izvor) gradiva, ki dodatno služi kot dokazilo avtentičnosti. V primeru pa, da izvor ne obstaja več, je naloga skrbnika gradiva, da ohranja vse metapodatke, ki zagotavljajo avtentičnost in dokazujejo izvor gradiva;
- celovitost: pomeni, da mora hramba dokumentarnega gradiva zagotavljati nespremenljivost in celovitost dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenost dokumentarnega gradiva oziroma njegove vsebine ter dokazljivost izvora dokumentarnega gradiva (provenienca);
- dostopnost in uporabnost digitalnega gradiva: pomeni, da mora biti dokumentarno gradivo oziroma reprodukcija njegove vsebine ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom. V primeru arhivskega gradiva govorimo o ohranjanju brez časovnih omejitev.

2.1 Standard SIST ISO 15489-1:2005

Enega prvih mednarodnih standardov na področju upravljanja z dokumenti različnih vrst in izvora (digitalni, analogni ali papirni) je izdala Mednarodna organizacija za standardizacijo (angl. *International standard organization*, v nadaljevanju ISO) kot

slovenskega pa prevzel Slovenski inštitut za standardizacijo (v nadaljevanju SIST) in sicer gre za SIST ISO 15489-1:2005– Informatika in dokumentacija – Upravljanje zapisov (v nadaljevanju ISO 15489), ki je naslednik avstralskega standarda za upravljanje z dokumenti Standards Association of Australia 4390:1996 (v nadaljevanju ASA4390:1996) (Higgins, 2007). Standard ureja področje upravljanja z dokumenti vseh formatov in na vseh medijih, ustvarjenih ali pridobljenih s strani javnih ali zasebnih organizacij ali posameznikov, katerih naloga je ustvarjanje in vzdrževanje dokumentov.

Namen standarda je vzpostavitev smernic za ugotavljanje odgovornosti organizacije za dokumente, politike, pravila in sisteme za upravljanje z njimi. Poleg tega se s svojimi smernica navezuje še na standarda SIST EN ISO 9001:2008 Sistemi vodenja kakovosti - Zahteve (v nadaljevanju ISO 9001) in SIST EN ISO 14001:2005 Sistemi ravnanja z okoljem – Zahteve z navodili za uporabo (v nadaljevanju ISO 14001) ter nudi tudi usmeritve za razvoj in implementacijo dokumentnih sistemov.

Kljub temu, da standard ne podaja okvirjev za upravljanje z dokumenti znotraj arhivskih inštitucij, je bil to prvi standard (Gunnlaugsdottir, 2002, str.1), ki je podal enotne usmeritve ustvarjalcem dokumentarnega in arhivskega gradiva, kako naj upravljajo z gradivom v času, ko je to gradivo še pri njih v uporabi. Ob njegovi predstavitvi oktobra 2001, je standard predstavljal mejnik na področju upravljanja z zapisi in vrhunec vseh dotedanjih izkušenj in dobrih praks na tem področju. Standard definira dokument kot zapisano informacijo, ki je nastala, bila prejeta, ali pa se upravlja kot dokaz za organizacijo in osebo v zakonskih ali poslovnih zadevah.

Standard utemeljuje tudi osnovna načela arhivske stroke, na katerih temelji ohranjanje gradiva – avtentičnost, zanesljivost, celovitost in uporabnost. Čeprav standard kot tak ne posega na področje arhivskega gradiva, je iz navedenega razumljivo, da osnovna načela hrambe gradiva veljajo za vsakogar, ki želi hraniti gradivo z namenom njegove nadaljnje uporabe, bodisi kot dokazno ali poslovno gradivo, in ne samo kot arhivsko gradivo. Standard prvič definira tri značilnosti vsakega dokumenta in sicer je to vsebina, ki mora biti povezana z metapodatki z ostalima dvema značilnostma, in sicer strukturo dokumenta (npr. format) in kontekstom ali opisom dokumenta, ki govori predvsem o nastanku dokumenta, prejemu ali uporabi dokumenta, torej kdo ga je naredil, zakaj in kdaj.

Standard postavlja tudi okvire za implementacijo sistema za upravljanje z dokumenti, kjer opredeljuje njegove lastnosti in funkcionalnosti. Ob nastanku je bil standard izjemen napredek in čeprav je nastal najprej v okviru knjižničarske stroke, je utemeljeval tudi arhivska načela. Ker pa se kot tak ni ukvarjal s hrambo arhivskega gradiva, ki je po svojem statusu gradivo, kateremu namenjamo posebno skrb, saj ga moramo hraniti za vedno, je leta 2003 nastal prvi standard ISO 14721 Trajno ohranjanje podatkov in sistemi za prenos informacij - Odprti arhivski informacijski sistem (OAIS) - Referenčni model, ki je bil v celoti namenjen upravljanju z arhivskim gradivom. Priporočila v standardu ISO 15489 niso

omejena samo na sisteme, ki so neposredno udeleženi pri upravljanju z dokumenti, temveč posveča pozornost tudi:

- procesom, ki potekajo v takšnih sistemih (od zajema, hrambe, uporabe, do sledenja spremembam na dokumentih);
- nadzoru in sledenju toka dokumentov znotraj takšnih sistemov (eden od pomembnih dejavnikov za zagotavljanje avtentičnosti);
- nadzorovanemu in dokumentiranemu uničenju dokumentov;
- dokumentiranju procesov upravljanja z dokumenti (npr. upravljanje z roki hrambe);
- nadzorom in revizijam sistemov za upravljanje z dokumenti;
- stalnemu izobraževanju in usposabljanju na področju upravljanja z dokumenti.

2.2 MoReq – Modular Requirements for Records Systems

Model zahtev za upravljanje elektronskih dokumentov (angl. *Modular Requirements for Records Systems,* v nadaljevanju MoReq) je skupek modularnih zahtev za dokumentne sisteme in je na tem področju zgolj de-facto standard brez dejanskega statusa standarda (MoReq2, 2013) Prva različica MoReq je izšla leta 2002 pod okriljem Evropske komisije, nadaljnje različice pa so izšle pod okriljem Document Lifecycle Management foruma (v nadaljevanju DLM forum), kot institucije znotraj Evropske unije, ki se ukvarja z upravljanjem, hrambo, skrbništvom in uporabo strojno-bralnih podatkov. Zadnja različica je MoReq2010. Cilj MoReq2010 je, da na razumljiv in enostaven način uporabnikom, kupcem in razvijalcem programske opreme predstavi zahteve, ki jih mora izpolnjevati programski produkt za upravljanje z dokumenti (Document Lifecycle Management Forum Foundation, 2011). Zahteve MoReq2010, ki jih je izpostavil že standard ISO 15489, so zahteve po zagotavljanju:

- avtentičnosti dokumentov: dokument je tisto, kar naj bi bil in ga je ustvarila oseba, ki ga je morala ustvariti;
- zanesljivosti informacij: informacija v dokumentu je natančna in zanesljiva;
- celovitosti dokumentov: dokument je popoln in nespremenjen;
- uporabnosti dokumentov: dokument se lahko locira, pridobi, prikaže in razloži.

Zahteve so podane glede na posamezne module oz. servise, ki sestavljajo programski produkt. Moreq2010 opisuje minimalne generične zahteve, ki jih morajo programski servisi izpolnjevati, da lahko govorimo o programskem produktu, ki ustrezno upravlja z dokumenti in zagotavlja izmenljivost in prenosljivost podatkov z drugimi programskimi produkti, ki izpolnjujejo zahteve iz MoReq2010. Zahteve definirajo servise, ki so namenjeni upravljanju sistema, upravljanju uporabnikov in njihovih vlog, upravljanju klasifikacije dokumentov, upravljanju dokumentov, upravljanju metapodatkov in metapodatkovnih modelov in upravljanju z roki hrambe. Poleg omenjenih servisov pa

MoReq2010 zahteva tudi dodatne procesne servise, ki ne upravljajo direktno z gradivom kot je sistem iskanja in poročanja ter servis, ki omogoča izvoz dokumentov.

2.3 Standard SIST ISO 14721:2013

Osnovni standard na področju arhivskih informacijskih sistemov, ki je s 1.7.2013 postal tudi slovenski standard, je SIST ISO 14721:2013 - Trajno ohranjanje podatkov in sistemi za prenos informacij - Odprti arhivski informacijski sistem (OAIS) - Referenčni model (v nadaljevanju OAIS). Kljub temu, da je bil OAIS referenčni model leta 2003 s strani Consultative Committe for space Data Systems (v nadaljevanju CCSDC) definiran za ohranjanje vesoljskih podatkov (ISO Archiving Standards – Overview, 2006), je v svoji osnovi nevtralen in se izogiba uporabi specifičnih izrazov tako iz arhivske kot tudi informacijske znanosti.

Prav tako leta 2003 pa je bil referenčni model CCSDS 650.0-B-1 prevzet s strani mednarodne organizacije za standardizacijo ISO kot standard ISO 14721:2003 (Document History, 2013). Na tak način je OAIS postal *lingua franca* za arhivski informacijski sistem (Klump, 2011). Standard se ne omejuje samo na upravljanje z dokumenti, temveč želi celoten življenjski cikel dokumenta, od priprave na predajo dokumenta v hrambo do njegove nadaljnje uporabe, postaviti na skupne temelje.

OAIS je referenčni model za digitalni arhiv, ki ga sestavljajo organizacija, ljudje in sistemi, ki so prevzeli odgovornost za ohranjanje digitalnega gradiva na način, da bo na razpolago zainteresirani javnosti. Beseda »odprt« v imenu standarda označuje dejstvo, da je ta standard in vsi bodoči, ki bodo nastali na tem področju, nastal kot rezultat odprtega delovanja v raznih forumih in ne, da omogoča neomejen dostop do hranjenega gradiva. Niti ni namen standarda predpisati načrt ali implementirati digitalni arhiv, temveč je zgolj skupek okvirjev in priporočil, katerim naj bi ob dejanski implementaciji digitalnega arhiva posvetili pozornost. Namen standarda OAIS je:

- zagotoviti okvir za osveščanje in razumevanje konceptov arhivske stroke, ki se uveljavljajo pri zagotavljanju dolgotrajne hrambe in uporabnosti digitalnega gradiva;
- postaviti načela, katerim naj sledijo organizacije, ki se ne ukvarjajo neposredno z arhiviranjem, da bodo učinkovit sodelavec v procesih ohranjanja digitalnega gradiva;
- postaviti terminološke in konceptualne okvire za opis in primerjavo arhitekture in postopkov sedanjih in bodočih arhivov;
- postaviti okvire za primerjavo in opis strategij in tehnik dolgotrajnega ohranjanja digitalnega gradiva;
- razširjati dogovore na področju procesov dolgotrajnega ohranjanja digitalnega gradiva, tako da lahko proizvajalci opreme sledijo s svojim razvojem;
- voditi ustvarjanje novih z OAIS povezanih standardov.

OAIS kot referenčni model opisuje celo vrsto nalog, ki so povezane z dolgotrajnim ohranjanjem digitalnega gradiva. Tako opisuje prevzem gradiva v arhiv (angl. *ingest*), hrambo prevzetega gradiva, upravljanje tega gradiva, dostop in diseminacijo oz. razširjanje tega gradiva zainteresirani javnosti. Prav tako izpostavlja kot pomembno nalogo migracijo digitalnega gradiva na novejši medij ali novejši format in ustreznost programske in strojne opreme, ki zagotavlja hrambo. Standard ne postavlja minimalnih okvirjev samo za organizacije, ki digitalno gradivo dolgotrajno hranijo, temveč tudi ustvarjalcem gradiva, ki bo v prihodnosti postalo predmet dolgotrajne hrambe, in tudi vsem tistim, ki bodo do takšnega gradiva v prihodnosti dostopali.

OAIS definira informacijo kot znanje, izraženo s podatki na način, ki je primeren za izmenjavo. Pred digitalno dobo so to bile črke na papirju. Za njihovo interpretacijo je bila potrebna osnova baza znanja – pismenost in poznavanje jezika, v katerem je besedilo napisano. V digitalnem svetu pa so podatki predstavljeni z biti. Za njihovo razumevanje ni dovolj znanje branja bitov temveč moramo vedeti tudi, kako bite interpretirati oz, kaj ti biti predstavljajo. Pomeni, da moramo imeti t.i. informacijo o zastopanosti (angl. *representation information*), ki nam pove, za kakšno vrsto informacije gre (npr. slika, zvok, besedilni dokument,ipd..).

OAIS definira osnovne koncepte in objekte, ki se pojavljajo v postopkih prevzema, hrambe in diseminacije digitalnega gradiva. Osnovni objekt je informacijski paket (v nadaljevanju IP), ki je skupek digitalne vsebine (angl. *content information*, v nadaljevanju CI) npr. slika1.jpg, slika2.jpg, in opisa te vsebine (angl. *preservation description information*, v nadaljevanju PDI). Opis vsebine je pomemben, saj omogoča razumevanje okolja in pogojev, pod katerimi je gradivo nastalo. Opis vsebine naj bi obsegal vsaj:

- podatke o izvoru oz. kdo je bil upravljavec gradiva in tudi o spremembah, ki so se dogajale na gradivu v času njegovega obstoja pri ustvarjalcu, predno je gradivo prišlo v dolgotrajno hrambo;
- kontekst ali vsebinsko povezavo glede na ostalo gradivo izven IP, npr. zakaj je gradivo sploh nastalo;
- referenca ali sklic, ki vsebuje enega ali več identifikatorjev za enolično identifikacijo vsebine;
- varnostne vsebine (npr. kontrolne vsote ali angl. *checksum*), ki zagotavljajo ovoj za zaščito vsebine pred nedokumentirano spremembo;
- dovoljenja za dostop vključno z ohranjanjem, razširjanjem in uporabo vsebine.

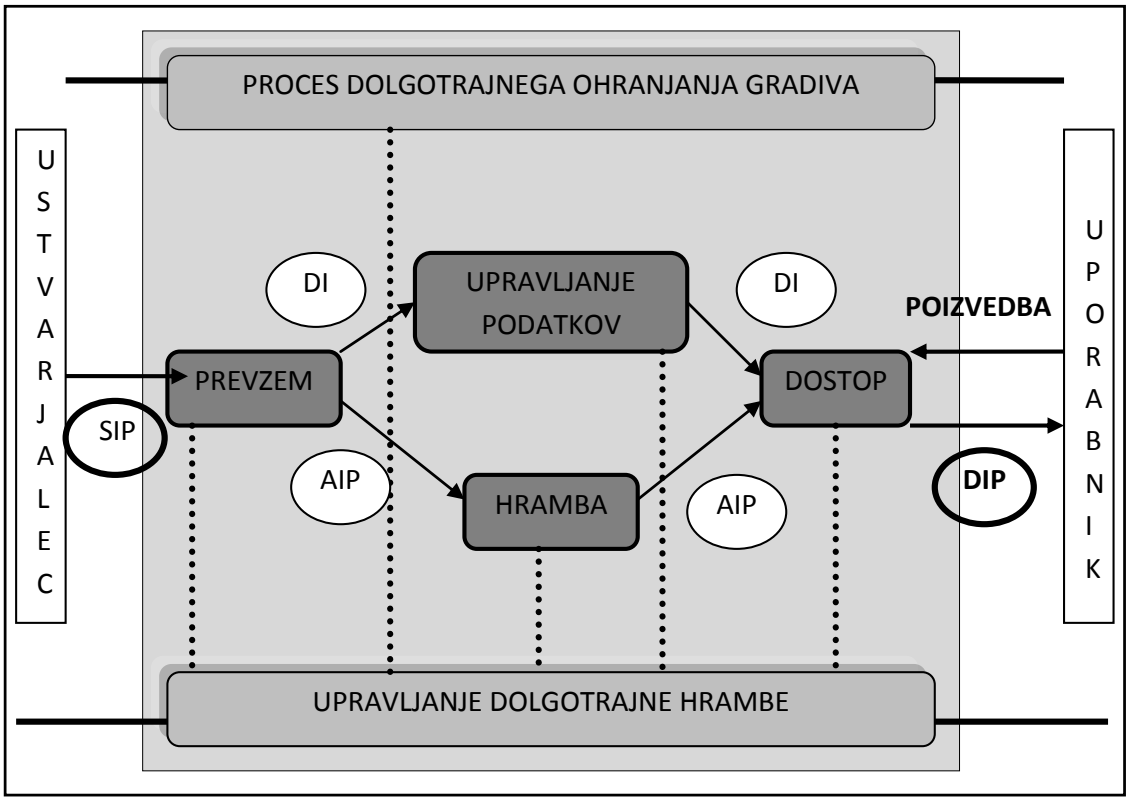
Informacijski paket v OAIS referenčnem modelu poleg osnovnih gradnikov (CI in PDI), vsebuje še podatke o paketu (angl. *packaging information*, v nadaljevanju PI) , ki fizično ali logično povezujejo vsebino paketa z opisom vsebine paketa (npr. podatki na CD bi imeli poleg CI in PDI še podatke o datotečni strukturi na CD). Za uporabo podatkov v paketu pa je zelo pomembna še opisna informacija (angl. *descriptive information*, v nadaljevanju DI), ki opisuje vsebino paketa (npr. slike poplav v Prekmurju v leti 2012).

Razlika med referenčnim modelom in realnostjo pa je velika. Že standard predvideva, da v realnosti informacijski paket verjetno ne bo imel vseh priporočenih vsebin. Zato OAIS referenčni model predvideva tri različne informacijske pakete:

- sprejemni informacijski paket (angl. *submission information package*, v nadaljevanju SIP) v dolgotrajno hrambo posreduje ustvarjalec. Vsebina paketa je stvar pogajanj med ustvarjalcem in organizacijo, ki gradivo hrani, običajno pa je odvisna od stopnje zavedanja ustvarjalca o pomembnosti dodatnih vsebin, potrebnih za dolgotrajno hrambo, ki morajo biti ustvarjene že ob nastanku gradiva;
- arhivski informacijski paket (angl. *archival information package*, v nadaljevanju AIP) je sestavljen iz enega ali več SIP in je opremljen z vsemi dodatnimi vsebina, s katerimi se zagotavlja dolgotrajno hrambo po načelih arhivske stroke. Če dodatne vsebine niso prisotne ob nastanku, jih ustvarjalec dopolni pred predajo gradiva v dolgotrajno hrambo, zopet v dogovoru z organizacijo, ki bo gradivo hranila;
- diseminacijski informacijski paket (angl. *dissemination information package*, v nadaljevanju DIP) je arhivsko gradivo, ki ga predstavimo uporabniku glede na njegovo poizvedovanje z upoštevanjem omejitve dostopa.

OAIS referenčni model (Slika 1) predstavlja model elektronskega arhiva, katerega temeljna naloga je enaka kot je naloga klasičnega arhiva – torej prevzem in trajna hramba arhivskega gradiva.

Slika 1: OAIS referenčni model



Vir: OAIS, slika 4-2.

S tem, ko je ustvarjalec predal gradivo pristojnemu arhivu, je le-ta odgovoren za zagotavljanje njegove avtentičnosti, celovitosti, zanesljivosti, uporabnosti in dostopnosti. Standard pa ne postavlja okvirjev samo za prevzem, hrambo in diseminacijo gradiva, temveč nalaga tudi odgovornosti posameznikom, ki so udeleženi v postopku. Odgovornost za pripravo gradiva in dodatne vsebine, ki bodo omogočale nadaljnjo uporabo gradiva, nalaga ustvarjalcem gradiva. Organizacijam, ki takšno gradivo hranijo, pa nalaga odgovornosti in obveznosti, ki jih le-te morajo izpolnjevati, če se želijo deklarirati kot OAIS digitalni arhiv, ki hrani gradivo po načelih arhivske stroke. Odgovornosti obsegajo:

- dogovor z ustvarjalci gradiva, da le-tega pripravijo v ustrezni obliki in s čim več dodatnimi vsebinami, ki bodo olajšale obdelavo in nadaljnjo uporabo gradiva;
- pridobitev ustreznih kontrolnih in varnostnih vsebin, ki bodo omogočale nadaljnjo uporabo gradiva in zagotavljale dolgotrajno hrambo;
- določitev (skupaj z ustvarjalcem, če je to mogoče) zainteresirane javnosti, ki ji bo gradivo na razpolago in, ki ima ustrezna znanja za interpretacijo tega gradiva, saj se s tem poveča in podaljša njegova uporabnost;
- predstavitev informacije na tak način, da je zainteresirani javnosti razumljiva brez dodatnih strokovnjakov, ki bi interpretirali vsebino ali brez dodatne specialne strojne in programske opreme (neodvisna razumljivost – angl. *independently understandable*);
- sledenje dokumentiranim postopkom in politikam, ki zagotavljajo, da je informacija ustrezno hranjena in da nikoli ni naključno nepovratno izbrisana;
- hranjeno informacijo ponuditi zainteresirani javnosti kot kopijo izvornega dokumenta s podatki, ki dokazujejo avtentičnost in povezujejo kopijo z izvornim dokumentom v obliki DIP in z upoštevanjem omejitev dostopa.

2.4 Standard ISO 16363:2012

Standard angl. *ISO 16363:2012 Audit and certification of trustworthy digital repositories* (v nadaljevanju ISO 16363) predstavlja tehnična priporočila in natančne specifikacije kriterijev, ki naj bi bili upoštevani pri nadzoru in certificiranju zanesljivih digitalnih repozitorijev oz. e-arhivov. Standard OAIS samo izpostavlja potrebo po standardih za certificiranje, medtem, ko standard ISO 16363 to potrebo izraža v obliki priporočil in kriterijev za izvajanje nadzora. Kot je navedeno v standardu, je kritična komponenta infrastrukture za digitalno arhiviranje zadostno število zanesljivih organizacij, ki so sposobne hrambe, skrbništva in omogočanja dostopa do digitalnega gradiva.

Izpostavljeno je stališče, da se repozitorij ne more samooklicati za zanesljivega, temveč je treba s procesom certificiranja, ki vključuje ustrezen nadzor, vzpostaviti vsesplošno klimo zaupanja v ohranjanje digitalnega gradiva. Standard, poleg priporočil, vsebuje tudi merila, katerih namen je ugotavljanje vzdržnosti repozitorija glede na OAIS standard oz. odkrivanje njegovih slabosti ali pomanjkljivosti in vzpostavitev procesov nenehnega izboljševanja. Osnovno poslanstvo zaupanja vrednega repozitorija je zagotavljati zanesljiv

dostop do upravljanega digitalnega gradiva zainteresirani javnosti zdaj in v prihodnosti. Za zagotavljanje te naloge pa je zahtevan konstanten nadzor, planiranje in vzdrževanje kot tudi zavestni ukrepi in strategije za implementacijo izboljšav. Periodičen nadzor poskrbi za transparentno delovanje repozitorija in s tem povečuje zaupanje javnosti.

Repozitorij pa lahko izkaže določeno stopnjo zaupanja tudi s pridobivanjem certifikatov na področju standardov za dolgoročnega ohranjanja digitalnih dokumentov, ki so upoštevani pri izvajanju nadzora. Kriterije, katerim mora zaupanja vreden digitalni repozitorij zadostiti in so tudi predmet rednih nadzornih procesov, lahko razdelimo v tri večje skupine in sicer:

I. Organizacijska infrastruktura repozitorija kot institucije:

- upravljanje in organizacijski ukrepi za preživetja: repozitorij se mora na najvišjem upravljavskem nivoju pisno zavezati k ohranjanju, skrbi, upravljanju in omogočanju dostopa do digitalnega gradiva, ki ga hrani. Imeti mora strateški plan ohranjanja digitalnih vsebin, ki bo zagotavljal dolgotrajno vzdržnost njegovega poslanstva in tudi ustrezen načrt nasledstva, načrte za nepredvidljive situacije in / ali escrow dogovor, v primeru, da repozitorij preneha delovati ali pa se bistveno spremeni način in obseg upravljanja in financiranja;
- organizacijska struktura in kadrovanje: repozitorij mora identificirati in vzpostaviti naloge za svoje nemoteno delovanje in določiti odgovorne osebe z ustreznim znanjem in sposobnostmi za izpolnjevanje teh nalog. Skrbeti mora za nenehno izpopolnjevanje in usposabljanje odgovornih oseb v skladu s svojim strokovnim, tehnološkim in organizacijskim razvojem;
- okvir procesne odgovornosti in politike ohranjanja dokumentov: repozitorij mora vzpostaviti dokumentacijo, ki odraža njegov namen, plane in opisuje procese, postopke odločanja in cilje na način, ki bo razumljiv vsem zainteresiranim, hkrati pa bo zagotavljala, da se procesi in postopki, povezani z dolgotrajnim ohranjanjem digitalnega gradiva, izvajajo na dogovorjen, konsistenten način. Repozitorij mora imeti vzpostavljen načrt rednega samoocenjevanja in zunanjih nadzornih pregledov v postopkih certificiranja z namenom ohranjanja zaupanja;
- finančna vzdržnost repozitorija: repozitorij mora imeti kratkoročne in dolgoročne plane in postopke za zagotavljanje finančne stabilnosti, ki morajo biti skladni z ustaljenimi praksami, transparentni in nadzorovani s strani zunanjih institucij glede na obstoječo zakonodajo. Zavezati se mora h konstantnemu analiziranju in poročanju na področju finančnih tveganj, vključno z dohodki, naložbami in odhodki. S tem repozitorij izkazuje zavezanost k obvladovanju tveganj na finančnem področju, zavezanost k transparentnemu delovanju in povečuje stopnjo zaupanja;
- pogodbe, dovoljenja in obveznosti: repozitorij mora vzpostaviti in vzdrževati ustrezna pogodbena razmerja z ustanovami ali posamezniki, katerih gradivo hrani, skrbi zanj in omogoča dostop do njega. S pogodbo so določene in na repozitorij prenesene pravice

do zbiranja, hrambe in skrbništva nad gradivom, dolžnosti, povezane z dostopom do gradiva in dolžnost repozitorija, da te pravice pravno ščiti.

II. Upravljanje z digitalnim gradivom:

- prevzem gradiva v obliki SIP (angl. *ingest*): repozitorij mora opredeliti vsebino in lastnosti digitalnega gradiva, ki ga bo hranil in svoje dolžnosti in naloge ob prevzemu gradiva, kot tudi dolžnosti in naloge ustvarjalca, ki bo gradivo pripravil za predajo v repozitorij. Vzpostavljeni morajo biti nadzorni mehanizmi za preverjanje celovitosti in pravilnosti SIP;
- kreiranje AIP (angl. *ingest*): repozitorij mora imeti definiran in nadzorovan postopek, kako iz SIP nastane ustrezen, zainteresirani javnosti razumljiv AIP, ki je primeren za dolgotrajno hrambo. Za to, da se lahko prevzeto gradivo predstavi in da v uporabo zainteresirani javnosti, pa mora imeti repozitorij na razpolago tudi vsa potrebna orodja in metode za dostop in razumevanje opisa digitalne vsebine in z njo povezane vsebine. S tem je zagotovljena avtentičnost, omogočena sledljivost neavtoriziranim spremembam na digitalnem gradivu in tudi identifikacija oz. postavitev digitalnih objektov v ustrezen kontekst;
- načrt ohranjanja digitalnega gradiva: repozitorij mora imeti dokumentirano strategijo in vzpostavljen sistem nadzora, vrednotenja ustreznosti in spreminjanja metod ohranjanja digitalnega gradiva. V primeru, ko opis vsebine postane zainteresirani javnosti nezadosten za uporabo gradiva, mora repozitorij imeti mehanizme za kreiranje, identificiranje ali pridobivanje dodatnih opisov digitalne vsebine v takšni meri, da bo le-ta ponovno postala razumljiva zainteresirani javnosti;
- ohranjanje AIP: repozitorij mora imeti do bita natančen opis, kako je shranjen AIP in vseh akcij, ki so bile izvedene nad njim. Ta podatek je pomemben za pridobivanje informacij iz AIP v prihodnosti. Ohraniti mora tudi informacijo o vsebini in ves čas hrambe nadzorovati celovitost AIP;
- upravljanje z informacijami: repozitorij mora definirati minimalen nivo informacij, ki omogočajo zainteresirani javnosti identificiranje iskanega gradiva. V ta namen mora repozitorij kreirati minimalno opisno informacijo in zagotoviti njeno povezanost z ustreznim AIP ves čas hrambe;
- upravljanje dostopa: repozitorij mora za upravljanje dostopov vzpostaviti dostopne politike in delovati v skladu z njimi. Govorimo predvsem o upravljanju dostopov uporabnikov do gradiva. Poleg tega pa gre pri upravljanju dostopa tudi za sposobnost repozitorija, da predstavi dokazano avtentične digitalne objekte kot DIP.

III. Upravljanje z infrastrukturnimi in varnostnimi tveganji:

- upravljanje s tveganji na tehnični infrastrukturi: repozitorij mora identificirati in upravljati informacijsko infrastrukturo na način, da zmanjšuje tveganja povezana s cilji in nalogami ohranjanja digitalnega gradiva. Infrastruktura mora biti varna in zanesljiva,

obstajati pa mora tudi sistem, ki jo nadzoruje. Repozitorij mora imeti učinkovit sistem odkrivanja izgub ali okvar podatkov ali medijev in v ta namen vzpostavljen sistem varnostnega kopiranja z ustrezno infrastrukturo, ki bo zadoščal za ohranjanje vsebine repozitorija in sledil njegovim nalogam v procesu ohranjanja gradiva. Prav tako pa mora biti vzpostavljen tudi sistem upravljanja in sledenja sprememb na identificiranih kritičnih procesih ohranjanja digitalnega gradiva;

- upravljanje z varnostnimi tveganji: repozitorij mora izvajati sistematično analizo varnostnih tveganj povezanih s podatki, sistemom, osebjem ali okoljem, da lahko nudi stalno in neprekinjeno storitev. Vzpostavljene morajo biti kontrole in pripravljeni načrti, ki bodo zadostili varnostnim zahtevam repozitorija.

2.5 Družina standardov ISO 27000

Informacija je premoženje, zato mora biti ustrezno varovana. Varovanje informacij je še posebej pomembno v poslovnem okolju, ki je ranljivo in izpostavljeno različnim grožnjam. Informacijska varnost je zaščita informacij z namenom zagotovitve neprekinjenega poslovanja, zmanjšanjem poslovnega tveganja in povečanjem donosa naložb in poslovnih priložnosti. Informacijska varnost je vzpostavljena z uvedbo ustreznih nadzornih mehanizmov kot so varnostne politike, definiranje poslovnih procesov na področju varovanja informacij in vzpostavitev ustreznih organizacijskih struktur za podporo informacijski varnosti.

Veliko poslovnih okolij ima informacijske sisteme, ki sami po sebi ne zagotavljajo informacijske varnosti. V takšnih okoljih je vzpostavitev ustreznih upravljavskih ukrepov in procesov ključnega pomena za dvig informacijske varnosti. Družina mednarodnih standardov ISO 27000 vsebuje priporočila in nasvete za pomoč pri zaščiti zaupnosti, integritete in dosegljivosti informacij. Ne gre samo za priporočila na področju tehnološke varnosti, temveč tudi na področju izvedbe ocene tveganja in izvajanje nadzora z namenom izboljšanja informacijske varnosti (The ISO/IEC 27000 Family of Information Security Standards, 2014). Ocena tveganja naj bi odkrila, ovrednotila in prednostno razporedila tveganja glede na njihovo sprejemljivost in cilje informacijske varnosti v poslovnem okolju. Rezultati ocene tveganja pa naj bi bili izhodišče za upravljanje in izboljšanje informacijske varnosti.

2.5.1 Standard SIST ISO/IEC 27001:2013

Že leta 1992 je The Department of Trade and Industry (v nadaljevanju DTI), ki je del državne uprave Velike Britanije, objavil Kodeks ravnanja za upravljanje informacijske varnosti, ki je vseboval priporočila za področje informacijske varnosti in iz katerega se je leta 2000 razvil mednarodni standard ISO 17799 (The history of ISO 17799 and ISO 27001, 2013). Le-ta je vzpostavil smernice na področju informacijske varnosti in je bil leta 2005 preimenovan v ISO 27002:2005. Standard SIST ISO/IEC 27001:2013 Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti - Zahteve (v

nadaljevanju ISO 27001) pa ne vsebuje smernic temveč zapoveduje ukrepe in je tudi standard, na osnovi katerega se lahko pridobi certifikat o skladnosti.

Namen ISO 27001 je zagotoviti model za vzpostavitev, izvajanje, upravljanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema za upravljanje varovanja informacij (v nadaljevanju SUVI) (An Introduction To ISO 27001, 2013). Namen SUVI je zagotoviti ustrezne in učinkovite varnostne kontrole, ki bodo v zadostni meri varovale informacije in vsem zainteresiranim stranem vzbujale zaupanje v sistem. Standard je pripravljen na način Plan – Do – Check – Act oz. Načrtuj – Naredi – Preveri – Analiziraj (v nadaljevanju PDCA) cikla. PDCA cikel je iterativna metoda, ki se uporablja v poslovnih okoljih za nadzor in stalno izboljševanje procesov in proizvodov (PDCA, 2013).

Standard je nabor zahtev, ki jih mora okolje, v katerem poteka proces vzpostavitve SUVI, izpolniti. Zahteve standarda so generične in se jih lahko aplicira v vsako okolje. V prvem delu so opisane posamezne zahteve in določila, ki jih je treba upoštevati pri vzpostavitvi sistema upravljanja varovanja informacij. V drugem delu pa so našteti normativni cilji in kontrolne točke, ki so vodilo in hkrati kontrolni seznam za izvajanje nadzora učinkovitosti vzpostavljenega SUVI. Zahteve, ki morajo biti izpolnjene, so razdeljene v šest sklopov:

I. Vzpostavitev in upravljanje SUVI:

- proces vzpostavitve SUVI je določen z nekaj zahtevami, ki jih mora organizacija v svojem okolju izpolniti in sicer:
  - definirati obseg in opredeliti politiko SUVI glede na značilnosti podjetja, organizacije, njeno lokacijo, sredstva in tehnologijo;
  - določiti metodologijo za upravljanje s tveganji v organizaciji;
  - pridobiti zavezanost vodstva za implementacijo in upravljanje s SUVI.
- uvedba in upravljanje SUVI: organizacija mora oblikovati in implementirati načrt upravljanja s tveganji, v katerem bodo navedene ustrezne akcije, viri, odgovornosti in prioritete pri upravljanju tveganj na področju informacijske varnosti;
- nadzor in ocena SUVI: uvedene morajo biti ustrezne kontrole za takojšnje odkrivanje varnostnih dogodkov glede na cilje nadzora in vzpostavljen sistem merjenja učinkovitosti kontrol. Organizacija mora redno pregledovati upravljanje s SUVI z namenom potrditve obsega SUVI in izboljšave procesov in varnostnih načrtov glede na ugotovitve pregledov;
- vzdrževanje in izboljšanje SUVI: postopki izboljšav SUVI naj izvirajo iz naloženih korektivnih in preventivnih ukrepov in dobrih praks iz okolja. Ukrepi morajo biti usklajeni z vsemu deležniki v izvajanju SUVI glede na njihove pristojnosti in odgovornosti. Organizacija mora zagotoviti in nadzirati, da bodo ukrepi dosegli želene cilje.

II. Zahteve glede dokumentacije:

- dokumentacija mora vsebovati zapise o upravljalnih odločitvah, saj je s tem zagotovljena njihova usklajenost s politikami in zagotovljena ponovljivost dobljenih rezultatov. Vsi postopki, ki so opisani v interni dokumentaciji, morajo biti vzpostavljeni, dokumentirani, implementirani in vzdrževani;
- vzpostavljeni morajo biti mehanizmi za izvajanje zaščite, upravljanje in nadzor dokumentacije SUVI ter mehanizmi za nadzor nad zapisi oz. evidencami dostopov, revizijskimi poročili in obrazci za dodeljevanje dostopnih pravic.

III. Odgovornost vodstva:

- vodstvo mora dokazati zavezanost k vzpostavitvi, uvedbi, nadzoru, vzdrževanju in nenehnemu izboljševanju SUVI z vzpostavitvijo varnostnih politik, dodelitvijo vlog in odgovornosti na področju informacijske varnosti in z določitvijo obsega in ciljev varnostne politike;
- določila varnostne politike morajo biti znana in razširjena v organizaciji. Izvajanje varnostne politike mora biti podvrženo nenehnemu notranjemu nadzoru. Vodstvo mora zagotoviti zadostna sredstva tako za izobraževanje vseh odgovornih v postopkih SUVI kot tudi za izvajanje in izboljševanje SUVI.

IV. Notranji nadzor:

- naloga notranjega nadzora je ugotoviti skladnosti zahtev in izvajanja varnostne politike s trenutno veljavno zakonodajo. Notranji nadzor mora tudi pokazati ali so varnostni ukrepi še učinkovito izvajani in dajejo pričakovane rezultate;
- nadzorniki morajo biti izbrani tako, da ne bodo presojali lastnega dela, sam postopek nadzora pa mora biti načrtovan in dokumentiran.

V. Pregled SUVI s strani vodstva:

- vodstvo se mora zavezati, da bo vsaj enkrat letno pristopilo k pregledu izvajanja SUVI. S tem zagotovi ustreznost, zadostnost in učinkovitost SUVI. Osnova nadzora naj bodo poročila notranjega nadzora, povratne informacije odgovornih oseb SUVI, status preventivnih in korektivnih ukrepov ter grožnje in ranljivosti, ki jih predhodne ocene tveganja niso odkrile ali dovolj izpostavile;
- rezultat pregleda vodstva mora biti izboljšan SUVI, ki bo obvladoval novo odkrita tveganja in povečal nivo učinkovitega obvladovanja obstoječih tveganj.

VI. Proces izboljšave SUVI:

- proces nenehne izboljšave SUVI mora izhajati iz ciljev varnostne politike, temeljiti na rezultatih notranjih in zunanjih nadzorov, analizah zapisov varnostnih dogodkov, rezultatih preventivnih in korektivnih ukrepov in rezultatih nadzora vodstva;

- namen korektivnih ukrepov je odstranitev vzrokov neskladnosti z zahtevamo SUVI ali preprečitev izvajanje akcij, ki niso skladne z določili SUVI. Namen preventivnih ukrepov pa je odstranitev vzrokov, ki bi lahko vodili v neskladnost izvajanja politike SUVI ali preprečitev oz. omejitev pojava potencialnih tveganj. Preventivni ukrepi so običajno stroškovno učinkovitejši – cenejši kot korektivni.

2.5.2 Standard SIST ISO/IEC 27002:2013

Mednarodni standard SIST ISO/IEC 27002:2013 Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti (v nadaljevanju ISO 27002) vsebuje vrsto praktičnih smernic in nadzornih mehanizmov za razvoj, organiziranje in upravljanje učinkovite informacijske varnosti. Standard uvede 11 varnostnih kategorij na področju informacijske varnosti. Nekatere kategorije sovpadajo z zahtevami standarda ISO 27001, druge pa so nove in z njimi tudi nove povezane zahteve in sicer:

- informacijska varnostna politika: politika, ki jo sprejme in potrdi vodstvo, in mora biti jasna ter v skladu s poslovnimi cilji. Izkazovati mora zavezo k upravljanju in vzdrževanju ustrezne in učinkovite informacijske varnosti v organizaciji;
- organiziranje informacijske varnosti: vodstvo mora odobriti politiko, določiti vloge, koordinirati in nadzirati uvedbo politike v organizaciji. Vzpostavljeni morajo biti stiki z zunanjimi varnostnimi strokovnjaki, skupinami in organi z namenom spremljanja razvoja trendov, standardov, metod ocenjevanja in upravljanja incidentov na področju informacijske varnosti;
- upravljanje premoženja: za doseganje in vzdrževanje ustrezne varnosti premoženja, mora biti vse premoženje popisano, imenovan pa mora biti tudi skrbnik – odgovorna oseba. Skrbnik mora imeti jasno opredeljene naloge in odgovornosti v zvezi z informacijsko varnostjo;
- varnost človeških virov: zagotoviti je treba, da zaposleni, izvajalci in tretje stranke razumejo svoje vloge in odgovornosti na področju informacijske varnosti. Odgovornosti morajo biti pojasnjene pred zaposlitvijo, podpisan pa mora biti tudi sporazum o prevzemu varnostnih vlog in odgovornosti. Vsi kandidati za zaposlitev, izvajalci ali uporabniki - tretje osebe morajo biti glede na občutljivost delovnega mesta ustrezno varnostno pregledani. Ob prenehanju dela morajo biti odvzeta vsa sredstva, preklicana vsa pooblastila in dostopne pravice;
- fizična in okoljska varnost: določena morajo biti varnostna območja in varnostni ukrepi, ki bodo preprečili nepooblaščen dostop, povzročanje motenj in škode v prostorih, opremi in na informacijskem sistemu. Nivo varovanja mora biti sorazmeren ugotovljenim tveganjem;
- upravljanje informacijskega okolja: za zagotovitev pravilnega in varnega delovanja informacijskega okolja morajo biti vzpostavljeni ustrezni postopki in odgovornosti. Za zmanjšanje tveganja napak iz malomarnosti ali namerne zlorabe sistema mora biti

uvedeno ločevanje nalog in odgovornosti. Obstajati morajo ločena okolja za razvoj, testiranje in produkcijo in sistem upravljanja s spremembami. Informacijsko okolje mora biti zaščiteno tako pred zlonamernimi vplivi iz okolja kot tudi pred tveganji s strani zunanjih izvajalcev;

- nadzor dostopa: v skladu s poslovnimi in varnostnimi zahtevami je treba nadzorovati dostop do informacij, do poslovnih sistemov in poslovnih procesov za obdelavo informacij;
- nakup, razvoj in vzdrževanje informacijskih sistemov: načrtovanje in uvedba sprememb informacijskega sistema je lahko ključnega pomena za informacijsko varnost. V izogib dodatnim tveganjem mora vsaka sprememba biti identificirana in upravičena v začetnih fazah projekta prenove informacijskega sistema. Vsaka sprememba pa mora biti dogovorjena in dokumentirana kot del poslovnega procesa spremljanja sprememb informacijskega sistema;
- dostop do sistemskih datotek in izvorne kode programske opreme mora biti omejen in strogo nadzorovan. Za zagotavljanje avtentičnosti in celovitosti podatkov mora biti uvedena metoda kriptiranja podatkov in vzpostavljeno upravljanje s kriptirnimi ključi;
- ločeno mora biti razvojno, testno in produkcijsko okolje na način, ki onemogoča nenadzorovano uvajanje sprememb v produkcijsko okolje brez predhodno izvedenih testov. Vsa testiranja, kjer se uporablja realne podatke, morajo biti izvedena na način, ki onemogoča zlorabo zaupnih podatkov;
- upravljanje s tveganji informacijske varnost: zagotoviti je treba, da so varnostni dogodki in pomanjkljivosti, povezane z informacijsko varnostjo, posredovani na način, ki omogoča ustrezno in pravočasno ukrepanje. Vzpostavljen mora biti formalni postopek evidentiranja, zaščite dokazov in poročanja o varnostnih incidentih, ki ga morajo poznati zaposleni, uporabniki in zunanji izvajalci. Vzpostavljena mora biti baza znanja na osnovi izvedenih ukrepov pri reševanju varnostnih incidentov, ki služi kot osnova za izboljšanje informacijske varnosti;
- upravljanje in zagotavljanje neprekinjenega poslovanja: namen načrta neprekinjenega poslovanja je, da s pomočjo preventivnih in obnovitvenih postopkov ob incidentih zmanjšamo verjetnost izgube premoženja na sprejemljiv nivo. Načrt mora identificirati kritične poslovne procese in združiti zahteve informacijske varnosti z ostalimi zahteva, ki morajo biti izpolnjene, če želimo zagotoviti neprekinjeno poslovanje. Načrt neprekinjenega poslovanja mora biti implementiran na način, ki bo omogočal najhitrejšo možno vzpostavitev ključnih procesov. Informacijska varnost mora biti eden od ključnih elementov načrta neprekinjenega poslovanja;
- skladnost: načrtovanje, uvajanje, uporaba in upravljanje informacijskih sistemov morajo biti v skladu z zakonskimi in pogodbenimi zahtevami, ki veljajo v okolju ali državi, kjer bo informacijski sistem deloval. Upoštevane morajo biti posebne zahteve na področju intelektualne lastnine, na področju preprečevanja izgube, potvarjanja ali uničenja informacij in varovanja osebnih podatkov. Informacijski sistemi morajo biti skladni s standardi in tehničnimi zahtevami posameznega okolja in redno nadzorovani s strani uradnih nadzornih organov.

2.6 Standard SIST-TP ISO/TR 17068:2013

Mednarodni standard SIST-TP ISO/TR 17068 - Informatika in dokumentacija - Repozitorij za digitalne zapise zaupanja vredne tretje strani (v nadaljevanju ISO 17068) je spisek zahtev za vzpostavitev in dokazovanje zanesljivega repozitorija. Namen zahtev je definirati servise, sistem in odgovornosti zaposlenih tretjih strani oz. ponudnikov storitve hrambe na način, da bo za zaupano digitalno gradivo zagotovljena zanesljivosti in avtentičnost ter vzpostavljen zanesljiv dostop do gradiva za ves čas hrambe.

V tem standardu so tudi določeni kriteriji zanesljivosti in posebne zahteve za strojno, programsko opremo in upravljanje, ki jih morajo izpolnjevati ponudniki. Glavni namen standarda je zagotoviti zanesljivost hrambe dokumentov, ki si jih izmenjujeta dve stranki ali instituciji, zahteve pa se lahko uporabijo tudi pri dokazovanju zanesljivosti repozitorijev, ki dokumente zgolj hranijo, ne da bi igrali vlogo posrednika med dvema strankama ali ustvarjalcema. Standard je nastal novembra leta 2012, julija 2013 pa je bil prevzet tudi kot slovenski standard.

Tako kot ISO 16363 je tudi standard ISO 17068 odziv na vse večjo potrebo po zanesljivi hrambi digitalnega gradiva in predstavlja eno od možnih rešitev dokazovanja zanesljivosti digitalnih repozitorijev. Dosedanji standardi so se omejevali na zahteve strojne in programske opreme, upravljanja z zapisi in informacijsko varnost. Standard ISO 17068 pa skupaj s standardom ISO 16363 postavlja predvsem kriterije in zahteve za celoten informacijski sistem, ki ustvarjalcem digitalnega gradiva dokazuje zanesljivost in jih lahko preveri pooblaščen nadzorni organ.

Standard v svojih zahtevah povzema dobre prakse iz nekaterih standardov drugih področij, na področju dolgotrajne hrambe digitalnega gradiva pa dosega nivo zahtevnosti že uveljavljenih standardov kot npr. ISO 15489 in ISO 14721 (ISO 17068, str. 4). ISO 17068 pa uvaja tudi nekaj novih izrazov in definicij na področju dolgotrajne hrambe, hkrati pa prinaša izraze in definicije iz ostalih področij in prilagaja njihov pomen. Povsem novi izrazi in definicije so (ISO 17068, str. 1):

- tretja stran (angl. *third party*) je oseba ali ustanova, neodvisna od ustvarjalcev gradiva-strank;
- repozitorij zaupanja vredne tretje osebe (angl. *trusted third party repository*, v nadaljevanju TTPR) je nabor storitev, sistemov in osebja, ki zagotavljajo avtentičnost in zanesljivost digitalnega gradiva, ki ga je v hrambo predal ustvarjalec;
- TTPR certifikat je digitalni dokument, izdan z namenom dokazovanja avtentičnosti dokumenta v hrambi pri TTPR;
- TTPR storitev je neopredmeten proizvod, rezultat vsaj ene aktivnosti med ustvarjalcem in ponudnikom;

- zanesljiv SIP (angl. *trusted SIP*, v nadaljevanju TSIP) je SIP, ki ga je ustvarjalec predal TTPR in vsebuje digitalni podpis ustvarjalca in časovni žig ponudnika, ki vsebuje čas predaje in informacije o pošiljatelju;
- zanesljiv AIP (angl. *trusted AIP*, v nadaljevanju TAIP) je AIP, ki poleg vsebine vsebuje še informacijo o vsebini (CI), digitalni podpis ustvarjalca, časovni žig ponudnika in ustrezno informacijo o opisu vsebine (PDI);
- zanesljiv DIP (angl. *trusted DIP*, v nadaljevanju TDIP) je IP, pridobljen iz enega ali več TAIP na osnovi zahteve, ki jo je stranka podala TTPR.

Prvič pa ISO 17068 definira zanesljiv repozitorij, in sicer je zanesljivost (angl. *trustworthiness*) lastnost TTPR, da je zanesljiv in verodostojen. Zanesljivemu TTPR lahko zaupamo, da bo svoje storitve izvajal na verodostojen način z dokumentiranimi politikami in ves čas zagotavljal zanesljivo hrambo gradiva. Znotraj procesa izvajanja storitev mora zanesljiv repozitorij zagotavljati avtentičnost, verodostojnost, celovitost in uporabnost digitalnega gradiva za obdobje pogodbene hrambe. (ISO 17068, str. 3). V standardu so določene tudi tri glavne značilnosti TTPR, in sicer:

- stabilnost – TTPR mora zagotoviti stabilnost svojega obstoja. Poleg plana varovanja pred nesrečami in obnovitvenega načrta mora TTPR razpolagati z ustreznimi finančnimi in kadrovskimi viri, upravljavskimi strategijami in izvedbenimi zmožnostmi, da je zmožen ohranjati zaupano gradivo tudi v izrednih razmerah;
- strokovnost – TTPR mora imeti dovolj strokovnega znanja za upravljanje digitalnega gradiva. TTPR mora zaposlovati osebje, ki je dovolj strokovno usposobljeno za vzdrževanje in upravljanje informacijskega sistema ter za vzdrževanje in upravljanje postopkov in procesov, povezanih z upravljanjem digitalnega gradiva;
- nevtralnost – TTPR mora ostati nevtralna tretja stranka, neodvisna od politične situacije, zahtev ustvarjalcev ali deležnikov, saj bo le tako lahko dokazovala svojo zanesljivost in verodostojnost.

Glavne zahteve ISO 17068 glede vzpostavitve storitve posegajo na področje:

- poteka postopka storitve – ko je pogodba med TTPR in ustvarjalcem sklenjena, mora ustvarjalec v svojem sistemu vzpostaviti vse procedure in postopke, ki bodo zagotavljali pripravo gradiva in ustreznih dodatnih vsebin v obliki TSIP, kot jih zahteva TTPR (npr. vzpostavitev sistema digitalnega podpisovanja);
- pogodbe o izvajanju storitve – TTPR mora v pogodbi s stranko določiti vrsto storitve, obdobje izvajanja storitve, dolžnosti stranke in odgovornosti TTPR. Posebno mesto v pogodbi mora imeti določilo, ali je stranka dolžna posredovati TTPR podatke za dokazovanje in zagotavljanja avtentičnosti predanega gradiva. Na tem mestu standard predlaga tudi Service level agreement (v nadaljevanju SLA) povzet po standardu ISO/IEC 20000-1:2011 (ISO 17068, str. 2) kot del pogodbe. Z SLA naj bi bilo določeno obdobje izvajanja storitve, načini in postopki prenos gradiva v repozitorij, tip

storitve repozitorija, varovanje podatkov in način obveščanja. Standard navaja naslednje tipe storitve:

- preprost repozitorij – za določeno obdobje se izvaja hramba dokumentov brez dokazov o njihovi avtentičnosti. Po preteku pogodbenega obdobja se dokumentne izbriše na način, da ni možna njihova obnova;
- storitev prenosa in migracije – repozitorij lahko deluje le kot zanesljiv posrednik gradiva med dvema institucijama z ali brez zagotavljanja vmesne hrambe gradiva;
- storitev hrambe in certificiranja – repozitorij hrani gradivo v pogodbenem obdobju. Repozitorij preveri informacije o avtentičnosti gradiva ob prevzemu in zagotavlja njegovo avtentičnost v obdobju hrambe. Po izteku pogodbenega obdobja se gradivo izbriše na način, da ni možna njegova obnova;
- certificiranje brez repozitorija – repozitorij hrani samo metapodatke o gradivu brez gradiva. Z metapodatki lahko dokazuje avtentičnost gradiva.

Standard ISO 17068 pa med svojimi zahtevami našteva tudi obvezne in neobvezne storitve, ki jih mora TTPR nuditi svojim strankam. Te storitev so:

- Storitev pridobivanja gradiva: je obvezna storitev TTPR, ki obsega vse postopke in procese, ki jih mora izvesti ustvarjalec gradiva pred predajo gradiva in vse postopke in procese, ki jih izvaja TTPR v procesu prevzema gradiva.
- Storitev hrambe: je obvezna storitev TTPR, ki obsega vse postopke in procese povezane z upravljanjem gradiva in zagotavljanjem zanesljive in verodostojne hrambe.
- Storitev dostopa in uporabe gradiva: je obvezna storitev, ki omogoča ustvarjalcem iskanje in uporabo gradiva v skladu s pogodbenimi dovoljenji.
- Storitev izdaje gradiva: je obvezna storitev, ki zagotavlja, da bo TTPR gradivo ustvarjalca predal njemu ali kateri drugi stranki v skladu s pogodbenimi dogovori.
- Storitev pretvorbe formatov: je neobvezna storitev pretvorbe gradiva iz enega v drug format, ki jo svojim strankam lahko nudi TTPR.
- Storitev prenosa in migracije: je neobvezna storitev, s katero TTPR omogoča svojim strankam prenos gradiva k drugemu TTPR ali v drug repozitorij.
- Storitev odstranjevanja gradiva: je obvezna storitev TTPR, s katero TTPR zagotavlja uničenje gradiva po izteku pogodbeno določenega roka hrambe. Uničenje mora biti izvedeno na način, da ni možna obnova gradiva.
- Storitev izdajanja certifikatov: je obvezna storitev, ki omogoča TTPR, da izda certifikat o avtentičnosti za neko gradivo v hrambi.
- Storitev izdaje certifikata brez izvajanja hrambe: je neobvezna storitev, ki omogoča ustvarjalcem, da TTPR hrani samo metapodatke o dokumentu, sam dokument pa je pri ustvarjalcu. Ta storitev omogoča TTPR, da oddaljeno podeli certifikat o avtentičnosti za takšno gradivo.

Za zagotavljanje zanesljivosti in verodostojnosti je ključnega pomena tudi vzpostavitev varnega in zanesljivega informacijsko komunikacijskega okolja. Sistem mora biti zaščiten

tako pred okoljskimi nevarnostmi, pred nevarnostmi računalniških vdorov kot tudi pred nevarnostmi zaradi izpostavljenosti javnemu omrežju. Zato ISO 17068 obravnava tudi zahteve na tem področju, ki jih mora upoštevati vsak TTPR od začetka delovanja dalje. Te zahteve so:

- zahteva po uporabi ustrezne programske opreme, ki zagotavlja vse zahtevane funkcionalnosti v postopku hrambe gradiva;
- zahteva po uporabi prenosnega sistema, ki zagotavlja zanesljiv in zaščiten način prenosa informacij in gradiva med ustvarjalcem in TTPR;
- zahteva po računalniškem omrežju, ki zagotavlja varen in zaščiten prenos iz zunanjega sveta v okolje TTPR;
- zahteva po uvedbi sistema časovnega žigosanja, ki zagotavlja sledljivost prenosa gradiva v repozitorij in je del sistema zagotavljanja avtentičnosti in celovitosti gradiva v hrambi;
- zahteva po revizijski sledi, kjer bo evidentiran vsak postopek ali proces, ki je bil izveden nad nekim gradivom od trenutka, ko je prišlo v repozitorij do izteka pogodbeno dogovorjenega roka hrambe;
- zahteva po zagotavljanju informacijske varnosti sistema z vsemi nadzornimi in kontrolnimi mehanizmi, ki so potrebni za zagotavljanje zanesljivosti TTPR;
- zahteva po sistemu nadzora dostopa, ki obsega nadzor, beleženje in hrambo evidenc fizičnega in logičnega dostopa do sistema, ne glede na to ali gre za pooblaščen ali nepooblaščen dostop;
- zahteva po vzpostavitvi sistema preprečevanja nesreč, s katerim TTPR zagotavlja neprekinjeno delovanje;
- zahteva po izdajanju certifikatov in vrednotenji digitalnega gradiva, s katerim TTPR zagotavlja procese in postopke za vrednotenje gradiva in izdajo certifikatov, s katerimi izkazuje avtentičnost gradiva;
- zahteva po vzpostavitvi nadomestnega (angl. *backup*) sistema, s katerim vzpostavlja ustrezen nivo varovanja gradiva za ves čas njegove hrambe;
- zahteva po vzpostavitvi sistema oddaljenega repozitorija, ki omogoča potrjevanje in izdajo certifikatov o avtentičnosti gradiva.

ISO 17068 pa postavlja tudi sklop upravljavskih zahtev, katerih namen je zagotavljanje zanesljivosti in stabilnosti delovanja sistema. Te zahteve so:

- upravljanje s klienti – strankami TTPR, ki mora zagotavljati upravljanje z dovoljenji in pooblastili ustvarjalcev za dostop in uporabo gradiva;
- upravljanje z administratorskimi dovoljenji, kjer je treba zagotoviti ustrezen nivo pooblastil glede na vlogo v sistemu in sledenje dostopom uporabnikov z administratorskimi pooblastili;
- upravljanje z računalniškim omrežjem in varnostjo, kjer gre za sledenje in nadzor dostopa do sistema;

- upravljanje z zapisi, kjer gre za preprečevanje uporabe škodljive programske opreme, nadzor nad formati in zagotavljanje uporabnosti gradiva s postopki migracije;
- upravljanje s prejetimi in poslanimi sporočili, kjer gre za upravljanje vseh sporočil, ki potujejo med ustvarjalcem oz. stranko in TTPR od začetka postopka registracije (npr. uporabniško ime in geslo, ki lahko potujeta po računalniškem omrežju) pa do zaključka pogodbene hrambe in uničenja gradiva;
- upravljanje z revizijskimi sledmi, kjer gre za spremljanje in preprečevanje spreminjanja ali brisanja revizijskih sledi v sistemu;
- upravljanje z nadomestnimi (angl. *backup*) postopki in postopki okrevanja (angl. *recovery*), ki morajo zagotoviti razpoložljivost sistema in zagotavljati njegovo celovitost in nespremenljivost;
- upravljanje z informacijsko varnostjo, kjer gre za postopke spremljanja informacijske varnosti in odkrivanja kršitev; na tej točki standard priporoča tudi dodaten sistemski prostor za nadomestni (angl. *backup*) sistem;
- upravljanje s postopki prejema in migracije gradiva, kjer gre za vzpostavitev takšnega sistema, ki omogoča prejem gradiva od drugih repozitorijev ali TTPR ali prenos/migracijo gradiva v druge repozitorije ali TTPR
- upravljanje s sistemom za kliente, kjer gre za omogočanje sistemskemu klientu, da pripravi ustrezen SIP za prenos v TTPR, da dostopa in pregleduje vsebino predanega gradiva brez možnosti njegovega spreminjanja, in da vse to počne preko šifriranega ali kako drugače zaščitenega prenosa (npr. s sistemom javnega ključa).

3 OHRANJANJE DIGITALNEGA ARHIVSKEGA GRADIVA V SLOVENIJI

3.1 Zakonodaja v Sloveniji

V Republiki Sloveniji področje varovanja dokumentarnega in arhivskega gradiva ureja kar nekaj predpisov. Krovni zakon je ZVDAGA. Zakon dopolnjuje podzakonski akt Uredba o varstvu dokumentarnega in arhivskega gradiva (Ur.l. RS, št. 86/2006, v nadaljevanju UVDAG). Na področju upravljanja in varovanja gradiva v digitalni obliki pa imamo še dva dodatna predpisa in sicer Enotne tehnološke zahteve (Arhiv Republike Slovenije, 2013, v nadaljevanju ETZ) in Splošne pogoje za izvajanje akreditacije (Arhiv Republike Slovenije, 2012). Pravilnik, ki ureja usposabljanje delavcev, ki delajo z dokumentarnim in arhivskim gradivom, pa je Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom (Ur.l. RS št. 132/2006).

ZVDAGA med drugim ureja način, organizacijo, infrastrukturo in izvedbo hrambe dokumentarnega gradiva v fizični in elektronski obliki, vključno s pravnimi učinki takšne hrambe (Žumer, 2007, str. 29). Zakon je ob sprejetju leta 2006 bistveno nadgradil dotedanjo ureditev varstva gradiva s celovitim pristopom k varstvu gradiva v digitalni

obliki. Določeni so postopki in pogoji varstva gradiva v digitalni obliki tako, da je od zajema, pretvorbe, hrambe do uporabe in reprodukcije zagotovljena njegova uporabnost, dostopnost, nespremenljivost, celovitost vsebine in oblike, avtentičnost, verodostojnost in prenosljivost. ZVDAGA opredeljuje dolgoročno hrambo kot hrambo gradiva za časovno obdobje daljše od 5 let. Storitve hrambe gradiva v digitalni obliki pa opredeljuje kot neločljivo povezane z ohranjanjem vsebine gradiva v digitalni obliki, vendar ne gre za ponudbo opreme za takšno hrambo.

3.1.1 Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih

Slovenski arhivski zakon ZVDAGA v 40. členu določa, da so ustvarjalci arhivskega gradiva dolžni le-to izročiti pristojnemu arhivu najkasneje 30 let po nastanku gradiva. Za digitalno gradivo je to dolga doba tako s stališča zagotavljanja uporabnosti, celovitosti in avtentičnosti, kot s stališča količine gradiva, ki v takšnem obdobju nastane. Ker je arhivsko gradivo ne samo kulturna dediščina, temveč lahko predstavlja tudi dokumentacijo, pomembno za pravno varnost države, njenih institucij in posameznika, pa je razumljivo, zakaj poskuša Republika Slovenija in slovenska arhivska stroka dobiti zagotovilo, da se bo z arhivskim gradivom, ki ga hranijo ponudniki, ravnalo v skladu z načeli arhivske stroke.

Ponudnik storitve hrambe dokumentarnega gradiva v digitalni obliki je, po ZVDAGA, vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči hrambo dokumentarnega gradiva v digitalni obliki na svoji infrastrukturi. Definira pa tudi pojem notranjih pravil za zajem in hrambo gradiva v digitalni obliki kot pravil, ki jih kot svoj interni pravni akt sprejme pravna oseba, da bi definirala vse postopke, procese in odgovornosti glede hrambe svojega gradiva.

Trenutno veljavna zakonodaja uporablja izraz »akreditacija«, ki ni najbolj ustrezen. V Sloveniji obstaja samo en akreditacijski organ (Slovenska akreditacija), ki podeljuje akreditacije organom, ki izvajajo postopke certificiranja proizvodov, naprav in storitev (Slovenska akreditacija, 2013). Iz tega je razvidno, da bi bil primernejši izraz za postopke, ki ugotavljajo skladnost delovanja ponudnika storitve s trenutno veljavno zakonodajo *certificiranje* in v povezavi s tem tudi izraz *certificiran* ponudnik storitve in ne akreditiran ponudnik storitve.

Ponudniki storitve zajema in hrambe digitalnega gradiva v Sloveniji niso dolžni svoje storitve akreditirati, saj ZVDAGA v svojem 72. členu jasno govori, da so zavezani k akreditaciji svoje storitve samo tisti ponudniki, ki želijo izvajati hrambo gradiva v digitalni obliki za javnopravne osebe in arhive. Iz 1. odstavka 83. člena ZVDAGA torej sledi, da se lahko za storitev zajema in hrambe digitalnega gradiva na trgu v Sloveniji registrira vsakdo. Samo ponudnik akreditirane storitve zajema in hrambe pa ima dokazilo, da je zaupanja vreden in da posluje skladno s predpisi .

3.1.2 Uredba o varstvu dokumentarnega in arhivskega gradiva

UVDAG nadgradi zakon ZVDAGA s podrobno pojasnjenimi določbami o varstvu dokumentarnega in arhivskega gradiva v digitalni obliki. ETZ zahteve pa določajo oz. standardizirajo način in sistem ter pogoje za izvajanje dolgotrajne hrambe digitalnega gradiva fizičnih in pravnih oseb, ki morajo do izročitve gradiva pristojnemu arhivu zagotavljati tudi njegovo dolgotrajno hrambo. Obveznost dolgotrajne hrambe ni mogoče naložiti samo državnim in javnim arhivom, saj so roki izročitve gradiva pristojnemu arhivu lahko tudi 30 let, kar pa je predolga doba, da bi lahko ohranili gradivo v digitalni obliki brez ukrepov.

Problem digitalnega gradiva je, da ga lahko spreminjamo ali uničimo brez sledi, zato je za zagotavljanje pravne veljavnosti in dokazne vrednosti takšnega gradiva nujno potreben proces sledljivosti zapisa oz. zagotavljanje revizijske sledi. Postopek zajema in hrambe mora biti podprt z ustreznimi varnostnimi tehnologijami in organizacijskimi ukrepi. ZVDAGA v 31., 32. in 33. členu določa tri različne scenarije, po katerih se presoja pravna veljava takšnega gradiva:

- če ima organizacija, ki zajema in hrani digitalno gradivo, pri državnemu arhivu potrjena notranja pravila in dokazano posluje v skladu z njimi, pravne veljavnosti gradiva ni treba posebej dokazovati;
- če ima organizacija notranja pravila za zajem in hrambo, vendar le-ta niso potrjena pri državnem arhivu, potem mora za priznanje pravne veljavnosti dokazati, da so notranja pravila skladna s slovenskimi predpisi na tem področju in da posluje v skladu z njimi;
- če organizacija nima notranjih pravil ali pa jih ima, vendar se jih v konkretnem primeru ni držala, mora dokazovati pravno veljavnost gradiva za vsak primer posebej.

3.1.3 Enotne tehnološke zahteve

ETZ so vrsta zahtev, ki podrobneje opredeljujejo poslovne, organizacijske in tehnološke pogoje za zajem in hrambo in so vezni člen med zakonskimi zahtevami in hitro spreminjajočimi se potrebami prakse. Dokument je razdeljen na tri dele, ki po vrsti obravnavajo:

- 1. del: Uvodna poglavja in priloge – kjer poleg pojmovnika vsebuje še seznam priporočenih oblik zapisa za dolgoročno hrambo in seznam najpogosteje uporabljenih mednarodnih standardov, ki so služili kot vodilo pri pripravi zahtev;
- 2. del: Enotne tehnološke zahteve za zajem in hrambo gradiva v digitalni obliki – vsebuje zahteve, ki opredeljujejo pomembne postopke in procese pri zajemu in hrambi in so opredeljene v notranjih pravilih organizacije;
- 3. del: Dodatne enotne tehnološke zahteve za ponudnike, strojno in programsko opremo ter storitve - vsebuje zahteve, ki so namenjene ponudnikom opreme in storitev in se nanašajo na postopke akreditacije opreme in storitev.

V II. delu ETZ so navedene zahteve, ki jih morajo upoštevati vsi, ki pripravljajo notranja pravila za zajem in hrambo. Nekaj zahtev je posebej izpostavljenih in jih morajo izpolnjevati samo ponudniki storitve zajema in hrambe. Zahtev v II. delu je 143, kar za pripravo notranjih pravil pomeni, da je treba za vsako zahtevo predložiti ustrezen dokument, v katerem je napisano, kako jo ponudnik izpolnjuje. V primeru ponudnika, ki ima enega izmed certifikatov (ISO 9001, ISO 27001) ali celo oba, pa je teh zahtev precej manj. Tabela 1 prikazuje primerjavo števila zahtev ETZ, ISO 9001 in ISO 27001.

Tabela 1: Primerjava zahtev EZT 2.1 II. del z zahtevami ISO 9001 in ISO 27001

Poglavje v ETZ 2.1 II.del	**Št. zahtev**	**Standard ISO 9001**	**Standard ISO 27001**
1.1.2. Notranja pravila za zajem in hrambo	8	X	X
1.1.3. Nadzor nad izvajanjem	6	X	X
1.2.1. Notranja organizacija	4	X	X
2.1. Splošno o delovnih postopkih	1	X	X
2.5.2. Neprekinjeno poslovanje	14		X
2.7. Izločanje in uničevanje dokumentarnega gradiva	4		X
3.1. Popis in varnostna razvrstitev informacijskih virov	3		X
3.2. Organiziranje informacijske varnosti	7	X	X
3.3. Fizično in tehnično varovanje prostorov in opreme	4		X
3.4. Upravljanje dostopnih pravic do sistema in gradiva	5	X	X
3.5. Revizijske sledi	3		X
3.6. Upravljanje varnostnih incidentov	4	X	X
4.1. Električna in telekomunikacijska napeljava	1		X
4.2. Strojna oprema	6	X	X
4.3. Nosilci zapisa	4		X
4.4. Programska oprema	10	X	X
5.1. Upravljanje sprememb	1		X
5.2. Ločevanje operativnega okolja od okolja, namenjenega razvoju, in od okolja za preizkušanje	1		X
5.4. Zaščita pred zlonamerno programsko opremo in vdori	1		X
5.5. Sinhronizacija sistemskih ur	1		X
5.6. Vzdrževanje informacijske opreme in infrastrukture	1		X
5.7. Nadzor, varnostni pregledi in zagotavljanje zapisov o delovanju sistema	4	X	X
6.1. Pogodbeno urejanje izvajanja storitve (med naročnikom in izvajalcem)	2	X	X

V primeru, da ima ponudnik certifikat ISO 9001, ima z njim izpolnjenih 57 zahtev, v primeru, da pa ima certifikat ISO 27001, pa še dodatnih 38 zahtev, kar pomeni, da

ponudnik s certifikatom ISO 27001 izpolnjuje 95 od 143 zahtev oz. 66% vseh zahtev. V tabeli so v prvem stolpcu navedena poglavja ETZ 2.1 II. del, v drugem število zahtev v poglavju, v tretjem in četrtem stolpcu pa je označeno, če se enakovredne zahteve nahajajo bodisi v standardu ISO 9001 ali ISO 27001. Tudi za postopke akreditacije strojne in programske opreme ter storitev lahko v mednarodnih standardih najdemo enakovredne zahteve:

- v postopku akreditacije strojne opreme, je vseh 6 zahtev iz ETZ 2.1 III. del poglavje 2 Akreditacija strojne opreme vsebovanih tudi v poglavju 6.3 Infrastruktura standarda ISO 9001;
- v postopku akreditacije storitve je treba v ETZ 2.1 III. del izpolniti samo eno zahtevo, ki je enakovredna z zahtevami ISO 27001 v 4. poglavju in ISO 9001v 4. poglavju;
- v postopku akreditacije programska opreme pa je v ETZ 2.1 III. del navedenih 132 zahtev. V primeru, da ima ponudnik certifikat ISO 9001 ali ISO 27001 in razvija lastno programsko opremo, potem je poglavje 3.2 Razvoj in vzdrževanje programske opreme s svojimi 8 zahtevam enakovredno zahtevam, ki jih najdemo v obeh standardih.

Ponudnik storitve, ki bo akreditiral programsko opremo, ki jo je kupil ali samostojno razvil, mora izpolniti ETZ 2.1 III. del poglavje 3. Število zahtev, ki jih mora izpolnjevati programska oprema je odvisno od tega, v kateri funkcionalni tip jo bo ponudnik razvrstil. Programska oprema je razdeljena v funkcionalne tipe glede na namen, ki ga ima v postopku zajema in hrambe. Tabela s funkcionalnimi tipi in seznamom zahtev, ki morajo biti izpolnjene za vsak posamezne funkcionalni tip, se nahaja v drugem delu ETZ 2.1 III. del v poglavju Obrazložitev.

3.1.4 Splošni pogoji za izvajanje akreditacije

V predpisu Splošni pogoji za izvajanje akreditacije (Arhiv Republike Slovenije, 2012) je natančno opisan postopek in opredeljeni stroški akreditacije. Predpis opredeljuje pojem akreditacije kot postopek, s katerim Arhiv RS priznava skladnost opreme oz. storitev z veljavnimi predpisi v Republiki Sloveniji. V samem postopku akreditacije poleg ponudnika in Arhiva RS sodelujejo še s strani Arhiva RS pooblaščeni zunanji presojevalci. Če je v postopku pridobivanja akreditacije ugotovljeno, da ponudnik izpolnjuje vse zahteve iz veljavnih predpisov in pravil stroke se mu v skladu z 86. členom ZVDAGA izda sklep o podelitvi akreditacije.

Akreditacijo storitve lahko ponudnik v skladu s 35. členom UVDAG in 9. členom Splošnih pogojev za izvajanje akreditacije pridobi samo za obdobje 1 leta in je ni mogoče pridobiti za nedoločen čas, kar pomeni, da mora ponudnik vsako leto v postopkih podaljšanja akreditacije ponovno dokazovati skladnost izvajanja svoje storitve z veljavnimi predpisi. Arhiv RS pa ima v svojih rokah tudi instrument izrednega odločevalnega postopka (9. člen Splošnih pogojev za izvajanje akreditacije), ki ga lahko izvede pri ponudniku v primeru

suma kršitve predpisov, pravil stroke ali pogodbe o izvajanju akreditacije. Če so kršitve potrjene, lahko Arhiv RS akreditacijo takšnemu ponudniku tudi odvzame.

3.2 Postopek pridobitve certifikata ponudnika storitve hrambe v Sloveniji

Postopek akreditacije storitve oz. pridobivanja certifikata za ponudnike je večstopenjski.

1. stopnja –registracija ponudnika

ZVDAGA v 83. členu nalaga vsem ponudnikom, da svojo storitev zajema in hrambe registrirajo pri državnem arhivu najmanj 8 dni pred začetkom izvajanja. Le-ta preveri, če ponudnik izpolnjuje pogoje in če jih, izda odločbo o registraciji in vpiše ponudnika v Register akreditirane opreme in storitev. V tem primeru govorimo o upravnem postopku, ki ne vsebuje nikakršnih nadzornih pregledov pri ponudniku. UVDAG v svojem 21. členu sicer navaja pogoje, ki jih mora izpolnjevati ponudnik, ki želi biti registriran, vendar ti pogoji ne govorijo o infrastrukturi ali organizacijskih ukrepih, temveč zgolj o izobrazbi in strokovni usposobljenosti zaposlenih, ki bodo delali z gradivom.

2. stopnja - potrjena notranja pravila

Predpogoj za začetek postopka akreditacije storitve so pri državnem Arhivu RS potrjena notranja pravila. Kot nalaga ZVDAGA v svojem 18. členu, mora ponudnik storitve, ki bo plačno ali neodplačno zajemal in hranil gradiva v digitalni obliki, sprejeti notranja pravila v skladu s tem zakonom, na njegovi podlagi izdanimi podzakonskimi predpisi in Enotnimi tehnološkimi zahtevami ter pravili stroke (npr. arhivska stroka, informacijska varnost, itd.). Notranja pravila zajema in hrambe gradiva v digitalni obliki ZVDAGA v 2. členu opredeljuje kot interni pravni akt, ki ga sprejme ponudnik storitve.
Po 19. členu ZVDAGA mora ponudnik storitve svoja notranja pravila predložiti v presojo in potrditev Arhivu RS. V notranjih pravilih so opisani postopki in procesi na področju zajema in hrambe digitalnega gradiva, dodeljene odgovornosti za te postopke in opredeljena informacijska varnostna politika. Za samoocenitev svojega okolja je Arhiv RS vlagateljem pripravil predpis ETZ II. del, v katerem so navedene zahteve, ki se tičejo procesov, postopkov in odgovornosti pri zagotavljanju zanesljivega zajema in hrambe digitalnega gradiva.

3. stopnja –akreditirana strojna in programska oprema

Naslednji od predpogojev, ki ga mora ponudnik storitve izpolnjevati, če želi svojo storitev akreditirati, je tudi uporaba akreditirane strojne in programske opreme, s katero bo storitev izvajal. Strojno in programsko opremo lahko akreditira sam, če pa uporablja opremo, ki jo je akreditiral že drug ponudnik opreme, pa se lahko sklicuje na že podeljeno akreditacijo in mu ni treba opreme še enkrat akreditirati. Postopek akreditacije strojne ali programske

opreme je poseben postopek, kjer se preverja skladnost opreme z zahtevami, ki so navedene v ETZ III. del. Ko so predpogoji izpolnjeni, ponudnik lahko vloži zahtevek za akreditacijo storitve pri državnem arhivu.

Postopek akreditacije je pogodbeni odnos med Arhivom RS, vlagateljem zahtevka in zunanjim revizorjem, ki ga Arhiv RS pooblasti za izvedbo nadzornega postopka pri vlagatelju. Nadzorni postopek obsega najprej preverjanje izpolnjevanja predpogojev na področju izobrazbe zaposlenih in uporabe akreditirane strojne in programske opreme. V drugem koraku nadzornega postopka pa se preverja tudi ali vlagatelj posluje v skladu s potrjenimi notranjimi pravili. Če nadzorni postopek ne ugotovi neskladij, ki bi predstavljale omejitev za zagotavljanje zanesljivega zajema in hrambe digitalnega gradiva, Arhiv RS vlagatelju – ponudniku storitve izstavi sklep in ga vpiše v Register akreditirane opreme in storitev. S tem se proces pridobivanja akreditacije zaključi.

Ponudnik akreditirane storitve pa mora podeljeno akreditacijo vsako leto podaljševati. Postopek podaljšanja je enak postopku prve akreditacije, saj morajo biti še vedno izpolnjeni vsi predpogoji. Tako so zaposleni, ki rokujejo z gradivom, dolžni vstopiti v proces konstantnega usposabljanja in pridobivanja kreditnih točk na področju varovanja arhivskega in dokumentarnega gradiva z udeležbo na tečajih, seminarjih in delavnicah.

Ob vsakoletnem podaljšanju zunanji revizor, pooblaščen s strani Arhiva RS, preverja tudi, če ponudnik storitve za izvajanje svoje storitve še vedno uporablja akreditirano strojno in programsko opremo in če je njegovo poslovanje še vedno v skladu z njegovimi potrjenimi notranjimi pravili. Tako postopek pridobitve kot tudi vsakoletni postopek podaljšanja akreditacije pa za ponudnika ne predstavlja samo organizacijsko temveč tudi finančno breme.

Arhiv RS sklene s ponudnikom in zunanjim pooblaščencem za izvajanje nadzornih pregledov pogodbo, katere del so tudi ocenjeni stroški postopka. Stroški nadomestila Arhivu za vodenje postopkov so navedeni v Splošnih pogojih za izvajanje akreditacije in se gibljejo od 300 EUR za akreditacijo posameznega modela ali serije strojne opreme do 2000 EUR za akreditacijo aplikativne programske opreme, ki zagotavlja celovit sklop funkcionalnosti varstva dokumentarnega in arhivskega gradiva v digitalni obliki oz. 2000 EUR za akreditacijo storitve za zajem in hrambo digitalnega gradiva.

Tem stroškom je treba dodati še nadomestilo pooblaščenemu revizorju, ki izvede nadzorni pregled. To nadomestilo je ocenjeno v obliki svetovalnega dne. Glede na vrsto akreditacije (strojna oprema, programska oprema ali storitev) lahko nadzorni pregled obsega od 1 do 7 dni. Vlagatelji se torej srečajo najprej s stroškom za pridobitev akreditacije, nato pa še z vsakoletnim stroškom za obnovitev akreditacije. Simulacija ocenjenih stroškov, s katerimi se sreča vlagatelja, ki še ni registriran, pa bi želel pridobiti akreditacijo svoje storitve:

I. Vlagatelj vloži zahtevek za registracijo z vsemi dokazili o izpolnjevanju pogojev. Arhiv RS mu izstavi odločbo o registraciji ponudnika opreme in storitev (upravni postopek – strošek 22,66 EUR).

II. Vlagatelj za svojo storitev uporablja strežnik, diskovno polje in optični bralnik. Ker oprema še ni akreditirana, pristopi k postopku akreditacije strojne opreme:

- organizacijski ukrep – za vsak kos opreme mora opraviti samoocenitev v obliki izpolnitve ETZ III. del poglavje 2 Akreditacija strojne opreme in pridobiti od proizvajalca opreme vsa zahtevana dokazila;
- strošek
  - za vsak kos opreme je nadomestilo Arhivu RS za vodenje postopka – skupaj 900 EUR;
  - za vsak kos opreme je nadomestilo revizorju za pregled skladnosti strojne opreme z zahtevami naših predpisov in pripravo poročila – 3 svetovalni dnevi.

III. Vlagatelj za svojo storitev uporablja aplikativno programsko opremo, ki zagotavlja celovit sklop funkcionalnosti na področju zajema in hrambe, vendar oprema še ni akreditirana:

- organizacijski ukrep – samoocenitev v obliki izpolnjenega ETZ III. del poglavje 3 Akreditacija programske opreme in če ne gre za v svetu razširjen programski produkt, pridobiti še vsa dokazila o razvoju in testiranju programske opreme;
- strošek
  - nadomestilo Arhivu RS za vodenje postopka – 2000 EUR;
  - nadomestilo revizorju za izvedbo nadzornega pregleda na lokaciji ponudnika in pripravo poročila– 5 svetovalnih dni.

IV. Vlagatelj za svojo storitev uporablja aplikativno programsko opremo, ki zagotavlja posamezno funkcionalnost na področju zajema in hrambe (npr. programski produkt za digitalizacijo papirnega gradiva), vendar oprema še ni akreditirana:

- organizacijski ukrep – samoocenitev v obliki izpolnjenega ETZ III. del poglavje 3 Akreditacija programske opreme in če ne gre za v svetu razširjen programski produkt, pridobiti še vsa dokazila o razvoju in testiranju programske opreme;
- strošek
  - nadomestilo Arhivu RS za vodenje postopka – 500 EUR;
  - nadomestilo revizorju za izvedbo nadzornega pregleda na lokaciji ponudnika in pripravo poročila– 3 svetovalni dnevi.

VII. Vzpostavitev ustreznega okolja za izvajanje storitve:

- organizacijski ukrepi - priprava notranjih pravil in uskladitev poslovanja z njimi;

- strošek
  - implementacija informacijske varnostne politike (ETZ 2.1 II. del) in načrta neprekinjenega poslovanja. ETZ 2.1 v II. delu v poglavju 2.5. predvidevajo vzpostavitev dveh oddaljenih lokacij za namene varnostnega kopiranja podatkov, pri čemer mora biti ena vsaj 30 km zračne linije oddaljena od primarne lokacije izvajanja storitve. – neopredeljen strošek, odvisen od tega, kaj vlagatelj že ima oz. kaj mora vzpostaviti zaradi zahtev naših predpisov – strošek gre lahko v nekaj 100.000 EUR;

VIII. Postopek pridobivanja akreditacije storitve:

- organizacijski ukrep – priprava samoocenitve v obliki izpolnjenih zahtev iz ETZ 2.1 II. del;
- strošek:
  - nadomestilo Arhivu RS za vodenje postopka – 2000 EUR;
  - nadomestilo revizorju za izvedbo nadzornega pregleda na lokaciji ponudnika in pripravo poročila– 5 svetovalnih dni.

Če ocenimo svetovalni dan revizorja na 500 EUR, potem lahko zgolj strošek pridobitve akreditacije , v primeru da ponudnik sam akreditira tudi strojno in programsko opremo, presega 12.000 EUR. V tem znesku niso upoštevani stroški vzpostavitve dveh geografsko oddaljenih lokacij in vse finančne posledice, ki nastanejo zaradi prilagajanja ponudnikovega poslovanja predpisom na področju zajema in hrambe digitalnega gradiva. Vsakoletno podaljšanje pa obsega:

- podaljšanje akreditacije strojne opreme, kjer gre za 50% nižje nadomestilu Arhivu RS za vodenje postopka glede na prvi postopek in ni nadzornega pregleda;
- podaljšanje akreditacije programske opreme, kjer gre za 50% nižje nadomestilo Arhivu RS za vodenje postopka in nadzorni pregled v obsegu 1,5 svetovalnega dneva;
- podaljšanje akreditacije storitve, kjer gre za 50% nižje nadomestilo Arhivu RS za vodenje postopka in 5 svetovalnih dni za nadzorni pregled in pripravo poročila.

Stroški vsakoletnega podaljšanja storitve pa lahko presegajo 6000 EUR. Ponudnik si lahko stroške zmanjša, če uporablja strojno in programsko opremo, ki jo je akreditiral drug ponudnik, vendar je v tem primeru skladnost njegove storitve s predpisi odvisna od tretje osebe – ponudnika akreditirane strojne in programske opreme in njegove želje ter finančnih zmožnosti za vsakoletno podaljševanje. Vsi ponudniki akreditirane storitve zajema in hrambe pa so dolžni najmanj vsakih pet let oz. ob večjih organizacijskih spremembah prenoviti in predložiti v ponovno potrditev svoja notranja pravila.

4 OHRANJANJE DIGITALNEGA ARHIVSKEGA GRADIVA NA DANSKEM

4.1 Zakonodaja na Danskem

Danski državni arhiv se na področju ohranjanja digitalnega gradiva srečuje s podobnimi izzivi kot državni Arhiv Republike Slovenije. Po besedah vodje oddelka za digitalno arhiviranje pri Danskem državnem arhivu gospoda Jana Dalstena Sørensena pa je pristop k reševanju drugačen, kot ga poznamo in izvajamo v Sloveniji. Danski arhivski zakon v prvem členu navaja, da veljajo določila zakona samo za državni, lokalne in regionalne arhive, državne agencije in pravosodni sistem in ne za zasebni sektor (The Danish State Archives, 2007).

Danska zakonodaja na področju dolgotrajnega ohranjanja digitalnega gradiva določa, da se vse arhivsko gradivo lahko dolgotrajno hrani le v državnem ali regionalnih ter javnih arhivih. Državne agencije za kratkotrajno hrambo svojega digitalnega gradiva lahko uporabljajo katerokoli programsko ali strojno opremo za zajem in hrambo, morajo pa o svoji storitvi obvestiti Danski državni arhiv 3 mesece pred začetkom njenega izvajanja. Državni arhiv odobri implementacijo sistema in ne sistem sam. Zakon v 8. členu 2. poglavja zahteva le, da programska oprema omogoča hrambo gradiva na tak način in v takšni obliki, da ga je mogoče prenesti v državni ali javni arhiv.

Po besedah gospoda Sørensena je praksa na področju ohranjanja digitalnega gradiva na Danskem pokazala, da država potrebuje dolgoročno strategijo na tem področju. Zato je Državni arhiv izdal dva dokumenta, s katerima je želel podati usmeritve in navodila tako državnim agencijam - ustvarjalcem arhivskega gradiva kot tudi javnim arhivom, ki to gradivo hranijo. Prvi dokument Strategija arhiviranja digitalnih zapisov je bil objavljen januarja 2013 (The Danish State Archives, 2013b) in se osredotoča predvsem na strategijo Danskega državnega arhiva za sprejemanje in ohranjanje digitalnega gradiva državnih agencij in pravosodja.

Drugi pa je Zbiranje in ohranjanje zasebnega gradiva v Državnem arhivu - Strategija 2016 (The Danish State Archives, b.l. b), ki se osredotoča na knjižnice, muzeje, politične stranke in zasebno gradivo, ki je označeno kot nacionalna kulturna dediščina 21. stoletja. Strategija arhiviranja digitalnih zapisov podpira splošne cilje Danskega državnega arhiva, ki so določeni v arhivskem zakonu in sicer zagotovitev ohranitve zapisov, ki so zgodovinske vrednosti ali pa so s pravnega ali upravnega vidika pomembni za državljane in državne agencije.

Usmeritev strategije je, da se digitalne zapise hrani tako, da ohranijo svojo verodostojnost in da jih je mogoče poiskati in ponovno uporabiti. Pri tem se je arhiv odločil za strategijo migracije, ki zahteva od ustvarjalcev digitalnega arhivskega gradiva, da pretvorijo, prepišejo oz. migrirajo gradivo iz obstoječih produkcijskih formatov v formate, primerne

za dolgoročno hrambo, ki jih predpiše Danski državni arhiv. Ta strategija predvideva ne samo prepis v sodobnejše formate temveč tudi na sodobnejše pomnilniške medije. Ker so ob odločitvi za takšno strategijo imeli v mislih tudi stroške in možnost poškodbe gradiva, ki nastane ob takšnih akcijah, so v strategijo zapisali tudi, naj se migracija izvaja le na osnovi predhodne analize stroškov in tveganja migracije v primerjavi s stroški in tveganji, če podatki ostanejo v obstoječih formatih in na obstoječih pomnilniških medijih.

Naslednja usmeritev strategije je tudi, da morajo vsi arhivski podatki, če želijo zadostiti zahtevi po ponovni uporabi, biti neodvisni od sistema v katerem so nastali. S tem so razširili obseg digitalnega gradiva ne samo na gradivo samo, temveč tudi na vse podatke o okolju in okoliščinah, v katerih je gradivo nastalo in se uporabljalo. Seveda so s tem povzročili, da se kar naenkrat ohranja precej več kot zgolj digitalno gradivo. Izvajanje strategije v Danskem državnem arhivu torej sloni na treh stebrih:

- zgodnjem odkrivanju in potrditvi informacijskih sistemov za prenos gradiva v državni arhiv;
- pogostem prenosu gradiva v arhive v sistemsko neodvisnih formatih;
- v rednem načrtovanju ohranjanja gradiva in periodičnih migracijah v nove formate za dolgotrajno hrambo.

Državne agencije morajo vsak nov informacijski sistem, namenjen ohranjanju podatkov, priglasiti Danskemu državnemu arhivu. Le-ta na osnovi dostavljene dokumentacije oceni, ali informacijski sistem deluje v skladu z zahtevami danske zakonodaje. Ocena ne temelji na preverjanju dejanskega delovanja sistema temveč na ugotavljanju, ali bodo v sistemu podatki, ki jih je vredno ohraniti in ali je sistem sposoben te podatke v Danski državni arhiv dostaviti v vnaprej predpisani obliki. Ocena, ali je podatek vredno ohraniti, ne temelji na nekem specifičnem formatu podatka ali na njegovem ustvarjalcu, temveč Danski državni arhiv oceni, katere podatke morajo posamezni ustvarjalci v resnici hraniti kot arhivsko gradivo. Po strategiji se hranijo podatki, ki:

- se lahko uporabljajo za ponazoritev konkretnih zgodovinskih in družbenih vprašanj (ponovna uporaba);
- pokrivajo interese dovolj velike populacije, bodisi v časovnem obdobju ali glede na število posameznikov (reprezentativnost);
- so singularni (oceni se ali so edinstveni ali redundantni v odnosu do drugih podatkov).

Najpomembnejši ukrep na področju ohranjanja digitalnega gradiva pa je zahteva, da so podatki in dokumenti preneseni v arhive preden postanejo tehnološko zastareli. Danski državni arhiv vsakih 5 let pridobi od vseh državnih agencij kopije vseh podatkov iz informacijskih sistemov, ki jih je določil za trajno ohranjanje in jih prenese v svoje informacijsko okolje (The Danish State Archives, b.l. a). Pomemben del hrambe pa je tudi zagotavljanje varnosti na nivoju bitov in bajtov digitalnega zapisa v skladu z informacijsko varnostno politiko. Za zaščito na bitnem nivoju uporabljajo porazdeljeno

digitalno arhiviranja , pri čemer se podatki nahajajo v več enakih kopijah na optičnih in magnetnih medijih na več različnih geografskih lokacijah.

Strategija, ki sega izven okolja državnih agencij in pravosodja, pa je Zbiranje in ohranjanje zasebnega gradiva v Državnem arhivu - Strategija 2016. Tudi tukaj strategija ne zapoveduje zasebnemu sektorju, kako naj hranijo gradivo, saj le ti niso zakonsko vezani k temu, temveč bolj nalaga arhivom, kako naj hranijo gradivo, nastalo izven ustanov, ki so podvržene določilom arhivskega zakona. Državni arhiv je nase prevzel nalogo, da bo koordiniral prizadevanja vseh institucij, ki delujejo na področju dolgotrajne hrambe, v doseganju konsenza o tem, katero gradivo je treba ohranjati ter kaj bo hranjeno v državnem in kaj v ostalih arhivih. Usmeritev strategije je, da se zasebnemu arhivskemu gradivu zagotovi ustrezna pozornost in proaktivno poskrbi, da se ohrani tisto, kar je pomembno za narod, lokalno zgodovino in kulturo glede na učinke globalizacije.

4.2 Postopek pridobitve certifikata ponudnika storitve hrambe na Danskem

Danska zakonodaja, po besedah gospoda Sørensena, na področju dolgotrajnega ohranjanja digitalnega gradiva ne predvideva zasebnega ponudnika certificirane ali akreditirane storitve zajema in hrambe digitalnega arhivskega gradiva, saj se vse arhivsko gradivo lahko dolgotrajno hrani le v državnem ali javnih arhivih. Imajo pa ponudnike potrjene programske opreme oz. informacijskih sistemov za zajem in hrambo, kar bi lahko enačili z našimi ponudniki akreditirane programske opreme, čeprav je postopek za pridobitev naziva v Sloveniji bistveno bolj zahteven in dražji kot postopek na Danskem.

Državne agencije lahko hranijo digitalno gradivo, ki ga bodo predale arhivom, na svoji informacijski infrastrukturi, vendar morajo o tem pravočasno obvestiti državni arhiv. Vse državne agencije in pravosodni sistem je državni arhiv s posebno okrožnico (The Danish State Archives, 2013a) 21.6.2013 obvestil o pomenu, načinu in proceduri odobritve informacijskih sistemov za ohranjanje digitalnega arhivskega gradiva.

Prva od zahtev je določitev obsega – se pravi, da morajo vse agencije določiti, kaj se bo hranilo v digitalni in kaj v papirni obliki, kdo bo sistem uporabljal – npr. posamezne pisarne, celotna agencija ali celo več agencij hkrati. Določena pa mora biti tudi vsebina uporabe sistema – npr. za analizo podatkov, splošni sistem, za obdelavo posebne vrste podatkov ipd. Zahteva je tudi, da mora vsaka agencija priglasiti svoj sistem državnemu arhivu 3 mesece pred začetkom njegove uporabe v produkciji, da ima arhiv dovolj časa za pregled sistema. Ta del postopka bi lahko enačili z zahtevo slovenskih predpisov po predhodni analizi in pripravi na zajem in hrambo.

Priglasitev sistema se izvede preko posebnega spletnega obrazca na straneh državnega arhiva in arhiv se na osnovi dokumentacije sistema in agencije, ki je izvedla priglasitev, odloči ali je treba podatke ohraniti. Ohranitev pomeni, da bo morala agencija najkasneje v

5 letih arhivu predati kopijo vseh podatkov, ki so označeni kot trajni, ter da v vmesnem času agencija ne sme brisati teh podatkov ne glede na zakonodajo (npr. brisanje osebnih podatkov).

Za potrditev novega IT sistema, ki še ne deluje v produkciji, mora agencija arhivu predložiti tehnično dokumentacijo, E-R diagram in dokazilo, da je sistem zmožen izvoziti podatke (izgraditi SIP) v takšni obliki, kot jo zahteva arhiv. V primeru, ko pa gre za že delujoč sistem z obstoječimi živimi dokumenti, pa mora predložiti navodila za uporabo sistema, popoln podatkovni model z opisom podatkovne strukture, z opisom tabel, posameznih atributov, kaj tabele vsebujejo in kako so med seboj povezane. Danski državni arhiv je izdal Navodila k okrožnici za pregled in potrditev informacijskih sistemov (The Danish State Archives, 2013c), v katerih je natančno opisana posamezna faza v postopku pridobivanja potrditve IT sistema (Tabela 2).

Tabela 2: Postopek potrditve programske opreme - Danska

Naloga	Predpogoj	Izdelek	Čas	Odgovornost
1. faza - Obvestilo o sistemu				
Obvestilo o sistemu	Predložen osnutek opisa novega sistema	Pregled preko digitalnega obrazca na www.sa.dk	3 mesece pred zagonom novega sistema	Organ, ki predloži sistem v potrditev
Ocena ali mora zaradi ohranitve organ predati arhivsko verzijo sistema	Prejem obvestila. Predana je bila popolna informacija o namenu in vsebini sistema.	Odločitev o ohranitvi ali zavrženju sistema.	Ocena mora biti podana v roku dveh mesecev po oddaji popolne dokumentacije sistema.	državni arhiv
2. faza - Odobritev sistemov, ki jih je treba ohranjati (tj. izročiti kopijo na državni arhiv)				
Predaja dodatne dokumentacije in podatkov v potrditev.	Državni arhiv se odloči o ohranitvi sistema	Izpolnjen obrazec na www.sa.dk		Organ, ki predloži sistem v potrditev
Pregled dokumentacije in novih podatkov	Vsa potrebna dokumentacija in podatki so prejeti	Potrditev sistema	Dovoljenje bo izstavljeno v dveh mesecih po zaključku pregleda.	državni arhiv

Vir: The Danish State Archives. 2013c., Priloga 1

Arhiv ima na svoji spletni stani objavljen seznam odobrenih sistemov in če gre za sistem, ki ga je arhiv že odobril, ga agenciji ni treba posebej priglasiti. Arhiv pa po 2 letih delovanja pogleda vsak sistem v produkciji, da oceni, ali sistem v resnici deluje tako, kot je bilo predstavljeno z dokumentacijo ob priglasitvi. Poleg zahteve, da je sistem sposoben zgraditi SIP v skladu z navodili državnega arhiva, pa je ena od pomembnejših zahtev tudi

sposobnost sistema, da vodi revizijske sledi dogajanja z dokumenti, saj je to eden od načinov za zagotavljanje in dokazovanje avtentičnosti in celovitosti. Seveda pa tudi Danski državni arhiv pričakuje od državnih agencij, da se ne bodo zadovoljile samo z opisom postopkov in delovanja sistema na papirju, temveč jim nalaga procese upravljanja sprememb in izvajanje nadzora delovanja sistema v obliki notranjih ali zunanjih revizij.

5 OHRANJANJE DIGITALNEGA ARHIVSKEGA GRADIVA V ESTONIJI

Na področju zajema in hrambe digitalnega dokumentarnega in arhivskega gradiva je bila estonska zakonodaja do leta 2012 precej podobna slovenski. Digitalni državni arhiv Estonije ima še vedno na svojih spletnih straneh objavljenih več dokumentov z načeli, standardi in smernicami, ki naj bi se jih držali vsi, ki delujejo na področju dolgotrajnega ohranjanja digitalnega gradiva v Estoniji (The National Archives of Estonia, b.l. a). Ob kreiranju digitalnega arhiva se estonski arhiv opira na standarde s tega področja kot sta ISO 14721 in ISO 27001, ki podajata usmeritve in zahteve, ki jih morajo izpolnjevati sistemi za upravljanje digitalnega gradiva in informacijsko okolje za njegovo hrambo.

Estonski državni arhiv je vizijo svojega razvoja in tudi usmeritve za vse ostale institucije, ki bi želele v prihodnosti vzpostaviti ustrezno hrambo digitalnih podatkov, objavil v štirih dokumentih:

- Vizija digitalnega arhiva (The National Archives of Estonia, 2006a), ki opisuje vizijo razvoja digitalnega arhiviranja v državi Estoniji, kot jo vidi državni arhiv. Ena od zanimivih zahtev je, da se arhivske kopije vseh dokumentov hranijo na CD (točka 3.2.2.), na online sistemih in magnetnih trakovi se hranijo samo varnostne in ogledne kopije. Prav tako kot slovenska zakonodaja, pa tudi estonska zahteva tri geografsko oddaljene lokacija za hrambo (točka 3.2.7);
- opis delovanja arhiva (The National Archives of Estonia, 2008), kjer podobno, kot naš predpis ETZ 2.1 v II. delu, določijo v 2. poglavju funkcije in odgovornosti v arhivu, vendar za razliko od naše zakonodaje povsem iz stališča odgovornih oseb v procesu prevzema in hrambe gradiva in ne iz stališča zagotavljanja informacijske varnosti;
- operativni model digitalnega arhiva (The National Archives of Estonia, 2006b) vsebuje v poglavju 5.1 seznam zahtev in funkcionalnosti, ki jih mora izpolnjevati digitalni arhivi, kar je zelo podobno našim zahtevam, zbranim v dokumentu ETZ 2.1 II. del Notranja pravila.

Vsa omenjena zakonodaja, ki je v Estoniji stopila v veljavo v letu 2008 za obdobje 2008-2011, je predvidevala tudi podobne postopke preverjanje izpolnjevanja zahtev pri ponudnikih storitve zajema in hrambe kot v Sloveniji. Nov estonski Arhivski zakon, v veljavi od 1.1.2012, pa je ukinil reguliranje ponudbe storitve hrambe digitalnega gradiva s strani državnega arhiva Estonije (Arhiiviseadus, 2013). Po besedah namestnika direktorja Estonskega digitalnega arhiva, gospoda Kuldarja Assa, se je v praksi izkazalo, da je

dejanski nadzor ponudnikov storitve hrambe digitalnega gradiva za estonski arhiv prezahtevna naloga, saj niso mogli zagotoviti dovolj kadrovskih resursov za celovito izvajanje naloge.

Ravno tako pa se jim, po besedah gospoda Assa, ni zdelo korektno do uporabnikov, da bi objavljali ponudnike storitve, ne da bi lahko jamčili za njihovo zanesljivo delovanje. Tako je z novo zakonodajo Estonski državni arhiv sam postal ponudnik hrambe tako za državne in javne ustanove, kot tudi za zasebni sektor. Sicer so za zasebni sektor samo ponudnik repozitorija brez kakršnekoli posebne skrbi za dolgotrajno ohranjanje njihovega gradiva, v skladu z zahtevami arhivske stroke pa hranijo digitalno arhivsko gradivo državnih in javnih ustanov. V prihodnosti pa, po besedah gospoda Assa, Estonija načrtuje certificiranje ponudnikov storitve hrambe po mednarodnih standardih ISO 16363 in ISO 17068. Digitalni arhiv državnega arhiva Estonije po novi zakonodaji temelji na naslednjih principih delovanja:

- hramba podatkov je podprta s podvojeno hrambo na večjem številu lokacij in s pomočjo back-up in recovery postopkov;
- predstavitev podatkov je zagotovljena s pomočjo migracije v sodobne formate in na sodobne pomnilniške medije, ki so dostopni povprečnemu uporabniku;
- kreiranje in upravljanje z metapodatki je v pomoč pri iskanju in razumevanju podatkov.

Tako kot slovenska zakonodaja, tudi estonska opisuje sistem za dolgotrajno hrambo digitalnih podatkov kot skupek programske in strojne opreme, organizacije in pravil, ki zagotavljajo dolgotrajno uporabnost podatkov (The National Archives of Estonia, b.l. b). Nov Arhivski zakon velja za državni arhiv, arhive lokalnih uprav, vse, ki opravljajo dela s pooblastilom države, muzeje, knjižnice, šolstvo, institucije na področju raziskovanja in razvoja in vse, ki imajo v posesti dokumente kulturne ali zgodovinske vrednosti.

V novi zakonodaji ni eksplicitnih zahtev, ki bi jih morali izpolnjevati ponudniki storitve zajema in hrambe, temveč so samo načelna priporočila, katerih izpolnjevanje nihče ne preverja. Vse institucije na področju državne in javne uprave in tiste, ki ustvarjajo gradivo, ki ga estonski državni arhiv označi kot arhivsko, pa morajo spoštovati nekaj zahtev, če želijo ustanoviti svoj digitalni arhiv. Zahteve so naveden v novem estonskem Arhivskem zakonu in sicer:

- v 2. poglavju zakona so navedeni pogoji za ustanovitev javnega arhiva. Zakon določa, da morajo vse institucije, ki se ukvarjajo z ohranjanjem digitalnega gradiva, uporabljati takšne materiale, produkte, formate in tehnologijo, ki zagotavljajo dolgotrajno ohranjanje in omogočajo uporabo gradiva. Nabor formatov, materialov, produktov in tehnologij predlaga državni arhiv Estonije;
- v 6. poglavju, ki navaja pogoje prenosa gradiva v javni arhiv, je določeno, da vse stroške priprave gradiva in prenosa gradiva v javni arhiv krije ustvarjalec gradiva.

Državni arhiv mu lahko pomaga zgolj s programsko opremo, ki mu jo lahko ponudi v pomoč pri pripravi gradiva;

- v 9. poglavju, ki se ukvarja z ohranjanjem javnega arhivskega gradiva, zakon določa, da mora biti gradivo hranjeno v skladu s predpisanimi materiali, produkti, formati in tehnologijami, zagotovljeni morajo biti ustrezni klimatski pogoji v prostorih hrambe. Prostori morajo imeti ustrezno zaščito pred zunanjimi kemičnimi, mehanskimi, biološkimi ali zlonamernimi poškodbami gradiva. Vzpostavljen mora biti sistem varnostnega kopiranja in izbrani optimalni tipi medijev za hrambo glede na tip gradiva:
- ravno tako v 9. poglavju so navedene tudi zahteve za repozitorij, ki se nanašajo na zgradbo, v kateri je repozitorij, ki naj bi imela kontrolirano okolje in nadzor tako znotraj kot v okolici zgradbe. Določa tudi pripravo ustrezne varnostne politike v skladu z mednarodnimi standardi na tem področju in pripravljen akcijski načrt za primer nesreče, ki mora biti narejen z vidika preprečevanja škode na gradivu.

Dokumentarno digitalno gradivo z rokom hrambe daljšim od 10 let lahko državne institucije prenesejo v estonski državni arhiv, vendar morajo stroške prenosa in hrambe gradiva kriti institucije same. Na spletni strani estonskega digitalnega arhiva je objavljen cenik (The National Archives of Estonia, b.l. c) in sicer:

- prenos digitalnega gradiva v državni arhiv, skrb za to gradivo v prvem letu po prenosu ter uničenje gradiva po izteku roka hrambe stane 940 EUR za vsak prenos gradiva, ne glede na velikost paketa;
- skrb za gradivo ene institucije, kot tudi uničenje gradiva po izteku roka hrambe od začetka drugega leta hrambe stane 470 EUR na leto.

6 PREGLED PONUDNIKOV STORITVE V REPUBLIKI SLOVENIJI

V Republiki Sloveniji je pristojna institucija za izvajanje postopkov registracije in akreditacije Arhiv RS oz. Sektor za elektronske arhive in računalniško podporo kot organizacijska enota Arhiva. Del postopkov akreditacije predstavlja tudi revizijski pregled, ki ga Arhiv RS izvaja s pomočjo zunanjih pooblaščenih preizkušenih revizorjev informacijskih sistemov, s katerimi ima sklenjene okvirne sporazume za izvajanje postopkov. Vsi ponudniki, ki so pridobili odločbo o registraciji svoje ponudbe, sklep o akreditaciji strojne opreme, programske opreme, spremljevalnih storitev ali storitev zajema in hrambe ali pa odločbo o potrditvi notranjih pravil, so vpisani Register akreditirane opreme in storitev Arhiva RS.

Na dan 16. februar 2014 je tako v registru vpisanih 27 registriranih in od tega so 4 akreditirani ponudniki storitve zajema in hrambe, en ponudnik pa je v postopku pridobivanja akreditacije (Arhiv Republike Slovenije, b.l.). Ker v Arhivu RS vodim postopke registracije in akreditacije ter sodelujem v postopkih potrjevanja notranjih pravil, se dnevno srečujem s pritožbami vlagateljev nad preveč zahtevnimi in preobsežnimi postopki. Ker pa je kriza oklestila ne samo proračun ponudnikov temveč tudi

povpraševanje po teh storitvah, predstavljajo vedno večji strošek tudi vsakoletna podaljšanja akreditacij. Z vprašalnikom sem želela ugotoviti, kaj dejansko ponudnikom predstavlja največjo težavo. Ugotoviti pa sem želela tudi, na kakšen način in s katerimi postopki bi ponudniki dokazovali, da so zaupanja vredni.

6.1 Registriran ponudnik storitve zajema in hrambe

Za registrirane ponudnike storitve zajema in hrambe, ki svoje storitve niso akreditirali, smo z vprašalnikom hoteli ugotoviti razloge, zakaj niso pristopili k akreditaciji svoje storitve. Zanimalo nas je tudi, če kljub temu, da storitve nimajo akreditirane, poznajo in svoje stranke opozarjajo na problematiko ohranjanja digitalnega gradiva. Pridobitev akreditacije storitve je, poleg certifikatov na tem področju, eden od načinov dokazovanja zanesljivosti. Zanimalo pa nas je tudi, katere pogoje bi moral registrirani ponudnik izpolnjevati in na kakšen način bi moral dokazovati, da je njegova storitev zajema in hrambe zaupanja vredna.

Od 22 registriranih ponudnikov storitve zajema in hrambe, ki so 17. februarja 2014 vpisani v Register akreditirane opreme in storitev Arhiva RS (Arhiv Republike Slovenije, b.l.-a), jih ima Agencija Republike Slovenije za javnopravne evidence in storitve (v nadaljevanju AJPES) evidentiranih še 20, dve družbi pa ne obstajata več (AJPES, 2014). Od evidentiranih 20 registriranih ponudnikov storitev zajema in hrambe na svojih spletnih straneh oglašuje 13 družb. Vsem 20 družbam je bil posredovan vprašalnik. Na vprašanja so odgovorili predstavniki družb Griffin d.o.o., TSE d.o.o., Ljubljanski urbanistični zavod d.d., Actual I.T. d.o.o., HTZ Velenje I.P. d.o.o., Logitus d.o.o. in Panteon Group svetovanje in inženiring d.o.o..

Vzrok za tako majhen odziv je lahko iskati v vsaj dveh razlogih. Od 20 družb, ki imajo storitev zajema in hrambe registrirano, jih dejansko storitev oglašuje le 13. Drug razlog pa je lahko tudi v zakonodaji. Večina registriranih ponudnikov storitve svojo storitev oglašujejo kot zakonsko skladno. ZVDAGA v 6. stavku 97. člena predvideva globo za vse pravne osebe ali samostojne podjetnike, ki neupravičeno uporabljajo naziv ponudnik akreditirane storitve ali opreme. V postopku akreditacije Arhiv RS ugotavlja zakonsko skladnost ponudnikove opreme in storitev in če je le-ta skladna, izda sklep o akreditaciji. Arhiv RS je torej edina institucija v Republiki Sloveniji, ki lahko poda izjavo o zakonski skladnosti opreme in storitev.

S prvim vprašanjem v vprašalniku smo hoteli odkriti razloge oz. ovire, da po uspešni registraciji ponudniki niso pristopili k postopku akreditacije svoje storitve. Trije ponudniki so odgovorili, da se jim je postopek akreditacije zdel samo dodaten strošek in v njem niso videli poslovne prednosti. Težavo jim predstavlja akreditirana strojna (1 ponudnik) in programska oprema (1 ponudnik) in da nimajo notranjih pravil (1 ponudnik) oz. da je sam postopek pridobivanja akreditacije storitve preobsežen in prezapleten (1 ponudnik). Trije ponudniki so napisali, da storitve ne izvajajo za stranke, dva ponudnika pa sta v fazi

priprave na postopek akreditacije. Kljub temu pa imajo 3 od 7 ponudnikov certifikate in sicer eden ISO 9001, eden ISO 27001 in ponudnik, ki je označil postopek akreditacije storitve za prezahteven, celo oba, kar so napisali v odgovorih na drugo vprašanje.

Namen tretjega in četrtega vprašanje je bil ugotoviti, koliko se ponudniki zavedajo problematike ohranjanja digitalnega gradiva z vidika avtentičnosti, celovitosti in uporabnosti in če jo upoštevajo pri hrambi lastnega gradiva oz. o tem seznanjajo tudi svoje stranke. Dva od treh registriranih ponudnikov opozarjata svoje stranke na problematiko zastarevanja formatov in s tem problematiko uporabnosti gradiva. Štirje ponudniki pa se zavedajo tudi problematike zagotavljanja avtentičnosti, zato ob zajemu preverjajo in hranijo tudi varnostne vsebine.

Ponudniki zaradi različnih razlogov, predvsem pa zaradi zapletenosti, zahtevnosti in stroškov niso pristopili k postopku akreditacije. Namen naslednjega vprašanja je bil ugotoviti, kakšni bi bili za ponudnike sprejemljivi predpogoji za pristop k postopku akreditacije in kakšen bi bil primeren način za njihovo preverjanje. Odgovori ponudnikov so precej v nasprotju z odgovori na vprašanje, zakaj niso pristopili k postopku akreditacije. V seznamu pogojev, ki naj bi jih ponudnik moral izpolnjevati v dokaz, da je zaupanja vreden, so tako potrjena notranja pravila, kot tudi certificiranje po ISO standardih, ki je v marsikateri zahtevi bolj strogo, kot naši predpisi na tem področju.

Odgovori pri tem vprašanju so tudi bolj načelne narave, saj je eden od ponudnikov odgovoril, da bi moral izpolnjevati pogoj zaupnosti, varnosti, celovitosti in razpoložljivosti. Ti pogoji so vse, kar zahteva tudi naša zakonodaja, le da v eksplicitni obliki z izvedbenim predpisom Enotnih tehnoloških zahtev. Eden od ponudnikov, ki pa je v postopku pridobivanja akreditacije za svojo storitev, pa se z načinom in postopkom, ki ga določajo naši predpisi, strinja.

Namen drugega dela vprašanja pa je bil ugotoviti, kakšen bi, po mnenju ponudnikov, bil primernejši način preverjanja izpolnjevanja pogojev od sedanjega. Predvsem so bili odgovori v smeri redkejših revizijskih pregledov, saj bi s sedanjega obveznega vsakoletnega revizijskega pregleda ob postopku podaljšanja akreditacije storitve, izvajali revizijski pregled enkrat na tri ali celo pet let. Tudi tukaj pa se ponudnik, ki je v postopku pridobivanja akreditacije svoje storitve, strinja s sedanjo ureditvijo obveznih vsakoletnih revizijskih pregledov.

Z zadnjim sklopom vprašanj pa smo želeli ugotoviti, kako omogočajo strankam dostop do storitve in kakšne stroške imajo stranke s tem. Vprašanje je bilo tudi, če svojo storitev tržijo tudi izven meja Slovenije. Trije od sedmih ponudnikov, ki so odgovarjali na vprašanja, ponujajo svojo storitev strankam in to preko spleta. To vprašanje je pomembno predvsem s stroškovnega vidika, saj ponudniki lahko zaračunavajo ne samo hrambo temveč tudi dostop do posameznega dokumenta. Če je dostop uporabniku olajšan z

uporabo običajne programske opreme, se lahko pojavijo dodatni stroški zgolj zaradi nenehnega vpogleda v dokumente.

Slovenija kot majhen trg, je s ponudniki zajema in hrambe precej zasičena. Na primer na Danskem, po besedah gospoda Sørensena, obstajajo na zasebnem trgu 4 ponudniki hrambe, večina pa jih svojo storitev zaradi ekonomije obsega trži tudi izven Danske. V Sloveniji pa le eden od 7 registriranih ponudnikov, ki so odgovarjali na vprašanja, svojo storitev trži tudi izven meja Slovenije, pa še to predvsem zato, ker podjetje posluje v več državah. Cenik svojih storitev (Tabela 3) je predstavil samo en ponudnik, pri ostalih pa je cena stvar pogodbenega odnosa:

Tabela 3: Cenik storitev registriranega ponudnika

Storitev	Cena
Vključitev v storitev	200 EUR +, po obsegu
Strošek uporabe storitve za prvega in vse nadaljnje uporabnike	Storitev ne obračunavamo po uporabnikih.
Strošek prenosa paketa 100 dokumentov v hrambo	39 EUR
Strošek hrambe za paket do 100MB, ki ima 100 dokumentov in 3 uporabnike, ki bodo dostopali do teh dokumentov	Storitev ne obračunavamo po uporabnikih; 0,001EUR/dokument/mesec
Strošek prenosa in hrambe dodatnega dokumenta (skupna velikost paketa ne presega 100MB)	0,39 EUR/dokument
Strošek hrambe in varovanja dokumentov brez vpogledov	0,001 EUR/dokument/mesec z neomejenimi vpogledi
Strošek vpogleda v dokumente (20 vpogledov na mesec s strani 1 uporabnika – prenos cca 10MB podatkov)	Storitev ne obračunavamo po uporabnikih in vpogledih v dokumente.
Strošek zagotavljanja uporabnosti dokumentov - pretvorba v format primeren za dolgotrajno hrambo	Zajem in pretvorba 0,39 EUR/dokument (+ količinski popusti)
Strošek izbrisa posameznega dokumenta	50 + EUR/leto, po obsegu.

6.2 Ponudnik akreditirane storitve zajema in hrambe

V Registru akreditirane opreme in storitev (Arhiv Republike Slovenije, b.l.-a) so vpisani 4 ponudniki akreditirane storitve in sicer Avtenta, napredne poslovne rešitve d.o.o., Pošta Slovenije d. o. o., Mikrografija d.o.o. in ZZI d.o.o.. V postopku pridobivanja akreditacije svoje storitve pa je še Mikrocop d.o.o., ki ima do 17.2.2014 pridobljeno akreditacijo strojne in programske opreme, potrjena notranja pravila in je oddal zahtevek za

akreditacijo storitve. Vsem petim ponudnikom sem poslala vprašalnik z vprašanji o izvajanju njihove storitve. Vsi so izrazili željo, da so njihovi odgovori predstavljeni anonimno.

Prvi del vprašalnika je namenjen ugotavljanju nivoja sodelovanja med ponudnikom in stranko v fazi priprave na zajem in hrambo in v času, ko ponudnik za stranko že izvaja storitev. Vsi ponudniki imajo za svoje stranke pripravljena ustrezna navodila za pripravo na zajem in hrambo. Po naši zakonodaji pa bi morala tako ponudnik akreditirane storitve zajema in hrambe kot tudi potencialna stranka izvesti predhodno pripravo na zajem in hrambo, kjer bi stranka natančno analizirala svoje potrebe in za potrebe zajema pripravila lastna notranja pravila, ki jih ni treba predložiti v potrditev Arhivu RS.

V naslednji fazi bi morala stranka skupaj s ponudnikom izvesti testiranje storitve in si zagotoviti takšno pogodbo, ki bi pokrivala vse izjemne situacije od prenehanja poslovanja ponudnika do spremembe njegove ponudbe v takšnem obsegu ali pod takšnimi pogoji, ki bi bistveno spreminjali v pogodbi dogovorjen način delovanja in uporabe storitve. Kot je razvidno iz odgovorov, ponudniki v manjši meri skupaj s stranko pripravijo notranja pravila za zajem in hrambo, vsi pa strankam nastavijo sistem zajema in hrambe, pripravijo dokumentacijo in izobrazijo uporabnike za delo v sistemu.

Namen naslednjega sklopa vprašanj je bil ugotoviti, kako ponudniki zagotavljajo celovitost, uporabnost in avtentičnost gradiva. Za zagotavljanje uporabnosti gradiva je zelo pomembno, da ponudniki stranke opozarjajo na problematiko zastarevanja formatov in pravočasno pretvorbo v formate za dolgotrajno hrambo. Prav vsi ponudniki pred prvim prenosom gradiva razložijo svojim strankam problematiko zastarevanja formatov, jim priporočajo hrambo v formatih za dolgotrajno hrambo in jim omogočajo pretvorbo. Pretvorba je organizirana na način, da jo lahko izvede stranka, kadarkoli želi (3 ponudniki) oz. je pretvorba del storitve, ki jo opravi ponudnik glede na pogodbo (3 ponudniki) oz. je pretvorba del ponudbe, ki je na voljo ob dodatnem plačilu (4 ponudniki).

Ko pa ima stranka enkrat gradivo preneseno v hrambo, pa samo štirje ponudniki tudi v obdobju hrambe opozarjajo stranko na zastarevanje formatov. Ponudnik, ki tega ne izvaja, je komentiral, da se do sedaj še ni zgodilo, da bi za kakšno stranko izvedli pretvorbo formatov. Za zagotavljanje avtentičnosti gradiva pa je pomembno, da se hranijo tudi varnostne vsebine, ki so nastale ob nastanku gradiva ali bile ustvarjene ob prenosu gradiva v hrambo. Prisotnost varnostnih vsebin preverjajo trije ponudniki, en ponudnik zagotavljanje varnostnih vsebin prepuščata stranki, en pa jih niti ne zahteva niti ne preverja.

Namen naslednjega sklopa vprašanj je bil ugotoviti, kaj vse so morali ponudniki storiti v svojem okolju samo zaradi pridobivanja akreditacije za svojo storitev. Ker so postopki finančno in organizacijsko zahtevni, je bilo vprašanje tudi, katere zahteve so jim povzročale največ stroškov oz težav. Preglednica (Tabela 4) je povzetek odgovorov, kjer je

v prvem stolpcu tabele navedena zahteva, ki so jo morali izpolniti, v drugem stolpcu odgovori na vprašanje, katere zahteve so morali izpolniti samo zaradi postopka akreditacije storitve, v tretjem stolpcu odgovori na vprašanje, katere zahteve so bile za njih največji organizacijski zalogaj in v zadnjem stolpcu odgovori na tiste zahteve, ki so bile za njih največji finančni zalogaj. Vsak ponudnik je lahko izbral tri zahteve pri vsakem vprašanju.

Tabela 4: Odgovori ponudnikov o zahtevah postopka akreditacije

Zahteva	**Nismo imeli pred akreditacijo**	**Največji organizacijski zalogaj**	**Največji finančni zalogaj**
Vzpostaviti dve geografsko oddaljeni rezervni lokaciji	3	1	2
Kupiti akreditirano strojno opremo oz. obstoječo akreditirati	1		2
Kupiti akreditirano programsko opremo oz. obstoječo akreditirati	1	1	1
Razviti lastno programsko opremo in jo akreditirati	4	5	4
Pripraviti informacijsko varnostno politiko	1		
Implementirati informacijsko varnostno politiko	1		
Pripraviti notranja pravila na področju upravljanja dokumentarnega in arhivskega gradiva	4	3	4
Implementirati notranja pravila na področju upravljanja dokumentarnega in arhivskega gradiva	4	4	1

Trije ponudniki pred postopkom akreditacije niso imeli vzpostavljenih dveh dodatnih geografsko oddaljenih lokacij, vendar je bil to največji finančni zalogaj samo za dva. Iz odgovorov lahko ugotovimo, da ponudnikom z lastno programsko opremo največji organizacijski in finančni zalogaj predstavlja prav njen razvoj, saj mora ustrezati zahtevam iz ETZ 2.1 III.del. Poseben problem pa ponudnikom predstavljajo notranja pravila tako v organizacijskem kot tudi v finančnem smislu. Organizacijsko priprava in implementacija notranjih pravil ne pomeni samo priprava dokumentacije temveč tudi prilagoditev poslovanja zahtevam v ETZ 2.1 II.del. Če pa priprava notranjih pravil predstavlja tudi finančno breme, pa je lahko eden od razlogov tudi najem specializiranega podjetja za pripravo notranjih pravil, ki jih je na slovenskem trgu že kar nekaj.

Postopke pridobivanja in vsakoletnega podaljševanja akreditacije storitve je nedvomno predvsem velik finančni zalogaj, zato smo želeli ugotoviti, katere od vseh zahtev tako za pridobitev kot tudi za podaljšanje akreditacije storitve, bi ponudniki akreditirane storitve ukinili. Odgovori niso presenečenje, saj so najbolj problematične ravno zahteve po uporabi akreditirane strojne in programske opreme in njihovo vsakoletno podaljševanje. Novela ZVDAGA, ki je v potrditi že drugič v zadnjih treh letih, med drugim ukinja ravno vsakoletno podaljšanje akreditacije strojne opreme. En ponudnik pa bi ukinil tudi registracijo ponudnika.

Ponudniki pa bi poleg obvezne uporabe akreditirane strojne in programske opreme in njihovega vsakoletnega podaljšanja ukinili tudi vsakoletno obvezno podaljšanje akreditacije storitve in vsakoletni obvezni revizijski nadzor. Podaljšanje storitve ni samo strošek, temveč za ponudnika predstavlja tudi breme, saj se morajo zaposleni, ki delajo na področju zajema in hrambe, redno dodatno izpopolnjevati in ob revizijskem pregledu dokazila o tem tudi predložiti. Ob vsakoletnem revizijskem pregledu pa mora ponudnik revizorju predložiti tudi dokazila, da je vse leto posloval v skladu z notranjimi pravili.

Ponudnikom predstavlja velik problem tudi priprava notranjih pravil v skladu z našimi predpisi. Zato me je v nadaljevanju zanimalo, katere od zahtev se jim zdijo prezahtevne ali celo nepotrebne. Med prezahtevnimi so uvrstili zahteve:

- obvezna uporaba akreditirane strojne in programske opreme;
- obvezna vzpostavitev dodatnih lokacij;
- priprava načrta neprekinjenega poslovanja v okviru informacijske varnostne politike;
- obvezen zunanji revizijski pregled;
- skupna ocena tveganja, ki jo morajo pripraviti s stranko;
- obvezno potrjevanje notranjih pravila s strani Arhiva RS;
- obvezno redno usposabljanje.

Kot nepotrebne pa so navedli:

- obvezna uporaba akreditirane opreme;
- vsakoletno podaljšanje akreditacij;
- pripravo ocene tveganja;
- predhodna priprava na zajem in hrambo – bolj pomembno za stranko;
- vse zahteve s področja informacijske varnostne politike, ki bi jih nadomestila zahteva po implementaciji ISO 27001 za procese in oddelke, povezane z zajemom in hrambo gradiva.

Namen naslednjega sklopa vprašanj pa je bil dati ponudnikom možnost navesti, poleg težav v sedanjih postopkih, tudi kakšen konkreten predlog, kako bi se postopke lahko naredilo manj zahtevne in obsežne, da pa bi še vedno služili svojemu namenu, ki je

dokazovanje, da je ponudnik hrambe zanesljiv. V prvem delu so ponudniki navedli, katere pogoje bi moral izpolnjevati ponudnik hrambe, da bi lahko pristopil k postopku pridobivanja akreditacije svoje storitve oz. javno izkazoval, da je zanesljiv.

Med odgovori zasledimo veliko zahtev, ki jih morajo že sedaj izpolnjevati ponudniki in nekaj še strožjih. Predlog o uporabi svetovno priznane strojne in programske opreme je enak zahtevam v ETZ, le da naši postopki akreditacije to, da je neka oprema res svetovno priznana in uveljavljena, tudi potrdijo. Obvezno certificiranje po ISO standardih pa presega zahteve naše zakonodaje. Ker govorimo o dokazovanju, da nek ponudnik pozna problematiko dolgotrajnega ohranjanja digitalnega gradiva in z zaupanim gradivom ravna v skladu z dobro prakso na tem področju, pa predlog, da bi ponudnik svojo zanesljivost dokazoval z izkazano finančno stabilnostjo skozi daljše obdobje ne more biti zadosten dokaz.

Tudi pri predlogih, na kakšen način bi se preverjalo izpolnjevanje pogojev pri ponudnikih, se predlogi bistveno ne razlikujejo od sedanje prakse. Poleg predloga, da bi bili revizijski pregledi na dve ali tri leta, so ostali predlogi vsaj tako strogi, nekaj pa še strožjih, kot predvidevajo sedanji predpisi v Republiki Sloveniji na tem področju. Eden takšnih je predlogov je tudi obvezno podaljšanje pridobljenih certifikatov po ISO 9001 in ISO 27001, kar pomeni dvakrat na leto revizijski pregled. Zadnje vprašanje v tem sklopu pa je bilo, če ima kateri ponudnik že pridobljen ISO certifikat. Iz odgovorov je razbrati, da imajo kar 4 ponudniki pridobljen certifikat ISO 9001, trije pa tudi ISO 27001. Le eden od ponudnikov nima nobenega mednarodnega certifikata.

Pridobitev in vsakoletno podaljšanje akreditacije storitve je tudi velik finančni zalogaj, zato trije ponudniki zaradi ekonomije obsega tržijo svojo storitev tudi v tujini. Ker je akreditacija storitve potrebna predvsem zaradi ponujanja storitve javnopravnim osebam v Republiki Sloveniji, je bilo vprašanje tudi, kolikšen delež njihovih strank predstavljajo javnopravne osebe. Pri dveh ponudnikih je ta delež 30%, pri enem 10%, pri enem 2% in pri enem 1%. Za vse ponudnike je to s stroškovnega vidika precej nizek delež, zato so kar trije odgovorili, da pridobivanje akreditacije storitve za njih ni bila pravilna in dobičkonosna odločitev.

En ponudnik je odgovoril, da so šli v akreditacijo storitve izključno zato, ker vedno več pravnih oseb v svojih razpisih za najem tovrstnih storitev to zahteva, eden od ponudnikov pa je odgovoril, da je bila odločitev pravilna. Pojasnil je, da podjetje dobičkonosnosti na račun akreditacij posebej ne beleži, bi pa lahko v prid akreditacijam govorili vsako leto uspešnejši finančni izkazi. Dodal pa je tudi, da na trgu akreditirana v primerjavi z ne-akreditirano storitvijo ne prinaša pomembnejše prednosti, niti v primeru javnopravnih oseb.

Z zadnjim vprašanjem pa smo hoteli ugotoviti, kakšne so cene njihovih storitev. Glede na finančni vložek ponudnikov akreditirane storitve, je pričakovati, da bodo del stroškov krili

s trženjem storitve izven meja Slovenije, del pa poskusili pokriti tudi z višjimi cenami. Eden od ponudnikov je pojasnil, da je njihova storitev res dražja zgolj zato, ker je akreditirana, vendar pa stranke tega velikokrat ne razumejo. Odgovorili so samo trije ponudniki (Tabela 5), ostala dva nimata javnega cenika za pravne osebe in so cene stvar pogodbenega odnosa.

Tabela 5: Primerjava cenikov ponudnikov akreditirane storitve

Storitev	**Ponudnik A (v EUR)**	**Ponudnik B (v EUR)**	**Ponudnik C (v EUR)**
Vključitev v storitve	1.100 (enkratni strošek)	100 (enkratni strošek)	10 (za vsakega uporabnika)
Strošek uporabe storitve za prvega in vse nadaljnje uporabnike	11	mesečna naročnina na storitev je 30 EUR za prvih 5 uporabnikov za 2GB, nad 2GB je 10EUR/GB	6
Strošek prenosa paketa 100 dokumentov v hrambo	1	0	1,25
Strošek hrambe za paket do 100MB, ki ima 100 dokumentov in 3 uporabnike, ki bodo dostopali do teh dokumentov	34	v okviru mesečne naročnine	18,81
Strošek prenosa in hrambe dodatnega dokumenta (skupna velikost paketa ne presega 100MB)	0,01	v okviru mesečne naročnine	0,0125
Strošek hrambe in varovanja dokumentov brez vpogledov	120	v okviru mesečne naročnine	0
Strošek vpogleda v dokumente (20 vpogledov na mesec s strani 1 uporabnika – prenos cca 10MB podatkov)	0	neomejeno (vključeno v mesečno naročnino)	0
Strošek zagotavljanja uporabnosti dokumentov - pretvorba v format primeren za dolgotrajno hrambo	0,065	0,08 do 0,5	0,0065
Strošek izbrisa posameznega dokumenta	0	0	0,0063

6.3 Simulacija stroškov uporabe storitve

Primer: stranka, ki pri ponudniku hrani 100MB gradiva v obliki 100 dokumentov, do katerih bo dostopali 5 uporabnikov eno leto. Vse dokumentne bo treba enkrat v letu pretvoriti v sodobnejši format, na koncu leta pa pobrisati 50 dokumentov.

Tabela 6: Simulacija izračuna stroškov najema storitve

Storitev	**Ceniki ponudnikov akreditirane storitve (v EUR)**			**Cenik registriranega ponudnika (v EUR)**
Vključitev v storitve	1.100	100 + 30 mesečne naročnine	50	200
Letni strošek uporabe storitve za prvega in vse nadaljnje uporabnike	55	Vključeno v mesečno naročnino	72	0
Strošek prenosa paketa 100 dokumentov v hrambo	1	0	1,25	39
Strošek hrambe za paket do 100MB, ki ima 100 dokumentov in 3 uporabnike, ki bodo dostopali do teh dokumentov	34	Vključeno v mesečno naročnino	225,72	1,2
Strošek prenosa in hrambe dodatnega dokumenta (skupna velikost paketa ne presega 100MB)	0,01	Vključeno v mesečno naročnino	0,0125	0,39
Strošek hrambe in varovanja dokumentov brez vpogledov	120	Vključeno v mesečno naročnino	0	1,2
Strošek vpogleda v dokumente (20 vpogledov na mesec s strani 1 uporabnika – prenos cca 10MB podatkov)	0	Vključeno v mesečno naročnino	0	0
Strošek zagotavljanja uporabnosti dokumentov - pretvorba v format primeren za dolgotrajno hrambo	6,5	8 - 50	6,5	39
Strošek izbrisa 50 dokumentov	0	0	0,315	50
Skupaj stroški za stranko	1316,51	368 - 410	355,79	330,79

Primerjava stroškov pokaže na veliko odstopanje med ponudniki akreditirane storitve, ki so oddali cenike. Z daljšim obdobjem uporabe se razlike sicer zmanjšajo, vendar pa je kljub vsemu zanimivo, da se stranke pri registriranem ponudniku ne srečajo s toliko nižjimi stroški, da bi zgolj to opravičevalo najem takšne storitve pred najemom ene od cenejših akreditiranih storitev.

7 GLAVNE UGOTOVITVE

V primerjavi s slovensko zakonodajo sta zakonodaji Danske in Estonije relativno preprosti. Zakonodaja Estonije ne predvideva posebnih postopkov za certificiranje strojne in programske opreme niti kakšnih posebnih pravil, ki jih morajo ponudniki pripraviti, predložiti v potrditev državnemu arhivu in implementirati v svojem okolju. Zakonodaja Danske pa več kot zahtevo, kakšen SIP mora biti sposobna pripraviti programska oprema, tudi ne določa. Eden glavnih razlogov za takšno zakonodajo tiči v pristopu k ohranjanju arhivskega digitalnega gradiva.

Od vseh treh držav zaenkrat edino Slovenija dopušča možnost, da se digitalno arhivsko gradivo hrani tudi pri zasebnih ponudnikih storitve hrambe in ne samo v državnem arhivu. Od tod tudi zelo stroge in specifične zahteve za ureditev okolja ponudnikov storitve na tak način, da bo zagotovljeno enakovredno varstvo, kot bi ga zagotavljal državni arhiv. Vzrok za takšno ureditev tiči tudi v informacijsko komunikacijskem okolju, ki ga imajo državni arhivi v posamezni državi.

Tako danski kot estonski državni arhiv imata ustreznejše vire za zagotavljanje hrambe digitalnega gradiva kot slovenski državni arhiv, saj imata oba arhiva, po besedah gospoda Assa in gospoda Sørensena, že nekaj let vzpostavljeno elektronsko hrambo na državnem nivoju z zadostnimi informacijskimi, infrastrukturnimi, finančnimi in kadrovskimi viri. Slovenska javna arhivska služba ima že od leta 2010 potrjeno strategijo razvoja slovenskega javnega elektronskega arhiva e-ARH.si (dostopna na http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/Predlog_str__e-ARH.si_1.5.pdf) , ki predvideva izgradnjo elektronskega arhiva do leta 2015. Projekt sicer teče, vendar je zaradi pomanjkanja finančnih virov v zaostanku.

Drug razlog, zakaj je naša zakonodaja bolj stroga do ponudnikov storitve pa leži tudi v zakonskem določilu, ki omogoča našim ustvarjalcem, da lahko držijo digitalno arhivsko gradivo na svoji infrastrukturi ali infrastrukturi ponudnika tudi do 30 let od nastanka, ne da bi ga morali predati pristojnemu arhivu. ZVDAGA v 40. členu v 1. odstavku postavlja rok 30 let, v 3. odstavku istega člena pa dovoljuje celo podaljšanje tega roka za izjemno vrsto gradiva (npr. sodne spise ipd..). To pomeni, da je lahko obdobje od nastanka gradiva do obvezne predaje gradiva arhivu tako dolgo, da tehnologija sama po sebi ne more več zagotavljati, da hranjeno gradivo še izpolnjuje vse zahteve arhivske stroke.

Če primerjamo to z zakonodajo Estonije , ki določa, da državni arhiv sam hrani in skrbi za arhivsko gradivo ustvarjalce in zakonodajo Danske, ki sicer dopušča hrambo gradiva izven državnega arhiva vendar nalaga vsem ustvarjalcem vsakih pet let obvezno predajo kopije arhivskega gradiva v digitalni obliki arhivu, ki jih shrani na lastni infrastrukturi, so vsi ukrepi, ki jih določa slovenska zakonodaja in izvaja Arhiv Republike Slovenije upravičeni in lažje razumljivi.

Ukrepi, ne glede na to koliko so lahko upravičeni s stališča zagotavljanja ustreznega varstva arhivskega gradiva, pa so, sodeč po odgovorih ponudnikov storitve, prezahtevni tako v finančnem kot tudi organizacijskem smislu. Kar nekaj ponudnikov v akreditaciji svoje storitve ne vidijo neke poslovne prednosti niti nimajo samo zaradi nje nekih dokazljivih finančnih uspehov. Kljub obvezni akreditaciji storitve, če želijo biti ponudniki javnopravnim osebam, jih ima tudi kar nekaj pridobljene mednarodne certifikate na področju informacijske varnosti, kar dokazuje, da se tudi sicer zavedajo potrebe po zagotavljanju informacijske varnosti.

Pripombe, tako zaradi zahtevnosti, nepotrebnosti, finančne in organizacijske preobremenjenosti, so ponudniki v svojih odgovorih podali praktično na vse postopke. Tako so za večino nepotrebni tako postopki pridobivanja akreditacije za strojno in programsko opremo, priprava in implementacija notranjih pravil kot tudi vsi postopki vsakoletnega podaljševanja akreditacij v okviru katerih se izvajajo tudi dodatni revizijski pregledi. Najbolj pa izstopata razvoj in akreditacija lastne programske opreme in priprava in implementacija notranjih pravil, ki sta večini ponudnikom v vseh pogledih predstavljali največje težave.

Razvoj in akreditacija lastne programske opreme je sicer poslovna odločitev ponudnika, saj Arhiv RS za akreditacijo storitve ne zahteva, da ponudnik uporablja programsko opremo, ki jo je sam razvil. Je pa s tem ponudnikova storitev vsekakor manj odvisna od obstoja zunanjega razvijalca programske opreme. Kar pa se tiče nepotrebnih postopkov, pa bi ponudniki skoraj enoglasno ukinili akreditacijo strojne opreme in vsakoletna podaljšanje vseh akreditacij, predvsem podaljšanje za strojno opremo. Ukinili bi tudi vsakoletni obvezni zunanji nadzorni pregled izvajanj storitve. Vsi našteti postopki so zahtevni tako v finančnem kot organizacijskem smislu, če pa ima ponudnik še pridobljene mednarodne certifikate (npr. ISO 9001 ali ISO 27001), pa je revizijski pregled v okviru podaljševanja storitve še dodatno breme.

Kljub trenutni slovenski zakonodaji, ki omogoča hrambo arhivskega gradiva pri ponudnikih storitve v zasebnem sektorju in vsem predpisom, ki takšno hrambo urejajo, pa menim, da bi se s pojavom novih mednarodnih standardov tudi to področje lahko prilagodilo in uredilo na način, da bi ponudniki s svojo storitvijo bili primerljivi v mednarodnem merilu. Trenutno veljavna slovenska zakonodaja predvideva postopke, ki so redkost v zakonodajah držav EU na področju dolgotrajne hrambe. S tem se od naših ponudnikov zahteva pridobivanje dokazil in certifikatov, ki so veljavni samo na področju Republike Slovenije. V sedanjem času globalizacije in približevanja lokalnih zakonodaj zakonodaji EU pa bi lahko tudi na tem področju Slovenija približala svoje postopke in zahteve mednarodnim standardom. Če pa bi temu sledile vse države EU, bi dobili tudi mednarodno primerljive repozitorije.

Postopke akreditacije bi v Republiki Sloveniji lahko nadomestili z zahtevo po obveznem pridobivanju certifikatov po uveljavljenih mednarodnih standardih. Tako bi vsak ponudnik

storitve zajema in hrambe v Republiki Sloveniji, ne glede na to ali svojo storitev ponuja javnopravnim osebam ali ne, moral pridobiti mednarodne certifikate ISO 16363 in ISO 17068. S tema dvema certifikatoma bi bile pokrite vse zahteve s področja zagotavljanja zaupanja vredne hrambe, ki je v skladu z osnovnimi načeli arhivske stroke. Odpravljeni pa bi bili ločeni postopki akreditacije strojne in programske opreme, saj je precej zahtev s tega področja v obeh standardih. Ker mednarodno certificiranje zahteva vsakoletno podaljševanje certifikatov, bi bili odpravljeni tudi vsi revizijski pregledi, ki jih sedaj na letni ravni izvaja Arhiv RS, slovenski ponudniki zanesljive hrambe pa bi lahko svojo zanesljivost dokazovali tudi v mednarodnem prostoru.

SKLEP

Zakonodaja v Sloveniji je, v primerjavi z zakonodajo nekaj drugih držav v EU, zahtevna, obsežna in predvideva celo vrsto nadzornih instrumentov na področju storitve zajema in hrambe digitalnega gradiva, saj je Slovenija ena redkih držav v EU, ki dovoljuje, da se arhivsko gradivo lahko hrani tudi pri zasebnikih. Državna uprava, organi in institucije državne in javne uprave običajno nimajo ustrezne informacijsko komunikacijske infrastrukture niti ostalih pogojev, da bi takšno gradiva lahko v skladu z zakonom hranile pri sebi.

Državni arhiv po zakonu ne more prevzeti gradiva pred iztekom 30 letnega roka od nastanka, zato zakonodaja omogoča hrambo takšnega gradiva tudi pri zasebnih ponudnikih zajema in hrambe, če so le-ti zanesljivi in zaupanja vredni. Kot je pokazala analiza slovenskih predpisov in odgovorov ponudnikov v vprašalniku pridobitev akreditacije storitve ni niti enostaven niti poceni postopek. Kar nekaj ponudnikov akreditirane storitve ima pridobljene tudi certifikate za mednarodna standarda s področja kakovosti poslovanja in informacijske varnosti, s čimer so že pred akreditacijo storitve izkazovali urejenost svojega okolja.

Trditve, da je nabor ponudnikov akreditirane storitve v Republiki Sloveniji tako majhen zaradi zahtevnih in obsežnih postopkov in stroškov akreditacije, ne morem niti potrditi niti ovreči. Ponudniki so res potrdili, da so postopki zahtevni tako v finančnem kot tudi organizacijskem smislu, vendar, če primerjamo Republiko Slovenijo in obseg njene javne in državne uprave s Kraljevino Dansko, lahko ugotovimo, da je za slovenske potrebe ponudnikov akreditirane storitve še preveč. Ne samo, da nihče od ponudnikov nima več kot 30% strank iz javnega sektorja, tudi potreba po širjenju ponudbe izven meja Slovenije kaže na to, da povpraševanje po tovrstni storitvi v Sloveniji ni visoko oz. da je ponudbe (registrirane, akreditirane ali druge) preveč in ponudniki zgolj s trženjem storitve v Sloveniji ne dosegajo ekonomije obsega.

Tudi trditev, da akreditirano storitev v glavnem uporabljajo organi in institucije državne in javne uprave, so ponudniki sami ovrgli, saj delež strank javne uprave pri nobenem ponudniku ne presega 30%. Primerjava stroškov, ki bi jih imela stranka za uporabo

akreditirane ali samo registrirane storitve je, glede na dejstvo, da je cenik prispeval samo en registriran ponudnik in trije ponudniki akreditirane storitve, površna ali celo neprimerna, vendar lahko kljub temu zaključimo, da ni nujno, da je uporaba akreditirane storitve zaradi vseh stroškov, ki jih ima ponudnik s pridobivanjem akreditacije, dražja. Kar nekaj registriranih ponudnikov je v odgovorih navedlo, da bodo pristopili k postopku pridobivanje akreditacije za svojo storitev, iz česar lahko sklepamo, da se zavedanje o pomenu akreditacije tako med ponudniki kot tudi med potencialnimi strankami dviguje.

Za javnopravne osebe zakon določa uporabo akreditirane storitve, vendar jih je premalo, da bi lahko vsi obstoječi in bodoči ponudniki akreditirane storitve upali na obstoj svoje storitve zgolj s strankami javne uprave. V prihodnosti bo količina digitalnega gradiva tako v javnem kot zasebnem sektorju samo naraščala in potrebe po tovrstnih storitvah se bodo povečevale. V vsakem primeru pa bo trg odločal, ali je akreditacija oz izkazovanje zanesljivosti pri ohranjanju digitalnega gradiva pomembnejše od stroškov, ki jih imajo stranke z najemom takšne storitve.

LITERATURA IN VIRI

1. Agencija RS za javnopravne evidence in storitve - AJPES. Najdeno 17. februarja 2014 na spletnem naslovu http://www.ajpes.si/prs/Default.asp?
2. American library association - ALA.(2007). Definitions of Digital Preservation. Najdeno 15. junija 2013 na spletnem naslovu http://www.ala.org/alcts/resources/ preserv/defdigpres0408
3. *An Introduction To ISO 27001 (ISO27001)* . Najdeno 31. oktobra 2013 na spletnem naslovu http://www. 27000.org/iso-27001.htm
4. *Arhiiviseadus*. Najdeno 27. novembra 2013 na spletnem naslovu https:// www.riigiteataja. ee/akt/13314609
5. Arhiv Republike Slovenije. (b.l.-a). Register akreditirane opreme in storitev. Najdeno 10. junija 2013 na spletnem naslovu http://reh.ars.gov.si/index.php?page=webInterface &idDefinition=1
6. Arhiv Republike Slovenije. (b.l.-b).Register ustvarjalcev javnega arhivskega gradiva. Najdeno 17. februarja 2014 na spletnem naslovu http://www.arhiv.gov.si/si/javne _evidence/
7. Arhiv Republike Slovenije. (2012). Splošni pogoji za izvajanje akreditacije 4.0. Najdeno 1. avgusta 2013 na spletnem naslovu http://www.arhiv.gov.si/fileadmin/ arhiv.gov.si/ pageuploads/zakonodaja/Spik_4.0.pdf
8. Arhiv Republike Slovenije. (2013). Enotne tehnološke zahteve 2.1. Najdeno 1. avgusta 2013 na spletnem naslovu http://www.arhiv.gov.si/si/zakonodaja_in_ dokumenti/ predpisi_s_ podrocja_arhivske_dejavnosti_v_sloveniji/
9. Barateiro, J., Antunes, G., Freitas, F., & Borbinha, J. (2010). Designing Digital Preservation Solutions: A Risk Management-Based Approach. *The International Journal of Digital Curation, 5(1),* 4-17
10. Dobratz, S., Rödig, P., Borghoff, U.M., Rätzke, B., & Schoger, A. (2010). The Use of Quality Management Standards in Trustworthy Digital Archives. *The International Journal of Digital Curation, 5(1),* 46-63
11. *Document History*. Najdeno 31. oktobra 2013 na spletnem naslovu http://www. techstreet.com/products/ 1085204#document
12. Document Lifecycle Management Forum Foundation. (2011). MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules. Najdeno 15. novembra 2013 na spletnem naslovu http://moreq2010.eu/ pdf/moreq2010_ vol1_v1_1 _en.pdf
13. File formats that are supported in Excel. Najdeno 12. januarja 2014 na spletnem naslovu http://office.microsoft.com/en-us/excel-help/file-formats-that-are-supp ort ed-in-excel-HP010014103.aspx
14. Garrett, J., & Waters, D. (1996). Preserving Digital Information: Report of the Task Force on Archiving of Digital Information. Najdeno 26.septembra 2013 na spletnem naslovu http://www.clir.org/pubs/abstract//reports/pub63

15. Giaretta, D. (2011). *Advanced Digital Preservation*. Berlin, Heidelberg, New York: Springer
16. Gladney, H. (2007). *Preserving Digital Information*. Berlin, Heidelberg, New York: Springer
17. Gunnlaugsdottir, J. (2002). An International Standard on RecordsManagement: An Opportunity for Librarians. *Libri (52), 231-240*. Najdeno 26. oktobra 2012 na spletnem naslovu http://www.librijournal.org/pdf/2002-4pp231-240.pdf
18. Higgins, S. (2007). ISO 15489. Najdeno 31. oktobra 2013 na spletnem naslovu http:// www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/ iso-15489
19. ISO Archiving Standards – Overview.(2006). Garrett, J. (ur.) Najdeno 27. oktobra 2013 na spletnem naslovu http://nost.gsfc.nasa.gov/isoas/overview.html
20. Klump, J. (2011). Criteria for the Trustworthiness of Data Centres. *D-Lib Magazine*, 17(1/2). Najdeno 26. septembra 2013 na spletnem naslovu http://www.dlib. org/dlib/january11/klump/01klump.html
21. Mednarodni standard SIST ISO 14721:2013 Trajno ohranjanje podatkov in sistemi za prenos informacij - Odprti arhivski informacijski sistem (OAIS) - Referenčni model.(2013). 1.izd.Ljubljana: Slovenski inštitut za standardizacijo
22. Mednarodni standard SIST ISO 15489-1:2005 Informatika in dokumentacija – Upravljanje zapisov. (2005).1.izd.Ljubljana: Slovenski inštitut za standardizacijo
23. Mednarodni standard ISO 16363:2012 Audit and Certification of Trustworthy Digital Repositories . (2012).(1st ed.). Ženeva: International Organization for Standardization.
24. Mednarodni standard SIST-TP ISO/TR 17068:2013 - Informatika in dokumentacija - Repozitorij za digitalne zapise zaupanja vredne tretje strani.(2013).1.izd. Ljubljana: Slovenski inštitut za standardizacijo
25. Mednarodni standard SIST ISO/IEC 27001:2013 - Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti – Zahteve. (2013).1.izd.Ljubljana: Slovenski inštitut za standardizacijo
26. Mednarodni standard SIST ISO/IEC 27002:2013 - Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti. (2013).1.izd.Ljubljana: Slovenski inštitut za standardizacijo
27. MoReq2. Najdeno 26. oktobra 2013 na spletnem naslovu http://moreq2.eu/moreq2
28. PDCA. Najdeno 27. oktobra 2013 na spletnem naslovu http://www.valuebased management .net/methods_demingcycle.html
29. Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom. *Uradni list RS* št. 132/2006
30. Slovenska akreditacija. (2013). Pravila postopka akreditiranja S03. Najdeno 31. oktobra 2013 na spletnem naslovu http://www.slo-akreditacija.si/ media/ s03.pdf
31. The Consultative Committee for Space Data Systems. (2009). Audit and certification of trustworthy digital repositories. Najdeno 23. junija 2012 na spletnem naslovu http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS%206520R1/Attachments/652x0r1.p df.

32. The Danish State Archives.(b.l.-a) Arkivering af data i it-systemer. Najdeno 10. novembra 2013 na spletnem naslovu http://www.sa.dk/content/dk/for_statslige_ myndigheder/aflevering/ data_fra_it-systemer
33. The Danish State Archives.(b.l.-b) Strategy 2016 Collecting and preserving private records in the State Archives. Najdeno 10. novembra 2013 na spletnem naslovu http://www.sa.dk/ media (5079,1033)/Strategy_2016_-_Private_Archives.pdf
34. The Danish State Archives. (2007). Danish Archives Act. Najdeno 5. novembra 2013 na spletnem naslovu http://www.sa.dk/ media(3000,1033)/ Danish_Archives_Act.pdf
35. The Danish State Archives. (2013a). Cirkulære om anmeldelse og godkendelse af it-systemer. Najdeno 15. novembra 2013 na spletnem naslovu https://www.rets information.dk/Forms/R0710.aspx?id= 145237
36. The Danish State Archives. (2013b). Strategy for archiving digital records. Najdeno 15. novembra 2013 na spletnem naslovu http://www.sa.dk/media(4826,1033)/Strategy_for _ archiving_digital_records.pdf
37. The Danish State Archives.(2013c). Vejledning til cirkulære om anmeldelse og godkendelse af it-systemer . Najdeno 15. novembra 2013 na spletnem naslovu http:// www.sa.dk/media(4900,1030)/Vejledning_om_ anmeldelse_og_godkendelse .pdf
38. *The history of ISO 17799 and ISO 27001*. Najdeno 27. oktobra 2013 na spletnem naslovu http://www.pc-history.org/17799.htm
39. The ISO/IEC 27000 Family of Information Security Standards. Najdeno 14. februarja 2014 na spletnem naslovu https://www.itgovernance.co.uk/iso27000-family.aspx
40. The National Archives of Estonia. (b.l.-a). Principles, standards, guidelines. Najdeno 27. novembra 2013 na spletnem naslovu http://rahvusarhiiv.ra.ee/en/principles-standards-guidelines/
41. The National Archives of Estonia. (b.l.-b). Digital Preservation. Najdeno 26. novembra 2013 na spletnem naslovu http://rahvusarhiiv.ra.ee/en/digital-preservation/
42. The National Archives of Estonia. (b.l.-c). Digital records with a long-term retention period. Najdeno 26. novembra 2013 na spletnem naslovu http://rahvusarhiiv.ra.ee/en/ digital-records-with-a-long-term-retention-period/
43. The National Archives of Estonia. (2006a). Digitaalarhiivi visioon. Najdeno 26. novembra 2013 na spletnem naslovu vir http://rahvusarhiiv.ra.ee/ public/Digiarhiiv/ da_visioon.pdf.
44. The National Archives of Estonia. (2006b). Digitaalarhiivi toimimismudel. Najdeno 27. novembra 2013 na spletnem naslovu http://rahvusarhiiv.ra.ee/public/Digiarhiiv/ da_toimimismudel.pdf
45. The National Archives of Estonia. (2008). Digitaalarhiivi infosüsteem Funktsionaalne kirjeldus. Najdeno 26. novembra 2013 na spletnem naslovu http://rahvusarhiiv.ra.ee/ public/Digiarhiiv/da_funktsionaalsus.pdf.
46. Uredba o varstvu dokumentarnega in arhivskega gradiva. *Uradni list RS* št. 86/2006.
47. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih. *Uradni list RS* št. 30/2006.

48. Žontar, J. (2003). *Arhivska veda v 20. Stoletju*. Ljubljana: Arhiv Republike Slovenije
49. Žumer,V. (2007). Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih. V. Žumer (ur.), Arhivski predpisi v Republiki Sloveniji (str. 29-43). Ljubljana: Arhiv Republike Slovenije

PRILOGE

KAZALO PRILOG

Priloga 1: Vprašalnik z odgovori registriranih ponudnikov storitve zajema in hrambe

1. Za ponujanje svoje storitve javnopravnim osebam, bi morali pristopiti k postopku pridobivanja akreditacije storitve. Kaj je bila za vas ovira, da k temu postopku niste pristopili (možnih več odgovorov):

Akreditacija storitve za nas ne predstavlja poslovne prednosti temveč zgolj dodaten strošek	3
Ne poznamo razlike med registrirano in akreditirano storitvijo	0
Ne poslujemo z javnopravnimi osebami	1
Postopek akreditacije je za nas preobsežen in prezapleten	1
Ne izpolnjujemo osnovnih pogojev, ker nimamo dveh dodatnih geografsko oddaljenih lokacij	0
Ne izpolnjujemo osnovnih pogojev, ker nimamo akreditirane strojne opreme	1
Ne izpolnjujemo osnovnih pogojev, ker nimamo akreditirane programske opreme	1
Ne izpolnjujemo osnovnih pogojev, ker nimamo vzpostavljene informacijske varnosti	0
Ne izpolnjujemo osnovnih pogojev, ker nimamo notranjih pravil za zajem in hrambo	1
Storitve ne izvajamo oz. ne ponujamo na trgu	3
Drugo: Smo v postopku priprave notranjih pravil in priprave na revizijski pregled	2

2. Ali ima vaše podjetje pridobljen kakšen certifikat na področju kakovosti poslovanja (družina ISO 9000) ali na področju informacijske varnosti (družina ISO 27000)? Prosim, če navedete, katere?

ISO/IEC 27001:2005	2
ISO 9000	2
nobenega	5

3. Ali v procesu hrambe gradiva opozarjate stranke na zastarelost formatov in na pravočasno pretvorbo v sodobnejše formate?

Storitev elektronske hrambe za stranke ne izvajamo	4
DA	2
NE, najemamo infrastrukturo od ponudnikov, ki imajo ISO27001	1

4. Ali ob vstopu dokumenta v sistem hrambe preverjate njegove varnostne vsebine ali je to prepuščeno stranki, ki vam dokument posreduje v hrambo?

Storitev elektronske hrambe za stranke ne izvajamo	3
Vse dokumente pretvarjamo v PDF/A	1
DA	3

5. Namen postopka akreditacije je dokazovanje zainteresirani javnosti, da je digitalna hramba, ki jo ponuja ponudnik, zanesljiva. Ker pa so postopki zahtevni tako v organizacijskem kot tudi v finančnem smislu, nam povejte svoje mnenje:

- *Katere pogoje bi moral izpolnjevati ponudnik hrambe, da bi lahko pristopil k postopku pridobivanja akreditacije svoje storitve oz. javno izkazoval, da je zaupanja vreden (navedite vsaj 3 pogoje)?*

Varnost, zaupnost, celovitost, razpoložljivost	1
Potrjena NP, imeti mora celovito tehnično in organizacijsko rešitev za posamezno branžo in reden stik z arhivsko stroko	1
Odlično poslovanje, reference, imeti mora ISO certifikate	2
Zelo se strinjamo z načinom pristopa preko Notranjih pravil in akreditirane opreme	1
Ne izvajamo hrambe za stranke	2

- *Kakšen način preverjanje izpolnjevanja pogojev bi zadoščal?*

Primerljiv z dobrimi praksami v EU	1
neodvisen revizorski pregled na vsake 3 leta ter enkrat letno samoocena	1
letno interno preverjanje, 5 letno zunanje preverjanje	2
Strinjamo se s sedanjim načinom. Predlagamo pa večji nadzor nad razpisi in končnim izvajalcem opravljanja storitev hrambe dokumentacije	1
Ne izvajamo hrambe za stranke	2

6. Ali mora stranka za uporabo vaše storitve namestiti kakršnokoli programsko opremo v svojem okolju?

Storitev elektronske hrambe za stranke ne izvajamo	4
Vse deluje preko spletnega brskalnika	3

7. Ali svojo storitev tržite tudi izven Slovenije? Zakaj?

DA – ker smo podjetje, ki posluje v več državah	1
NE	6

8. Ali lahko navedete ceno v EUR za:

Vključitev v storitev	200 + EUR, po obsegu
Strošek uporabe storitve za prvega in vse nadaljnje uporabnike	Storitev ne obračunavamo po uporabnikih.
Strošek prenosa paketa 100 dokumentov v hrambo	39 EUR
Strošek hrambe za paket do 100MB, ki ima 100 dokumentov in 3 uporabnike, ki bodo dostopali do teh dokumentov	Storitev ne obračunavamo po uporabnikih; 0,001EUR/dokument/mesec
Strošek prenosa in hrambe dodatnega dokumenta (skupna velikost paketa ne presega 100MB)	0,39 EUR/dokument
Strošek hrambe in varovanja dokumentov brez vpogledov	0,001 EUR/dokument/mesec z neomejenimi vpogledi
Strošek vpogleda v dokumente (20 vpogledov na mesec s strani 1 uporabnika – prenos cca 10MB podatkov)	Storitev ne obračunavamo po uporabnikih in vpogledih v dokumente.
Strošek zagotavljanja uporabnosti dokumentov - pretvorba v format primeren za dolgotrajno hrambo	Zajem in pretvorba 0,39 EUR/dokument (+ količinski popusti)
Strošek izbrisa posameznega dokumenta	50 + EUR/leto, po obsegu.

Priloga 2: Vprašalnik z odgovori ponudnikov akreditirane storitve zajema in hrambe

1. Ali imate za svoje stranke pripravljena ustrezna navodila za pripravo na uporabo storitve zajema in hrambe (analiza potreb, predhodna priprava na zajem in hrambo)?

DA	5
NE	0

2. Če navodila imate, označite, kaj od spodaj naštetega vsebujejo:

Analizo potreb	4
Določitev obsega zajema in hrambe	4
Pripravo notranjih pravil za zajem	3
Nastavitev sistema e-hrambe(klasifikacijski načrt, pooblastila, uporabniki, politika hrambe)	5
Zajem obstoječe dokumentacije (elektronska in papirna oblika)	4
Testiranje	4
Dokumentiranje, izdelava navodil za uporabo	5
Izobraževanje uporabnikov	5
Prehod v produkcijo in podporo	4

3. Ali razložite stranki problematiko zastaranja formatov pred prvim prenosom gradiva v e-hrambo?

DA	5
NE	0

4. Ali stranki priporočite hrambo gradiva v formatu za dolgotrajno hrambo?

DA	5
NE	0

5. Kako imate urejeno pretvorbo gradiva v ustrezen format za dolgotrajno hrambo?

Pretvorbo opravlja stranka sama, kadar želi	3
Pretvorba je del storitve in jo opravi ponudnik glede na dogovor v pogodbi	3
Pretvorba je del ponudbe, ki je na voljo strankam ob dodatnem plačilu	4

6. Ali v procesu hrambe gradiva opozarjate stranke na zastarelost formatov in na pravočasno pretvorbo v sodobnejše formate?

DA	4
NE	1 – stranke ne opozarjamo posebej na zastarelost formatov

7. Ali ob vstopu dokumenta v sistem hrambe preverjate njegove varnostne vsebine ali je to prepuščeno stranki, ki vam dokument posreduje v hrambo?

DA - preverjamo	3
NE – prepuščeno je stranki	2

8. Kaj ste morali narediti samo zaradi postopka akreditacije storitve:

Vzpostaviti dve geografsko oddaljeni rezervni lokaciji	3
Kupiti akreditirano strojno opremo oz. obstoječo akreditirati	1
Kupiti akreditirano programsko opremo oz. obstoječo akreditirati	1
Razviti lastno programsko opremo in jo akreditirati	4
Pripraviti informacijsko varnostno politiko	1
Implementirati informacijsko varnostno politiko	1
Pripraviti notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	4
Implementirati notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	4

9. Kaj od naštetega je za vas predstavljalo največji organizacijski zalogaj (izberite 3 možnosti):

Vzpostaviti dve geografsko oddaljeni rezervni lokaciji	1
Kupiti akreditirano strojno opremo oz. obstoječo akreditirati	0
Kupiti akreditirano programsko opremo oz. obstoječo akreditirati	1
Razviti lastno programsko opremo in jo akreditirati	5
Pripraviti informacijsko varnostno politiko	0
Implementirati informacijsko varnostno politiko	0
Pripraviti notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	3
Implementirati notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	4

10. Kaj od naštetega je za vas predstavljala največji finančni zalogaj (izberite 3 možnosti):

Vzpostaviti dve geografsko oddaljeni rezervni lokaciji	2
Kupiti akreditirano strojno opremo oz. obstoječo akreditirati	2
Kupiti akreditirano programsko opremo oz. obstoječo akreditirati	1
Razviti lastno programsko opremo in jo akreditirati	4
Pripraviti informacijsko varnostno politiko	0
Implementirati informacijsko varnostno politiko	0
Pripraviti notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	4
implementirati notranja pravila za upravljanje dokumentarnega in arhivskega gradiva	1

11. Kaj od naštetega v postopku akreditacije bi ukinili:

Registracija ponudnika storitve	1
Obvezna uporaba akreditirane strojne opreme	3
Obvezna uporaba akreditirane programske opreme	1
Obvezna priprava in potrditev notranjih pravil za zajem in hrambo	0
Revizijski pregled v postopku pridobitve akreditacije	0
Vsakoletno obvezno podaljšanje akreditacije strojne opreme	5
Vsakoletno obvezno podaljšanje akreditacije programske opreme	4
Vsakoletno obvezno podaljšanje akreditacije storitve	3
Vsakoleten obvezni zunanji nadzorni pregled izvajanja storitve	3
Obvezna priprava samoocenitve (izpolnjen ETZ) v postopkih	0

12. V okviru priprave in implementacije notranjih pravil za zajem in hrambo je veliko zahtev, ki jih mora ponudnik izpolniti. Prosim, da navedete najmanj tri, ki so se vam zdele v postopku priprave in implementacije vaših notranjih pravil:

prezahtevne:

- akreditacija mednarodno priznane programske in strojne opreme,
- dolgotrajnost postopka potrjevanja notranjih pravil s strani Arhiva RS,
- vzpostavitev tretje geografsko oddaljene lokacije,
- dodaten zunanji revizijski pregled izvajanja NP, ki ni v okviru podaljšanja,
- redno usposabljanje zaposlenih (najmanj enkrat letno in sistem pridobivanja kreditnih točk),
- skupna ocena tveganja, ki jo pripravita ponudnik in potencialna stranka in izvedba predpriprave na zajem in hrambo pri potencialni stranki,
- načrt neprekinjenega poslovanja – prezahtevne, preobširne in prestroge zahteve,

in še komentar enega od ponudnikov - zahteve niso prehude, problem je, da je posledica izpolnjevanja vseh zahtev kasneje dražja storitev, kar pa stranke težko razumejo.

nepotrebne:

- akreditacija mednarodno priznane programske in strojne opreme,
- vsakoletno podaljšanje akreditacij,
- Za ponudnike z redno letno presojo, je notranja presoja (po vzoru ISO standardov) nepotrebna, ker pomeni zgolj dodatno delo,
- točke v poglavjih 2.3 Zajem gradiva in 2.4 Pretvorba gradiva v obliko za dolgoročno e-hrambo v ETZ 2.1 II. del, kjer gre za odločanje uporabnika o načinu uporabe storitve in njegovih potreb in niso smiselne za ponudnika,
- navajanje tehničnih specifikacij v organizacijskih dokumentih. Strojna oprema se lahko z leti spremeni, kar posledično pomeni spremembo notranjih pravil in povezane aktivnosti, ki vključujejo Arhiv RS,
- ocena tveganja,
- predhodna priprava na zajem in hrambo, saj je to bolj pomembno za stranko

in še komentar enega od ponudnikov - za ponudnike storitve bi poglavje o zahtevah informacijske varnosti izdvojil v zahtevo po implementaciji ISO 27001 za procese in oddelke, povezane z zajemom in hrambo gradiva.

13. Namen vseh zgoraj omenjenih postopkov je dokazovanje zainteresirani javnosti, da je digitalna hramba, ki jo ponuja ponudnik, zanesljiva. Ker pa so postopki zahtevni tako v organizacijskem kot tudi v finančnem smislu, nam povejte svoje mnenje:

Katere pogoje bi moral izpolnjevati ponudnik hrambe, da bi lahko pristopil k postopku pridobivanja akreditacije svoje storitve oz. javno izkazoval, da je zaupanja vreden (navedite vsaj 3 pogoje)?

- svetovno priznana strojna oprema na tem področju (brez slovenske akreditacije),
- uporaba programske opreme, ki je široko priznana in uporabljana (pa ni potrebna akreditacija),
- uporaba akreditirane programske opreme (ustrezen nabor funkcionalnosti rešitve in način delovanja)
- pridobljen certifikat ISO 9001 in 27001 zaradi procesov in informacijske varnosti,
- uporaba naprednih tehnoloških sredstev za zagotavljanje verodostojnosti varnostnih vsebin digitalnega gradiva v e-hrambi,
- certificiranje s strani kompetentne organizacije (npr. SA),
- registracija ponudnika,
- prilagojena potrjena notranja pravila za ponudnike, ki se razlikujejo od notranjih pravil za uporabnike hrambe - določene točke so namreč smiselne za ponudnike, nekatere za uporabnike, nekatere pa za oboje,
- ISO 9001:2008, ISO 27001,
- izkazana finančna stabilnost skozi daljše obdobje,
- ustrezna strokovna usposobljenost več zaposlenih.

Kakšen način preverjanje izpolnjevanja pogojev bi zadoščal?

- letni pregled oz. revizija izpolnjevanja zahtev sta potrebna,
- pregled dejanskega stanja opreme in uvedenih tehnoloških ter organizacijskih ukrepov,
- prvo preverjanje revizorski pregled, nato pregled na vsake tri leta ali ob spremembi zakonodaje,
- presoje skladnosti poslovanja skladno z ISO 9001:2008 in ISO 270001 (redne letne presoje),
- predložitev dokazil in revizorski pregled s strani preizkušenih revizorjev IS vsaki dve leti.

14. Ali ima vaše podjetje pridobljen kakšen certifikat na področju kakovosti poslovanja (družina ISO 9000) ali informacijske varnosti (družina27000)? Prosim navedite jih:

NE	**ISO 9001**	**ISO 27001**
1	4	3

15. Ali mora stranka za uporabo vaše storitve namestiti kakršnokoli programsko opremo v svojem okolju?

DA	0
NE	5 – storitev je dostopna preko spleta

16. Ali svojo storitev tržite tudi izven Slovenije? Zakaj?

NE	2
DA	3 – zaradi ekonomije obsega

17. Ali lahko navedete kolikšen delež strank, ki pri vas hranijo gradivo, predstavljajo javnopravne osebe?

1%	3%	10%	30%
1	1	1	2

18. Glede na organizacijske in finančne vložke, ali je bil postopke akreditacije pravilna in dobičkonosna odločitev za vaše podjetje?

NE	3
DA	akreditacija je pri določenih pravih osebah zahtevana
DA	Menimo, da je bila odločitev pravilna. Dobičkonosnosti na račun akreditacij posebej ne beležimo, bi pa lahko v prid akreditacijam govorili vsako leto uspešnejši finančni izkazi. Vendar moramo omeniti, da na trgu akreditirana v primerjavi z neakreditirano storitvijo žal ne prinaša pomembnejše prednosti (tudi v primeru javno pravnih oseb)

19. Ali lahko navedete ceno v EUR za:

Pri dveh ponudnikih ceniki niso javni in so predmet pogodbenega odnosa ali pogajanj.

Vključitev v storitve	1.100 EUR (enkratni strošek)	100EUR	10EUR /up
Strošek uporabe storitve za prvega in vse nadaljnje uporabnike	11 EUR/na uporabnika	mesečna naročnina na storitev je 30 EUR za prvih 5 uporabnikov za 2GB, nad 2GB je 10EUR/GB	6EUR/m
Strošek prenosa paketa 100 dokumentov v hrambo	1 EUR/paket	0	1,25EUR
Strošek hrambe za paket do 100MB, ki ima 100 dokumentov in 3 uporabnike, ki bodo dostopali do teh dokumentov	34 EUR/paket	mesečna naročnina na storitev je 30 EUR za prvih 5 uporabnikov za 2GB, nad 2GB je 10EUR/GB	18,81EUR/m
Strošek prenosa in hrambe dodatnega dokumenta (skupna velikost paketa ne presega 100MB)	0,01 EUR/kos	mesečna naročnina na storitev je 30 EUR za prvih 5 uporabnikov za 2GB, nad 2GB je 10EUR/GB	0,0125EUR/dok
Strošek hrambe in varovanja dokumentov brez vpogledov	120 EUR/paket	mesečna naročnina na storitev je 30 EUR za prvih 5 uporabnikov za 2GB, nad 2GB je 10EUR/GB	/
Strošek vpogleda v dokumente (20 vpogledov na mesec s strani 1 uporabnika – prenos cca 10MB podatkov)	0 EUR/vpogled	neomejeno (vključeno v mesečno naročnino)	/
Strošek zagotavljanja uporabnosti dokumentov - pretvorba v format primeren za dolgotrajno hrambo	0,065 EUR/stran	0,08 - 0,5EUR/dokument	0,0065EUR/dok
Strošek izbrisa posameznega dokumenta	0 EUR/izbris	0	0,0063EUR/dok