Sveučilište u Zagrebu

Filozofski fakultet

Edvin Buršić

Koncept stvaranja digitalnih izvornika postupkom digitalizacije

DOKTORSKI RAD

Mentor: dr. sc. Hrvoje Stančić, red. prof.

Zagreb, 2018.

University of Zagreb

Faculty of Humanities and Social Sciences

Edvin Buršić

Concept of creation of digital originals by digitisation

DOCTORAL THESIS

Supervisor: Ph. D. Hrvoje Stančić, full professor

Zagreb, 2018

Informacija o mentoru

Dr. sc. Hrvoje Stančić, redovni profesor, rođen je 2. listopada 1970. u Zagrebu gdje je završio osnovnu i srednju školu. Diplomirao je 1996. godine studijske grupe Informatologija (smjer Opća informatologija) i Engleski jezik i književnost na Filozofskom fakultetu u Zagrebu. Godine 1996. prihvaćen je kao znanstveni novak na projektu koji se vodi na Odsjeku za informacijske znanosti Filozofskog fakulteta u Zagrebu (broj znanstvenika 244003). Magistrirao je 2001. godine s temom *Upravljanje znanjem i globalna informacijska infrastruktura*. Doktorirao je 2006. s temom *Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata*. Od 2014. godine je u zvanju znanstveni savjetnik. Od ožujka 2018. je u zvanju redovnoga profesora.

Nastavu izvodi na preddiplomskom, diplomskom i doktorskom studiju informacijskih i komunikacijskih znanosti. Predaje predmete – preddiplomski: Osnove informacijske tehnologije, Osnove digitalne obrade teksta i slike, diplomski: Digitalizacija i migracija dokumenata, Digitalizacija 3D objekata i prostora, Digitalni arhivi, Planiranje i oblikovanje sustava za upravljanje gradivom doktorski: Očuvanje autentičnosti digitalnih zapisa, Planiranje procesa digitalnog očuvanja.

Kao gostujući predavač predavao je pet godina na diplomskom studiju na Filozofskom fakultetu Sveučilišta u Sarajevu te dvije godine na diplomskom i doktorskom studiju na Fakultetu za administraciju i menadžment informacijskih sistema Univerziteta Sv. Kliment Ohridski u Bitoli.

Predstojnik je Katedre za arhivistiku i dokumentalistiku od 2008. godine.

Autor je knjige *Digitalizacija*, koautor knjige *Heritage Live. Upravljanje baštinom uz pomoć informacijskih alata* i rječnika *Arhivistički rječnik. Englesko-hrvatski i hrvatsko engleski*, urednik šest knjiga, a objavio je, samostalno ili u koautorstvu, više od 80 znanstvenih i stručnih radova.

Kao istraživač sudjelovao je u radu četiriju nacionalnih znanstveno-istraživačkih projekata i jednom međunarodnom TEMPUS projektu. Vodio je, na razini fakulteta, međunarodni projekt HERITAGE Live koji se odvijao u okviru IPA operativnog programa prekogranične suradnje Slovenija – Hrvatska 2007.-2013. Na razini Hrvatske koordinirao je aktivnosti europske koordinacijske inicijative Digital Preservation Europe – DPE. Istraživač je i voditelj europskog istraživačkog tima na međunarodnom projektu InterPARES Trust – Trust and Digital Records in an Increasingly Networked Society (2013.-2019.).

Koordinator je radionica na Odsjeku te je od 2007. aktivno uključen u organizaciju odsječke bienalne međunarodne konferencije INFuture – The Future of Information Sceinces.

U Ministarstvu kulture RH član je radnih skupina za izradu nacionalne strategije za digitalizaciju kulturne baštine, za izradu novog Zakona o arhivskom gradivu i arhivima, za zaštitu pisane baštine i za izradu projektnog prijedloga digitalizacija kulturne baštine.

Član je predsjedništva Hrvatskog arhivističkog društva (HAD), član Hrvatskog informacijskog i dokumentacijskog društva (HIDD), Hrvatskog nacionalnog komiteta ICOM-a, te član kanadskog Centre for the International Study of Contemporary Records and Archives (CISCRA).

U Hrvatskom zavodu za norme Predsjednik je hrvatskog zrcalnog tehničkog odbora za izradu međunarodne norme ISO/TC 307 Ulančani blokovi i tehnologija distribuirane glavne knjige (engl. Blockchain and Electronic Distributed Ledger Technologies).

Izdvojeni radovi:

1. Stančić, Hrvoje; Rajh, Arian; Brzica, Hrvoje. Archival Cloud Services: Portability, Continuity, and Sustainability Aspects of Long- term Preservation of Electronically Signed Records. // Canadian journal of information and library science-revue canadienne des sciences de l information et de bibliotheconomie. 39 (2015), 2; 210-227
2. Mihaljević, Marta; Mihaljević, Milica; Stančić, Hrvoje. Arhivistički rječnik. Englesko-hrvatski, hrvatskoengleski. Zagreb : Zavod za informacijske studije, 2015.
3. Stančić, Hrvoje; Pavlina, Krešimir; Rajh, Arian; Strasberger, Vito. Creation of OAIS-Compliant Archival Packages for Long-Term Preservation of Regulatory Metadata, Records and Dossiers // The Fourth International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED 2012) : DigitalWorld 2012 : proceedings / Van Gemert-Pijnen, Lisette ; Ossebaard, Hans C. ; Smedberg, Åsa ; Wynchank, Sincalir ; Giacomelli, Piero (ur.). Valencija : IARIA, 2012. 105-110
4. Hrvoje Brzica; Boris Herceg; Tihomir Katulić; Hrvoje Stančić. Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata. // Arhivski vjesnik. 2014 (2014), 57; 129-157
5. Stančić, Hrvoje. Pohrana arhivskih materijala u računalnom oblaku // Specijalizirani arhivi i zbirke gradiva izvan arhiva / Babić, Silvija (ur.). Varaždin : Hrvatsko arhivističko društvo, 2012. Str. 187-196.

Zahvale

U prvom redu želim zahvaliti mojoj Ivani na strpljenju, toplini i razumijevanju tijekom svih sati, a bilo ih je zaista mnogo i po danu i po noći, provedenih u radu na disertaciji. Zatim želim zahvaliti svojim roditeljima bez kojih ne bi bilo puno stvari, puno vrijednih stvari, posebno mene i disertacije. Također hvala mojoj teti na pažnji, ljubavi i slušanju. Posebnu zahvalu šaljem svom bratu koji svojim pristupom životu nadahnjuje i mene u postavljanju novih i novih ciljeva.

Veliko hvala svim prijateljima s ove i one strane oceana koji su mi svojom dobrotom i žarom uljepšali sve ove godine, hvala poslovnim kolegama bez kojih se ne bi dogodio žar za arhivistikom i stalnom učenju, hvala kolegama muzičarima i plesačima, hvala mojoj posebnoj veseloj družini s „capo di banda“ na čelu bez kojih upornost može biti i ostati samo tinta na papiru.

I na kraju veliko veliko hvala Hrvoju koji me svojim mudrim i ljudskim načinom vodio uspješno ka cilju.

Sažetak

Cilj doktorske disertacije je izrada *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije*, odnosno određivanje uvjeta za dobivanje autentičnih kopija (zapisa koji jest ono što tvrdi da jest i koji nije bio mijenjan) nastalih digitalizacijom izvornika u fizičkom obliku.

Za postizanje cilja korištene su metoda analize, metoda sinteze, metoda konkretizacije, metoda komparativne analize te metode modeliranja.

Pomoću navedenih metoda, kao prvo, utvrđeni su uvjeti pod kojima se digitalnu kopiju dokumenta može smatrati jednakovrijednom izvorniku. Ti uvjeti zadovoljavaju zahtjeve za autentičnošću koji uključuju: propisane, ovjerene i odobrene procedure i upute korištenih koraka digitalizacije, karakteristike skenera, glavne slike, pokretačkog programa i softvera za digitalizaciju, potrebne metapodatke kojima se objašnjava kontekst digitaliziranog dokumenta, korištene aplikacije i repozitoriji podataka, provedbene, kontrolne i nadzorne uloge i revizijski tragovi provedenih aktivnosti unutar procesa digitalizacije.

Drugo, za postizanje autentičnosti prepoznata su i u model ugrađena 45 zahtjeva koje je potrebno zadovoljiti. Komparativnom analizom predloženog Modela i tehničkih izvještaja ISO/TR 15801 i ISO/TR 13028 utvrđeno je da tehnički izvještaj ISO/TR 15801:2009 zadovoljava 32 zahtjeva, a ISO/TR 13028:2010 zadovoljava 17 zahtjeva. To znači da je uz korištenje spomenutih normi potrebno ugraditi dodatne kontrole i njihove evidencije kojima se može osigurati dovoljna količina podataka i tako dokazati da je stvorena digitalizirana slika autentična digitalna kopija.

Konačno, razvijeni model obuhvaća korak ispisa digitalnog ili digitaliziranog dokumenta kao dokumenta koji se po svojim svojstvima može smatrati jednakovrijednim izvorniku. Takav dokument mora zadovoljavati određene, u modelu definirane, zahtjeve ispisa.

Ključne riječi: digitalizacija, skeniranje, glavna slika, PDF, XLS, indeksiranje, metapodaci, konverzija, mikroprint, PIQL

Summary

The aim of this PhD dissertation is to develop the *Model of the process of creation of authentic digital copies in the form of originals by digitization* and to determine conditions for acceptance of the digitized document as authentic to the original analogue document, as being what it purports to be and is free from tampering or corruption, and that includes internal and external evidence, taking into account physical characteristics, structure, content and context – and to find the totality of the properties of digitized document which establish its origin, reliability, credibility and accuracy of its content.

To create this model, the relevant legal framework, technical framework, existing relevant standards and good practice routines were analyzed. Additionally, digital signature, digital stamp, digital certificate, software for digitization, EXIF standard, RFID, microprint, PIQL's film, XML language and technical components (image sensors for digitizing) etc. were also analyzed with the goal of producing a model of digitizing analogue originals in a way that the digital form can be considered authentic.

The aim was achieved by creating a *Model of the process of creation of authentic digital copies in the form of originals by digitization,* i.e. determining the conditions for obtaining authentic copies generated by the digitization of the originals in physical form.

The methods used were the method of analysis and synthesis, method of concretization, comparative analysis method and modeling method.

Using the above methods, the conditions under which a digital copy of a document can be considered equivalent to the original were first established. Concepts that meet the authentication requirements include: defined, certified and approved procedures and instructions of the used digitization process, scanner characteristics, master image characteristics, driver and digitization software characteristics, necessary metadata explaining the context of the digitized document, requirements for the used application, data repository requirements, control and supervisory roles and audit trails of the activities carried out within the digitalization process.

Secondly, to achieve authenticity 45 requirements are identified that need to be met. Comparative analysis of the proposed Model and ISO/TR 15801:2009 and ISO/TR 13028:2010 standards established that ISO/TR 15801:2009 technical report meets 32 requirements and ISO/TR 13028:2010 complies with 17 requirements. These results show

that the use of these standards requires additional controls and records to provide sufficient data to show that a digitized image is an authentic digital copy.

Finally, the model covers the situation in which a digital or digitized document can be printed as a document that, by its properties, may be considered as original. The model proposes that it could be the case if the printed document meets a set of requirements.

Key words: digitization, scanning, master image, PDF, XLS, indexing, metadata, Conversion, microprint, PIQL

Sadržaj

1. UVOD 1
2. CILJ I METODOLOGIJA ISTRAŽIVANJA 4
3. AUTENTIČNOST 5
3.1. Digitalizacija u Sjevernoj Americi i Europi 5
3.2. Elektronički račun 7
3.3. Dokument u elektroničkom obliku 9
3.4. Rasprava: autentičnost 11
3.5. Zaključak o konceptu autentičnosti 17
4. ŽIVOTNI CIKLUS DOKUMENTA 19
4.1. Papirnata dokumentacija 19
4.2. Proces digitalizacije 25
4.3. Digitalizirana dokumentacija 32
4.4. Zaključak 35
5. ZAKONSKI OKVIR 37
5.1. Zakon o arhivskom gradivu i arhivima 37
5.1.1. Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva 40
5.1.2. Pravilnik o uvjetima smještaja, opreme, zaštite i obrade arhivskog gradiva, broju i strukturi stručnog osoblja arhiva 43
5.1.3. Pravilnik o korištenju arhivskoga gradiva 45
5.1.4. Pravilnik o predaji arhivskoga gradiva arhivima 45
5.1.5. Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva 48
5.1.6. Pravilnik o evidencijama u arhivima 49
5.2. Zakon o knjižnicama 51
5.3. Zakon o muzejima 52
5.3.1. Pravilnik o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju 53
5.3.2. Pravilnik o sadržaju i načinu vođenja muzejske dokumentacije o muzejskoj građi 54
5.4. Zakon o elektroničkom potpisu i eIDAS uredba 55
5.5. Zakon o elektroničkoj trgovini 58
5.6. Zakon o elektroničkoj ispravi 60
5.7. Zakon o autorskom pravu i srodnim pravima 62

5.8. Zakon o zaštiti osobnih podataka i opća uredba o zaštiti osobnih podataka (GDPR)64
5.9. Zakon o pravu na pristup informacijama 68
5.10. Zaključak 69
6. NORME 71
6.1. HRN ISO 11799:2004 71
6.2. ISO/TR 15801:2009 73
6.3. ISO/TR 13028:2010 85
6.4. HRN ISO/IEC 27001:2006 90
6.5. ISO 15489-1:2001 92
6.6. ISAD (G) - Opća međunarodna norma za opis arhivskoga gradiva 97
6.7. Zaključak 100
7. KOMPONENTE DIGITALIZACIJE 101
7.1. Senzori u digitalizaciji - CCD i CIS 101
7.2. Tehnički standardi 110
7.2.1. Vlada Alberte, Kanada 110
7.2.2. Kongresna knjižnica, Washington D.C. 113
7.3. Softveri za digitalizaciju 119
7.3.1. DpuScan 120
7.3.2. ScandAll-PRO 123
7.3.3. Capture Perfect 124
7.4. XML 126
7.5. Zaključak 130
8. TEHNIČKA RJEŠENJA ZA SIGURNOST FIZIČKOGA I DIGITALIZIRANOGA GRADIVA 132
8.1. Prihvat dokumentacije 132
8.1.1. RFID 133
8.2. Digitalizacija 135
8.2.1. Standard EXIF 135
8.2.2. PIQL film 142
8.2.3. ISO 19005 skupina standarda 150
8.3. Ispis iz sustava 155
8.3.1. eGRAĐANI 156
8.3.2. Mikroprint 161
8.4. Zaključak 162

9. ANALIZA PRIMJERA DOBRE PRAKSE 164
9.1. Digitalizacija dokumentacije o lijeku - HALMED 164
9.2. Digitalizacija dokumentacije - Fina 170
9.3. Digitalizacija dokumentacije – Hrvatska poštanska banka (HPB) 176
10. MODEL PROCESA STVARANJA AUTENTIČNIH DIGITALNIH KOPIJA U OBLIKU ORIGINALA POSTUPKOM DIGITALIZACIJE 181
10.1. Autentičnost prije digitalizacije 181
10.2. Masovna digitalizacija i njezini problemi 182
10.3. Dokumentacijska cjelina 184
10.4. Digitalizirani dokument 185
10.5. Proces digitalizacije 186
10.5.1. Testni uzorak 186
10.5.2. Priprema 187
10.5.3. Skeniranje 188
10.5.4. Kontrola glavne slike 189
10.5.5. Slanje u repozitorij dokumentacijskih cjelina 189
10.5.6. Indeksiranje i pridruživanje metapodataka 190
10.5.7. Kontrola pridruženih metapodataka i digitaliziranih slika 191
10.5.8. Ponavljanje skeniranja 192
10.5.9. Isporuka digitaliziranih dokumentacijskih cjelina 192
10.6. Zatvoreni sustav digitalizacije 193
10.7. Izrada uputa 193
10.8. Podijeljenost uloga i odgovornosti u sustavu digitalizacije 194
10.9. Karakteristike skenera 196
10.10. Karakteristike pokretačkog programa i softvera za prihvat slike 197
10.11. Karakteristike glavne slike 200
10.12. Slanje datoteka u središnji repozitorij 202
10.13. Korištenje vremena i datuma 202
10.14. Sustav za upravljanje dokumentima od povjerenja 203
10.15. Metapodaci koji se stvaraju digitalizacijom 203
10.16. Aplikacije u sustavu 206
10.17. Repozitoriji podataka 206
10.18. Revizijski trag 207
10.19. Zaključak 207

11. KOMPARATIVNA ANALIZA PREDLOŽENOG MODELA PROCESA STVARANJA AUTENTIČNIH DIGITALNIH KOPIJA U OBLIKU ORIGINALA I NORMI ISO/TR 15801 I ISO/TR 13028 209
11.1. Obrazac za analizu 209
11.2. Analiza norme ISO/TR 15801:2009 i zahtjeva autentičnosti 211
11.3. Analiza tehničkog izvještaja ISO/TR 13028:2010 i zahtjeva autentičnosti 224
11.4. Analiza predloženog modela procesa stvaranja autentičnih digitalnih kopija u obliku originala i zahtjeva autentičnosti 234
11.5. Rezultat analize 242
11.6. Zaključak 244
12. UVJETI ZA ISPIS JEDNAKOVRIJEDAN IZVORNIKU 246
13. ZAKLJUČAK 248
14. LITERATURA 250
15. POPIS SLIKA 258
16. POPIS TABLICA 259
17. POPIS DIJAGRAMA 260

1. UVOD

Svaka organizacija, društvena, politička, vjerska, privatna, državna, školska, u svojem radu stvara određenu dokumentaciju. Ovisno o količini posla i veličini organizacije, količina novostvorene dokumentacije varira, korištenjem papirnatih izvornika dolazi do oštećenja, po zakonskim zahtjevima potrebno je izvornike očuvati u zahtijevanom periodu, što povećava troškove u smislu kadra i adekvatnih spremišnih prostora, te nakon određenog perioda zahtijeva nova rješenja u upravljanju dokumentacijom.

Digitalizacijom izvornih papirnih dokumenata te adekvatnim označavanjem (indeksiranjem) digitaliziranih dokumenata, zahtjev za brzim pronalaskom digitalizirane dokumentacije svodi se na karakteristike i brzine računala, računalnih baza i ostale tehnologije koja se koristi u tom procesu te kvalitetnog, preciznog i točnog označavanja. Na taj se način štite izvornici, poboljšava dostupnost te omogućuje stvaranje novih ponuda na tržištu. Nedostatak postojećih rješenja vidljiv je u nepostojanju modela/uvjeta zadovoljenjem kojih je moguće sa sigurnošću odgovoriti na pitanje je li digitalizirani zapis autentičan izvorniku.

U dokumentu proizašlom iz istraživanja InterPARES 2 koje je obuhvaćalo kako zakon gleda na autentičnost i autentifikaciju u državama Sjeverne Amerike, Europe i Kine, navodi se kako je u Sjevernoj Americi zapis autentičan ako jest ono što tvrdi da jest što znači kako se njegov identitet (ukupnost svojstava koji ga jedinstveno određuju kao što je ime autora i datum) i integritet (cjelokupnost i očuvanost) mogu pretpostaviti ili potvrditi[1]. U Europi se pojam autentičnosti promatra kroz pouzdanost sadržaja zapisa i zapisa kao cjeline, što je povezano s podrijetlom zapisa, proceduri i formi (pogotovo njegovi vanjski elementi kao što je pečat). U Kini se autentičan zapis definira kao zapis čije je bitne osobine (osobe suglasne za njegovo stvaranje, autor, primatelj, pisac, datum izrade, prijenosa i prijema) moguće identificirati, čiji je proces stvaranja, održavanja te umnožavanja strogo kontroliran, čiji je sadržaj registriran, i čiji oblik je kompletan (uključujući memorandum i pečat). Arhivistički rječnik autentičnost definira kao svojstvo zapisa da jest ono što se tvrdi da jest i da nije bio mijenjan te se najčešće odnosi na unutarnje i vanjske dokaze uzimajući u obzir fizičke značajke, strukturu, sadržaj i kontekst, odnosno ukupnost svojstava zapisa koja utvrđuju njegovo podrijetlo, pouzdanost, vjerodostojnost i točnost njegova sadržaja[2]. Otvorenim ostaje

[1] Duranti, L. (2005.). Authenticity and Authentication in the Law, InterPares 2 Project. Preuzeto 30.. 9. 2016. iz http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf

[2] Mihaljević, M., Mihaljević, M., & Stančić, H. (2015). Arhivistički rječnik. Zagreb: Zavod za informacijske studije Odsjeka za informacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.

pitanje koje karakteristike ili uvjete je potrebno zadovoljiti kako bi se potvrdila autentičnost digitaliziranog dokumenta.

Pregledom dosadašnjih istraživanja (Mckenna i De Loof[3], Deegan i Tanner[4], tehnički standard kongresne knjižnice[5], UNESCO[6], Vlada Alberte[7], mnoga tehnička rješenja kojima se upravlja procesima stvaranja i vođenja dokumentacije, prihvata, procesiranja (digitalizacije) i pohrane digitalnih slika[8]) i objavljenih publikacija proizlazi kako ne postoji jedan sveobuhvatni standard ili model koji odgovara na pitanje što je sve potrebno zadovoljiti, koje evidencije je potrebno voditi od stvaranja izvornika do izrade digitalne kopije i spremanja digitalne kopije u sustav za pretraživanje, pohranu, arhiviranje, očuvanje i prikaz, a pri čemu bi se digitalna kopija mogla smatrati autentičnom kopijom izvornika, tj. jednakovrijednom izvorniku.

Unutar InterPARES istraživanja grupa stručnjaka s fakulteta i državnih i općinskih arhiva iz Kine, SAD-a, Kanade, Hong Konga i Velike Britanije zvana Authenticity Task Force, provela je istraživanje koje je trajalo tri godine s ciljem identifikacije konceptualnih zahtjeva za procjenu i održavanje autentičnosti elektroničkih zapisa. Iz tog istraživanja proizlazi kako je za procjenu autentičnosti elektroničkih zapisa potrebno odrediti identitet i dokazati integritet elektroničkih zapisa[9]. U izvještaju navode skup zahtjeva koji služe kao referentna točka kojom se postiže pretpostavka autentičnosti elektroničkih zapisa te skup minimalnih zahtjeva kojima se određuje način izrade autentičnih kopija elektroničkih zapisa. Ovo istraživanje daje odgovor na probleme vezane uz autentičnost kad je riječ o elektroničkim dokumentima (izvorno nastalim ili digitaliziranim), međutim otvoreno ostaje pitanje kako osigurati autentičnost tijekom cijelog procesa nastanka dokumenta, pripreme za digitalizaciju i digitalizacije sve do uvoza u sustav koji čuva autentičnost.

[3] McKenna, G., & De Loof, C. (2009.). Digitisation : standards landscape for European museums, archives, libraries, ATHENA project.
[4] Deegan, M., & Tanner, S. (2002.). Digital futures : strategies for the information age. New York : London: Neal-Schuman Publishers, Library Association Publishing,.
[5] The Library of Congress Technical Standards for Digital Conversion Of Text and Graphic Materials. (7. 3. 2007.). Preuzeto 30. 9. 2016. iz http://memory.loc.gov/ammem/about/techStandards.pdf
[6] Fundamental principles of digitization of documentary heritage. (n.d.). Preuzeto 30.. 9. 2016. iz http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/digitization_guidelines_for_web.pdf
[7] Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf
[8] Angeles, C. N. (n.d.). Standards and Procedure in Digitization and Digital Preservation. Preuzeto 30.. 9. 2016. iz https://paarl.wikispaces.com/file/view/Standards+and+Procedure+in+Digitization+and+Digital+Preservation.pdf
[9] InterPares. (n.d.). Authenticity Task Force Report. Preuzeto 30.. 9. 2016. iz http://interpares.org/book/interpares_book_d_part1.pdf

Pri izradi ovog modela koji je razvijen u sklopu istraživanja u okviru ove doktorske disertacije, kao i definiranju uvjeta za postizanje autentičnosti, analiziran je pravni okvir, tehnički okvir, postojeći standardi i saznanja iz dobre prakse. Također, analiziran je elektronički potpis, elektronički žig i digitalni certifikat, digitalizacijski softveri, EXIF standard, RFID rješenje, mikroprint rješenje, PIQL-ov film, XML jezik i tehničke komponente koje se koriste u procesu digitalizacije.

NAPOMENA

Stavovi izneseni u ovoj disertaciji osobni su stavovi autora i ne mogu se ni pod kojim uvjetima smatrati službenim stavovima institucije u kojoj je autor disertacije zaposlen.

2. CILJ I METODOLOGIJA ISTRAŽIVANJA

Cilj doktorske disertacije je izrada *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije*, odnosno određivanje uvjeta za dobivanje autentičnih kopija (zapisa koji jest ono što tvrdi da jest i koji nije bio mijenjan) nastalih digitalizacijom izvornika u fizičkom obliku.

Za izradu navedenog modela potrebno je utvrditi unutarnje i vanjske dokaze s obzirom na fizičke značajke, oblikovanje obavijesti, raspored unutarnjih elemenata, dodatke, sadržaj, medij i kontekst, odnosno ukupnost svojstava digitaliziranog dokumenta koji utvrđuju njegovo podrijetlo, pouzdanost, vjerodostojnost i točnost njegova sadržaja.

Istraživačka pitanja za izradu modela su:

1. Pod kojim se uvjetima digitalnu kopiju dokumenta može smatrati jednakovrijednom izvorniku?
2. Postoji li korelacija između definiranih uvjeta i normi koje se odnose na pojedine sastavnice zapisa i procesa sa zapisom?
3. Pod kojim se uvjetima digitalni i digitalizirani dokument može ispisati kao dokument koji se po svojim svojstvima smatra jednakovrijednim izvorniku?

Metodologija istraživanja se sastoji od nekoliko koraka. Prvi korak bio je proučiti i prikupiti informacije iz relevantne literature i projekata ili slučajeva dobre prakse što je provedeno putem metode analize. Zatim je uslijedio korak sistematizacije prikupljenih informacija metodom sinteze. Korak definiranja uvjeta kojima se digitalizirana kopija dokumenta može smatrati jednakovrijednom izvorniku obavljena je korištenjem metode sinteze i konkretizacije. Slijedeći korak bio je utvrditi korelaciju između definiranih uvjeta i relevantnih normi, odnosno utvrditi osnovne zajedničke ili slične značajke između definiranih uvjeta i prepoznatih normi što je izvršeno metodom komparativne analize. Dobiveni uvjeti iz prethodnog koraka poslužili su kao temelj za izradu *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* korištenjem metode modeliranja. Izradom modela omogućeno je utvrđivanje uvjeta pod kojima se digitalni i digitalizirani dokument može ispisati kao dokument koji se smatra izvornikom. Ovaj korak proveden je metodom konkretizacije. Činjenice i procesi su se opisivali metodom deskripcije te obrađivali metodama analize i sinteze.

3. AUTENTIČNOST

3.1. Digitalizacija u Sjevernoj Americi i Europi

U SAD prihvatljiv dokaz na sudu bio je usmeno svjedočanstvo časnih građana[10]. Tijekom vremena i promjenom tehnologije pojavio se papir koji je postepeno postajao prihvatljiv na sudu, kojem je još uvijek bila potrebna dodatna potkrjepa usmenim svjedočanstvom, a kasnije se vodilo računa o pečatima, potpisima, formalnom dijelu dokumenta kao što je forma dokumenta, dizajn, rukopis i pisani oblik. S vremenom je donesen zakon (Zakon o ujednačenim fotografskim kopijama poslovnih i javnih evidencija kao dokaz, 1949.) koji je omogućavao fotokopiranim i mikrofilmiranim dokumentima prihvaćanje na sudu. Isti zakon omogućava uništavanje originala nakon postupka digitalizacije samo u slučaju kada su ispunjena tri zahtjeva:

1. korišteni ulazni postupci se moraju moći pokazati,
2. provedeni su testovi točnosti i pouzdanosti i mogu se priložiti,
3. može se dokazati da su zapisi stvoreni tijekom redovnog poslovanja.

Dodatno na ove zahtjeve AIIM (Association for Image and Information Management) 1992. godine određuje tri zahtjeva kojima se postiže visoka vjerojatnost prihvaćanja na sudu:

1. postoje pisane procedure o tome što je na ulazu a što na izlazu iz sustava,
2. provodi se obrazovni program za korisnike sustava,
3. postoji i provodi se sustav revizije.

Njemački porezni zakon omogućava digitalizaciju fizičkog papira i uništavanje originala ukoliko se digitalizacija provodi prema pravilima koja se odnose na obradu podataka pomoću pomoćnih računovodstvenih sustava[11]. Talijanski zakon, također omogućava u mnogim slučajevima stvaranje digitalne arhive od papirnate arhive koristeći takozvani zamjenski sustav za pohranu[12]. Prema tom zakonu elektronička pohrana se definira kao oni procesi koji osiguravaju pravnu valjanost dokumenta koji je kasnije digitaliziran. Pri tome takav sustav mora osigurati:

1. mogućnost identifikacije osobe koja je stvorila dokument,
2. integritet dokumenta,

[10] Piasecki, S. J. (1995). Legal Admissibility of Electronic Records as Evidence and Implications for Records Management. Preuzeto 30. 9 2016 iz American Archivist: http://americanarchivist.org/doi/pdf/10.17723/aarc.58.1.h715312706n38822

[11] VOI - Verband Organisations- und Informationssysteme e.V. (March 2010). Legal Requirements for Document Management in Europe. Dohvaćeno iz http://www.tech-arrow.com/wp-content/uploads/2015/01/legal-requirements-for-dms-in-eu1.pdf

[12] ibid.

3. čitljivost dokumenta,
4. laku dostupnost dokumenta,
5. identifikaciju informacija koje uključuju:
    a. izvornu registraciju,
    b. klasifikacijske podatke,
6. sigurnosne procedure,
7. pohranu slika dokumenata direktno na optički medij ili drugi prikladan nosač,
8. pohranu elektroničkog potpisa pripadajućeg dokumenta,
9. vremenski žig osobe odgovorne za pohranu, čime se osigurava točnost razvoja procesa,
10. format dokumenta koji se pohranjuje mora biti u statičnom i nepromjenjivom obliku:
    a. što znači da mora biti stvoren na način da se sadržaj ne može promijeniti tijekom faza pristupa dokumentu i pohrane dokumenta,
    b. kao ni protokom vremena.

Nakon dovršetka procesa elektroničke pohrane dopušteno je uništenje originalnog papirnatog dokumenta.

Španjolska porezna agencija izradila je proces certificirane digitalizacije kojim se digitalna slika dobivena digitalizacijom papirnatog računa pravno prihvaća kao original[13]. Taj proces određuje zahtjeve:

1. digitalna slika se elektronički potpisuje,
2. korišteni su certificirani uređaji dobiveni homologizacijskim procedurama,
3. vodi se revizijsko izvješće digitalizacijskog procesa,
4. koristi se ES-X-L kompletan elektronički potpis za koji nije potrebno tražiti mehanizam za provjeru valjanosti jer je njime zadovoljena neospornost i nepobitnost.

Francuska i Velika Britanija nemaju zakone kojima se omogućava da se dokumenti koji su nastali postupkom digitalizacije, odnosno pretvorbom papirnatog dokumenta u elektroničku kopiju unište[14]. Iako zakona nema u Velikoj Britaniji mnoge tvrtke na osnovu niske rizičnosti dokumentacije a radi značajnog poboljšanja poslovanja digitaliziraju svoju dokumentaciju i uništavaju originale, pri tome nakon procesa digitalizacije rezultirajuće slike pohranjuju na mikrofilm vodeći se standardom BS 6498:2002 Vodič za pripremu mikrofilmova i drugih mikrooblika koji se mogu tražiti kao dokaz, te standardom ISO/TR

[13] ibid.
[14] ibid.

15801:2009 Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost.

Austrijski Zakon o građanskom pravu dijeli dokumentaciju na javne i privatne dokumente, i ovisno o ovoj podijeli razlikuje način postizanja autentičnosti. Tako se autentičnim smatraju[15]:

1. javni dokumenti koji su izdani od strane vlasti, ovjereni kod javnog bilježnika ili javne strane vlasti,
2. privatni dokumenti koji su potpisani od osobe koja je stvorila dokument.

U nastavku će se objasniti različiti uvjeti za postizanje autentičnosti kod različitih vrsta dokumenata kao što su to npr. elektronički račun i dokument u elektroničkom obliku.

3.2. Elektronički račun

U Austriji se autentičnost i integritet sadržaja **elektroničkog računa** postiže[16]:

1. koristeći sigurni digitalni potpis (engl. secure electronic signature),
2. sigurni digitalni potpis se temelji na certifikatu izdanom od CA,
3. CA posluje prema zakonu o elektroničkom potpisu.

Zakon dopušta pohranu u elektroničkom obliku e-Računa u skladu s Francuskim standardom NF Z 42-013 Elektroničko arhiviranje - Zahtjevi za projektiranje i rad računalnih sustava kako bi se osiguralo očuvanje i cjelovitost dokumenata pohranjenih u takvim sustavima koji u zahtjevima za praćenje kronologije i sljedivosti informacija navodi:

1. svim provedenim procesima se može pratiti trag i oni su pohranjeni i čuvani,
2. svim provedenim procesima se može napraviti revizija,
3. koriste se pouzdane vremenske oznake (engl. time-stamp).

Zanimljivo je kako isti zakon ne propisuje ispis digitalno stvorenog dokumenta koji bi imao dokaznu vrijednost originala.

Talijanski zakon definira korištenje e-Računa kao pravno valjanog ukoliko je zadovoljeno slijedeće[17]:

1. e-Račun ne smije imati izvršne kodove ni makro naredbe.
2. autentičnost izvora i integritet sadržaja se garantira:
    a. dodavanjem vremenske oznake,

[15] ibid.
[16] ibid.
[17] ibid.

b. kvalificiranog elektroničkog potpisa izdavatelja,

3. sustav elektroničke pohrane mora osigurati:
    a. mogućnost identifikacije osobe koja je stvorila dokument,
    b. integritet dokumenta,
    c. čitljivost dokumenta,
    d. laku dostupnost dokumenta,
    e. identifikaciju informacija koje uključuju:
        i. izvornu registraciju,
        ii. klasifikacijske podatke,
    f. sigurnosne procedure.

Španjolsko Ministarstvo za gospodarstvo i financije propisalo je metodu za održavanje elektroničkih računa. Metoda propisuje[18]:

1. e-Računi se pohranjuju u bazama podataka zajedno s generiranim ili verificiranim elektroničkim potpisima,
2. baza podataka mora dodijeliti autentifikacijski kod svim porukama koje su vezane na svaku fakturu,
3. sve fakture koje su ispisane na papiru ispisane su zajedno sa pripadajućim autentifikacijskim kodom,
4. postoji mehanizam provjere potpisa,
5. mora biti moguće pristupiti fakturi putem elektroničkog autentifikacijskog koda.

Od kada je u Švicarskoj 2009. godine uveden EIDI-V (Pravilnik o elektroničkim podacima i informacijama) moguće je koristiti **elektroničke račune**. U pravilniku se razlikuje prije spomenuti sigurni digitalni potpis koji se koristi u Austriji i napredni digitalni potpis koji se koristi u Švicarskoj. Pravilnik propisuje tehničke, organizacijske i proceduralne zahtjeve kao na primjer[19]:

1. korištenje naprednog elektroničkog potpisa (engl. advanced electronic signature),
2. elektronički potpis izrađuje certifikacijska kuća,
3. certifikacijska kuća mora biti odobrena od strane ZertES,
4. vrši se provjera integriteta podataka,
5. vrši se provjera autentičnosti,
6. kvalificiranost potpisa se provjerava potvrdom digitalnog potpisa nakon prijenosa ili najkasnije prije upotrebe,

[18] ibid.
[19] ibid.

7. rezultat provjere mora biti dokumentiran,
8. javni ključ korišten prilikom provjere se mora pohraniti zajedno s ostalim podacima,
9. prilikom elektroničke pohrane potrebno je voditi računa da nije moguće mijenjati podatke,
10. ukoliko je omogućena promjena podataka postoje sigurni mehanizmi koji bilježe promjene,
11. sve procedure i infrastruktura koja je uključena u održavanje moraju biti dokumentirane,
12. sve procedure i infrastruktura koja je uključena u održavanje ažuriraju se prema potrebi,
13. sve procedure i infrastruktura koja je uključena u održavanje čuvaju se tijekom cijelog trajanja perioda čuvanja dokumentacije na koju se odnosi,
14. postoji inventar svih informacija,
15. inventar svih informacija je čuvan od neovlaštenog pristupa,
16. pristup i pregled dokumentima treba biti zapisan,
17. zapisi se čuvati tijekom cijelog perioda čuvanja dokumentacije na koju se odnosi,
18. sve operacije pristupa čitanju arhiviranom materijalu trebaju biti zapisane,
19. provodi se redovna provjera čitljivosti podataka,
20. u slučaju narušavanja čitljivosti radi se migracija podataka na nove medije.

U Velikoj Britaniji se **elektronički račun** pravno prihvaća ukoliko se može garantirati autentičnost porijekla i integritet podataka što se postiže korištenjem naprednog elektroničkog potpisa, EDI (sustav za elektroničku razmjenu podataka) ili drugim sredstvima[20]. Kada se radi o javnim ili privatnim institucijama tada se dokument prihvaća bez dodatnih dokaza ukoliko se može pokazati kako on pripada dosjeu. Dokaz da dokument pripada dosjeu mora biti opravdan podnošenjem potvrde koju je potpisao službenik javne ili privatne institucije kojoj dosje pripada.

3.3. Dokument u elektroničkom obliku

U Francuskoj je dokument u elektroničkom obliku prihvatljiv kao dokaz na isti način kao i papirnati dokument ukoliko se mogu zadovoljiti slijedeći zahtjevi[21]:

[20] ibid.
[21] ibid.

1. moguće je identificirati osobu koja je izdala dokument, na primjer korištenjem elektroničkog potpisa,
2. dokument je stvoren i pohranjen pod takvim uvjetima pod kojima se garantira integritet dokumenta.

U Njemačkoj **elektronički dokumenti** koji su potpisani sigurnosnim mehanizmom kvalificiranog elektroničkog potpisa prema Zakonu o digitalnom potpisu utvrđuju vlasnika potpisnog ključa te se autentičnost pretpostavlja sve dok se ne pokaže suprotno[22]. Kvalificirani elektronički potpis je još jedna vrsta elektroničkog potpisa, pored navedenog sigurnog elektroničkog potpisa i naprednog elektroničkog potpisa.

Međutim kada je riječ o **e-mail porukama** nije jednoznačno je li poslan e-mail također i primljen. Problem primitka i slanja e-mail poruka sastoji se u tome što potvrdu o primitku može poslati sustav sam iako osoba nije primila poruku, kao što može neautorizirana strana poslati određenu mail poruku (na primjer krađom lozinki). Ovo se može izbjeći na slijedeći način:

1. po primitku poruke vrati se obavijest koja je potpisana kvalificiranim elektroničkim potpisom (koji sadrži originalni tekst),
2. slanje e-mail poruke se potpiše kvalificiranim elektroničkim potpisom.

Prema Pravilniku o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva gradivo u elektroničkom obliku treba zadovoljiti slijedeće zahtjeve:

1. gradivo se pohranjuje na sustavu koji onemogućuje brisanje, mijenjanje i dodavanje podataka,
2. podaci se pohranjuju u najmanje dvije kopije, od kojih je jedna izvan sustava koji se koristi za pregled gradiva,
3. pristup gradivu je očuvan tijekom cijelog perioda čuvanja,
4. opisan je format i struktura zapisa,
5. propisan je način njegovog čuvanja,
6. gradivo se štiti od neovlaštenog pristupa ili mijenjanja podatka,
7. propisano je provođenje izlučivanja gradiva,
8. svi opisi su dostavljeni nadležnom Državnom arhivu,
9. prilikom izdvajanja gradiva u sustav za čuvanje arhivskog gradiva potrebno je provjeriti čitljivost i cjelovitost elektroničkih zapisa,
10. postoji određen stručni radnik za poslove s papirima i s elektronskim dokumentima.

[22] ibid.

3.4. Rasprava: autentičnost

U dokumentu Advice 21, Dokazi i javni elektronički dokumenti, koji je izdala australska država Viktorija, kaže se kako je jedan o primarnih razloga za čuvanje dokumenata pružanje dokaza o aktivnostima, odlukama i poslovnim procesima[23]. Zatim se navodi da dokument treba biti autentičan, pouzdan i dostupan. Autentičan znači da zapis može dokazati da jest to što tvrdi da jest, pouzdan znači da se može dokazati kako ga se nije mijenjalo odnosno da je nepromijenjen, i dostupan znači da ga je moguće čitati i interpretirati kad god se za to ukaže potreba.

Nadalje se navode tri kriterija kojima se može postići da dokumentacija bude dobar dokazni materijal, a to su:

1. moguće je dokazati autentičnost i pouzdanost,
2. postoji stalna dostupnost dokumentacije (za cijelo vrijeme trajanja roka čuvanja),
3. moguće je pokazati točnost reprodukcijskog procesa (u slučajevima konverzije zapisa).

Zatim se dodaje da je, neovisno o formatu, autentičan onaj dokument koji može dokazati:

1. da jest ono što tvrdi da jest,
2. da je stvoren i poslan od strane osobe za koju se tvrdi da je zapis stvorila i poslala,
3. da je stvoren i poslan u vrijeme kada se tvrdi da je stvoren i poslan.

Kada je riječ o papirnatom dokumentu kontekst je reprezentiran fizički, međutim kada se papirnati dokument konvertira u digitalni, digitalizirani dokument, kontekst se reprezentira korištenjem odgovarajućih metapodataka koji se u prihvatnom procesu (engl. capturing process) zapisuju kako bi osigurali razumijevanje konteksta te na taj način ograničili ranjivost pouzdanosti i autentičnosti. Digitalizirani dokument je pouzdan ukoliko je moguće pokazati kako reprodukcijski proces konstantno proizvodi kompletnu i točnu kopiju originala. To znači da ukoliko se u bilo kojoj situaciji može pokazati kako se određeni zapisi:

1. uvijek stvaraju,
2. uvijek stvaraju na istoj točki procesa,
3. uvijek pohranjuju na istom mjestu,
4. uvijek održavaju na isti način,

[23] Public Record Office Victoria. (January 2010). Evidence and Electronic Public Records. Preuzeto 30. 9. 2016. iz State of Victoria, Australia: http://studylib.net/doc/18578486/evidence-and-electronic-public-records

5. uvijek im pristupaju iste osobe i za iste svrhe,

tada se:

1. za svaku transakciju može tvrditi kako su svi zapisi prisutni i moguće ih je nabrojati,
2. za svaki dokument lakše može tvrditi da je autentičan zbog konzistentnosti procesa koji ga okružuje te svjedočanstva koja izviru iz pripadajućih metapodataka.

U procesu digitalizacije potpuna i točna kopija podrazumijeva osiguranje da su sve stranice (uključujući obje strane, te gdje je primjereno podaci s raznih papirića i post-it-a) reproducirane.

Integritet i pouzdanost zapisa se odnosi na činjenicu da su zapisi kompletni i nepromijenjeni, što znači da su osigurani od neovlaštenog pristupa i mijenjanja. Ukoliko zapisi trebaju biti mijenjani ili postoji rizik da se zapis može promijeniti tada je potrebno voditi dnevnik promjena. Stvaranje i čuvanje logova treba biti dokumentirani dio strategije vođenja dokumentacije (engl. records management), te bi trebala biti automatska funkcija sustava bez uključivanja ljudskog faktora. Takav zapis u logu bi trebao uključivati informaciju o okolnostima koje su dovele do promijene. Očuvanje integriteta moguće je postići i dobro definiranim kontrolama kvalitete.

Stephen Mason Barrister, odvjetnik, i direktor programa koji istražuje dokaze, u dokumentu Dokaz autentičnosti dokumenta u digitalnom formatu koji je uveden kao dokazni materijal, autentičnost definira na slijedeći način: autentičnost treba dati odgovor na pitanje je li dokument ono za što se tvrdi da jest[24].

Ovo može uključivati izvornost, autorstvo, ovjeru i druge zahtjeve koji mogu utjecati na nepobitnost dokumenta.

Odnosno, ukoliko bilo koja strana treba dokazati autentičnost dokumenta tada je svaka pretpostavka koja se može primijeniti na kreiranje dokumenta relevantna i potreban je usmeni dokaz kojim će se provjeriti nepobitnost dokumenta i to:

1. od čega se, u fizičkom obliku, dokument sastoji,
2. izvor dokumenta (je li bilo svjedoka prilikom potpisivanja dokumenta, postoje li bilo kakve oznake identifikacije dokumenta kao što je na primjer ime i adresa, postoje li drugi dokazi koji povezuju dokument s kontekstom u kojem se dokument nalazi kao na primjer povezujuća korespondencija, postoji li fizička karakteristika nosača dokumenta kao što je to zaglavlje, postoji li poštanska oznaka ili drugi vanjski dokazi

[24] Barrister, S. M. (2006.). Proof of the authenticity of a Document in electronic format Introduced as evidence. Preuzeto 30. 9. 2016. iz ARMA International Educational Foundation: http://www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/Proof_of_authenticity_of_a_document.pdf

ili svjedočanstvo treće strane o postojanju transakcije kao na primjer svjedočanstvo stručnjaka),

3. integritet sadržaja, odnosi se na sadržaj dokumenta i dokaz da nije bilo mijenjanja dokumenta.

Posebno se ističe da je sljedeće kategorije potrebno uzeti u obzir:

1. fokus na dokument:
    a. određivanje izvornosti podataka koji se čuvaju,
    b. bilježenje i čuvanje podataka kojima dokument postaje cjeloviti zapis,
2. fokus na tehnički proces:
    a. osigurati pouzdanost procesa stvaranja, prihvata i rukovanja podacima,
    b. osigurati integritet podataka, uključujući korištenu tehnologiju i proces kontrole podataka,
    c. s ciljem osiguranja da se podaci mogu ispravno dohvatiti i interpretirati,
3. fokus na organizacijski proces:
    a. osigurati da se politike i procedure kojima se rukuje podacima ispravno dokumentiraju, te da postoje dokazi kojima je moguće prikazati da su se te politike primjenjivale.

U svojoj osnovi, navodi se, karakteristike autentičnosti su:

1. pouzdanost – postoje dokazi kako su zapisi stvarani i digitalizirani kao dio propisanog poslovnog procesa, i podložni su procesima upravljanja poduzeća,
2. integritet – dokument je zaštićen od neovlaštenih izmjena,
3. dostupnost – moguće je na ispravan način dohvatiti, prikazati i tumačiti dokument.

Barrister sugerira da je potrebno obavljati potpunu dokumentiranost svega što se čini kako bi se osiguralo očuvanje podataka.

Seth Dalby napravio je popis definicija i izvora koji se odnose na autentičnost i autentifikaciju. Tako se navode slijedeće definicije[25]:

- **Dokument je autentičan** ili se dokazala autentičnost originala kada je dokazano kada je dokument pisan, ispisan na papiru, izvršen ili potpisan kao što se tvrdi da jest.
    - Autentičan znači vjerodostojan, na koji se može osloniti, pouzdan, pravi, stvaran, istinit, ili originalan. Originalno ili autentično ili stvarno je ono što

[25] Dalby, S. (December 2004). Authenticity/Authentication Definitions and Sources. Preuzeto 30. 9. 2016. iz InterPARES 2 Project: http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity_definitions-sources.pdf

posjeduje kvalitetu onoga za što se tvrdi da jest; ili, da nije lažno ili krivotvoreno.

- Fotografija je autentična ako predstavlja dovoljnu i preciznu reprezentaciju onoga što se tvrdi da opisuje.

- **Dokazana kopija** označava dokument koji je prava kopija originala. Pri čemu prava kopija znači kopiju pravnog dokumenta identičnog originalu sa svim bilješkama, sudskim pečatima, potpisima svih stranaka i sudskog registra, svim dodacima i ispravcima upisanih u kopiju unutar navodnih znakova.
    - Dokazana kopija pisma, telekomunikacije ili telegrama čiji original je poslan kada se tvrdi i primljen od strane primatelja.
- **Dokument se smatra autentičnim** ukoliko svjedok jamči autentičnost ili dokument ispunjava zahtjeve samoautentifikacije. Samoautentifikacija je autentifikacija bez vanjskih dokaza istinitosti i izvornosti. U SAD-u se u državnim sudovima određeni dokumenti, kao što je ovjereni dokument i potvrđena kopija javnih spisa, prihvaćaju kao dokazni materijal po principu samoautentifikacije.

Arhivistički rječnik daje slijedeće definicije povezane s autentičnosti[26]:

- **Autentična kopija** (engl. authentic copy) je službeno ovjerena kopija koja je pravno valjana te se njome može koristiti kao dokazom na sudu.
- **Autentični zapis** (engl. authentic record) je zapis koji jest ono što tvrdi da jest i koji nije bio mijenjan.
- **Potvrditi** (engl. authenticate) znači:
    a. Pokazati se točnim, istinitim ili vjerodostojnim.
    b. Proglasiti usmeno ili pismeno ili dodavanjem pečata da je entitet ono što jest tek nakon provjere njegova identiteta.
- **Autentificiran** (engl. authenticated) znači koji je izvoran, koji zaista potječe od onoga kojemu se pripisuje.
- **Potvrđeni zapis** (engl. authenticated record) je zapis čiju je autentičnost u određenome trenutku potvrdila tada mjerodavna pravna osoba kao što je javni službenik, javni bilježnik, certifikacijska služba i sl.
- **Autentifikacija** (engl. authentication), sinonim je potvrđivanje, je
    1. a. Provjera je li koji objekt ono za što se tvrdi da jest temeljem čega se on prihvaća ili ne prihvaća kao izvornik.

[26] Mihaljević, M., Mihaljević, M., & Stančić, H. (2015). Arhivistički rječnik. Zagreb: Zavod za informacijske studije Odsjeka za informacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.

b. Utvrđivanje identiteta pošiljatelja.

2. Čin potvrđivanja dokumenta ili reprodukcije dokumenta kao izvornoga.
3. Potvrda mjerodavne pravne osobe kao što su javni bilježnik, certifikacijska služba i sl. ili autoriziranoga sustava o autentičnosti zapisa u trenutku provjere.

- **Autentičnost** (engl. authenticity) znači:
  1. Svojstvo zapisa da jest ono što se tvrdi da jest i da nije bio mijenjan te se najčešće odnosi na unutarnje i vanjske dokaze uzimajući u obzir fizičke značajke, strukturu, sadržaj i kontekst.
  2. Ukupnost svojstava zapisa koja utvrđuju njegovo podrijetlo, pouzdanost, vjerodostojnost i točnost njegova sadržaja.
- **Autor** (engl. author) je:
  1. a. Fizička ili pravna osoba pod čijim djelovanjem i čijim radom nastaje arhivsko i registraturno gradivo.

     b. Odjel ili druga ustrojstvena jedinica koja stvara ili izvorno zaprima zapis.
  2. Fizička ili pravna osoba koja ima pravo i sredstva da izda zapis ili u čije ime ili po čijem se nalogu zapis izdaje.
  3. Osoba, korporativno tijelo ili obitelj koji su odgovorni za intelektualni ili umjetnički sadržaj dokumenta.

S druge strane Arhivistički rječnik razlikuje autentičnost od vjerodostojnosti te definira:

- **Vjerodostojna kopija** (engl. authoritative copy) je inačica zapisa koju stvaratelj smatra službenim zapisom i koja je najčešće podvrgnuta procedurnomu nadzoru koji drugi oblici kopija ne zahtijevaju.
- **Vjerodostojni zapis** (engl. autoritative record) je zapis koji stvaratelj smatra službenim i koji je najčešće podvrgnut procedurnom nadzoru koji drugi oblici kopija ne zahtijevaju.

Zbog sličnosti pojmova dobro je istaknuti definiciju Arhivističkog rječnika prijave korisnika u sustav:

- **Autentikacija** (engl. login) je provjera korisnika pri ulasku u sustav.

Norma ISO 15489-1:2001 - Informacije i dokumentacija - Upravljanje zapisima - 1. dio: Općenito definira pojmove: dokumentirati transakciju, autentičan zapis, pouzdan zapis, integritet zapisa i iskoristiv zapis na slijedeći način:

- **Autentičan zapis** je zapis za koji se može dokazati**:**

1. da jest ono što tvrdi da jest,
2. da ga je izradila ili odaslala osoba za koju se tvrdi da ga je izradila ili poslala,
3. da je izrađen ili odaslan u vrijeme za koje se to tvrdi.

- **Pouzdan zapis** je zapis za čiji se sadržaj može vjerovati da potpuno i točno predstavlja transakcije, aktivnosti ili činjenice koje potvrđuje i o kojima može biti ovisan tijekom sljedećih transakcija i aktivnosti. Zapisi trebaju nastati u vrijeme transakcije ili događaja na koji se odnose, ili kratko nakon toga, trebaju ih stvarati pojedinci koji izravno poznaju činjenice ili uređaji koji se u poslovanju rutinski koriste za obavljanje transakcija.
- **Integritet zapisa** postoji za zapis koji je potpun i neizmijenjen. Politikom i postupcima u upravljanju zapisima treba biti određeno koji se dodaci i bilješke mogu dodati zapisu nakon što je nastao, pod kojim se uvjetima dodaci i bilješke autoriziraju i tko je ovlašten dodavati. Svaka autorizirana bilješka, dodatak ili brisanje trebaju biti eksplicitno naznačeni i provjerljivi.
- **Iskoristiv zapis** je onaj zapis kojemu je moguće utvrditi smještaj, dohvatiti ga, predočiti i interpretirati (povezati s aktivnošću ili transakcijom koja ga je proizvela).

Kako bi se postigla autentičnost spisa norma ISO 15489-1:2001 predlaže slijedeće zahtjeve:

1. primijenjena je i dokumentirana politika i postupci koji upravljaju stvaranjem, zaprimanjem, prosljeđivanjem, čuvanjem i stavljanjem zapisa na raspolaganje,
2. u politikama i postupcima su navedeni stvaratelji zapisa koji su za to ovlašteni te zaštita zapisa od neovlaštenog dodavanja, brisanja, mijenjanja, korištenja i uništenja.

Navedeni zahtjevi se mogu ispuniti, prema normi ISO 15489-1:2001, ukoliko je moguće pomoću stvorenog i pripremljenog materijala pokazati kako:

1. zapisi nastaju u skladu s pravnim propisima, politikama organizacije i procedurama koje su na snazi tijekom životnog vijeka sustava,
2. sustav djeluje i jest djelovao u skladu s poslovnom praksom organizacije,
3. se vodi dokumentacija o nadzoru i provjerama procesa koji djeluju i propisani su unutar sustava.

Kada se govori o autentičnosti često se spominje pouzdanost. Prema Duranti dokumenti se smatraju pouzdanim ukoliko su stvoreni od pouzdane osobe, dok taj isti dokument tijekom vremena dobiva oznaku autentičnosti ukoliko sadrži elemente kao što su

pečati ili potpisi koje je teško mijenjati[27]. Razlikujući dalje pouzdanost Duranti navodi: „Stupanj potpunosti i stupanj kontrole procedura nastanka su jedina dva čimbenika kojima određujemo pouzdanost zapisa.“[28] U ovom smislu razlika između pouzdanog dokumenta i autentičnog dokumenta je u tome što autentičan označava dokument „koji jest ono za što se tvrdi da jest“ [29], odnosno „[...] da nije proizvod manipulacije, zamjene ili krivotvorenja nakon dovršetka procedure stvaranja [...]“[30]. Dodatni koncept, kako ističe Duranti, je koncept istinitosti (engl. truthfulness) koja se sastoji od pouzdanosti i autentičnosti.

3.5. Zaključak o konceptu autentičnosti

Kako bi opisali autentičnost možemo se osvrnuti na predložene definicije spomenutih autora. Slažu se kako je **autentičnost** svojstvo dokumenta ili zapisa kojim se dokazuje da jest ono što tvrdi da jest.

Ovako definiranu autentičnost možemo postići ukoliko:

- znamo tko je stvaratelj, koji podaci i oznake trebaju biti prisutni na dokumentu i mogu li se svi podaci i oznake ispravno čitati i interpretirati,
- postoje dokazi kako je dokument stvaran i digitaliziran kao dio propisanog poslovnog procesa, i podložan je procesima upravljanja poduzeća te postoje dokazi kako dokument nije bio mijenjan,
- je moguće dokumentu ispravno pristupiti, prikazati i tumačiti,
- postoje dokazi kako su sve stranice dokumenta reproducirane (uključujući obje strane, te gdje je primjereno podaci s raznih dodatnih papira i post-it-a),
- su u postupku digitalizacije zapisani svi podaci koji vjerno opisuju proces.

Drugim riječima, digitalizirani dokument je autentičan ukoliko je ispunjeno:

1. POTPUNOST: podaci i oznake su prisutni na dokumentu i povezani su s dokumentom, sve stranice dokumenta su snimljene uključujući obje strane i pripadni dodaci i poznat je podatak o stvaratelju,
2. POUZDANOST PROCESA: proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije, proces je nadziran i provjeravan tijekom digitalizacije i o tome postoje evidencije,

[27] Duranti, L. (1995). Reliability and Authenticity: The Concepts and Their Implications. Preuzeto 1. 2018. iz Archivaria: https://archivaria.ca/index.php/archivaria/article/download/12063/13035
[28] ibid., str. 6
[29] ibid., str. 7
[30] ibid., str. 7

3. INTEGRITET DOKUMENTA: podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta ili od trenutka prihvata u poslovni sustav,
4. DOSTUPNOST: dokumentu i svim podacima i oznakama na dokumentu i povezanim s dokumentom može se pravilno pristupiti i ispravno ih čitati i tumačiti.

4. ŽIVOTNI CIKLUS DOKUMENTA

Danas postoje mnogi različiti modeli životnih ciklusa koje dokument prolazi, kao što je primjer složenog modela koji su izradili u Digital Curation Centru (vidi http://www.dcc.ac.uk/resources/curation-lifecycle-model op.a.). U nastavku je opisan ciklus koji dokument prolazi od stvaranja i prihvata u dokumentacijski sustav tvrtke, proces digitalizacije te daljnji životni ciklus tako stvorenog digitaliziranog dokumenta. Koraci koje dokument prolazi prepoznati su u tehničkim izvještajima ISO/TR 15801:2009, ISO/TR 15498-2:2001 Informacije i dokumentacija – Upravljanje zapisima – Drugi dio: Smjernice i ISO/TR 13028:2010 Informacije i dokumentacije - Implementacijske smjernice za digitalizaciju, normama ISO 15489-1:2001, HRN ISO 11799:2004 – Informacije i dokumentacija – Zahtjevi za pohranu dokumenata arhivske i knjižnične građe, u Zakonu o arhivskom gradivu i arhivima, Pravilniku o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva, Pravilniku o korištenju arhivskog gradiva, te u primjerima dobre prakse koji su popisani u tehničkim standardima Kongresne knjižnice D.C. i ministarstva Vlade Alberte. Ovi koraci se međusobno isprepliću i nadopunjavaju a ovdje su prikazani u sažetom obliku.

4.1. Papirnata dokumentacija

STVARANJE

Australski Public records Ofiice opisuje proces stvaranja dokumenta na sljedeći način: autor izradi dokument kako bi se „[...] pokrenula određena aktivnost, donijela određena odluka ili definirao određeni proces[...]“[31], potpiše ga i on postaje autentičan trenutkom ulaska u poslovni sustav bilo predajom unutar organizacije, primjer toga je Odluka Uprave o radnom vremenu, ili predajom u određenu organizaciju (javnu ili privatnu), primjer toga je predaja dokumentacije za natječaj za nabavu skenera.

PRIHVAT ILI REGISTRACIJA

Norma ISO 15489-1:2001, koja se odnosi na upravljanje zapisima, ali se ne odnosi na upravljanje arhivskim zapisima, koji su nastali ili su zaprimljeni od strane javne ili privatne

[31] Public Record Office Victoria. (January 2010). Evidence and Electronic Public Records. Preuzeto 30. 9. 2016. iz State of Victoria, Australia: http://studylib.net/doc/18578486/evidence-and-electronic-public-records, str. 3

organizacije u obavljanju njezine djelatnosti, kao i bilo kojeg pojedinca koji je dužan stvarati i čuvati zapise, prepoznaje ovaj korak kao **prihvat** ili **registraciju** dokumenta i preporuča dokument označiti jedinstvenom oznakom odnosno klasifikacijskom oznakom prema pravilu koji je tvrtka odredila. Prihvatom u sustav je potvrđena autentičnost dokumenta.

KRETANJE I PRAĆENJE

Nakon zaprimanja dokumenta slijedi korak u kojem dokument dalje putuje prema unaprijed propisanom tijeku te obavlja svrhu koja mu je namijenjena i zbog koje je stvoren. Na primjer, prikupljena dokumentacija za natječaj za nabavu skenera se skuplja i predaje osobama koje su određene za provođenje nabave kao što su stručnjak za davanje tehničke ocjene ili stručnjak za davanje ekonomske ocjene svih prikupljenih ponuda. Ovaj korak norma ISO 15489-1:2001 prepoznaje kao **kretanje i praćenje** dokumenta.

Dokument u svojem kretanju, odnosno korištenju, može obavljati različite aktivnosti te mu se mogu pripojiti novi dokumenti. Primjer toga su prethodno navedena ekonomska i tehnička ocjena ili odluka o odabiru ponuđača skenera, a svi dokumenti zajedno čine spis koji se preporuča smjestiti u tehničku jedinicu, na primjer zaštitni omot ili registrator, radi čuvanja dokumentacije. Norma ISO 15489-1:2001 preporuča tijekom korištenja zapisa provoditi sigurnosnu mjeru **praćenja** dokumenta koja se postiže određivanjem statusa dostupnosti i sigurnosti zapisa, određivanje prava pojedinaca unutar i izvan organizacije kojima je dopušteno koristiti zapise, osiguravanje da samo ti određeni pojedinci zaista i koriste zapise, praćenje dokumenta tko ga čuva i vođenje evidencije tko ga je čuvao te provođenje redovite revizije provođenja praćenja, dostupnosti i klasifikacije dokumenta.

SREĐIVANJE GRADIVA

Ovako stvoreni niz daljnjih dokumenata koji prate početni nakon završetka aktivnosti tvore dokumentacijsku cjelinu. Primjer toga je dokument smješten u zaštitni omot koji čini predmet, dosje ili svezak[32]. Preporuka norme je **dokumentacijsku cjelinu registrirati i klasificirati**, odnosno dodijeliti joj jedinstvenu oznaku. Članak 8. Pravilnika o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva određuje arhivsko gradivo odlagati i čuvati **u sređenom stanju**, tehnički opremljenim, u zaštitnom omotu, oblikovano u arhivske jedinice te s popisom svih zapisa i dokumenata koji pripadaju arhivskoj jedinici, kao i podatak

[32] Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan ARHIVA. (19. 5. 2004.). (NN 63/04).

o dokumentima koji nedostaju. Zbog ovog zahtjeva iz Pravilnika dokumenti uloženi u spis se popisuju i popis postaje sastavni dio dokumentacijske cjeline. Ovdje je dobro napomenuti kako je jedan od zahtjeva autentičnosti potpunost dokumentacije koju često nije moguće provjeriti ukoliko nije poznat broj stranica svakog dokumenta prilikom stvaranja dokumentacijske cjeline, ili prilikom prihvata u sustav.

POHRANA

Kada je namjena dokumenta završena spis, koji se sada već nalazi uložen u zaštitni omot i čini predmet, se odlaže na predviđeno mjesto koje norma ISO 15489-1:2001 prepoznaje kao **smještaj zapisa**, odnosno **pohrana** i preporučaju da pohrana bude uključena u „[...] cjelinu spisovodstvenog programa.“[33]. Prilikom pohrane potrebno je voditi računa o spremišnom prostoru te postupcima čuvanja i rukovanja dokumentacijom. Na primjer, police trebaju biti metalne s takvim premazima koji ne ispuštaju tvari koje mogu prouzročiti uništavanje dokumentacije. Prostor za čuvanje s ciljem dugoročne pohrane je dobro opisan normom HRN ISO 11799:2004, a kada je riječ o arhivskom gradivu prostor za čuvanje gradiva, odnosno smještaj gradiva, propisan je točkom IV. Smještaj gradiva u Pravilniku o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva.

ODABIR

Trenutno važeći[34] Zakon o arhivskom gradivu i arhivima sve gradivo koje nastaje radom javnih ili privatnih fizičkih ili pravnih osoba zove registraturnim gradivom. Registraturno gradivo u prijedlogu novog Zakona o arhivskom gradivu i arhivima mijenja naziv u dokumentarno gradivo. Dokumentarno gradivo koje je od važnosti za Republiku Hrvatsku, odnosno na koje se može primijeniti Zakon o arhivskom gradivu i arhivima, treba, prema važećem Zakonu **odabirati**, **predavati** nadležnom Državnom arhivu i redovito **izlučivati** nakon primljene suglasnosti nadležnog Državnog arhiva. Postupak odabira gradiva provodi se prema Pravilniku o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva i propisan je Člankom 12.

[33] ISO/TR 15498-2:2001 Informacije i dokumentacija – Upravljanje zapisima – Drugi dio: Smjernice. (2001)., 4.3.7.1. Odluke o pohrani spisa

[34] Trenutno važeći zakon je onaj iz 1997. godine. Prijedlog novog Zakona o arhivskom gradivu i arhivima je u postupku prihvaćanja i za vrijeme pisanja ovog rada prošao je 1. čitanje u Hrvatskome Saboru.

PREDAJA U ARHIV

Nadležnom državnom arhivu predaje se samo ono gradivo koje je Arhiv odabrao kao arhivsko gradivo. Neovisno je li riječ o arhivskom gradivu ili je riječ o gradivu koje je pravna ili fizička osoba klasificirala za dugoročno čuvanje. Primjer toga su platne liste zaposlenika koje se prema Zakonu o računovodstvu trebaju čuvati trajno.

POHRANA U ARHIV

Norma ISO 15489-1:2001 prepoznaje gradivo za trajno čuvanje te napominje kako ono treba biti dostupno tijekom cijelog perioda čuvanja, ali i sve značajke gradiva trebaju biti sačuvane tijekom cijelog perioda čuvanja. Predaja arhivskog gradiva propisana je člankom 15. koji kaže: „stvaratelji i imatelji javnoga arhivskog i registraturnog gradiva dužni su ga predati nadležnom arhivu u izvorniku, sređeno, označeno, popisano, u zaokruženim cjelinama te tehnički opremljeno, u skladu s Pravilnikom o predaji arhivskoga gradiva arhivima“[35].

IZLUČIVANJE I UNIŠTAVANJE

Sva dokumentacija prije ili kasnije dolazi do koraka **uništavanja**, hotimičnog ili zbog propusta tijekom čuvanja dokumentacije ili drugih nepredvidljivih okolnosti. Kao što je Zakonom o arhivskom gradivu i arhivima prepoznato uništavanje gradiva, tako se i tehnički izvještaj ISO/TR 15801:2009 također osvrće na ovaj korak. U tom koraku je potrebno voditi računa o određenim zahtjevima koji mogu biti zakonskog karaktera ili operativnog karaktera ili oboje. Prema izvještaju, koraku uništavanja dokumentacije prethodi provjera je li potrebno čuvati originalni papir, te ukoliko je potrebno čuvati originalni papir postoje li propisani postupci čuvanja. Ukoliko čuvanje nije potrebno, originalni papir se može uništiti. Ukoliko je čuvanje potrebno, potrebno ga je provoditi prema propisanim postupcima sve dok ne nastupi istek roka čuvanja. Nakon što nastupi istek roka čuvanja, originalni papir se može uništiti. U slučaju kada je moguće uništiti originalni papir izvještaj napominje kako je potrebno provjeriti je li propisan postupak uništavanja dokumenata te čuva li se dokumentacija o uništavanju. Uništenje gradiva je propisano člankom 13. Zakona o arhivskom gradivu i arhivima koje se provodi na način da se poduzimaju mjere zaštite tajnosti podataka.

[35] Zakon o arhivskom gradivu i arhivima (ZAGA). (29. 09. 1997.). (NN 105/97, 64/00, 65/09, 125/11, 46/17)., Članak 15

KORIŠTENJE ARHIVSKOG GRADIVA

Predajom **arhivskog gradiva** ne završava životni ciklus dokumenta zbog toga što je i takvom gradivu moguće pristupiti i zatražiti ga na uvid i **korištenje**. Primjer toga su različite studije kretanja stanovništva koje se rade prema sačuvanim popisima stanovništva.

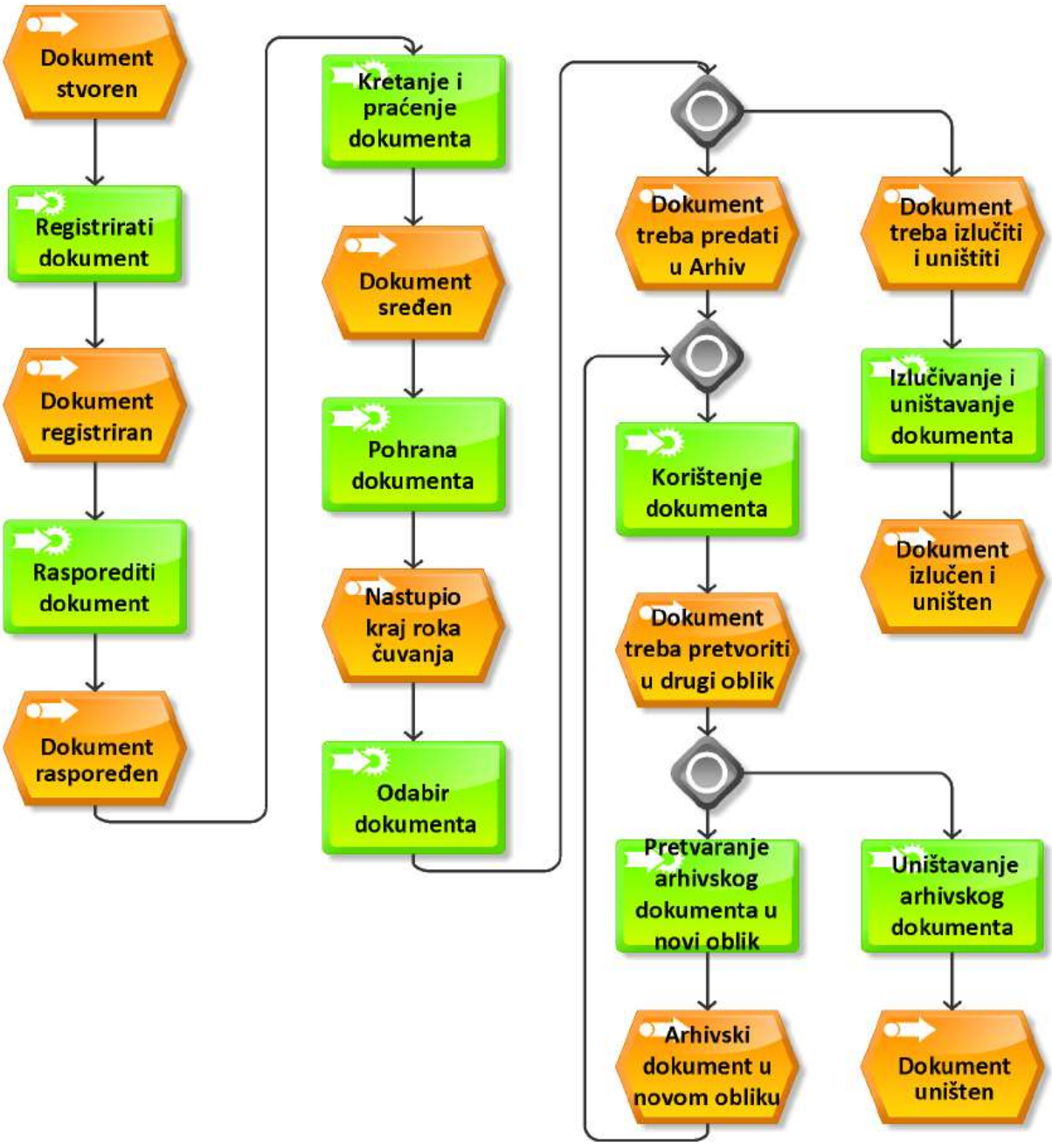
PRETVORBA U DRUGI OBLIK

Zakon o arhivskom gradivu i arhivima propisuje člankom 23. kako se na korištenje daju „[…] snimci arhivskog gradiva“[36] osim iznimno gradivo je moguće dati na korištenje u izvorniku ukoliko se prethodno napravi zaštitni snimak. Članak 26. istog zakona upućuje na „Način, uvjete i postupak korištenja javnoga arhivskog gradiva […]“[37] kako je propisano Pravilnikom o korištenju arhivskog gradiva.

UNIŠTAVANJE ARHIVSKOG GRADIVA

Uništavanje arhivskog gradiva prema trenutno važećem Zakonu nije dopušteno odnosno izričito nema riječi o toj mogućnosti. Prijedlog novog Zakona dopušta **uništavanje izvornog arhivskog gradiva** nakon pretvorbe u drugi oblik i uz pribavljenu suglasnost Hrvatskog arhivskog vijeća. Članak 9. prijedloga novog Zakona o arhivskom gradivu i arhivima za pretvorbu u drugi oblik koristi termine „reproducirati, konvertirati ili migrirati“[38]. Slično tome tehnički izvještaj norme ISO/TR 15489-2 naziva „strategiju zaštite spisa radi čuvanja dostupnosti, cjelovitosti i autentičnosti spisa tijekom vremena“[39] i kao strategije navode kopiranje – „stvaranje identične kopije na istoj vrsti medija, konverzija promjena formata zapisa ali osiguranje da zapis zadržava identične primarne informacije“[40] i migraciju – „skup organiziranih zadaća namijenjenih povremenom prijenosu digitalnih zapisa iz jedne konfiguracije hardvera/softvera u drugu ili iz jedne generacije tehnologije u drugu“[41]. Dijagram 1 pokazuje kretanje fizičkog papira od stvaranja do uništenja.

[36] ZAGA, Članak 23
[37] ibid., Članak 26
[38] Prijedlog Zakona o arhivskom gradivu i arhivima, Članak 9
[39] ISO/TR 15489-2 (n. dj.), točka 4.3.9.2 Trajno čuvanje
[40] ibid.
[41] ibid.



Dijagram 1. Kretanje fizičkog papira od stvaranja do uništenja

4.2. Proces digitalizacije

ODABIR

Postupak digitalizacije je postupak prilikom kojeg prevodimo analogni zapis u digitalni[42]. Primjer toga su zapisi na gramofonskoj ploči koji su postupkom digitalizacije pretvoreni u digitalne zapise, na primjer u WAV formatu, ili filmovi koji su snimljeni na velikim filmskim vrpcama za prikazivanje u kinima i isti takav film pretvoren u zapis koji možemo čitati pomoću DVD čitača i gledati na kućnom ekranu, ili pretvorba papira u sliku u JPG formatu. Tijekom ovog postupka potrebno je proći određene korake. Prvi korak, kako navodi Stančić, je odabir gradiva za digitalizaciju[43]. Odabir gradiva treba pratiti propisane procedure i zahtjeve tvrtke koja se odlučuje na digitalizaciju, te normativna i zakonska ograničenja koja se odnose na odabranu građu kao što je autorsko pravo.

ANALIZA GRADIVA I PLANIRANJE SUSTAVA

Odabir gradiva slijedi korak analize odabranog gradiva, primjera iz dobre prakse, zakonskog i normativnog okruženja kako bi se odredili potrebni zahtjevi na sustav. Tehnički izvještaj ISO/TR 15801:2009 govori o važnosti informacijske sigurnosti te o dobroj dokumentiranosti cijelog procesa. Primjeri dobre prakse digitalizacije dokumentacije ministarstva Vlade Alberte[44] i Kongresne knjižnice[45] govore o analizi procesa i planiranju sustava, te o analizi tehničkih zahtjeva, kao što je na primjer dubina bita slike, kompresija, format datoteke, ograničenja u obradi digitalizirane slike. Rezultat planiranja sustava se upisuje u Priručnik digitalizacijskih procedura[46].

[42] Leksikografski zavod Miroslav Krleža. (n.d.). Digitaliizacija. Preuzeto 13. 1. 2018. iz Hrvatska enciklopedija: http://www.enciklopedija.hr/natuknica.aspx?id=68025
[43] Stančić, H. (2009). Digitalizacija. U H. Stančić, Digitalizacija. Zagreb: Zavod za informacijske studije Odsjeka za informacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.
[44] Digitization Standard Process - Government of Alberta, URL: http://www.im.gov.ab.ca/documents/imtopics/Digitization_Standard_Process.pdf (30.9.2016.)
[45] Peterson, A. K. Standards Related to Digital Imaging of Pictorial Materials. Library of Congress, Washington, D.C. 2004., URL: http://www.loc.gov/rr/print/tp/DigitizationStandardsPictorial.pdf (30.9.2016.)
[46] Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf

USPOSTAVLJANJE I ODOBRENJE PROCESA

Prije samog postupka digitalizacije potrebno je uspostaviti proces temeljem analize gradiva i kao rezultat planiranog sustava. U ovom koraku na testnom uzorku koji predstavlja dokumentaciju i koji uključuje i dokumente slabije kvalitete[47] provodi se test propisanih digitalizacijskih procedura iz Priručnika iz prethodnog koraka, te se rezultat zapisuje za kasnije potrebe provjere uspostavljenog procesa. Primjer toga je propisan korak skeniranja u kojem se nalazi zahtjev za skeniranjem u boji i provjerava se jesu li sve digitalizirane slike zaista u boji. Ili, postoji dokumentacija koja je spojena klamericama i spajalicama. Tijekom faze pripreme potrebno je voditi računa o čuvanju dokumentacije te se u ovom koraku provjerava je li dokumentacija spojena klamericama zaista očuvana nakon digitalizacije. Dodatno se u ovoj fazi obavlja test prihvaćanja od strane korisnika[48].

PRIPREMA GRADIVA

Prije skeniranja sva dokumentacija prolazi pregled potrebe konzervacije originala kao i provjeru potpunosti originalne dokumentacije, dokumentaciji se provjerava redoslijed i potpunost[49]. Važno je voditi računa da se ne uništava dokumentacija prilikom digitalizacijskog procesa i zato je važno voditi računa o tome skenira li se knjiga ili druga uvezena dokumentacija ili na primjer osjetljiva dokumentacija koja je bila dugo presavijena kao što su na primjer stari notni zapisi. Oštećenja su moguća u slučajevima pretjeranog rukovanja, inverzija krhkih stranica, ravnanja, abrazivnih površina, prekomjerno osvjetljenje i prekomjerna toplina. Osjetljivi materijali se ne smiju ravnati pomoću stakla niti se smiju okretati licem dolje tijekom skeniranja.

Dodatno na ove zahtjeve primjera digitalizacije materijala Kongresne knjižnice, tehnički izvještaj ISO/TR 15801:2009 navodi kako je potrebno voditi računa o veličini papira, težini papira, na primjer standardni 80 gramski papir koji se koristi prilikom ispisivanja na pisačima ili papir koji se koristi kod višestraničnih obrazaca kojima su druga i treća stranica vrlo tanke i prilikom skeniranja dolazi do prosvjetljavanja informacija koje se nalaze s druge strane.

[47] ISO/TR 15801:2009 Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost. (2009).
[48] Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf
[49] Peterson, A. K. (2004.). Standards Related to Digital Imaging of Pictorial Materials. Preuzeto 30. 9. 2016. iz Library of Congress, Washington, D.C.: http://www.loc.gov/rr/print/tp/DigitizationStandardsPictorial.pdf

U ovom koraku potrebno je voditi računa i o dodacima koji su fizički prisutni na dokumentu kao što je žuta samoljepljiva bilješka (engl. post-it) te načinu pripreme u tom slučaju, na primjer ukoliko se skenira papir s zalijepljenom bilješkom može doći do prekrivanja podataka na originalu. Tehnički izvještaj ukazuje na mogućnost postojanja neprozirne bijele boje, na primjer bijeli korekturni premaz, na dokumentu i potrebe za provođenjem pripreme na način da ovaj podatak o postojanju premaza ostane sačuvan.

Sva dokumentacija treba slijediti izvorni redoslijed te je potrebno osigurati potpunost dokumenta i tijekom faze pripreme, na primjer dokument koji se sastoji od više od jednog lista kao što je izdanje nekog službenog lista tijekom faze pripreme treba zadržati redoslijed numeracije koji ima u originalu. Ukoliko je moguće dokumentacija iste veličine i drugih karakteristika se slaže u pakete kako bi se proces digitalizacije maksimalno ubrzao. Primjer toga je dokumentacija ulaznih računa za određeni mjesec koji se nalazi u registratorima i koji se vađenjem iz registratora pripremaju kao jedan paket.

SKENIRANJE GRADIVA

Pripremljena dokumentacija odlazi na skener. Tijekom faze skeniranja vodi se računa o postavkama skenerskog programa za prihvat slike. Na primjer u skenerskom programu za prihvat slike su podešene opcije slika u crno-bijelom tonu, 300 dpi (engl. dots per inch; točaka po inču op.a.), obostrano skeniranje.

Skeniranje je proces u kojem papir prolazi kroz kompleksan automatiziran sustav koji pomiče papir od ulaza preko sklopa koji se sastoji od senzora i izvora svjetlosti, te dalje do izlaza iz skenera. Iz pripremljenog paketa skener samostalno povlači jedan po jedan papir i pretvara ga u digitaliziranu sliku vidljivu na ekranu računala koji pokreće program za prihvat slike.

Tehnički izvještaj ISO/TR 13028:2010 navodi kako tijekom izrade digitalizirane slike, slike treba imenovati odnosno označiti jedinstvenim identifikatorom te daje preporuke o čemu voditi računa. Jedinstveni naziv datoteke propisan je Priručnikom i zadan unutar programa za prihvat slike.

SLANJE DOKUMENTACIJE U SREDIŠNJI REPOZITORIJ

Postoje dvije mogućnosti nakon skeniranja. Računalo na koje je spojen skener skuplja sve digitalizirane slike. Nakon dovršenog skeniranja pripremljenog paketa provodi se korak

slanja, pomoću pomoćnog programa za slanje, u središnji repozitorij. Druga mogućnost je da program za prihvat slike automatski šalje digitaliziranu sliku u središnji repozitorij nakon što operater zada funkciju autorizacije koja se nalazi unutar programa za prihvat slike. Na primjer, program za prihvat slike Capture Perfect svu dokumentaciju skenira u mapu koja se nalazi na računalu na koje je spojen skener.

Svim slikama se može pristupiti preko datotečnog sustava računala. I za potrebe slanja digitaliziranih slika na daljnju obradu potrebno je odrediti središnji repozitorij, na primjer dediciran centraliziran datotečni poslužitelj (engl. file server) tvrtke koji je određen upravo za prihvat digitaliziranih slika i kojem pristupa program za upravljanjem datoteka.

KONTROLA SKENIRANOG GRADIVA

Skenirano gradivo podložno je kontroli koju najprije obavlja operater tijekom faze skeniranja. Slike nakon prolaska kroz skener se pojavljuju na ekranu. Sve one koje ne izgledaju potpune, a koje uoči operater, ponavljaju se. Međutim, zbog velikih brzina koje skener može postići, kao na primjer deklarirana brzina 130 ppm (engl. pages per minute; stranica u minuti op.a.) kod skenera Canon DR-X10C što je u prosjeku više od dvije slike u sekundi, ne može se realno očekivati da će operater vidjeti sve slike. U stvarnosti je ova brzina nešto manja i ovisi o kvaliteti papira i obično se kod spomenutog skenera kreće oko 100 stranica u minuti, što je još uvijek više od jedne stranice u sekundi i vrlo brzo za ljudsko oko. Moguće je uvesti kontrolu operatera prije slanja dokumentacije na daljnje postupanje.

Druga vrsta kontrole je kontrola koja se obavlja nakon slanja na centralizirani poslužitelj. U fazi kontrole kvalitete tehnički izvještaj ISO/TR 13028:2010 navodi kako se ona obavlja prema dokumentiranoj proceduri i vodi se računa o odstupanjima od propisane procedure, kontrole kvalitete skenera, verifikacije da digitalizirana dokumentacija na izlazu odgovara količini izvorne papirnate dokumentacije na ulazu, kriteriji kontrole kvalitete slika, količini i periodu odabira uzorka na kojem se vrši kontrola, procesu ponavljanja digitalizacije te obuci operatera.

Sva dokumentacija koja ne prođe kontrolu u ovoj fazi se označava za ponavljanje skeniranja i ponovno se skenira i ponovno se provodi kontrola.

Digitalizacijski standard Vlade Alberte navodi kako kontrolu kvalitete trebaju provoditi radnici koji nisu direktno uključeni u proces digitalizacije i indeksiranja[50]. Za minimalni nivo kvalitete potrebno je provjeriti 5-10% ukupno digitaliziranih stranica.

PRIDRUŽIVANJE METAPODATAKA

Pridruživanje metapodataka je korak koji je važan zbog toga što u ovom koraku se opisuje ne samo dokument već i daje kontekst stvorenoj digitaliziranoj slici. Tehnički izvještaj ISO/TR 15801:2009 govori o pridruživanju metapodataka kao o bitnom dijelu procesa zbog toga što ukoliko dođe do gubitka ovih podataka može doći do gubitaka pohranjenih podataka kao što je digitalizirana slika. Primjer toga je podatak o putanji (engl. path) do pozicije digitalizirane slike na centraliziranom datotečnom poslužitelju. Upisivanje metapodataka se može obaviti ručno ili automatski. Automatski se mogu upisati podaci kao što su podaci koji se pročitaju korištenjem funkcije optičkog prepoznavanja znakova (engl. optical character recognition; skr. OCR) ili podaci pročitani pomoću barkod tehnologije. Ručno se upisuju podaci koji se ne mogu pročitati automatski, na primjer ručno upisani podaci kao što je potpis.

Tehnički izvještaj ISO/TR 13028:2010 napominje kako je pridruživanje metapodataka od kritične važnosti za postizanje i održavanje autentičnosti i integriteta digitaliziranih zapisa. U tom smislu ručno upisivanje se treba svesti na najmanju moguću mjeru te maksimalno provoditi automatsko upisivanje. Metapodaci koje je potrebno upisivati dva tipa metapodataka, koji se odnose na proces digitalizacije i specifične za svaku digitaliziranu sliku, te koji se odnose na dokument i proces unutar kojeg se dokument nalazi i sve podatke o operaterima koji su sudjelovali u procesu digitalizacije. Primjer metapodataka su podaci iz klasifikacijske sheme ili podaci i podaci o vrsti softvera za prihvat slike.

Određeni dio metapodataka se može zapisati unutar same slike tijekom procesa prihvata pomoću softvera za prihvat slike. Određeni ili svi metapodaci se mogu upisati u zaseban sustav koji upravlja upisani podacima. U svakom slučaju svi metapodaci trebaju biti povezani s digitaliziranom slikom tijekom cijelog životnog vijeka digitalizirane slike.

[50] Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf

KONTROLA PRIDRUŽENIH METAPODATAKA

Tehnički izvještaj ISO/TR 13028:2010 navodi kako je nakon obavljene faze pridruživanja metapodataka potrebno obaviti kontrolu. Kontrola se obavlja vodeći računa o ispravnosti upisa i ukoliko postoji rječnik odobrenih termina, kao što je na primjer rječnik naziva dokumenata iz klasifikacijske sheme. Kontrolu je moguće obaviti automatizirano na cjelokupnoj dokumentaciji.

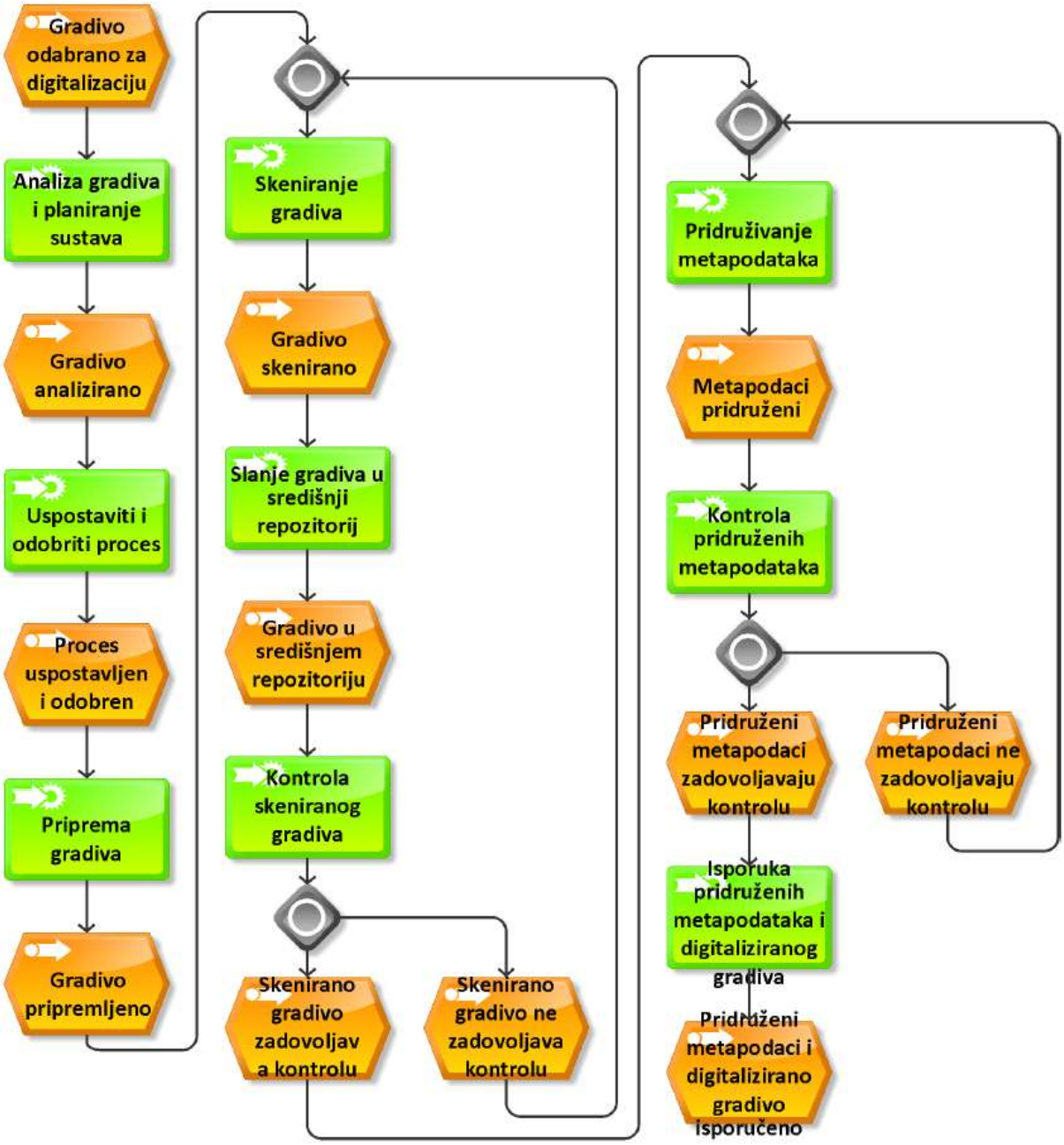
ISPORUKA DIGITALIZIRANOG GRADIVA I PRIDRUŽENIH METAPODATAKA

Nakon obavljene kontrole stvorena i odobrena slika i s njom povezani metapodaci i podaci prenose se mrežom na glavno spremište podataka. Ovo spremište podataka je povezano sa sustavom koji upravlja zapisima i slikama na način da vodi računa o tome da su podaci i slike dostupni tijekom cijelog propisanog vremenskog perioda.

REVIZIJSKI TRAG

Cijeli proces treba biti popraćen dnevnikom ili revizijskim tragom (engl. audit log data), treba biti u cijelosti dokumentiran uključujući i tehničke zahtjeve sustava, slika i podataka[51]. Dijagram 2 pokazuje proces digitalizacije.

[51] ibid.



Dijagram 2. Proces digitalizacije

4.3. Digitalizirana dokumentacija

PRIHVAĆANJE

Norma ISO 15489-1:2001 se odnosi kako na upravljanje zapisima u fizičkom formatu tako i na upravljanje zapisima u elektroničkom formatu, te u ovom slučaju odnosi se i na digitaliziranu građu. Prvi proces koji digitalizirano gradivo treba proći je prihvaćanje digitaliziranog dokumenta, tijekom čega se obavlja njegova registracija i klasifikacija. U tom trenutku Digitalizacijski standard Vlade Alberte navodi otvaranje dnevnika zapisa ili revizijskog traga (engl. logging), odnosno vođenje dnevnika po svim fazama procesa kako bi se mogao pratiti trag prolaska dokumenta[52].

POHRANA

Digitalizirani dokument je potrebno negdje pohraniti radi dugoročnog čuvanja, na primjer u datotečni sustav kojem pristupa sustav za upravljanje digitaliziranim dokumentima ili u SQL bazu podataka koja pohranjuje metapodatke o digitaliziranoj slici.

PRIČUVNA KOPIJA

ISO/TR 15489-2 napominje da je u istom trenutku potrebno izraditi i pričuvnu kopiju kako bi se spriječio gubitak digitaliziranih dokumenata zbog pogreški sustava. S druge strane, ISO/TR 15801:2009 traži izradu barem dvije pričuvne kopije, te svih ostalih podataka, za slučaj „pada“ sustava. Na primjer, u slučaju elementarne nepogode kao što je požar i nastanak potpunog uništenja cijelog hardverskog sustava na kojem se nalaze podaci, slike i sustav koji upravlja s njima, mora postojati pričuvna kopija iz koje se može rekonstruirati cijeli sustav i nastaviti s radom.

PRISTUP

Glavni razlog dugoročnog očuvanja je mogućnost pristupa građi. Norma ISO 15489 ovaj korak prepoznaje kao korištenje, praćenje i stavljanje digitaliziranog dokumenta na

[52] ibid.

raspolaganje. Tada se provodi provjera dostupnosti zapisa ovisno o dodijeljenim ovlastima. Primjer toga su sklopljeni ugovori koje mogu pregledavati samo radnici koji upravljaju tvrtkom dok je onemogućen pregled radnicima na operativnim poslovima i zadacima. Tijekom stavljanja zapisa na raspolaganje potrebno je voditi evidenciju tko pristupa i kojem gradivu pristupa.

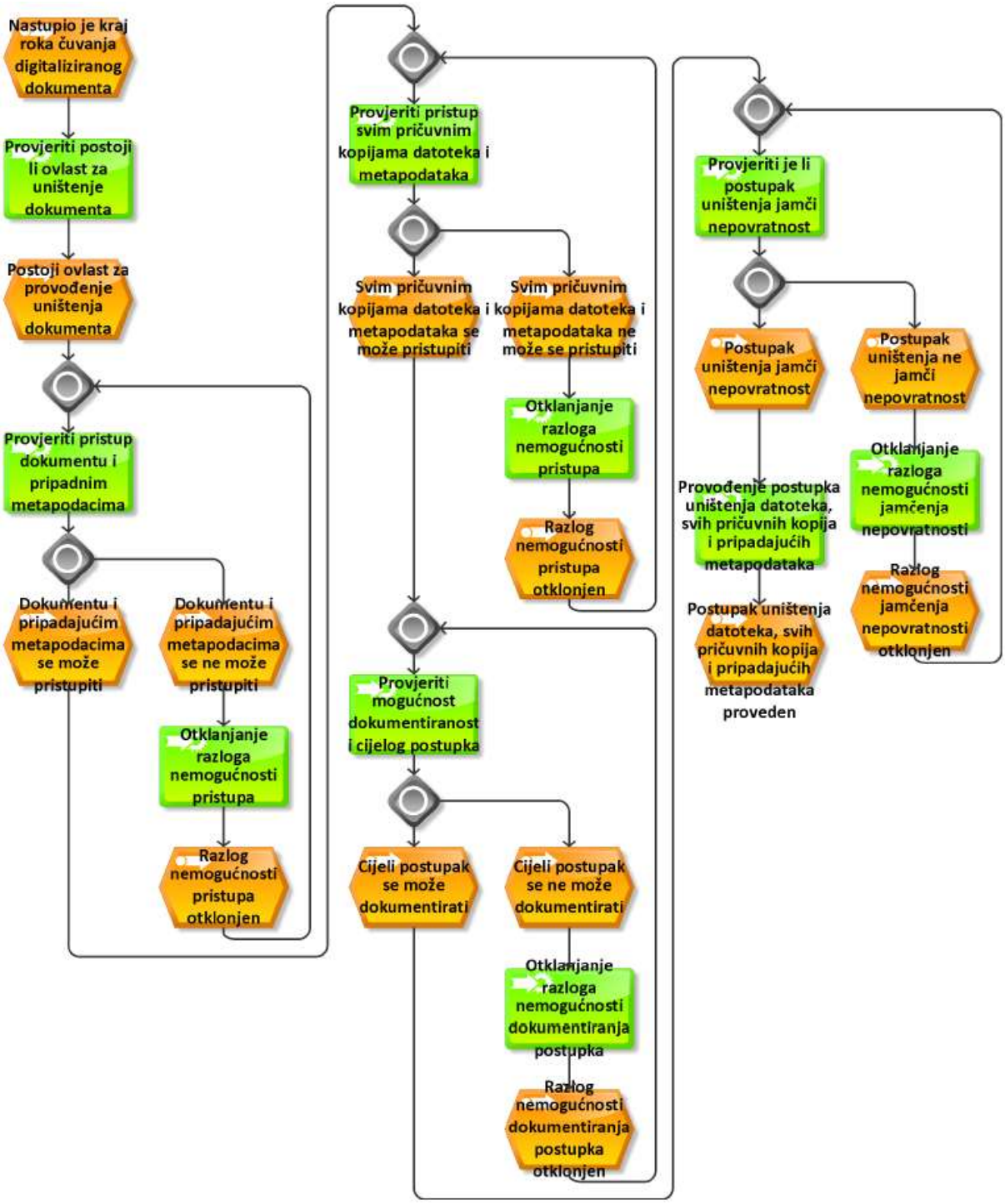
MIGRACIJA

Brzina promjene današnje tehnologije je toliko velika da je nužno očekivati kako će nastupiti trenutak promjene unutar određenog roka čuvanja digitaliziranog gradiva i pripadajućih metapodataka. Tehnički izvještaj ISO/TR 15801:2009 prepoznaje ovu činjenicu te predlaže planiranje migracije koja uključuje mogućnost promjene medija kao i promjene računalnog hardvera i softvera. Zbog toga je dobro imati na umu da način provedbe migracije treba zadržati autentičnost digitalizirane građe, metapodataka i pripadajućih revizijskih tragova o proteklim transakcijama i akcijama pristupa i promjene građe i podataka.

UNIŠTENJE

Zadnji korak u procesu upravljanja digitaliziranom dokumentacijom je njeno uništenje. Prilikom provedbe uništenja potrebno je provjeriti je li nastupio kraj roka čuvanja digitaliziranog dokumenta, kao i postojanje ovlasti da se provede uništenje određenog digitaliziranog gradiva. Način uništenja mora se provesti tako da se "[…] jamči nepovratnost"[53]. Prilikom uništenja potrebno je voditi računa i o svim pričuvnim kopijama i metapodacima te ispravno provesti njihovo uništenje. Tehnički izvještaj ISO/TR 15801:2009 upozorava da uništenje treba obaviti vodeći računa o osjetljivosti podataka koji se uništavaju, na primjer osjetljivih podataka kao što su osobni podaci o radnicima. Procedure uništenja trebaju, prema tehničkom izvještaju, biti provedene na način da se dokumentira cjelokupni postupak. Dijagram 3 pokazuje proces uništenja dokumentacije.

[53] ISO/TR 15489-2 (n. dj.), točka 4.3.9.3 Fizičko uništenje



Dijagram 3. Proces uništenja

4.4. Zaključak

Životni ciklus papirnate dokumentacije prepoznaje više koraka tijekom kojih postoji određena mogućnost gubitka autentičnosti zaprimljene građe. Prilikom zaprimanja dokumentacije ona se označava jedinstvenom oznakom i nadalje se vodi u sređenom obliku uz obavezno praćenje kretanja dokumenta tijekom cijelog životnog ciklusa dok ne nastupi rok kada je moguće dokument uništiti. Prema sadašnjem Zakonu o arhivskom gradivu i arhivima fizički dokument je moguće uništiti tek kada nastupi kraj roka čuvanja. Prema prijedlogu novog Zakona fizički dokument će se moći uništiti ukoliko se napravi pretvorba u drugi oblik i pribavljanjem suglasnosti Hrvatskog arhivskog vijeća. Ovdje se predlaže, prije uništavanja fizičkog dokumenta, pribaviti dovoljnu količinu dokaza kojima se garantira da je pretvorba u drugi oblik učinjena poštujući zahtjeve za izradom autentičnog dokumenta.

Način pretvorbe u drugi oblik koji se predlaže je pretvorba digitalizacijom poštujući, u ovoj disertaciji razvijen, model procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije. Prije same digitalizacije preporuča se planiranje sustava, određivanje zadovoljavajućih tehničkih zahtjeva i mogućih ograničenja, te izrada Priručnika digitalizacijskih procedura. Osim što je potrebno voditi računa da se tijekom digitalizacije ne uništi papir i da se tijekom digitalizacije ne izgube potrebni detalji bez kojih nije moguće govoriti o autentičnosti, također cijeli proces treba prethodno biti odobren. Odobravanje procesa se može učiniti jedino ukoliko se izradi dovoljna količina podataka odnosno provjera provedenih na testnom uzorku, između koji se nalazi i dokumentiranost odabranog testnog uzorka. Nakon skeniranja slijedi slanje digitalizirane dokumentacije u središnji repozitorij što je omogućeno na više načina koji sami po sebi ne zadovoljavaju zahtjev nepromjenjivosti, već je to potrebno osigurati korištenjem potrebnih alata. Pokazivanje autentičnosti ovisiti će o provedenim kontrolama digitaliziranog gradiva, zbog toga je važno napraviti adekvatnu kontrolu te zapisati rezultat kojem se u kasnijim zahtjevima može pristupiti te uz dovoljnu razinu sigurnosti zaključiti je li proces obavljen uredno ili je došlo do nedozvoljene manipulacije. Digitalizirani dokument obavezno prati pridruživanje kritične količine metapodataka kojima se postiže i održava autentičnost i integritet digitaliziranih zapisa, koji se trebaju provjeriti kako bi zadovoljili zahtjev potpunosti i ispravnosti upisa.

Stvoreni digitalizirani dokument se dalje prihvaća u sustav kojim se garantira autentičnost tijekom cjelokupnog roka čuvanja i dodatno se izrađuje pričuvna kopija za slučaj havarije sustava, a radi ponovnog pokretanja sustava. Pristup podacima treba biti nadziran i vođen na način da se jasno zna koje ovlasti kome pripadaju. Brzi razvoj tehnologije dovodi do

situacije kada je potrebno migrirati dokumentaciju na novu tehnologiju, i to treba obaviti zadržavajući autentičnost digitalizirane dokumentacije i njenih pripadajućih metapodataka. Uništenje dokumentacije nastupa nakon prolaska rokova čuvanja. Ovaj korak ne bi bio važan kada ne bi postojao zahtjev autentičnosti kojim se traži da dokumentu budu pripojeni svi pripadajući dodatni dokumenti. Zbog toga je potrebno voditi računa da se cijeli postupak dokumentira.

5. ZAKONSKI OKVIR

U svrhu boljeg razumijevanja uvjeta koje autentični digitalizirani dokument treba zadovoljiti u nastavku se obrađuje nacionalno zakonodavstvo, pripadajući pravilnici i uredbe koji se odnose na papirnu dokumentaciju i digitalnu dokumentaciju. Digitalizacijski proces se može obaviti na različitim vrstama dokumentacije i dobro je prepoznati vrste gradiva koji se mogu pojaviti u arhivima, tehničke zahtjeve za njihovu obradu i čuvanje, podatke i evidencije koji opisuju ili se odnose na to gradivo u svom životnom vijeku, jer će biti važni kasnije za dokazivanje autentičnosti digitaliziranog dokumenta, tehničke zahtjeve za nepromjenjivost digitaliziranog dokumenta, kao što je primjerice korištenje elektroničkih potpisa, te što se trenutno prema pravilnicima smije pretvoriti u drugi oblik.

5.1. Zakon o arhivskom gradivu i arhivima

Zakon o arhivskom gradivu i arhivima iz 1997. godine uređuje zaštitu i uvjete korištenja, čuvanja, uporabe i obrade arhivskoga gradiva, javnu arhivsku službu, te nadležnosti i zadaće arhiva.

Definicije u Članku 3. Zakona o arhivskom gradivu i arhivima:

- **Arhivsko gradivo** su „zapisi ili dokumenti koji su nastali djelovanjem pravnih ili fizičkih osoba u obavljanju njihove djelatnosti, a od trajnog su značenja za kulturu, povijest i druge znanosti, bez obzira na mjesto i vrijeme njihova nastanka, neovisno o obliku i tvarnom nosaču na kojem su sačuvani.“[54]
- **Zapisi ili dokumenti** „su spisi, isprave, pomoćne uredske i poslovne knjige, kartoteke, karte, nacrti, crteži, plakati, tiskovnice, slikopisi, pokretne slike (filmovi i videozapisi), zvučni zapisi, mikrooblici, strojnočitljivi zapisi, datoteke, uključujući i programe i pomagala za njihovo korištenje.“[55]
- **Registraturno gradivo** je „cjelina zapisa ili dokumenata nastalih ili primljenih djelovanjem i radom pojedine pravne ili fizičke osobe.“[56]
- **Imatelji arhivskog i registraturnog gradiva** su „pravne i fizičke osobe koje su vlasnici ili posjednici gradiva, koje njime upravljaju ili ga drže s bilo kojega naslova.“[57]

[54] ZAGA, Članak 3.
[55] ibid.
[56] ibid.
[57] ibid.

- **Stvaratelji arhivskog i registraturnog gradiva** su „pravne ili fizičke osobe čijim djelovanjem i radom ono nastaje.“[58]
- **Arhivi** su „ustanove za čuvanje, zaštitu, obradu i korištenje arhivskoga gradiva koje mogu biti javne i privatne.“[59]
- **Pismohrana** je „ustrojstvena jedinica u kojoj se odlaže i čuva arhivsko, odnosno registraturno gradivo do predaje nadležnom arhivu.“[60]
- **Odabiranje arhivskog gradiva** je „postupak kojim se iz registraturnog gradiva na temelju utvrđenih propisa odabire arhivsko gradivo.“[61]
- **Arhivski fond** - „arhivsko gradivo nastalo djelovanjem i radom pojedine pravne ili fizičke osobe čini cjelinu (arhivski fond) i u načelu se ne može dijeliti [...]“[62], osim kada dolazi do „[...] promjene unutarnjeg ustrojstva stvaratelja, prenošenja dijela ili svih njegovih poslova na drugog stvaratelja, zbog preuzimanja dijela ili svih poslova drugog stvaratelja [...]“[63] i pri tome je potrebno primiti odluku nadležnoga državnog arhiva kojom se utvrđuje imatelj svakog dijela ovako podijeljenoga ili spojenoga gradiva.
- **Javno arhivsko ili registraturno gradivo** je „gradivo nastalo djelovanjem i radom tijela državne vlasti, tijela jedinica lokalne samouprave i uprave, javnih ustanova i javnih poduzeća, trgovačkih društava koja su nastala iz bivših javnih poduzeća, javnih bilježnika i drugih osoba koje obavljaju javnu službu ili imaju javne ovlasti (dalje: stvaratelji javnoga arhivskog i registraturnog gradiva). [...] Nadležni državni arhiv utvrđuje popis stvaratelja i imatelja javnoga arhivskog i registraturnoga gradiva na području svoga djelovanja.“[64]
- **Privatno arhivsko gradivo** je „arhivsko gradivo nastalo djelovanjem privatnih pravnih i fizičkih osoba, ukoliko nije nastalo u obavljanju javnih ovlasti ili u obavljanju javne službe i ako nije u državnom vlasništvu.“[65]

Članak 3. definira registraturno gradivo „[...] arhivskim gradivom u nastajanju [...]“[66], što znači da se na registraturno gradivo primjenjuje ovaj zakon i ostali propisi koji se odnose na arhivsko gradivo.

[58] ibid.
[59] ibid.
[60] ibid.
[61] ibid.
[62] ZAGA, Članak 4.
[63] ibid.
[64] ZAGA, Članak 5.
[65] ZAGA, Članak 29.

Zakon o arhivskom gradivu i arhivima nalaže svim stvarateljima gradiva od važnosti za Republiku Hrvatsku, prema Članku 7, srediti gradivo, čuvati i osigurati od oštećenja, dostavljati popise gradiva i sve promijene u vezi s njim, postupati s gradivom prema uputama nadležnog državnog arhiva za zaštitu i postupanje s gradivom, odabirati arhivsko gradivo iz registraturnog, te „[..] omogućiti ovlaštenim djelatnicima nadležnoga državnog arhiva obavljanje stručnog nadzora nad čuvanjem njihova gradiva“[67]. Prema Članku 8. za provođenje svih radnji nad gradivom odgovoran je za to određeni djelatnik koji upravlja radom pismohrane. Postupak odabira gradiva provodi se prema Pravilniku o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva, propisan Člankom 12. Uništenje gradiva je propisano Člankom 13. koje se provodi na način da se poduzimaju mjere zaštite tajnosti podataka. Predaja arhivskog gradiva propisana je preko Članka 15. koji kaže kako „Stvaratelji i imatelji javnoga arhivskog i registraturnog gradiva dužni su ga predati nadležnom arhivu u izvorniku, sređeno, označeno, popisano, u zaokruženim cjelinama te tehnički opremljeno, u skladu s Pravilnikom o predaji arhivskoga gradiva arhivima.“[68]. Korištenje javnog arhivskog gradiva propisuje se Pravilnikom o korištenju arhivskog gradiva putem Članka 26., te putem Članka 23. propisuje se način davanja gradiva na korištenje i to putem snimaka, osim u specijalnim slučajevima to može biti izvorno arhivsko gradivo na primjer kada to zahtjeva znanstvena metoda rada ili za izložbe ukoliko su osigurani uvjeti za njegovu zaštitu i sigurnost i uz obvezu da se original zaštitno snimi prije predaje.

Osim popisa stvaratelja i imatelja javnog arhivskog gradiva, Članak 30. propisuje Hrvatskom državnom arhivu izradu popisa stvaratelja i imatelja privatnog arhivskog gradiva za koje utvrdi da je od interesa za državu. Članak 31. propisuju podatke koje upisnik javnog i privatnog arhivskog gradiva mora sadržavati:

1. naziv tvrtke ili ime i prezime vlasnika,
2. sjedište tvrtke ili prebivalište vlasnika,
3. ime i prezime odgovorne osobe,
4. prebivalište odgovorne osobe,
5. osnovni podaci o stvaratelju arhivskoga gradiva,
6. kratki opis sadržaja,
7. vremenski raspon gradiva,
8. količina gradiva,

[66] ZAGA, Članak 3.
[67] ZAGA, Članak 7.
[68] ZAGA, Članak 15.

9. datum upisa,
10. broj rješenja o proglašenju gradiva dijelom spomeničke baštine,
11. nadnevak rješenja o proglašenju gradiva dijelom spomeničke baštine.

Imatelji privatnoga arhivskog gradiva Člankom 33. obavezni su: obavještavati nadležni Državni arhiv o posjedovanju gradiva, čuvati gradivo i poduzimati mjere potrebne za njegovo sigurno čuvanje i zaštitu, srediti gradivo i izraditi popis, te dopustiti ovlaštenoj osobi nadležnoga arhiva da pregleda gradivo i po potrebi provede sigurnosno snimanje.

Prema Članku 47. arhivi su obvezni voditi, prema svojem pravilniku, slijedeće evidencije:

1. knjigu primljenoga arhivskog gradiva,
2. opći našastar arhivskog gradiva i našastare za pojedine fondove i zbirke,
3. knjigu pohranjenoga arhivskog gradiva,
4. knjigu snimljenoga arhivskog gradiva,
5. knjigu restauriranoga i konzerviranoga arhivskoga gradiva,
6. evidenciju o stvarateljima i imateljima arhivskoga i registraturnoga gradiva na svom području,
7. evidenciju o korištenju arhivskoga gradiva.

Arhivi imaju ravnatelja, stručno vijeće (raspravlja o svim stručnim pitanjima rada arhiva, daje ravnatelju mišljenje i prijedloge glede organizacije rada i uvjeta za razvitak arhivske djelatnosti, te obavlja i druge stručne poslove sukladno sa statutom arhiva), te upravni nadzor. Savjetodavno tijelo ministra kulture je Hrvatsko arhivsko vijeće sa svojim članovima i odgovornostima utvrđenim ovim zakonom.

5.1.1. Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva

Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva uređuje uvjete čuvanja i zaštite javnog i privatnog arhivskog gradiva koje je određeno kao kulturno dobro. Člankom 3. arhivsko gradivo organizira se u dokumentacijske zbirke ili cjeline po principu nastanka djelovanjem istoga stvaratelja, ili nastankom kao zbirka dokumentacije određene vrste ili namjene ili dokumentacija koja je nastala obavljanjem određene djelatnosti. U pravilniku arhivska jedinica označava dokument, predmet, dosje, svezak.

Članak 5. zahtjeva izradu popisa svih dokumentacijskih zbirki ili cjelina u kojem se upisuje:

1. naziv,

2. stvaratelj,
3. vrijeme nastanka gradiva,
4. količina gradiva,
5. medij,
6. vrsta zapisa,
7. opis sadržaja,
8. popis manjih skupina na koje je dokumentacijska zbirka ili cjelina podijeljena.

Dodatno na popis dokumentacijskih zbirki imatelji, prema Članku 6., vode podatke koji opisuju dokumentacijsku cjelinu te podatke koji opisuju arhivsku jedinicu u dokumentacijskoj cjelini.

Podaci koji opisuju dokumentacijsku cjelinu[69]:

1. redni broj,
2. oznaka (klasifikacijska oznaka, arhivski ili drugi znak koji jednoznačno identificira cjelinu),
3. naziv,
4. sadržaj (opis dokumentacije u cjelini, predmeta ili djelatnosti na koji se odnosi),
5. medij i vrsta zapisa (podaci o vrsti medija i obliku zapisa dokumentacije u cjelini),
6. količina (količina gradiva u cjelini iskazana u broju jedinica – dokumenata, predmeta, dosjea i dr. – koje sadrži, te dužnim metrima, veličini zapisa ili drugoj odgovarajućoj mjernoj jedinici),
7. tehničke jedinice (oznake ili raspon oznaka pripadajućih tehničkih jedinica – kutija, registratora i dr.),
8. vrijeme nastanka (godina ili raspon godina nastanka gradiva),
9. napomene.

Podaci koji opisuju arhivsku jedinicu[70]:

1. redni broj,
2. oznaka,
3. naziv,
4. vrsta,
5. vrijeme nastanka,
6. rok čuvanja,

[69] Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan ARHIVA. (19. 5. 2004.). (NN 63/04)., Članak 6.
[70] ibid.

7. tehničke jedinice.

Pravilnik, Člankom 7., propisuje da se ovi popisi mogu voditi bilo papirnato bilo kao baza podatka, ali je u oba slučaja potrebno „[…] zaštiti popis od neovlaštenog pristupa, gubitka, uništenja i oštećenja.“[71] Kada se popis vodi u elektroničkom obliku imatelj treba osigurati „[…] podatke od neovlaštenog upisivanja, mijenjanja i brisanja te jednu kopiju čuvati na sigurnom mjestu“[72].

Arhivsko gradivo se čuva u „[…] sređenom stanju, tehnički opremljeno i oblikovano u arhivske jedinice.“[73] Članak 8. dalje određuje upisivanje slijedećih podataka na zaštitnom omotu:

1. redni broj arhivske jedinice u popisu arhivskog gradiva,
2. oznaka arhivske jedinice,
3. naziv arhivske jedinice,
4. naziv dokumentacijske zbirke,
5. naziv stvaratelja.

Dodatno se na unutarnju stranu omota upisuju podaci o dokumentima u arhivskoj jedinici kao i o dokumentima koji nedostaju.

Ovako uređene i složene arhivske jedinice odlažu se u tehničke jedinice (mapa, fascikl, arhivska kutija i dr.) na kojima se upisuje[74]:

1. naziv dokumentacijske zbirke ili cjeline,
2. naziv stvaratelja,
3. redni broj tehničke jedinice,
4. godina ili raspon godina nastanka gradiva i
5. oznake ili raspon oznaka arhivskih jedinica koje se nalaze u tehničkoj jedinici.

Moguće je arhivsko gradivo u elektroničkom obliku prema Članku 10. pohraniti u elektroničkom obliku na način da se podaci izdvoje u sustav koji „[…] onemogućuje brisanje, mijenjanje i dodavanje podataka“[75], pri čemu je dopušteno da to bude isti sustav ali s navedenim funkcionalnostima. Isti članak propisuje pohranu u najmanje dvije kopije tako da je jedna kopija izvan sustava koji se koristi za pregled (pristup, pretraživanje i prikazivanje) gradiva a druga u tom sustavu. Prije izdvajanja gradiva potrebno je u pismenom obliku opisati format i strukturu zapisa, način njegovog čuvanja i zaštitu od neovlaštenog pristupa ili

[71] ibid., Članak 7.
[72] ibid., Članak 7.
[73] ibid., Članak 8.
[74] ibid., Članak 9.
[75] ibid., Članak 10.

mijenjanja podatka, način provođenja izlučivanja gradiva, način predaje nadležnom arhivu i obavezna je provjera čitljivosti i cjelovitosti.

Sve navedene poslove koji se tiču zaštite i obrade arhivskog gradiva Člankom 16. se omogućava osobama koje su stručno osposobljene za te poslove (stručni radnici).

Sva pitanja organizacije, obrade, odlaganja i čuvanja, odabiranja i izlučivanja arhivskog gradiva imatelji uređuju svojim pravilnikom o zaštiti i obradi arhivskoga gradiva koji, prema Članku 17., ovjerava nadležni arhiv. Pravilnik, po istom članku, obavezno sadrži:

1. način vođenja uredskog poslovanja,
2. način izrade, obrade i rukovanja predmetima i dokumentacijom u obradi, način i rokovi interne primopredaje,
3. način vođenja uredskih evidencija i drugih evidencija o gradivu,
4. tehničko opremanje, označavanje i odlaganje gradiva,
5. mjesto, uvjeti i način čuvanja arhivskog gradiva,
6. način korištenja arhivskoga gradiva,
7. rokovi i postupak vrednovanja i izlučivanja gradiva,
8. postupak uništavanja izlučenog gradiva i predaje gradiva nadležnom arhivu,
9. zaduženja i odgovornosti u rukovanju, obradi i zaštiti gradiva.

5.1.2. Pravilnik o uvjetima smještaja, opreme, zaštite i obrade arhivskog gradiva, broju i strukturi stručnog osoblja arhiva

Pravilnik o uvjetima smještaja, opreme, zaštite i obrade arhivskog gradiva, broju i strukturi stručnog osoblja arhiva navodi kako poslove vrednovanja, preuzimanja, zaštite, obrade i korištenja arhivskog gradiva, te „[…] druge stručne poslove u arhivima obavljaju osobe koje su stručno osposobljene za te poslove.“[76] Samo iznimno određene jednostavnije poslove mogu obavljati osobe koje nisu stručno osposobljene ali kada ih obavljaju pod nadzorom i uputama stručno osposobljenih osoba. U tom slučaju potrebno je pismeno opisati poslove koji će se obavljati, „[…] u kojem razdoblju i koja će stručno osposobljena osoba obavljati nadzor.“[77]

Nadalje Članak 17. Pravilnika propisuje broj i poslove stručnjaka u Državnom arhivu:

[76] Pravilnik o uvjetima smještaja, opreme, zaštite i obrade arhivskog gradiva, broju i strukturi stručnog osoblja arhiva. (11. 5. 2004.). (NN 65/04)., Članak 16.
[77] ibid.

- dva stručna djelatnika, od kojih barem jedan visoke stručne spreme, za obavljanje poslova evidentiranja i zaštite gradiva izvan arhiva i nadzor nad stvarateljima i imateljima u nadležnosti arhiva,
- jednog stručnog djelatnika visoke stručne spreme za obavljanje poslova sređivanja i obrade gradiva u arhivu, na svakih tisuću dužnih metara gradiva u arhivu, odnosno odgovarajuću količinu gradiva u elektroničkom ili drugim oblicima,
- jednog stručnog djelatnika za obavljanje poslova na zaštiti gradiva u arhivu, na svakih dvije tisuće dužnih metara gradiva u arhivu, jednog stručnog djelatnika za zaštitu elektroničkog ili audiovizualnog gradiva, ako arhiv posjeduje takvo gradivo,
- jednog stručnog djelatnika visoke stručne spreme za rad s korisnicima, te jednog stručnog djelatnika za dežurstvo u čitaonici,
- jednog stručnog djelatnika, odnosno djelatnika informatičke struke za obavljanje poslova vezanih uz upravljanje informatičkom infrastrukturom i informatičku podršku radnom procesu.

Ukoliko se radi o specijaliziranim i privatnim arhivima količina stručnjaka se mijenja[78]:

- najmanje jedan stručni djelatnik visoke stručne spreme, za obavljanje poslova na preuzimanju gradiva i vođenje akvizicijske politike arhiva,
- najmanje jedan stručni djelatnik visoke stručne spreme za obavljanje poslova sređivanja i obrade gradiva u arhivu, na svakih tisuću dužnih metara gradiva u arhivu, odnosno odgovarajuću količinu gradiva u elektroničkom ili drugim oblicima,
- najmanje jedan stručni djelatnik za obavljanje poslova na zaštiti gradiva u arhivu, na svakih dvije tisuće dužnih metara gradiva u arhivu, jednog stručnog djelatnika za zaštitu elektroničkog ili audiovizualnog gradiva, ako arhiv posjeduje takvo gradivo,
- najmanje jedan stručni djelatnik za rad s korisnicima i dežurstvo u čitaonici.

Općenito, „[…] arhivi koji samostalno obavljaju zaštitno snimanje gradiva trebaju imati barem dva stručna djelatnika za obavljanje odgovarajućih poslova.“[79] Ukoliko arhivi ove poslove prepuštaju drugoj ustanovi ili organizaciji trebaju imati barem jednog odgovarajuće osposobljenog stručnog djelatnika koji će voditi poslove koordinacije između arhiva i druge ustanove.

[78] ibid., Članak 19.
[79] ibid., Članak 20.

5.1.3. Pravilnik o korištenju arhivskoga gradiva

Prema Pravilniku o korištenju arhivskog gradiva, Članak 19., na korištenje se daju snimci arhivskoga gradiva što znači da se ne daje izvorno filmsko i slikopisno gradivo, kao ni sigurnosni snimci, a za potrebe službene svrhe daju se ovjerovljene preslike. Moguće je iznimno dati na korištenje izvorno arhivsko gradivo kada to zahtjeva znanstvena metoda rada i kada ne postoje snimci gradiva.

Pravilnik propisuje izradu mikrosnimaka svog starijeg gradiva do kraja 18. st., kao i svog gradiva za koje postoji mogućnost oštećivanja prilikom umnažanja (knjige, grafike, planovi, zemljovidi, fotografije i slično). Snimci koji se daju na korištenje se rade iz ovih zaštitnih mikrosnimaka.[80]

Izrada ovjerovljenih prijepisa i preslika arhivskog gradiva propisana je Člankom 40. koje je omogućeno potrebama državnih tijela i potrebama ostvarivanja prava građana i pravnih osoba nakon podnašanja zahtjeva u pisanom obliku uz navođenje svrhe. Pravilnik ističe Člankom 41. kako se ovjerom prijepisa ili preslike potvrđuje istovjetnost s izvornikom, ali ne i istinitost podataka u izvorniku.

5.1.4. Pravilnik o predaji arhivskoga gradiva arhivima

Pravilnik o predaji arhivskog gradiva arhivima definira:

- **Izvornik** "je svaki prvotni zapis bez obzira na podlogu i vrstu zapisa, a koji ima oznake pravne valjanosti."[81]
- **Označeno gradivo** – arhivsko gradivo u tehničkim jedinicama na kojima su slijedeći podaci[82]:
    - naziv javnopravne osobe,
    - naziv organizacijske jedinice čijim je djelovanjem nastalo arhivsko gradivo (ako postoji),
    - redni broj tehničke jedinice u popisu,
    - oznake jedinica gradiva/sadržaj,
    - vremenski raspon gradiva u tehničkoj jedinici.

[80] ibid., Članak 29.
[81] Pravilnik o predaji arhivskoga gradiva arhivima. (12. 7. 2002.). (NN br. 90/02)., Članak 6.
[82] ibid., Članak 11.

Elektroničke zapise se prema Članku 6. predaje u dogovorenom obliku i nosaču "[…] zajedno s dokumentacijom i podacima koji su potrebni za čitanje i razumijevanje zapisa, kompatibilnim s postojećom tehnologijom i takvi koji čuvaju sigurnost, autentičnost i vjerodostojnost."[83] Popis zahtjeva kojima se čuva sigurnost, autentičnost i vjerodostojnost zapisa nadležni arhiv šalje predavatelju.

Člankom 8. Pravilnika popisano gradivo sadrži slijedeće podatke:

1. naziv stvaratelja gradiva,
2. vrijeme nastanka gradiva obuhvaćenog popisom,
3. ukupna količina gradiva,
4. ime i prezime osobe koja je izradila popis,
5. datum popisa.

Pri tome za svaku jedinicu s popisa postoje minimalno slijedeći podaci:

1. redni broj,
2. naziv,
3. sadržaj,
4. vrijeme nastanka,
5. količina.

Zapisnik koji prati predaju gradiva mora sadržavati slijedeće podatke:

1. datum i mjesto primopredaje,
2. naziv javnopravne osobe koja predaje arhivsko gradivo, te ime i prezime odgovorne osobe,
3. naziv arhiva koji preuzima arhivsko gradivo te ime i prezime odgovorne osobe,
4. imena i prezimena osoba koje su obavile primopredaju,
5. zakonsku osnovu primopredaje,
6. naziv, sjedište i vrijeme djelovanja stvaratelja gradiva koje se predaje (ako se predaje gradivo nastalo djelovanjem više stvaratelja navode se podatci za svakoga stvaratelja pojedinačno),
7. naziv odnosno sadržaj arhivskoga gradiva,
8. vrijeme nastanka arhivskoga gradiva koje se predaje,
9. svežnjeva, knjiga, kolutova i dr.), u dužnim metrima ili drugoj odgovarajućoj mjernoj jedinici,

[83] ibid., Članak 6.

10. napomenu o sačuvanosti i cjelovitosti gradiva i objašnjenje što ga o tome daje predavatelj,
11. napomenu o uvjetima korištenja gradiva.

Uz zapisnik se prilaže[84]:

1. popis preuzetoga arhivskoga gradiva,
2. popis arhivskog gradiva koje je privremeno ostalo kod imatelja i rok do kojega će biti predano arhivu.

Ukoliko se preuzima privatno arhivsko gradivo, preuzimanje se provodi kako je propisano Člankom 17., odnosno postoji pisane isprave koja sadrži prava i obveze stranaka te slijedeće podatke:

- navod o vrsti pisane isprave (ugovora),
- naziv, odnosno ime i prezime, matični broj pravne osobe i adrese ugovornih strana (za pravnu osobu uz naziv se navodi i ime odgovorne osobe ili opunomoćenog predstavnika),
- predmet ugovora (naziv odnosno naznaka sadržaja gradiva, vrsta, količina i vrijeme nastanka gradiva),
- navod o vlasništvu nad arhivskim gradivom koje je predmet ugovora,
- navod o autorskim pravima ili drugim pravima i ograničenjima koja se odnose na korištenje i raspolaganje gradivom koje je predmet ugovora,
- naziv i sjedište arhiva u kojemu će se gradivo čuvati,
- navod o uvjetima i rokovima dostupnosti i korištenja gradiva,
- međusobne obveze ugovornih strana te prema trećim stranama,
- datum i potpis,
- popis preuzetoga arhivskog gradiva u kojem se nalazi:
    - sadržaj,
    - razdoblje nastanka,
    - količina gradiva,
- ograničenja (ukoliko postoje) o raspolaganju i korištenju gradiva,
- datum obnove (ukoliko postoji),
- podaci o produljenju ugovora (ukoliko je primjenjivo).

[84] ibid., Članak 12.

5.1.5. Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva

Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva Člankom 2. navodi nekoliko važnih definicija[85]:

- **Izlučivanje** je postupak kojim se iz neke cjeline gradiva izdvajaju jedinice čiji je utvrđeni rok čuvanja istekao.
- **Izvornik** je svaki prvotni zapis, bez obzira na podlogu i vrstu zapisa, koji ima značajke vjerodostojnosti i pouzdanosti.
- **Kategorizacija** je postupak kojim se stvaratelji gradiva razvrstavaju u skupine ovisno o značenju cjeline gradiva nastalog njihovim djelovanjem.
- **Popis s rokovima čuvanja** je popis jedinica neke cjeline gradiva ili funkcija obavljanjem kojih je gradivo nastalo, s označenim rokom čuvanja za svaku jedinicu popisa i postupkom s jedinicom gradiva po isteku roka čuvanja.
- **Vrednovanje** je postupak kojim se procjenjuje vrijednost zapisa i utvrđuje rok do kojega će se čuvati određena vrsta gradiva ili jedinice gradiva, te se određuje postupak sa svakom vrstom odnosno jedinicom gradiva po isteku roka čuvanja.

Pravilnik dalje propisuje kategorizaciju stvaratelja arhivskog gradiva, vrednovanja registraturnog gradiva, popis gradiva s rokovima čuvanja te postupak odabiranja, izlučivanja i uništavanja gradiva. Postupak odabiranja, izlučivanja i uništavanja gradiva propisano je člancima od 12. do 17. Prvi i drugi katergornik prvo sastavljaju prijedlog gradiva koje će biti izlučeno. Prijedlog se šalje na mišljenje i odobrenje nadležnog arhiva, te nakon primljenog pozitivnog mišljenja može se pristupiti izlučivanju.

Postupak izlučivanja provodi povjerenstvo koje u prvom koraku sastavlja prijedlog u kojem navodi slijedeće podatke:

- opći podatci o arhivskome fondu (naziv, vrijeme nastanka gradiva),
- podatak o ranijim izlučivanjima,
- podatci o cjelovitosti sačuvanoga gradiva,
- prijedlog kriterija za izlučivanje s obrazloženjem,
- popis gradiva ili vrsta (skupina) zapisa koji se predlažu za izlučivanje.

Nakon sastavljenog prijedloga ravnatelj arhiva donosi odluku o izlučivanju u pismenom obliku, a nakon provedenog izlučivanja sastavlja se zapisnik, sastavlja ga

[85] Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva. (26. 7. 2002.). (NN 90/2002)., Članak 2.

povjerenstvo koje provodi izlučivanje, i u zapisniku prilaže popis izlučenog gradiva[86]. Zatim se pristupa uništavanju gradiva koje se provodi vodeći računa o razini povjerljivosti podataka. Nakon uništavanja gradiva sastavlja se zapisnik koji se dostavlja nadležnom arhivu. Članak 17. određuje trajno čuvanje dokumentacije o postupku izlučivanja i uništavanja.

5.1.6. Pravilnik o evidencijama u arhivima

Pravilnik o evidencijama koje je potrebno voditi u arhivima donosi vrlo precizno ispisane zahtjeve za evidencije i propisuje vođenje slijedećih evidencija[87]:

- Knjiga primljenog arhivskoga gradiva (Knjiga akvizicija),
- Knjiga pohranjenog arhivskoga gradiva (Knjiga depozita),
- Opći inventar (našastar) arhivskoga gradiva,
- Dosje arhivskoga fonda/zbirke,
- Knjiga arhivskoga gradiva snimljenog u sigurnosne i zaštitne svrhe,
- Knjiga arhivskoga gradiva snimljenog u dopunske svrhe,
- Knjiga restauriranog i konzerviranog arhivskoga gradiva,
- Evidencija stvaratelja arhivskoga gradiva na području nadležnosti arhiva,
- Evidencija imatelja arhivskoga gradiva na području nadležnosti arhiva,
- Evidencije o korištenju arhivskoga gradiva.

Dodatno, Hrvatski državni arhiv, kao središnji i matični arhiv Republike Hrvatske, vodi i sljedeće evidencije[88]:

- Registar arhivskih fondova i zbirki Republike Hrvatske,
- Upisnik vlasnika i imatelja privatnoga arhivskoga gradiva u Republici Hrvatskoj,
- Evidencija o arhivskome gradivu od značenja za Republiku Hrvatsku u inozemstvu i o gradivu iseljene Hrvatske,
- Registar arhivskoga gradiva Republike Hrvatske koje je proglašeno kulturnim dobrom,
- Upisnik arhiva u Republici Hrvatskoj,
- Evidencija osoba zaposlenih u državnim arhivima.

Pravilnik o evidencijama u arhivima dalje navodi detaljne popise podataka koji se upisuju u navedene evidencije. Pravilnik u Članku 6. određuje slijedeće: "Upisi u Knjigu

[86] ibid., Članak 15.
[87] Pravilnik o evidencijama u arhivima. (26. 7. 2002.). (NN 90/2002, NN 106/2007)., Članak 3.
[88] ibid., Članak 4.

akvizicija u Knjigu depozita ne mogu se brisati. Ako je potrebno ispraviti netočan podatak, precrta ga se tako da ostane čitljiv, a pored njega upiše se ispravak. Stranice Knjige akvizicija i Knjige depozita trebaju biti numerirane, uvezane i prošivene zapečaćenom vrpcom te ovjerovljene potpisom ravnatelja i pečatom arhiva. Ako se Knjiga akvizicije i Knjiga depozita vode u elektroničkom obliku, mora se osigurati autentičnost zapisa. Ispravci se provode tako da ostane sačuvan raniji podatak. Unos i ispravak podataka može obavljati samo za to ovlaštena osoba. Podatci o osobi koja je unijela ili ispravila podatak u Knjizi akvizicija i Knjizi depozita te o nadnevku unosa odnosno ispravka upisuju se automatski i ne mogu se naknadno mijenjati. Po završetku kalendarske godine elektronički upisi u Knjigu akvizicija i Knjigu depozita za tu kalendarsku godinu se ispisuju na papir, a ispisane se stranice numeriraju, uvezuju i prošivaju na način utvrđen u stavku 4. Članka 6..”[89]

Zanimljivost vezana za digitalizaciju je Članak 9. koji za knjigu arhivskoga gradiva snimljenog u sigurnosne i zaštitne svrhe određuje se vođenje evidencije sa slijedećim podacima:

1. redni broj upisa preslike,
2. signatura i naziv izvornika,
3. signatura preslike,
4. cjelovitost snimanja,
5. podloga i tehnika snimanja (podloga – disketa, magnetno-optički disk, CD ROM, DVD i dr.; tehnika snimanja – crno-bijelo ili u boji, mikrofilmiranje, fotografiranje, skeniranje; format filma – 16 mm, 35 mm i dr.; format digitalnog zapisa – TIFF, GIF, JPEG i dr.; oblik filma – mikrofilmski svitak, aperturna kartica, mikrofiš i dr.),
6. vrsta preslika (matični negativ, posredni negativ, dijapozitiv i sl.) i generacija preslika (prva, druga i treća itd.),
7. količina zapisa (količina analognih zapisa, mikrooblika i fotografija – broj snimaka; količina zvučnih, filmskih i video zapisa – trajanje reprodukcije; količina digitalnih zapisa – broj zapisa, broj kilobajta i broj datoteka),
8. podaci o odgovornosti za izradu preslike (prezime i ime osobe koja je izradila presliku, naziv ustanove u kojoj je preslika izrađena i datum izrade preslike),
9. topografska oznaka preslike odnosno oznaka smještaja,
10. dostupnost,

[89] ibid., Članak 6.

11. napomena.

Prema ovom Pravilniku u Članku 22. za opis arhivskog gradiva propisano je korištenje Opće međunarodne norme za upis arhivskoga gradiva (ISAD/G) te sukladno Međunarodnoj normi arhivističkoga normiranoga zapisa za pravne i fizičke osobe te obitelji (ISAAR(CPF)) kao i upute, pravilnici i smjernice koje donosi Hrvatski državni arhiv.

Pravilnik propisuje da se evidencije koje se vode u elektroničkom obliku moraju zaštititi od neovlaštenog unosa, brisanja, izmjene, pristupa i upotrebe podataka i to na način da se[90]:

- pristupa koristeći korisničke podatke,
- evidentiranje odgovornosti za unos i promjenu podataka,
- obavlja redovito sigurnosno kopiranje,
- donese pisani akt, pri čemu se jedna kopija dostavlja Hrvatskome državnom arhivu, kojim se utvrđuje plan i metodologija dugoročne zaštite podataka i sadrži:
    - opis tehnologije za izradu evidencija,
    - opis primijenjenih standarda,
    - opis formata podataka,
    - plan i opis postupaka kopiranja, konverzije, reformatiranja i migracije podataka koji se predviđaju.

5.2. Zakon o knjižnicama

Zakon o knjižnicama uređuje knjižničnu djelatnost, rad knjižnica i njihov nadzor. Člankom 6. obvezuje na pristupačnost knjižnične građe, korištenje, posudbu i protok informacija, i pri tome voditi dokumentaciju o građi i korisnicima. Zadatak provođenja zaštite knjižnične građe koja ima svojstvo kulturnog dobra propisana je Člankom 15. Knjižnice u svojoj građi posjeduje tiskovine: knjige, brošure, skripte, posebni otisci, časopisi, novine, magazini, bilteni, zemljopisne i druge karte, reprodukcije slikovnih umjetničkih djela, muzikalije, katalozi, kalendari, kazališni i drugi programi, te njihovi dodaci u tiskanom, audiovizualnom i elektroničkom obliku, plakati, letci, kratki oglasi i priopćenja, razglednice, službene i trgovačke tiskanice [...]“[91].

[90] ibid., Članak 24.
[91] Zakon o knjižnicama. (25. 6. 2009.). (NN 105/97, 05/98, 104/00, 69/09)., Članak 38.

Stručni nadzor nad radom knjižnica obavljaju matične knjižnice na način propisan pravilnikom o matičnoj djelatnosti, dok stručni nadzor nad radom matičnih knjižnica i općeznanstvenih knjižnica obavlja Nacionalna i sveučilišna knjižnica u Zagrebu.[92]

Zakon propisuje poduzimanje mjera zaštite i čuvanja knjižnične građe u skladu s pravilniku o zaštiti knjižnične građe.[93] Pravilnikom su propisani uvjeti čuvanja, način korištenja i pohrane knjižnične građe koji su po zahtjevima vrlo slični čuvanju arhivskog gradiva. Člankom 7. Pravilnika propisan je način označavanja nove građe koju se uvodi u knjižnični fond, na primjer „Signature se upisuju na prvi slobodni predlist kad je riječ o staroj knjizi, odnosno na poleđinu lista ukoliko je riječ o neknjižnoj građi [...]“[94].

Članak 15. propisuje stariju građu presnimiti na „[...] tehnološki stabilniji medij.“[95] Nadalje Članci 16. i 17. omogućuju zaštitno snimanje fotokopiranjem, mikrofilmiranjem i digitalizacijom, pri čemu za digitalizaciju ne postoje uvjeti niti ograničenja osim zahtjeva da se može „[...] prenositi digitalizacijom uz odgovarajuću opremu.“[96]

Korištenje knjižnične građe, Članak 18., treba biti propisano knjižničnim općim aktom i treba istaknuti upute o rukovanju na vidljivom mjestu u učionici. Korištenje se nadzire od strane voditelja odjela za rad s korisnicima.

Knjižnice mogu u svom fondu imati zaštićenu građu. Članak 23. određuje kako se na korištenje ne daje izvorno zaštićeno gradivo već se ona mora mikrofilmirati u dvije kopije na srebrno-halogenom filmu te čuvati u optimalnim mikroklimatskim uvjetima.

5.3. Zakon o muzejima

Zakon o muzejima propisuje muzejima i galerijama te muzejima, galerijama i zbirkama unutar pravnih osoba redovito upisivanje muzejskih predmeta u inventarnu knjigu i vođenje druge dokumentacije o muzejskoj građi i muzejskoj djelatnosti te prijavljivanje nadležnom tijelu muzejsku građu i dokumentaciju radi uspostavljanja zaštite u skladu s propisima o zaštiti i očuvanju kulturnih dobara.[97]

Nadzor nad radom muzeja i galerija propisan je točkom VIII. Nadzor nad radom Zakona o muzejima. U točki VIII propisan je stručni nadzor, nadzor nad zakonitošću rada te inspekcijski nadzor.

[92] ibid., Članak 47.
[93] ibid., Članak 45.
[94] Pravilnik o zaštiti knjižnične građe. (22. 4. 2005.). (NN 52/2005)., Članak 11.
[95] ibid., Članak 15.
[96] ibid., Članak 17.
[97] Zakon o muzejima. (21. 10. 2015.). (NN 110/15)., Članak 8.

Članak 8. Zakona o muzejima propisuje način vođenja i ostvarivanje uvida u muzejsku građu putem donesenog Pravilnika o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju kojeg donosi ministar zadužen za kulturu.

5.3.1. Pravilnik o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju

Način korištenja muzejske građe i dokumentacije propisan je Pravilnikom o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju. Članak 3. Pravilnika propisuje muzejima obavezu omogućavanja uvida u njihovu građu i dokumentaciju svim zainteresiranim osobama za što se podnosi pisani zahtjev[98], i muzeji vode evidenciju vanjskih korisnika[99]. Muzejska građa se štiti kao kulturno dobro, daje se na uvid samo u prostorijama muzeja u obliku preslika i snimaka, a u izvornom obliku samo ako zahtjeva stručna i znanstvena metoda rada i ako to dopušta očuvanost, i na način kojim se garantira sigurnost i primjerena upotreba[100].

Propisana procedura za ostvarivanje uvida sadrži slijedeće korake[101]:

1. zainteresirana osoba podnosi pisani zahtjev koji sadrži:
   a. osobni podaci/podaci o instituciji,
   b. podatke o mjestu stanovanja/institucije,
   c. temu istraživanja ili drugu svrha uvida u građu i dokumentaciju,
2. ravnatelj/voditelj muzeja daje odobrenje za uvid u muzejsku građu i dokumentaciju,
3. osoba koja je podnijela zahtjev potpisuje dokument kojim potvrđuje kako je upoznata s načinom i uvjetima uvida u muzejsku građu i dokumentaciju.

Pravilnik Člankom 13. dopušta povjeravanje muzejske građe i dokumentacije ukoliko je ona inventarizirana i snimljena.

[98] Pravilnik o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju. (21. 12. 2001.). (NN 115/2001)., Članak 5.
[99] ibid., Članak 7.
[100] ibid., Članak 9.
[101] ibid., Članak 5.

5.3.2. Pravilnik o sadržaju i načinu vođenja muzejske dokumentacije o muzejskoj građi

Ovim Pravilnikom utvrđuju se sadržaj i način vođenja muzejske dokumentacije koja nastaje u muzejima i galerijama, te muzejima, galerijama i zbirkama unutar ustanova i drugih pravnih osoba, kao i postupci koji se odnose na stvaranje i pohranjivanje muzejske dokumentacije.

Muzejska dokumentacija, definiran Člankom 2. Pravilnika o sadržaju i načinu vođenja muzejske dokumentacije o muzejskoj građi, „[...] je sustavno izrađen, prikupljen, organiziran i pohranjen skup podataka, koji je nastao u tijeku procesa stručne obrade, zaštite i prezentacije muzejske građe, te se temelji na dogovorenom i utvrđenom broju i kvaliteti podataka o predmetu, grupi predmeta ili cjelokupnom fondu“[102], a stvara se „[...] u postupcima inventarizacije, katalogiziranja i indeksiranja, koji predstavljaju trajan proces obrade i nadopunjavanja podataka.“[103]

Podaci o muzejskoj dokumentaciji vode se u pisanom obliku ili u računalnoj bazi podataka. Tako stvoreni podaci pohranjuju se na trajne medije uz obvezno snimanje na mikrofilm i čuvanje u odgovarajućim prostorima i uvjetima.[104]

Muzejska dokumentacije se vodi kroz primarnu (temeljnu), sekundarnu i tercijarnu dokumentaciju. Primarnu dokumentaciju čine: inventarna knjiga muzejskih predmeta, katalog muzejskih predmeta, knjiga ulaska muzejskih predmeta, knjiga izlaska muzejskih predmeta, knjiga pohrane muzejskih predmeta i zapisnici o reviziji muzejske građe. Sekundarnu dokumentaciju čine: inventarne knjige audio-vizualnih fondova, inventarna knjiga hemeroteke, knjiga evidencije o izložbama, evidencija o konzervatorsko-restauratorskim postupcima, evidencija o pedagoškoj djelatnosti, evidencija o stručnom i znanstvenom radu, evidencija o izdavačkoj djelatnosti, dokumentacija o marketingu i odnosima s javnošću te dokumentacija o osnivanju i povijesti muzeja. Tercijarnu dokumentaciju čine: pomagala u obliku raznovrsnih kataloga i indeksa (predmetnih, autorskih, kronoloških, topografskih i drugih), generira se iz fondova primarne i sekundarne dokumentacije u obliku tezaurusa, indeksa, kataloških listića i sažetaka, radi bržeg pretraživanja i korištenja podataka iz postojećih dokumentacijskih fondova.

[102] Pravilnik o sadržaju i načinu vođenja muzejske dokumentacije o muzejskoj građi. (16. 9. 2002.). (NN 108/2002)., Članak 2.
[103] ibid.
[104] ibid., Članak 3.

5.4. Zakon o elektroničkom potpisu i eIDAS uredba

Zakon o elektroničkom potpisu definira izradu i korištenje elektroničkog potpisa i vremenskog žiga. Elektronički potpis služi za identifikaciju potpisnika i potvrdu vjerodostojnosti potpisanog elektroničkog zapisa[105], pri čemu elektronički zapis može biti i slika. Na primjer digitaliziranu sliku možemo potpisati elektroničkim potpisom i time identificirati da je upravo skup tih podataka koje predstavlja digitalizirana slika izradio operater koji se nalazi u identifikacijskim podacima elektroničkog potpisa.

Prirodno se postavlja pitanje tko jamči točnost podataka o operateru. Zbog toga zakon uvodi pojam certifikat kao potvrdu u elektroničkom obliku „[...] koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe.“[106] i pojam kvalificiranog certifikata. Kvalificirani certifikat je certifikat koji je izdao davatelj usluga za izdavanje kvalificiranog certifikata kako je Zakonom regulirano i odobreno od strane Ministarstva[107]. Na taj način certifikat operatera potvrđuje drugo tijelo koje ima obavezu vođenja evidencije svih izdanih i opozvanih certifikata[108] te čuvati svu dokumentaciju o izdanim i opozvanim certifikatima minimalno 10 godina od izdavanja[109]. Davatelju usluga certificiranja je propisano čuvanje, podataka o potpisnicima, izdanih certifikata, liste opozvanih certifikata kao i svih tehničkih podataka koji su nastali radom sustava certificiranja, na medijima koji osiguravaju trajnost zapisa od najmanje 20 godina, te izradu sigurnosnih kopija smještenih na drugoj lokaciji izdvojeno od sustava u upotrebi.

Izdavanje kvalificiranog certifikata propisano je Člankom 29. Zakona o elektroničkom potpisu u kojem se propisuje način osiguranja istinitosti podataka koji se nalaze u certifikatu. Ukratko, davatelj usluga certificiranja provjerava istinitost kvalificiranog certifikata koji se koristi prilikom izrade naprednog elektroničkog potpisa.

Napredan elektronički potpis definiran u Zakonu pouzdano jamči identitet potpisnika[110], i to na način kako je ranije opisano. Napredan elektronički potpis zamjenjuje vlastoručni potpis.

Razina sigurnosti prilikom izdavanja certifikata je propisana na izrazito visokom nivou. Osoba koja traži uslugu (potpisnik) osobno podnosi zahtjev te za iste odgovara pravno i materijalno. Uz podatke prilaže dokument s fotografijom (na primjer osobna iskaznica,

[105] Zakon o elektroničkom potpisu. (6. 3. 2014.). (NN 10/02, 80/08, 30/14)., Članak 3.
[106] ibid., Članak 2.
[107] ibid., Članak 18.
[108] ibid., Članak 30.
[109] ibid., Članak 31.
[110] ibid., Članak 2.

putovnica, europska identifikacijska kartica) te se dopunski, prilikom predaje, provjerava tako da potpisnik ispravno i potpuno izgovara i piše ime i prezime potpisnika. Ovi se podaci zatim upisuju i arhiviraju u sustavu a sadržaj certifikata se upisuje u Registar izdanih certifikata. Potpisnik osobno preuzima izdati certifikat a izdavanje certifikata obavlja isključivo osoba koja je za te poslove ovlaštena.

Dodatno što elektronički potpis potvrđuje je nepromjenjivost sadržaja. Ova nepromjenjivost se postiže kriptiranjem sadržaja koji se upisuje u elektronički potpis, točnije izrađuje se hash sadržaja korištenjem RIPEMD 160 SHA-1 (engl. Secure Hash Algoritam) kako je propisano Pravilnikom o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata.

Elektroničkim potpisom potvrđujemo potpisnika i sadržaj elektroničkog zapisa međutim ne potvrđujemo vrijeme kada je elektronički zapis potpisan. Zbog toga Zakon definira vremenski žig kojim se potvrđuje sadržaj na koji se vremenski žig odnosi te vrijeme na koje se vremenski žig odnosi, na primjer operater na skeneru izradi digitaliziranu sliku i potpiše ju vremenskim žigom kojim se potvrđuje vrijeme kada je slika izrađena. Slično kao kod elektroničkog potpisa postavlja se pitanje je li to vrijeme usklađeno s globalnim vremenom odnosno je li računalo koje je izradilo vremenski žig imalo postavljeno vrijeme na kojem možemo vjerovati, a ne primjerice dva dana ranije. U tu svrhu Zakon definira napredan vremenski žig koji je izrađen prema uvjetima za izradom naprednog elektroničkog potpisa. [111]

eIDAS uredba sastavljena je u Bruxellesu 23.7.2014. i stupila je na snagu 1.7.2016., s periodom prilagodbe od dvije godine, odnosno od 1.7.2018. u potpunosti zamjenjuje Zakon o elektroničkom potpisu. Većim dijelom uredba propisuje izradu elektroničkog potpisa i vremenskog žiga na isti način kao i Zakon o elektroničkom potpisu. Međutim postoje određene izmjene.

Elektronički potpis je definiran slično definiciji u Zakonu o elektroničkom potpisu. Pored naprednog elektroničkog potpisa uvodi se pojam kvalificirani elektronički potpis. Napredan elektronički potpis je izrađen koristeći kvalificirani certifikat za elektronički potpis, dok je kvalificirani elektronički potpis upravo napredan elektronički potpis koji je izrađen koristeći kvalificirana sredstva za izradu elektroničkog potpisa.[112] Kvalificirani elektronički

[111] ibid., Članak 2.
[112] eIDAS, UREDBA (EU) br. 910/2014 EUROPSKOG PARLAMENTA I VIJEĆA. (23. 7. 2014.)., Članak 2.

potpis definiran uredbom ima jednak pravni učinak kao vlastoručni potpis[113] što se razlikuje od Zakona o elektroničkom potpisu koji je to odredio naprednom elektroničkom potpisu.

Za korištenje elektroničkog potpisa koristi se certifikat za elektronički potpis. Za korištenje elektroničkog pečata koristi se certifikat za elektronički pečat. Za izradu elektroničkog vremenskog žiga koristi se elektronički potpis ili elektronički pečat ili jednako vrijedna metoda.[114]

Nadzor kvalificiranih pružatelja usluga povjerenja[115] provodi tijelo za ocjenjivanje sukladnosti koje potvrđuje da kvalificirani pružatelji usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u eIDAS Uredbi. Nadzorno tijelo reviziju može obaviti u bilo kojem trenutku te svoj izvještaj šalje tijelima za zaštitu podataka, a ukoliko rezultat revizije pokaže potrebu za ukidanjem statusa tog pružatelja usluge ukidanje se evidentira u pouzdanom popisu koji se vodi u svakoj državi članici.

Uredba uvodi novi element elektronički pečat. Elektronički pečat je stvoren radi osiguranja izvornosti i cjelovitosti elektroničkih podataka na koje se odnose.[116] Za izradu elektroničkog pečata koristi se certifikat za elektronički pečat koji služi kao elektronička potvrda za podatke o pravnoj osobi koja je izradila elektronički pečat.[117] Međutim, slično kao kod elektroničkog potpisa i kvalificiranog elektroničkog potpisa i istog razloga, uvodi se pojam kvalificirani certifikat za elektronički pečat kojeg izdaje kvalificirani pružatelj usluge povjerenja.[118]

Napredan elektronički pečat mora ispunjavati sljedeće[119]: na nedvojben način je povezan s autorom pečata, omogućava identificiranje autora pečata, izrađen je korištenjem podataka za izradu elektroničkog pečata koje autor pečata koristi samostalno i pod svojom kontrolom za izradu elektroničkog pečata i povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka.

Vremenski žig definiran Zakonom o elektroničkom potpisu eIDAS uredbom dobiva novo ime i zove se elektronički vremenski žig. Razlikuju se elektronički vremenski žig i kvalificirani elektronički vremenski žig. Elektronički vremenski žig dokazuje da su podaci na koje se odnosi postojali u vrijeme na koje se odnosi. Kvalificirani elektronički vremenski žig povezuje datum i vrijeme s podacima tako da isključuje mogućnost nezapažene promjene

[113] ibid., Članak 25.
[114] ibid., Članak 42.
[115] ibid., Članak 17.
[116] ibid., Članak 2.
[117] ibid.
[118] ibid.
[119] ibid., Članak 36.

podataka, temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom i potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.[120]

Elektronički potpis, elektronički pečat i elektronički vremenski žig definiran uredbom primjenjuju se na elektroničke dokumente. Elektronički dokument, slično elektroničkom zapisu u Zakonu o elektroničkom potpisu, je svaki sadržaj koji je pohranjen u elektroničkom obliku, bilo kao tekstualni, zvučni, vizualni ili audiovizualni zapis, što znači da je elektronički dokument i digitalizirana slika.

Uredba, Člankom 32., propisuje kako kvalificiranu uslugu validacije kvalificiranih elektroničkih potpisa može pružati samo kvalificirani pružatelj usluga povjerenja koji validaciju obavlja u skladu uvjetima navedenim u tom članku i omogućuje pouzdajućim stranama primanje rezultata postupka validacije na automatizirani način koji je pouzdan, učinkovit i nosi napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluge validacije.

Korištenje elektroničkih potpisa, elektroničkih pečata i elektroničkih vremenskih žigova koji se temelji na kvalificiranim certifikatima je vremenski ograničeno.[121] Tako, na primjer, Narodni list podsjeća kako „[…] certifikate za fiskalizaciju potrebne za izdavanje fiskaliziranih računa izdaje Financijska agencija (FINA) na rok od pet godina […]“[122], što znači da je certifikat potrebno obnoviti. U slučaju kada se digitalizirane slike potpisuju koristeći kvalificirane certifikate dobro je na umu imati ovu činjenicu te predvidjeti moguće posljedice.

5.5. Zakon o elektroničkoj trgovini

Komunikacija korištenjem modernih elektroničkih uređaja jeftinija je od klasične. Na primjer u marketinške svrhe izrada papirnatih promotivnih materijala puno je skuplja od izrade digitalnih kataloga. Zatim, cijena određenih proizvoda može biti puno niža zbog smanjenja stajanja proizvoda u više skladišnih prostora kao što su različite trgovine u različitim gradovima u odnosu na jedno skladište na povoljnijem prostoru povezana s elektroničkom komunikacijom pri naručivanju proizvoda i slanjem poštom.

[120] ibid., Članak 42.
[121] ibid., Prilog I
[122] Valkaj, T. (24. 6. 2017.). Provjerite rok trajanja vaših certifikata za fiskalizaciju. Preuzeto 10. 1. 2018. iz Narodni list: URL: http://www.narodni-list.hr/posts/338405001

Zakon o elektroničkoj trgovini uređuje pružanje usluga putem elektroničkih usluga te sklapanja ugovora u elektroničkom obliku.[123] Unutar zakona reguliran je način i potrebni podaci davatelja usluga koji moraju biti dostupni korisnicima[124], sadržaj komercijalnih priopćenja[125] i način prihvata komercijalnih priopćenja[126].

Odredbe ovog zakona ne primjenjuju se „[...] na zaštitu podataka, područje oporezivanja, javnobilježničku djelatnost, zastupanje stranaka i zaštitu njihovih interesa pred sudovima, te na igre na sreću s novčanim ulozima, uključujući lutrijske igre, igre u casinima, kladioničke igre i igre na sreću u automatima, a u skladu s odredbama posebnih zakona koji uređuju odnosna područja.“[127]

Zakon o elektroničkoj trgovini Člankom 9. propisuje način sklapanja ugovora elektroničkim putem. Člankom 11. propisuje za sve ugovore za koje se za valjanost ugovora traži potpis osobe dovoljno je poslati elektroničku poruku potpisanu elektroničkim potpisom, pri čemu nije jasno radi li se o kvalificiranom elektroničkom potpisu ili običnom elektroničkom potpisu. Sklapanje ugovora u elektroničkom obliku odvija se „[...] onog trenutka kada ponuditelj primi elektroničku poruku koja sadrži izjavu ponuđenog da prihvaća ponudu.“[128] Pri tome, poruka koja sadrži ponudu ili prihvat ponude a upućena je davatelju usluga mora bez odgode biti potvrđena posebnom elektroničkom porukom.[129]

Smatram da je važno istaknuti kako se ovaj zakon ne odnosi na sklapanje svih ugovora kao što je ranije navedeno. Člankom 9. je izrijekom navedeno na koje ugovore se ne primjenjuje:

- „imovinske, predbračne, odnosno bračne ugovore i druge ugovore koje uređuje Obiteljski zakon,
- ugovore o opterećenju i otuđenju imovine za koje je potrebno odobrenje centra za socijalnu skrb,
- ugovore o ustupu i raspodjeli imovine za života, ugovore o doživotnom uzdržavanju i sporazume u vezi s nasljeđivanjem, ugovore o odricanju od nasljedstva, ugovore o prijenosu nasljednog dijela prije diobe, oporučne poslove i druge ugovore koje uređuje Zakon o nasljeđivanju,
- darovne ugovore,

[123] Zakon o elektroničkoj trgovini. (6. 3. 2014.). (NN 173/03, 67/08, 36/09, 130/11, 30/14)., Članak 1.
[124] ibid., Članak 6.
[125] ibid., Članak 7.
[126] ibid., Članak 8.
[127] ibid., Članak 1.
[128] ibid., Članak 15.
[129] ibid., Članak 14.

- ugovore o prijenosu prava vlasništva na nekretninama ili druge pravne poslove kojima se uređuju stvarna prava na nekretninama, osim ugovora o najmu i zakupu nekretnina,
- druge ugovore za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave,
- druge ugovore za koje je posebnim zakonom ili propisom donesenom na temelju zakona izričito određena uporaba vlastoručnog potpisa u dokumentima na papiru ili ovjera vlastoručnog potpisa,
- ugovore i očitovanja volje jamaca, ako je jamac osoba koja djeluje izvan svoje trgovačke, poslovne ili profesionalne djelatnosti.“[130]

Člankom 22. propisuje se inspekcijski nadzor nad provedbom Zakona o elektroničkoj trgovini koji obavljaju inspektori Ministarstva financija

5.6. Zakon o elektroničkoj ispravi

Zakon o elektroničkoj ispravi uređuje uporabu elektroničke isprave fizičkim i pravnim osobama u svim poslovnim radnjama, djelatnostima i postupcima koji se vode pred tijelima javne vlasti kojima se pomoću elektroničke opreme i programa mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, osim u onim slučajevima gdje se drugim zakonima izričito traži uporaba isprava na papiru, te izričito daje pravnu snagu elektroničkoj ispravi koju ima isprava na papiru, ukoliko je njena uporaba i promet u skladu sa Zakonom o elektroničkoj ispravi.[131]

Upotreba i promet elektroničkih isprava regulira se Člankom 3. na način da svaka fizička i pravna osoba svojim očitovanjem prihvaća upotrebu i promet, a ukoliko se upotreba i promet provode u skladu sa Zakonom o elektroničkoj ispravi ima istu pravnu snagu kao i isprava na papiru.

Isprava na papiru je dokument koji je pisani tekst na papiru, ovjeren potpisom ili žigom od strane izdavatelja. Elektronička isprava se bitno razlikuje zbog toga što je potrebno osigurati identitet stvaratelja, vjerodostojnost poruke i vremensko obilježje kreiranja, slanja i izmjene sadržaja. Zakon definira elektroničku ispravu kao jednoznačno povezan cjelovit skup podataka koji su elektronički oblikovani, poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva kojima se utvrđuje izvor (stvaratelj), vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu. Sadržaj

[130] ibid., Članak 9.
[131] Zakon o elektroničkoj ispravi. (9. 12. 2005.). (NN 150/05)., Članak 1.

elektroničke isprave uključuje sve oblike pisanog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor.[132]

Elektronička isprava prolazi dokumentacijski ciklus odnosno radnje izrade, slanja, primanja, pohranjivanja i čuvanja tijekom kojih se potvrđuje stvaratelj, pošiljatelj, primatelj, vrijeme otpreme i vrijeme prijema, vjerodostojnost i cjelovitost elektroničke isprave.[133] Za razliku od ostalih elektroničkih dokumenata elektronička isprava se sastoji od dva dijela, sadržaja isprave i dokumentacijskog svojstva. Dokumentacijsko svojstvo je obavezan skup podataka koji se sastoji od jednog ili više naprednih elektroničkih potpisa, podaci o vremenu nastajanja odnosno završetka izrade elektroničke isprave, naziva stvaratelja i drugih podataka kojima je svrha zadržavanje vjerodostojnosti, cjelovitosti i valjanosti kroz vremensko razdoblje.[134]

Zakonom je određeno kako elektronička isprava ne može imati presliku u elektroničkom obliku, već „Ako ista osoba izradi dvije i više isprava s istim sadržajem, od kojih je jedan primjerak izrađen u elektroničkom obliku a drugi izrađen na papiru, te se isprave smatraju neovisnim. U tim slučajevima isprava izrađena na papiru ne smatra se preslikom elektroničke isprave.“[135] Dopušteno je izraditi elektroničku ispravu na papiru i da pri tome bude ovjerovljena preslika elektroničke isprave. Ukoliko se elektronička isprava vodi u tijelima javne vlasti tada ju ovjerovljuje ovlaštena osoba, a u svim ostalim slučajevima ovjeru obavlja javni bilježnik i pri tome obavezno preslika sadrži oznaku kako se radi o preslici elektroničke isprave.[136]

Upotreba i promet se reguliraju na način da se svaka radnja s elektroničkom ispravom unutar dokumentacijskog ciklusa označi jedinstvenom oznakom i svojstvima kojima se osigurava izravna povezanost prethodne i slijedeće radnje te se oni moraju ugraditi u elektroničku ispravu.[137] Nakon izrade elektroničke isprave slijedi slanje i prijem. Prijem elektroničke isprave slijedi potvrda primatelja o prijemu. Ukoliko do te potvrde ne dođe u propisanom vremenu pošiljatelj obavještava primatelja kako nije zaprimio potvrdu prijeme. Ponovnim protekom određenog vremena tijekom kojeg nije stigla potvrda primatelja elektronička isprava se smatra neposlanom. Podaci o vremenu otpreme i vremenu prijema se upisuju u sadržaj elektroničke isprave i zakonom je zabranjeno mijenjanje tih podataka.[138]

[132] ibid., Članak 4.
[133] ibid.
[134] ibid., Članak 4. i Članak 7.
[135] ibid., Članak 9.
[136] ibid., Članak 10.
[137] ibid., Članak 14.
[138] ibid., Članak 18.

Ovako definirana elektronička isprava može se koristiti kao dokaz u slučajevima koji se vode pred tijelima javne vlasti i arbitražama. Prilikom ocjene ispravnosti zakon određuje uzimanje u obzir pojedinosti o njenoj izradi, pohrani, prijenosu, čuvanju, vjerodostojnosti i nepromjenjivosti.[139] Članak 19. određuje elektroničku ispravu kao pravovaljanu ukoliko ona sadrži podatke o stvaratelju, pošiljatelju i primatelju, sadrži podatke o vremenu otpreme i prijema, tijekom cijelog ciklusa ostaje nepromijenjena kakva je bila pri izradi i u bilo kojem trenutku je dostupna i čitljiva.[140]

Zakonom je zahtijevano čuvanje elektroničkih isprava u izvornom obliku.[141] Izričito se traži čuvanje na medijima koji omogućuju trajnost zapisa tijekom cijelog vremena čuvanja, oblik izrade, otpreme, primanja i pohrane ne smije mijenjati niti informaciju niti sadržaj, tijekom cijelog vremena čuvanja moraju biti čitljive i dostupne, čuvaju se podaci o elektroničkim potpisima i za ovjeru elektroničkih potpisa, vjerodostojnost i cjelovitost treba biti očuvana tijekom perioda čuvanja, može se utvrditi podrijetlo, stvaratelj, vrijeme, način i oblik zaprimanja u sustav na čuvanje, vodi se računa o nepromjenjivosti i neovlaštenog brisanja, vodi se računa o očuvanju cjelovitosti i nepovredivosti prilikom postupaka održavanja i zamjene medija za pohranu.[142]

Tijela javne vlasti koji koriste elektroničke isprave s tajnim podacima moraju ovjeriti informacijsku i komunikacijsku opremu za zaštitu elektroničkih isprava preko nadležnog tijela za poslove informacijske sigurnosti.[143]

5.7. Zakon o autorskom pravu i srodnim pravima

Zakon o autorskom pravu i srodnim pravima uređuje autorsko pravo, te prava umjetnika izvođača na njihovim izvedbama, prava proizvođača fonograma na njihovim fonogramima, prava filmskih producenata (proizvođača videograma) na njihovim videogramima, prava organizacija za radiodifuziju na njihovim emitiranjima, prava nakladnika na njihovim izdanjima, prava proizvođača baza podataka na njihovim bazama podataka koje zakon imenuje srodnim pravima.[144]

[139] ibid., Članak 12.
[140] ibid., Članak 19.
[141] ibid., Članak 20.
[142] ibid., Članak 20.
[143] ibid., Članak 25.
[144] Zakon o autorskom pravu i srodnim pravima. (8. 7. 2017.). (NN 167/03, 79/07, 80/11, 125/11, 141/13, 127/14, 62/17)., Članak 1.

Autorsko djelo zakon definira kao originalnu intelektualna tvorevina iz književnoga, znanstvenog i umjetničkog područja koja ima individualni karakter, bez obzira na način i oblik izražavanja, vrstu, vrijednost ili namjenu[145], kao što su na primjer pisana djela poput knjiga, djela likovne umjetnosti kao što su slike, fotografska djela kao što su umjetničke fotografije, kartografska djela kao što su karte napravljene ranijih stoljeća, prikazi znanstvene ili tehničke prirode kao što su crteži, planovi skice, tablice[146].

Zakon prepoznaje različite vrste autora autorskog djela. Tako imamo jednog autora[147] koji je fizička osoba koja je autorsko djelo stvorila, više autora[148] koji stvore samostalno autorsko djelo radi zajedničkog korištenja, koautore[149], više osoba, koji stvore zajedničkim radom jedno autorsko djelo, kada autor nije poznat tada se djelo zove djelo siročadi[150] sve do otkrivanja stvarnog autora. Autorsko djelo može biti stvoreno i u radnom odnosu. U tom slučaju autorstvo ovisi o sklopljenom ugovoru o radu ili aktom s kojim je uređen radni odnos.[151]

Člankom 17. Zakona o autorskom pravu i srodnim pravima propisuje se pravo autora da bude priznat i označen kao autor djela i pri korištenju autorskog djela autor mora biti naveden osim u slučaju kada autor to izričito u pismenom obliku zabrani. Pravo umnožavanja ili reproduciranja pripada isključivo autoru.[152] Reproduciranje znači postupak izrade autorskog djela bilo kojim sredstvima i u bilo kojem obliku kao što je na primjer fotokopiranje ili drugi fotografski postupci i pohrana autorskog djela u elektroničkom obliku. Na primjer svaka izrada autorskog djela postupkom digitalizacije mora navesti autora te prilikom javnog prikazivanja mora dobiti odobrenje autora za navodom autorskih podataka. Prestankom autorskog prava, autorsko djelo postaje javno dobro, smije se slobodno koristiti ali uz obavezu navođenja autorstva.[153]

Reproduciranje autorskog djela dopušteno je fizičkoj osobi ako to čini za svoje privatno korištenje.[154] Za potrebe očuvanja i osiguranja građe ili druge vlastite potrebe javni arhivi, javne knjižnice, muzeji i druge pravne osobe koje obavljaju muzejsku djelatnost, obrazovne i znanstvene ustanove, ustanove za predškolski odgoj i socijalne ustanove mogu

[145] ibid., Članak 5.
[146] ibid.
[147] ibid., Članak 9.
[148] ibid., Članak 10.
[149] ibid., Članak 11.
[150] ibid., Članak 12., 12a. i 12b.
[151] ibid., Članak 75.
[152] ibid., Članak 18.
[153] ibid., Članak 106.
[154] ibid., Članak 82.

reproducirati autorsko djelo iz vlastitog primjerka na bilo koju podlogu, na primjer radi očuvanja knjige knjižnice mogu digitalizirati knjigu.[155] Članak 84. dopušta reprodukciju djela siročadi u obliku digitalizacije a radi stavljanja na raspolaganje javnosti za kulturne i obrazovne potrebe javno dostupnim knjižnicama, obrazovnim ustanovama, muzejima i drugim pravnim osobama koje obavljaju muzejsku djelatnost, arhivima, ustanovama za filmsku i audiobaštinu i javnim organizacijama za radiodifuziju.

Prilikom uništenja autorskog djela Zakon o autorskom pravu i srodnim pravima izričito navodi kako je potrebno voditi računa o postojanju izvornika. Ukoliko vlasnik izvornika autorskog djela želi uništiti izvornik dužan je autora obavijestiti o tome koji tada odlučuje otkupiti izvornik ili napraviti fotografiju izvornika ili dopustiti uništenje. Ukoliko ne postoji izvornik i želi se uništiti umnoženi primjerci autorskog djela potrebno je obavijestiti autora koji tada odlučuje kao i s izvornikom.[156]

5.8. Zakon o zaštiti osobnih podataka i opća uredba o zaštiti osobnih podataka (GDPR)

Zakonom o zaštiti osobnih podataka uređuje se zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka i odnosi se na državna tijela, tijela lokalne i područne (regionalne) samouprave te pravne i fizičke osobe, predstavništva i podružnice stranih pravnih osoba i predstavnika stranih pravnih i fizičkih osoba koje obrađuju osobne podatke u Republici Hrvatskoj, ali ne i ukoliko se obrada osobnih podataka provodi za osobnu primjenu ili za potrebe kućanstva a koju provode fizičke.

Osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati.[157] Ispitanik je svaka fizička osoba čiji se osobni podaci prikupljaju.[158] Osobne podatke je dopušteno prikupljati u svrhu s kojom je ispitanik upoznat i uz njegovu privolu, moguće ih je dalje obrađivati samo u svrhu u koju su prikupljeni. Privola ispitanika je slobodno dano i izričito očitovanje volje ispitanika kojom on izražava svoju suglasnost s obradom njegovih osobnih podataka u određene svrhe.[159]

Ukoliko se poduzmu odgovarajuće zaštitne mjere dopušteno je obrađivati osobne podatke u povijesne, statističke ili znanstvene svrhe. Svi prikupljeni osobni podaci moraju biti

[155] ibid., Članak 84.
[156] ibid., Članak 79.
[157] Zakon o zaštiti osobnih podataka. (12. 6. 2003.). (NN 103/03, 118/06, 41/08, 130/11, 106/12)., Članak 2.
[158] ibid., Članak 2.
[159] ibid., Članak 2.

točni, potpuni i ažurni i moraju se čuvati u obliku koji dopušta identifikaciju ispitanika ali ne duže nego je to potrebno za svrhu u koju se podaci prikupljaju.

Izričito je zabranjeno prikupljanje i daljnja obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku.[160]

Svrha prikupljanja osobnih podataka je njihova obrada. Zakon definira obradu osobnih podataka: „[...] svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima.“[161]

Iz prikupljenih i obrađenih osobnih podataka izrađuju se zbirke osobnih podataka. Zbirka osobnih podataka je svaki strukturirani skup osobnih podataka koji je dostupan prema posebnim kriterijima, bilo centraliziranim, decentraliziranim, ili raspršenim na funkcionalnom ili zemljopisnom temelju i bez obzira na to je li sadržan u računalnim bazama osobnih podataka ili se vodi primjenom drugih tehničkih pomagala ili ručno.[162]

Prikupljanje osobnih podataka provodi se tako da je ispitanik, osoba čiji se podaci prikupljaju, jasno upoznat sa svrhom prikupljanja, identitetom voditelja zbirke koji prikuplja osobne podatke, pravima koje ispitanik ima, svrsi obrade prikupljenih podataka te posljedicama ukoliko se uskraćuje davanje podataka.[163] Voditelj zbirke osobnih podataka je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka.[164]

Prikupljeni podaci smiju se dati na korištenje drugima odnosno primateljima ukoliko postoji pravna osnova kao što je pisani zahtjev primatelja, zakonom utvrđena potreba radi obavljanja djelatnosti primatelja i za znanstveno-istraživačke svrhe pri čemu ne smije biti moguće identificirati osobu.[165] Primatelj je fizička ili pravna osoba, državno ili drugo tijelo kojem se osobni podaci otkrivaju, neovisno o tome je li on ujedno i treća strana ili nije. Državna tijela koja mogu primati podatke u okviru provođenja istraga ne smatraju se primateljima.[166]

[160] ibid., Članak 8.
[161] ibid., Članak 2.
[162] ibid., Članak 2.
[163] ibid., Članak 9.
[164] ibid., Članak 2.
[165] ibid., Članak 11.
[166] ibid., Članak 2.

Prikupljeni osobni podaci trebaju biti zaštićeni od uništenja, gubitka, neovlaštenih promjena, zloupotrebe ili neovlaštenog pristupa i to primjenjujući odgovarajuće tehničke, kadrovske i organizacijske mjere zaštite uz obavezu potpisivanja izjave o povjerljivosti od strane osoba koje su zaposlene u obradi osobnih podataka.[167] Nadzor nad obradom osobnih podataka obavlja Agencija za zaštitu osobnih podataka.[168]

Opća Uredba o zaštiti osobnih podataka, odnosno GDPR (engl. General Data Protection Regulation) regulira zaštitu osobnih podataka građana Europske unije, službeno je donesena 27. travnja 2016., i stupa na snagu 25. svibnja 2018. Ova uredba punog naziva UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka stavlja izvan snage Direktivu 95/46/EZ (Opća uredba o zaštiti podataka) s kojom je usklađen Zakon o zaštiti osobnih podataka kojeg isto stavlja izvan snage.[169]

Uredba ima slične zahtjeve kao i Zakon o zaštiti osobnih podataka, osobni podaci moraju biti zaštićeni[170], sigurni[171], za njihovo prikupljanje mora se dobiti privole[172] i ista se može uskratiti[173]. Prilikom davanja privole osoba ima pravo na informiranje za što će se podaci koristiti i koje obrade će se obavljati.[174] Posebno je regulirana zaštita osobnih podataka maloljetnika za što je potrebna dozvola roditelja ili skrbnika.[175]

Pristup korištenju osobnih podataka nailazi na promjenu.[176] Na primjer odjel za ljudske resurse koji raspolaže osobnim podacima radnika treba zaštititi te podatke i koristiti ih isključivo za ono za što su namijenjeni. Ili, marketing koji prikuplja osobne podatke korisnika moraju točno odrediti koje podatke prikupljaju i zašto ih obrađuju.

Korištenje osobnih podataka mora prethodno biti dopušteno od strane građana EU. To je jednako kao u Zakonu o zaštititi osobnih podataka i naziva se privola.[177] Svaki građanin sam raspolaže svojim podacima i zbog toga ima pravo na informiranje za što će se njegovi

[167] ibid., Članak 18.
[168] ibid., Članak 27.
[169] UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (skraćeno: Opća uredba o zaštiti osobnih podataka (GDPR)). (27. 4. 2016.). (L 119/1), Službeni list Europske unije.
[170] ibid., Članak 25.
[171] ibid., Članak 32.
[172] ibid., Članak 6.
[173] ibid., Članak 7.
[174] ibid., Članak 5.
[175] ibid., Članak 8.
[176] ibid., Članak 5.
[177] ibid., Članak 7.

osobni podaci koristiti[178], ima pravo ispraviti osobne podatke ili zatražiti ispravak[179], uskratiti privolu[180], dopustiti preseljenje podataka[181] i ima pravo na zaborav[182].

Na primjer, web trgovac zatraži od korisnika dopuštenje za slanje informacija o popustima i pri tome jasno navede koje podatke treba, recimo ime, prezime, broj telefona i adresu elektroničke pošte. Popunjavanjem korisnik koji želi primati informacije o popustima označi kućicu koja označava da želi primati obavijesti. Trgovac je dužan u tom trenutku jasno naznačiti za što će koristiti korisnikove upisane podatke, kakve obrade će s njima raditi te koliko dugo će biti pohranjeni.[183] Korisnik u svakom trenutku ima pravo zatražiti od trgovca koje podatke posjeduje[184] i u svakom trenutku ima pravo uskratiti privolu. Uskratiti privolu znači da taj trgovac tom korisniku nema više pravo slati obavijesti.

Ili, drugi primjer, od web trgovca korisnik kupi proizvod i zatraži dostavu poštom. Za dostavu potrebno je popuniti određene podatke koji su osobni podaci kao što je ime, prezime, adresa, broj telefona i adresa elektroničke pošte. Ukoliko korisnik nije dao privolu za primanje bilo kakvih obavijesti, prema ovoj uredbi trgovac to ne smije učiniti. Dodatna mogućnost su podaci koji su prikupljeni za određenu svrhu mogu biti korišteni u drugačije svrhe. Kao u prethodnom primjeru podaci koji su prikupljeni radi slanja proizvoda poštom mogu biti korišteni za slanje reklamnih obavijesti. U tom slučaju uredba propisuje trgovcima prethodno obavještavanje korisnika te traženje njihove privole.[185]

Pravo na zaborav znači da tvrtka mora obrisati sve prikupljene osobne podatke.[186] Na primjer, web trgovac je prikupio osobne podatke radi određenih promocija. Korisnik koji ne želi primati podatke od trgovca, a nije više siguran u odobrenje za što se podaci mogu koristiti ima pravo zatražiti od trgovca „zaborav“ svih svojih podataka, odnosno brisanje podataka iz svih registara trgovca. Korisnik također ima pravo zatražiti od trgovca zabranu obrade[187] svojih podataka ili ograničiti obradu određenih podataka[188].

Pravo na preseljenje podataka je pravo građana da se svi osobni podaci prenesu na siguran način bez zadržavanja. Na primjer korisnik je s teleoperaterom sklopio ugovor. Nakon isteka ugovorenog roka korisnik ima pravo promijeniti teleoperatera zadržavajući pri tome

[178] ibid., Članak 5.
[179] ibid., Članak 16.
[180] ibid., Članak 7.
[181] ibid., Članak 20.
[182] ibid., Članak 17.
[183] ibid., Članak 18.
[184] ibid., Članak 12.
[185] ibid., Članak 13.
[186] ibid., Članak 17.
[187] ibid., Članak 9.
[188] ibid., Članak 18.

telefonski broj. U tom slučaju preseljenje podataka od jednog operatera drugome treba biti obavljen na siguran način i prvi teleoperater ne smije u svojim sustavima zadržati osobne podatke.

5.9. Zakon o pravu na pristup informacijama

Zakonom o pravu na pristup informacija uređuje pravo na pristup informacijama i ponovnu uporabu informacija koje posjeduju tijela javne vlasti, način rada i uvjete za imenovanje i razrješenje Povjerenika za informiranje te inspekcijski nadzor nad provedbom ovoga Zakona, a ne primjenjuju se na informacije za koje postoji obveza čuvanja tajnosti kao ni na informacije koje predstavljaju klasificirane informacije čiji su vlasnici međunarodne organizacije ili druge države, te klasificirane informacije tijela javne vlasti koje nastaju ili se razmjenjuju u okviru suradnje s međunarodnim organizacijama ili drugim državama.[189]

Informaciju zakon definira kao svaki podatak koji posjeduje tijelo javne vlasti u obliku dokumenta, zapisa, dosjea, registra, neovisno o načinu na koji je prikazan (napisani, nacrtani, tiskani, snimljeni, magnetni, optički, elektronički ili neki drugi zapis), koji je tijelo izradilo samo ili u suradnji s drugim tijelima ili dobilo od druge osobe, a nastao je u okviru djelokruga ili u vezi s organizacijom i radom tijela javne vlasti.[190]

Tijela javne vlasti imaju obavezu objavljivanja informacija na internetskim stanicama na lako pretraživ način[191]. Informacije koje su dužne na taj način objaviti odnose se na zakone i propise, opće akte i odluke, nacrte zakona i drugih propisa i akata, godišnje planove, izvještaje o radu, podatke o izvoru financiranja, informacije o unutarnjem ustrojstvu, zapisnike sa službenih sjednica, informacije o postupcima javne nabave, registre i baze podataka.[192] Navedene informacije objavljuje odlukom određena osoba, službenik za informiranje.[193]

Sve ostale informacije mogu se zatražiti službenim putem podnošenjem zahtjeva kojeg rješava službenik za informiranje tijela javne vlasti kojem je zahtjev podnesen.[194] Na izdano rješenje može se uputiti žalba koju rješava Povjerenik za informiranje kojem je obaveza

[189] Zakon o pravu na pristup informacija. (9. 8. 2015.). (NN 25/13, 85/15)., Članak 1.
[190] ibid., Članak 5.
[191] ibid., Članak 10.
[192] ibid., Članak 10.
[193] ibid., Članak 13.
[194] ibid., Članak 18.

pratiti, štititi i promicati pravo na pristup informacijama koje jamči Ustav Republike Hrvatske.[195]

Ponovna upotreba informacije odnosi se na upotrebu informacije tijela javne vlasti za svrhu koja je različita od izvorne svrhe za koju su informacije nastale.[196] „Na primjer, privatne ili pravne osobe mogu ponovno koristiti informacije dostupne u javnim bazama podataka kako bi izradile elektroničke proizvode koji će kasnije biti prodani kupcima – primjerice kombiniranjem različitih baza podataka o vremenskim statistikama i urbanom razvoju, neko trgovačko društvo može sačiniti program koji izračunava ekološke rizike koji postoje u pojedinim područjima.“[197]

5.10. Zaključak

Analizom zakonskog okvira može se uočiti zahtjev za vođenje arhivskih jedinica, odnosno dokumenata, u sređenom obliku što znači da je ono popisano prema određenim zahtijevanim podacima koji se nalaze na zaštitnom omotu. Radi postizanja autentičnosti ove podatke je u fazi prihvata dokumentacije moguće proširiti s navođenjem veličine dokumenta, označavanjem postojanja kritičnih elemenata kao što su pečat, potpis i slično. Pored ovih podataka vodi se i druga dokumentacija kao što je zapisnik o predaji gradiva u kojem se nalazi podatak o stvaratelju gradiva koji je važan za dokazivanje autentičnosti. Dodatni podaci se mogu dobiti korištenjem Opće međunarodne norme ISAD/G.

Osjetljivo gradivo se mikrofilmira i takvo daje na korištenje. Osim izrade mikrofilma Pravilnik o evidencijama u arhivima propisuje podatke koji se vode kada se obavi digitalizacija. Unutar ovih propisanih podataka traži se informacija o cjelovitosti snimanja koju bi trebalo detaljnije formulirati ili jednostavno proširiti ovaj popis kako bi zadovoljio zahtjeve za autentičnost. Zakon o knjižnicama i Zakon o muzejima također govore o zaštiti građe mikrofilmiranjem.

Zanimljiv je zahtjev Pravilnika o evidencijama u arhivima koji određuje kako se zapisi u Knjigu akvizicija i knjigu depozita ne smiju brisati već se ispravci vode tako da bude sačuvan raniji podatak. Ovakav pristup je dobro provesti u procesu digitalizacije kako bi se vidjeli koraci kontrole upisanih metapodataka odnosno kako bi se vidjelo da je upisivanje

[195] ibid., Članak 35.
[196] ibid., Članak 5.
[197] Ponovna uporaba informacija. (n.d.). Preuzeto 20. 1. 2018. iz Institut za javne financije: http://www.ijf.hr/hr/o-institutu/pravo-na-pristup-informacijama/652/ponovna-uporaba-informacija/673/

metapodataka nastalo u jednom neprekinutom ciklusu a proces kontrole nastao u drugom neprekinutom ciklusu.

Elektroničke zapise, kao što je digitalizirana slika, je moguće u bilo kojem trenutku u vremenu izmijeniti. Za dokazivanje autentičnosti potrebno je omogućiti provjeru tko je sliku izradio što se postiže elektroničkim potpisom koji koristi kvalificirani certifikat kojeg izdaje davatelj usluga izdavanja kvalificiranih certifikata. Dodatna prednost elektroničkog potpisa je izrada hash sadržaja, odnosno kriptografskog sažetka, kojim se potvrđuje nepromjenjivost digitalizirane slike. Potpisivanjem digitaliziranih slika u trenutku skeniranja omogućuje se potvrda tko je koristio skener i potvrda da sadržaj nije promijenjen.

Elektronička isprava također spominje osiguravanje identiteta stvaratelja, vjerodostojnost i vremenski podatak o stvaranju i slanju. Svaka radnja s elektroničkom ispravom treba biti označena jedinstvenom oznakom kojom se osigurava povezanost radnji unutar dokumentacijskog ciklusa. Podatak o stvaratelju treba biti poznat i zbog potrebe zadovoljenja Zakona o autorskom pravu i srodnim pravima te Opće uredbe o zaštiti podataka (GDPR). Među podacima kojima se opisuje digitalizirana slika mogu se naći informacije tijela javne vlasti za koje je potrebno ishoditi odobrenje od strane tijela javne vlasti.

6. NORME

Pored nacionalnog zakonodavstva koje se brine o očuvanju nastale dokumentacije provode se mnoge studije i izrađuju različiti propisi. Prepoznate norme, opisane u nastavku, odnose se na smještaj, čuvanje i rukovanje papirnate dokumentacije kako ne bi došlo do uništenja prije propisanog roka čuvanja, zatim na proces digitalizacije i uvjete za stvaranje digitalizirane slike te očuvanja digitalizirane slike na siguran način tijekom cijelog roka čuvanja. Digitalizirana slika gubi dio informacija koje papirnati dokument ima. Prepoznata norma koja govori o opisu arhivskog gradiva može pomoći kako bi se te informacije sačuvale jednom kada su prepoznate. Zbog dugoročnog očuvanja digitaliziranog gradiva koje se sastoji od digitalizirane slike i pripadajućih metapodataka važno je prepoznati kritične informacije te nad njima provesti sigurnosne mjere kakve su prepoznate u međunarodnoj normi informacijske sigurnosti.

6.1. HRN ISO 11799:2004

Norma HRN ISO 11799:2004 međunarodni je standard koji određuje karakteristike spremišta općenitog tipa koja se koriste za dugoročnu pohranu arhivskih i knjižničnih materijala.

Kako bi se osiguralo čuvanje dokumentacije tijekom cijelog propisanog roka, što zahtjeva Zakon o arhivskom gradivu i arhivima te u svojim prijedlozima naglašava norma ISO 15489-1:2001, te zadržala autentičnost gradiva koja uključuje cjelovitost gradiva, pored propisanih uputa, procedura i postupaka i zaduženog djelatnika koji je odgovoran za gradivo potrebno je osigurati prostor u kojem će se gradivo čuvati. Norma HRN ISO 11799:2004 daje dobre smjernice kojima se može postići visoki stupanj sigurnosti gradiva. Tako predlaže smjernice za zgradu, spremište, klimu i mikroklimu, instalacije i uređaje, sustav za gašenje požara, protuprovalni alarm, osvjetljenje, namještaj, čišćenje, zaštitu, smještaj, izložbe i plan za slučaj katastrofe.

Na papirnatu građu djeluje mnogo čimbenika, na primjer voda, vatra, rukovanje, svjetlost, temperatura, vlaga, štetne tvari u zraku, čađa, dim, prašina i način čišćenja odnosno održavanja građe. Norma postavlja različite zahtjeve koji se odnose na zgradu, spremišta u zgradi, instalacije kao što su struja, plin i voda, namještaj, kvaliteta zraka, utjecaj sunca i umjetnog svjetla, moguća mehanička oštećenja te što učiniti ukoliko do katastrofe ipak dođe.

Zgrada u kojoj se nalazi spremište ne bi smjela biti na tlu kojem prijeti propadanje, poplava, opasnost od potresa, plimnih valova, klizišta, požara, eksplozija susjednih zgrada. Također ne bi smjela biti u blizini mjesta ili zgrade koja privlači glodavce, kukce ili druge nametnike, tvornice ili instalacija koje emitiraju štetne plinove, dim, prašinu, zagađenih područja ni blizu strateških pozicija koje mogu biti ciljane u slučaju oružanih sukoba. Zgrada treba biti projektirana za odgovarajuću nosivost, što znači da treba biti unaprijed određeno koliko dokumentacije će biti spremljeno u svakom spremištu. Osiguranje od neovlaštenog ulaska se može provesti omogućavanjem ulaska posjetitelja samo na jedan ulaz a ostalim ulazima pristup bi trebao biti onemogućen.

Zgrada se sastoji od jednog ili više spremišta u kojoj se čuva dokumentacija. Spremišta trebaju biti u dobroj međusobnoj komunikaciji. Sustavi koji se odnose na vodu, plin i električnu energiju mogu biti unutar spremišta osim ukoliko je to nužno za funkcioniranje. Spremišta trebaju imati vatrodojavni i protuprovalni alarm. Nadzor rada i javljanja sustava treba biti centralizirano. Također je potrebno voditi računa o sunčevim zrakama i izloženosti sunčevih zraka i zaštititi prozore od ulaska sunčevih zraka, a umjetna svjetlost ne smije prelaziti 50 lux-a.

Za dobro održavanje papira važna je uloga mikroklime, prozračivanje, temperatura i vlaga. Mikroklima treba biti stabilna bez velikih varijacija a vlaga ne smije prelaziti 60% jer se tada razvija plijesan. Zbog toga treba voditi računa o postavljanju polica koja trebaju zaštititi papir od dodira, ne smiju biti blizu poda, stropa niti zidova jer oni imaju visok toplinski kapacitet.

Vatra je još jedan čimbenik koji utječe na papir. Gašenje požara treba biti osigurano pomoću sprinklera ili plina na odgovarajući način. Prostori spremišta trebaju biti podijeljeni na odjeljke koji su svaki posebna požarna zona čime se postiže efikasnost u očuvanju od požara i omogućuje se stabilna klima. Svaka požarna zona treba imati otpornost od minimalnih 2 sata. Vrata trebaju biti tako napravljena da se u slučaju požara sama zatvore, što se može postići s magnetnim držačima vrata.

Dim, čađa, štetne tvari i prašina također utječu na održavanje odnosno pospješuju propadanje papira. Zbog toga unutrašnjost spremišta kao i police trebaju biti napravljena od materijala koji ne ispuštaju, ne privlače i ne zadržavaju prašinu, koji u slučaju požara emitiraju minimalnu količinu dima, štetnih tvari i čađe.

Rukovanje dokumentacijom može dovesti do oštećenja. Police ne smiju imati oštre rubove, pri iznošenju građe iz hladnih u toplije prostore potrebno je građu aklimatizirati, položaj dokumentacije treba biti takav da ne stvara preveliki pritisak na primjer pritisak na

knjigu ili papir ne smije prelaziti 350 Pa. Pohrana dokumentacije treba biti u kutije koje nemaju plastične dijelove i koje ne emitiraju kisele ili štetne plinove. Sav materijal prije pohrane treba biti pregledan i u slučaju biološke zaraze dezinficiran. Dezinfekciju je u tom slučaju potrebno učiniti i sa policama i dokumentacijom koja je bila pored zaražene dokumentacije.

Sve se prostorije trebaju redovito čistiti sredstvima za čišćenje koja nisu štetna za pohranjen materijal. Čišćenje se obavlja korištenjem usisavača koji imaju filtere koji zadržavaju spore gljivica. Ukoliko se dokumentacija zarazi insektima potrebno ju je duboko zamrznuti. Za pregled dokumentacije potrebno je osigurati posebnu prostoriju, na taj način je moguće voditi brigu o tome tko dolazi u kontakt s kojom dokumentacijom.

Norma navodi detaljan popis zahtjeva koji se odnosi na za zgradu u kojoj se spremište nalazi, uvjeti za spremište, za postavljenu klimu, unutarnju strukturu i nosivost, za postavljene instalacije i korištene uređaje, sustav za gašenje požara, protuprovalni alarm, osvjetljenje, ventilaciju, kvalitetu zraka i klimu u prostoriji, karakteristike korištenog namještaja, način čišćenja, način zaštite dokumentacije i smještaja knjiga i velikih formata, kako postupiti u slučaju izložbi i u slučaju katastrofe.

6.2. ISO/TR 15801:2009

Tehnički izvještaj ISO/TR 15801:2009 opisuje implementaciju i operativnost sustava za upravljanje dokumentima (engl. Document Management System; skr. DMS) sustava za koji se može smatrati da pohranjuje elektroničke informacije na autentičan i vjerodostojan način, ali se ne odnosi na postupke kojima se ove informacije mogu smatrati autentičnim a odnose se na period prije pohrane u DMS. Puni naziv standarda je „Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost“. Ovaj tehnički izvještaj sustav od povjerenja (engl. trusted system) definira kao sustav za pohranu elektroničkih informacija na točan, pouzdan i upotrebljiv odnosno čitljiv način, osiguravajući integritet tijekom vremena.

Politika upravljanja dokumentima je način kojim organizacija ili tvrtka određuje način postupanja s informacijama i jasno određuje da su informacije koje se nalaze u DMS sustavu pouzdane, točne i od povjerenja. Sadržaj dokumenta u kojem je ovo propisano treba sadržavati: na koje se informacije odnosi, politiku medija za pohranu, politiku formata elektroničkih datoteka i kontrola verzija, politiku vezanu za primjenjive standarde upravljanja

dokumentima, vrijeme čuvanja i način uništavanja informacija, odgovornosti unutar sustava upravljanja dokumentima, odgovornosti nadgledanja i praćenja usklađenosti s ovim pravilima.

Ukoliko elektronički objekti postoje u različitim verzijama, svaka verzija bi se trebala promatrati kao zaseban izvorni ili originalni objekt. Način rukovanja s kopijama elektroničkih objekata se treba propisati u dokumentu o politici upravljanja dokumentima.

U dokumentu trebaju biti navedeni dopušteni formati datoteka kao i kompresijske tehnologije koje se mogu koristiti po svakom navedenom formatu. Ukoliko postoji više relevantnih verzija dokumenta potrebno je sve verzije pohraniti i očuvati vezu među njima.

Sustav za upravljanje dokumentima od povjerenja, prema tehničkom izvještaju, osigurava da se sve elektronički pohranjene informacije mogu smatrati pravom i točnom kopijom izvornih informacija, bez obzira na izvorni format i minimalno sadrži:

1. bar jedna kopija pohranjenih podataka je pohranjena na medij koji čuva pohranjeni podatak od izmjene, neprikladnih dodavanja ili brisanja tijekom životnog vijeka podataka, i čuva se i održava na sigurnoj lokaciji koja je odvojena od ostalih kopija pohranjenih informacija,
2. koristi se hardver i medij za pohranu koji štiti pohranjenu informaciju od izmjene, neprikladnih dodavanja ili brisanja tijekom životnog vijeka podataka,
3. mogućnost potvrđivanja od strane neovisne revizijske metodologije. Potvrđuje se kako se originalno pohranjene informacije mogu točno prikazati tijekom životnog vijeka. Provjerava se softver, hardver i mediji za pohranu.

Kako bi tvrtka pokazala pouzdanost i vjerodostojnost sustava za upravljanje dokumentima od povjerenja koristi se kombinacija organizacijskih pravila, operativnih postupaka i odgovarajuće instaliranih i upravljanih tehnologija. I zbog toga je potrebno: odrediti slijed odgovornosti i dodijeliti odgovornosti za aktivnosti koje uključuju upravljanje elektroničkim informacijama na svim razinama, imati pojam o zakonodavnim i regulatornim tijelima relevantnim za poslovanje, pridržavati se tehničkih, proceduralnih, regulatornih i zakonodavnih razvoja i promjena održavanjem kontakata s odgovarajućim tijelima i organizacijama, i provesti politiku informacijske sigurnosti. Kada je riječ o rolama potrebno je voditi računa da se razgraniči: priprema dokumentacije, kontrola kvalitete, unos podataka, brisanje i uništavanje informacije, informacijska sigurnost.

Ključni ciljevi informacijske sigurnosti su osigurati integritet pohranjenih informacija, dostupnost pohranjenih informacija i revizija provedbi postupaka i procedura od strane svih zaposlenika. U dokumentu se treba minimalno nalaziti: opseg na što se politika odnosi, izjava o ciljevima upravljanja u pogledu sigurnosti, specifičnosti politike, zahtjevi na različite

kategorije klasifikacije informacija, definiranje i dodjeljivanje odgovornosti za informacijsku sigurnost, politika za rješavanje kršenja sigurnosti, politika vezana za usklađenost s odgovarajućim standardima, procjena rizika (bazirano na vrijednosti imovine, ranjivosti sustava i vjerojatnosti napada) kao i mjere koje se poduzimaju i koje se provjeravaju na učinkovitost, plan nastavka poslovanja u slučaju nesretnih događaja.

Za svaki sustav za upravljanje dokumentima od povjerenja potrebno je održavati priručnik i/ili radne upute koje trebaju minimalno uključivati cjeline: snimanje informacija (engl. information capture), skeniranje, snimanje podataka, indeksiranje, procedure autentifikacije izlaza, prijenos datoteka, čuvanje dokumenata, čuvanje informacija, uništavanje informacija, pričuvna kopija (engl. backup) i oporavak sustava (engl. system recovery), održavanje sustava, sigurnost i zaštita, korištenje ugovornih usluga, tijek rada (engl. workflow), žigovi datuma i vremena, kontrola verzija, održavanje dokumentacije. Kako bi se osigurala usklađenost s propisanim procedurama, zaposlenike je potrebno educirati bilo kroz određene vježbe, tečajeve ili tijekom dnevno operativnog posla. Ukoliko dođe do promjena, što je normalno tijekom radnog vijeka, potrebno je evidentirati sve promjene i na što se promjene odnose, kao i jesu li promjene u skladu s politikom i operativnim zahtjevima koji su propisani. Sva dokumentacija se treba revidirati jednom godišnje ili češće, a reviziju je potrebno dokumentirati.

Elektronički dokumenti mogu biti stvoreni bilo procesom skeniranja, pri čemu nastaje digitalizirana slika, bilo izvorno u elektroničkom obliku. Oba elektronička objekta se mogu pohraniti u sustavu. Procedure kojima su stvoreni trebaju biti dokumentirane i mogu uključiti: snimanje elektroničkog dokumenta, priprema dokumenta, paketi dokumenata, fotokopiranje, skeniranje i kontrola kvalitete. Potrebno je napraviti procjenu mogućeg gubitka podataka i ukoliko određeni gubitak podataka nije prihvatljiv potrebno je definirati korake kako bi se informacija snimila i/ili zadržala. U svim slučajevima organizacija mora osigurati da je informacija ona za koju se misli da je, da nije bila mijenjana i da je identitet izvornika pravi. Unutar organizacije nije dovoljno smatrati da je dokument od povjerenja samim time što je nastao u nekom drugom dijelu organizacije.

Svaki elektronički dokument treba pratiti određeni skup metapodataka i zbog toga je potrebno voditi računa da su svi potrebni metapodaci snimljeni i proslijeđeni za što je nekada potrebno revidirati sadržaj i osigurati potpunost i prikladnost.

Kada elektronički dokument nastaje skeniranjem potrebno je dokumentirati procedure za: pripremu dokumenata, stvaranje paketa dokumenata, skeniranje i procesuiranje slike. U procesu pripreme dokumentacije potrebno je voditi računa o težini papira, veličini papira, boji

papira i tiska (crno-bijelo, boja, sivi ton), stanju papira (tanak papir, izgužvan, spajalice), papire koje je potrebno fotokopirati ili skenirati u posebnim košuljicama, ukoliko papiri imaju dodatno zalijepljene samoljepljive bilješke potrebno je propisati način rada u tim slučajevima (takav papir može sakriti određenu bitnu informaciju na dokumentu). Potrebno je dokumentirati način rada s više straničnim dokumentima pri čemu je potrebno voditi računa o izvornom redoslijedu, ili s dodacima na dokumentu kao što je bijela neprozirna boja koju je potrebno evidentirati. Dokumenti se mogu grupirati u pakete dokumenata pri čemu se vodi računa što predstavlja paket, na primjer ukoliko u jednom registratoru ima 100 dokumenata, to se može smatrati paketom, ukoliko registrator ima 10 dokumenata, 10 registratora se može smatrati paketom i na taj način pripremiti. Način pripreme paketa se treba dokumentirati. Oštećena ili osjetljiva dokumentacija se može tijekom procesa skeniranja uništiti, dokumenti koji imaju izraziti kontrast mogu u paketu biti skenirani i izgubiti podatke, kao i dokumenti koji imaju tisak ili tintu takvu da se informacije tijekom skeniranja mogu izgubiti ili postoje dokumenti koji su preveliki za skener, u svim ovim slučajevima dokumente je potrebno prethodno fotokopirati pazeći da ne nastane gubitak informacija. Ukoliko se napravi fotokopija, potrebno je to naznačiti kako bi korisnik imao takvu informaciju prilikom pregleda dokumenta. To se može postići označavanjem u procesu pripreme oznakom da je nastao fotokopiranjem ili da je stigao u proces pripreme kao fotokopija. Proceduru je potrebno dokumentirati.

Proces skeniranja je potrebno propisati. Pri tome se vodi računa radi li se o obostranom ili jednostranom skeniranju, skeniranju u boji ili bitonalno, kako se osigurava da su svi dokumenti u paketu skenirani, na primjer usporedbom broja skeniranih slika s brojem dokumenata u paketu ukoliko je poznat. Za osiguranje skeniranja svih dokumenata u paketu izrađuje se analiza rizika i pronalazi se procedura za koju je rizik prihvatljivo malen. Mnogi skeneri mogu provjeravati dupli ulazak dokumenta ili se može prethodno numerirati stranice u paketu ili se može koristiti tehnika duplog skeniranja. Ukoliko se skenira skenerom koji može snimati samo jednu stranu papira, potrebno je osigurati procedure snimanja i druge strane kada je to potrebno. Veliki papiri koji se skeniraju u dijelovima trebaju se skenirati tako da dođe do preklapanja kako bi se osiguralo da je sve skenirano. Svaki digitalizirani dokument treba dobiti svoj jedinstveni broj, najbolje sistemski stvoren, kako bi se osiguralo da ne dođe do neželjenog prepisivanja dva dokumenta.

Kako bi se osigurala kvaliteta skeniranja potrebno je obavljati kontrolu kvalitete jer se time lakše dokazuje autentičnost. Kontrolom kvalitete se provjerava jesu li slike odgovarajuće kvalitete i je li skener radio unutar dogovorenih standarda. Prije početka procesa skeniranja

potrebno je napraviti test kvalitete kojim se određeni reprezentativni skup dokumenata pripremi i skenira. Ovaj skup dokumenata treba sadržavati dokumente koji su slabije kvalitete u odnosu na većinu dokumenata. Prilikom kontrole potrebno je voditi računa: o čitljivosti cijelog dokumenta, da je i najmanji detalj čitljiv, o cjelovitosti detalja na dokumentu, o točnosti dimenzija u odnosu na izvornik, stvara li skener mrlje koje ne postoje na dokumentu (engl. speckle), o potpunosti cjelokupne slike (nedostaju li informacije koje su na rubovima), o gustoći punih crnih područja i o vjernost boje (engl. color fidelity). Nakon provedene kontrole na testnom skupu, potrebno je evidentirati rezultate. Tijekom procjene kvalitete u procesu kontrole potrebno je voditi računa o karakteristikama skenera, rezoluciji printera i preciznosti reprodukcije sive skale ili boje, a rezultate procjene evidentirati. Količina digitaliziranih slika koju je potrebno provjeriti na početku je veća, na primjer 20%, što se smanjuje ukoliko se tijekom kontrole kvalitete pokazala konzistentnost kvalitete. Postotak kontrole može se smanjiti na 5% ukupne količine.

Potrebno je kontrolirati rad skenera kako bi se pokazalo da se nalazi unutar dogovorenog odstupanja. Ova kontrola se može obaviti pomoću testnih uzoraka opisanih u standardu ISO 12653-2. Također potrebno je pratiti preporuke proizvođača. Ovaj testni uzorak se ne smije zamijeniti s testiranjem rada sustava na testnom skupu dokumenata.

Procedure ponovnog skeniranja dokumenta je potrebno opisati i dokumentirati i prilikom ponovnog skeniranja potrebno je osigurati da se prethodno skeniran dokument neprihvatljive kvalitete ispravno zamijeni novim. Moguće je raditi postupke kojima se poboljšava kvaliteta slike, i ti se postupci trebaju evidentirati, a ponekad je potrebno pohraniti izvorni digitalizirani dokument kao i dokument dobiven poboljšanjima, te poveznicu između njih.

Podaci koji su povezani s dokumentom mogu se zapisati bilo ručnim unosom (unosom s tipkovnice), bilo automatskim unosom (čitanjem barkoda, OCR-a) ili polu-automatski (čitanjem OCR-a te provjerom od strane operatera). U svakom slučaju postotak unosa je rijetko a ponekad i nemoguće osigurati u potpunosti, i zbog toga je potrebno obaviti procjenu rizika te obavijestiti korisnika o tome. Kako bi se osigurao dogovoreni nivo preciznosti moguće je slučajnim odabirom napraviti kontrolu na određenom paketu, te ukoliko ne zadovoljava ponavlja se unos podataka. Rezultati provjere se trebaju dokumentirati.

Tijekom konverzije i migracije podataka moguće je izgubiti određene podatke, te je potrebno propisati procedure kojima će se to spriječiti, a kada nije moguće spriječiti gubitak, potrebno je zapisati informacije o gubicima. Neki sustavi trebaju periodično obnoviti svoje indekse što treba detaljno propisati i evidentirati.

Dokumenti koji se nalaze u sustavu od povjerenja, za potrebe dokumentarnih dokaza, ispisuju se na papir uz potvrdu od strane ovlaštene osobe da se radi o autentičnoj kopiji. Pri tome se može dogoditi da dođe do gubitka boje (ispis dokumenta u boji na pisaču koji ne podržava ispis u boji), gubitka rezolucije (može dovesti do gubitka informacije vitalne za taj dokument), ili gubitka formata odnosno forme. Ove situacije mogu biti ne prihvatljive za određene dokumente pa je potrebno voditi računa da su pohranjene sve relevantne informacije kako bi se dobila tražena kvaliteta preslike originala (na primjer font se može promijeniti, pri čemu je potrebno evidentirati ovu promjenu).

Tijekom životnog ciklusa dokument je moguće prenositi putem unutarnjih mreža (engl. local area network), unutar hijerarhijske baze podataka ili između podsustava kojima upravlja operater, ali i izvan organizacije prema trećim stranama. Procedure i procese je potrebno osmisliti i dokumentirati kako bi se osigurao integritet prenesenih datoteka. Kada se datoteke šalju trećoj strani potrebno je osigurati da nije došlo do promjene tijekom prijenosa trećoj strani, i da nije došlo do promjene tijekom slanja od strane treće strane. Tom prilikom je potrebno voditi revizijski tijek koji zapisuje vremena slanja, kao i informacije o potvrdi prihvata datoteke od strane treće strane i korisnika koje uključuju i datum i vrijeme prihvata datoteke.

Ponekad je potrebno osigurati da se originalni papir ne uništi, na primjer: dokument je slabe kvalitete takve da se u procesu skeniranja neće dobiti čitljivi podaci, ili potrebo je osigurati da se čitljivost nije namjerno onemogućila, dokument sadrži dodatke koji se ne mogu ispravno prikazati kao slika, u tijeku je procedura dokazivanja originalnih dokumenata, dokument je velike vrijednosti kao što je to ugovor na veliki iznos. U tim slučajevima je potrebno čuvati originalni dokument, a proceduru za ove slučajeve je potrebno propisati i evidentirati.

Potrebno je planirati migracijske procedure za dokumente kojima neće isteći rok čuvanja.

Potrebno je propisati uništavanje dokumenata nakon pohrane digitaliziranih dokumenata na sustav za pohranu i stvaranja sigurnosnih kopija. Dokumentaciju o uništavanju je potrebno evidentirati i čuvati.

Prilikom izrade pričuvnih kopija (engl. backup) rade se najmanje dvije ažurne pričuvne kopije za slučaj gubitka ili uništenja dijelova podataka. Kada se rade pričuvne kopije produkcijskih podataka potrebno je voditi računa da se kopiraju svi potrebni podaci iz kojih se može pokrenuti produkcija u slučaju havarije. Ove procedure se trebaju evidentirati, kontrolirati i testirati na pouzdanost. Ove se kopije mogu koristiti i prilikom dokazivanja

autentičnosti produkcijskih podataka. Sustav treba u redovnim intervalima obaviti verifikaciju svih datoteka i povezanih podataka, uključujući revizijske podatke. Aktivnost izrade pričuvnih kopija također treba biti zapisana u revizijskom tragu koji treba uključiti sve probleme koji su se pojavili prilikom izrade kopija. Ukoliko dođe do havarije i sustav se pokreće iz pričuvnih kopija potrebno je dokumentirati cijeli proces posebno vodeći računa da integritet podataka nije narušen. Pričuvni podaci se trebaju redovito testirati koristeći različite čitače podataka. Jedan od načina kojim se može postići zaštita podataka je pohrana pričuvnih kopija kod treće strane od povjerenja (koji pokazuju učinkovitost i sigurnost svojih usluga).

Sustav za upravljanje dokumentima od povjerenja je potrebno redovito održavati. Održavanje trebaju obavljati samo kvalificirani i educirani stručnjaci. Trebaju se voditi zapisnici o održavanju i svim zahvatima koji su napravljeni. Redovito se trebaju provoditi preventivna održavanja prema preporukama proizvođača. Trebaju se voditi zapisnici o preventivnim održavanjima. Procedure kojima se zaobilaze kontrole sustava za pristup je potrebno dokumentirati i pristup takvim alatima se treba strogo nadzirati. Nakon obavljenih održavanja skenera potrebno je provjeriti da je sustav na propisanom nivou kvalitete.

Kako bi se ostvarila sigurnost potrebno je kontrolirati pristup različitim nivoima sustava. Pohrana, označavanje, rukovanje, transport i održavanje medija za pohranu se trebaju obavljati u skladu s preporukama proizvođača, ili relevantnih nacionalnih ili internacionalnih standarda. Centralni sustav treba biti smješten u sigurnosnim zonama s dokumentiranim i ograničenim pristupom. Kako bi se poboljšala sigurnost pohranjenih podataka mogu se koristiti enkripcijske tehnike. Kada se ovim tehnikama kriptiraju podaci koji se čuvaju na duži period potrebno je voditi računa o isteku certifikata ili nedostupnosti certifikata. Potrebno je osigurati kontinuiranost procesa kriptiranja i u slučaju kada zaposlenik koji je dogovoran za održavanje ključeva prestane raditi na tom poslu.

Moguće je neki od ovih procesa (skeniranje, indeksiranje, pretvorba podataka, pohrana, i tako dalje) predati trećoj strani. U tom slučaju treća strana treba osigurati autentičnost koju kontrolira korisnik na način da se ne pretpostavlja da bilo koji dio usluge zadovoljava kompletnost, kvalitetu i preciznost obavljene usluge. Korisnik treba voditi svu dokumentaciju vezanu za prijevoz ili prijenos podataka do treće strane kao i svu dokumentaciju koja je u sukladnosti s politikom upravljanja dokumentima (posebno se treba voditi zapisnik o podacima: vrijeme i datum predaje, popis što je predano, vrijeme i datum preuzimanja i popis-kontrola što je preuzeto). Procedure koje je potrebno ugraditi i revidirati, u slučaju rada s trećom stranu, a koje moraju biti navedene u ugovoru ovisno o usluzi, su:

- je li usluga u skladu s dogovorenim i prihvatljivim standardima kvalitete,

- može li se obraditi testni skup dokumenata, isporučiti na traženom mediju i u traženom formatu te može li se učitati u sustav klijenta,
- može li treća strana dostaviti kopiju revizijskog traga obrade, u čitljivom obliku,
- je su li indeksni podaci zadovoljavajuće precizni, prihvatljivi i dokumentirani,
- zadovoljava li mjesto rada sigurnosne kriterije primjerene potrebama klijenta,
- je li postupci i procesi koje treća strana obavlja ne uključuju veći rizik oštećenja materijala klijenta,
- provode li se učinkoviti postupci otkrivanja i sprječavanja požara na mjestu gdje se obavlja obrada dokumentacije,
- na koji se način osigurava povjerljivost podataka u smislu radnika koji rade na obradi podataka, na primjer mogu svi zaposlenici potpisati ugovor o povjerljivosti,
- dogovoriti dostupnost dokumenata koji se skeniraju za slučaj potreba klijenta.

Ukoliko se koristi sistemsko vrijeme i datum potrebno je redovito testirati preciznost, voditi računa o promjeni vremena ovisno o dnevnom računanju vremena (ljetno i zimsko računanje). Samo ovlašteni radnici smiju mijenjati i održavati sistemsko vrijeme prema propisanim procedurama, sve izmjene se trebaju evidentirati i sve greške se trebaju evidentirati.

Sva dokumentacija je podložna izmjenama, zbog toga je potrebno voditi računa o propisanom označavanju verzija kao i o načinu čuvanja svih verzija barem onoliko dugo koliko se čuvaju podaci na koje se ta dokumentacija odnosi. Na primjer, ukoliko nisu poznate procedure za skeniranje kojima su nastali dokumenti prije nekoliko godina i nisu poznate procedure za pohranu nastalih digitaliziranih slika i godinama koje su slijedile, tada je upitno ili nemoguće odbaciti sumnju na autentičnost i integritet tih podataka. Sve procedure (uključujući i revizijske procedure i postupke) koje se odnose na očuvanje ažurnosti dokumentacije trebaju biti dokumentirane i trebaju se čuvati.

Opis hardvera i softvera kao i mrežnih elemenata od kojih se sastoji sustav, sve konfiguracije sustava i sve promjene sustava trebaju biti dokumentirani. Za svaku promjenu potrebno je napraviti novu verziju uputa kako bi se točno znalo kako je izgledao sustav u svakoj točki vremena. Sustavi koji koriste pohranu preko mreže ne mogu u potpunosti osigurati neautorizirane izmjene. Međutim, kada se koriste magnetne trake, ili drugi serijski zapisi, puno je teže napraviti promjene, jer je potrebno kopirati sve zapise koji se nalaze nakon promijenjenih zapisa. Ukoliko se traka nalazi van mreže tada je moguće napraviti izmjene bez autorizacije pa je potrebno voditi računa o fizičkoj sigurnosti medija. Potrebno je

dokumentirati točku u procesu kada se pristupa zapisu elektroničkih datoteka sa medija za pohranu.

Svi pristupni nivoi: upravljanje sustava, administracija sustava, održavanje sustava, autori podataka, pohrana podataka, indeksiranje podataka, dohvat podataka, trebaju biti dokumentirani i strogo odijeljeni i dodijeljeni osobama koje zadovolje potrebne kompetentnosti.

Kako bi se osigurao i očuvao integritet pohranjenih informacija može se napraviti kontrolni zbroj (engl. checksum) podataka koji su pohranjeni u trenutku pohrane. Međutim ova metoda ne garantira integritet podataka sve do trenutka pohrane. Tome se može doskočiti izradom kontrolnog zbroja prilikom skeniranja, te zapisivanjem u revizijski trag, i potom usporedbom podataka iz revizijskog traga i podataka dobivenih u trenutku pohrane.

Digitalni i elektronički potpisi omogućuju dokaz je li pohranjena datoteka zaista ona koja je originalno poslana. U ovom slučaju potrebno je voditi računa o pohrani digitalnih potpisa, načinu pristupa potpisanim datotekama, ključevima i algoritmima. Elektronički potpisi trebaju sadržavati kontrolni zbroj datoteke ili hash vrijednost datoteke. Proces je potrebno dokumentirati.

Prilikom skeniranja mogu se obaviti razne izmjene odnosno poboljšanja dobivenih slika, kao što su: poravnanje (engl. de-skew), brisanje pozadinskih točaka (engl. de-speckle), brisanje crnih rubova (engl. black border removal) i brisanje formi (engl. form removal). Ove funkcije se trebaju pažljivo koristiti vodeći računa da se ne izgube vrijedni podaci. Na primjer brisanje pozadinskih točaka može obrisati decimalnu točku ili neki drugi važan podatak. Zato je potrebno napraviti test, i rezultat tog testa dokumentirati. Sve promjene koje se naprave na datotekama koristeći poboljšanja je potrebno dokumentirati. Konverziju sive skale ili boje u crno-bijeli ton također treba testirati u smislu prihvatljivosti. Nekada je jednostavnije pohraniti originalno dobivenu sliku bez poboljšanja, te pohraniti sliku nakon poboljšanja.

Određene kompresijske tehnike također mogu dovesti do gubitaka podataka. Postoje dvije vrste kompresijskih tehnika, kompresija bez gubitaka podataka i kompresija s gubitkom podataka. Bez obzira koja je tehnika korištena treba biti evidentirana uključujući i korišteni algoritam i omjer kompresije. Na primjer, radiografije (medicinske snimke) nije dobro komprimirati korištenjem algoritama s gubitkom podataka.

Postoje određene tehnike kojima se uklanja forma dokumenta te se posebno zapisuje forma a posebno podaci. Autentičnost podataka dobivenih spajanjem forme i podataka se ne može potvrditi zbog različitih kritičnih situacija, na primjer forma prelazi preko podataka. U

tom slučaju je bolje original mikrofilmirati ili pohraniti kompletnu sliku čime se dokazuje autentičnost.

Migracijske procedure kao i procedure brisanja trebaju biti pažljivo propisane i dokumentirane. U slučaju migracije može doći do promjene medija za pohranu kao i hardvera i softvera kojima se pristupa podacima na tim medijima. Zato je dobro koristiti industrijske standarde za medije za pohranu, sačuvati preglednike podataka za pohranjene podatke, osigurati da se datoteke, indeksni podaci kao i revizijski tragovi migriraju na novu tehnologiju bez gubitka podataka. Sve je potrebno strogo evidentirati kako bi se pokazao integritet pohranjenih podataka u bilo kojem trenutku. Brisanje podataka treba proći revizijski proces koji uključuje potrebne potvrde prije brisanja podataka. Ukoliko je brisanje podložno zakonskim procedurama i zahtjevima, potrebno je pohraniti potvrde i podatke kojima se pokazuje kako su ti zahtjevi i procedure bile zadovoljene.

Revizijskim tragovima se stvaraju povijesni zapisnici svih značajnih događaja povezanih s pohranjenim podacima u sustavu za upravljanje dokumentima od povjerenja a koji bi u budućnosti mogli biti potrebni kako bi se rekonstruirale aktivnosti i događaji provedeni nad pohranjenim podacima. Najčešće su to podaci dobiveni od sustava i od operatera. Najbolje je kada su podaci dobiveni automatskim zapisivanjem od strane sustava, međutim kada su dobiveni ručnim unošenjem trebaju biti strogo propisani. Svaki zapis mora imati pridruženo vrijeme i datum događaja koji se pohranjuje. Zapise je potrebno unositi odmah nakon događaja, u slučaju automatskog zapisivanja, ili čim je prije moguće, u slučaju ručnog unošenja. Na primjer, u zapis kada je operater počeo raditi upisuje se vrijeme netom prije početka rada, u zapis kada je operater započeo pripremu paketa dokumenata upisuje se vrijeme netom prije početka pripreme paketa. Pri tom je dobro voditi računa da se upisuje vrijeme od povjerenja. Revizijski tragovi se trebaju čuvati minimalno koliko i informacije na koje se odnose. Potrebno je propisati način pristupa ovim podacima i osigurati pristup vanjskim nezavisnim revizorima koji nemaju pojam o sustavu. Nivo sigurnosti mora biti takav da sprječava svaku promjenu što se može postići čuvanjem sigurnosnih kopija. Revizijski tragovi u elektroničkom obliku se mogu pohraniti na magnetne trake. Kako je zapis na magnetnim trakama sekvencijalan postoji velika vjerojatnost da zapisi nisu mijenjani. Revizijski tragovi na papiru se mogu skenirati i skenirane kopije se mogu pohraniti na sustavu od povjerenja. Svi revizijski tragovi sustava moraju omogućiti utvrđivanja o kojem se procesu radi i datum i vrijeme događaja. Može biti ne praktično zapisivati ove podatke na nivou svakog papira, na primjer tijekom pripreme paketa dokumenata, stoga je dovoljno zapisati vrijeme početka i završetka pripreme tog paketa te ime operatera koji je pripremao paket.

Revizijske informacije procesa skeniranja mogu biti od značaja za dokazivanje autentičnosti pohranjenih podataka. Slijedeći popis je sažeti popis podataka koje Norma navodi kao najčešće zapisivane podatke:

1. općeniti podaci:
    a. identifikator datoteke,
    b. datum i vrijeme procesa,
    c. identifikator paketa,
    d. broj stranica,
    e. odobrenje kontrole kvalitete,
    f. identifikator svake datoteke koja je indeksirana,
    g. identifikator operatera ili radne stanice,
    h. konačni zapis na pohranu,
2. informacije o datoteci:
    a. jedinstvena oznaka,
    b. broj dokumenata/stranica u datoteci,
    c. veličina datoteke (npr. u kilobajtima),
    d. format datoteke,
    e. kod datoteke (npr. EDI vrijednosti, DTD i slično),
3. informacije o skeniranim dokumentima:
    a. jedinstveni interni identifikator datoteke,
    b. broj stranica slika koje su skenirane,
    c. broj stranica koje su poslane u sustav pohrane,
4. informacije o paketima dokumenata:
    a. jedinstvena oznaka paketa,
    b. identifikator operatera,
    c. vrsta skeniranog materijala (na primjer papir, mikrofilm),
    d. količina dokumenata u paketu (na primjer broj stranica (uključene obje strane), broj stranica s mikrofilma),
    e. detalji obrade slike ukoliko se razlikuju od onih koji su propisane,
5. informacije o indeksiranju:
    a. datum i vrijeme stvaranja indeksnih datoteka,
    b. datum i vrijeme svih dodavanja u indeksnu datoteku,
    c. datum i vrijeme brisanja indeksnih datoteka,
    d. podatak o indeksnim pojmovima koji su povezani s obrisanom datotekom,

e. identifikator dokumenta, datoteke, slike koja se briše,

6. informacije o promjenama:
    a. vrsta promjene,
    b. ime osobe ili program koji je napravio promjenu,
    c. poveznica na prethodnu verziju informacije (gdje je prikladno),
7. informacije o digitalnim potpisima:
    a. identifikator datoteke,
    b. identifikator certifikata,
    c. identifikacija izdavatelja certifikata,
    d. datumski i vremenski potpis,
    e. potvrda slanja,
    f. potvrda primanja,
    g. dokaz valjanosti,
8. informacije o uništavanju:
    a. podaci o uništenju nakon procesa skeniranja,
    b. podaci o uništenju nakon isteka roka čuvanja,
    c. podaci o autorizaciji uništavanja.

Slijedi još nekoliko načina koje norma predlaže za postizanje visokog stupnja povjerenja u autentičnost digitalizirane slike:

- slike su visoke kvalitete,
- postoje dokazi da je skener u fazi obrade radio prema propisanim standardima,
- indeksni podaci o slici su relevantni i potpuni,
- ukoliko postoji originalni dokument moguće ga je lako pronaći,
- postoje dokazi koji potvrđuju da pričuvna kopija nije kompromitirana (predlaže se napraviti kopiju samo za slučaj pokazivanja autentičnosti),
- struktura pričuvnih kopija je propisana uputom,
- ukoliko se pričuvna kopija predaje trećoj strani za sigurnosno čuvanje prijenos je obavljen fizički ili elektronički uz korištenje mjera sigurnosti i o tome postoje dokazi,
- korištenje vremena od povjerenja za izradu elektroničkih vremenskih žigova je dokumentirano,
- kada se radi o pouzdanosti ispisa dokumenata iz sustava od povjerenja preporuča se dokumentirana provjera u kojoj je reprezentativni skup dokumenata nakon digitalizacije ispisan na pisaču i uspoređen s izvornicima,

- ukoliko je korištena funkcija brisanja pozadinskih točaka kako bi se poboljšala slika potrebno je voditi računa da nije došlo do brisanja podataka zbog primjerice već oštećenih znakova, uskličnika ili dijelova finih detalja unutar crteža,
- postoje dokumentirane procedure postupanja s datotekom u koju se upisuje revizijski trag za situaciju kada ta datoteka bude puna,
- podaci o revizijskom tragu preporučuju se zapisati na WORM (engl. write once read many) medij, a za slučaj da se zapisuju na medij s višestrukim snimanjem (engl. rewritable media) postoje procedure koje onemogućavaju mijenjanje,
- u revizijski trag se zapisuju podaci o vremenu snimanja (engl. capture time) odnosno digitalizacije, imenu operatera, podaci o skeneru i vrsti originala.

6.3. ISO/TR 13028:2010

Tehnički izvještaj ISO/TR 13028:2010 govori o konverziji papira, odnosno ne digitalnih zapisa, u digitalne zapise. Prilikom konverzije stvaraju se statičke slike u točkama (engl. pixel) ili se obrađuju tehnologijom optičkog prepoznavanja znakova (engl. Optical Character Recognition, skr. OCR) koji točke pretvaraju u digitalne reprezentacije i time slike postaju pretražive, promjenjive ili oboje.

Norma govori o izradi glavnih kopija i izvedenih kopija iz glavnih kopija, u kojem slučaju se glavne kopije čuvaju na odvojenom sigurnom spremištu, a izvedene kopije koriste gdje je potrebno. Međutim ovo nije obaveza ukoliko je digitalizirani zapis korišten za donošenje poslovnih odluka, dokaz za poslovne aktivnosti ili sudjeluje kao potporni referentni materijal.

Cijeli proces digitalizacije bi trebao biti planiran, određen i dokumentiran. Dokumentacija bi trebala uključiti opseg poslovanja na koji se odnosi uključivši i ograničenja, cilj i očekivano korištenje digitaliziranog materijala, prednosti, korištenje, pristup, format, rezoluciju, dubinu bita slike, kompresije, metapodatke koji će biti zapisani, potrebne uređaje, kontrole procesa digitalizacije prije, tijekom i nakon digitalizacije, kontrole kvalitete, strategije integracije digitaliziranih slika u poslovne procese, strategije održavanja digitaliziranih slika i fizičkih izvornih dokumenata te zakonski okvir.

Općeniti zahtjevi koje tehnički izvještaj navodi s obzirom da se tehničke mogućnosti uređaja neprestano mijenjaju i povećavaju:

- tehničke specifikacije koje omogućavaju najveću kvalitetu,

- formati bi trebali biti otvorenog izvora (engl. open source), ili koristiti otvorene standarde (engl. open standards), javno dostupne tehničke standarde za formate, ili one formate koji su u širokoj upotrebi relevantnog sektora,
- formati ne bi smjeli uključivati ugniježđene objekte kao ni poveznice na druge objekte,
- formate bi trebale podržavati mnoge softverske aplikacije,
- formati bi se trebali moći čitati koristeći dostupne dodatke programima (engl. plug-in),
- podrška bi trebala doći od strane nezavisnih stručnjaka (neovisnih o proizvođačima),
- tehnička podrška bi trebala neprestano održavati sustav i migraciju,
- glavne kopije bi se trebale izraditi koristeći najviše tehničke standarde,
- glavne kopije bi se trebale držati na neovisnim sustavima pohrane,
- izvedene kopije mogu biti u formatima koji su najprilagođeniji poslovnoj upotrebi.

Ukoliko se koriste mogućnosti skenerskog softvera za poboljšanje slike trebalo bi se dobro dokumentirati ovo korištenje, jer na primjer oštrenje slike, izrezivanje dijelova sjena (engl. clipping), zamućivanje, uklanjanje mrlja i točkica mogu promijeniti sliku na način da ne odgovara izvorniku. Ukoliko se na digitaliziranu sliku dodaju poruke, bojom označi tekst, dodaju pečati i slično tada oni moraju biti prikačeni kao sloj koji prekriva sliku (engl. overlay) koji ne utječe na samu digitaliziranu sliku i prilikom ispisa na papir ovi dodaci se mogu ispisati a i ne moraju.

Analizom dokumentacije može se zaključiti da boja ne utječe na samu informaciju koju dokument prenosi i u tom slučaju se može napraviti slika u crno-bijelom tonu ili u sivoj skali. Zbog ovakvih primjera potrebno je napraviti i dokumentirati analizu dokumentacije koja će biti digitalizirana.

Prilikom procesa pripreme potrebno je voditi računa o:

- kvaliteti papira i stanju papira,
- različitim veličinama papira i kako utječe na proces digitalizacije, uključujući i kontrolu kvalitete da nije došlo do gubitka informacija,
- metodama koje vode računa o ručnim zabilješkama, bijelim korekturnim dijelovima, samoljepljivim trakama ili drugim bojom označenim dijelovima,
- metodama koje razlikuju original i fotokopiju,
- upute za materijal koji se neće digitalizirati,
- upute o čišćenju dokumentacije od klamerica, spajalica, kako pravilno poravnati dokumentaciju, o količini papira u jednom paketu,

- upute o tome što čini cjelinu jednog dokumenta (na primjer obostrano ispisan papir, samoljepljivi dodaci i slično),
- poveznice izvornih dokumenata s digitaliziranim dokumentima,
- procedure koje omogućavaju provjeru i verifikaciju da je sva dokumentacija digitalizirana,
- principe kojima se vodi a odnose se na grupiranje sličnih vrsta dokumenata (boja, veličina, redoslijed datuma, formati, orijentacija, jednostrano, obostrano).

Metapodaci koji će se spremati uglavnom se mogu grupirati u dvije grupe: oni koji se odnose na pojedinu sliku i proces digitalizacije i oni koji se odnose na zapise koje prenose poslovne informacije. U svakom slučaju potrebno je svesti na najmanju moguću mjeru ručni unos. Metapodaci se mogu upisati u samu sliku ili u zasebni sustav pri čemu je potrebno voditi računa da postoji poveznica između slike i sustava na kojem se nalaze metapodaci. Automatski se mogu upisati slijedeći podaci:

- jedinstvena oznaka slike,
- datum i vrijeme digitalizacije,
- ime osobe koja je obavila digitalizaciju,
- naziv uređaja koji je digitalizirao uključujući i naziv softvera,
- datum zadnje kalibracije uređaja.

Kontrola kvalitete je bitni čimbenik u dokazivanju da je digitalna slika autentični reprezentant izvornog dokumenta. Zbog toga je potrebno dobro propisati i dokumentirati proces kontrole kvalitete, koja minimalno treba uključiti:

- prihvatljiva odstupanja od normalnog procesa,
- kontrolu kvalitete skenera,
- verifikaciju da je izlazna količina jednaka ulaznoj,
- opseg i učestalost uzorkovanja digitaliziranih slika,
- kriterije provjere kvalitete slike,
- kriterije i frekvenciju provjere metapodataka,
- proces ponavljanja digitalizacije,
- obuku operatera.

Nakon obavljene digitalizacije trebaju postojati dokumentirane upute i procesi koji se odnose na održavanje sustava, migracije, procedure rada s pričuvnim kopijama, uništenje dokumentacije u digitalnom obliku i u fizičkom obliku – odnosno originala.

Dodatak C tehničkog izvještaja govori o preporukama imena datoteka koje je potrebno definirati prije početka digitalizacije. Općeniti zahtjevi za nazivima datoteka su:

- jedinstvenost,
- konzistentne strukture,
- vodi se računa o veličini brojčanika koji treba odgovarati maksimalnoj količini originala,
- trebaju se koristiti vodeće nule za lakše sortiranje,
- izbjegavaju se prazna mjesta a kao alternativa koristi se „_“,
- izbjegavaju se kompleksna imena zbog mogućnost ljudske pogreške,
- ograničena duljina je 30 znakova zbog mogućih problema prilikom migracije,
- koriste se mala slova i ekstenzije datoteka,
- koriste se brojevi i slova ali ne i ostali znakovi,
- metapodaci se zapisuju dodatno pored upisa u samu sliku.

Organizacija digitaliziranih slika i mapa u kojima se nalaze može predstavljati reprezentaciju stvarne strukture originalne dokumentacije.

Također, od glavne slike moguće je napraviti različite verzije s različitima obradama na pojedinoj slici. Ukoliko je to slučaj sve obrade i verzije je potrebno zapisati, a ukoliko je moguće ove promjene je dobro upisati i u samo ime datoteke.

Dodatak D daje preporuke za kontrolu kvalitete i obraća se pažnja na skener, količinu dokumenata te kontrola uzorka. Skenere je potrebno periodički testirati na performanse i provjeriti je li zadovoljavaju dozvoljene tolerancije. Uređaji bi trebali zapisivati količinu dokumenata i količinu dokumenata unutar jednog skupa dokumenata. Frekvencija kontrole stanja uređaja treba odgovarati preporukama proizvođača. U početku se može raditi kontrola uređaja pomoću testnog ciljanog dokumenta (engl. target) (prema ISO 12653-1, ISO 12653-2, ISO 12641) na svakih nekoliko tisuća dok se ne postigne odgovarajuće mjerilo (engl. benchmark) a tada se smanjuje na ispod 5% uzorka. Također se preporuča testiranje na uzorku koji predstavlja dokumentaciju koja se skenira.

Digitalizirana slika i pripadajući metapodaci su jedna cjelina. Zbog toga se preporučuje napraviti kontrolu kvalitete slike, metapodataka, naziva datoteke i kompletnost više straničnih dokumenata.

Kontrola kvalitete slike treba uključivati:

- je li najmanji detalj snimljen i čitljiv,
- je su li detalji snimljeni u cijelosti,
- postoji li točnost dimenzije kopije u usporedbi s originalom,
- postoje li točkice na digitaliziranoj slici koje ne postoje na originalu,
- je li original snimljen u cijelosti – jesu li svi rubovi uključeni i snimljeni,

- gustoća crnih polja,
- postojanost boje.

Kontrola metapodataka treba uključiti provjeru:

- zadovoljava li standarde politike tvrtke,
- što učiniti u slučaju da su metapodaci nepotpuni,
- relevantnost i točnost metapodataka,
- gramatičke ispravke,
- konzistentnost u stvaranju i čitanju metapodataka,
- evaluaciju korisnosti bilježenih metapodataka,
- sinkronizaciju metapodataka koji se bilježe na više od jednog repozitorija,
- je su li sva obavezna polja popunjena.

Posebno se treba kontrolirati:

- preciznost identifikacije datoteke,
- verifikaciju korektnosti slijeda i kompletiranosti višestaničnih dokumenata.

Svi podaci dobiveni kontrolom kvalitete trebaju biti evidentirani i postati sastavni dio metapodataka koji se odnose na digitaliziranu sliku.

Ukoliko proces kontrole kvalitete pokaže greške na više od 1% dokumentacije, sva dokumentacija obrađena nakon posljednje provjere se treba provjeriti. Ukoliko je greška na manje od 1% dokumentacije samo ona dokumentacija koja je otkrivena kontrolom se ispravlja.

U svojoj osnovi greške je moguće diferencirati na greške implementacije, greške procesa i greške operatera, te se o njima treba voditi računa i učiniti sve što je moguće da se one smanje.

Implementacijske greške se mogu izbjeći pravodobnim kontrolama kao što je:

- prljavi izvornici,
- odgovarajuće veličine i formati datoteka, npr. skenira se A3 a na skeneru je postavljen izlaz A4,
- kompresija, datoteke se komprimiraju na neodgovarajući način.

Procesne greške uklanja osoba koja je zadužena za nadgledanje procesa i uključuju:

- nekompletna i netočna specifikacija procesa,
- netočno kalibrirani uređaji i postavke uređaja,
- netočna povezanost procesa sa bazama podataka,
- netočno utvrđena obrada boje,
- slaba kvaliteta originala,

- nepreciznost izvornih metapodataka.

Operaterske pogreške su pogreške koje se događaju na dnevnoj razini i uključuju:

- osnovne greške skeniranja,
- obrezivanje slike koje je obrezalo dio same kopije dokumenta,
- orijentacija slike je kriva,
- ekspozitura slike je previše tamna ili previše svjetla,
- slika je izvan fokusa,
- skener nije bio kalibriran,
- greške u osnovnim procesima na slici,
- netočna korekcija boje, kontrasta, svjetline,
- netočno nazivanje datoteka,
- greške osnovnih dodataka metapodataka,
- netočnost upisa podataka,
- netočnost upisa unaprijed određenog rječnika.

6.4. HRN ISO/IEC 27001:2006

Norma HRN ISO/IEC 27001:2006 Sustavi upravljanja informacijskom sigurnošću (ISMS) – Zahtjevi primjenjuje procesni pristup uspostave, implementacije, upravljanja, pregleda, održavanja i poboljšanja ISMS-a (engl. Information Security Management System; Sustav informacijske sigurnosti op.a.), sustava informacijske sigurnosti. Norma je pisana primjenjujući procesni pristup prilikom kojeg se ističe važnost razumijevanja potrebe za donošenje politike i ciljeva informacijske sigurnosti, važnost uspostavljanja upravljanja prepoznatim rizicima, važnost nadgledanja i revizije provedbe i učinkovitosti uspostavljenog sustava te važnost neprestanog rada na poboljšanjima i objektivnom mjerenju provedenosti sustava.

Model koji norma primjenjuje sastoji se od 4 faze s ciljem kontinuiranog unaprjeđivanja nivoa sigurnosti tvrtke (engl. Plan-Do-Check-Act; skraćeno PDCA op.a.). To su faze:

1. PLAN: Faza planiranja – uspostava politika, ciljeva, procesa i procedura za upravljanje rizikom i poboljšanja informacijske sigurnosti u skladu sa sveukupnim politikama i ciljevima tvrtke,
2. DO: Faza implementacije – implementacija i rukovođenje politikama, kontrolama, procesima i procedurama definiranog sustava informacijske sigurnosti,

3. CHECK: Faza nadzora i pregledavanja – procjena i mjerenje učinkovitosti uspostavljenih procesa s definiranim politikama sigurnosti te slanje izvještaja upravi na pregled,
4. ACT: Faza održavanja i poboljšavanja – poduzimanje korektivnih i preventivnih aktivnosti temeljenih na internim revizijama i pregledima uprave, kao i drugim relevantnim informacijama kako bi se postigla kontinuiranost poboljšanja sustava sigurnosti.

U fazi planiranja određuje se opseg i granice na koje se sustav informacijske sigurnosti odnosi, na primjer kod digitalizacije to se može odnositi na skenere i pridružena računala, ali se ne odnosi na računala kojima se provodi javna nabava u potpuno drugom odjelu koji je neovisan o odjelu digitalizacije. Određuje se metodologija procjene rizika koja uključuje kriterije prihvaćanja rizika i određivanja visine rizika. Prepoznaje se imovina i prijetnje, na primjer ukoliko je računalu koje je spojeno na skener moguće pristupiti izvana ovaj rizik je potrebno prepoznati. Prepoznati rizici se dalje analiziraju i vrednuju, te im se određuju mogućnosti odgovora na prepoznate rizike. Odabiru se ciljevi kontrole i kontrola postupanja u vezi prepoznatih rizika. Sve se to dokumentira u dokumentu Izjava o primjenjivosti (engl. Statement of Applicability).

Faza implementacije obvezuje organizaciju provedbu svega prepoznatog u fazi planiranja. Pri tome organizacija vodi računa kako provoditi mjerenje učinkovitosti čiji se rezultat može uspoređivati. Zatim, provodi programe edukacije i svjesnosti povezane s rizicima. Dodatno se, u ovoj fazi, uspostavlja upravljanje radom sustava informacijske sigurnosti, upravljanje resursima na koje se ISMS odnosi, te provode postupci i kontrole otkrivanja sigurnosnih incidenata i odgovora na te incidente, na primjer skener proizvodi neobjašnjivu količinu grešaka a servisni termin mjesečnog održavanja još nije nastupio, u tom slučaju operater javlja informaciju na daljnje postupanje.

Nadzor i pregled uspostavljenog sustava uključuje provjeru provođenja prepoznatih kontrola koje otkrivaju greške u procesima, sigurnosne proboje, te učinkovitost odgovora na sigurnosne proboje. Redovita revizija učinkovitosti treba u svoju procjenu uključiti rezultate svih incidenata, odgovora na incidente, mjerenja uspješnosti odgovora na incidente, prijedloge i sve povratne informacije uključenih strana.

Faza održavanja i poboljšavanja sustava uključuje redovitu primjenu prepoznatih poboljšanja uključujući korektivne i preventivne akcije prepoznate tijekom iskustva organizacije ili drugih organizacija, obavještavanje svih poduzetih poboljšanja svim

uključenim stranama s odgovarajućim stupnjem detalja, i sve to usklađeno s postizanjem svojih prepoznatih ciljeva iz faze planiranja.

Posebnost ove norme je popis predloženih kontrola kojih ima ukupno 133 poredanih u 11 područja, koji se mogu pronaći u normi. Posebna napomena u samoj normi je da taj popis nije konačan te ga tvrtka može povećati ovisno o svojim potrebama.

6.5. ISO 15489-1:2001

Norma ISO 15489-1:2001 se odnosi na upravljanje zapisima, u svim formatima i medijima, koji su nastali ili zaprimljeni od strane javne ili privatne organizacije u obavljanju njezine djelatnosti, odnosno bilo kojeg pojedinca koji je dužan stvarati i čuvati zapise. Norma daje smjernice kako odrediti odgovornosti organizacije za zapise i politiku, postupke, sustave i procese koji se odnose na zapise, daje smjernice za oblikovanje i izgradnju sustava za upravljanje zapisima, ali se ograničava od upravljanja arhivskim zapisima u arhivskim ustanovama.

Norma se sastoji od dva dijela, općeg dijela opisanog u ISO 15489-1:2001, te tehničkog izvješća provedbe opisanog u ISO/TR 15489-2:2001.

Uspostavljanje sustava upravljanja zapisima uključuje:

- donošenje politike i normi,
- raspodjelu odgovornosti i nadležnosti,
- uspostavu i objavljivanje postupaka i smjernica,
- pružanje niza usluga koje se odnose na upravljanje i korištenje zapisa,
- oblikovanje, primjenu i upravljanje specijaliziranim sustavima za upravljanje zapisima,
- integriranje upravljanja zapisima u poslovne sustave i procese.

Kako bi se navedeno postiglo norma predlaže:

- identifikaciju normativnog okruženja,
- utvrđivanje, dokumentiranje, održavanje i objavljivanje politika, procedura i postupka upravljanja zapisima,
- uspostavljanje i provođenje programa upravljanja zapisima,
- određivanje osobina zapisa (uključujući metapodatke za dokumentiranje nastalih aktivnosti, osiguranje autentičnosti, pouzdanosti, integriteta i iskoristivosti),
- utvrđivanje koji su zapisi potrebni i kada, kako i gdje se prihvaćaju u spisovodstveni sustav,

- osiguranje pouzdanosti, integriteta, sukladnosti, cjelovitosti i sustavnosti spisovodstvenih sustava,
- određivanje radnji sa zapisima koje je potrebno dokumentirati,
- određivanje fizičkih medija za pohranu i zaštitu, kao i alternativne mogućnosti smještaja zapisa,
- oblikovanje sustava na način da zadrže autentičnost, pouzdanost i iskoristivost zapisa za vrijeme čitavog perioda čuvanja,
- zaštita integriteta zapisa primjenjivanjem nadzora nad pristupom,
- dokumentiranje diskontinuiranih spisovodstvenih sustava,
- određivanje procesa i kontrola upravljanja zapisima (koliko dugo se čuvaju zapisi, osiguranje prihvaćanja zapisa u sustav, registracija zapisa u sustav, klasificirati zapise korištenjem klasificiranih rječnika, indeksiranje, dodjeljivanje brojeva i oznaka),
- određivanje prava pristupa (tko i kada),
- praćenje kretanja i korištenja zapisa s ciljem sprječavanja gubitka zapisa ili uništavanja,
- dokumentiranje svih postupaka u upravljanju zapisima,
- provođenje redovitog nadzora usklađenosti s politikama i zahtjevima organizacije,
- uvođenje stalnog programa osposobljavanja za spisovodstvo.

Pojmovi koji su definirani u normi:

- **Dokumentirati transakciju** znači zapisati:
  1. sadržaj,
  2. metapodatke s informacijama o:
     a. obliku i vezama među elementima koji čine zapis,
     b. poslovnom kontekstu:
        i. u kojem je zapis nastao,
        ii. u kojem je zaprimljen,
        iii. u kojem je korišten,
     c. poslovnom procesu u kojem je nastala transakcija,
     d. datumu i vremenu transakcije,
     e. sudionicima u transakciji,
     f. vezama među dokumentima, koji se drže odvojeno ali zajedno čine zapis.
- **Autentičan zapis** je zapis za koji se može dokazati**:**
  1. da jest ono što tvrdi da jest,
  2. da ga je izradila ili odaslala osoba za koju se tvrdi da ga je izradila ili poslala,

3. da je izrađen ili odaslan u vrijeme za koje se to tvrdi.

- **Pouzdan zapis** je zapis za čiji se sadržaj može vjerovati da potpuno i točno predstavlja transakcije, aktivnosti ili činjenice koje potvrđuje i o kojima može biti ovisan tijekom sljedećih transakcija i aktivnosti. Zapisi trebaju nastati u vrijeme transakcije ili događaja na koji se odnose, ili kratko nakon toga, trebaju ih stvarati pojedinci koji izravno poznaju činjenice ili uređaji koji se u poslovanju rutinski koriste za obavljanje transakcija.
- **Integritet zapisa** označava zapis koji je potpun i neizmijenjen. Politikom i postupcima u upravljanju zapisima treba biti određeno koji se dodaci i bilješke mogu dodati zapisu nakon što je nastao, pod kojim se uvjetima dodaci i bilješke autoriziraju i tko je ovlašten da ih dodaje. Svaka autorizirana bilješka, dodatak ili brisanje trebaju biti eksplicitno naznačeni i provjerljivi.
- **Iskoristiv zapis –** onaj zapis kojemu je moguće utvrditi smještaj, dohvatiti ga, predočiti i interpretirati (povezati s aktivnošću ili transakcijom koja ga je proizvela).

Za postizanje autentičnosti predlaže se primjena i dokumentiranje politika i postupaka koji upravljaju stvaranjem, zaprimanjem, prosljeđivanjem, čuvanjem i stavljanjem zapisa na raspolaganje. U politikama i postupcima trebaju biti navedeni stvaratelji zapisa koji su za to ovlašteni te zaštita zapisa od neovlaštenog dodavanja, brisanja, mijenjanja, korištenja i uništenja.

Drugi dio norme ISO/TR 15489-2:2001 navodi spisovodstvene procese:

1. prihvaćanje,
2. registriranje,
3. klasifikaciju,
4. klasifikaciju pristupa i sigurnosti,
5. identifikaciju statusa stavljanja zapisa na raspolaganje,
6. smještaj,
7. korištenje i praćenje,
8. stavljanje zapisa na raspolaganje.

Minimalni metapodaci koji se zapisuju prilikom registracije su:

1. jedinstvena identifikacija (dodjeljuje sustav),
2. datum i vrijeme registracije,
3. naslov ili kratki opis,
4. autor (fizička ili pravna osoba), pošiljatelj ili primatelj.

Predlaže se za jedinstvenu oznaku zapisa koristiti slijedeće podatke:

- naziv ili naslov dokumenta,
- opis teksta ili sažetak,
- datum nastanka,
- datum i vrijeme slanja i primanja,
- navod radi li se o: ulaznom, izlaznom ili internom dokumentu,
- ime autora (sa svojom funkcijom),
- ime pošiljatelja (sa svojom funkcijom),
- ime primatelja (sa svojom funkcijom),
- navod o kojem se fizičkom obliku radi,
- klasifikacijski podaci u skladu s klasifikacijskom shemom,
- veza s povezanim zapisima,
- podatak o poslovnom sustavu iz kojeg je zapis prihvaćen,
- naziv aplikacijskog softvera i verzije u kojoj je zapis nastao ili u kojoj je zahvaćen,
- standard s kojim je struktura zapisa usklađena (na primjer Standard Generalized Markup Language - SGML, Extensible Markup Language - XML),
- detalj o ugrađenim vezama dokumenata, uključujući aplikacijski softver i verziju pod kojom je povezani zapis stvoren,
- podatak o predlošku koji je potreban za interpretiranje strukture dokumenata,
- vrsta pristupa zapisa,
- rok čuvanja,
- ostali podaci o strukturi i kontekstu koji mogu biti korisni za upravljanje.

Kako bi se lakše pronašli zapisi norma preporučuje slijedeće indeksne pojmove:

- format ili priroda zapisa,
- naslov ili glavno zaglavlje zapisa,
- tematski sadržaja zapisa, (na primjer u skladu s poslovnom aktivnosti),
- sažetak dokumenta,
- datumi povezani s transakcijama koje su zabilježene u dokumentu,
- imena klijenata i organizacija,
- posebni zahtjevi za rukovanje ili obradu,
- priložena dokumentacija koja nije identificirana na drugi način,
- svrha zapisa.

Prilikom dodjele prava i ograničenja pristupa preporučuje se provođenje slijedećih koraka:

1. identifikacija transakcija ili poslovne aktivnosti koju zapis dokumentira,

2. identifikacija poslovne jedinice kojoj zapisi pripadaju,
3. provjera klasifikacije za pristup i sigurnost da se ustanovi jesu li aktivnost i područje poslovanja identificirani kao područje rizika ili postoje sigurnosni problemi i/ili zakonski propisana ograničenja,
4. dodjela odgovarajuće razine pristupa ili ograničenja zapisu i specificiranje odgovarajućih kontrolnih mehanizama za rukovanje,
5. bilježenje statusa pristupa i sigurnosti zapisa u spisovodstvenom sustavu da se naznači potreba za dodatnim mjerama nadzora.

Za praćenje korištenja zapisa unutar sustava preporuča se:

1. identificiranje korisničkih prava u spisovodstvenom sustava, koja su vezana uz pojedince i njihov položaj unutar organizacije,
2. identificiranje statusa dostupnosti i sigurnosti zapisa,
3. identificiranje prava pristupa za osobe izvan organizacije,
4. osiguravanje da samo pojedinci s prikladnom korisničkom klasifikacijom ili sigurnosnim pravima imaju pristup zapisima s ograničenim pristupom,
5. praćenje kretanja zapisa da se identificira tko ih čuva ili ih je čuvao,
6. osiguravanje da se svako korištenje zapisa bilježi do prikladne razine detalja,
7. revidiranje klasifikacije dostupnosti zapisa da se osigura da ona vrijedi i da je još primjenjiva.

Kako bi se osiguralo da zapisi i pridruženi podaci budu dostupni i iskoristivi tijekom cijelog perioda čuvanja (što uključuje i razne migracije) predlaže se da se prilikom oblikovanja sustava vodi briga o strategijama za njihovo očuvanje.

Prilikom fizičkog uništenja zapisa predlaže se vođenje računa o stupnju povjerljivosti, dokumentiranom tragu, provjeru svakog uništavanja, pristanak nadležnih tijela, potvrdu o uništenju i slične sigurnosne oblike koji mogu spriječiti neovlašteno i neželjeno uništavanje spisa.

Postoji mogućnost da organizacija prenese dokumentaciju na upravljanje drugoj organizaciji ili trećoj strani pri čemu se predlaže razmatranje slijedećih ključnih točaka:

1. za zapise:
    a. jesu li operativne i administrativne potrebe za predaju zapisa mjerodavno utvrđene,
    b. je li uređena odgovornost i nadležnost zapisa,
    c. je li uračunat učinak predaje na zapise organizacije koja ih predaje,
    d. jesu li ispunjene tekuće obveze koje proizlaze iz zakona, propisa i politike organizacije,

2. za elektroničke dokumente:
    a. je li se vodilo računa o kompatibilnosti hardvera i softvera,
    b. je li se vodilo računa o metapodacima (kontrolne i kontekstualne informacije),
    c. je li se vodi dokumentacija o podacima (tehničke informacije o obradi i strukturi podataka),
    d. je li se vodilo računa o licenčnim ugovorima,
    e. jesu li korišteni svi propisani standardi.

Svaki zapis ili predočeni dokument na sudu može biti osporavan. Radi toga preporuka je spisovoditeljima pripremiti dokazne materijale iz kojih je vidljivo kako zapisi nastaju u skladu s pravnim propisima, politikama organizacije i procedurama koje su na snazi tijekom životnog vijeka sustava, da sustav djeluje i jest djelovao u skladu s poslovnom praksom organizacije, te da se vodi dokumentacija o nadzoru i provjerama procesa koji djeluju i propisani su unutar sustava.

6.6. ISAD (G) - Opća međunarodna norma za opis arhivskoga gradiva

Međunarodno arhivsko vijeće izradilo je opću međunarodnu normu ISAD(G)[198] za opis arhivskog gradiva, koje je odobrilo Povjerenstvo za norme opisa arhivskog gradiva u Stockholmu, 19-22. rujna 1999. godine. U normi su dane smjernice za opis arhivskog gradiva s ciljem identificiranja i pojašnjavanja konteksta i sadržaja arhivskog gradiva kako bi se olakšala njegova dostupnost. Iako je norma pisana za gradivo koje je odabrano kao arhivsko, preporuča se upotreba u svim fazama (stvaranje, životni ciklus, vrednovanje, preuzimanje, čuvanje, sređivanje) a s ciljem da je sigurno pohranjeno i nadzirano te dostupno za korištenje svima koji na to imaju pravo. Pravila su opća bez obzira na oblik ili nosač arhivskih zapisa, ali se ne odnosi na posebnu vrstu gradiva kao što su pečati, zvučni zapisi ili karte jer za njih već postoje pravila za opis takvih vrsta gradiva.

Norma navodi korištene pojmove i definicije koje ovdje ne navodim.

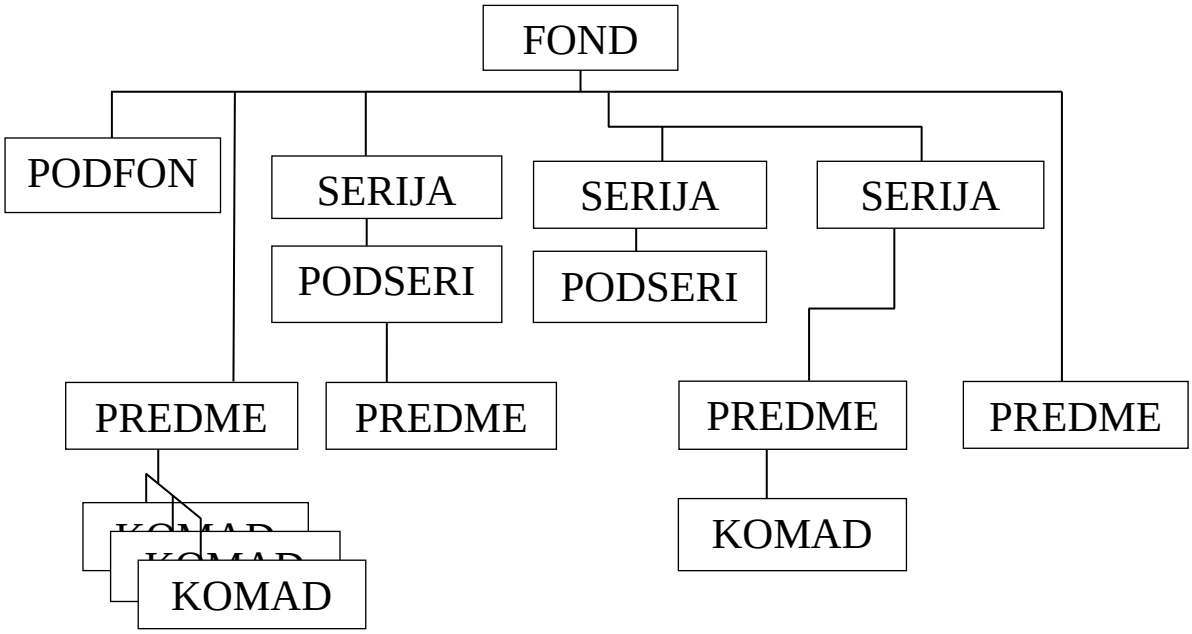
Za stvaranje opisa nekog arhivističkog entiteta norma je identificirala 26 elemenata kojima je cilj:

- osigurati izradu dosljednih, uporabivih i razumljivih opisa,
- olakšati pronalaženje i razmjenu obavijesti o arhivskome gradivu,
- omogućiti razmjenu normativnih podataka,

[198] ISAD (G) - OPĆA MEĐUNARODNA NORMA ZA OPIS ARHIVSKOGA GRADIVA, MEĐUNARODNO ARHIVSKO VIJEĆE, Zagreb, 2001, drugo izdanje, URL: http://zagreb.arhiv.hr/hr/pdf/, pristupljeno: 15.3.2017.

- omogućiti objedinjavanje opisa iz različitih arhiva u jedinstveni informacijski sustav.

Norma daje hijerarhijski model razina sređivanja i njihovih sastavnih dijelova (slika 1) iz kojeg se vidi kako Fond predstavlja najvišu razinu koja se može sastojati od podfonda, serija i podserija, predmeta i komada, gdje podfond može sadržavati serije, podserije, predmete i komade. Prikazani hijerarhijski model ne pokazuje sve moguće kombinacije.



Slika 1. Hijerarhijski model razina sređivanja

Norma prepoznaje 26 elemenata opisa podijeljenih u sedam područja opisa:

1. područje identifikacije (sadrži bitne obavijesti za identifikaciju jedinice opisa):
    a. identifikacijska oznaka(e)/signatura(e),
    b. naslov,
    c. vrijeme nastanka gradiva,
    d. razina opisa,
    e. količina i nosač jedinice opisa (količina, opseg, veličina),
2. područje konteksta (sadrži obavijesti o porijeklu i sačuvanosti jedinice opisa):
    a. naziv stvaratelja,
    b. upravna povijest / biografski podaci,
    c. povijest arhivskog fonda,
    d. način preuzimanja ili predaje,
3. područje sadržaja i ustroja (sadrži obavijesti o predmetu i sređenosti jedinice opisa):
    a. sadržaj,
    b. odabiranje, izlučivanje i rokovi čuvanja,
    c. dopune,

    d. plan sređivanja,
4. područje uvjeta dostupnosti i korištenja (sadrži obavijesti o dostupnosti jedinice opisa):
    a. uvjeti dostupnosti,
    b. uvjeti objavljivanja ili umnožavanja,
    c. jezik / pismo u gradivu,
    d. tvarne značajke i tehnički uvjeti,
    e. obavijesna pomagala,
5. područje dopunskih izvora (sadrži obavijesti o gradivu koje je u važnom odnosu s jedinicom opisa):
    a. postojanje i mjesto čuvanja izvornika,
    b. postojanje i mjesto čuvanja preslika,
    c. dopunski izvori,
    d. bibliografija,
6. područje napomena (sadrži posebne obavijesti i obavijesti koje ne mogu biti smještene u bilo koje drugo područje):
    a. napomena,
7. područje kontrole opisa (sadrži obavijesti o tome kako, kada i tko je izradio arhivistički opis):
    a. napomena arhivista,
    b. pravila ili propisi,
    c. nadnevak izrade opisa.

Norma napominje kako nije potrebno imati svih 26 elemenata za pojedini opis, ali nužno je imati njih šest, dok se ostali mogu prema potrebi upotrijebiti. Obaveznih šest su:

1. identifikacijska oznaka(e)/signatura(e),
2. naslov,
3. stvaratelj,
4. vrijeme nastanka gradiva,
5. količina jedinice opisa,
6. razina opisa.

Dodatno su u normi navedene smjernice kojima se ukazuje da je potrebno na nacionalnoj razini ili posebno za svaki jezik razraditi rječnike i pravila koji će se koristiti i preporuča slijedeće norme za pomoć u razvoju i održavanju kontroliranih rječnika:

- ISO 5963 Dokumentacija – Metoda za raščlambu dokumenata, utvrđivanje njihova sadržaja i izbor riječi za indeksiranje.
- ISO 2788 Dokumentacija – Smjernice za izradu i razradu jednojezičnih tezaurusa.
- ISO 999 Informacija i dokumentacija – Smjernice za sadržaj, organizaciju i prikaz kazala.
- ISO 690 Dokumentacija – Bibliografske uputnice – Sadržaj, oblik i ustroj.

6.7. Zaključak

Dugoročno čuvanje dokumentacije može dovesti do uništavanja, zbog toga je potrebno urediti uvjete čuvanja i rukovanja dokumentacijom tijekom cijelog perioda čuvanja. Digitaliziranu dokumentaciju treba čuvati na autentičan i vjerodostojan način osiguravajući integritet tijekom vremena. Ovu pouzdanost i vjerodostojnost tvrtka postiže kombinacijom organizacijskih pravila, operativnih postupaka i pravilno korištenih tehnologija. Sve korišteno je potrebno propisati odgovarajućim dokumentom. Tako je, na primjer, potrebno propisati procedure skeniranja, ponovnog skeniranja, kontrole rada skenera, kontrole kvalitete skeniranja, planirati migracijske procedure, procedure izrade pričuvnih kopija i tako dalje.

Očuvanje integriteta pohranjenih podataka je moguće postići izradom kontrolnog zbroja podataka u trenutku pohrane, ali i izradom ovog kontrolnog zbroja u trenutku skeniranja. Tijekom digitalizacije je moguće koristiti tehnike poboljšanja slike prilikom čega je potrebno voditi računa da se sve tehnike zapišu i da se ne koriste one tehnike koje vode do gubitka podataka. Sve što se obavlja u trenutku digitalizacije, ali i kasnije tijekom čuvanja digitaliziranih slika je potrebno zapisivati u adekvatnim revizijskim tragovima. Potrebno je voditi računa o metapodacima koji se upisuju te smanjiti ručni unos odnosno posebno provjeriti ručni unos, ali i automatski unos ukoliko je dobiven korištenjem OCR tehnike.

Imenovanje datoteke treba definirati prije početka digitalizacije. Tijekom digitalizacije se izrađuju glavne slike koje se čuvaju na odvojenom sigurnom spremištu. Pored digitalizirane slike na odvojenom sigurnom spremištu potrebno je čuvati i pripadajuće metapodatke koji su nastali prije i tijekom digitalizacije. Ciklus digitalizacije treba proći kroz faze planiranja, implementacije, nadzora i pregleda te održavanja i poboljšavanja.

7. KOMPONENTE DIGITALIZACIJE

Kvaliteta digitalizirane slike u direktnoj je ovisnosti o komponentama koje se pritom koriste. Senzori prihvaćaju svjetlosne frekvencije i šalju ih dalje na obradu. Upravo o kvaliteti senzora ovisi kakav će podatak softver za digitalizaciju primiti na daljnju obradu. Digitalizacijom, osim slike, nastaju metapodaci koji joj daju kontekst i koji trebaju ostati povezani s njom tijekom cijelog perioda čuvanja. Kako bi se to postiglo važno je omogućiti provjeru jesu li svi podaci predani u sustav za čuvanje u svojoj cjelovitosti i zadržavajući integritet što se može postići izradom strukture datoteke koja sadrže potrebne podatke te provjerom zadovoljavanja propisane strukture i drugih uvjeta.

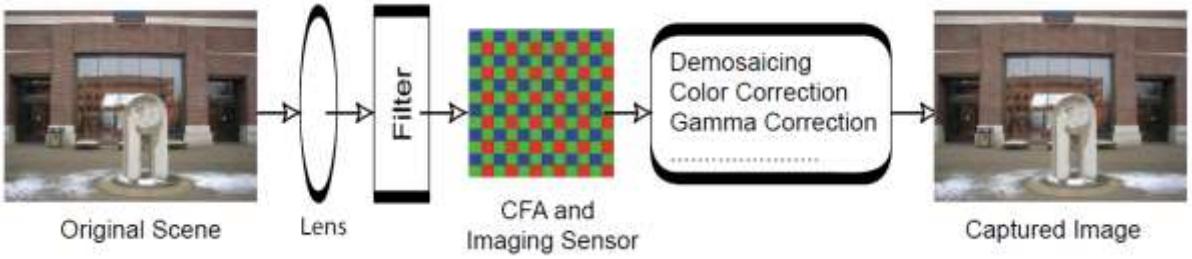
7.1. Senzori u digitalizaciji - CCD i CIS

OBJEKTIVNO PREPOZNAVANJE SENZORA

Forenzička analiza jedan je od alata za objektivno prepoznavanje senzora iz digitalne slike. Ispravno korištenje forenzičke analize ovisi o poznavanju podatka je li slika stvorena pomoću fotoaparata ili pomoću skenera. U svojem radu autori Khanna, Mikkilinenib, Chiub, Allebacha, Delpa, raspravljaju o forenzičkoj analizi digitaliziranih slika te navode kako su najvažniji alati: utvrditi provenijenciju, autentičnost i proces čuvanja digitaliziranih slika.[199] Oni dalje navode da je moguće, promatrajući neispravne točke ili šum uzorka koji stvara senzor, odrediti koji je skener stvorio sliku upravo zbog jedinstvenosti stohastičkih karakteristika senzora. Ovaj šum koji se stvara ovisi o nekoliko faktora kao što su: neuniformnost točaka, čestica prašine na optici, optičke smetnje te šuma tamne struje (engl. dark current).[200]

[199] Khanna, N., Mikkilinenib, A. K., Chiub, G. T., Allebacha, J. P., & Delpa, E. J. (2007.). Forensic Classification of Imaging Sensor Types. Preuzeto 14. 3. 2017. iz SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents: https://engineering.purdue.edu/~prints/public/papers/ei07-nitin1.pdf
[200] ibid.

NASTANAK DIGITALNE SLIKE



Slika 2. Model stvaranja slike digitalnim fotoaparatom[201]

Slika 2 pokazuje tipičan tijek procesa nastanka digitalne slike korištenjem digitalnog fotoaparata. Svjetlo se odbija od prizora, prolazi kroz leću objektiva te kroz set filtara. Zatim se svjetlost prihvaća kroz senzor, na primjer CCD, CMOS, CIS ili PMT (engl. photomultiplier tube), odnosno, svaka točka očitava intenzitet svjetla koji prolazi kroz polje filtara boja (engl. Color Filter Array; skr. CFA) koji zatim svakoj točki senzora dodjeljuje jednu od osnovnih boja, na primjer RGB ili CMYK, prema bloku točaka veličine 4x4 (vidi sliku 3). Cijela površina boja se dalje interpolira koristeći ove vrijednosti na svakoj točki. Prije nego se dobije konačna slika u željenom formatu, na primjer RAW, TIFF ili JPEG, obave se dodatne operacije kao na primjer interpolacija boja, korekcija bijelih polja, gamma korekcija i tako dalje.

R	G	R	G
G	R	G	R
R	G	R	G
G	R	G	R

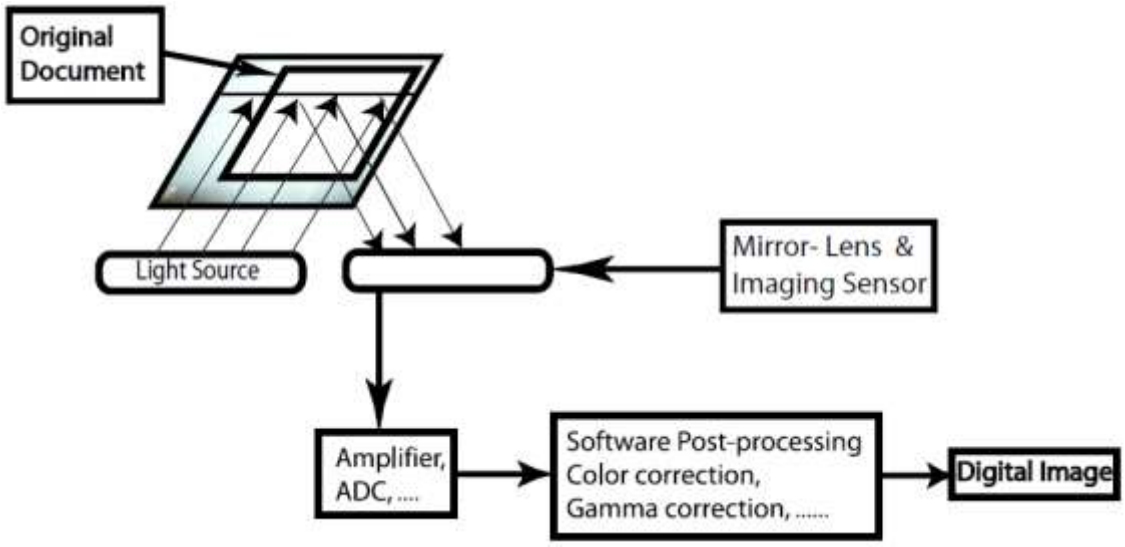
K	M	K	M
C	Y	C	Y
M	K	M	K
C	Y	C	Y

Slika 3. Blok točaka RGB i CMYK

Slika 3 prikazuje tijek procesa pretvorbe originalnog, papirnatog dokumenta u digitalni korištenjem plošnog skenera. Lampa, primjerice CCFL lampa (engl. Cold Cathode Flourescent Lamp), ksenon lampa ili fluorescentna lampa, osvijetli papir, zatim se, pomoću motora, glava skenera, koja sadrži leće, ogledala, filtre i senzore, linearno pomiče i hvata liniju po liniju svjetlosnog snopa. Iz ovog možemo zaključiti kako horizontalna rezolucija ovisi o broju foto elemenata u senzoru, dok vertikalna rezolucija ovisi o stupnju pomaka, odnosno veličini koraka, motora koji pomiče glavu skenera. Kako bi se dobila tražena

[201] ibid.

rezolucija, koja je manja od stvarne optičke rezolucije senzora koji se nalazi u glavi skenera, mogu se primijeniti dvije tehnike. Jedna se obavlja tijekom skeniranja kada se odabire određeni podskup očitane linije, dok se druga obavlja nakon prihvata cijelog skupa primljenog u punoj rezoluciji a rezultat se smanji u memoriji skenera. Od ove dvije metode precizniji rezultat daje druga metoda.[202]



Slika 4. Proces stvaranja slike kod plošnog skenera[203]

VRSTE SENZORA

Prilikom rada skenera postoji nekoliko važnih komponenti: senzor - koji pretvara svjetlosni signal u digitalni podatak, pokretački program (engl. driver) i program za prihvat slike. Prema Đurek, za kvalitetu skeniranja izravno je odgovoran upravo senzor.[204] Na tržištu postoji više vrsta senzora: CCD, CMOS, CIS, PMT i drugi. U pravilu se razlikuju po cijeni, međutim glavna razlika je u tehnologiji konverzije signala u digitalni podatak.

PMT senzor je cijevni senzor koji se nalazi u rotacijskim skenerima u kojem se dokument umeće u rotacijski bubanj. Rotacijski bubanj se velikom brzinom okreće oko senzora. Pomoću filtara svjetlost se razdvaja na tri dijela i tako razdvojena dovodi do senzora. Ovako skenirani dokumenti imaju široki tonski raspon i visoku oštrinu, ali su vrlo spori i skupi.[205]

[202] ibid.
[203] ibid.
[204] Đurek, I. (8. 6. 2002.). DIGITALIZACIJA SVJETLA. Preuzeto 20. 3. 2017. iz Filos: http://www.filos.com/mkrzak/Djurek1.doc
[205] ibid.

CCD (engl. charge-coupled device) senzor se sastoji od niza povezanih kondenzatora koji su osjetljivi na svjetlo. Senzor filtrira svjetlo kroz crveni, zeleni i plavi filtar. Sastoji se od višestrukih linija senzorskih točaka visoke preciznosti i osjetljivosti na svjetlo.

CMOS (engl. complementary-symetry/metal-oxide semiconductor) senzor se bazira na tehnologiji poluvodiča i postavlja se na isti mikročip na kojem je procesor.

CIS (engl. contact image sensor) senzor je novija tehnologija koja se najviše koristi na manjim skenerima ili plošnim skenerima budući je za konverziju slike potrebno postaviti senzor blizu dokumenta koji skeniramo jer ima usku dubinu polja koji može skenirati. Senzor sadrži jedan ili dva reda senzorskih točaka i koristi crvene, zelene ili plave LED diode kojima stvara bijelo svjetlo.

Dodatno po čemu se razlikuju ovi senzori je dubina polja koju mogu obuhvatiti prilikom konverzije analogne slike u digitalnu. CCD senzor ima najveću dubinu polja jer koristi ogledala i leće koje CMOS i CIS senzori ne koriste.[206] Međutim, tehnologija CCD senzora je osjetljivija na vibracije i mehaničke udarce od CIS i CMOS tehnologije. Kvaliteta slike je najbolja kod CCD senzora, ali je tehnologija izrade skuplja.[207]

Prednost CMOS tehnologije je mogućnost postavke senzora na isti mikročip na kojem je i procesor s čime se smanjuje veličina potrebnog prostora, dok je prednost CIS senzora u energetskoj učinkovitosti i jednostavnosti izrade zbog čega se koristi u vrlo malim skenerima.

Kvaliteta dobivenih slika je najveća kod CCD senzora, kod CMOS senzora je bolja nego kod CIS senzora, dok je kvaliteta slike dobivena korištenjem CIS senzora dobra.[208]

Još jedna razlika u radu CMOS i CCD senzora je u tome što CMOS senzor prihvaća po jedan red svjetlosnih informacija, nazvan *rolling shutter* efekt jer se različiti dijelovi senzora u različito vrijeme izlažu svjetlosnom snopu što dovodi do raznih iskrivljenja prilikom velikih brzina, dok CCD senzor prihvaća cijelu sliku odjednom. Efekt se zove *global shutter*, i ne dovodi do iskrivljenja prilikom brzih pokreta ili brzih bljeskova svjetla.[209]

ŠUM SENZORA

Tijekom proizvodnog procesa senzora, zbog nesavršenosti proizvodnje samih točaka, događaju se određene nesavršenosti koje stvaraju šum u vrijednostima točaka. Tako se šum

[206] Buyers Laboratory Inc., NJ, USA. (2006.). Digital Imaging REVIEW, vol. 28. NO. 10. Preuzeto 16. 3. 2017. iz Fujitsu: http://www.fujitsu.com/downloads/COMP/fcpa/reviews/market-roundup-1006.pdf
[207] ibid.
[208] ibid.
[209] Lumis. (7. 5. 2015.). Koja je razlika između načina rada CMOS i CCD senzora? Preuzeto 17. 3. 2017. iz Lumis: https://lumis.hr/clanci/tehnologija/koja-je-razlika-izmedu-nacina-rada-cmos-i-ccd-senzora/

dijeli na slijedeće nedostatke: nedostatak točke, nedostatak vruće točke, mrtve točke, klopke točaka, nedostatak kolone i nedostatak grupe.[210] Na primjer, mrtva točka daje crnu točku na slici, dok vruća točka daje svijetlu točku na slici, neovisno o stvarnoj boji originala. Druga vrsta šuma je šum uzorka koji se odnosi na bilo koji prostorni uzorak koji se ne mijenja značajno promjenom originala tijekom skeniranja, a odnosi se na tamnu struju koja varira od točke do točke ali je za svaku točku fiksna, i šum uzorka koji nastaje zbog nejednolikosti odgovora fotoćelija.[211]

CRNE TOČKE

Prilikom skeniranja svjetlost prolazi kroz optičke dijelove skenera sve do senzora, međutim nisu svi dijelovi senzora iskorišteni kako bi pretvorili svjetlost u digitalni prikaz. Točke koje se nalaze na periferiji senzora, crne točke (engl. black pixel), ne dobivaju svjetlost što omogućuje uređaju prepoznavanje količine tamne struje koja se stvara tijekom ekspozicije kada nema svjetlosti što stvara šum. Mjerenjem ove količine tamne struje dobiva se podatak o količini tamne struje koja se stvara u aktivnim točkama te se može oduzeti od očitane vrijednosti i kao rezultat dobiti sliku s manje šuma.[212]

PRAVA REZOLUCIJA

Senzori koji prihvaćaju valnu duljinu svjetlosti postavljeni su u liniji. Broj senzora nam govori o optičkoj rezoluciji skenera, takozvana stvarna rezolucija skenera. Na primjer, kada skener želi skenirati A4 stranicu, dužine 21 cm ili 8,5 inča, rezolucijom od 600 dpi (engl. dpi = dot per inch; tpi = točaka po inču op.a.) to znači da u liniji treba biti 5100 senzora.[213] Za veću rezoluciju potrebno je više senzora u liniji.

Na ScanTastik[214] stranicama mogu se pronaći podaci o različitim skenerima proizvođača Canon, Fujitsu, Kodak, Panasonic i Xerox. Podaci za brze skenere, skenere

[210] Khanna, N., Mikkilinenib, A. K., Chiub, G. T., Allebacha, J. P., & Delpa, E. J. (2007.). Forensic Classification of Imaging Sensor Types. Preuzeto 14. 3. 2017. iz SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents: https://engineering.purdue.edu/~prints/public/papers/ei07-nitin1.pdf
[211] ibid.
[212] Golowczynski, M. (20. 1. 2016.). Digital camera sensors explained. Preuzeto 20. 3. 2017. iz WHAT DIGITAL CAMERA: http://www.whatdigitalcamera.com/technical-guides/technology-guides/sensors-explained-11457
[213] Đurek, I. (8. 6. 2002.). DIGITALIZACIJA SVJETLA. Preuzeto 20. 3. 2017. iz Filos: http://www.filos.com/mkrzak/Djurek1.doc
[214] ScanTastik. (n.d.). High Speed Scanners. Preuzeto 9. 3. 2018. iz http://www.scantastik.com/high-speed-scanners.htm

kojima je brzina skeniranja 100 stranica u minuti i više, maksimalna dnevna količina skeniranja iznad 30.000 stranica na dan te mogućnost ulaganja više od 300 listova u paketu odjednom, pokazuju kako skeneri imaju optičku rezoluciju od 600 dpi-a. Također, podaci pokazuju da neki navedeni skeneri imaju mogućnost izrade slika od 1200 dpi-a pri čemu rade softversku interpolaciju točaka.

Postoje dva rješenja kojima je moguće dobiti rezoluciju 1200 dpi korištenjem 600 senzora po inču: VAROS dizajn i Hyper CCD dizajn. VAROS dizajn koristi lom svjetlosti i dva prolaza po istoj liniji pri čemu se u prvom prolazu skeniraju neparne točke, a u drugom prolazu parne točke, do kojih se dolazi okretanjem stakla za točno određeni kut. Mana ovog rješenja je duljina skeniranja, ali i lom svjetla zbog različitog kuta loma.[215] Hyper CCD dizajn koristi dva reda s po 600 senzora po inču koji su pomaknuti za pola točke. Kod ove tehnologije brzina skeniranja se ne mijenja ali postoji preklapanje točaka, zbog pomaka od pola točke.[216]

Tijekom skeniranja dolazi do zagrijavanja cijelog sustava što može dovesti do promjene mehaničkih dijelova sustava, zato je važno da se oni dijelovi na kojima se nalazi optika i drugi osjetljivi dijelovi nalaze na materijalu koji nije podložan takvim utjecajima, kao što je na primjer metal.

Optička rezolucija je ograničena brojem senzora, ali se ona može umjetno, interpolacijom točaka, povećati koristeći matematičke algoritme interpolacije.[217] Na primjer, skener ima deklariranu rezoluciju 1200x600 dpi. Broj 1200 označava broj točaka dobiven pomakom glave skenera a broj 600 broj točaka dobiven pomoću senzora. Skenirani dokumenti imaju jednaku rezoluciju u oba smjera. To znači da kada se želi dobiti rezolucija od 1200 dpi potrebno je napraviti povećanje točaka, interpolaciju. Kada se želi dobiti rezolucija od 600 dpi-a potrebno jer napraviti smanjenje, ekstrapolaciju, točaka. Ili, drugim riječima ukoliko se želi dobiti rezolucija od 300 dpi tada je potrebno smanjiti broj točaka u oba smjera.

IZVOR SVJETLOSTI

Svjetlost se odbija od prizora te prolazi kroz niz uređaja koji pretvaraju svjetlost u električni impuls i na kraju u sliku na ekranu. U ovom procesu uključena je svjetlost, koja

[215] Đurek, I. (8. 6. 2002.). DIGITALIZACIJA SVJETLA. Preuzeto 20. 3. 2017. iz Filos: http://www.filos.com/mkrzak/Djurek1.doc
[216] ibid.
[217] ibid.

može biti prirodna ili umjetna, objekt, optika, kao što je ogledalo i leća, senzor i kompleksan sklop dijelova koji pretvaraju zabilježenu valnu duljinu u digitalni zapis.[218]

Cijeli spektar boja dobiva se uz odgovarajući izvor svjetlosti. Ukoliko je izvor svjetlosti prirodan tada je cijeli spektar boja prisutan, međutim kada je izvor svjetlosti lampa tada bi lampa trebala emitirati bijelu svjetlost, jer ona prema fizikalnim zakonima sadrži sve valne duljine ili sve boje. Takve su lampe na primjer fluorescentna lampa, ksenon lampa i lampa na principu hladne katode (engl. cold-cathode lamp). Fluorescentna lampa ne može dugo emitirati bijelu svjetlost i emitira toplinu, što može uzrokovati izobličenje. Ksenon lampa radi na nižim temperaturama, ali troši više energije.

KVALITETA KORIŠTENOG MATERIJALA

Na kvalitetu slike utječu do sada spomenuta vrsta senzora, šum na senzoru, količina fotoelemenata na senzoru i izvor svjetlosti. Pored navedenog na sliku može utjecati kvaliteta materijala u optičkom dijelu, mehanički dijelovi i utjecaj magnetskih i električkih polja.[219] Optički dio procesa usmjerava reflektiranu svjetlost prema senzoru i trebao bi biti takve kvalitete koja što manje iskrivljuje sliku, na primjer izrađena od stakla. Ili, može se koristiti prizma koja raspršuje bijelu svjetlost na različite boje. Mehanički dijelovi, zbog zahtjeva zadržavanja uniformnosti performansi tijekom cijelog vremena skeniranja treba biti odgovarajuće čvrstoće. Tijekom pretvaranja svjetlosti u elektronički signal dolazi do različitih električkih smetnji kao što je utjecaj magnetskih i električkih polja.

POKRETAČKI PROGRAM

Pokretački program se koristi za povezivanje skenera i računala. Dvije su različite tehnologije koje se koriste za rad skenera, TWAIN i ISIS.[220] TWAIN je razvijen 1992. godine od strane TWAIN Working Group kao besplatan proizvod otvorenog koda koji se, ovisno o postavkama korisnika, prilagođava. ISIS je razvio Pixel Translations 1990. godine, danas je vlasnik EMC Captiva, za potrebe skenera velikih volumena.

Razlika između ova dva pokretačka programa je u tome što TWAIN može kupac podešavati ovisno o svojim potrebama i funkcionalnost se mijenja ovisno o tim

[218] ibid.
[219] ibid.
[220] Buyers Laboratory Inc., NJ, USA. (2006.). Digital Imaging REVIEW, vol. 28. NO. 10. Preuzeto 16. 3. 2017. iz Fujitsu: http://www.fujitsu.com/downloads/COMP/fcpa/reviews/market-roundup-1006.pdf

karakteristikama, dok je ISIS standardiziran i unaprijed određen pri čemu EMC Captiva garantira istu funkcionalnost na svim uređajima koji ga koriste, odnosno ukoliko su potrebne druge funkcionalnosti tvrtka ih ugrađuje uz odgovarajuću nadoplatu.[221]

DUBINA BOJE

U početku su skeneri koristili 4 bitova što im je omogućavalo prikaz 2^4 odnosno 16 boja ili su koristili 8 bitova što im je omogućavalo prikaz 2^8 odnosno 256 boja. Skeneri koji koriste 48 bitova za prikaz boja mogu prikazati stotinu milijuna boja, što odgovara kvaliteti sličnoj kvaliteti fotografije. Sa 48 bitova moguće je lako prikazati 256 tonova crvene, plave i žute boje, 3 boje po 8 bitova za svaku što iznosi ukupno 24 bita, točnije moguće je prikazati 2^{16} tonova osnovnih boja jer za 3 boje po 16 bitova iznosi 48 bitova. Međutim ljudsko oko može razlikovati najviše 256 tonskih prijelaza, pa nije potrebno koristiti više od 24 bita.[222] Koliko će bitova biti iskorištenih ovisi o tome s koliko bitova može upravljati program za prihvat slike. Prednost veće količine bitova za prikaz boja je u tome što prilikom skeniranja dolazi do gubitka informacija zbog raznih šumova, nesavršenosti rada skenera i pretvarača.

TONSKA DINAMIKA

Tonska dinamika (engl. dynamic range) prikazuje razliku između najtamnijih i najsvjetlijih dijelova slike, tonskih prijelaza između njih i povezana je s kvalitetom A/D pretvarača te sa čistoćom izvora svjetlosti, kvalitete optike i razine šuma.[223] Mjeri se u rasponu od 0 do 4, gdje je 0 savršeno bijela i 4 savršeno crna, pri čemu je nemoguće imati tonsku dinamiku veću od 4. Što je veći broj tonske dinamike to je bolja slika, na primjer profesionalni skeneri imaju tonsku dinamiku veću od 3.5.

SKENIRANJE – KOLIČINA DPI

Prilikom skeniranja dokumenata postavlja se razumno pitanje koliko točaka po inču je potrebno kako bi se dobila kvalitetna slika. Na ovo pitanje je moguće odgovoriti promatranjem iz drugog kuta, odnosno iz kuta ispisa dokumenata na medij kao što je papir.

[221] ibid.
[222] Đurek, I. (8. 6. 2002.). DIGITALIZACIJA SVJETLA. Preuzeto 20. 3. 2017. iz Filos: http://www.filos.com/mkrzak/Djurek1.doc
[223] ibid.

Na primjer časopisi se ispisuju količinom od 133 lpi (engl. lines per inch; linija po inču op.a.). Pravilo za pretvorbu lpi u dpi je 2 x lpi = dpi.[224] Međutim, fotografije se pretvaraju u polutonove prije ispisa, koriste se dvije točke – po jedna za svaki poluton, zbog čega se preporuča 266 dpi-a za skeniranje.[225] Nadalje, ilustracije nastale iscrtavanjem (engl. line art illustration) pretvaraju se u polutonove prije ispisa pa se preporuča što veća količina dpi, na primjer 1200 dpi.[226] Slike koje se ispisuju na laserskim ili pisačima u boji rezolucijom od 300 do 600 dpi, odnosno 50 do 100 lpi, preporuča se rezolucija skeniranja od 100 do 200 dpi.[227] Ukoliko se nakon skeniranja obavlja optičko prepoznavanje znakova (engl. Optical Character Recognition; skr. OCR) tada se preporuča skeniranje u rezoluciji od 400 dpi jer daje bolje rezultate.[228]

[224] EasyCalculation.com. (n.d.). LPI To DPI Converter. Preuzeto 9.. 2. 2018. iz EasyCalculation.com: https://www.easycalculation.com/unit-conversion/lpi-to-dpi-converter.php
[225] UCONN College of Liberal Arts and Sciences, Biology Central Services. (n.d.). Scanning and scanners. Preuzeto 20. 3. 2017. iz Scanner Resolutions: http://www.bcs.uconn.edu/Illustration/content/Scanners_Resolution.pdf
[226] ibid.
[227] ibid.
[228] ibid.

7.2. Tehnički standardi

7.2.1. Vlada Alberte, Kanada

Vlada države Alberte u Kanadi propisala je IMT Standard broj A000015. Riječ je o Standardu za proces digitalizacije koji se primjenjuje u svim ministarstvima koja ulaze u proces digitalizacije s ciljem stvaranja digitalnih poslovnih zapisa[229]:

1. kojima je moguće dokazati autentičnost i pouzdanost,
2. koji su pravno prihvatljivi u zamjenu za izvorne dokumente,
3. koji su usklađeni s kanadskom normom CGSB 72.11-93,
4. kojima je moguće pristupiti u bilo koje vrijeme.

Prema IMT standardu proces digitalizacije uključuje slijedeće korake:

1. analiza procesa – prije početka projekta digitalizacije potrebno je napraviti detaljnu analizu temeljenu na primjerima dobre prakse.
2. propisivanje digitalizacijskog programa – mora sadržavati Priručnik digitalizacijskih procedura za slučaj da digitalizaciju obavlja treća strana, te sadrži detalje o provođenju digitalizacije i obrazloženje navedenih procedura.
3. priprema izvorne dokumentacije – sve procedure pripreme moraju biti opisane u Priručniku.
4. prihvat slike – proces skeniranja izvornog dokumenta, a u slučaju kada digitalizirana slika ne prođe kontrolu kvalitete ili provjeru osiguranja kvalitete ona se ponovno skenira i ponovno provjerava kvaliteta.
5. indeksiranje i metapodaci – obavlja se u četiri faze: skeniranje, ponavljanje skeniranja, osiguranje kvalitete i podatkovni transfer.
6. osiguranje kvalitete – osiguranje kvalitete moraju provoditi radnici koji nisu direktno uključeni u proces digitalizacije i indeksiranja, te se sve evidentira u revizijski zapis koji uključuje podatke: ime operatera, datum, je li zapis prošao test ili nije. Za minimalni nivo kvalitete potrebno je provjeriti 5-10% ukupnih digitaliziranih zapisa. U revizijski zapis se zapisuju prihvatljive granice pogreške kao i statistički način odabira podskupa digitaliziranih zapisa koji će biti provjereni.
7. pohrana slika – nakon provedbe kontrole kvalitete digitalizirane slike se automatski prenose u sigurne repozitorije, što može uključiti dodatnu kontrolu nad prenesenim podacima jesu li kompletni i točni.

[229] Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf

8. uvažavanje zahtjeva za upravljanje zapisima – potrebno je voditi računa o ovim zahtjevima tijekom cijelog procesa digitalizacije kako bi izvorni dokument i digitalizirani dokument zadovoljili ove zahtjeve.
9. kontrola kvalitete – validacija sustava se obavlja prilikom dizajna sustava i testiranja prihvaćanja od strane korisnika (engl. user acceptance testing). Kontrola kvalitete mora biti osigurana kroz sve faze digitalizacije. Sve testne točke moraju biti dokumentirane u Priručniku kako bi se smanjio rizik loše kvalitete slike i netočnih indeksnih informacija.
10. formiranje dnevnika zapisa – potrebno je voditi dnevnik po svim fazama procesa kako bi se mogao pratiti trag prolaska dokumenta kroz digitalizacijske faze.
11. poštivanje tehničkih zahtjeva – prema standardu A000013[230], vidi Tablicu 1.

Tehnički zahtjevi se odnose na minimalne zahtjeve za digitalizaciju, kontrolu kvalitete glavnog zapisa i minimalne zahtjeve za indeksiranje. Tehnički zahtjevi za digitalizaciju određuju kako se sva oprema treba održavati prema programu za održavanje koji je propisan i po kojem se postupa. Tablica 1 sadrži propisane karakteristike glavnog zapisa koji mora biti skeniran s minimalno 300 dpi (točaka po inču gledano prema zaslonu računala op.a.).

Tablica 1. Tehničke specifikacije prihvatljivih formata

vrsta dokumenta	tonalnost	bit	kompresija	format
crno-bijeli dokument	bitonalno	1	bez gubitaka	TIFF, PDF, PDF/A
dokument u boji	bitonalno ili boja	24	prihvatljivo s gubicima, poželjno bez gubitaka	TIFF, PDF, PDF/A
crno-bijela fotografija	siva skala	8	bez gubitaka	TIFF, PDF, PDF/A, JPEG
fotografija u boji	bitonalno ili u boji	24	prihvatljivo s gubicima, poželjno bez gubitaka	TIFF, PDF, PDF/A, JPEG

Kontrola kvalitete uključuje kontrolu odabira dokumentacije, kontrolu pripreme dokumentacije i kontrolu skenirane i ponovno skenirane slike. Uključuje čitljivost glavnih slika i kontrolu odgovara li broj skeniranih stranica broju dobivenih slika. Dopušteno je napraviti poravnanje (engl. de-skew) i brisanje praznih stranica, ali nije dopušteno automatsko brisanje pozadinskih točaka (engl. de-speckle). Dopušta se obaviti optimizacija PDF

[230] Government of Alberta. (1. 3. 2013.). Digitization Technical Requirements, Standard number A000013. Preuzeto 30. 9. 2016. iz http://imtdocs.alberta.ca/A000013_Digitization_Standards_Technical_v3.pdf

dokumenta na način da se slojevi (engl. layers) postave na vrijednost 0, optimizacija bijelog prostora (engl. white space) i različite kombinacije rasterizacije (engl. rasterization).

Minimalni zahtjevi za indeksiranje odnose se na biografske i bibliografske podatke i potrebno ih je zadovoljiti u fazama skeniranja, ponavljanja skeniranja, kontrole kvalitete i prijenosa podataka. Indeksni podaci se čuvaju minimalno do kraja čuvanja zapisa na koje se odnose.

Biografski podaci se odnose na životni ciklus slike povezan je s kontekstom slike i svojstava datoteke koja mora biti snimljena, zapisana i potvrđena tijekom digitalizacijskog procesa. U tablici (tablica 2) su popisani obavezni, preporučeni i izborni podaci kako ih sugerira IMT Standard.

Tablica 2. Biografski podaci

zahtjev	faza digitalizacije	indeksni podaci
obavezno	skeniranje	• oznaka slike • datum i vrijeme digitalizacije • broj stranica • naziv uređaja • naziv operatera • putanja do slike
obavezno	ponovno skeniranje	• oznaka slike • datum i vrijeme digitalizacije • broj stranica • naziv uređaja • naziv operatera • putanja do slike
obavezno	osiguranje kvalitete	• oznaka paketa • ime operatera koji provodi kontrolu kvalitete • datum odobrenja kvalitete
obavezno kad je primjenjivo	prijenos podataka	• datum prijenosa • naziv prijenosa • opis prijenosa • razlog prijenosa • potvrda primitka prijenosa

Bibliografski indeksni podaci se odnose na sadržaj i kontekst dokumenta, a odnosi se na ručni unos ili automatski unos podataka (ukoliko se provodi ručno indeksiranje moguće je napraviti dvostruko indeksiranje, nakon koje se obavlja automatska usporedba i razlike se ponovno ručno unose. U slijedećoj tablici (tablica 3) popisani su obavezni, preporučeni i izborni podaci kako ih sugerira IMT Standard.

Tablica 3. Bibliografski podaci

zahtjev	indeksni podaci
obavezno	• ime operatera • datum stvaranja • datum promijene • naslov
obavezno kad je primjenjivo	• alternativni naslov • opis • klasa sigurnosti • format • jezik • medij • identifikator
preporučeno	• predmet • ograničenja upotrebe
izborno	• opseg

Sva dokumentacija se može digitalizirati prateći ovaj standard međutim postoje određeni dokumenti koji se neće prihvatiti na sudu kao valjani dokument kao što su, na primjer, oporuke, dodaci oporukama, zaklade nastale na osnovu oporuka, pravne punomoći, zadužnice, vrijednosni papiri.

7.2.2. Kongresna knjižnica, Washington D.C.

Dokument Kongresne knjižnice navodi standarde koji se odnose na digitalizaciju fizičke dokumentacije i održavanje digitalizirane dokumentacije kako bi se mogle pratiti promjene i razvoj novih tehnologija.[231] Također navode se praktični alati kao što su kontrolni (kalibracijski) uzorci (engl. targets) pomoću kojih je moguće osigurati učinkovitost skeniranja i očuvanja zapisa. Navedeni standardi se odnose na terminološke definicije, specifikacije konverzijskih funkcija, rezoluciju, odstupanja, dinamički raspon, brzinu, uvjeti pregleda, održavanje boja, održavanje projekata, medije za pohranu, formate datoteka, funkcionalne zahtjeve za repozitorije digitalnih slika i kontrolu kvalitete. Pomoću kontrolnih uzoraka moguće je odrediti mogućnosti skenera, osigurati konzistentnost stvorenih slika, te kao dodatni podatak kontrolni uzorak služi za očuvanje zapisa koji je dokumentiran u procesu digitalizacije.

[231] Peterson, A. K. (2004.). Standards Related to Digital Imaging of Pictorial Materials. Preuzeto 30. 9. 2016. iz Library of Congress, Washington, D.C.: http://www.loc.gov/rr/print/tp/DigitizationStandardsPictorial.pdf

Konverzija papirnate građe u digitaliziranu započela je pilot projektima i programima 80-tih godina prošlog stoljeća, i slijedećih godina su nastajali i razvijali se standardi i dobre prakse kojima su se vodili radnici Knjižnice u postupku digitalizacije.[232] Tijekom vremena standardi su se mijenjali i u navedenom se dokumentu nalaze najsvježiji digitalizacijski standardi koje Knjižnica koristi. Standard se bavi digitalizacijom materijala koji sadrži bilo tekst bilo grafiku bilo oboje. Prepoznati slijed organizacijskih koraka uključuje: planiranje, produkciju, sastavljanje web okruženja i održavanje web stranica, pri čemu prva dva koraka uključuju: planiranje, prihvat digitalizirane slike uključujući karakteristike uređaja, rukovanje papirima, standarde kvalitete slike i proces kojim prolazi digitalizirana slika, zatim upravljanje digitaliziranom slikom što uključuje format datoteke, imenovanje i pohrana, te tehničke metapodatke pri čem se u oznaci zaglavlja TIF-a nalaze tehnički, strukturni i opisni metapodaci i metapodaci o očuvanju datoteke, te konačno faza osiguranje kvalitete.

Tijekom procesa planiranja projekta osim osnovnih opisnih podataka o projektu vodi se računa o predloženim materijalima, osnovnim karakteristikama digitalizacije, autorskom pravu, konzervaciji originala, dostupnosti, pohrani i ponašanju, odnosno ovlastima i kretanju digitaliziranog objekta.

Trenutni tehnički standardi određuju kako procesom digitalizacije nastaje glavni (engl. master) zapis, ili glavna slika ili glavni digitalizirani dokument, koji se sprema u glavno spremište iz kojeg se mogu pretvoriti datoteke u one primjerene za prikaz na web stranicama ili za distribuciju koju zovu kopija glavne slike. Ovisno o namjeravanoj upotrebi digitaliziranih dokumenata izrađuju se različiti oblici glavnih slika u TIFF formatu:

1. TIFF u sivoj skali – kada original nema boju ili nije bitna kao na primjer knjige, rukopisi, notni zapisi.
2. TIFF u sivoj skali visoke kvalitete ili u boji – kada postoji informacije u boji ili dokument ima umjetničku vrijednost, kao na primjer rijetke knjige, zemljopisne karte i fotografije.
3. TIFF u crno-bijelom tonu – za dokumente kojima je važan samo prikaz sadržaja.

Tehnički zahtjev glavnog zapisa je: TIFF verzija 6, bitonalna Group 4 kompresija, dok se slika u sivoj skali i slika u boji ne smiju komprimirati.

[232] The Library of Congress Technical Standards for Digital Conversion Of Text and Graphic Materials. (7. 3. 2007.). Preuzeto 30. 9. 2016. iz http://memory.loc.gov/ammem/about/techStandards.pdf

PRIPREMA

Prije skeniranja sva dokumentacija prolazi pregled potrebe konzervacije originala kao i provjeru potpunosti originalne dokumentacije pri čemu se dokumentaciji provjerava redoslijed i potpunost.

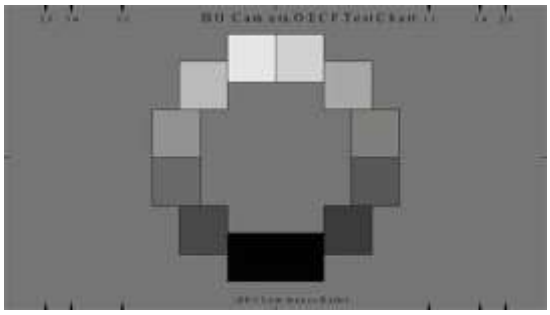
Važno je voditi računa da se ne uništava dokumentacija prilikom digitalizacijskog procesa, te se vodi računa o tome skenira li se knjiga ili druga uvezena dokumentacija ili na primjer osjetljiva dokumentacija koja je bila dugo presavijena kao što su na primjer stari notni zapisi. Oštećenja su moguća u slučajevima pretjeranog rukovanja, inverzija krhkih stranica, ravnanja, abrazivnih površina, prekomjerno osvjetljenje i prekomjerna toplina. Materijalima koji se nalaze na filmu a koji se ne nalaze u Mylarovim košuljicama je potrebno rukovati koristeći čiste pamučne rukavice. Osjetljivi materijali se ne smiju ravnati pomoću stakla niti se smiju okretati licem dolje tijekom skeniranja.

SKENERI

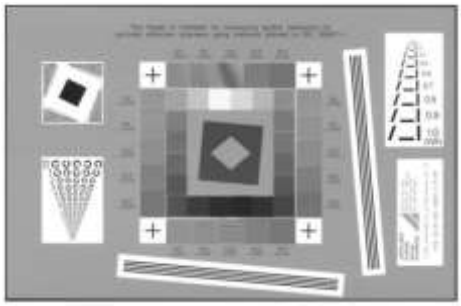
Skeneri se testiraju koristeći uzorke i kontrolne uzorke kojima se mjeri tonalna reprodukcija, dinamički raspon, šum, preciznost boje i dodatne karakteristike od važnosti za konkretnu primjenu. Pomoću ovih podataka operateri podešavaju (kalibriraju) uređaje i programe koji se koriste na projektu. Kontrolni uzorci se mogu koristiti tokom procesa i digitalizacije svake slike ili u određenim situacijama kao što je to na prvoj i zadnjoj stranici dokumenta. Tonalna reprodukcija se provjerava vizualnim pregledom uzorka i konkretnih slika odabranih iz skupa izlaznih slika nakon digitalizacije.

Primjeri kontrolnih uzoraka koji se koriste u Knjižnici vide se na slijedećim slikama (slike 5 do 8).

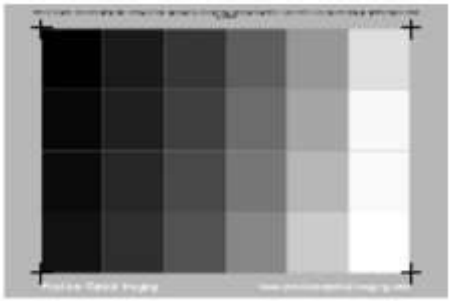
Slika 5. Kontrolni uzorak ISO-15739 za testiranje šuma digitalnog fotoaparata[233]



Slika 6. Kontrolni uzorak ISO-14524 za testiranje kontrasta digitalnog fotoaparata[234]



Slika 7. Kontrolni uzorak ISO-16067-1 za test skenera[235]



Slika 8. Kontrolni uzorak ISO 21550 za provjeru raspona tonske dinamike[236]

Kontrolni uzorci se koriste prije početka projekta, prilikom prve ugradnje opreme, prilikom ugradnje nove opreme, tijekom obuke novog operatera na procesima i uređajima za skeniranje, kada pregled zapisa o kvaliteti pokažu značajni porast problema s kvalitetom, na mjesečnom nivou za sve projekte koji isporučuju veću količinu serija digitalizirane dokumentacije. Ukoliko se nakon digitalizacije dokumenta obavlja optičko prepoznavanje znakova tada je zahtijevana razlučivost od 400 ppi (engl. pixels per inch; piksela po inču op.a.) i ciljana točnost od 90% riječi na pripremljenom tekstnom uzorku.

Ukoliko značajan broj digitaliziranih slika ne uspije postići zahtjeve projekta ponavlja se skeniranje cijele serije.

Tablica 4 pokazuje zahtjeve po tipovima dokumenata, očekivane rezultate i standarde parametara digitalizirane slike (dokumenta) [237].

[233] ISO-15739 Digital camera noise test chart. (n.d.). Preuzeto 9. 3. 2017. iz Sine Image: http://www.sineimage.com/en/ImageTest/Test_Charts/ISO_Test_Charts/38.html
[234] ISO-14524 Ddigital camera contrast chart. (n.d.). Preuzeto 9. 3. 2017. iz Sine Image: http://www.sineimage.com/en/ImageTest/Test_Charts/ISO_Test_Charts/ISO-14524.html
[235] ISO-16067-1 Scanner Test Chart. (n.d.). Preuzeto 9. 3. 2017. iz APPLIED IMAGE Inc: https://www.appliedimage.com/files/wFsNSe/QA-61_spec_v1-08.pdf
[236] ISO-21550 Dynamic Range. (n.d.). Preuzeto 9. 3. 2017. iz PRECISION OPTICAL IMAGING: http://www.precisionopticalimaging.com/products/products.asp?type=21550

Tablica 4. Zahtjevi po tipovima dokumenta

tip dokumenta	očekivani izlaz	standard parametara slike				bilješke
		rezolucija	dubina bita	faktor sive skale	točnost boje	
ispisan tekst na pisaču: knjige s ilustracijama, brošure, strojopisne stranice, novine	slika teksta	minimalno 300 dpi	8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%		
	OCR na tekstu	400 dpi	8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%		
glazba: notni zapisi, zapisi muzičkih nota za jednog muzičara, glazbeni rukopisi	pristup sadržaju	minimalno 300 dpi	*8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%		*ukoliko je boja važan atribut dokumenta trebalo bi koristiti boju 24-bita
	prepoznavanje obilježja artefakta	400 dpi	8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%		
rukopisi: rukom pisani, napisani na pisaćoj mašini	pristup sadržaju	minimalno 300 dpi	*8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%	za 24-bitnu boju delta-e < 8	*ukoliko je boja važan atribut dokumenta trebalo bi koristiti boju 24-bita
	prepoznavanje obilježja artefakta	400 ppi	8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%	za 24-bitnu boju delta-e < 8	
karte: tiskani tonovi, tiskani u boji, veličina do (22in x 34in)*	istraživanje sadržaja	minimalno 250 dpi	24-bitna boja		delta-e < 8	*dpi ovisi o veličini karte, osobito kada se dijelovi karte moraju „lijepiti“ jedan na drugi i kada veličina slike karte naraste do 500mb ili više
	reprodukcija karte	400 ppi	24-bitna boja		delta-e < 6 icc profil	

[237] The Library of Congress Technical Standards for Digital Conversion Of Text and Graphic Materials. (7. 3. 2007.). Preuzeto 30. 9. 2016. iz http://memory.loc.gov/ammem/about/techStandards.pdf

tip dokumenta	očekivani izlaz	standard parametara slike				bilješke
		rezolucija	dubina bita	faktor sive skale	točnost boje	
fotografije: kontinuirani ton, boja	pristup sadržaju	minimalno 300 dpi	*8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%	za 24-bitnu boju delta-e < 8	*ukoliko je boja važan atribut dokumenta trebalo bi koristiti boju 24-bita
	reprodukcija	maksimum uređaja	minimalno 24-bitna boja		delta-e < 6 icc profil	
grafička umjetnost: izvodi s ograničenim tonovima, kontinuirani ton, boja	pristup sadržaju	minimalno 300 dpi	*8-bitna siva skala	minimalno 18 koraka minimalno 5.5 f-zaustavljanja šum y kanala <=5%	za 24-bitnu boju delta-e < 8	*ukoliko je boja važan atribut dokumenta trebalo bi koristiti boju 24-bita
	reprodukcija	maksimum uređaja	minimalno 24-bitna boja		delta-e < 6 icc profil	
rijetke knjige: predmeti visoke umjetne vrijednosti	prepoznavanje obilježja artefakta	minimalno 400 dpi	24-bitna boja		delta-e < 8 icc profil	
	istraživanje obilježja artefakta	minimalno 600 dpi	minimalno 24-bitna boja		delta-e < 5 icc profil	

Nakon skeniranja i dostave u centralnu prihvatnu točku obavlja se pregled digitalizirane dokumentacije pomoću softvera koji pregledava potpunost propisanih tehničkih karakteristika i dogovorenih standarda. Obrada digitalizirane slike može uključivati popravljanje rotacije, oštrine, tonalnog raspona i boje. Podaci o transformaciji boje moraju se upisati u tag 34675 i slika se mora pohraniti kao 24-bitna TIFF datoteka. Izrezivanje slike (engl. cropping) se ne smije raditi, a u nekim slučajevima potrebno je imati dodatni rub kako je propisano u tehničkom standardu.

OSIGURANJE KVALITETE

Kvaliteta se provjerava nakon zaprimanja digitalizirane dokumentacije pomoću automatiziranog programa koji provjerava točnost formata, zahtijevane metapodatke i propisano imenovanje datoteka. Zatim se vizualno provjeravaju odabrane slike u veličini 1:1 kako bi se osigurala specificirana kvaliteta. Točnost mora biti potpuna za: format datoteke, sadržaj zaglavlja i tagova datoteke, algoritama kompresije i rezolucije dubine bita. Točnost od 99,5% je zahtijevana za propisano imenovanje datoteke, nedostajuće slike, duple slike i slike koje su nevaljale. Program automatski zapisuje greške kada pređu zahtijevanu točnost.

Prilikom vizualne kontrole zahtijeva se točnost od 99,5% za: mutne ili nejasne slike, gubitak posebnih karakteristika ili linija, nepotpunost u sadržaju, iskrivljenje, neuspjelu obradu nijansi slike i neuspjelo prikazivanje naslova. U kontroli šuma ne prihvaćaju se slike kojima je zamagljen detalj, iskrivljena boja i objekt, ili ima značajne šare na inače glatkim površinama. Rezolucija se može provjeriti i programski ukoliko postoji OCR, smanjena količina pročitanih podataka može biti pokazatelj da je rezolucija neadekvatna (prema iskustvu djelatnika Knjižnice 400 dpi daje bolje rezultate prilikom OCR-a). Oštrina slike se vizualno provjerava u tamnim i svijetlim točkama originala. Tijekom vizualnog pregleda sve procjene se upisuju u standardizirani upitnik prema dogovorenoj listi pregleda i izrađuje se izvješće. Vizualni pregled obavlja operater prilikom skeniranja.

Minimalna količina slika koje se provjeravaju ili kojima se testira kvaliteta je 10% ukupne količine digitaliziranih slika u jednoj seriji ili minimalno 10 slika, ovisno o tome koji broj je veći.

7.3. Softveri za digitalizaciju

Proizvođači uz svoje skenere nude različita softverska rješenja koja su potrebna tijekom procesa skeniranja. Pored rješenja koja se isporučuju uz skenere moguće je koristiti drugačija rješenja ali uz određenu nadoplatu. Softver za digitalizaciju ScandAll-PRO isporučuje se uz Fujitsu skenere i ima određene mogućnosti koje se kombiniraju s mogućnostima pokretačkog programa. Pri tome je potrebno voditi računa da se određene funkcionalnosti ne poništavaju. Rješenje Capture Perfect omogućava slične funkcionalnosti kao i prethodni softver s dodatnom mogućnošću izrade PDF datoteke kojoj se ograničava pregled, ispis i određivanje lozinke za otvaranje datoteke. Rješenje DpuScan je puno kompleksnije od navedenih rješenja i omogućava puno više funkcionalnosti. Također, za rad s DpuScanom potreban je nepromjenjiv ključ čime se omogućava nadzor ili kontrola korištenja samog softvera.

7.3.1. DpuScan

DpuScan je skenerski program s mnoštvom mogućnosti organiziranih u četiri razine[238]:

1. osnovna,
2. standardna,
3. profesionalna,
4. zlatna,

pri čemu svaka dopušta određeni nivo mogućnosti.

Za svoj rad DpuScan treba .NET-Framework 2.0, i posebne licenčne opcije[239]:

1. USB Dongle (nepromjenjiv ključ na USB nosaču),
2. Product Key and Activation Key (aktivacijski ključ za proizvod i za aktivaciju),
3. DpuServer (rješenje ugrađeno na serversko računalo s administracijskim profilom).

Ovaj softver omogućava izradu protokola za serijsku digitalizaciju pripremljenih paketa (engl. batch processing) kojim je moguće odrediti obradu svake vrste i tipa dokumentacije osiguravajući da se svi dokumenti skeniraju u istim postavkama. Omogućava skeniranje jednostrano i obostrano, u boji, sivoj skali i crno-bijelo. Pretvorba slike iz sive skale u crno-bijeli ton je također moguća korištenjem filtra boje, odnosno korištenjem kombinacije filtra za crvenu, zelenu i plavu boju kao da su tri kamere koje očitavaju svaka svoju boju, čime je moguće postići odvajanje plave tinte kemijske olovke od plave pozadine, ili odvajanje teksta ispisanog ispod crveno označenog teksta. Uklanjanje boje je omogućeno i preko složenih algoritama koji prilikom odluke o dodjeljivanju boje određenoj točki u obzir uzimaju okolne točke.

U nastavku će detaljno biti opisane sve opcije koje ovaj softver nudi, jer će se na temelju njih kasnije argumentirati da one mogu utjecati na proces digitalizacije s ciljem osiguranja autentičnosti.

U tijeku obrade, nakon skeniranja, softver omogućava razne opcije poboljšanja slike, kao što je na primjer uklanjanje točaka, poravnanje slike, uklanjanje sjene, uklanjanje linija, poboljšanje rubova, rezanje slike i tako dalje, prepoznavanje barkodova u svim smjerovima, moguće je prepoznavanje više od jednog barkoda i različitog tipa, svi očitani barkodovi se

[238] Janich & Klass Computertechnik GmbH. (n.d.). We made Document Capture Easy and Efficient: DpuScan 4.0, The universal Scan Sotfware for Color and black/white. Preuzeto 24. 3. 2017. iz Dpuscan: http://www.dpuscan.de/pdf/DpuScan-Brochure-english.pdf

[239] Janich & Klass Computertechnik GmbH. (n.d.). Getting Started. Preuzeto 24. 3. 2017. iz Dpuscan: URL:http://www.dpuscan.de/pdf/GettingStarted.pdf

mogu spremiti u posebnu datoteku, pretraživanje barkoda može se ograničiti na dio skenirane stranice i automatskog prepoznavanja teksta OCR alatom pri čemu se očitani podaci mogu pohraniti u posebnom dokumentu u RTF formatu za daljnju obradu. Također, moguće je tijekom obrade unositi određene podatke kroz korisničke dijaloge, kao i, ovisno o pročitanim barkodovima, OCR rezultatima, brojačima, varijablama, veličinama datoteke i slično, upravljati događajima koji se pokreću ovisno o navedenim očitanjima.

Slikama je moguće dodavati Batesove pečate (engl. Bates stamping; elektronički pečat kojim se upisuje slika ili tekst direktno na digitaliziranu sliku na unaprijed definiranu poziciju op.a.), izraditi statističke datoteke u koje se upisuju sve akcije i korekcije koje je bilo potrebno napraviti tijekom procesa skeniranja. Moguće je upisati slijedeće: vrsta protokola, ime stanice, podaci o korisniku, podaci o zadatku (engl. task), podaci o poslu (engl. job), datum početka i završetka zadatka, vrijeme početka i završetka zadatka, broj skeniranih slika, broj pohranjenih slika, broj pohranjenih datoteka, broj mijenjanih slika, broj ponovljenih skeniranja dokumenata, broj slika promijenjenih kroz prozor za promjenu, broj obrisanih slika, broj stvarnih skenerskih pogrešaka kao na primjer zaglavljivanje papira, dvostruki ulazak papira itd., broj poziva korisničkih dijaloških okvira, broj ručno postavljenih oznaka, broj ručno pomaknutih slika i novih paginacija, korišteni korisnički parametri, moguće je privremeno pohranjivanje nekomprimiranih podataka iz kojih se naknadno rade izračuni i odluke kako bi se spriječio gubitak podataka.

Nakon što je slika obrađena, DpuScan se može povezati s aplikacijom za vođenje arhiva dokumenata, nekim poslovnim procesom ili sustav za upravljanje dokumentima (engl. Document Management System; skr. DMS).

Putem softvera mogu se odrediti postavke skenera kao što je veličina papira, svjetlina, kontrast, rezolucija, jednostrano ili obostrano skeniranje, pejzažno usmjerenje, rotacija (inverzija, 90^o, 180^o ili 270^o), odvajanje presavijenog višestraničnog dokumenta u jednostruke slike, rezanje crnih kutova dokumenta i poravnavanje, vodoravna i okomita poravnanja odnosno korekcije slike poravnavajući skenirani dokument u lijevi i gornji dio slike.

Slike se mogu spremati u slijedećim oblicima:

1. TIFF – pojedinačne slike ili više slika u jednoj datoteci, slike mogu biti u sivoj skali ili u boji, mogu biti komprimirane na bilo koji niže navedeni način, bitonalne slike se spremaju u kompresiji G4, u zaglavlju datoteke je moguće upisati do 8 podataka kao na primjer broj posla, broj skeniranih stranica, datum i vrijeme, naziv računala, korisničko ime,
2. JPEG/JFIF – samo za pojedinačne slike u datoteci, i samo za slike u boji ili sivoj skali,

3. PDF – pojedinačne slike ili više slika u jednoj datoteci, slike mogu biti u boji, sivoj skali ili bitonalne kao i u kombinaciji,
4. PDF/A – kao PDF ali sadrže samo slike bez dodatnih objekata kao što je tekst i po tome zadovoljavaju PDF/A-1b standard,
5. pretraživi PDF – može sadržavati dodatne informacije, ali ne može stvoriti PDF/A dokument,
6. JPG2000,
7. skenerski sirovi podaci (engl. raw data)

i razinama kompresije:

1. G4 – po CCITT normi koja je bez gubitaka,
2. LZW – također bez gubitaka, samo za TIFF datoteke u boji ili sivoj skali,
3. JPEG – postoje gubici tako da podaci više ne odgovaraju točno originalnim podacima slike, manje je prilagođena linearnoj grafici a više slikama koje imaju blage tranzicije boja,
4. JPEG2000,
5. bez kompresije.

Omogućena je izrada profila protokola kojem se određuju postavke za slijedno skeniranje pripremljenih paketa, kojem se ograničava korištenje onemogućavajući promjenu slike, ili omogućavajući označavanje slike koja bi trebala biti obrisana, dok drugi korisnik obavlja brisanje slike ili uklanja oznaku za brisanje. Unaprijed su definirane tri vrste korisnika: administrator, gost i svi, a može se omogućiti ili zabraniti na primjer dodavanje prazne slike, dodavanje slike kopiranjem, iz datoteke/a, nakon filtra, sa skenera, ali i mnoštvo drugih postavki. Preporuka proizvođača je definirati nove korisnike i za svakog odrediti što smije a što ne smije mijenjati unutar profila.[240]

DpuScan omogućuje dodavanje određenih funkcionalnosti preko dodatnih modula (engl. plug-in): indeksiranje, povezivanje s bazom podataka putem ODBC veze (engl. Open DataBase Connectivity; način povezivanja s bazom podataka op.a.), smanjenje šuma u boji (engl. color noise reduction), optičko prepoznavanje oznaka (engl. Optical Mark Recognition; skr. OMR), prepoznavanje rukom pisanih dokumenata (engl. Intelligent Character Recognition; skr. ICR) i dodatni softver za optičko prepoznavanje znakova, gama korekcija na slikama u boji i slikama u sivom tonu, poboljšanje rubova za slike u boji i sivim tonovima,

[240] Janich & Klass Computertechnik GmbH. (2010.). User Manual, DpuScan 5, Document Scanning and Document Processing. Preuzeto 24. 3. 2017. iz Dpuscan: http://www.dpuscan.de/pdf/DpuScan-User-Manual.pdf

čitanje dvodimenzionalnih barkodova, prepoznavanje lica na slikama u boji (engl. facesnap), ekstrakcija i skaliranje potpisa, dodavanje digitalnog potpisa.

7.3.2. ScandAll-PRO

ScandAll Pro je aplikacija za prihvat digitalizirane slike koja je u skladu s TWAIN/ISIS standardom koristeći TWAIN, ISIS ili Kofax VRS pokretački program.[241] Koristi se za digitalizaciju papirnate građe kod rutinski obavljanog posla.

Mogućnosti aplikacije uključuju uređivanje skeniranih slika, prepisivanje podataka, pohranu uređivanih podataka pod različitim nazivom i tipom datoteke, osim u slučaju PDF tipa datoteke koji nije moguće spremiti pod drugim tipom nakon uređivanja podataka, te istovremeno stvaranje digitalizirane slike u boji ili jednobojne. Tip datoteke može biti BMP, JPEG, JPEG2000, TIFF, PDF i PDF/A, pri čemu PDF i PDF/A mogu biti pretražive datoteke i datoteke s visokim stupnjem kompresije. Automatska pohrana je omogućena bilo u mapu na lokalnom disku bilo na unaprijed određeni server. Također, omogućen je OCR, zonalni OCR i prepoznavanje barkoda čiji se rezultati mogu spremiti u zasebnu datoteku, kao i pokretanje određenih programa kojima je ulazni parametar izlazna digitalizirana slika ili indeksirana informacija.

Za rad aplikacije preporuča se procesor Intel Core 2 Duo 2.2 GHz ili viši, 2 GB memorije, te minimalno 1,3 GB diskovnog prostora.

Kada je potrebno skenirati veće količine dokumenata s istim zahtjevima i postavkama skeniranja to je moguće napraviti izradom profila i pohranom postavki profila.

Posebna funkcija ADF Virtual Duplex omogućava skeniranje paketa papira prvo s jedne strane a zatim s druge strane nakon čega funkcija pravilno razmješta i slaže prve strane pa druge strane originalnih dokumenata.

Dokumente koji imaju više stranica moguće je odvojiti koristeći *patch kod* ili određivanjem točno određenog broja stranica koje mogu biti u jednom dokumentu. Aplikacija omogućava odjeljivanje i stvaranje višestraničnih dokumenata koristeći jednodimenzionalne barkodove UPC/EAN/JAN, CODE39, CODE128/EAN128, CODABAR NW7 i ITF ili dvodimenzionalne barkodove PDF417 i QR code, koji moraju biti crni na bijeloj podlozi, rezolucije 200 do 600 dpi, orijentirani okomito ili vodoravno, visine 10 do 30 mm, širine 300 mm i margine 5 mm sa svih strana.

[241] ScandAll PRO V2.0 User's Guide. (6. 2012.). Preuzeto 24. 3. 2017. iz PFU LIMITED: URL: http://origin.pfultd.com/downloads/IMAGE/manual/p2ww-2860-03enzo.pdf

Kod zonalnog OCR-a aplikaciji se određuje prostor skeniranog dokumenta koji će se uzeti u obzir za prepoznavanje simbola, a rezultat je moguće koristiti kao indeksni podatak, za naziv datoteke, koji je ograničen na najviše 32 znaka, ili za naziv mape. Međutim, potrebno je voditi računa o rezoluciji koja mora biti 400 ili 600 dpi za jednobojne slike, odnosno 200 ili 300 dpi za slike u boji ili sivoj skali.

Kada je važno da aplikacija ne prebriše već postojeću datoteku moguće je zadati stvaranje nove mape svaki puta kada se pokreće protokol za skeniranje paketa.

Prilikom rada s protokolom za skeniranje paketa stvorene datoteke se privremeno spremaju u pomoćnu mapu, koju je moguće koristiti ukoliko dođe do prekida u radu aplikacije zbog nekog prioritetnijeg posla, te se vratiti privremeno pohranjenoj datoteci i nastaviti rad.

Kao indeksne podatke moguće je aplikativno pospremiti u datoteku: rezultat zonalnog OCR-a, prepoznati barkod, naziv datoteke s cijelom putanjom, broj stranice u dokumentu, te povezati indeksnu datoteku s nekom aplikacijom. Ove indeksne podatke je moguće spremiti u Unicode tekst formatu, CSV formatu ili XML formatu.

Aplikacija sama obavlja određene sigurnosne provjere kao što su pokidani rubovi dokumenta ili savinuti rubovi dokumenta, prolazak dvostrukog papira ili prolazak papira različitih dimenzija.

7.3.3. Capture Perfect

Capture Perfect je aplikacija koja omogućava prihvat digitaliziranih slika koje stvara Canonov skener i kompatibilan je s ISIS/TWAIN pokretačkim programima i u suradnji s njima i njihovim mogućnostima obavlja prihvat slike.

Digitalizirane slike je moguće spremiti kao TIFF, BMP, JPEG, PDF ili PowerPoint datoteke kao crno-bijele, naizgled u skali sive (engl. error diffusion; crne točke se razmještaju tako da daju izgled slike u skali sive, op.a.), poboljšanog teksta, naprednog poboljšanog teksta, poboljšanog teksta visokih brzina, 256 tonova sive, 24-bita u boji, ili na način automatskog određivanja slike u boji ili binarne slike. Rezolucije koje su dopuštene su: 100 dpi, 150 dpi, 200 dpi, 240 dpi, 300 dpi, 400 dpi, 600 dpi i 1200 dpi. Također, aplikacija omogućava zanemarivanje crvene, zelene i plave boje, odnosno pojačavanje crvene, zelene i plave boje i njihovih kombinacija.[242]

Tablica 5 prikazuje moguće kompresije i tonove boja ovisno o tipu datoteke.

[242] CANON. (2007.). Canon CAPTUREPERFECT 3.1 Operation Manual. Preuzeto 24. 3. 2017. iz manualslib the ultimate manuals library: https://www.manualslib.com/manual/24880/Canon-Captureperfect-3-1.html

Tablica 5. Kompresija i ton boje po tipovima datoteke

tip datoteke	kompresija	ton boje
TIFF	CCITT Group 4	bitonalno
TIFF	OLD JPEG(6) i OLD JPEG(7)	siva skala ili boja
PDF i PDF/A	visoka kompresija	siva skala ili boja
PDF i PDF/A	standardna kompresija	siva skala ili boja
PDF i PDF/A	prednost karaktera	siva skala ili boja
JPEG	visoka kvaliteta	siva skala ili boja
JPEG	standardna kvaliteta	siva skala ili boja
JPEG	visoka kompresija	siva skala ili boja
JPEG	ručno podešavanje	siva skala ili boja

Ukoliko se PDF datoteke spreme zajedno s OCR podacima poravnanje se obavi automatski.

PowerPoint kao izlaznu datoteku je moguće odrediti samo kada je rezolucija skenera postavljena na 300 dpi i u sivoj skali ili u boji, pri čemu je moguće napraviti OCR za birani jezik i dodatnu datoteku željenog tipa.

Aplikacija omogućava spremanje digitaliziranih slika u datoteke koje imaju jednu, više ili određeni, ali točan, broj slika.

Omogućeno je određivanje imena datoteka kao i mapa u koje se spremaju stvorene datoteke. Za izradu imena datoteke moguće je koristiti slijedeće podatke: barkod ili OCR, do maksimalno 64 znaka, ili imprinter koji ispisuje podatke na skenirani dokument, datum, skenirana strana, tip slike, rezolucija, izbačena boja, separator, brojač koji može biti i automatske vrijednosti ili točno određene vrijednosti koje se odnose na: broj znakova, početnu vrijednost, pomak za vrijednost i vrijednost od koje se ponovno pokreće brojač. Ukupan broj znakova u imenu datoteke ne smije prijeći 200 znakova. Prilikom određivanja imena mape omogućen je upis: barkoda ili OCR do maksimalno 64 znaka, datum, separator i brojač koji može biti i automatske vrijednosti ili točno određene vrijednosti koje se odnose na: broj znakova, početnu vrijednost, pomak za vrijednost i vrijednost od koje se ponovno pokreće brojač.

Capture Perfect omogućava, ukoliko skener to može podržati, spremanje datoteka različitih tonova, na primjer: boja i crno-bijela, ili siva skala i crno-bijela, istovremeno, neovisno o tome je li skenirana prednja strana ili stražnja strana ili obje strane. Istovremeno se u imenu datoteke upisuje oznaka radi li se o primarnoj datoteci ili sekundarnoj datoteci.

Kada se provodi OCR skeniranog dokumenta moguće je odrediti prostor slike na kojem će biti obavljen OCR i jezik koji se prepoznaje. Rezultat prepoznavanja putem OCR-a

bilo teksta bilo barkod oznaka sprema se u datoteku u CSV formatu, pri čemu je omogućeno obaviti potrebne modifikacije u prepoznatom rezultatu.

Od ostalih mogućnosti koje Capture Perfect daje tu su: okretanje slike – rotacija lijevo, desno i za 180^{o}C, spremanje slike kao dvije slike – dvostruka slika, slika podijeljena vodoravno i okomito što se može koristiti kada se želi A3 spremiti kao dvije A4 slike, odvajanje datoteke – pomoću patch koda ili barkoda pri čemu je moguće spremiti odjeljivač kao i stvoriti novu mapu ili dodati sliku već postojećoj datoteci. Dodavanje slike je omogućeno samo za tip datoteke TIFF ili PDF i u tom slučaju je moguće zamijeniti ili dodati novo skeniranu sliku ili već postojeću sliku spremljenu u datoteku.

Skenirati se može dokument po dokument, stranica po stranica, ili više stranica odjednom preko unaprijed pripremljenog protokola za snimanje paketa.

Osim u definirane mape aplikacija omogućava slanje skeniranih datoteka na SharePoint server pri čemu je moguće odrediti informacije koje će biti proslijeđene kao što je komentar, ručni unos svojstava datoteke ili automatski unos svojstava datoteke.

Dodatna mogućnost koju aplikacija nudi je stvaranje PDF datoteke s ograničavanjem pregleda, ispisa ili uređivanja datoteke koristeći lozinku za otvaranje datoteke, i/ili lozinku za promjenu autorizacije i lozinke, te koristeći enkripcijski nivo: 128-bit RC4 ili 40-bit RC4.

Navedene opcije i mogućnosti koje aplikacija Capture Perfect nudi odnose se na slike koje je ISIS/TWAIN pokretački program prethodno oblikovao.

7.4. XML

U ovome dijelu će se objasniti uloga XML-a u procesu digitalizacije. U svom radu Kirasić piše kako je SGML (engl. Standard Generalized Markukp Language) složen i opsežan jezik iz obitelji jezika za označavanje i opisivanje dokumenata i podataka, a XML (engl. Extensible Markup Language) je njegov podskup kojim zapisujemo dokumente i podatke u tekstualnom obliku, kao na primjer HTML koji je osnovni jezik za izradu Web stranica.[243] Velika prednost XML-a je u tome što korisnici mogu sami odrediti dozvoljene oznake koje će se koristiti za opisivanje dokumenata i podataka, pri čemu sve strane uključene u komunikaciju trebaju koristiti iste oznake. Također, prednost je što je XML tekstualni format koji je neovisan o računalnoj platformi i operacijskom sustavu jer je njegov standard i

[243] Kirasić, D. (n.d.). XML tehnologija i primjena u sustavima procesne informatike. Preuzeto 20. 3. 2017. iz IEEE Hrvatska sekcija: http://www.ieee.hr/_download/repository/mipro_xml_tekst.pdf

specifikacija javna i dostupna svima. Postoji minimalan skup pravila koje XML dokument mora zadovoljiti, ali imena oznaka nisu unaprijed definirana.

Minimalan skup pravila koje XML mora slijediti kako bi se označio kao „ispravno formiran“ je:

- dokument bi trebao početi s XML deklaracijom,
- postoji samo jedan korijenski element,
- imena elemenata ili atributa ne smiju sadržavati praznine,
- elementi koji nisu prazni moraju imati početnu i završnu oznaku,
- prazni element ima na kraju oznake znak „/“,
- elementi moraju biti ispravno ugniježđeni,
- atributi unutar istog elementa moraju imati jedinstvena imena,
- vrijednost atributa se mora definirati unutar navodnika,
- u sadržaju elemenata ili vrijednostima atributa ne smijemo izravno koristiti znakove: < > & već moramo koristiti reference na predefinirane entitete: < > &.

XML dokument se sastoji od XML deklaracije, elemenata (od čega je samo jedan korijenski element), te atributa elemenata, ali može sadržavati i slijedeće:

- komentare,
- procesorske naredbe,
- DTD i XML shemu,
- reference na entitete, u DTD sekciji se definira vrijednost entiteta, koja se može pozivati kroz cijeli XML dokument,
- CDATA sekcije koje se koriste kada želimo unijeti tekst koji je potrebno tumačiti kao običan tekst kao što je sadržaj u kojem se nalaze kontrolni znakovi.

Također, XML podržava imenike (engl. namespace) pomoću kojih možemo spajati dijelove jednog XML dokumenta s dijelovima drugog XML dokumenta.

Ako XML dokument pored minimalnih uvjeta zadovoljava ograničenje iz DTD-a ili XML sheme tada kažemo da je „valjan“.

Ukoliko želimo odrediti tip atributa ovisno o sadržaju tada koristimo:

- CDATA = niz znakova,
- vrijednost1|vrijednost2|... – mi određujemo koje vrijednosti su prihvatljive,
- ID = vrijednost je jedinstvena oznaka,
- IDREF = vrijednost je jedinstvena oznaka drugog elementa,
- IDREFS = vrijednost je lista drugih jedinstvenih oznaka,
- NMTOKEN = ispravan naziv XML-a,

- NMTOKENS = lista ispravnih naziva XML-a,
- ENTITY = entitet,
- ENTITIES = lista entiteta,
- NOTATION = naziv notacije,
- xml = unaprijed definirana vrijednost XML-a.

Atributi mogu imati i svoje vrijednosti:

- #REQUIRED – vrijednost atributa mora biti navedena,
- #IMPLIED – vrijednost atributa ne mora biti uključena,
- #FIXED – vrijednost je fiksno određena,
- kada nije zadana vrijednost u dokumentu podrazumijeva se da je fiksno zadana.

XML shema, kao i DTD, ima ulogu postavljanja uvjeta i ograničavanja sadržaja i strukture XML dokumenta, definiranja rječnika oznaka i gramatike koji se mogu pojaviti u dokumentu te odrediti pravila kojima se određuje je li XML dokument valjan.

Velika prednost XML-a je upravo u dijelovima XML sheme i DTD-u jer su to mehanizmi kojima se mogu odrediti formati zapisa podataka i dokumenata što omogućava programima provjeru jesu li primljeni podaci u dogovorenom i potrebnom formatu, čime se izbjegavaju određene greške.

Primjeri:

1. Primjer tekstualne datoteke u XML formatu:

```
<?xml version="1.0" encoding="UTF-8" ?>
<memo>
	<contact type="person">
		<name>Ivo Ivić</name>
		<mobile>098 1234567</mobile>
		<email>ivo.ivic@fer.hr</email>
	</contact>
	<contact type="company">
		<name>Best Corporation</name>
		<mobile>091 123456</mobile>
		<email>best@best.com</email>
	</contact>
	<contact type="person">
		<name>Josip Horvat</name>
```

```
            <mobile>098 123456</mobile>
            <email>josip.horvat@fer.hr</email>
        </contact>
</memo>
```

Ovo je primjer XML dokumenta koji služi za prijenos podataka o kontaktima za ljude i tvrtke. Korištene oznake se nalaze unutar < i > znakova. I one se mogu proizvoljno odrediti. Elementi koje se prenose pomoću ovog primjera XML-a su: <memo>, <contact>, <name>, <mobile>, <email>. Također, jedan od pravila je da XML ima samo jedan korijenski element, u ovom primjeru je to: <memo>, dok je <contact> podelement koji ima svoje atribute: <name>, <mobile> i <email>.

Prvi red: <?xml version="1.0" encoding="UTF-8" ?> označava XML deklaraciju koja obavezno, ako postoji, mora biti na početku dokumenta u koju se upisuje verzija koja se koristi, u ovom slučaju verzija 1.0, te tip znakova, u ovom slučaju UTF-8 znači Unicode Transformation Format 8.

Dodatno se iz ovog primjera vidi kako element <contact> ima dvije mogućnosti što je označeno s atributom <type> a to su <person> i <company>.

2. Komentar

```
<!-- XML komentar -->
```

Ovako se ispravno pišu komentari, oni služe za pojašnjavanje dijelova dokumenta kada je to potrebno i omogućavaju veću preglednost i bolje snalaženje. Komentar se uvijek mora započeti s „<!--„ a završiti s „-->“.

3. Procesne naredbe

```
<? progABC inputParam="123" ?>
```

Programi koji obrađuju XML tekstualnu datoteku ovisno o dogovorenim oznakama preuzimaju podatke te ih na primjer pohranjuju u bazu. Međutim, moguće je predati i informaciju o programu koji je potrebno pokrenuti kao u gornjem primjeru pokrenuti će se program progABC s početnim parametrom „123“. Ovo se naziva procesnom naredbom i njih

je moguće imati unutar XML dokumenta proizvoljan broj, a moguće je s njima postići određeni stupanj kontrole ukoliko je to potrebno.

4. DTD

```
<!DOCTYPE memo [
        <!ENTITY best "Best Corporation, The best is not good enough">
        <!ELEMENT memo (contact)* >
        <!ELEMENT contact (name, mobile, email)>
        <!ELEMENT name (#PCDATA) >
        <!ELEMENT mobile (#PCDATA) >
        <!ELEMENT email (#PCDATA) >
        <!ATTLIST contact type CDATA #REQUIRED >
]>
```

DTD određuje opis i ograničenja na dozvoljeni sadržaj XML dokumenta. Povezano s gornjim primjerom 1. vidimo definirano značenje entiteta <best> ("Best Corporation, The best is not good enough"), zatim <memo> koji je korijenski element s 0 ili više elemenata, to je informacija koju daje oznaka „*“, koji se zovu <contact>, dok podelement <contact> može imati atribute: <name>, <mobile>, <email>. Podelementima je određeno u kojem obliku moraju pisati vrijednosti, na primjer #PCDATA znači da se radi o proizvoljnom tekstu. Podatak ATTLIST govori o definiranju atributa <contact> koji može biti niz znakova, odnosno CDATA koji je i obavezan je podatak, označeno s #REQUIRED.

7.5. Zaključak

Zapisivanje podatka o korištenom uređaju pomaže prilikom određivanja skenera koji je izradio sliku postupkom analize neispravnih točaka koje se nalaze u slici i koja se primjenjuje u forenzičkoj analizi digitalne slike. Ovisno o broju točaka po inču za potrebu dobivanja željene rezolucije potrebno je obaviti interpolaciju ili ekstrapolaciju pročitane linije. Bolji rezultati se dobivaju kada se cijeli skup u punoj rezoluciji smanji u memoriji skenera što uvjetuje tehniku ekstrapolacije i postojanje većeg skupa točaka po inču u senzoru. Nesavršenost proizvodnje točaka u senzoru dodatno zahtjeva postojanje veće količine točaka po inču u senzoru. Prijedlog od 400 dpi za potrebe primjene OCR tehnologije znači da točaka

po inču u senzoru ne smije biti manje od 400, pri tome se misli na optičku razlučivost, pa se predlaže koristiti senzore koji imaju 600 ili više točaka po inču u senzoru. Najčešće korišteni senzori u skenerima za brzo skeniranje paketa dokumentacije su CIS, CMOS ili CCD. CCD senzor koristi *global shutter* efekt koji dalje bolje rezultate.

Slika nastaje zbog odbijanja svjetlosti od papira u različitim valnim duljinama te prihvatom pomoću senzora i slanjem dalje u postupak obrade. Svjetlost u tom slučaju treba biti bijela jer sadrži sve valne duljine, međutim izvor svjetlosti ne bi trebao emitirati toplinu jer može dovesti do izobličenja proslijeđenih podataka. Upravo zbog ovih mogućih izobličenja skener treba biti napravljen od odgovarajućih materijala i čvrstoće koje će smanjiti ili spriječiti izobličenja u neželjenim trenutcima. Tako optički dio treba biti od stakla, mehanika odgovarajuće čvrstoće i elektronički signal treba zaštititi od utjecaja magnetskih i električnih polja. Zatim, za ispravno prikazivanje boja potrebno je koristiti dovoljan broj bitova koji ne treba biti viši, ali ni manji od 24, a tonska dinamika treba biti veća od 3,5.

Stvaranje slike ovisi o korištenom pokretačkom programu i korištenom softveru za prihvat slike. Trenutno postoje dva pokretačka programa, TWAIN i ISIS. Čini se boljim ISIS pokretački program jer je on unaprijed standardiziran i garantira mu se ista funkcionalnost na svim uređajima, odnosno moguće je odrediti željenu funkcionalnost što se može iskoristiti za određivanje funkcionalnosti za izradu glavne slike u boji, dubine boje od 24 bita te bez poboljšanja koja dovode do gubitka podataka. Softveri za prihvat slike imaju razne mogućnosti, primjerice mogu sliku spremiti na lokalno računalo ali i poslati sliku na određeni server. Velika prednost je izrada profila te mogućnost prijave operatera pomoću korisničkih podataka. Time se postiže poznavanje postavki rada skenera tijekom faze skeniranja.

Podaci o nastanku digitalizirane slike mogu se upisati u datoteku te pohraniti. Za strojnu obradu podataka moguće je iskoristiti dobro strukturirano XML rješenje. Najveća prednost ovog rješenja nalazi se u mogućnosti definiranja željnih podataka koji se mogu provjeravati prema različitim zahtjevima kao što je obavezno postojanje podataka i slično.

8. TEHNIČKA RJEŠENJA ZA SIGURNOST FIZIČKOGA I DIGITALIZIRANOGA GRADIVA

Autentičnost digitalizacije ovisi o mnogo čimbenika koji su ranije navedeni. Pored njih veliko pitanje je što je s autentičnošću dokumenta prije nastanka digitalizirane slike, odnosno kako se može tvrditi da je dokument koji je ušao u proces digitalizacije zaista onaj koji je zaprimljen u sustav. Odgovor na ovo pitanje može dati korištenje RFID naljepnice i praćenja kretanja, odnosno automatsko zapisivanje praćenja kretanja, dokumenta prije dolaska na digitalizaciju ali i potvrdom da je bio dio paketa digitalizirane dokumentacije. Digitalizacijom mogu nastati različiti formati datoteke koji su dobro propisani za primjere TIFF datoteke i PDF datoteke unutar EXIF standarda i ISO 19005 grupe standarda. Rješenje PIQL film omogućuje zapisivanje digitalizirane slike na medij koji je teško promijeniti te pored toga omogućava zapis u obliku snimljene slike, baš kao što to omogućava i mikrofilm, ali dodatno i u obliku digitalnih podataka čime se znatno ubrzava čitanje i osigurava nepromjenjivost. Osiguranje autentičnosti prije digitalizacije, digitalizacijom i unutar sustava za pohranu digitalizirane slike i pripadnih metapodataka dobro je povezati u cjelinu ukoliko se želi taj dokument kasnije ispisati na papir za različite druge potrebe, a s ciljem zadržavanja autentičnosti što se može postići korištenjem rješenja koja onemogućavaju nedozvoljene promjene dokumenta.

8.1. Prihvat dokumentacije

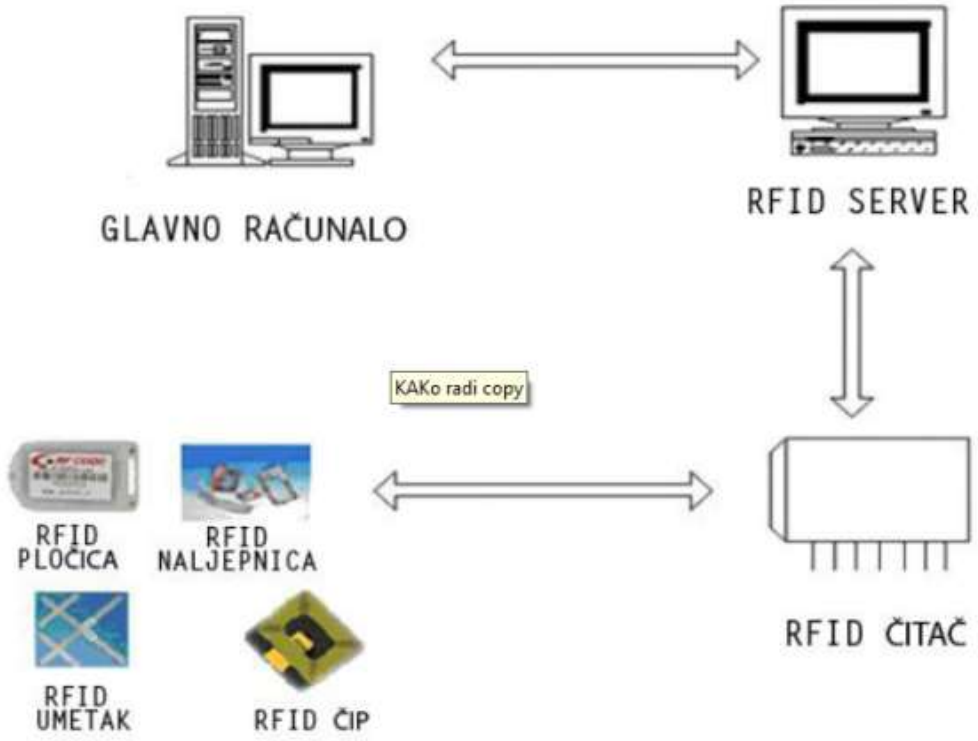
Fizička dokumentacija se prihvaća u sustav, propisno se označava te smješta prema unaprijed dogovorenim standardima ili pravilnicima tvrtke. Od trenutka prihvaćanja u sustav do trenutka uništenja nakon proteka rokova čuvanja dokumentacija prolazi različite faze te njome rukuju djelatnici ovisno o dodijeljenim pravima. Postoji više načina označavanja dokumenta, npr. dodjeljivanjem jedinstvenog broja direktnim upisivanjem, lijepljenjem jedinstvenog barkoda ili označavanjem pomoću RFID naljepnice. Označavanje pomoću RFID naljepnice omogućuje praćenje kretanja dokumenta u dozvoljenom području putem aplikacije ili računala koji zapisuje točna kretanja dokumenta.

8.1.1. RFID

Sustav RFID sastoji se od RFID odzivnika (engl. transponder), RFID čitača i RFID antene. RFID je skraćenica za Radio Frequency Identification, odnosno za identifikaciju putem radio frekvencije. Pomoću RFID-a moguće je obaviti identifikaciju bez kontakta. Kada RFID odzivnik uđe u područje RFID čitača tada se događa očitavanje podataka koji su zabilježeni u RFID odzivniku. RFID se sastoji od integriranog kruga i RF antene.

Postoji više RFID odzivnika kao što su naljepnice, kartice, privjesci, staklene cijevi, pločice, diskovi, kutije i tako dalje, i moguće ih je koristiti za praćenje i označavanje životinja, proizvoda, brodskih kontejnera, plaćanje cestarine, zaduživanje knjiga, registraciju radnog vremena, kontrolu pristupa, kodiranje ključeva, praćenje proizvodnih procesa i tako dalje. Primjena je zaista široka.

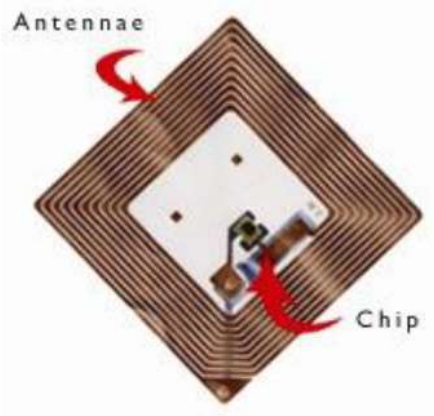
Primjer RFID sustava prikazan je na slijedećoj slici (slika 9).



Slika 9. RFID sustav[244]

Na slici (slika 9) prikazan je RFID odzivnik koji, ulazeći u radio-frekvencijsko područje antene RFID čitača, aktivira čitač prenoseći prethodno upisane informacije u RFID čip. Slika 10 prikazuje kako izgleda RFID odzivnik.

[244] Katedra za materijale u grafičkoj tehnologiji. (n.d.). RFID tehnologija. Preuzeto 21. 3. 2017. iz Grafički fakultet – Sveučilište u Zagrebu: http://materijali.grf.unizg.hr/media/RFID%20tehnologija.pdf



Slika 10. RFID odzivnik[245]

Ulazak RFID odzivnika u područje RFID antene aktivira RFID čitač koji preko antene RFID odzivnika prima podatke koji su spremljeni u čip odzivnika. Ukoliko RFID odzivnik ima ugrađenu bateriju tada je riječ o aktivnim RFID odzivnicima. RFID odzivnici bez baterije su pasivni RFID odzivnici koji struju potrebnu za rad čipa dobivaju preko radiovalova koje prima antena.

RFID čitač primljene podatke šalje dalje do servera koji dalje komunicira s glavnim računalom. Ova arhitektura može biti i drugačije postavljena ovisno o potrebama.

RFID odzivnike je moguće programirati[246] tako da ih je moguće samo čitati, što znači da su unaprijed programirani sadržavajući jedinstvenu oznaku, zatim programirati jedanput prema korisničkim potrebama ili višestruko programirati, ali u tom slučaju imaju jedinstven serijski broj kojem se dodaju željeni podaci.

Ovisno o korištenoj frekvenciji RFID odzivnika omogućen je i različiti domet. Tako postoje niske frekvencije, 125-134 kHz, kojima je domet do 30 cm, visoke frekvencije od 13,56 MHz dometa od 1 m do 16 m[247], ultra visoke frekvencije, UHF od 860 do 960 MHz, kojima je domet do 6 m te mikrovalne frekvencije od 2,45 GHz i 5,8 GHz koje imaju domet

[245] ibid.
[246] CARNet CERT i LS&S. (2007.). RFID identifikacija, CCERT-PUBDOC-2007-01-179. Preuzeto 21. 3. 2017. iz https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-01-179.pdf
[247] SkyRFID inc. (n.d.). RFID Tag Maximum Read Distance. Preuzeto 21. 3. 2017. iz http://skyrfid.com/RFID_Tag_Read_Ranges.php

do 100 m[248]. Veće RFID naljepnice mogu dostići udaljenosti veće od 30 m[249]. RFID odzivnici kojima je domet do 100 m su aktivni odzivnici[250].

RFID sustav ima i neke ranjivosti kao što je zaštita privatnosti jer RFID odzivnik šalje odgovor na svaki upit čitača, a time ga je moguće i neovlašteno pratiti, ali isto tako moguće je fizički uništiti odzivnik, ometati radio signal, prisluškivati i neovlašteno analizirati komunikaciju, preuzeti ulogu odzivnika, manipulirati odzivnikom kako bi promijenili identitet objekta.[251] Na ove napade moguće je odgovoriti na različite načine. Moguće je u odzivnik ugraditi lozinku koja ga uništi prilikom prijema ove lozinke. Na primjer kupac izlaskom iz trgovine aktivira ovu funkciju prolazeći pored RFID antene koja šalje lozinku RFID odzivniku. Zatim je moguće koristiti kriptografiju, hash funkcije i druge enkripcijske metode kao i korištenje autorizacijskih algoritama koji šalju upite RFID odzivniku, a koji na svako pitanje odgovara s određenim unaprijed definiranim znakom pohranjenim u listi znakova u samom odzivniku.

8.2. Digitalizacija

Prolaskom papirnatog dokumenta kroz skener nastaje digitalizirana slika. Ova slika može biti pohranjena u više formata kao što su TIFF, JPEG, PDF, BMP ili PowerPoint datoteka u slučaju navedenog softvera za prihvat slike Capture Perfect. Standard EXIF izrađen je kako bi se odredila polja unutar TIFF datoteke u koje se mogu spremati podaci koji su važni za proces skeniranja a koji mogu utjecati na dokazivanje autentičnosti digitalizirane slike.

8.2.1. Standard EXIF

Standard EXIF[252] (engl. Exchangeable image file format; format za razmjenu digitalnih slika op.a.) određuje formate koje koriste digitalni fotoaparati prilikom stvaranja

[248] Nikitin, P. V., Rao, K. V., & Lazar, S. (2007.). An Overview of Near Field UHF RFID. Preuzeto 21. 3. 2017. iz https://www2.ee.washington.edu/people/faculty/nikitin_pavel/papers/RFID_2007.pdf
[249] Smiley, S. (2016.). Active RFID vs. Passive RFID: What's the Difference. Preuzeto 21. 3. 2017. iz RFID INSIDER TRACKING THE RFID INDUSTRY: http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid
[250] SkyRFID inc. (n.d.). RFID Tag Maximum Read Distance. Preuzeto 21. 3. 2017. iz http://skyrfid.com/RFID_Tag_Read_Ranges.php
[251] CARNet CERT i LS&S. (2007.). RFID identifikacija, CCERT-PUBDOC-2007-01-179. Preuzeto 21. 3. 2017. iz https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-01-179.pdf
[252] Camera & Imaging Products Association. (2010.). Standard of the Camera & Imaging Products Association, CIPA DC-008-Translation-2012, Exchangeable image file format for digital still cameras: Exif Version 2.3. Preuzeto 24. 3. 2017. iz http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf

slika, zvuka i oznaka i koji se koriste prilikom obrade digitalnih slika i zvuka snimljenih digitalnim fotoaparatima. Standard se koristi kod svih uređaja koji imaju mogućnost snimanja, zapisivanja, prikazivanja, uređivanja i ispisivanja digitalnih slika. Formati koji se koriste u standardu definirani su kao struktura mapa koje su bazirane na EXIF-JPEG-u i formatima zapisivanja u memoriju. Aplikacijski softveri su oni koji omogućavaju uređivanje, prikazivanje, ispis, zapisivanje metapodataka kao i uvoz i uređivanje digitalnih slika.

Standard se odnosi na specifikacije vezane uz datoteke digitalnih slika i digitalnih audio datoteka, dok je specifikacija medija na kojem su zapisane datoteke prepuštena standardu za određeni medij. Specifikacija EXIF datoteke slike se sastoji od:

1. strukture datoteke s podatcima slike,
2. oznaka korištenim u ovom standardu,
3. definicije upravljanja verzijama formata.

Komprimirane datoteke se zapisuju kao JPEG format poštujući ISO/IEC 10918-1 standard. Nekomprimirane datoteke se zapisuju koristeći TIFF Rev. 6.0 format.

Informacije vezane za atribute komprimiranih i nekomprimiranih podataka pohranjuju se u oznake kako je propisano u TIFF Rev. 6.0 formatu, one koji u ovom formatu nisu propisane a specifične su za sustav digitalnog fotoaparata zapisuju se u privatne oznake koje su zabilježene u EXIF standardu. Standard dodatno određuje metodu zapisivanja indeksnih sličica (engl. thumbnails).

Standard pretpostavlja korištenje triju elemenata:

1. oprema, kao što su kamere, printeri i slični uređaji za snimanje,
2. komercijalni softver, softver za obradu slika koji radi na osobnom računalu,
3. specijalizirani softver, namjenski softver za obradu slike koji radi na osobnom računalu.

Postupak je takav da digitalna kamera zapisuje podatke u formatu datoteke koji je specificiran ovim standardom, a koje će drugi uređaji moći čitati.

Specifikacija se sastoji od slijedećih dijelova:

1. definicija verzije formata, zapisuje se u 4 bajta,
2. specifikacije vezane za podatke o slici, odnosi se na: broj točaka koji nije ograničen u slučaju nekomprimiranih ili komprimiranih podataka, odnos točaka koji je 1:1, te sastav i uzorkovanje točaka,
3. osnovne strukture podataka o slici koje ovisno o tipu mogu biti:
    a. RGB nekomprimirani podaci se zapisuju sukladno Baseline TIFF Rev. 6.0 RGB Full Color images,

b. YCbCr nekomprimirani podaci se zapisuju sukladno TIFF Rev. 6.0 RGB Full Color images,
c. JPEG komprimirani podaci se zapisuju sukladno JPEG Baseline ADCT (engl. Adaptive Discrete Cosine Transform; vrsta matematičke transformacije op.a.),

4. oznake,
   a. koriste se oznake definirane u TIFF Rev. 6.0 kako su popisane u tablici 6,
5. JPEG oznake segmenata koje se odnose na oznake početka slike, aplikacijskih dijelova, tablice kvantizacije, definicije Hufmanove tablice, definicije početka interoperabilnosti, definicije okvira, početka skeniranja i oznaka kraja slike,
6. specifikacije podataka vezanih za snimanje.

Tablica 6. Popis korištenih oznaka za tip datoteke TIFF

broj	naziv	kratak opis
0	GPSVersionID	Označava verziju GPSInfoIFD (engl. Image File Directories; skr. IFD).
1	GPSLatitudeRef	Označava je li zemljopisna širina sjever ili jug.
1	InteroperabilityIndex	Označava pravilo interoperabilnosti.
2	GPSLatitude	Označava zemljopisnu širinu.
3	GPSLongitudeRef	Označava je li zemljopisna dužina istok ili zapad.
4	GPSLongitude	Označava zemljopisnu dužinu.
5	GPSAltitudeRef	Označava visinu koja se uzima za referentnu točku.
6	GPSAltitude	Označava visinu u odnosu na referentnu visinu
7	GPSTimeStamp	Označava vrijeme po univerzalnom vremenu (UTC).
8	GPSSatellites	Označava GPS satelita korištenog u mjerenjima.
9	GPSStatus	Označava status GPS prijamnika kada je slika snimljena.
10	GPSMeasureMode	Označava način mjerenja GPS-a.
11	GPSDOP	Označava stupanj točnosti GPS.
12	GPSSpeedRef	Označava jedinicu korištenu pri izražavanju brzine kretanja GPS prijemnika.
13	GPSSpeed	Označava brzine kretanja GPS prijemnika.
14	GPSTrackRef	Označava oznaku smjera kretanja GPS prijemnika.
15	GPSTrack	Označava smjer kretanja GPS prijemnika.
16	GPSImgDirectionRef	Označava oznaku smjera slike u trenutku snimanja.
17	GPSImgDirection	Označava smjer slike u trenutku snimanja.
18	GPSMapDatum	Označava geodetske podatke koje koristi GPS prijemnik.

broj	naziv	kratak opis
19	GPSDestLatitudeRef	Označava je li zemljopisna širina odredišne točke sjever ili jug.
20	GPSDestLatitude	Označava zemljopisnu širinu odredišne točke.
21	GPSDestLongitudeRef	Označava je li zemljopisna dužina odredišne točke istok ili zapad.
22	GPSDestLongitude	Označava zemljopisnu dužinu odredišne točke.
23	GPSDestBearingRef	Označava oznaku koja se daje azimutu odredišne točke.
24	GPSDestBearing	Označava azimut odredišne točke.
25	GPSDestDistanceRef	Označava jedinicu kojom se izražava udaljenost do odredišne točke.
26	GPSDestDistance	Označava udaljenost do odredišne točke.
27	GPSProcessingMethod	Niz znakova korištenih pri zapisivanju naziva metode koja se koristi za pronalaženje lokacije.
28	GPSAreaInformation	Niz znakova korištenih pri zapisivanju naziva GPS područja.
29	GPSDateStamp	Niz znakova korištenih pri zapisivanju datuma i vremena u odnosu na univerzalno vrijeme (UTC).
30	GPSDifferential	Označava koristi li se diferencijalna korekcija u GPS prijemniku.
31	GPSHPositioningError	Označava grešku vodoravnog pozicioniranja, u metrima.
256	ImageWidth	Broj stupaca u slici, tj. broj točaka u retku.
257	ImageLength	Broj redaka u slici, tj. broj točaka u stupcu.
258	BitsPerSample	Broj bitova po komponenti.
259	Compression	Kompresijska shema koja je korištena na podacima slike.
262	PhotometricInterpretation	Prostor boja slikovnih podataka.
270	ImageDescription	Niz podataka koji opisuje predmet na slici.
271	Make	Proizvođač skenera.
272	Model	Naziv modela skenera ili njegov broj.
273	StripOffsets	Za svaku traku* (engl. strip), broj bajtova ofseta snimke.
274	Orientation	Orijentacija slike u odnosu na retke i stupce.
277	SamplesPerPixel	Broj komponenti po točki.
278	RowsPerStrip	Broj stupaca po traci*.
279	StripByteCounts	Za svaku traku, broj bajtova u traci nakon kompresije.
282	XResolution	Broj točaka po jedinici rezolucije u smjeru širine slike.
283	YResolution	Broj točaka po jedinici rezolucije u smjeru dužine slike.
284	PlanarConfiguration	Način pohrane točaka za svaku komponentu.

broj	naziv	kratak opis
296	ResolutionUnit	Jedinica mjere XResolution i YResolution.
301	TransferFunction	Opisuje funkciju prijenosa za sliku u tabličnom stilu.
305	Software	Ime i broj verzije softverskog paketa koji je korišten pri stvaranju slike.
306	DateTime	Vrijeme i datum stvaranja slike.
315	Artist	Ime osobe koja je stvorila sliku
318	WhitePoint	Kromatičnost bijele točke na slici.
319	PrimaryChromaticities	Kromatičnost predizbora slike.
513	JPEGInterchangeFormat	Ofset početnog bajta početka slike kod JPEG komprimirane indeksne sličice.
514	JPEGInterchangeFormatLength	Broj bajtova JPEG komprimirane indeksne sličice.
529	YCbCrCoefficients	Funkcija transformacije iz RGB u YCbCr.
530	YCbCrSubSampling	Određuje faktor poduzorkovanja koji se koristi kod sjajnosti komponente boje YCbCr slike.
531	YCbCrPositioning	Određuje poziciju poduzorkovanja sjajnosti komponente boje u odnosu na uzorak osvijetljenosti.
532	ReferenceBlackWhite	Određuje vrijednost para podataka donjeg i gornjeg ranga za svaku komponentu točke.
33432	Copyright	Podatak o autorskom pravu.
33434	ExposureTime	Vrijeme ekspozicije u sekundama.
33437	FNumber	Žarišna duljina, broj F.
34665	Exif IFD	Pokazivač na Exif IFD podatak.
34850	ExposureProgram	Klasa programa koje koristi kamera za podešavanje ekspozicije prilikom snimanja slike.
34852	SpectralSensitivity	Označava spektralnu osjetljivost svakog kanala koji koristi digitalni fotoaparat.
34853	GPS IFD	Pokazivač na GPS Info IFD podatak.
34855	ISOSpeedRatings	Označava ISO brzinu i širinu digitalnog fotoaparata ili drugog ulaznog uređaja prema specifikaciji ISO 12232 norme.
34856	OECF	Označava optičko-električnu funkciju pretvorbe definiranu u normi ISO 14524.
34864	SensitivityType	Označava tip senzitivnosti prema normi ISO 12232.
34865	StandardOutputSensitivity	Oznaka standardne izlazne vrijednosti osjetljivosti uređaja prema normi ISO 12232.
34866	RecommendedExposureIndex	Oznaka indeksa preporučene ekspozicije prema normi ISO 12232.
34867	ISOSpeed	Oznaka brzine ISO prema normi ISO 12232.
34868	ISOSpeedLatitudeyyy	Oznaka geografske širine brzine ISO prema normi ISO 12232.

broj	naziv	kratak opis
34869	ISOSpeedLatitudezzz	Oznaka geografske duljine brzine ISO prema normi ISO 12232.
36864	ExifVersion	Verzija podržanog EXIF standarda.
36867	DateTimeOriginal	Datum i vrijeme stvaranja originalne slike.
36868	DateTimeDigitized	Datum i vrijeme zapisivanja slike kao digitalnog podatka.
37121	ComponentsConfiguration	Navodi kanale i nadopunjuje podatak o fotometrijskom tumačenu.
37122	CompressedBitsPerPixel	Daje podatak o komprimiranim bitovima po točki.
37377	ShutterSpeedValue	Brzina zatvarača.
37378	ApertureValue	Vrijednost otvora objektiva.
37379	BrightnessValue	Vrijednost sjaja.
37380	ExposureBiasValue	Vrijednost ekspozicije.
37381	MaxApertureValue	Najmanja žarišna vrijednost leće.
37382	SubjectDistance	Udaljenost od objekta, u metrima.
37383	MeteringMode	Način mjerenja.
37384	LightSource	Vrsta izvora svjetlosti.
37385	Flash	Označava status bljeskalice (engl. flash) prilikom snimanja slike.
37386	FocalLength	Stvarna žarišna vrijednost leće, u mm.
37396	SubjectArea	Označava mjesto i područje glavnog objekta u ukupnoj sceni.
37500	MakerNote	Informacija specifična za proizvođača.
37510	UserComment	Ključne riječi ili komentari o slici, nadopunjuje podatak ImageDescription.
37520	SubsecTime	Oznaka se koristi za snimanje dijela sekunde za oznaku datetime.
37521	SubsecTimeOriginal	Oznaka se koristi za snimanje dijela sekunde za oznaku DateTimeOriginal.
37522	SubsecTimeDigitized	Oznaka se koristi za snimanje dijela sekunde za oznaku DateTimeDigitized.
40960	FlashpixVersion	Verzija formata Flashpix koja je podržana FPXR datotekom.
40961	ColorSpace	Oznaka o prostoru boja.
40962	PixelXDimension	Širina zapisane slike.
40963	PixelYDimension	Visina zapisane slike.
40964	RelatedSoundFile	Koristi se pri zapisivanju imena audio datoteke koja je povezana s digitalnom slikom.
40965	Interoperability IFD	Pokazivač na podatak Interoperability IFD.
41483	FlashEnergy	Označava energiju bljeska u trenutku snimanja slike

broj	naziv	kratak opis
41484	SpatialFrequencyResponse	Zapis o tablici prostorne frekvencije i vrijednosti odgovora prostornih frekvencija prema specifikaciji norme ISO 12233.
41486	FocalPlaneXResolution	Označava broj točaka u širini slike po jedinici žarišne rezolucije.
41487	FocalPlaneYResolution	Označava broj točaka u duljini slike po jedinici žarišne rezolucije.
41488	FocalPlaneResolutionUnit	Označava jedinice za mjerenje FocalPlaneXResolution i FocalPlaneYResolution.
41492	SubjectLocation	Označava poziciju glavnog predmeta u sceni.
41493	ExposureIndex	Označava odabrani indeks ekspozicije u vrijeme snimanja slike.
41495	SensingMethod	Označava tip senzora na uređaju.
41728	FileSource	Označava izvor slike (vrsta uređaja).
41729	SceneType	Označava vrstu scene.
41730	CFAPattern	Označava geometrijski uzorak polja filtra boja senzora kada se koristi jedan čip za polja boja.
41985	CustomRendered	Označava korištenje posebne obrade slikovnih podataka.
41986	ExposureMode	Označava način ekspozicije postavljen u trenutku snimanja slike.
41987	WhiteBalance	Označava način balansa bijele boje postavljen u trenutku snimanja slike.
41988	DigitalZoomRatio	Označava omjer digitalnog zuma u trenutku snimanja slike.
41989	FocalLengthIn35mmFilm	Označava ekvivalent žarišne duljine uz pretpostavku 35 mm fotoaparata, u mm.
41990	SceneCaptureType	Označava vrstu scene koja je snimljena.
41991	GainControl	Označava sveukupni stupanj prilagodbe slike.
41992	Contrast	Označava smjer obrade kontrasta primijenjen u trenutku snimanja slike.
41993	Saturation	Označava smjer primijenjene saturacije u trenutku snimanja slike.
41994	Sharpness	Označava smjer primijenjene oštrine u trenutku snimanja slike.
41995	DeviceSettingDescription	Označava podatak o opisu postavki uređaja.
41996	SubjectDistanceRange	Označava udaljenost od objekta.
42016	ImageUniqueID	Označava jedinstveni identifikator za svaku sliku.
42032	CameraOwnerName	Vlasnik digitalnog aparata.
42033	BodySerialNumber	Serijski broj digitalnog fotoaparata.
42034	LensSpecification	Određuje karakteristike leće: žarišna duljina (minimalna i maksimalna), najmanji F broj u najmanjoj i najvećoj žarišnoj duljini.

broj	naziv	kratak opis
42035	LensMake	Proizvođač leće.
42036	LensModel	Ime i broj modela leće.
42037	LensSerialNumber	Serijski broj leće
42240	Gamma	Gamma korekcija.

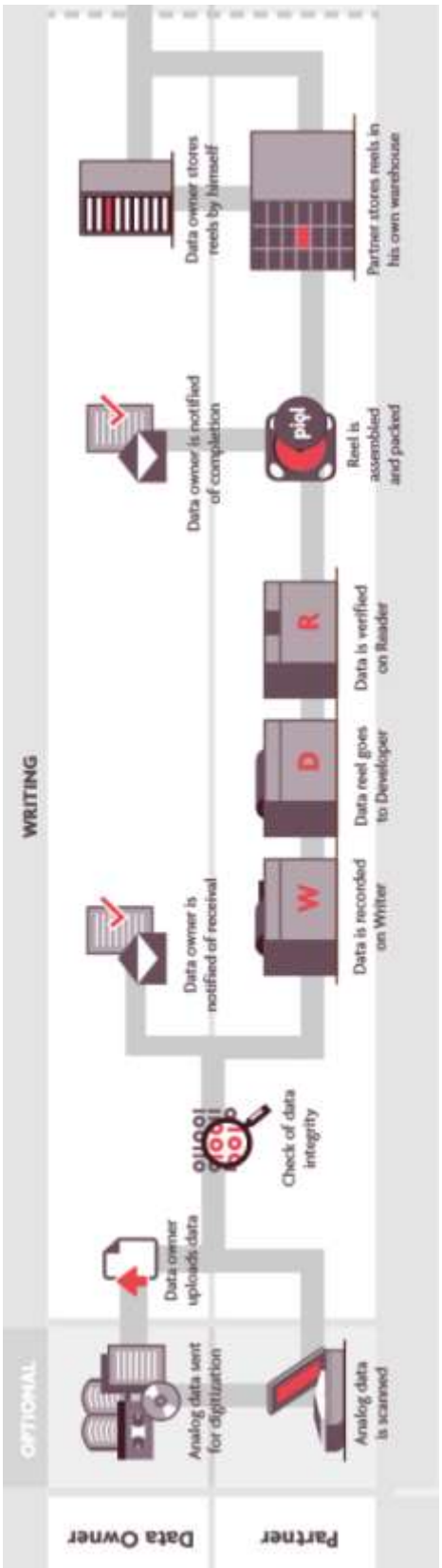
* Baseline TIFF slika se sastoji od više traka. Ove trake su podsekcije digitalne slike.

8.2.2. PIQL film

Piqlov film je mikrografski arhivski film posebno dizajniran za dugovječnost i visoku gustoću digitalnog zapisa. Radi se o rješenju kojim se digitalizirana ili izvorno digitalna slika pohranjuje i čuva na mediju za koji je poznato da mu je vijek trajanja 500 godina, te za koji je potrebna tehnologija koja se napretkom ne mijenja. Kako bi se vlasnicima podataka omogućilo sigurno i pristupačno rješenje bez problema s migracijom Piql film koristi kompatibilno OAIS (ISO 14721:2003) rješenje. Dakle, riječ je o filmu na koji se istovremeno mogu zapisati informacije u analognom i digitalnom obliku.

Karakteristike filma kao medija za pohranu podataka su slijedeće:

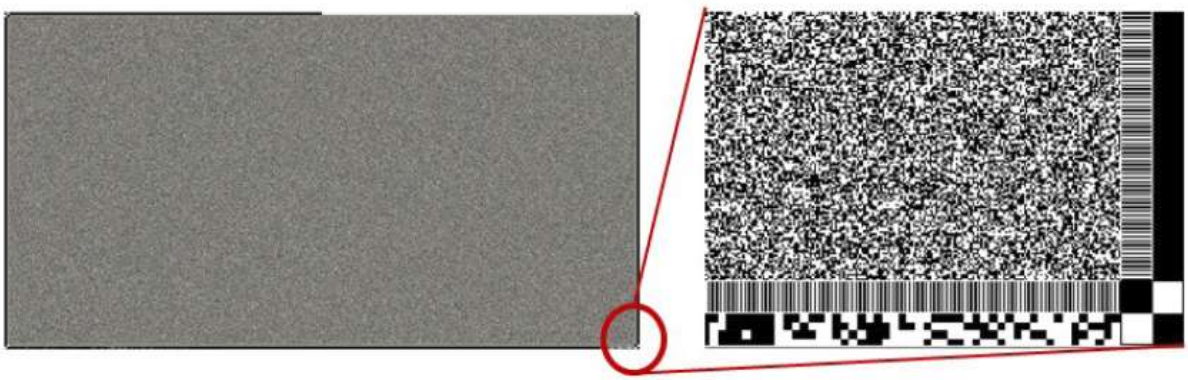
1. film je fotoosjetljiv i kemijski stabilan medij kojem je osigurana dugovječnost od 500 godina. Film, kutija za film i naljepnica na kutiji su testirane prema ISO zahtjevima za dugovječnost od najmanje 500 godina,
2. film nije moguće mijenjati jednom kada su podaci zapisani,
3. u slučaju nestanka struje ili u slučaju elektromagnetnog udara film neće biti oštećen jer je pohranjen na vanjskom sustavu,
4. kako bi se spriječilo zastarijevanje sustava na filmu se nalaze svi podaci i metapodaci zapisani kao ljudskom oku čitljiv tekst te s objašnjenjem kako pročitati podatke.



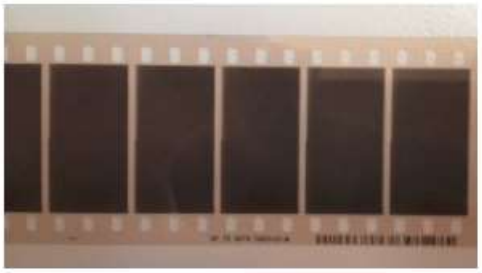
Slika 11. Tijek procesa stvaranja i pohrane Piql trake[253]

[253] Piql AS. (n.d.). Creating the ultimate digital insurance, Behind the curtains, Rev. 150306. Preuzeto 9. 11. 2016. iz https://slidex.tips/download/creating-the-ultimate-digital-insurance

Slika 11 prikazuje u prvom koraku provjeru integriteta, točnosti i autentičnosti podataka prije zapisivanja podataka i čitanja podataka s filma. U tu svrhu koriste se tehnike prethodnog ispravljanja pogreške (engl. Forward Error Correction; skr. FEC) i kontrolnog zbroja. Nakon primitka datoteke provjerava se postojanje virusa, normalizira se u format za zapisivanja na filmu, te se izrađuje kontrolni zbroj datoteke koji se šalje vlasniku datoteke na provjeru i zapisuje se u bazu radi buduće verifikacije. Zatim se datoteka dekodira i dijeli u manje elemente informacija u binarnom obliku koji odgovara jednom okviru (engl. frame) na filmu (vidi slike 12 i 13). Za svaki okvir izrađuje se njegov kontrolni zbroj koji se dodaje podatkovnom okviru i šalje uređaju za zapisivanje na film. Podatkovni okvir (engl. data frame) je svaka slika zapisana na film. Dodatno se prije zapisivanja na film verificira svaki kontrolni zbroj kako bi se osigurao integritet tijekom slanja. Zapisivanje počinje automatski nakon smještaja novog filma u PiqlWriter. PiqlWriter je uređaj kojim se primljene slike zapisuju na film.



Slika 12. Digitalni okvir podataka. Desno je uvećani dio okvira. [254]



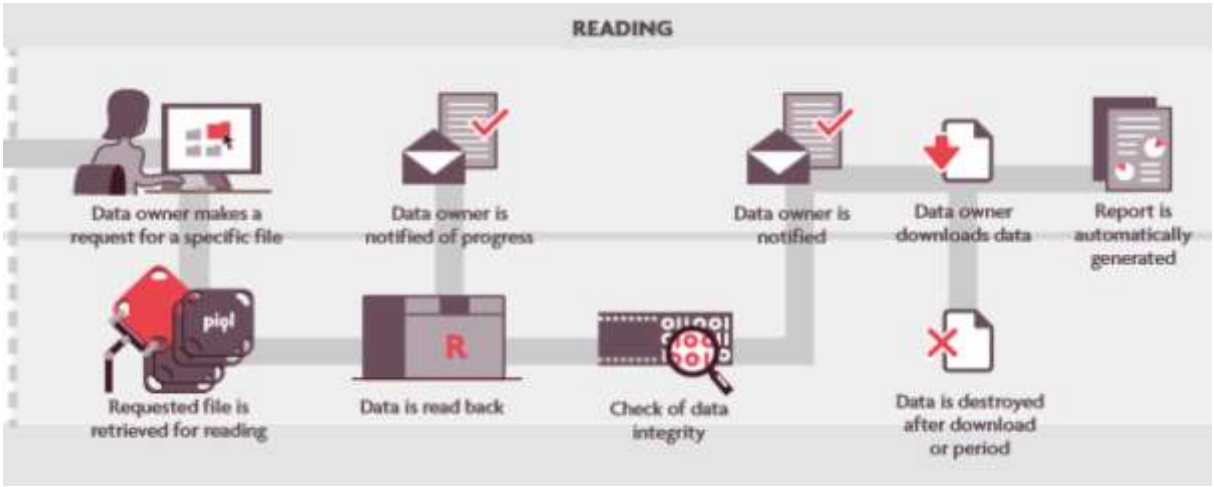
Slika 13. Okvir podataka na mikrofilmskom svitku[255]

[254] ibid.
[255] ibid.

Nakon razvijanja filma verificiraju se zapisani podaci kako bi se osigurao integritet i pristupačnost u budućnosti, i to se obavlja putem PiqlReader-a, odnosno čitača filma. PiqlReader je skener koji ima dvije funkcije, prva čita zapisane okvire dok druga dekodira svaki okvir i „sklapa“ originalnu datoteku. Tijekom procesa sklapanja originalne datoteke provjerava se kontrolni zbroj pročitanog okvira s kontrolnim zbrojem zapisanim u bazi podataka. Tek nakon verifikacije svih zapisa na filmu film se šalje na pohranu.

Film se može pohraniti kod vlasnika ili u vlastitim jedinicama za pohranu (engl. Warehouse management system; skr. WMS). Ukoliko se koristi WMS tada se svaki film povezuje preko barkod skenera koji čita naljepnicu s podacima o filmu u bazi podataka.

Slika 14 prikazuje proces čitanja i „sklapanja“ originalne datoteke. Kada je potrebno pročitati podatke određene datoteke koju je zatražio vlasnik podataka nakon umetanja traženog filma u PiqlReader, svitak se pozicionira na točnu poziciju tražene datoteke, te se na prethodno opisan način pročita i „sklopi“ originalna datoteka verificirajući kontrolne zbrojeve svakog okvira tijekom cijelog procesa. Nakon što vlasnik kopira datoteku s dogovorenog mjesta za razmjenu datoteka se briše.



Slika 14. Proces čitanja i "sklapanja" originalne datoteke[256]

Kako bi se osigurala čitljivost i za kasnija vremena svi podaci potrebni za dekodiranje zapisani su na početku filma u formi koja je čitljiva za ljudsko oko ali i u digitalnom obliku. Na taj način dovoljno je posjedovati kameru/skener i računalo za čitanje podataka s filma.

PIQL specifikacija filma:

1. 35 mm film, Bell and Howell perforacije, crno-bijeli, visoke rezolucije,

[256] ibid.

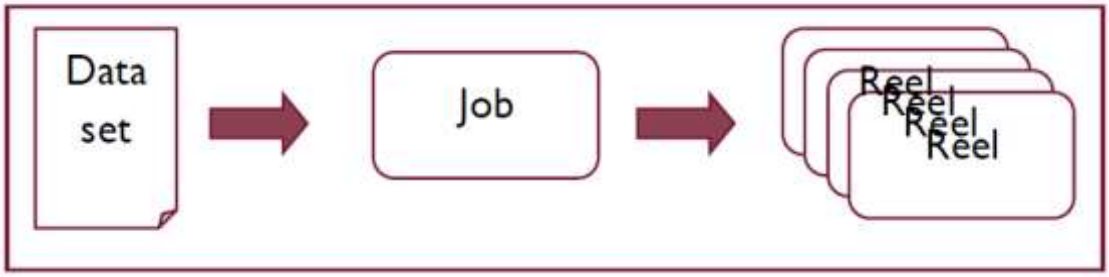
2. duljina 945 m,
3. srebrno halidni veličine 20 – 40 nm,
4. rezolucije 1070 lp/mm (parova linija po milimetru),
5. visoke svjetline,
6. suha ogrebotina (engl. dry scratch): 60g,
7. čvrstoće kidanja: 153 Mpa,
8. dugovječnost testirana na više od 500 godina prema ISO 18911, ISO 18924 i ISO 18936,
9. kapacitet podataka: 100 GB.

Piql film koristi tri skupa metapodataka:

1. administrativni i tehnički ili strukturalni metapodaci, npr. dubina bita, broj okvira, FEC (engl. Forward Error Correction; algoritam za korekciju greške op.a.) algoritam, i tako dalje,
2. metapodaci za prikaz u OAIS modelu za digitalne repozitorije, svi podaci potrebni za dekodiranje otvorenog izvornog koda, opis korištenog softvera, opisni dokumenti o Piql tehnologiji i specifikacije formata datoteke,
3. opisne informacije za zaštitu u OAIS referentnom modelu, svi podaci koje traži vlasnik podataka kako bi datoteci dao bolji kontekst, kao što su: naziv datoteke, ime vlasnika, provenijencija, pravo vlasništva i slično.

Proces zaštite podataka zapisivanjem na Piql film se sastoji od nekoliko koraka:

1. prikupljanje i pohrana metapodataka kao objekt posla (engl. job object),
2. datoteka se dijeli na manje elemente koji sadrže sve podatke koji se pohranjuju kao jedna slika na filmu,
3. na svaki element se primjenjuje FEC korekcija kako bi se osiguralo da se podaci mogu pročitati u budućnosti, te se primjenjuje metoda preplitanja (engl. interleaving) kako bi se spriječila velika količina pogreški,
4. stvara se podatkovni okvir koji uključuje informacije za praćenje točaka i metapodataka,
5. ukoliko, zbog veličine skupa datoteka koji su stvoreni prilikom izrade okvira, okviri moraju biti distribuirani na više svitaka (slika 15) stvaraju se dodatni metapodaci koji se također pohranjuju prema modelu na slici.

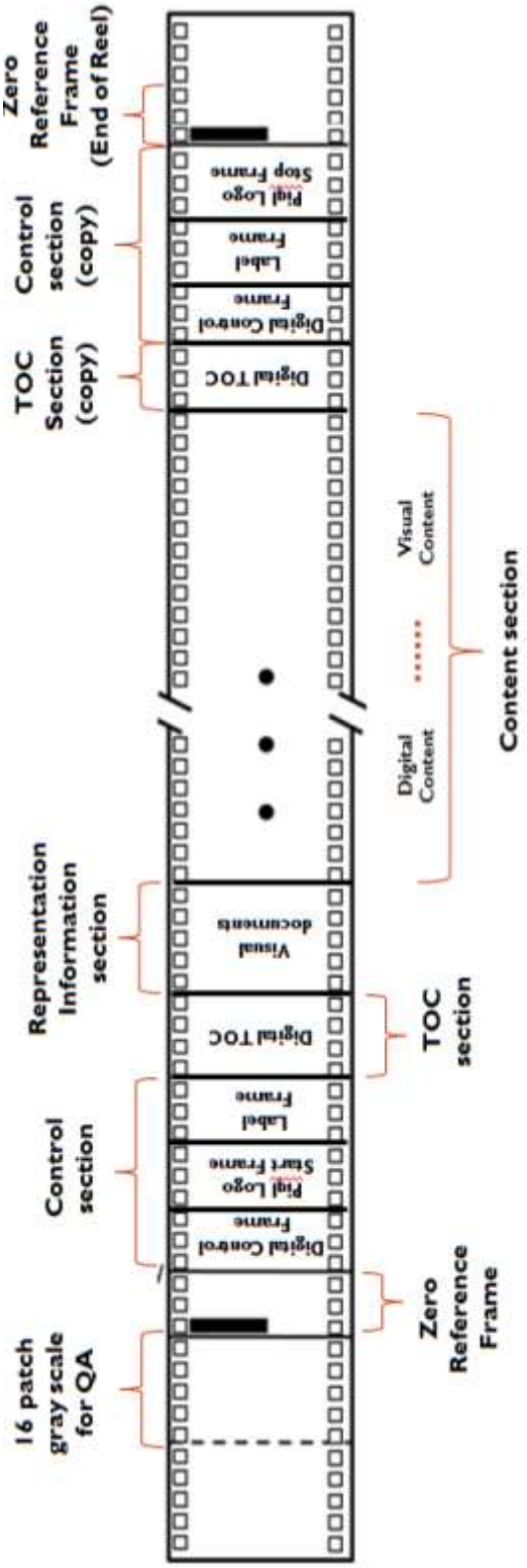


Slika 15. Model metapodataka nakon pripreme podataka[257]

Svaki film sadrži slijedeće podatke (slika 16):

1. 16 sivih okvira za osiguranje kvalitete zapisuju se na početku svakog filma,
2. nulta oznaka za automatsko pozicioniranje skenera na početak filma,
3. kontrolni dio koji sadrži administrativne i tehničke metapodatke, koji su potrebni za dekodiranje podatkovnih okvira, uključujući fizički izgled okvira, FEC i korišteni algoritmi preplitanja, broj bitova zapisanih u sadržajnom dijelu, koji se zapisuje digitalno i analogno, potrebnih za čitanje pomoću svjetla i povećala,
4. sadržaj cijelog posla, koji uključuje i poziciju svake datoteke na filmu,
5. informacije za prikaz koji uključuje i dokumente u formatu čitljivom ljudskom oku za slučaj da nije moguće koristiti drugu tehnologiju u budućnosti,
6. dio koji sadrži podatkovne okvire i okvire s metapodacima o datoteci zapisani u digitalnom ili u obliku čitljivom za ljudsko oko, ili oboje,
7. zatim se radi redundancije ponavlja kontrolni i sadržajni dio, točka 4.,
8. na kraju se izrađuje termalna naljepnica koja se smješta na kutiju filma.

[257] Piql AS. (n.d.). Piql Archival Storage Format, Product Data Sheet, Rev. 150306. Preuzeto 9. 11. 2016. iz https://www.piql.com/

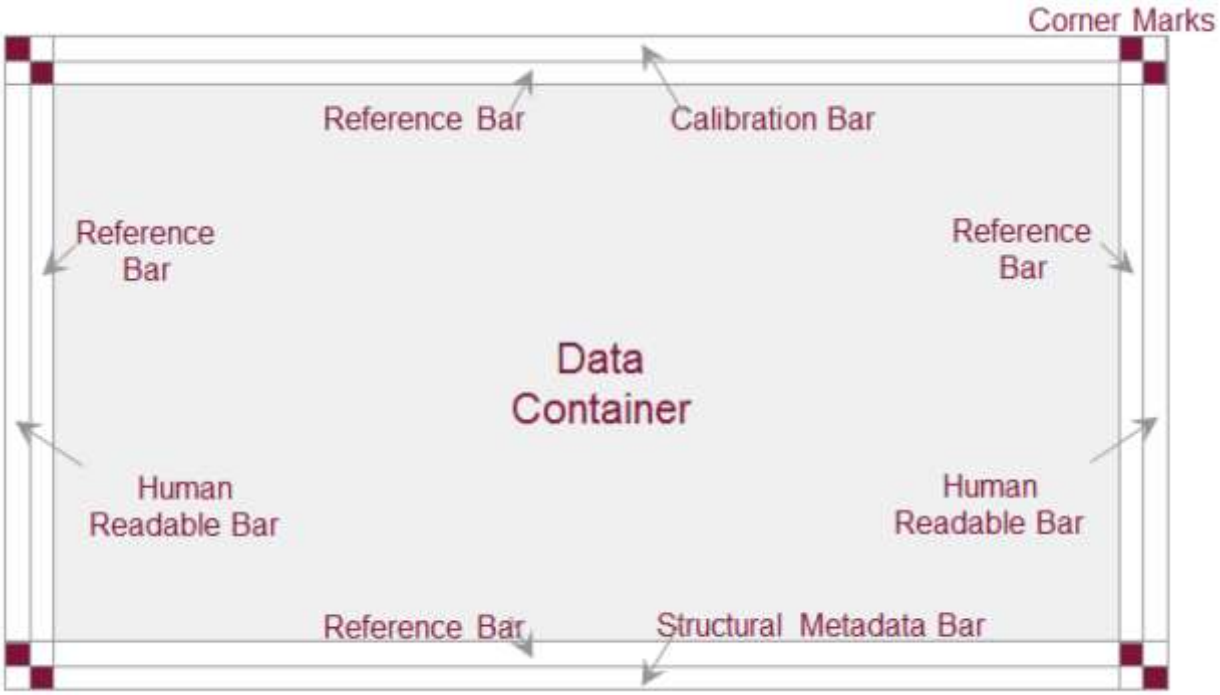


Slika 16. Raspored na svitku[258]

Na slici 17 vidi se format okvira, koji se sastoji od nekoliko dijelova:

[258] ibid.

1. strukturna metapodatkovna linija (engl. Structural Metadata Bar) koja sadrži podatke o samom okviru, tip podatka koji može biti kontrolni okvir, sadržajni okvir, slika ili podaci, zatim kontrolni zbroj sadržaja, identifikator svitka, identifikator kojoj datoteci pripada okvir, i slični podaci,
2. referentna linija (engl. Reference Bar),
3. kalibracijska linija (engl. Calibration Bar),
4. oznake kuta okvira (engl. Corner Marks),
5. sadržaj podataka (engl. Data Container).



Slika 17. Raspored okvira[259]

Svi metapodaci su kodirani kao veliki blokovi veličine 1 bit po točki, svi algoritmi su otvorenog tipa i dobro dokumentirani te zapisani na način koji je vidljiv za potrebe dekodiranja podataka. Model metapodataka je pohranjen u bazu podataka kako bi se omogućio pregled i pretraživanje arhivskih podataka. Ukoliko se baza podataka uništi u slučaju nesreće moguće ju je ponovno stvoriti dekodiranjem kontrolnih i indeksnih sekcija arhiviranih svitaka.

[259] ibid.

8.2.3. ISO 19005 skupina standarda

Prvi cilj norme ISO 19005 je definiranje formata datoteke koji omogućava reprezentaciju elektroničkog dokumenta na način da sačuva statički vizualni izgled kroz protok vremena neovisno o alatima i sustavima koji su ga stvorili, pohranili ili prikazali, a koji je temeljen na PDF formatu i koji se naziva PDF/A.

Drugi cilj norme je definirati logičku strukturu i druge semantičke podatke dokumenta, te zapisivanje konteksta i povijesti elektroničkih dokumenata unutar metapodataka koji su sadržani u samoj datoteci.

Treći dio norme ISO 19005 ima cilj omogućiti PDF dokumentima da sadrže druge formate datoteka i pri tome uključujući ne samo vizualni prikaz već i originalnu autorsku verziju, bogatiji semantički format i tako dalje. Pri tome norma ne vodi računa o dugoročnoj primjerenosti formata koje sadrže osim onih koji su kompatibilni s ISO standardima.

ISO 19005-1:2005 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 1. dio: Korištenje PDF 1.4 (PDF/A-1)

Norma ISO 19005-1 ima za cilj definirati format datoteke na temelju PDF-a, poznat kao PDF/A, koji osigurava mehanizam za predstavljanje elektroničkih dokumenata na način koji čuva njihov vizualni izgled tijekom vremena, neovisno o alatima i sustavima koji se koriste za stvaranje, pohranjivanje ili prikazivanje datoteka.

Nadalje, cilj joj je pružiti okvir kojim se u metapodacima zapisuje kontekst i povijest elektroničkih dokumenata. Treći cilj je definirati okvir za logičku strukturu i druge semantičkih informacija koje se nalaze zapisane unutar datoteke. Kako bi cilj bio postignut potrebno je prepoznati koje komponente PDF-a mogu biti korištene i pod kojim uvjetima. Međutim sam po sebi PDF/A ne osigurava da vizualni prikaz sadržaja precizno odražava originalni izvorni dokument, na primjer proces pretvorbe može zamijeniti font, konvertirati i komprimirati slike korištenjem algoritama s gubitkom informacija (engl. lossy compression) i slično. Organizacija koja ima potrebu osigurati da vizualni prikaz u datoteci PDF/A precizno odražava originalni izvorni dokument mora to provesti prije konverzije u PDF/A.

PDF/A je sinonim za ISO 19005 skupinu standarda. PDF/A-1 je sinonim za ISO 19005-1. PDF/A-1a je sinonim za ISO 19005-1 sukladnost nivoa A. Datoteka je sukladna nivou A ukoliko zadovoljava sve zahtjeve ISO 19005-1. PDF/A-1b je sinonim za ISO 19005-1 sukladnost nivoa B. Datoteka je sukladna nivou B ukoliko zadovoljava sve zahtjeve ISO

19005-1 osim točaka 6.3.8. i 6.8. Nivo B sadrži minimalne uvjete za vizualne podatke koje datoteka treba zadovoljiti za dugoročno očuvanje.

Norma specificira samo kako koristiti PDF 1.4 verziju za dugoročno očuvanje elektroničkih dokumenata koji koriste kombinaciju znakova, rasterskih i vektorskih podataka, ali nije primjenjiva na konverziju papira u elektronički dokument, računalni hardver i softver, metode fizičke pohrane na medije ni bilo koji dio prikazivanja podataka (engl. rendering).

Uvjeti koje je potrebno zadovoljiti kako bi se datoteka mogla smatrati PDF/A-1 datotekom su definirani kroz tehničke zahtjeve u kojima se definira struktura datoteke, grafika, fontovi, transparentnost, napomene, akcije, metapodaci, logička struktura i interaktivne forme.

Kako bi se uspješno upravljalo životnim ciklusom datoteke neophodno je pravilno koristiti i unositi ispravne podatke u metapodatke datoteke, kao što su opisi tehničkih i administrativnih pitanja. Način kako se metapodaci upisuju u datoteku opisan je dokumentom Specifikacija XMP (engl. XMP Specification).

Ukoliko postoji u datoteci, rječnik dokumenta mora sadržavati slijedeće metapodatke:

1. naslov datoteke,
2. naziv autora datoteke,
3. predmet datoteke,
4. ključne riječi,
5. naziv stvoritelja datoteke,
6. naziv proizvođača,
7. datum stvaranja datoteke,
8. datum modifikacije datoteke.

Kako bi se moglo pratiti povijesna kretanja i akcije nad datotekom potrebno je u povijesno polje, xmpMM:History, upisati podatke o aktivnostima, parametrima, vremenima, softverima koji su korišteni ili rađeni na datoteci, na primjer transformacija iz PDF 1.4 u PDF/A-1, ugrađen JavaScript ili audio zapis nije uključen, protokol koji je korišten ili uputa koja je korištena, zamjena fontova, odnosno sve ono što je potrebno, a što se odnosi na kontekst vezan za stvaranje i upotrebu datoteke.

U dodatku B norme navodi se kako nemogućnost očuvanja metapodataka može prouzročiti probleme u nalaženju, interpretiranju, upravljanju i autentifikaciji datoteke u budućnosti, što smanjuje ili poništava arhivsku vrijednost. Zbog toga se preporuča sve ne-XMP podatke izbjegavati ili konvertirati u XMP podatke, a konverziju upisati u polje History. U isto polje se preporuča upis svih elemenata koji nisu u XMP formatu i koji nisu

konvertirani u XMP. Jezike je potrebno identificirati prema normama ISO 639-1, ISO 3166-1 ili IANA (engl. Internet Assigned Numbers Authority).

Preporuke za pretvorbu dokumenata u PDF/A navode kako organizacija treba propisati uvjete za predavanje dokumenata arhivskoj službi kojima se navode zahtjevi, standardi i politike koje određuju kvalitetu dokumenta kao što je minimalna rezolucija, zahtjevi na kompresiju u smislu njihovih ograničenja, zabranu procesa koji mijenjaju ili uništavaju podatke. Ovi zahtjevi, standardi i politike se trebaju primijeniti prilikom konverzije u PDF/A. Kako bi se ovi kritični arhivski zahtjevi ispunili potrebno je u konverzijskom procesu osigurati točnu kopiju sadržaja i kvalitete izvornog dokumenta, što se može postići:

- tako da se ne koriste kompresije s gubitkom podataka, poduzorkovanjem ili smanjenjem uzorka ili bilo koji postupak kojim se mijenja sadržaj ili degradira kvaliteta izvornih podatka u nastaloj datoteci,
- tako da se softverski ne izmijeni izvorni skenirani tekst s podacima koji su dobiveni optičkim prepoznavanjem znakova, zbog toga što optičkim prepoznavanjem može doći do gubitka podataka zbog nepreciznosti skeniranih znakova.

Točka 6.3.8. norme govori o Unicode znakovima koji moraju biti uključeni. Točka 6.8. govori o logičkoj strukturi koja se propisuje za nivo „a“ a koja se ne mora slijediti za nivo „b“.

ISO 19005-2:2011 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 2. dio: Korištenje ISO 32000-1 (PDF/A-2)

Drugi dio norme ISO 19005 opisuje korištenje PDF formata verzije 1.7 za očuvanje statičke vizualne reprezentacije elektroničkih dokumenata baziranih na straničnom prikazu.

Usklađena PDF/A-2a datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme. Usklađena PDF/A-2b datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme osim točaka 6.2.11.7. i 6.7. Usklađena PDF/A-2u datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme osim točke 6.7.

Norma opisuje tehničke zahtjeve za strukturu datoteke propisujući kako treba izgledati zaglavlje datoteke, kraj datoteke (engl. file trailer), koje simbole koristiti, koja su ograničenja, filtri koji se koriste mogu biti samo oni definirani u ISO 32000-1:2008, kompresiju JPG2000 i način njenog korištenja, fontove i zahtjev da se svi korišteni fontovi u svojoj potpunoj definiciji nalaze unutar datoteke, zabranjuje tipove 3D, zvuk, film i ekran (engl. screen), datoteka može imati podatke o pravu korištenja, certifikat i digitalni potpis, zabranjuje bilo

kakve akcije ili događaje pokrenute određenim okidačem, propisuje da se svi podaci trebaju unositi prema XMP specifikaciji, akcije stvaranja, transformacije ili bilo koja druga akcija na datoteci treba zapisati vrstu akcije, parametre akcije i vrijeme akcije u polju xmpMM:History, logičku strukturu kako bi se pomoglo u štićenju tekstualnog sadržaja kakav je bio u izvornom jeziku u kojem je pisan.

Zahtjevi za digitalni potpis su slijedeći:

1. digitalni potpis se mora odnositi na cijelu datoteku uključujući i rječnik potpisa ali isključujući sam potpis,
2. digitalni potpis mora biti smješten u polju Contents rječnika,
3. informacije vremenske oznake certifikata i opoziva certifikata moraju biti uključene.

Norma daje primjer dobre prakse te navodi kako se ne preporuča korištenje ne-XMP metapodataka, a za slučaj potrebe korištenja moraju se detaljno opisati u polju xmpMM:History. Kodovi jezika moraju biti korišteni prema normama ISO 639-2 i 3166-2, a oni koji su po ovim normama nepoznati koristi se oznaka x-unknown. Za arhivske potrebe očuvanja s ciljem očuvanja kvalitete i integriteta zapisa za koje je posebnim procedurama propisana minimalna rezolucija, ograničenja kompresije ili zabranjene procese koji uništavaju ili mijenjaju podatke predlažu konverziju u PDF/A format, zbog toga što konverzijski procesi repliciraju točan sadržaj i kvalitetu izvornog dokumenta u usklađenoj PDF/A datoteci. To se postiže na način da alati koji vrše konverziju:

- ne koriste kompresiju s gubitkom, poduzorkovanje (engl. subsampling), smanjenje uzorka (engl. downsampling) ili bilo koju drugu tehniku koja mijenja sadržaj ili kvalitetu izvorne datoteke,
- ne zamjenjuju pretraživi tekst na osnovu optičkog prepoznavanja zakova,
- procesiranje slike se obavlja uključivanjem originalno komprimirane slike ili procedurom dekompresije slike i ponovne kompresije koristeći kompresijske algoritme bez gubitaka.

Točka 6.2.11.7. govori o Unicode znakovima koji moraju biti uključeni bez obzira koriste li se u datoteci ili ne. Točka 6.7. govori o logičkoj strukturi koja se propisuje za nivo „a“ a koja se ne mora slijediti za nivoe „b“ i „u“.

ISO 19005-3:2012 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 3. dio: Korištenje ISO 32000-1 s podrškom za sadržane datoteke (PDF/A-3)

Ovaj dio norme opisuje korištenje PDF/A-3 formata verzije 1.7 za očuvanje statičke vizualne reprezentacije elektroničkih dokumenata baziranih na straničnom prikazu. Usklađena PDF/A-3a datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme. Usklađena PDF/A-3b datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme osim točaka 6.2.11.7. i 6.7. Cilj je ovog nivoa odrediti minimalne zahtjeve kojima se osigurava očuvanje vizualnog prikaza kroz vrijeme. Ali se ne odnosi na logičku strukturu i prirodni slijed sadržaja. Usklađena PDF/A-3u datoteka je ona koja zadovoljava sve zahtjeve ovog dijela norme osim točke 6.7. Cilj ovog nivoa je osigurati vizualnu reprezentaciju kroz protok vremena ali i mogućnost da se bilo koji tekst koji je sadržan u dokumentu pouzdano pročita kao serija Unicode kodnih znakova.

Razlika trećeg dijela norme 19005 je u Dodatku E koji omogućava ugnježđivanje drugih dokumenata unutar PDF datoteke. Na primjer, dokument nastao programom za tekstualnu obradu može sadržavati tekstualni sadržaj, matematičke izraze ili grafički prikaz tabličnih podataka. Zahtjevom za izradu PDF datoteke nastaje datoteka koja sadrži slijedeće ugniježđene datoteke, pri čemu su sve veze su upisane u polje AFRelationship:

- tekstualnu datoteku s vezom s izvornom datotekom i upisanu u katalog,
- MathML verziju matematičkog izraza s vezom kao dodatkom koristeći strukturni ili Form Xobject,
- tabličnu datoteku s vezom na slikovni ili Form XObject grafičkog prikaza,
- CSV datoteku s vezom na podatke i vezom na slikovni ili Form Xobject.

Točka 6.2.11.7. govori o Unicode znakovima koji moraju biti uključeni bez obzira koriste li se u datoteci ili ne. Točka 6.7. govori o logičkoj strukturi koja se propisuje za nivo „a“ a koja se ne mora slijediti za nivoe „b“ i „u“.

Zaključak

Norma ISO 19005 u svoja tri dijela (ISO 19005-1:2005 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 1. dio: Korištenje PDF 1.4 (PDF/A-1); ISO 19005-2:2011 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 2. dio: Korištenje ISO 32000-1 (PDF/A-2); ISO 19005-3:2012

Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 3. dio: Korištenje ISO 32000-1 s podrškom za sadržane datoteke (PDF/A-3)) opisuje elektronički format dokumenta za dugoročno očuvanje metodom statičke vizualne reprezentacije elektroničkih dokumenata baziranih na straničnom prikazu čuvajući njihov vizualni izgled tijekom vremena neovisno o alatima i sustavima koji se koriste za stvaranje, pohranjivanje ili prikazivanje datoteka. Prvi dio norme propisuje korištenje PDF 1.4 datoteke u formatu PDF/A-1 s dvije verzije „a“ i „b“. Drugi dio norme propisuje korištenje PDF 1.7 verzije datoteke u formatu PDF/A-2 s tri verzije „a“, „b“ i „u“. Dodatak verzije 1.7 je mogućnost upisivanja podataka o digitalnom certifikatu i digitalnom potpisu. Razlika verzija „a“ i „b“ je u propisivanju logičke strukture, prirodnog slijeda sadržaja te korištenje UNICODE kodnih znakova radi pouzdanosti čitanja tekstualnog sadržaja. Ukoliko ove dvije karakteristike nisu važne dovoljno je koristiti PDF/A-1b ili PDF/A-2b.

Prilikom konverzije slikovne datoteke u format PDF/A, kako bi se zadržala točna kopija sadržaja i kvalitete izvornog dokumenta, potrebno je voditi računa o slijedeća dva zahtjeva:

1. nisu korištene kompresije s gubitkom podataka, poduzorkovanja ili smanjenja uzorka, odnosno nije korišten bilo koji postupak kojim se mijenja sadržaj ili degradira kvalitetu izvornih podatka u nastaloj datoteci, i
2. vodi se računa da se softverski ne mijenja izvorni skenirani tekst s podacima koji su dobiveni optičkim prepoznavanjem znakova.

   Sve izmjene prilikom konverzije trebaju se upisati u polje History.

Velika prednost PDF datoteke je mogućnost upisa metapodataka i informacija koje su povezane s tom datotekom direktno u predviđena polja unutar same datoteke.

8.3. Ispis iz sustava

Sustav koji pohranjuje digitaliziranu dokumentaciju, pored prikazivanja i pretrage pohranjene dokumentacije može omogućiti ispis. U tom slučaju važno je znati je li ispisani dokument zaista dokument koji je bio pohranjen u tom sustavu te odgovara li zaista digitaliziranoj slici za koju se tvrdi. Rješenje mikroprint omogućava ispis dodatnog podatka kojeg je kasnije nemoguće promijeniti postupcima fotokopiranja i skeniranja, dok rješenje eGRAĐANI koristi različite nivoe za pristup u sustav.

8.3.1. eGRAĐANI

Sustav e-Građani je projekt Vlade RH kojemu je cilj modernizacija, pojednostavljenje i ubrzanje komunikacije građana i javne uprave i povećanja transparentnosti javnog sektora u pružanju javnih usluga, kako ističu na svojim službenim stranicama.[260] Sustav se sastoji od središnjeg portala, osobnog korisničkog pretinca i Nacionalnog identifikacijskog i autentifikacijskog sustava (skraćeno NIAS). Kroz osobni korisnički pretinac građani pristupaju elektroničkim uslugama javne uprave i primaju elektroničke poruke od strane javne uprave.

Građanima je preko pretinca omogućeno:

- pristupiti elektroničkim izvodima iz matične knjige rođenih, vjenčanih ili knjige državljana,
- provjeriti svoje podatke u Registru birača,
- zatražiti promjenu mjesta glasovanja u RH i inozemstvu, preko e-Privremeni upis,
- obaviti registraciju za glasovanje, za osobe bez osobne iskaznice RH,
- pribaviti uvjerenja o prebivalištu, boravištu te vlasništvu cestovnih vozila,
- saznati ocjene djeteta u školi,
- pregledati recepte u ljekarnama u zadnjih 6 mjeseci,
- provjeriti podatke o izabranom liječniku,
- naručiti Europsku karticu zdravstvenog osiguranja,
- zatražiti svoju elektroničku radnu knjižicu,
- dobiti informaciju o očekivanom iznosu mirovine,
- registrirati se kao potencijalni posloprimac,
- provjeriti uplaćene doprinose u drugi stup mirovinskog osiguranja,
- pribaviti potvrde od REGOS-a,
- provjeriti svoju poreznu knjigovodstvenu karticu,
- pregledati ukupne primitke, obračunate doprinose i poreze po pojedinim isplatiteljima,
- provjeriti svoje podatke u OIB sustavu,
- sudjelovati u procesima savjetovanja sa zainteresiranom javnošću,
- pregledati osnovne katastarske podatke,
- podnositi zahtjeve za izdavanje javnih isprava,

[260] O sustavu e-Građani. (n.d.). Preuzeto 23. 3. 2017. iz Središnji državni portal: https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584

- primiti poruke i obavijesti o isteku osobne iskaznice, putovnice, vozačke dozvole ili registracije vozila,
- primiti poruke i obavijesti o biračkom mjestu,
- primiti poruke i obavijesti o pravima iz mirovinskog i zdravstvenog osiguranja,
- primiti poruke i obavijesti o pravima za vrijeme nezaposlenosti,
- primiti poruke i obavijesti o cijepljenju kućnih ljubimaca,
- primiti poruke i obavijesti o novom dokumentu u sustavu eSPIS,
- primiti poruke i obavijesti o obračunatom porezu na dohodak,
- primiti poruke i obavijesti o jedinstvenoj uplatnici Zagrebačkog holdinga d.o.o,
- primiti poruke i obavijesti o početku blokade računa i deblokadi računa.

Sve usluge koje sustav omogućuje mogu se pronaći na internetskoj stranici: https://pretinac.gov.hr/KorisnickiPretinac/eGradani.html, gdje su navedene dostupne e-usluge sustava e-Građani navedene po temama, institucijama ili abecedno, zatim ostale e-usluge u RH također navedene po temama, institucijama ili abecedno, te popis e-poruka u Osobnom korisničkom pretincu naveden po temama, institucijama ili abecedno. Popis usluga je zaista velik.

Kako bi se postalo e-Građanin potrebno je dobiti elektroničku vjerodajnicu i kreirati Osobni korisnički pretinac. Elektroničke vjerodajnice izdaje Financijska agencija i to:

- **ePass** korisničko ime i lozinka, razine sigurnosti 2,
- **mToken** - aplikacija izrađena od CARNet-a za pametne telefone, razine sigurnosti 3,
- **FinaCertRDC** certifikat Financijske agencije, razine sigurnosti 4.

Po vjerodajnice koje izdaje Fina se dolazi osobno ili dolazi opunomoćenik koji mora imati pisanu punomoć, te je potrebno imati popunjenu i potpisanu pristupnicu te identifikacijski dokument na primjer osobna iskaznica ili putovnica.

Ukoliko korisnik posjeduje ePass vjerodajnicu i ne uspije se prijaviti u pet pokušaja treba ponovno otići u poslovnicu Fine na ponovno izdavanje.

Elektroničke vjerodajnice koje se mogu koristiti bez registracije u poslovnicama Fine za pristup sustavu e-Građani su:

- **Elektronička osobna iskaznica** (eOI) s identifikacijskim certifikatom, to je elektronička javna isprava koju svakom hrvatskom državljaninu izdaje Ministarstvo unutarnjih poslova RH a sadrži identifikacijski certifikat koji je vjerodajnica najviše razine kojom se može pristupiti svim elektroničkim uslugama sustava e-Građani,

- **Pametna kartica Hrvatskog zavoda za zdravstveno osiguranje** koju posjeduju zdravstveni djelatnici,
- **Korisničko ime i lozinka iz sustava AAI@EDU** koja je u nadležnosti Sveučilišnog računskog centra,
- **HPB token/mToken** Hrvatske poštanske banke d.d.,
- **Korisničko ime i lozinka ePošta HP** - Hrvatske pošte d.d.,
- **FinaSoft certifikat -** certifikat Financijske agencije,
- **ZABA token/m-token** Zagrebačke banke d.d.,
- **PBZ mToken/čitač kartica** Privredne banke Zagreb d.d.,
- **RBA Token/mToken i CAP čitač** Raiffeisenbank Austria d.d.,
- **SMS jednokratni pin** KentBank d.d..

Na stranicama Središnjeg državnog portala nalazi se lista prihvaćenih vjerodajnica[261] i popisane su u tablici 7.

Tablica 7. Lista prihvaćenih vjerodajnica

izdavatelj vjerodajnice	vjerodajnica za NIAS	sigurnosna razina	status
MUP RH - Ministarstvo unutarnjih poslova	Elektronička osobna iskaznica (eOI)	4	Trajna
CARNet - Hrvatska akademska i istraživačka mreža	mToken za e-Građane	3	Trajna
FINA - Financijska agencija	e-Građani ePass	2	Trajna
SRCE - Sveučilišni računski centar	Korisničko ime i lozinka - AAI@EduHr	2	Trajna
HZZO - Hrvatski zavod za zdravstveno osiguranje	Pametna kartica s certifikatom	3	Trajna
FINA - Financijska agencija	FinaSoft certifikat	3	Trajna
FINA - Financijska agencija	FinaCertRDC certifikat	4	Trajna
HPB – Hrvatska poštanska banka d.d.	HPB token / mToken	3	Trajna
HP - Hrvatska pošta d.d.	ePošta	2	Trajna
ZABA - Zagrebačka banka d.d.	ZABA token/m-token	3	Trajna
PBZ - Privredna banka Zagreb d.d.	PBZ mToken/čitač kartice	3	Trajna
RBA - Raiffeisenbank Austria d.d.	RBA token/mtoken i CAP čitač	3	Trajna
KentBank d.d.	SMS jednokratni pin	3	Trajna
OTP banka d.d.	OTP token/mobilni token	3	Trajna
HZMO - Hrvatski zavod za mirovinsko osiguranje	Korisničko ime i lozinka	2	Privremena
REGOS - Središnji registar osiguranika	Korisničko ime i lozinka	2	Privremena
HZZ - Hrvatski zavod za zapošljavanje	Korisničko ime i lozinka	2	Privremena

[261] Lista prihvaćenih vjerodajnica, e-Građani. (n.d.). Preuzeto 24. 3. 2017. iz Središnji državni portal: https://gov.hr/e-gradjani/lista-prihvacenih-vjerodajnica/1667

Pored popisa prihvaćenih vjerodajnica nalaze se i dokumenti iz kojih su vidljive ocjene i odluke po kojima su vjerodajnice prihvaćene.

Kako bi se odredila razina sigurnosti osiguranja kvalitete autentifikacije revizijski tim, koji se sastoji od najmanje jednog predstavnika Fine koji ima završen tečaj za internog revizora za ISO 27001 ili za glavnog revizora ISO 27001 i najmanje jednog predstavnika Ministarstva uprave, ocjenjuje fazu registracije i fazu elektroničke autentifikacije, i to po kategorijama:

1. faza registracije korisnika (R):
    a. ID – kvaliteta procedure identifikacije,
    b. IC – kvaliteta procesa izdavanja vjerodajnice,
    c. IE – kvaliteta izdavatelja vjerodajnice,
2. faza elektroničke autentifikacije korisnika (A):
    a. RC – vrsta i robusnost vjerodajnice,
    b. AM – sigurnost autentifikacijskog mehanizma.

Rezultirajuća ocjena odgovara najnižoj ocjeni faze registracije korisnika ili faze elektroničke autentifikacije korisnika. Ocijene i razine su točno propisane u dokumentu „Kriteriji za određivanje razine osiguranja kvalitete autentifikacije za Nacionalni identifikacijski i autentifikacijski sustav (NIAS) verzija 1.2“[262], koji je koncipiran na načelima EU projekta STORK (engl. Secure idenTity acrOss boRders linKed) i koji je usklađen s važećim pravnim aktima Republike Hrvatske i EU. Revizija se provodi svake dvije godine.

U spomenutom dokumentu su navedene slijedeće razine i opisi:

„**Razina 1 (nikakva ili najmanja sigurnost)** je najniža razina osiguranja, koja jamči najnižu razinu sigurnosti ili ne jamči nikakvu sigurnost. Vjerodajnice se prihvaćaju bez bilo kakve provjere. Ako se koristi adresa elektroničke pošte, jedina provjera je ispravnost adrese. Ova razina je odgovarajuća kad su posljedice od lažnog predstavljanja vrlo male ili nikakve. Prikladna je za usluge koje primjenjuju najmanji skup zaštitnih mjera ili ih ne primjenjuju.

Razina 2 (niska sigurnost) određuje razinu korištenu u uslugama kod kojih su štetne posljedice od lažnog predstavljanja male. Provjeru i potvrđivanje identiteta te izdavanje vjerodajnice mora obavljati tijelo koje ima odgovarajući ugovor s mjerodavnim državnim tijelom. Na ovoj razini se u postupku provjere i potvrđivanje identiteta ne zahtijeva fizička

[262] Kriteriji za određivanje razine osiguranja kvalitete autentifikacije za Nacionalni identifikacijski i autentifikacijski sustav (NIAS), verzija 1.2. (6. 12. 2013.). Preuzeto 24. 3. 2017. iz Projekt e-Građani: https://gov.hr/UserDocsImages//e-Gradjani_dok//NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2).pdf

prisutnost podnositelja zahtjeva za izdavanje vjerodajnice. Vjerodajnica se mora dostaviti točno podnositelju zahtjeva i sa zajamčenom sigurnošću. Prilikom korištenja vjerodajnice u autentifikaciji moraju se primijeniti dovoljno robusni protokoli autentifikacije.

Razina 3 (znatna sigurnost) određuje razinu korištenu u uslugama kod kojih su štetne posljedice od lažnog predstavljanja znatne. Provjera i potvrđivanje identiteta obavlja se metodama koje nedvosmisleno i s visokom sigurnošću identificiraju podnositelja zahtjeva za izdavanje vjerodajnice. Izdavatelje vjerodajnica nadzire, odnosno akreditira mjerodavno državno tijelo. Vjerodajnice ove razine su certifikati čiji se ključevi čuvaju u sigurnom softverskom spremniku (u daljnjem tekstu: soft certifikat), a mogu biti i certifikati čiji se ključevi čuvaju u sigurnom hardverskom spremniku (u daljnjem tekstu: hard certifikati). Postupci korištenja vjerodajnice prilikom udaljene autentifikacije su robusni.

Razina 4 (visoka sigurnost) je najviša razina osiguranja koju koriste usluge kod kojih bi lažno predstavljanje imalo visoke štetne posljedice. Postupak registracije zahtjeva barem jednu provjeru i potvrđivanje identiteta uz fizičku prisutnost podnositelja zahtjeva (npr. prilikom podnošenja zahtjeva za izdavanje vjerodajnice ili prilikom njenog preuzimanja). Alternativno, u slučaju on-line zahtjeva, identitet podnositelja zahtjeva se može ustanoviti korištenjem kvalificiranog e-potpisa, a u skladu s odredbama Zakona o elektroničkom potpisu RH. Certifikati su kvalificirani hard certifikati u skladu s direktivom 1999/93/EC. Postupci korištenja vjerodajnice prilikom udaljene autentifikacije su najrobusniji.“[263]

Dokument „Projekt e-Građani, Učestala pitanja i odgovori, verzija 1.0 iz 2014.“[264] daje informaciju kako je osobni korisnički pretinac izrađen u Java tehnologiji po najvišim sigurnosnim standardima, testiran performansno i sigurnosno kroz nekoliko kontrola i testiranja.

Isti dokument definira elektroničku vjerodajnicu: „**elektronička vjerodajnica** (vjerodajnica) je skup podataka kojim se korisnik predstavlja određenom entitetu, a služi kao dokaz za provjeru elektroničkog identiteta (e-ID) korisnika vjerodajnice za pristup uslužnim poslužiteljima pružatelja elektroničkih usluga (e-usluga). Vjerodajnica je nešto što korisnik zna ili/i posjeduje (npr. korisničko ime/lozinka, digitalni certifikat i sl.)“[265]

Tajni podaci vezani uz vjerodajnicu zna samo korisnik, što znači da NIAS sustav ne zna podatak o PIN-u, lozinci niti bilo koji drugi tajni podatak. Zbog toga je važno da korisnik

[263] ibid., str. 5-6
[264] Učestala pitanja i odgovori, verzija 1.0. (2014.). Preuzeto 24.. 3. 2017. iz Projekt e-Građani: https://www.gov.hr/UserDocsImages//e-Gradjani_dok/korisnicka_dokumentacija//2014-06-24-FAQ-e-Gradjani.pdf
[265] ibid., str.16

nikome ne povjerava tajne podatke vezane uz vjerodajnicu. Također, NIAS štiti samo komunikacijske kanale koji su pod njegovom kontrolom a to su: komunikacija između NIAS-a, pružatelja usluge i izdavatelja vjerodajnice. Komunikacijski kanal između pružatelja usluge i korisnika štiti pružatelj usluge, dok korisnik treba štititi svoj uređaj putem kojeg koristi svoju vjerodajnicu.

8.3.2. Mikroprint

Mikroprint, odnosno ispis prepoznatljivih znakova i shema, koristi se danas u izradi novčanica, na primjer novčanice Republike Hrvatske pored grba imaju ispisanu himnu Republike Hrvatske (slika 18) bankovnih čekova, i drugih papirnatih dokumenata s ciljem povećanja zaštite od neovlaštenog kopiranja i/ili distribucije. Svaki pokušaj kopiranja pomoću fotokopirnog uređaja, skenera ili pantografa[266] pretvara ove mikro-elemente u točke ili ravnu liniju.

Slika 18. Novčanica od 10 kn[267]

Albert Boni začetnik je ideje o mikroprintu.[268] Njegov cilj je bio smanjiti sliku kako bi izdavačke kuće i knjižnice imale veći pristup podacima s minimalnim ulaganjem u materijal i

[266] Pantograf je crtaća naprava koja je napravljena pomoću letvi koje su spojene zglobom i čine paralelogram a koristi se za mehaničko umanjivanje ili uvećavanje slika, crteža i slično. Vidi: http://www.enciklopedija.hr/natuknica.aspx?id=46478

[267] HNB. (1. 2. 2015.). Novac»Novčanice»Nevažeće novčanice»10 kuna. Preuzeto 23. 3. 2017. iz HNB: URL: https://www.hnb.hr/-/10-kuna, objavljeno 13.6.2015.

[268] Metcalf, K. D. (3. 1945.). The Promise of Microprint, A Symposium Based on The Scholar and the Future of the Research Library. Preuzeto 23. 3. 2017. iz COLLEGE AND RESEARCH LIBRARIES: https://www.ideals.illinois.edu/bitstream/handle/2142/35340/crl_06_02_170_opt.pdf?sequence=2

u prostor za pohranu. Boni je fotografirao stranice koristeći 35 mm mikrofilm koje je ispisivao na kartice koristeći ofset litografiju i na taj način postigao da na karticu veličine 15,24 mm x 22,86 mm stane 100 stranica teksta normalne veličine.

Videojet je u svojem izdanju iz 2015. godine objavio kako njihov 1650 High Resolution i 1620 HR Continuous Inkjet printeri mogu ispisivati znakove veličine 0,6 mm.[269] Veličina točke koju printeri ispisuju, prema internacionalnom sustavu mjernih jedinica SI, iznosi 0,35146 mm.[270]

Xerox je na svojim stranicama objavio kako su znanstvenici razvili tako mali font koji je veličine 1/100 dijela inča, odnosno 0,254 mm.[271] Na svojim stranicama dalje opisuju tehnologiju koju su razvili i koja može pomoći u povećanju sigurnosti samih dokumenata, odnosno, kako tvrde u Xerox-u, sam bi dokument za sebe garantirao autentičnost.

Tehnologija koju su razvili omogućuje mikro veličine slova, dvije razine ispisa koje su vidljive kroz posebne filtre, pod određenim kutom, pod fluorescentnim svjetlom ili infracrvenim svjetlom, ili kombinacijom svih navedenih tehnoloških rješenja.[272] Također tvrde da je njihova tehnologija u stanju ispisati knjigu od 100 stranica na standardnom papiru veličine 216 mm x 279 mm.

8.4. Zaključak

Dokumentacija koja je zaprimljena u trenutku prihvata u sustav i kojoj je dodijeljena jedinstvena oznaka prema klasifikacijskoj shemi dodatno se označava pomoću RFID naljepnice. Ovim označavanjem omogućava se praćenje kretanja fizičke dokumentacije tijekom cijelog perioda čuvanja sve do slanja na digitalizaciju. Praćenjem kretanja naljepnice i vođenjem revizijskog dnevnika postiže se održavanje izvornosti dokumentacije.

Digitalizirana slika može biti u mnogim formatima. Ukoliko se odabere TIFF format prema EXIF standardu moguće je u polja EXIF standarda upisati jedinstveni identifikator slike, broj točaka u retku i stupcu, korištena kompresijska tehnika, proizvođač i model

[269] VIDEOJET. (31. 3. 2015.). New Videojet Continuous Inkjet Printers Meet Micro Printing Needs. Preuzeto 23. 3. 2017. iz Recent Press Release: http://www.videojet.com/us/homepage/general/news/new-videojet-continuous-inkjet-printers-meet-micro-printing-needs.html

[270] Butcher, K., Crown, L., & Gentry, E. J. (5. 2006.). The International System of Units (SI) – Conversion Factors for General Use. Preuzeto 23. 3. 2017. iz NIST: https://www.gpo.gov/fdsys/pkg/GOVPUB-C13-f10c2ff9e7af2091314396a2d53213e4/pdf/GOVPUB-C13-f10c2ff9e7af2091314396a2d53213e4.pdf

[271] Xerox. (n.d.). Xerox Scientists Develop Microtext Font; Digitally Printing Tiny Words And Numbers Will Help Make, Documents More Secure. Preuzeto 22. 3. 2017. iz Innovation Home › Innovation Stories: https://www.xerox.com/innovation/news-stories/microtext/enus.html

[272] Xerox. (2013). Specialty Imaging Text. Preuzeto 22. 3. 2017. iz The sensible way to affordably secure your documents: https://www.xerox.com/digital-printing/latest/FFSBR-47U.pdf

skenera, podatke o digitaliziranoj slici, naziv softvera za prihvat slike, vrijeme i datum stvaranja slike, ime osobe koja je sliku stvorila, vrstu uređaja (skener ili fotoaparat), te vlasnika uređaja. Ove podatke moguće je upisati i u PDF format, pri čemu PDF verzija treba omogućiti očuvanje statičke vizualne reprezentacije digitalizirane slike. Dodatna prednost PDF formata je mogućnost upisa podataka o digitalnom certifikatu i digitalnom potpisu.

Dugoročna pohrana digitalizirane slike i pripadajućih metapodataka može se postići korištenjem PIQL film rješenja koje omogućava dugovječnost, očuvanje integriteta i autentičnosti podataka. Zapisivanje na film je moguće na dva načina od kojih je prvi jednak izradi mikrofilmskih svitaka, dok je drugi takav da se zapisuje digitalizirana slika u binarnom obliku.

Ispis elektroničke isprave se prema Zakonu o elektroničkoj ispravi dopušta izraditi na papiru i ovjeriti ju kod javnog bilježnika ili kod ovlaštene osobe tijela javne vlasti. Taj postupak rezultira ovjerovljenom preslikom elektroničke isprave. Digitalizirana slika može se također ispisati na papiru. Pitanje je kako se može znati iz kojeg sustava je ispisana takva preslika. Ispisom digitalizirane slike koja ima mikroprint zapis u kojem se nalazi podatak koji govori o izvornosti postiže se visok stupanj osiguranja od neovlaštenih manipulacija zbog toga što je takav zapis teško ili nemoguće promijeniti tehnikama fotokopiranja ili skeniranja. Za pristup originalnoj digitaliziranoj slici može se koristiti rješenje pomoću izdanih vjerodajnica te s odgovarajućim stupnjem sigurnosti.

9. ANALIZA PRIMJERA DOBRE PRAKSE

U nastavku slijedi analiza triju provedenih projekata pretvorbe fizičkog gradiva u elektroničko postupkom digitalizacije za dokumentaciju tvrtki HALMED, FINA i HPB, obraćajući posebnu pažnju na zadržavanje autentičnosti dokumenta tijekom procesa digitalizacije i nakon nje. Pažnja je posvećena i dodavanjem pripadajućih metapodataka u svakom koraku procesa.

9.1. Digitalizacija dokumentacije o lijeku - HALMED

U svojim radovima, Digitalizacija, prihvat i migracija gradiva u sustav upravljanja zapisima sa ciljevima ostvarivanja temeljnih funkcija HALMED-a i očuvanja gradiva[273] i Koncepti rada s metapodatcima nastalima u procesima digitalizacije[274], autori Rajh i Šimundža-Perojević detaljno opisuju projekt digitalizacije registraturnog i arhivskoga gradiva dokumentacije o lijeku. Projekt je započet 2013. godine preko vanjskog natječaja za dio koji se odnosi na digitalizaciju te vanjskog natječaja za uspostavljanje DAIS-a (Digitalni Arhivski Informacijski Sustav). Svake iduće godine, 2014., 2015. i 2016. ponavljani su natječaji za digitalizaciju gradiva.

HALMED[275], zbog velike količine i važnosti gradiva koje nastaje u procesima koji su potrebni kako bi se lijekovi i medicinski proizvodi odobrili za promet u Republici Hrvatskoj, 2013. godine započinje proces digitalizacije i uspostavljanja suvremenog sustava upravljanja dokumentima i zapisima DAIS.

Gradivo HALMED-a koje se digitaliziralo bilo je podijeljeno je u tri serije.

Serija 1 obuhvaća dokumentaciju o lijeku koja je upisana u aplikaciju Pismohrana (aplikacija kojom se prati životni vijek dokumentacije). Produkt digitalizacije su SIP (engl. Submission Information Package; dostavljeni informacijski paket nastao u procesu digitalizacije op.a.) paketi koji zadovoljavaju slijedeću strukturu:

1. krovna mapa,

[273] Rajh, A., & Šimundža-Perojević, Z. (2015.). Digitalizacija, prihvat i migracija gradiva u sustav upravljanja zapisima sa ciljevima ostvarivanja temeljnih funkcija HALMED-a i očuvanja gradiva. (S. Babić, Ur.) Radovi 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, 21.-23. listopada 2015., Topusko, str. 213-228.

[274] Rajh, A., & Šimundža-Perojević, Z. (2016.). Koncepti rada s metapodatcima nastalima u procesima digitalizacije. (S. Babić, Ur.) Radovi 49. savjetovanja hrvatskih arhivista Arhivi i domovinski rat, Plitvice 26.-28. listopada 2016., str. 389-404.

[275] Agencija za lijekove i medicinske proizvode osnovana je 2003. godine. U njenoj je nadležnosti proizvodnja, promet i primjena lijekova i medicinskih proizvoda u RH s osnovnim ciljem zaštite zdravlja ljudi.

a. XML datoteka s metapodacima i ostalim podacima za uvoz u DAIS,
b. PDF/A datoteka,

2. mapa kutije,
    c. mapa tehničke jedinice,
        i. PDF/A datoteka ili datoteke.

Metapodaci se sastoje od metapodataka iz aplikacije Pismohrana (arhivski metapodaci), aplikacije Nacionalni registar lijekova, te podataka koji su nastali u procesu digitalizacije, indeksiranja po nazivu skeniranog zapisa (prema detaljnoj uputi stručnjaka iz HALMED-a) i mikrofilmiranja (naziv mikrofilma, pozicija na mikrofilmu).

Budući da dokumentacija datira iz ranijih vremena kada se nije vodila elektroničkim putem postoji dio dokumentacije o lijeku koji nije upisan u aplikaciju Pismohrana. Za ovu dokumentaciju struktura SIP paketa izgleda nešto drugačije:

1. mapa nosi oznaku broja kutije i broja predaje,
    a. mapa označena brojem predaje i brojem tehničke jedinice,
        i. XML datoteka,
        ii. PDF/A datoteka.

Serija 2 obuhvaća tri podserije:

1. dokumentacija o odobrenim medicinskim/homeopatskim proizvodima,
2. rješenja upisa u očevidnik/izmjena/dopuna rješenja,
3. prijava medicinskoga proizvoda.

Struktura SIP paketa serije 2:

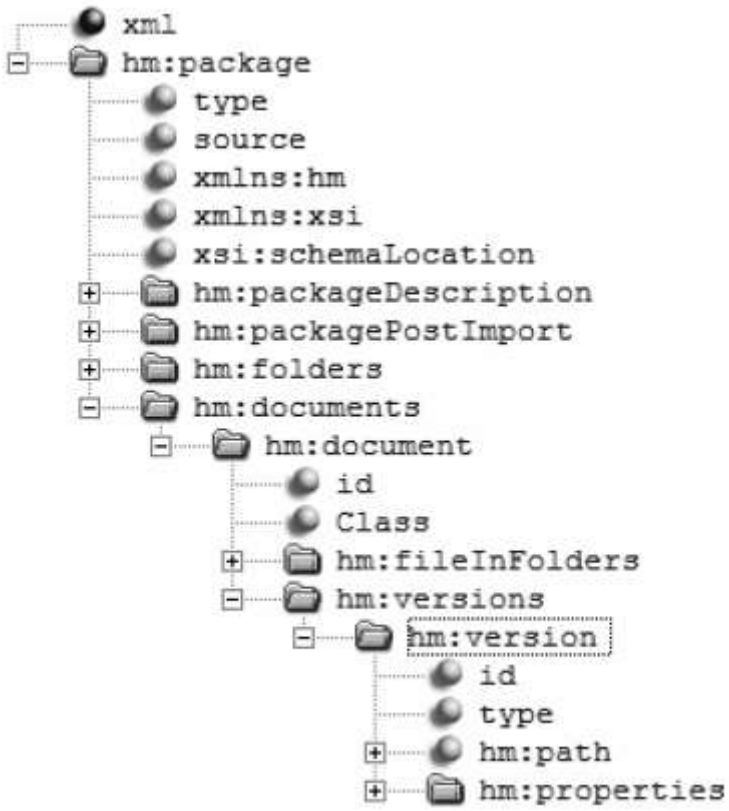
1. mapa nazvana prema barkodu izvorne tehničke jedinice,
    a. PDF/A datoteka,
    b. XML datoteka.

Serija 3 obuhvaća dokumentaciju farmakovigilancije sa svojim podserijama.

Struktura SIP paketa serije 3:

1. mapa s barkodom izvorne tehničke jedinice,
    a. PDF/A datoteka,
    b. XML datoteka.

Svaka XML datoteka (slika 19) sadržavala je potrebne informacije i instrukcije za sustav DAIS koji je prihvaćao isporučene pakete i učitavao ih u svoj sustav.



Slika 19. Primjer XML datoteke[276]

Autori ne ističu na koji način je obavljena digitalizacija, koji su skeneri korišteni, koja rezolucija slike, softver i njegove postavke koji su korišteni, ali ističu kako je proces digitalizacije obavljala druga tvrtka za što je napravljen natječaj koji je sadržavao detaljno ispisane zahtjeve za predviđenim isporukama te detaljnim sadržajima isporučenih paketa, kako bi se vršila adekvatna kontrola procesa digitalizacije, dok je sadržajnu kontrolu paketa obavljao tim djelatnika HALMED-a.

Prije samog početka projekta digitalizacije pripremljena je tehnička dokumentacija koja je sadržavala detaljan opis predmeta digitalizacije, informacije o projektnim izvještajima te informacije o normativno-tehnološkoj okolini projekta s ciljem adekvatne kontrole projekta. Dokumentacija koja je nastala tijekom rada na projektu sadržavala je slijedeće dokumente:

1. projektni prijedlog,
2. projektni obrazac (ekvivalentan projektnomu zadatku),

[276] Rajh, A., & Šimundža-Perojević, Z. (2015.). Digitalizacija, prihvat i migracija gradiva u sustav upravljanja zapisima sa ciljevima ostvarivanja temeljnih funkcija HALMED-a i očuvanja gradiva. (S. Babić, Ur.) Radovi 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, 21.-23. listopada 2015., Topusko, str. 224, Slika 4

3. projektni plan,
4. analiza rizika,
5. izvještaji sponzoru i internoj grupi za praćenje projekata,
6. popise dokumentacije za digitalizaciju i skeniranje,
7. potvrdu o predaji prototipa SIP paketa,
8. potvrdu o prihvaćanju prototipa,
9. upute za indeksere,
10. izvješća o projektu,
11. liste s podatcima o digitaliziranim i mikrofilmiranim tehničkim jedinicama (prilog izvješćima o projektu),
12. zapisnike o preuzimanju paketa, o povratu paketa s greškama i o ispravljenim paketima.

Kako bi se postigla propisana kvaliteta SIP paketa bilo je potrebno izraditi prototip prema tehničkoj specifikaciji i propisanoj kvaliteti.

Autori navode kako su se za izradu navedenih dokumenata vodili normom ISO 14721:2012 za otvorene arhivske informacijske sustave (OAIS), koja sadrži informacijski model i opis dostavljenoga informacijskog paketa, kako bi se postigao normiran oblik seta elektroničkoga ili elektroničkih zapisa i njegovih ili njihovih metapodataka, te normom ISO13008:2012 kako bi se uspostavila kvalitetna okolina, jer je projekt pretpostavljao da će biti potrebne konverzije međuformata (npr. TIFF u PDF/A) i migracije SIP paketa u HALMED-ov sustav DAIS (sustav kompatibilan OAIS sustavu).

Rajh i Šimundža-Perojević detaljnije opisuju prihvat SIP paketa u DAIS sustav.[277] DAIS sustav je podignut na Filenet P8 platformi koja ima modul za migraciju i prihvat u sustav sa tri procesa:

1. prihvat digitaliziranih zapisa iz SIP-ova za jedinice evidentirane u sustavu i u povezanu aplikaciju Pismohrana,
2. prihvat digitaliziranih zapisa iz SIP-ova za jedinice neevidentirane u Pismohrani,
3. migraciju dokumenata s optičkih medija uz deklariranje zapisa i konverziju u PDF/A.

Preduvjet za prihvat SIP paketa u DAIS je postojanje XML datoteke prema definiranoj strukturi i definiranim metapodacima.

Proces prihvata uključuje:

[277] Rajh, A., & Šimundža-Perojević, Z. (2015.). Digitalizacija, prihvat i migracija gradiva u sustav upravljanja zapisima sa ciljevima ostvarivanja temeljnih funkcija HALMED-a i očuvanja gradiva. (S. Babić, Ur.) Radovi 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, 21.-23. listopada 2015., Topusko, str. 213-228.

1. sadržajnu validaciju XML datoteke, odnosno provjeru metapodataka iz XML-a s metapodatcima iz poslovne baze Nacionalnoga registra lijekova,
2. presnimavanje paketa na mrežno mjesto mapirano s DAIS-om,
3. analizu i tehničku validaciju XML paketa iz DAIS-ova modula za migraciju i prihvat paketa,
4. prihvat ispravnog paketa u DAIS,
5. postimport operacije deklariranja zapisa.

DAIS sustav omogućuje pretraživanje prema svim metapodatcima iz XML-a i prema sistemskim podacima (npr. prema nazivu lijeka, jedinstvenom broju odobrenja, nazivu zapisa, klasi uredskoga poslovanja, datumu migracije itd.).

Kako u samoj dokumentaciji koja je predana na digitaliziranje postoje optički mediji s datotekama koje je također potrebno učitati u sustav DAIS, za to je korištena DAIS funkcija za migraciju s optičkih medija (ovo je rađeno s ciljem uništavanja optičkih medija zbog njihove kratkoće životnog vijeka, a prema mišljenju nadležnog arhiva koji je postupak presnimavanja dokumentacije s optičkih diskova odredila kao migraciju, a ne izlučivanje, nakon čega su se optički mediji uništili kada su bili ispunjeni uvjeti; internom uputom je propisan postupak migracije, provedeni postupak je svaki put dokumentiran, moguće je postupak identificirati u sustavu, a dokumentacija nema trajan rok čuvanja). Prilikom migracije DAIS koristi Aspose5 alat za automatsku konverziju tekstualnih datoteka u PDF/A format i pritom je uvijek moguće učitati izvornu inačicu datoteke jer sve verzije ostaju pohranjene u sustavu.

Dokumentacija digitalizirana u 2013. godini izlučena je i uništena uz odobrenje nadležnoga arhiva. Izlučeno i uništeno je 28369 tehničkih jedinica od ukupno 30799 tehničkih jedinica digitaliziranih u 2013. godini, osim tehničkih jedinica koje imaju trajan rok čuvanja.

Autori zaključuju kako je sustav u većoj mjeri kompatibilan ISO normi za otvorene arhivske informacijske sustave, a dugoročnu pohranu zapisa podupiru i procedure konverzije u arhivski PDF format i prijenos metapodataka putem XML formata za razmjenu podataka.

Koncept rada s metapodacima nastalim u postupku digitalizacije opisan je u radu istih autora „Koncepti rada s metapodatcima nastalima u procesima digitalizacije“[278]. Autori ističu kako je potrebno zabilježiti metapodatke koji dokumentiraju proces digitalizacije i

[278] Rajh, A., & Šimundža-Perojević, Z. (2016.). Koncepti rada s metapodatcima nastalima u procesima digitalizacije. (S. Babić, Ur.) Radovi 49. savjetovanja hrvatskih arhivista Arhivi i domovinski rat, Plitvice 26.-28. listopada 2016., str. 389-404.

metapodatke koji potvrđuju autentičnost i integritet dostavljenoga SIP paketa. U tu svrhu odredili su bilježenje slijedećih metapodataka:

1. metapodatci koji se bilježe za izvornik u knjigu pismohrane:
    a. identifikator – barkod komada,
    b. pripadnost konkretnoj registraturnoj jedinici,
    c. stavka posebnog popisa,
    d. rok čuvanja,
    e. klasa predmeta kojemu komad pripada,
    f. godina nastanka,
    g. datum zaprimanja zahtjeva iz predmeta,
    h. datum rješenja,
    i. rok važenja rješenja,
    j. medij izvornika,
    k. vrsta komada izvornika,
    l. posudbe komada,
    m. napomene,
2. metapodatci iz procesa digitalizacije:
    a. barkod izvornika kojim se digitalizirana kopija povezuje s izvornikom,
    b. naziv dokumenta koji je skeniran (indeksni pojam dokumenta),
    c. format datoteke,
    d. verzija formata datoteke,
    e. operater koji je skeniranje obavio,
    f. vrijeme skeniranja,
    g. tehnički podaci digitalizacije, kao što su hardverska i softverska okolina,
    h. vrijeme migracije,
3. metapodatci odredišnoga sustava:
    a. DAIS klasa entiteta,
    b. vrijeme migracije.

Prilikom skeniranja dokumentacije u HALMED-u operater očitava barkod čitačem barkod izvornika s naljepnice na dokumentaciji čime se izbjegavaju greške upisa barkoda i povezivanja s izvornikom te postiže da se na digitalizirani komad i fizički komad može primijeniti režim očuvanja definiran za tu registraturnu jedinicu.

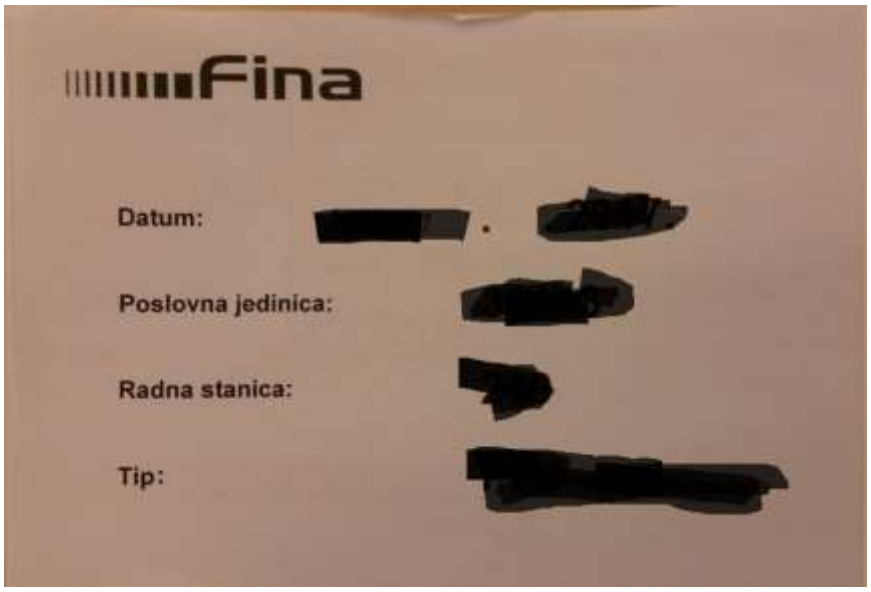
Prilikom digitalizacije dokumentacije povjerenoj vanjskoj tvrtki metapodaci iz točaka 1. i 3. ostaju isti kao i u internoj digitalizaciji, dok se metapodaci iz procesa digitalizacije (koji

su također isti) upisuju u dogovorenom formatu XML datoteke te učitavaju u sustav prilikom procesa učitavanja dostavljenih SIP paketa.

9.2. Digitalizacija dokumentacije - Fina

Dokumentacija nastaje u organizacijskim jedinicama Financijske agencije. Zaprimljena i obrađena dokumentacija pakira se u cjeline koje se dijele prema propisanom redoslijedu. Svaki paket dokumentacije je cjelina koja dobiva vodeći list (slika 21) na kojem se nalaze podaci:

- logo Fine,
- datum,
- broj poslovne jedinice,
- broj radne stanice,
- tip dokumentacije.



Slika 20. Vodeći list

Nastanak dokumentacije propisan je odgovarajućom internom uputom. U uputi je propisana obrada, postupanje i evidencije.

Dokumentacija se priprema u organizacijskoj jedinici gdje je zaprimljena. Slaže se u pakete dokumentacije prema datumu zaprimanja i na nivou organizacijske jedinice. Dalje se na razini organizacijske jedinice slaže redoslijedom radnih stanica. Prilikom slaganja paketa obavlja se priprema odnosno uklanjanje svih perforacija i/ili spajalica. Svaki paket se

označava vodećim listom s podacima: oznaka radne stanice, operativni broj jedinice i datum zaprimanja podataka. Dokumentacija se u paketu slaže prema redoslijedu zaprimanja i obrade.

Kontrolu pripremljene dokumentacije obavlja drugi operater prema listi dobivenoj iz evidencije radne stanice koje se nalaze u bazi podataka, i koja se ispisuje za svaku radnu stanicu. Lista kontrole se čuva u organizacijskoj jedinici u kojoj je nastala.

Rezultat obavljene pripreme i kontrole dokumentacije šalje se u organizacijsku jedinicu koja obavlja skeniranje ili mikrofilmiranje. Prijevoz se obavlja službenim vozilima koristeći obrazac za evidenciju preuzimanja dokumentacije koji sadrži slijedeće podatke:

- naziv dokumenta,
- datum slanja dokumentacije,
- naziv organizacijske jedinice,
- vrsta i opis dokumentacije,
- ime, prezime i potpis odgovorne osobe za slanje dokumentacije,
- datum prijevoza dokumentacije,
- naziv organizacijskog dijela koji prevozi dokumentaciju,
- ime, prezime i potpis odgovorne osobe za prijevoz dokumentacije,
- datum prijema dokumentacije,
- naziv organizacijske jedinice koja je dokumentaciju primila,
- ime, prezime i potpis odgovorne osobe za prijem dokumentacije.

Nakon preuzimanja, popunjavanja i potpisivanja, organizacijska jedinica koja je primila dokumentaciju, faksom šalje obrazac organizacijskoj jedinici koja je predala dokumentaciju kao obavijest da je dokumentacija preuzeta na skeniranje/mikrofilmiranje. Obrazac se čuva 11 godina koliko se čuva i sama dokumentacija na mikrofilmu.

Organizacijska jedinica koja skenira/snima dokumentaciju obavlja kontrolu primljenih radnih stanica prema listi dobivenoj iz baze podataka, slaže ih po rastućem redoslijedu, te ukoliko ima razlika dobivenih radnih stanica i liste dobivene iz baze podataka obavještava organizacijsku jedinicu gdje je dokumentacija nastala i rješavaju se razlike. Skeniranju/snimanju se pristupa nakon riješenih razlika.

Skeniranje se obavlja najkasnije u roku od sedam radnih dana od primitka dokumentacije. Ukoliko se prilikom obrade utvrdi nedostatak dokumenata kontaktira se organizacijska jedinica koja je predala dokumentaciju i rješava se nedostatak.

Mikrofilmiranje dokumentacije odvija se na dva načina. Jedan način je direktnim snimanjem na mikrofilm pomoću mikrofilmske kamere, opisan u uputi za rad s

mikrofilmskom kamerom, uz koju se veže uputa za rad i održavanje kamere te popis korištenih obrazaca.

Zaštitno snimanje na mikrofilm

Snimanje dokumentacije na mikrofilm pomoću kamere obavlja se kroz nekoliko koraka. Operater prilikom preuzimanja novog filma, mikrofilmskog svitka, u obrazac za evidenciju izdanih filmova upisuje:

- redni broj filma,
- datum snimanja,
- sadržaj, vrsta dokumentacije koja se snima,
- ime i prezime operatera.

Nakon zaduženja mikrofilmskog svitka operater na mikrofilmsku kutiju upisuje sljedeće podatke:

- na prednjoj strani kutije:
    - broj filma,
    - ime i prezime,
    - dokumentacija koja se obrađuje.

Prilikom snimanja operater mora voditi računa da uzima onoliko paketa dokumentacije koliko je siguran da će stati na mikrofilm, prema organizacijskoj jedinici i kompletnoj radnoj stanici te vodeći računa o rastućem redoslijedu. Prije početka snimanja na vodeći obrazac za snimanje upisuju se slijedeći podaci:

- datum snimanja,
- datum snimane dokumentacije,
- oznaka organizacijske jedinice,
- oznaka prve snimane radne stanice,
- ime i prezime operatera,
- broj filma,
- broj kamere na kojoj se dokumentacija snima.

Ovaj se obrazac prvi snima na mikrofilm.

Na kontrolni list operater upisuje podatke o snimanoj dokumentaciji prema redoslijedu snimanja:

- naziv organizacijske jedince,
- broj filma,

- vrsta dokumentacije,
- datum snimljene dokumentacije,
- ime i prezime kontrolora,
- operativna jedinica/radna stanica dokumentacije koja se snima,
- broj radne stanice/pozicija, blip, na filmu.

Ukoliko dođe do zastoja na kameri potrebno je ponoviti 5-10 zadnje snimljenih dokumenata uz dokumente koji su zastali u kameri. Prilikom ponavljanja prvo se snimi obrazac za ponavljanje snimanja, zatim ponovljeni dokumenti i oni koji su u kameri zastali, i na kraju obrazac za završetak ponavljanja.

Na kraju postupka snimanja dokumentacije operater snima obrazac za kraj snimanja na kojeg je prethodno unio podatke:

- datum i broj završnog dokumenta,
- broj snimljenih dokumenata,
- datum završetka snimanja,
- potpis operatera,
- naziv organizacijske jedinice.

Snimljeni mikrofilm se predaje na razvijanje i kontrolu zajedno s popunjenim obrascem za početak snimanja.

Kontrolor razvija mikrofilm prema uputi za rad s uređajem za razvijanje. Nakon završetka razvijanja kontrolor radi provjeru snimljene dokumentacije vizualnim pregledom koristeći uređaj za skeniranje s mikrofilma kontrolirajući ispravnost snimljene dokumentacije, kvalitetu snimljene dokumentacije i potpunost snimljene dokumentacije (ono što piše na kontrolnom listu mora odgovarati količini snimljene dokumentacije). Nakon izvršene kontrole obilježava kutiju filma upisujući:

- na poklopcu kutije filma:
    - datum dokumentacije koja se nalazi na mikrofilmu,
    - broj filma,
    - naziv organizacijske jedinice,
    - vrsta dokumentacije,
- na poleđinu kutije filma:
    - datum dokumentacije koja se nalazi na mikrofilmu,
    - broj filma,
    - naziv organizacijske jedinice,
    - vrsta dokumentacije.

Rad s kamerom je propisan s nekoliko uputa:

- uputa za rad s kamerom i uređajem za razvijanje mikrofilma,
- uputa za rad i održavanje kamere za snimanje dokumentacije,
- popis korištenih obrazaca.

Uputa za rad s kamerom i uređajem za razvijanje mikrofilma strogo propisuje način rada s kamerom i uređajem za razvijanje mikrofilma uključujući propisanu pripremu uređaja za snimanje, čišćenje kamere prije i za vrijeme obrade, periodično održavanje, pripremu uređaja za razvijanje, čišćenje uređaja za razvijanje prije i poslije razvijanja i periodično održavanje te upute za rad s uređajem za čitanje i reprodukciju slike s mikrofilma.

Digitalizacija i izvoz na mikrofilm

Drugi način izrade mikrofilma je prethodnim skeniranjem pripremljene dokumentacije po organizacijskim jedinicama, slanjem skenirane dokumentacije mrežom do arhivskog pisača koji digitalne slike snima na mikrofilm. Proces je u potpunosti propisan s nekoliko procedura koje određuju način snimanja, rad s aplikacijom za nadzor procesa, rad s aplikacijom za slanje i rad s uređajem za snimanje na arhivskom pisaču.

Procedura o načinu snimanja također navodi kako se dokumentacija priprema u organizacijskoj jedinici gdje se zaprima, te dalje opisuje korak koji se odnosi na skeniranje zaprimljene dokumentacije. Paketi se formiraju grupirajući dokumente na razini datuma, organizacijske jedinice, radne stanice te tipu dokumenta (može biti više vrsta dokumenata). Na vrh paketa stavlja se vodeći list na kojem pišu podaci: datum, organizacijska jedinica, radna stanica i tip. Zatim se dokumentacija reda redoslijedu unosa.

Skeniranje se obavlja koristeći unaprijed definirani profil za ovu vrstu posla u kojem je postavljeno: jednostrano skeniranje, crno-bijelo, rezolucija 200 dpi. Nakon skeniranog paketa pomoću aplikacije se upisuju:

- vrsta filma,
- datum paketa,
- poslovna jedinica,
- radna stanica,
- tip posla.

Aplikacija prenosi upisane podatke u bazu podataka te izrađuje potrebnu datoteku sa svim slikama koje se nalaze u jednoj mapi i dalje mrežom šalje na određeno centralno mjesto. Rad s aplikacijom za izradu datoteke opisano je uputom. Aplikacija omogućava pregled

statističkih podataka izvršenih pakiranja, brisanje/preimenovanje paketa, i na zahtjev kontrolora ponavljanje skeniranja dokumenta. U aplikaciju se prijavljuje korisničkim imenom i lozinkom. Osim osnovnih podataka potrebnih za imenovanje paketa aplikacija u bazu upisuje podatke: trenutno vrijeme, datum, IP adresu korisnika, identifikator korisnika i broj verzije paketa.

Tijekom skeniranja kontrolor provjerava proces i prema potrebi briše ili preimenuje pakete, a nečitke slike vraća na skeniranje. Nakon obavljene kontrole kontrolor postavlja status za snimanje na mikrofilm. Kontrola se obavlja koristeći aplikaciju za kontrolu, što je opisano uputom. Aplikacija omogućava provjeru cjelovitosti i integriteta digitalizirane dokumentacije, te njihovu kvalitetu (skenirane slike i indeksiranih podataka). U aplikaciju se prijavljuje korisničkim imenom i lozinkom. Kontrola upisanih indeksiranih podatka provodi se bilo slijedno redak po redak, bilo preko različitih SQL upita koji su prethodno definirani i proizašli iz dugotrajne obrade dokumentacije.

Slijedeći korak procesa je snimanje paketa na mikrofilm, što je opisano uputom za snimanje na arhivskom pisaču. Snimanje se provodi koristeći dvije aplikacije: prva se koristi za izradu ulazne liste koja vodi računa o dužini filma, u koju se operater prijavljuje korisničkim imenom i lozinkom, te druga za rad s arhivskim pisačem u kojoj je predefiniran profil za snimanje. Prema ulaznoj listi aplikacija za rad s arhivskim pisačem snima pripremljenu, skeniranu dokumentaciju na mikrofilm.

Nakon izrađenog, razvijenog, mikrofilma pristupa se kontroli mikrofilma. Svi paketi koji nisu ispravno snimljeni označavaju se i brišu se iz izlazne liste. Paketi koji su dobro snimljeni dobivaju podatak o vremenu kontrole. Svi pogrešni paketi javljaju se u organizacijsku jedinicu koja skenira dokumentaciju kako bi ih ponovno skenirali.

Nakon obavljene kontrole izrađuje se tablica koja sadrži podatke:

- paket,
- verzija snimljenog paketa,
- blip – pozicija na filmu.

9.3. Digitalizacija dokumentacije – Hrvatska poštanska banka (HPB)

Dokumentacija se zaprima u organizacijskim jedinicama prema ugovorenoj usluzi dobavljača, koja se na kraju dana sakuplja u pakete dokumentacije složene po redoslijedu zaprimanja ovisno o pojedinoj organizacijskoj jedinici. Za svaki paket se radi izlazna lista po kojoj se vrši kontrola paketa. Kontrolom se provjerava je li sva dokumentacija navedene na listi unutar fizičkog paketa koji se kontrolira. Nakon kontrole popunjava se vodeći list koji sadrži datum dokumenta, datum kontrole, broj komada u paketu, broj organizacijske jedinice, potpis osobe koja je sastavila paket i potpis osobe koja je izvršila kontrolu.

Svaku srijedu se dokumentacija, skupljena tijekom proteklog tjedna i smještena u kutije, predaje vanjskoj tvrtki koja digitalizira dokumentaciju. Prilikom predaje potpisuje se primopredajni zapisnik. Primopredajni zapisnik sadrži slijedeće podatke:

- naslov zapisnika,
- broj zapisnika,
- tip dokumentacije,
- mjesto nastanka dokumentacije,
- adresa,
- ime i prezime odgovorne osobe,
- broj telefona i faksa,
- e-mail,
- vrsta dokumentacije i raspon organizacijskih jedinica,
- zatim podaci o predanoj dokumentaciji koji sadrže podatke:
    - broj arhivske jedinice,
    - period nastanka od do,
    - raspon organizacijskih jedinica u kutiji,
- datum predaje,
- ime i prezime osobe koja je predala dokumentaciju,
- potpis osobe koja je predala dokumentaciju,
- datum predaje za dobavljača,
- ime i prezime osobe koja je preuzela dokumentaciju,
- potpis osobe koja je preuzela dokumentaciju.

Uz ovaj primopredajni zapisnik prilaže se popis arhivskog materijala za predani datum koji sadrži:

- naslov dokumenta,

- logo HPB-a,
- broj kutije,
- za svaku organizacijsku jedinicu:
    - broj organizacijske jedinice,
    - broj dokumenata,
- ime i prezime osobe koja je predala dokumentaciju,
- datum predaje,
- potpis i pečat ovjere predaje,
- ime i prezime osobe koja je preuzela dokumentaciju,
- datum preuzimanja dokumentacije.

Ovaj prilog se provjerava nakon izvršenog skeniranja te se upisuju odstupanja koja se javljaju HPB-u.

Nakon primitka dokumentacije kreće se sa procesom skeniranja prateći proceduru dobavljača o snimanju dokumentacije. Procedura propisuje slijedeće korake:

1. zaprimanje dokumentacije,
2. priprema kontrolnih podataka,
3. skeniranje,
4. indeksiranje,
5. administracija,
6. arhiviranje originalne dokumentacije,
7. eksport digitalizirane dokumentacije,
8. isporuka portabilne arhive.

Za sve korake su propisane detaljne upute kako se obavljaju. Upute su propisane kroz dokumente:

- uputa za pripremu kontrolnih podataka,
- uputa za skeniranje,
- uputa za rad s aplikacijom za slanje,
- uputa za indeksiranje,
- uputa za rad s aplikacijom za indeksiranje,
- uputa za administriranje obrade,
- uputa za rad s aplikacijom za administriranje.

Kontrolni podaci se preuzimaju u obliku datoteke s dogovorenih mrežnih stranica, na koje se prijavljuje pomoću korisničkog imena i zaporke. Preuzimanje se provodi automatski. Zatim se pomoću aplikacije preuzeti podaci učitavaju u sustav. Aplikacija se pokreće nakon

unosa korisničkog imena i lozinke. Podaci se dalje automatski raspakiraju i učitaju u sustav te se povratno, nakon učitavanja, dobije potvrda o uspješnom učitavanju.

Dokumentacija se skenira koristeći aplikaciju Capture Perfect koristeći slijedeće postavke:

- rezolucija 300 dpi-a,
- jednostrano skeniranje,
- crno-bijelo,
- postavka: Advanced text enhancement 2,
- naziv datoteke – kreira se iz datuma i vremena nastanka.

Prilikom skeniranja vodi se računa o veličini paketa i ukoliko paket ima više od 500 stranica, nakon 500 stranica radi se novi paket. Ovo ograničenje od 500 stranica određeno je kombinacijom zahtjeva za brzim radom prilikom procesa kontrole i zahtjevom za visokom brzinom skeniranja. Vodeći list se ne skenira. Prvo se skenira izlazna lista koja se nalazi u svakom paketu. Nakon izrađenog paketa od 500 ili manje slika pokreće se aplikacija na koju se operater prijavi pomoću korisničkog imena i zaporke, te se u nju upisuju podaci:

- datum,
- broj organizacijske jedinice,
- broj paketa (ako je paket od više od 500 dokumenata, tada će za istu organizacijsku jedinicu postojati paketi _01, _02, i tako dalje).

Sve nepravilnosti u radu, nepravilno složen paket, dokument koji nije prihvatljiv i kojeg nije moguće poboljšanjima pretvoriti u čitljiv dokument, javljaju se administratoru ovog posla koji dalje s predstavnicima HPB-a rješavaju situaciju.

Ukoliko operater na skeneru pogriješi prilikom skeniranja može, novu i ispravnu verziju, ponovno skenirati tražeći od administratora brisanje ili preimenovanje skeniranog paketa, što se odvija kroz aplikaciju.

Indeksiranje se obavlja pomoću aplikacije za indeksiranje u koju je potrebno prijaviti se pomoću korisničkog imena i zaporke. Prije prijave u aplikaciju napravljen je OCR skenirane dokumentacije. U tijeku indeksiranja provjeravaju se OCR-om upisani podaci. Koristeći OCR tehnologiju čita se identifikator dokumenta, koji je jedinstven. Pomoću pročitanog identifikatora iz baze podataka dobiva se odgovor koji sadrži sve ostale podatke prethodno dobivene od HPB-a, a stvorene u tijeku obrade dokumentacije u organizacijskoj jedinici. Podaci dobiveni iz baze podataka odgovaraju podacima stvorenim na šalterima i time predstavljaju točne unose zbog čega se daljnje indeksiranje odnosi na provjeru ispravno upisanog/pročitanog identifikatora. Neispravno pročitane identifikatore operater ručno upisuje

(ukoliko to nije moguće dokument dobiva oznaku iznimke). Pomoću tog upisa aplikacija za indeksiranje iz baze podataka dobiva odgovor o ostalim upisanim podacima u bazi. Sve upisane podatke provjerava operater i prilikom uočavanja pogreške označava dokument s oznakom iznimke.

U procesu administracije kontroliraju se svi dokumenti označeni oznakom iznimke, brisanja i ponavljanja. Ukoliko identifikator nije čitljiv, ostaje oznaka iznimke. Svi dokumenti s oznakom brisanja provjeravaju se prije brisanja i brišu se samo oni koje je zaista potrebno obrisati. Svi dokumenti s oznakom ponavljanja ponavljaju se u procesu skeniranja te se obavlja indeksiranje ovih dokumenata na prethodno opisan način.

Dodatne kontrole koje se obavljaju su:

- kontrola organizacijske jedinice i datuma se ne slaže s upisanom organizacijskom jedinicom i datumom u fazi skeniranja,
- svi dokumenti označeni oznakom izlazne liste moraju biti samo izlazne liste,
- razlika upisanih identifikatora, organizacijske jedinice i datuma s podacima koji se nalaze upisani u baznim tablicama,
- provjera duplih identifikatora (ne smije biti duplih identifikatora jer su identifikatori jedinstveni).

Na kraju svakog ciklusa obrade, jednom tjedno, i nakon obavljene provjere administracije i kontrole obavlja se isporuka obavljenog posla obrade dokumentacije. U fazi isporuke kreira se broj isporuke, potrebne mape (nazivi se stvaraju na nivou datuma s podmapom broj organizacijske jedinice i broj paketa, unutar kojih se nalaze slike), indeksne datoteke (koje sadrže podatke: identifikator, broj organizacijske jedinice, iznos), te statističke tablice. U aplikaciju za isporuku potrebno je prijaviti se pomoću korisničkog imena i zaporke.

Statistika sadrži podatke:

- broj organizacijske jedinice,
- datum,
- broj datoteka.

Ova tri podatka se uspoređuju s podacima dobivenim prilikom preuzimanja dokumentacije i upisanim greškama uočenim u fazi skeniranja i za njih se izrađuju razlike. U tablici razlika nalazi se popis koji sadrži podatke: organizacijska jedinica, datum, identifikator, koji se formira za razlike prema identifikatoru:

- za dokumente koji nisu bili u preuzetim kontrolnim podacima (ovo je moguće za slučaj da je dokumentacija nastala tjedan prije a nije predana tada već u ovom tjednu),

- za dokumente koji su bili u kontrolnim podacima a nisu obrađeni (ovo je moguće za dokumente koji još nisu predani u ovom tjednu već će biti predani u idućem tjednu),

i za razlike prema datumu:

- za dokumente koji se ne nalaze u rasponu po datumu preuzimanja.

Dodatno se izrađuje statistika svih dokumenata koji nisu mogli biti pročitani u fazi obrade.

10. MODEL PROCESA STVARANJA AUTENTIČNIH DIGITALNIH KOPIJA U OBLIKU ORIGINALA POSTUPKOM DIGITALIZACIJE

Stančić u svojem doktoratu navodi: "Imajući na umu koncept originala i kopije u elektroničkom obliku, rezultati InterPARES projekta pokazuju da se u načelu mogu razlikovati najmanje tri vrste kopija: kopija u obliku originala, imitirajuća kopija i jednostavna kopija. Kopija u obliku originala (engl. copy in the form of an original) je kopija koja je po svim svojstvima identična originalu, ali je nastala naknadno. (...) Imitirajuća kopija (engl. imitative copy) je kopija koja po svemu odgovara originalu, ali se odmah može vidjeti da je riječ upravo o kopiji, a ne o originalu. (...) Jednostavnu kopiju (engl. simple copy) predstavlja kopija koja reproducira samo sadržaj originalnog zapisa i u njoj nema informacije o kontekstu."[279] InterPARES projekt pojašnjava: "Bilo koja od ovih kopija je autentična ako je ovjerena kao takva (...) čime se smatra da odgovara zapisu koji reproducira sve dok se ne pojavi dokaz da nije tako. Ovakvo ovjeravanje proizlazi iz mogućnosti iskazivanja dokaza o (...) zadovoljavanju primjenjivih temeljnih zahtjeva za održavanje i svih zahtjeva za stvaranje autentičnih kopija."[280]

U poglavljima koji slijede razrađuje se *Model procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije*. Razvijeni model omogućava stvaranje autentičnih kopija prema zahtjevu za autentičnost razmatranom u poglavlju 3. Autentičnost. Budući da je riječ o konverziji papirnatog dokumenta u digitalini, te da se kontekst dokumenta osigurava pomoću odgovarajućih metapodataka, model razmatra stvaranje kopije u obliku originala u smislu rezultata InterPARES projekta.

10.1. Autentičnost prije digitalizacije

U ovom poglavlju neće se razmatrati autentičnost dokumenata prije digitalizacije. Obaveza organizacije je uredno vođenje dokumentacije i briga o dokazima autentičnosti tijekom svih faza kroz koje dokument prolazi, kao što je uredno vođenje svih primopredajnih zapisa i drugih dokaza autentičnosti. Također, svi podaci koji podržavaju autentičnost i pripadajući metapodaci trebaju podržavati mogućnost dokazivanja autentičnosti prije upućivanja u proces digitalizacije.

[279] Stančić, H. (2005). Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata, Doktorska disertacija. Zagreb., str. 159

[280] The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project – Authenticity Task Force Report. (n.d.). Dohvaćeno iz http://www.interpares.org/book/index.htm

10.2. Masovna digitalizacija i njezini problemi

Kada govorim o masovnoj digitalizacija podrazumijevam velike količine papirnatih dokumenata koji su složeni po određenom redoslijedu i pravilima u pakete koji dolaze i prolaze kroz skener s istim postavkama za cijeli paket. Može se dogoditi da se u paketu nalaze različite veličine papira, na primjer od A3 do A6 formata. U tom slučaju se može u softver za prihvat slike odabrati funkcija koja prepoznaje veličinu dokumenta, međutim moguće je, radi različitih nepravilnosti u radu skenera, ovom funkcionalnosti u kritičnom trenutku prenijeti pogrešnu informaciju zbog koje program može odrezati dio slike smatrajući da je manjeg formata.

Prolazak papira kroz skener odvija se koristeći sklop kotačića i vodilica. Ovaj sklop treba biti tako napravljen i podešen da ne uništi papir. Do greške može doći ako je papir loše kvalitete i ne može izdržati prolaz kroz skener te ga skener uništi i stvori djelomičnu sliku dokumenta. Zbog toga je potrebno obaviti kontrolu uređaja prije puštanja uređaja u rad. To obično obavlja serviser. Podatak o obavljenoj kontroli uređaja prije puštanja u rad serviser zapisuje na radnom nalogu.

Digitalizacijom papirnate dokumentacije nastaje digitalni reprezentant te dokumentacije. Odbijanjem svjetlosnih zraka od papira nastaju valne duljine koje se prihvaćaju u senzoru i pretvaraju u digitalne kombinacije koje se zatim prikazuju u obliku točaka na ekranu. Svaka takva digitalna kombinacija predstavlja određenu boju. Na dokumentu se mogu nalaziti sitni elementi, kao što su potpisi, decimalni zarezi i slično. Zbog čestica prašine i karbona ovi sitni elementi mogu biti prekriveni ili spojeni što senzoru može biti pogrešna svjetlosna informacija. Zato je potrebno osigurati da skener nije dodao niti oduzeo relevantne informacije.

Nadalje, tijekom skeniranja obaveza operatera je pratiti što se događa i kakve slike se stvaraju, međutim zbog samih brzina skenera koje se danas postižu nije moguće uvijek opaziti nedostatke na slici.

Original zaista može biti u takvom stanju da je oštećen i da mu nedostaju dijelovi. To ne smije, ali može, biti razlog za odbacivanje dokumenta iz procesa skeniranja, ali treba biti zapisano ovakvo stanje. Stanje papira se treba provjeriti prilikom stvaranja paketa na pripremi.

Kako prepoznati, odnosno kako izdvojiti, dokument koji ima kritične elemente iz velike količine stvorenih slika za slučaj kada sređivanje gradiva ili uredno vođenje podataka o dokumentima nije provođeno prije točke digitalizacije? U ovom slučaju pomogao bi alat koji

bi automatski provjeravao povezane skupove točaka iste boje. Ovo ima smisla ukoliko se izrađuje crno-bijeli dokument. Kada se izrađuje dokument u boji postojati će veliki broj nijansi koje u slučaju automatske provjere neće dati rezultat. Tako na primjer brisanje praznih stranica ne daje rezultate kada se primjenjuje na dokumentima u boji, međutim vrlo dobre rezultate daje prilikom izrade dokumenata u crno-bijelom tonu.

Drugi način je korištenjem automatske provjere ukoliko se iz istog papirnatog originala izrade dva dokumenta od kojih je jedan u boji a drugi u crno-bijelom tonu. Tada sve digitalizirane slike u boji za koje se automatskom provjerom digitaliziranih slika u crno-bijelom tonu pokaže da sadrže skupine crnih točaka mogu biti izdvojene za dodatnu provjeru operatera.

Postoje određene situacije u kojima se može naći skener tijekom faze skeniranja. Skener može uvući dva papira kroz vodilice i skenirati prednju stranicu prvog papira, a stražnju stranicu drugog papira. Skener može stvarati točke kojih na papiru nema, zbog posljedica prašine, tom prilikom na jednom dokumentu mogu biti navedene točke, dok na drugom dokumentu tih točaka neće biti jer su čestice prašine „otišle“ s prethodnim dokumentom. Skener može stvarati nepostojeće crne crte. Razlog tome može biti kvar na senzoru, oštećeno staklo koje štiti lampu i senzor, oštećena lampa ili oštećeno ogledalo. Kada ovakve crte primijeti operater potrebno je prijaviti kvar i zamijeniti element, a paket ponovno skenirati nakon servisa.

Ukoliko nema adekvatnog kontrasta između podloge i otiska tada se može u potpunosti izgubiti podatak. Primjer toga je zelena podloga na koju se pisalo grafitnom olovkom. Zbog pomanjkanja kontrasta i skeniranjem u crno-bijelom tonu, svjetlosni signal će se prevesti u bijelu pozadinu ili u potpuno crnu pozadinu. Skener može izgubiti postavke dobivene kalibracijom i u tom slučaju se boje neispravno stvaraju ili može oslabiti lampa koja daje bijelu svjetlost. Tijekom skeniranja velike količine dokumenata dolazi do zagrijavanja cjelokupnog hardvera što može dovesti do izobličenja pretvorbe svjetlosnih valnih duljina u digitalne reprezentante.

Promatramo li dokument i njegovo fizičko stanje očuvanosti nosača, na primjer papira ili kartona, i zapisa na nosaču, može se dogoditi da tijekom vremena nestanu određeni podaci, na primjer osušena tinta nalivpera može nestati (u potpunosti izblijediti) s kartonskog zapisa ukoliko nije adekvatno čuvan. U tom slučaju nastaje slika bez podataka i mora biti omogućena provjera i unos stanja originala.

U skeneru postoji i optički sklop koji se sastoji od izvora svjetla, elemenata koji odbijaju svjetlo, kao na primjer ogledala, elementa koji štiti izvor svjetla, kao na primjer staklo, i senzore. Sve se nalazi u kućištima skenera koje može biti različitih materijala.

Svjetlosni val se prihvaća na senzoru i dalje šalje kroz sklopove koje pokreće pokretački program koji dalje šalje informacije u softver za prihvat slike koji dalje obrađuje dobivene informacije te daje konačni proizvod u obliku digitalizirane slike. Pokretački program može biti različito izveden i imati funkcionalnosti kakve ima i softver za prihvat slike.

Izvorni dokument prije dolaska u proces digitalizacije bio je povezan s određenim metapodacima koji su ga dodatno opisivali i određivali svojstva kao što je izvornost, stvaratelj, proces u kojem je prihvaćen i slično. Ovi se podaci trebaju povezati i sa digitaliziranom kopijom. Tim podacima potrebno je pridružiti ostale metapodatke o stvaranju, kao što je proces u kojem je stvoren, tko je obavio pripremu i kada, tko je obavio skeniranje i kada, tko je obavio indeksiranje i kada te tko je obavio kontrolu i kada.

Dodatno, budući da je digitalizirana slika skup točaka u određenoj boji, tom skupu točaka potrebno je pridružiti podatke kao što su datum, ime, prezime, naslov dokumenta i slični podaci koji se nalaze na slici u obliku skupa točaka. Ovi se podaci mogu „pročitati“ korištenjem OCR tehnologije, ili se mogu ručno upisati. U svakom slučaju potrebno ih je nakon unosa provjeriti a zapis o ovoj kontroli evidentirati.

Pretvorbom u crno-bijelu sliku papir na kojem je ostatak prolivene kave postaje crna mrlja. Ovaj podatak se mogao pročitati s papira ali pretvorbom u crno-bijeli ton smeđa boja se stapa s crnom i postaje crna mrlja koju nije moguće OCR tehnologijom protumačiti kao prepoznatljive znakove. Dodatni je problem što ovakvu crnu mrlju ne možemo protumačiti niti vizualno jer su se podaci stopili i izgubili.

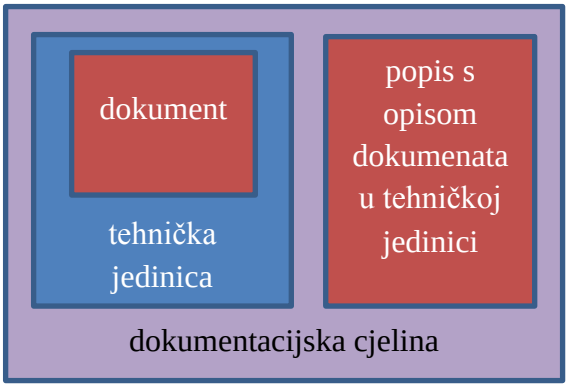
10.3. Dokumentacijska cjelina

Dokument koji je potrebno digitalizirati, kada je riječ o masovnoj digitalizaciji, nalazi se kao dio veće cjeline. Zakon o arhivskom gradivu i arhivima (iz 1997. godine) pod dokumentom u ovom smislu masovne digitalizacije podrazumijeva sve spise, isprave, pomoćne uredske i poslovne knjige, kartoteke, karte, nacrte, crteže, plakate, tiskovnice i slikopise. Isti zakon cjelinu dokumenata naziva registraturnim gradivom (prijedlog novog Zakona o arhivskom gradivu i arhivima ovu cjelinu naziva dokumentarnim gradivom, op.a.). Za potrebe daljnjeg rada ova cjelina dokumenata nazivat će se dokumentacijska cjelina.

Dalje, dokumenti koji čine dokumentacijsku cjelinu slažu se u tehničku jedinicu, na primjer mapa, fascikl, arhivska kutija i slično. Na ovaj način svaki dokument se nalazi u svojoj pripadnoj tehničkoj jedinici. Na primjer, odluka o pokretanju nabave dobiva svoj jedinstveni klasifikacijski broj i smješta se u spis (u žutu košuljicu, op.a.) koji dobiva svoj jedinstveni klasifikacijski broj. Na taj način postoje dva jedinstvena broja koji povezuju dokument i tehničku jedinicu. Može se dogoditi da više spisa budu složeni u veću tehničku jedinicu, kao što je to na primjer arhivska kutija, koja dobiva svoju jedinstvenu oznaku. Ili, primjerice, zaprimljena ulazna faktura redovito se smješta u odgovarajući registrator. Zaprimljena faktura dobiva svoj jedinstveni broj, ali i registrator dobiva svoj jedinstveni broj.

Prema Pravilniku o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva svaka dokumentacijska cjelina sadrži popis dokumenata koje sadrži te popis dokumenata koji nedostaju. U ovaj popis treba dodati podatak o broju stranica svakog dokumenta i broj praznih stranica kako bi se zadovoljio zahtjev potpunosti nakon skeniranja, jer ukoliko taj podatak nije poznat prije digitalizacije nije ga moguće provjeriti nakon digitalizacije. Popis dodatno sadrži i redoslijed nastajanja dokumenata.

Objašnjeni odnosi dokumenta, tehničke jedinice i pripadajućeg popis prikazani su na slici 24.

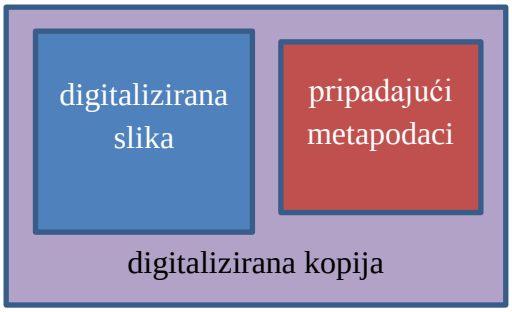


Slika 21. Dokumentacijska cjelina

10.4. Digitalizirani dokument

U procesu digitalizacije jedna ili više dokumentacijskih cjelina čini paket koji se digitalizira. Digitalizacijom dokument prelazi iz papirnatog nosača u digitalni oblik i na taj način može izgubiti izvorni redoslijed. Kako se to ne bi dogodilo poveznica dokumenta s dokumentacijskom cjelinom mora ostati očuvana, a time i izvorni redoslijed radi kasnijih potreba dokazivanja autentičnosti. Pored metapodataka koji nastaju tijekom životnog procesa dokumenta prije digitalizacije potrebno je dodati nove metapodatke koji dodatno opisuju

digitaliziranu kopiju dokumenta. Također, digitalizacijom se gube određeni podaci, vanjske oznake dokumenata, koji su prisutni u izvornom obliku. Zbog svega navedenog za ispravno tumačenje digitalizirane kopije, odnosno kopije u obliku originala, potrebno je svakoj slici pridružiti određene metapodatke. Na taj način digitalizirana kopija i pripadajući metapodaci postaju jedna cjelina kao što se vidi na slici 25.



Slika 22. Digitalizirana kopija

Kada je digitalizirana slika napravljena prema zahtjevima za glavnu digitaliziranu sliku (master op.a.) i kada su prisutni navedeni pripadajući metapodaci tada je riječ o **kopiji u obliku originala**.

10.5. Proces digitalizacije

Proces digitalizacije treba zadovoljiti zahtjev autentičnosti kojim se traži da je proces propisan, nadziran i provjeravan. Predloženi proces digitalizacije ima za cilj omogućiti prikupljanje dovoljne količine podataka kojima se dokazuje autentičnost digitalizirane slike u bilo kojem trenutku u vremenu.

10.5.1. Testni uzorak

Analizom gradiva koje je odabrano za digitalizaciju izrađuje se testni uzorak koji može zadovoljavajuće predstavljati ukupno gradivo koje se namjerava skenirati. Nakon analize gradivo se priprema u paket za skeniranje. Podešavaju se aplikacija za izradu vodećeg dokumenta, softver za prihvat slike, aplikacija za automatsku kontrolu slike, aplikacija za indeksiranje i aplikacija za kontrolu digitaliziranih glavnih slika i pripadnih metapodataka.

Uspješno provođenje digitalizacije i isporuka u repozitorij za pohranu glavnih slika i pripadajućih metapodataka daje dovoljno elemenata kako bi se izradile upute, i ovjerile te započeo rad. Ovaj cjelokupni korak odabira testnog uzorka, opravdanosti za takav odabir i

provođenje digitalizacije, treba biti evidentiran i zapisan te čuvan tijekom cijelog perioda čuvanja dokumenata na koje se testni uzorak odnosi.

Upute sadrže informacije o pripremi gradiva, skeniranju gradiva, slanju gradiva u repozitorij dokumentacijskih cjelina, automatskoj kontroli skeniranog gradiva, indeksiranju odnosno dodatnom pridruživanju metapodataka, kontroli pridruženih metapodataka te isporuci pridruženih metapodataka i digitaliziranog gradiva.

10.5.2. Priprema

Proces pripreme se obavlja na način opisan u poglavlju Proces digitalizacije stvaranjem paketa dokumentacije. Prilikom izrade paketa potrebno je voditi računa o pripadnim dodacima dokumentima, ukoliko postoje, kao što su post-it-i ili drugi povezani dokumenti te pravilno im označiti poveznicu s dokumentom na koji se odnose. Paketi mogu biti cjeline koje su i fizičke cjeline kao na primjeru digitalizacije HUB obrazaca gdje paket čini cjelina na mjestu unosa. Operater zadužen za pripremu paketa ili njegov koordinator prijavljuje se u sustav kako bi ispisao vodeći dokument paketa. Prijava se obavlja korištenjem dodijeljenih korisničkih podataka. Sustav evidentira prijavu: ime i prezime, datum, vrijeme prijave i podaci o izradi vodećeg dokumenta.

Unose se slijedeći podaci:

1. naziv paketa,
2. datum pripreme paketa,
3. vrijeme početka pripreme paketa,
4. vrijeme završetka pripreme paketa.

Sustav ispisuje vodeći dokument koji sadrži barkod s podacima:

1. naziv paketa,
2. datum pripreme paketa,
3. vrijeme početka pripreme paketa,
4. vrijeme završetka pripreme paketa,
5. ime i prezime operatera,
6. mjesto za potpis operatera.

Barkod koji se generira sadrži slijedeće podatke i oni su jedinstvena oznaka svakog paketa:

1. naziv,
2. datum pripreme paketa,

3. vrijeme početka pripreme paketa,
4. vrijeme završetka pripreme paketa,
5. ime i prezime operatera.

Nakon ispisa operater se potpisuje i potpisani vodeći dokument stavlja na početak pripremljenog paketa. Vodeći dokument ostaje s paketom sve do uništavanja fizičke dokumentacije. Potpisani vodeći dokument služi radi pokazivanja autentičnosti procesa pripreme. Vodeći dokumenti čine cjelinu digitaliziranog paketa i pohranjuju se zajedno s glavnim slikama digitaliziranog paketa.

10.5.3. Skeniranje

Na skeniranju obaveza operatera je provjeriti potpis, ukoliko ga nema vraća paket na pripremu. Operater na skeniranju se prijavljuje putem svojih korisničkih podataka u računalo. Nakon prijave u računalo operater se prijavljuje, koristeći korisničke podatke, u aplikaciju za skeniranje te odabire vrstu posla u kojoj je unaprijed kreiran posao za skeniranje primljenog paketa.

Postavke posla trebaju biti evidentirane u uputama, a u skenerskom programu definira ih koordinator skeniranja. Skenerski program treba biti podešen na način da čita barkod vodećeg dokumenta i automatski unosi podatke o paketu sustav. Također mora omogućiti stvaranje dvije slike: glavnu i izvedenu sliku.

Glavna slika treba imati postavke ovisno o rezultatima provedenog testiranja i analize dokumentacije. To može biti 24-bitna slika u boji ili 8-bitna slika u sivoj skali, bez kompresija. Izvedena slika može biti bitonalna s G4 kompresijom i svim potrebnim poboljšanjima. Glavna slika se obavezno izrađuje obostrano. Izvedena slika može biti bez praznih stranica radi uštede diskovnog prostora.

Skenerski program naprednim digitalnim potpisom (ovo je aplikativni napredni digitalni potpis, op.a.) potpisuje digitaliziranu sliku te ju šalje u sustav. Također, podatke pročitane s barkoda vodećeg dokumenta skenerski program šalje u sustav.

Podaci koji nastaju tijekom skeniranja su:

1. podaci s barkoda vodećeg dokumenta,
2. ime i prezime operatera na skeniranju,
3. datum skeniranja paketa,
4. vrijeme početka skeniranja paketa,
5. vrijeme završetka skeniranja paketa,

6. naziv posla,
7. postavke posla.

10.5.4. Kontrola glavne slike

Kontrolu glavne slike provodi operater tijekom skeniranja prije slanja u središnji repozitorij. Operater tijekom skeniranja promatra ponašanje procesa digitalizacije kroz funkciju praćenja koju omogućava program za prihvat slike. Ukoliko uoči razne anomalije, kao na primjer crte na dokumentu, može zaustaviti skeniranje i ukloniti razlog pojavljivanja anomalija čišćenjem skenera ili obavijestiti nadležnog koordinatora ako samostalno nije u mogućnosti ukloniti nepravilnost, te ponoviti skeniranje.

Ovdje je važno primijetiti kako tijekom ovakve provjere nije moguće uočiti postojanje malih detalja kao što su to, na primjer, potpis ili detalji koji se nalaze na rubu dokumenta jer se ne vidi originalni dokument s kojim bi se vršila usporedba. Međutim, operater koji sumnja u nedostatak detalja na slici može provjeriti sliku s fizičkim papirom vodeći računa o zadržavanju redoslijeda dokumenata u paketu. Drugi način je napraviti provjeru izdvajanjem određenog nasumičnog podskupa dokumenata i vizualnom usporedbom izvornika s digitaliziranom kopijom, međutim ovakav korak može biti zahtjevan i uvijek postoji mogućnost da kritični dokument ne bude provjeren.

Ukoliko se skeniranjem stvara digitalizirana kopija u boji moguće je da, zbog slabljenja lampe ili drugih anomalija u samom procesu, dođe do promjene u tumačenju frekvencije boje, pa će boja biti različita od one koja je na papiru (za točnost pregleda frekvencije boje potrebno je kalibrirati monitor na kojem se slika prikazuje ili napraviti ispis na pisaču u boji i usporediti boje, op.a.).

10.5.5. Slanje u repozitorij dokumentacijskih cjelina

Slanje u središnji repozitorij uključuje komunikaciju između softvera za prihvat slike i sustava koji prihvaća datoteke u repozitorij dokumentacijskih cjelina.

Sustav za prihvat datoteka u središnji repozitorij prihvaća poslane datoteke, provjerava digitalni potpis, evidentira rezultat provjere, podatke o digitalnom certifikatu i podatke o hash rezultatu. Digitalizirane slike sustav sprema na medij koji onemogućava brisanje ili promjenu odnosno koji dopušta samo dodavanje podataka. Primljene metapodatke sustav sprema u bazu podataka koja onemogućava brisanje ili promjenu.

Sve primljene digitalizirane slike mogu u sustavu postati nova verzija a prethodna verzija se mora sačuvati. Isto tako, primljeni metapodatak može samo dobiti status nove verzije, ali se stari metapodatak ne smije obrisati, i baš kao što arhivistički princip nalaže da se sve greške u vođenju dokumentacije precrtavaju, a ispravci dodaju u novi redak.

Digitalizirana slika i pripadajući metapodaci se čuvaju ovisno o roku čuvanja. Vodeći dokument paketa se također čuva koliko i digitalizirana slika koja se nalazila u tom paketu. Dokumenti se trebaju spremiti tako da se očuva poredak koji su dokumenti imali u fizičkom obliku unutar paketa. Ovo se može postići tako da svaka slika unutar svog imena ima i rastući redoslijed brojeva, te tako da svaka dokumentacijska cjelina bude jedna mapa na disku.

10.5.6. Indeksiranje i pridruživanje metapodataka

Faza indeksiranja označava trenutak prilikom kojeg se prepisuju traženi ili željeni podaci s dokumenta koji služe za označavanje dokumenta ali i za brzi pronalazak. Na primjer, kada je potrebno brzo pronaći neku primljenu fakturu može se to postići ukoliko se u aplikaciju za pretragu unesu podaci o datumu fakture, datumu primljene fakture, nazivu pošiljatelja fakture ili njegov OIB i iznosu fakture.

Podaci koji se prepisuju s dokumenta ovise o samom dokumentu i definirani su tijekom faze analize dokumentacije i testiranja procesa digitalizacije. Moguće je prilikom upisivanja napraviti određene kontrole koje mogu kasnije pomoći. Na primjer, ako se prepisuje datum tada polje u koje se datum upisuje treba omogućiti jedino upisivanje formata datuma. Isto tako se može osigurati da metapodatak mora biti popunjen. Moguće je napraviti listu naziva za određeni metapodatak ili koristiti rječnik.

Prilikom digitalizacije velike količine dokumentacije može se dogoditi da određenog metapodataka nema jer je specifičan samo za određeni dokument. Tako je na primjer iznos važan metapodatak za fakturu, ali nije važan i ne mora biti prisutan na dokumentu koji je specifikacija poslane fakture.

Tijekom faze indeksiranja radi se druga vizualna kontrola digitalizirane slike. Tom prilikom se uočava je li moguće sve metapodatke prepisati odnosno ispravno tumačiti. Ukoliko to nije moguće digitalizirana slika dobiva status „ponoviti“.

Moguće je da određenog podatka nema. Na primjer faktura nema iznos jer se nalazi na idućoj stranici. U tom slučaju može postojati dogovor da se takav slučaj označi s „0“ ukoliko se radi o numeričkom podatku, odnosno s „X“ ukoliko se radi o tekstualnom podatku.

Svaku digitaliziranu sliku moguće je obraditi pomoću algoritma za prepoznavanje znakova, odnosno OCR-om. Rezultati se zapisuju u bazu podataka koja onemogućava brisanje ili mijenjanje. Tijekom faze indeksiranja radi se provjera prepoznatih znakova budući da je poznato kako točnost OCR-a nije potpuna odnosno nije 100%-tna.

Upisivanje metapodataka se može dodatno ograničiti na upisivanje prethodno definiranog rječnika ili liste pojmova. Ili se može napraviti dvostruko indeksiranje na način da jedan operater u jednom prolazu indeksira jedan paket, a u drugom prolazu indeksiranja istog paketa indeksiranje obavlja drugi operater. Ovakvo dvostruko indeksiranje treba biti pažljivo izvedeno kroz aplikaciju za indeksiranje koja tada vodi računa da paket koji dodjeljuje operateru na indeksiranje nije paket koji je taj operater prethodno indeksirao.

10.5.7. Kontrola pridruženih metapodataka i digitaliziranih slika

Kontrolu pridruženih metapodataka moguće je napraviti korištenjem određenih upita koji mogu provjeriti unose „0“ ili „X“, unos inicijalno definiranih datuma kao na primjer „1.1.1900“ koji se automatski upisuje kada ovaj podatak ne postoji na dokumentu pa ga nije moguće upisati.

U ovoj fazi obavezna je provjera broja skeniranih stranica. Provjerava se nalazi li se u svakoj datoteci dvije slike te ima li cjelokupni dokument onoliko stranica koliko je evidentirano u fazi sređivanja gradiva. Provjera se može raditi na većem obimu dokumentacije ne samo na jednom paketu, što značajno ubrzava ovaj korak. Nesukladnosti se trebaju evidentirati. Na primjer, može se dogoditi da je tijekom faze indeksiranja pogrešno označen dokument, odnosno pripisani su mu metapodaci prethodnog dokumenta i na taj način je prethodni dokument dobio više stranica nego je prepoznato tijekom faze sređivanja gradiva.

Za dokumentaciju koja je sređena, postoji podatak o stvaratelju, postoji popis dokumenata u tehničkoj jedinici, popis dokumenata koji nedostaju, broj stranica, broj praznih stranica i redoslijed nastajanja, obavezno se provjeravaju ovi podaci i izrađuje se tablica usporedbe koji daju odgovore na pitanje jesu li svi dokumenti prisutni i koji dokumenti nedostaju među skeniranom dokumentacijom. Sve razlike se trebaju provjeriti te razriješiti prije slanja u sustav za dugoročno očuvanje glavne slike.

Osjetljiva dokumentacija koja ima kritične detalje mora biti pregledana vizualno i uspoređeni s izvornim dokumentima. Ovakvu kontrolu najlakše je izvesti ukoliko je za dokumente poznat podatak o postojanju takvih malih detalja ili kritičnih detalja. Zato je važan

korak sređivanja gradiva. Podaci iz koraka sređivanja gradiva mogu se programski koristiti kako bi se izdvojili kritični dokumenti koji se tada vizualno pregledavaju.

Dokumentacija koja je kritična, čijim uništavanjem može doći do velikog materijalnog gubitka, mora biti cjelokupno provjerena, sve glavne slike i svi izvornici trebaju biti provjereni.

Rezultati kontrole se upisuju u revizijski dnevnik iz kojeg je potrebno vidjeti kako su sve digitalizirane kopije prekontrolirane.

10.5.8. Ponavljanje skeniranja

Svi dokumenti koji su u prethodnim fazama dobili status "ponoviti" kroz funkcionalnosti aplikacije za kontrolu javljaju se operateru na skeneru koji ponavlja digitalizaciju vodeći računa o ispravnom imenovanju datoteke koja dobiva novu verziju u sustavu.

10.5.9. Isporuka digitaliziranih dokumentacijskih cjelina

Uredno provedena kontrola vodi do dodjeljivanja statusa za daljnje postupanje, na primjer status „OK", za dokumentacijske cjeline. Sada slijedi faza u kojoj se metapodaci i digitalizirane slike mogu proslijediti na daljnje korištenje.

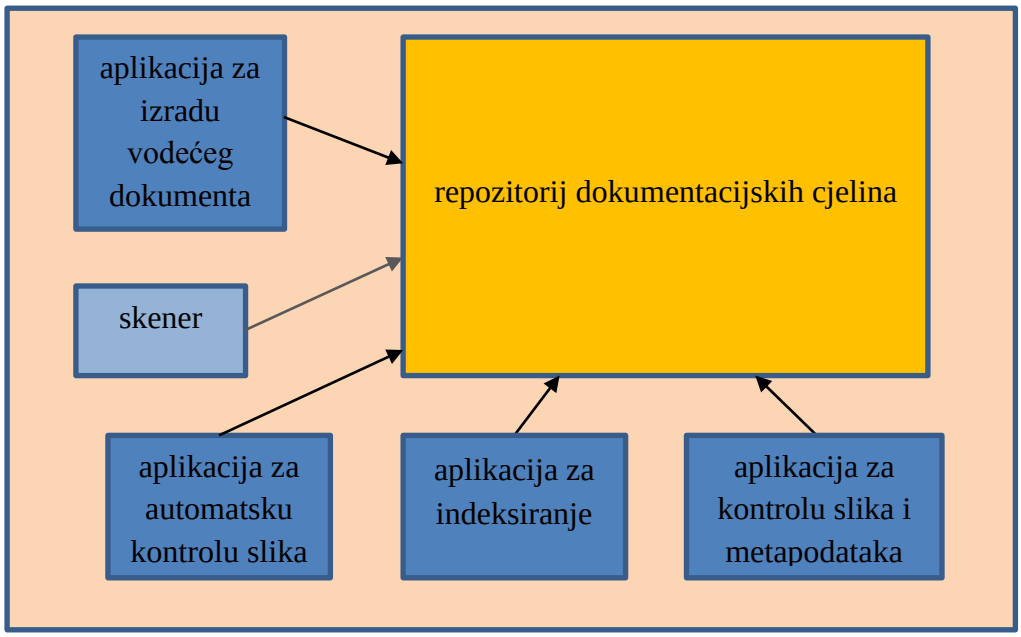
Prvi korak je slanje odobrenih paketa i svih metapodataka na repozitorij za dugoročnu pohranu. Paket u kojem su sve glavne slike dobile status „OK" i za koje su metapodaci dobili status „OK" šalju se na sustav za dugoročno očuvanje glavne slike koji dopušta samo pregled ali onemogućava brisanje ili promjenu. Za ove pakete potrebno je izraditi sigurnosnu kopiju.

Nakon toga iz glavnih slika mogu se napraviti izvedene kopije (rječnikom projekta InterPARES – imitirajuće kopije). Izvedene kopije se mogu izraditi tako da se obrišu prazne stranice i pridruže preostale pripadajuće stranice i izradi jedna datoteka za jedan dokument. Ovo pridruživanje treba biti strogo propisano i provedeno kako ne bi došlo do gubitka podataka.

Obrađene izvedene kopije i pridruženi metapodaci se šalju dalje u sustav kojim je svrha omogućavanje pretraživanja, pregleda i analiziranja gradiva, odnosno upravljanja gradivom kao što je na primjer RMS sustav.

10.6. Zatvoreni sustav digitalizacije

Zatvoreni sustav digitalizacije je sustav koji se sastoji od skenera i pripadnih programa za skeniranje, repozitorija za prihvat slika, baze podataka za prihvat metapodataka, aplikacije za kontrolu slika, indeksiranja (pridruživanje dodatnih metapodataka), kontrolu pridruženih metapodataka i kontrolu slika, te funkcionalnosti isporuke digitalizirane dokumentacijske cjeline u sustav za dugoročnu pohranu i sustav za pretraživanje i pregled dokumentacije (slika 26).



Slika 23. Zatvoreni sustav digitalizacije

Skener u repozitorij glavnih i izvedenih slika i metapodataka šalje digitalno potpisanu glavnu sliku i izvedenu sliku i pripadajuće metapodatke. Repozitoriju pristupaju aplikacije za izradu vodećeg dokumenta, kontrolu slika, indeksiranja i kontrolu slika i metapodataka u koje se prijavljuju operateri s korisničkim imenom i prezimenom. Sve akcije koje operateri obavljaju upisuju se u metapodatke slike na koju se akcije odnose.

10.7. Izrada uputa

Prethodno navedeni koraci procesa digitalizacije trebaju biti propisani uputom. U uputi se nalaze i svi zahtjevi za glavnom slikom i postavke softvera za prihvat slike i pokretačkog programa. Osoba koja izrađuje uputu i vodi brigu oko cjelokupne digitalizacije odabrane dokumentacije potpisuje uputu. Ista osoba nadzire provođenje testiranja na odabranom testnom uzorku te zapisuje sve podatke oko provedenog testiranja. Izrađenu uputu

je potrebno prekontrolirati i potpisati od strane nezavisne osobe koja uspoređuje podatke provedenog testiranja. Na kraju uputu potpisuje osoba koja odobrava cijeli proces.

Svaka promjena u procesu i sustavu digitalizacije se evidentira u novoj verziji dokumenta. Sve verzije dokumenta se čuvaju dok god se čuva digitalizirana slika na koju se odnosi taj dokument.

10.8. Podijeljenost uloga i odgovornosti u sustavu digitalizacije

U sustavu digitalizacije mogu se prepoznati i odijeliti određene uloge kako bi se podržao kontinuitet procesa koji osigurava autentičnost digitalnih kopija u obliku originala tijekom digitalizacije. Uloge se mogu podijeliti na procesne uloge, organizacijske uloge, nadzorne uloge, kontrolne uloge i uloge održavanja.

U procesne uloge ubrajaju se operateri na pripremi, skeniranju i indeksiranju. Organizacijske uloge su uloge za izradu uputa, kontrole izrađenih uputa i odobrenja uputa za početak obavljanja procesa. Nadzorne uloge su uloge koje uključuju koordinatore operatera na pripremi, skeniranju i indeksiranju. Kontrolne uloge uključuju ulogu koordinatora operatera na pripremi, skeniranju i indeksiranju, ulogu kontrole procesa i ulogu kontrole slika i metapodataka. Uloge održavanja se odnose na servisera skenera, programera pomoćnih aplikacija za izradu vodećeg dokumenta, indeksiranje i kontrolu, te uloga održavanja računala, računalne mreže, baza podataka i izrade pričuvnih kopija.

Za uspješno očuvanje autentičnosti dokumenata tijekom digitalizacijskog procesa masovne digitalizacije važno je da su odgovornosti za ove uloge podijeljene bez preklapanja. Operateri su podijeljeni na operatere na pripremi, skeniranju i indeksiranju. Operater na pripremi predaje pripremljenu dokumentaciju operateru na skeniranju. Tijekom skeniranja operater obavlja kontrolu pripreme što znači kako operater na skeniranju provjerava postojanje obaveznih podataka na vodećem dokumentu koje priprema prilaže uz svaki paket. Operater na indeksiranju ima obavezu obaviti vizualnu kontrolu digitalizirane slike te neodgovarajuće slike označiti oznakom „ponoviti“.

Koordinator operatera na pripremi obavlja kontrolu dnevnog provođenja postupka pripreme, izrađuje vodeće dokumente i izvještava na tjednom nivou o obavljenoj pripremi. Koordinator operatera na skeniranju obavlja kontrolu dnevnog provođenja postupka skeniranja i izvještava na tjednom nivou o obavljenom skeniranju. Koordinator operatera na indeksiranju obavlja dnevnu kontrolu provođenja postupka indeksiranja i izvještava na tjednom nivou o obavljenom indeksiranju. Koordinatori na kraju radnog vremena vode

evidenciju utrošenog vremena i obavljenog posla svakog operatera, i jednom tjedno izvještavaju osobu odgovornu za provođenje procesa.

Kontrolor slika i metapodataka provjerava digitalizirane slike i upisane metapodatke pomoću pripremljenih alata, na primjer algoritam za stvaranje OIB-a se može koristiti za provjeru točnog unosa a sve razlike trebaju se dodatno usporediti s informacijom koja se nalazi na slici, označava sva ponavljanja koja je potrebno izvršiti te obavještava koordinatore o potrebi obavljanja ponavljanja i dodjeljuje statuse „OK“ za uredno obavljen postupak digitalizacije.

Na mjesečnom nivou svi izvještaji se skupljaju u jedinstveni dokument koji priprema osoba koja je odgovorna za provođenje procesa što je najčešće osoba koja je provela testiranje i izradila upute. Dva puta godišnje, ili bar dva puta u toku perioda digitalizacije odabrane dokumentacije, nadzorno tijelo provodi nadzor cijelog sustava, pri čemu provjerava sve izvještaje, rezultat testiranja uzorka dokumentacije te urednost provođenja procesa, odijeljenost uloga i educiranost djelatnika. Svi djelatnici trebaju biti adekvatno educirani, a to uključuje edukaciju u spisovodstvenim procedurama, edukaciju za rad s računalom i rad sa skenerom, te druge specifične edukacije. Edukaciju je potrebno provesti prije početka digitalizacije ali i prilikom svake promjene. Potrebno je voditi dnevnik o provedenim edukacijama. Rezultat nadzora ispisuje u izvještaju za upravu organizacije. Ovdje treba biti uključena i kontrola rada aplikacija za izradu vodećeg dokumenta, kontrolu, i indeksiranje.

Dnevnu kontrolu rada skenera i održavanje obavlja operater na skeneru pri čemu uočava nepravilnosti u radu te održava skener prema uputi proizvođača, na primjer usisava prašinu ili briše staklo koje čuva lampu i senzor. Kontrola skenera se obavezno obavlja jednom mjesečno a može i češće ovisno o preporuci proizvođača i od strane nezavisnog stručnog servisera ovlaštenog od strane proizvođača. Tom prilikom se radi kalibracija skenera, a obavezno se vodi evidencija o stanju lampe i kalibracije uređaja kao i evidencija svih zamijenjenih dijelova.

Sve pomoćne aplikacije izrađuje programer prema uputama osobe koja je odgovorna za obavljanje procesa. Zahtjevi za aplikacije trebaju biti evidentirani. Nakon izrađenih aplikacija potrebno je provesti testiranje i rezultate testiranja rada aplikacija evidentirati skupa s aplikacijskim kodovima.

Održavanje informacijske infrastrukture koja uključuje računala, računalne mreže, baze podataka i izradu pričuvnih kopija treba biti propisano i provođeno u skladu s preporukama proizvođača, a provode ih osobe zadužene za njihovo održavanje i serviseri. Ugradnja i održavanje informacijske strukture treba biti evidentirano i propisano zasebnim

dokumentom. Evidencije o kontroli i nadzoru informacijske infrastrukture trebaju biti dostupni na zahtjev.

Izradu uputa prethodi testiranje provedeno na reprezentativnom uzorku. U obavljanje testiranja trebaju biti uključeni operateri, koordinatori, kontrolori slika i metapodataka i osoba odgovorna za provođenje digitalizacije. Izrađene upute se provjeravaju u dvije instance kod kontrolora upute i kod osobe koja je odgovorna za odobravanje uputa. U svakom slučaju se prilažu podaci o analizi dokumentacije i provedenom testu na testnom uzorku.

10.9. Karakteristike skenera

Ukoliko skener ima 600 senzora po inču u glavi skenera, kao što je slučaj sa skenerima koji velikim brzinama obrađuju velike pakete dokumenata o čemu je bilo govora u poglavlju o pravoj rezoluciji, a postavke profila za skeniranje traži izradu digitalizirane slike od 400 dpi-a, tada softver za prihvat slike radi ekstrapolaciju, o čemu je bilo govora u cjelini o komponentama digitalizacije. Tom prilikom potrebno je koristiti metodu koja očitanu liniju dokumenta kao cijeli skup podataka prima u punoj rezoluciji te rezultat smanjuje u memoriji skenera jer daje precizniji rezultat, ovo se zove *global shutter efekt*. Ukoliko skener ima manje od 600 senzora po inču u glavi skenera tada za izradu slike od 600 dpi radi dodavanje točaka koje nije pročitao, metodom interpolacije. O ovome je već bilo spomena u poglavlju o senzorima u digitalizaciji.

Koji senzor koristiti ovisi o tehnologiji koja daje bolje rezultate. Korištenje PMT senzora je najbolje, međutim za potrebe masovne digitalizacije može biti vrlo nepraktično. Od ostalih senzora najbolje rezultate daje CCD senzor zbog veće dubine polja od ostalih senzora. Zbog osjetljivosti na vibracije i mehaničke udarce ove tehnologije potrebno je provesti test rada skenera od strane ovlaštenog servisera nakon instalacije uređaja na mjesto gdje će se digitalizacija obavljati. Ova tematika je detaljnije objašnjena u poglavlju o vrstama senzora.

Izvor svjetlosti treba biti odgovarajući. Kako bi se ispravno prikazale sve boje treba koristiti bijelu svjetlost jer ona prema fizikalnim zakonima sadrži sve valne duljine ili sve boje. Više o tome vidjeti u poglavlju o izvoru svjetlosti prilikom rada senzora.

Optički dio procesa usmjerava reflektiranu svjetlost prema senzoru i trebao bi biti takve kvalitete koja minimalno iskrivljuje sliku, na primjer izrađena od stakla ili korištenjem prizme koja raspršuje bijelu svjetlost na različite boje što daje puno bolje rezultate. Više o tome vidjeti u poglavlju o izvoru svjetlosti.

Tijekom pretvaranja svjetlosti u elektronički signal dolazi do različitih električkih smetnji kao što je utjecaj magnetskih i električkih polja, zato je potrebno osigurati dodatnu zaštitu na ove utjecaje. Poglavlje o izvoru svjetlosti sadrži više o ovome.

Tijekom skeniranja dolazi do zagrijavanja cijelog sustava što može dovesti do promjene mehaničkih dijelova sustava, zato je važno da se oni dijelovi na kojima se nalazi optika i drugi osjetljivi dijelovi nalaze na materijalu koji nije podložan takvim utjecajima, kao što je na primjer metal. Više o tome vidjeti u poglavlju o pravoj rezoluciji.

Ukratko, na temelju istražene literature i analiziranih primjera iz prakse, zaključujem i preporučam da:

1. glava skenera treba imati minimalno 600 senzora po inču,
2. senzor treba učitati cijelu liniju u memoriju odjednom,
3. senzor treba raditi ekstrapolaciju točaka,
4. senzor je minimalno tipa CCD,
5. izvor svjetlosti treba biti bijela svjetlost,
6. optički dio treba biti napravljen od stakla,
7. treba biti provedena zaštita od magnetskih i električkih polja,
8. mehanički dijelovi sustava trebaju biti napravljeni od materijala koji nisu osjetljivi na zagrijavanje.

10.10. Karakteristike pokretačkog programa i softvera za prihvat slike

Između senzora i softvera za prihvat slike postoji pokretački program koji može biti TWAIN ili ISIS o čemu sam pisao u dijelu o pokretačkim programima. Pokretački program se ne bi smio mijenjati neovlašteno te je u ovom slučaju bolje koristiti ISIS program koji garantira istu funkcionalnost na svim uređajima koji ga koriste zbog toga što njega definira proizvođač. ISIS rješenje je bolje jer korisnik može od proizvođača tražiti dodatne ili drugačije funkcionalnosti međutim njih može izmijeniti samo proizvođač, što je za osiguranje autentičnosti važna kvaliteta.

Mogućnosti koje korištena verzija ISIS programa omogućava treba biti evidentirana i primljena od strane proizvođača. Mogućnosti programa trebaju biti takve da nije moguće na glavnoj slici obavljati funkcije koje dovode do gubitka pročitanih točaka. Ovo potvrđuju dokumenti ISO/TR 15801:2009, ISO/TR 13028:2010 te tehnički standard Kongresne knjižnice D.C. i Vlade Alberte.

Prilikom definiranja funkcionalnosti ISIS programa potrebno je omogućiti izradu glavne slike prema zahtjevima za glavnu sliku i izradu izvedene slike koja može koristiti sve mogućnosti.

U prethodnim poglavljima o normama, tehničkim izvještajima i primjerima dobre prakse Kongresne knjižnice Washington D.C.-a i Vlade Alberte bilo je riječi o različitim zahtjevima i karakteristikama softvera za prihvat slike. Slažu se kako se ne smiju koristiti tehnike poboljšanja slike koje vode do gubitaka podataka kao na primjer: brisanje pozadinskih točaka, brisanje crnih rubova, brisanje formi, oštrenje slike, izrezivanje dijelova sjena, zamućivanje, uklanjanje mrlja, rezanje slike ni uklanjanje forme. Dopušta se obavljanje funkcije poravnanja slike, a može se raditi dodavanje crnog ruba kako bi se označio kraj dokumenta i pokazalo da je cijeli dokument snimljen. Dodavanjem ruba se gubi prava veličina dokumenta.

Tehnički izvještaj ISO/TR 15801:2009 i ISO/TR 13028:2010 predlažu izradu glavne kopije i izvedene kopije glavne kopije za korištenje u druge svrhe. Pri tome u nazivu datoteke, prema tehničkom izvještaju ISO/TR 15801:2009, treba biti jedinstveni broj koji je stvoren sistemski i izrađen je i zapisan hash rezultat glavne slike. Dodatno predlažu glavne slike spremati u mape koje predstavljaju skenirane pakete kako bi na taj način zadržali sljedivost. U slučaju ponavljanja skeniranja mora biti zapisan razlog ukoliko je zatraženo ponavljanje iz faze kontrole slike i metapodataka, a u slučaju da je operater primijetio lošu kopiju ili povlačenje dva dokumenta softver za skeniranje bilježi ponavljanje. Izrada izvedenih kopija glavne slike, prema ISO/TR 13028:2010 treba dobiti novi broj kao novu verziju datoteke.

Softver za prihvat slike treba zapisati podatke o broju skeniranih slika na nivou paketa, prema tehničkom izvještaju ISO/TR 13028:2010.

U tablici se nalaze neke funkcije poboljšanja slike koje može koristiti softver za prihvat slike s opisom što poboljšanje čini te informacijom uklanja li podatke ili ne (tablica 8).

Tablica 8. Funkcije poboljšanja slike i učinak

funkcija poboljšanja slike (filtar)	**opis**	**uklanja podatke**
Barcode Detection	Prepoznaje i očitava barkodove.	Ne
Black Overscan Removal	Briše crnu pozadinu koju stvara skener kada nema točan podatak o dimenziji izvornika.	Da
Blank Page Removal	Prepoznaje i briše prazne stranice.	Da
Border Removal	Uklanja crni rub pretvarajući ga u bijelu pozadinu stvarajući veću marginu na dobivenoj slici.	Da

funkcija poboljšanja slike (filtar)	opis	uklanja podatke
Color Content	Prepoznaje količinu boje na dokumentu. Ovisno o tom podatku softver automatski odlučuje o stvaranju slike u boji ili u crno-bijelo.	Ne
Color Dropout	Uklanja zadanu boju sa 24-bitne slike.	Da
Crop	Obrezuje margine.	Da
Deskew	Ispravlja nakrivljene slike.	Ne
Digital Stamp	Automatski dodaje tekstualnu zabilješku slici.	Da
Dilation	Povećava crna područja objekta na slici, na primjer povećava rub slova.	Da
Erosion	Obrnuto od filtra *dilatation*. Smanjuje crna područja objekta na slici.	Da
Halftone Removal	Uklanja odsjaj ili šum koji je nastao skeniranjem poboljšavajući čitkost slike.	Da
Hole Removal	Uklanja objekte koji izgledaju kao crna rupa na lijevoj margini.	Da
Invert Image	Radi inverziju crnih u bijele točke.	Da
Line Removal	Uklanja linije na slici.	Da
Noise Removal	Uklanja točkice sa slike koje mogu nastati zbog ostatka ugljena ili prljavštine na izvorniku i skeneru.	Da
Patchcode Detection	Prepoznaje i očitava *patchcode* dokumente.	Ne
Rotation	Obavlja rotaciju slike za 90 stupnjeva.	Ne
Scaling	Proporcionalno povećava sliku zadržavajući proporciju svih elemenata na slici.	Da
Skeleton	Uklanja točke sa svih rubova znakova.	Da
Smoothing	Dodaje i uklanja crne točke na rubovima objekata čineći ih ravnim i čitljivijim.	Da
Threshold	Ovisno o zadanom pragu ispravlja boju, na primjer veći broj praga potamniti će dokument, dok manji broj praga osvjetljuje dokument.	Da

Ukratko, na temelju istražene literature i analiziranih primjera iz prakse, zaključujem i preporučam da:

1. pokretački program treba biti tvornički podešen za izradu glavne slike,
2. pokretački program treba imati unaprijed ograničene mogućnosti za izradu glavne slike i sve mogućnosti za izradu izvedene slike,
3. postavke trebaju biti propisane od strane proizvođača i evidentirane od strane proizvođača,
4. softver za prihvat glavne slike ne smije koristi tehnike poboljšanja koji vode do gubitka podataka,
5. softver za prihvat izvedene slike smije koristi sve tehnike poboljšanja slike,

6. softver za prihvat treba sistemski dodjeljivati jedinstveni broj svakoj slici,
7. softver za prihvat treba izrađivati hash rezultat glavne slike,
8. softver za prihvat treba omogućiti spremanje glavnih slika u mapu koja predstavlja skenirani paket,
9. softver za prihvat, prilikom ponavljanja skeniranja, treba zapisivati razlog ponavljanja,
10. softver za prihvat, prilikom izrade izvedene slike, treba izvedenoj slici dodijeliti oznaku u obliku nove verzije datoteke,
11. softver za prihvat treba zapisati broj skeniranih slika na nivou paketa.

10.11. Karakteristike glavne slike

Vlada Alberte i Kongresna knjižnica Washington D.C. predlažu izradu PDF, PDF/A ili TIFF datoteke s kompresijom bez gubitaka, osim u slučaju kada se izrađuje bitonalna TIFF datoteka tada je dopuštena G4 kompresija. Prilikom izrade PDF datoteke moguće je postavljanje slojeva na vrijednost 0 jer nema drugih slojeva, prema dokumentaciji Vlade Alberte.

Standardi Vlade Alberte i Kongresne knjižnice Washington D.C. ovisno o dokumentu daju smjernice za tonalnost. Tako crno-bijeli dokument može biti bitonalan, dokument u boji treba biti u boji, 24-bita, crno-bijela fotografija može biti u sivoj skali, 8-bita, fotografija u boji može biti u boji 24-bita. Ovdje je dobro primijetiti kako se među paketom dokumentacije mogu nalaziti dokumenti koji su različiti, na primjer dokumenti koji u boji imaju grafikone a tekst u crnom tisku na bijelom papiru. Tada bi trebalo skenirati u boji.

Rezolucija dobivene slike treba biti minimalno 400 dpi zbog potrebe obavljanja OCR algoritma koji automatski prepoznaje indeksne podatke, odnosno provjerava dobro obavljeno pretvaranje fizičkog originala u digitaliziranu kopiju, ali samo za znakove kao što su brojevi, slova, interpunkcijski znakovi. Međutim, OCR ne može dati informaciju o postojanju potpisa, pečata ili slike. Ukoliko na dokumentu postoje znakovi čija je veličina fonta manja od 6 potrebno je koristiti 600 dpi-a. O tome je bilo riječi u poglavlju o količini dpi prilikom skeniranja, senzori u digitalizaciji, kongresna knjižnica Washington D.C.

Glavna slika treba biti napravljena u formatu u boji sa 24 bita, kao što proizlazi iz poglavlja o dubini boje.

Veći broj tonske dinamike daje bolju sliku. Na primjer, tonska dinamika veća od 3,5 je prihvatljiva. Više o tome se nalazi u poglavlju tonske dinamike.

Glavna slika treba biti obostrano skenirana kako bi se vidjelo sadrži li druga strana podatke ili ne. Za izvedenu sliku druga strana koja je prazna nije važna, međutim za pokazivanje potpunosti treba postojati druga strana svakog papira svakog dokumenta koji se skenira.

EXIF standard govori o mogućnosti koje se mogu ugraditi u samu TIFF datoteku. U tablici 9 nalazi se popis izdvojenih oznaka, njihovi nazivi i kratki opisi. Popunjavanje tih oznaka može pomoći prilikom utvrđivanja autentičnosti glavne slike. Na primjer, u oznaku 270 se može upisati redni broj slike i jedinstveni broj paketa u kojem je bio prilikom digitalizacije. Ostali podaci iz Tablice 9 potvrđuju da je proces skeniranja proveden prema propisanim uputama.

Tablica 9. Izvadak iz EXIF standarda

broj	naziv	kratak opis
256	ImageWidth	Broj stupaca u slici, tj. broj točaka u retku.
257	ImageLength	Broj redaka u slici, tj. broj točaka u stupcu.
258	BitsPerSample	Broj bitova po komponenti.
259	Compression	Kompresijska shema koja je korištena na podacima slike.
270	ImageDescription	Niz podataka koji opisuje predmet na slici.
271	Make	Proizvođač skenera.
272	Model	Naziv modela skenera ili njegov broj.
305	Software	Ime i broj verzije softverskog paketa koji je korišten pri stvaranju slike.
306	DateTime	Vrijeme i datum stvaranja slike.
315	Artist	Ime osobe koja je stvorila sliku.
36868	DateTimeDigitized	Datum i vrijeme zapisivanja slike kao digitalnog podatka.
41728	FileSource	Označava izvor slike (vrsta uređaja).
42016	ImageUniqueID	Označava jedinstveni identifikator za svaku sliku.
42032	CameraOwnerName	Vlasnik digitalnog aparata.

Slično se u polja PDF datoteke upisuju podaci koji su potrebni za pronalazak i određivanje izvornosti. Hash rezultat pokazuje kako nije bilo promijene dok ovi podaci pokazuju izvornost. Podatak kada je dokument pripremljen i skeniran i tko je to obavio postaju nerazdvojivi dio glavne slike, bilo TIF bilo PDF formata.

Ukratko, na temelju istražene literature i analiziranih primjera iz prakse, zaključujem i preporučam:

1. potrebno je izrađivati glavnu sliku u PDF, PDF/A ili TIFF formatu,
2. treba koritiiti kompresiju bez gubitaka,

3. za bitonalne TIFF datoteke kompresija može biti G4,
4. PDF format može imati slojeve postavljene na vrijednost 0,
5. rezolucija treba biti minimalno 400 dpi u optičkoj rezoluciji,
6. tonalnost slike treba biti 24-bitna boja,
7. tonska dinamika treba biti minimalno 3,5,
8. svaki list treba biti obostrano skeniran,
9. u sliku se u odgovarajuća polja trebaju upisivati metapodaci potrebni za pronalazak slike i autentičnost.

10.12. Slanje datoteka u središnji repozitorij

Autentičnost datoteka koje se šalju u središnji repozitorij, kako predlaže tehnički izvještaj ISO/TR 15801:2009, može se poduprijeti na način da se pri skeniranju digitalno potpiše digitalizirana slika. Središnji repozitorij u tom slučaju obavlja provjeru digitalnog potpisa te zapisuje podatke o verifikaciji digitalnih potpisa, hash rezultat datoteke za kasnije usporedbe, i podatke o certifikatu.

Slanje datoteka se odnosi na glavne slike i na izvedene slike. U tom slučaju postoje dva repozitorija. Središnji repozitorij glavnih slika sadrži glavne slike. Središnji repozitorij izvedenih slika sadrži izvedene slike glavnih slika. Tada također postoje dvije baze metapodataka - baza metapodataka glavnih slika i baza metapodataka izvedenih slika.

Podaci o slanju kao i podatak o uspješnosti slanja zapisuju se u datoteku koja sadrži revizijski trag odnosno dnevnik zapisa.

10.13. Korištenje vremena i datuma

Korištenje vremena i datuma u cjelokupnom procesu bi trebalo biti jedinstveno kako bi se moglo ispravno pratiti proces nastanka digitalizirane slike. Ovaj zahtjev potvrđuje tehnički izvještaj ISO/TR 15801:2009 koji predlaže korištenje sistemskog vremena o kojem se vode zapisnici o održavanju.

Održavanje vremena i datuma se upisuje u datoteku koja sadrži revizijski trag obavljenog procesa.

10.14. Sustav za upravljanje dokumentima od povjerenja

Sustav za upravljanje dokumentima od povjerenja, prema tehničkom izvještaju ISO/TR 15801:2009, osigurava da se sve elektronički pohranjene informacije mogu smatrati pravom i točnom kopijom izvornih informacija, bez obzira na izvorni format. Ovakav sustav u svojim zahtjevima minimalno sadrži:

1. barem jedna kopija pohranjenih podataka je pohranjena na medij koji čuva pohranjeni podatak od izmjene, neprikladnih dodavanja ili brisanja tijekom životnog vijeka podataka, i čuva se i održava na sigurnoj lokaciji koja je odvojena od ostalih kopija pohranjenih informacija,
2. koristi se hardver i medij za pohranu koji štiti pohranjenu informaciju od izmjene, neprikladnih dodavanja ili brisanja tijekom životnog vijeka podataka,
3. mogućnost potvrđivanja od strane neovisne revizijske metodologije. Potvrđuje se da se originalno pohranjene informacije mogu točno prikazati tijekom životnog vijeka. Provjerava se softver, hardver i mediji za pohranu.

10.15. Metapodaci koji se stvaraju digitalizacijom

Dokazivanju autentičnosti pomaže ukoliko postoje podaci o povijesnom stanju dokumentacije na koju se odnose. Tako mogu postojati metapodaci o: stvaranju, prihvatu ili registraciji, kretanju i praćenju, sređivanju, pohrani, predaji u Arhiv ako postoji, pohrani u arhiv, korištenju gradiva, analizi gradiva, pripremi gradiva, skeniranju gradiva, slanju u središnji repozitorij, kontroli skeniranog gradiva, dodatni metapodaci prepisani sa slike, kontroli prepisanih metapodataka, isporuci u sustav za dugoročno očuvanje, revizijskom tragu, kontroli revizijskog traga, prihvaćanju u sustav, pohrani u sustavu, pričuvnoj kopiji, pristupu podacima, migraciji, uništenju slika i metapodataka.

U nastavku se navode metapodaci koji se stvaraju tijekom procesa digitalizacije i koji se odnose na korake, operatere i aplikacije koji se koriste tijekom procesa.

1. za kontrolnu datoteku na nivou dokumenta:
    a. jedinstvena oznaka dokumenta (iz klasifikacijskog sustava),
    b. naziv stvaratelja,
    c. datum i vrijeme stvaranja,
    d. datum i vrijeme prihvata u poslovni sustav,
    e. kratak opis ili naslov,

f. broj stranica,
g. broj praznih stranica,
h. postojanje kritičnih elemenata (boja, veličina, pečat, potpis, decimalni broj, drugi mali elementi),
i. podatak o dokumentacijskoj jedinici kojoj dokument pripada,
j. podatak o tehničkoj jedinici u kojoj se dokument nalazi,
k. rok čuvanja dokumenta (iz klasifikacijskog sustava),
l. broj upute po kojoj se radi,
m. naziv upute po kojoj se radi,
n. verzija upute po kojoj se radi,

2. o pripremi za ispis vodećeg dokumenta:
    a. jedinstvena oznaka paketa,
    b. naziv paketa,
    c. datum pripreme paketa,
    d. vrijeme početka pripreme paketa,
    e. vrijeme završetka pripreme paketa,
    f. ime i prezime operatera,
3. o skeniranju:
    a. podaci o skeneru:
        i. model skenera,
        ii. proizvođač skenera,
        iii. godina proizvodnje skenera,
        iv. vrsta svjetlosti,
        v. tip lampe,
        vi. optička razlučivost senzora,
        vii. tip senzora,
    b. podaci o slici:
        i. jedinstvena oznaka slike,
        ii. količina dpi,
        iii. vrsta kompresije,
        iv. tonalnost,
        v. broj bitova tonalnosti,
        vi. sve korištene funkcije poboljšanja slike,
        vii. verzija slike (svako ponavljanje skeniranja stvara novu verziju slike),

viii. vrsta slike (glavna slika, izvedena slika),
ix. poveznica na glavnu sliku (u slučaju izvedene slike),
x. hash rezultat digitalizirane slike,
xi. certifikat za potpis,
xii. digitalni potpis,
xiii. redni broj slike u paketu,

c. podaci o skeniranju:
i. vrijeme skeniranja (sistemsko vrijeme),
ii. datum skeniranja (sistemsko vrijeme),
iii. ime i prezime operatera (aplikativno upisano),
iv. korišteni posao,
v. razlog ponavljanja skeniranja (ako je operater ponovio skeniranje podatak o ponavljanju upisuje skener, na primjer prolaz dva dokumenta, prepoznata spajalica, i sl.),

4. o ponavljanju skeniranja (samo u slučaju kada se ponavlja zbog zahtjeva iz faze kontrole):
a. ime i prezime kontrolora,
b. datum zahtjeva za ponavljanjem skeniranja,
c. vrijeme zahtjeva za ponavljanjem skeniranja,
d. razlog ponavljanja skeniranja,
5. o indeksiranju:
a. jedinstvena oznaka aplikacije za indeksiranje,
b. ime i prezime operatera na indeksiranju,
c. datum indeksiranja,
d. vrijeme indeksiranja,
e. metapodaci koji se indeksiraju (ovise o fazi analize dokumentacije),
6. o kontroli digitalizirane slike i pripadnih metapodataka:
a. jedinstvena oznaka aplikacije za kontrolu,
b. ime i prezime kontrolora ili naziv automatske funkcije koja je obavila kontrolu,
c. datum kontrole,
d. vrijeme izvršene kontrole,
e. status kontrole („OK“ ili „PONOVITI“),
f. način kontrole (automatski ili ručno),
7. o slanju digitaliziranog paketa i pripadnih metapodataka:

a. jedinstvena oznaka aplikacije za slanje,
b. datum slanja,
c. vrijeme slanja
d. hash rezultat paketa koji se šalje,
e. certifikat za izradu digitalnog potpisa,
f. digitalni potpis.

10.16. Aplikacije u sustavu

U sustavu digitalizacije može se prepoznati nekoliko aplikacija i softvera koji su potrebni za rad. To su: aplikacija za pripremu kojom operateri na pripremi izrađuju vodeći dokument svakog paketa, upisuju podatke u bazu za kasniju provjeru ispravnog prihvata paketa centralni repozitorij; softver za prihvat slike koja uključuje skenerski program za prihvat slike, pokretački program i slanje na glavni repozitorij; aplikacija za indeksiranje koju koriste operateri na indeksiranju; aplikacija za kontrolu slika i metapodataka; i aplikacija za isporuku pridruženih metapodataka i izvedenih slika koja sve pakete sa statusom „OK“ isporučuje se na repozitorij za dugoročnu pohranu autentičnih slika i na repozitorij za prikaz izvedenih digitaliziranih slika.

Aplikacije trebaju biti izvedene na način kojim se kontrolira unos podataka ne dopuštajući preskakanje obaveznih polja za unos i dopuštajući samo aktivnosti i postupke unosa podataka. Može se koristiti rječnik dopuštenih unosa za svaki metapodatak i obaviti validaciju ispravnih unosa.

Svaku aplikaciju je moguće koristiti isključivo unosom korisničkih podataka ili certifikata. Na taj način postoji kontrolirani rad. Sve aplikacije trebaju biti testirane i ovjerene od strane nezavisne uloge. Sve aplikacije ispisuju u revizijski trag podatke o poduzetim akcijama.

10.17. Repozitoriji podataka

Tijekom digitalizacijskog postupka mogu se prepoznati različiti repozitoriji. Repozitorij za prihvat glavne digitalizirane slike i pripadnih metapodataka tijekom digitalizacijskog postupka. Paketi koji su odobreni se šalju u repozitorij za prihvat i dugoročnu pohranu glavne slike i pripadnih metapodataka. Ovaj repozitorij treba omogućiti samo dodavanje podataka i slika i za njega se trebaju izrađivati pričuvne kopije. Nadalje, u

procesu digitalizacije nalazi se i repozitorij koji je pričuvna kopija prethodnog repozitorija. Treća vrsta repozitorija je repozitorij koji sadrži digitalizirane slike za prikaz (izvedene slike glavne slike) i metapodatke za pretragu i prikaz koji su potrebni za uredno obavljanje funkcije kojoj su namijenjeni. Dodatna vrsta repozitorija je repozitorij koji evidentira sve revizijske tragove o provedenim akcijama.

Dobar primjer za pohranu glavne slike i pripadajućih metapodataka je PIQL film.

10.18. Revizijski trag

U revizijski trag potrebno je upisati sve podatke koji su potrebni za dokazivanje autentičnosti digitalizacijskog procesa. U njega se trebaju upisati podaci o pripremi paketa, skeniranju paketa, kontroli paketa, ponavljanju skeniranja dokumenta, hash rezultat digitalizirane slike, hash rezultat XML datoteke koja sadrži metapodatke digitalizirane slike koja se šalje u središnji repozitorij, rezultat slanja, korišten digitalni certifikat, rezultati periodičke kontrole središnjeg repozitorija glavne slike i baze podataka glavne slike, rezultati stanja sustava uključujući održavanje skenera, održavanje računala i računalne mreže, podaci o korištenim uputama koji uključuju naziv, verziju i broj upute, te podaci o korištenom sistemskom vremenu i njegovom održavanju.

10.19. Zaključak

Izrađeni prijedlog *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala* postupkom digitalizacije uključuje određivanje uloga koje se u postupku digitalizacije pojavljuju i koje se odnose na operativne, nadzorne i kontrolne uloge, zatim izradu i dokumentiranost uputa cijelog postupka koji uključuje dokumentiranost karakteristika glavne slike, skenera, korištenog vremena i datuma, potrebnih metapodataka i provedbenih procesa. U ranijim poglavljima promatrani su zahtjevi normativnog okruženja, zakonskog okruženja, tehničkih rješenja i primjera dobre prakse koji su pomogli pri stvaranju predloženog modela.

Prijedlog modela se prirodno nadovezuje na zakonski zahtijevanu sređenost dokumentacije koja je nadopunjena podacima iz zahtjeva autentičnosti. Dodatno, u modelu se prepoznaju sve korištene aplikacije, uključujući i pomoćne, koje trebaju unaprijed biti definirane, programirane od strane nezavisnih stručnjaka, te kontrolirane, i kojima se može garantirati pouzdanost rada i korištenja. Jedan od glavnih zahtjeva je korištenje sistemskog

vremena bez kojeg je nemoguće pratiti vremenski slijed provedenih akcija i koji je nužan za dokazivanje autentičnosti u bilo kojem kasnijem trenutku.

Pored potrebnih kontrola provedbe koraka digitalizacije model prepoznaje ulogu nadzora koja je kritična i koju obavljaju definirane uloge unutar tvrtke, ali i dodatnu vanjsku nezavisnu ulogu koja dobiva sve zapise u nadzor i koja sastavlja izvještaj za tvrtku kojim se potvrđuje urednost provedbe cjelokupnog procesa digitalizacije.

11. KOMPARATIVNA ANALIZA PREDLOŽENOG MODELA PROCESA STVARANJA AUTENTIČNIH DIGITALNIH KOPIJA U OBLIKU ORIGINALA I NORMI ISO/TR 15801 I ISO/TR 13028

U nastavku se nalazi komparativna analiza predloženog *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala* i dvije prepoznate norme tehničkog izvještaja ISO/TR 15801:2009 i ISO/TR 13028:2010 koji govore o stvaranju autentičnih digitaliziranih slika. Ovom analizom želi se pokazati postoji li korelacija, odnosno povezanost, između definiranih uvjeta za autentičnost, predloženog Modela i prepoznatih normi. Za očekivati je da rezultat analize pokaže da norme u velikoj mjeri zadovoljavaju zahtjeve autentičnosti, s blagim odstupanjima koje upravo predloženi Model zadovoljava i nadopunjuje. Za provedbu analize korišten je obrazac sastavljen slijedeći zahtjeve autentičnosti. U poglavlju Rezultat analize usporedno su popisani rezultati analize.

11.1. Obrazac za analizu

Prilikom izrade komparativne analize predloženog modela procesa stvaranja autentičnih digitalnih kopija u obliku originala i tehničkih izvještaja ISO/TR 15801:2009 i ISO/TR 13028:2010 koje su tijekom analize dokumentacije prepoznate kao važne na proces digitalizacije koji daje autentičnu kopiju, korišten je obrazac s pitanjima naveden u tablici (tablica 10). Obrazac je sastavljen prema zahtjevima autentičnosti opisanim u točki 3. Autentičnost, odnosno točki 3.5. Zaključak o konceptu autentičnosti.

Tablica 10. Obrazac s pitanjima za usporedbu autentičnosti

1. POTPUNOST	
A. Podaci i oznake su prisutni na dokumentu.	Je li napravljena kontrola prisutnosti podataka i oznaka na digitaliziranoj slici?
B. Podaci i oznake su povezani s dokumentom.	Postoji li poveznica između podataka i oznaka i digitalizirane slike?
C. Sve stranice dokumenta su snimljene.	Jesu li sve stranice dokumenta snimljene?
D. Uključeni su pripadajući dodaci.	Jesu li pripadajući dodaci povezani s dokumentom? (Postoji postupanje s dodacima dokumentu kao na primjer dodatni papiri, post-it-i i slično.)
E. Poznat je podatak o stvaratelju.	Je li poznat podatak o stvaratelju?

2. POUZDANOST PROCESA	
A. Proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije.	1. Postoje li uloge koje propisuju, odobravaju i ovjeravaju proces prije početka digitalizacije?
	2. Jesu li dokumentirani svi dijelovi procesa: a) priprema b) skeniranje c) indeksiranje d) kontrola e) ponavljanje skeniranja f) isporuka u središnji repozitorij glavni slika g) izrada revizijskih dnevnika h) prepoznati su potrebni metapodaci i) prepoznate su korištene aplikacije j) korištena infrastruktura (računala i mediji za pohranu) k) izrada pričuvnih kopija?
	3. Radi li se test na reprezentativnom uzorku?
	4. Jesu li popisani svi tehnički uvjeti: a) glavna slika b) izvedena slika c) skener d) softver za prihvat slike e) pokretački program f) aplikacija za pripremu g) aplikacija za indeksiranje h) aplikacija za kontrolu i) aplikacija za slanje na središnji repozitorij j) infrastruktura (računala i mediji za pohranu) k) korišteno sistemsko vrijeme?
	5. Postoje li odijeljene uloge za: a) svaki dio procesa b) nadzora c) kontrole
B. Proces je nadziran tijekom digitalizacije i o tome postoje evidencije.	1. Nadzire li se proces? 2. Jesu li provedene potrebne edukacije prije početka procesa digitalizacije? 3. Provode li se potrebne edukacije pri svakoj promjeni? 4. Postoje li uloge nadzora? 5. Postoje li evidencije provedenih nadzora? 6. Dokumentiraju li se sve promjene i dobiva li svaki dokument novu verziju?
C. Proces je provjeravan tijekom digitalizacije i o tome postoje evidencije.	1. Provjerava li se ili kontrolira proces? 2. Provodi li se održavanje svih elemenata procesa? 3. Postoje li uloge kontrole? 4. Postoje li evidencije o provedenim provjerama?

3. INTEGRITET DOKUMENTA	
A. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta.	Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni od trenutka stvaranja?
B. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni u trenutku prihvata u središnji repozitorij.	Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni u trenutku prihvata u središnji repozitorij?
4. DOSTUPNOST DOKUMENTA	
A. Podacima, oznakama na dokumentu i pripadajućim poveznicama s dokumentom može se ispravno pristupiti, čitati i protumačiti.	Može li se ispravno pristupiti, čitati i protumačiti podatke, oznake na dokumentu i pripadajuće poveznice?

11.2. Analiza norme ISO/TR 15801:2009 i zahtjeva autentičnosti

1. POTPUNOST

A. Podaci i oznake su prisutni na dokumentu. Je li napravljena kontrola prisutnosti podataka i oznaka na digitaliziranoj slici?

Točka 5.3.4. ove norme govori kako prilikom stvaranja digitaliziranih dokumenata treba voditi računa da se svi relevantni metapodaci također prenesu, da su svi potrebni podaci snimljeni i da su svi digitalni i/ili analogni dokumenti pravilno interpretirani. Također je potrebno obaviti reviziju sadržaja metapodataka po pitanju potpunosti i prikladnosti.

Zatim, točka 5.4.2., traži u procesu pripreme očuvanje primarnog redoslijeda, pažljivo rukovanje dokumentacijom kako bi se izbjeglo uništavanje, te postupanje s fizičkim dodacima dokumentu kao što su post-it-i.

Dodatno, točka 5.4.3. napominje kako je u određenim slučajevima potrebno osigurati dodatne metode kojima se garantira da su svi dokumenti skenirani kao što je na primjer provjera slika s papirnatim originalima.

Prilikom kontrole kvalitete, točka 5.4.6.1., obavlja se kontrola čitljivosti cijelog dokumenta, čitljivosti najmanjeg detalja, cjelovitosti detalja na dokumentu, točnosti dimenzija u odnosu na izvornik, provjera je li skener stvara mrlje koje ne postoje na dokumentu,

potpunost cjelokupne slike odnosno provjera nedostaju li informacije koje se nalaze na rubovima, provjera gustoće punih crnih područja i kontrola vjernosti boje.

Točka 6.7. predlaže korištenje kompresije bez gubitaka, te evidenciju korištenih kompresijskih tehnika bilo kao dio datoteke bilo kao povezani podaci ili u odvojenom dnevniku zapisa (log file).

Na kraju, točka 6.8., ograničava uklanjanje formi s digitalizirane slike jer može doći do gubitka podataka.

B. Podaci i oznake su povezani s dokumentom. Postoji li poveznica između podataka i oznaka i digitalizirane slike?

Točka 6.7. govori o povezanosti podatka o korištenim kompresijskim tehnikama upisom u samu datoteku ili upisom s ostalim povezanim podacima ili upisom u dnevnik zapisa (log file), te, točka 7.1.4. čuvanje dnevnika zapisa koliko i informacija na koju se odnosi.

KRITIKA: Ne govori se o ostalim podacima i oznakama koje su povezane s dokumentom.

C. Sve stranice dokumenta su snimljene. Jesu li sve stranice dokumenta snimljene?

Točka 5.4.5. predlaže prilikom procesa skeniranja brojanje ili prethodno indeksiranje papirnatih dokumenata kako bi se precizno snimio broj stranica po dokumentu ili paketu dokumenata. Predlaže se tehnika dvostrukog brojanja radi preciznijeg rezultata.

KRITIKA: Ne govori se o provedenoj kontroli skeniranih stranica i izbrojenih stranica.

D. Uključeni su pripadajući dodaci. Jesu li pripadajući dodaci povezani s dokumentom? (Postoji postupanje s dodacima dokumentu kao na primjer dodatni papiri, post-it-i i slično.)

Točka 5.4.2. govori o potrebi očuvanja primarnog redoslijeda tijekom pripreme te postupanju s fizičkim dodacima dokumentu kao što su post-it-i.

E. Poznat je podatak o stvaratelju. Je li poznat podatak o stvaratelju?

Točka 3.2.2. općenito govori o pohrani informacija te o upisivanju i popisivanju tih informacija u dokument Politika upravljanja dokumentima.

KRITIKA: Ne spominje se izričito podatak o stvaratelju, niti prepoznaje prethodno poznavanje ovog podatka za dokumentaciju koja se digitalizira.

2. POUZDANOST PROCESA

A. Proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije.

1. Postoje li uloge koje propisuju, odobravaju i ovjeravaju proces prije početka digitalizacije?

Točka 3.2.5. kaže kako organizacije koje su u svoje poslovanje ugradile sustav kvalitete ISO 9001 imaju organizirane uloge. Zatim u točki 3.2.7. se traži da sve odgovornosti za svaki tip informacije budu popisane u dokumentu Politike upravljanja dokumentima. Dodatno u točki 4.2.1 traže odobrenje dokumenta Politike informacijske sigurnosti od strane uprave te evidenciju tog odobrenja. Također, revizija Priručnika, prema točki 5.2.4., provodi se minimalno jednom godišnje a rezultat periodičke revizije treba biti dokumentiran i odobren od strane osobe koja je odgovorna za operativnost revidiranog dijela sustava.

2. Jesu li dokumentirani svi dijelovi procesa:

a) priprema

Točka 5.4. govori o procesu digitalizacije koji se sastoji od pripreme, stvaranje paketa dokumenata, skeniranja i obrade slike.

b) skeniranje

Točka 5.4. govori o procesu digitalizacije koji se sastoji od pripreme, stvaranje paketa dokumenata, skeniranja i obrade slike. Zatim, točka 5.2.2. govori o Priručniku koji uključuje skeniranje, indeksiranje, slanje datoteka, održavanje sustava, sigurnost i zaštitu, datum i vremenske žigove, kontrole verzija i dokumentaciju održavanja.

c) indeksiranje

Točka 5.4. govori o procesu digitalizacije koji se sastoji od pripreme, stvaranje paketa dokumenata, skeniranja i obrade slike. Zatim, točka 5.2.2. govori o Priručniku koji uključuje skeniranje, indeksiranje, slanje datoteka, održavanje sustava, sigurnost i zaštitu, datum i vremenske žigove, kontrole verzija i dokumentaciju održavanja. Dodatno točka 5.6. traži propisivanje pravila i procedure indeksiranja, te prilikom ručnog indeksiranja, točka 5.6.2., predlaže se provođenje treninga operatera.

d) kontrola

Kontrola kvalitete, točka 5.4.6., provodi se u prvom koraku od strane operatera na skeneru, točka 5.4.6.2., a u drugom koraku od strane osoblja koje nije odgovorno za skeniranje. Moguće je kontrolu kvalitete provesti tehnikom statističkog uzorkovanja, pri čemu se frekvencija statističkog uzorkovanja treba evidentirati. Točka 5.4.6.1. navodi što može se uključiti u kontrolu kvalitete: čitljivost cijelog dokumenta, da je i najmanji detalj čitljiv, cjelovitost detalja na dokumentu, točnosti dimenzija u odnosu na izvornik, stvara li skener mrlje koje ne postoje na dokumentu, potpunost cjelokupne slike (nedostaju li informacije koje su na rubovima), gustoća punih crnih područja i vjernost boje. Kontrolu kvalitete je potrebno organizirati temeljem rezultata testiranja provedenim na reprezentativnom uzorku koji trebaju biti realistični. Pored kontrole kvalitete digitalizirane slike potrebno je provesti kontrolu kvalitete ručnog unosa, odnosno indeksiranja, točka 5.6.3., te u slučaju automatskog indeksiranja, točka 5.6.3., npr. korištenje OCR tehnika treba se provesti provjera upisanih podataka. Točka 5.6.6. traži propisivanje postupaka kontrole kvalitete indeksnih podataka.

e) ponavljanje skeniranja

Točka 5.4.7. traži dokumentiranost procedura ponavljanja skeniranja.

f) isporuka u središnji repozitorij glavnih slika

Slanje datoteka treba biti propisano u Priručniku, točka 5.2.2. Zatim, točka 5.8.1.1. kaže kako slanje datoteka unutar sustava treba biti provedeno osiguravajući integritet, te kako

slanje datoteka s jednog uređaja na drugi treba provoditi aplikacija. Za dodatne mjere sigurnosti predlaže se korištenje digitalnih potpisa. Točka 5.8.1.2. napominje kako slanje datoteka preko lokalne mreže treba osigurati integritet.

g) izrada revizijskih dnevnika

Točka 7.1.1. dijeli revizijski trag, revizijski dnevnik, na sistemski i koji se odnosi na pohranjene informacije. Zatim, točka 7.1.2. napominje kako je u revizijski dnevnik bolje automatsko upisivanje podataka direktno iz sustava. Ručno upisivanje treba biti strogo propisano. Budući se revizijski trag upisuje u datoteku koja ima ograničenu količinu unosa potrebno je propisati adekvatno provođenje upisivanja kako ne bi došlo do gubitka podataka.

U revizijski trag, točka 7.3.1. upisuju se zapisi o provedenim aktivnostima: detalji o prihvatu slike, podacima o serijskoj obradi, podacima o indeksiranju, podaci o provedenim promjenama i korištenim digitalnim potpisima.

Točka 7.3.2. govori o informacijama koje mogu biti od značaja za dokazivanje autentičnosti pohranjenih podataka, pri tome ističe općenite podatke, podatke o datoteci, o skeniranim dokumentima, o paketima dokumenata, indeksiranju, promjenama i digitalnim potpisima:

1. općeniti podaci – točka 7.3.2.1.:
    a. identifikator datoteke,
    b. datum i vrijeme procesa,
    c. identifikator paketa,
    d. broj stranica za skenirani dokument ili paketa dokumenata,
    e. odobrenje kontrole kvalitete,
    f. identifikator svake datoteke koja je indeksirana,
    g. identifikator operatera ili radne stanice,
    h. konačni zapis na pohrani,
2. informacije o datoteci – točka 7.3.2.2.:
    a. jedinstvena oznaka,
    b. broj dokumenata/stranica u datoteci,
    c. veličina datoteke (npr. u kilobajtima),
    d. format datoteke,
    e. kod datoteke (npr. EDI vrijednosti, DTD i slično),
3. informacije o skeniranim dokumentima – točka 7.3.2.3.:

a. jedinstveni interni identifikator datoteke,
b. broj stranica slika koje su skenirane,
c. broj stranica koje su poslane u sustav pohrane,

4. informacije o paketima dokumenata – točka 7.3.3.:
    a. jedinstvena oznaka paketa,
    b. identifikator operatera,
    c. vrsta skeniranog materijala (na primjer papir, mikrofilm),
    d. količina dokumenata u paketu (na primjer broj stranica (uključene obje strane), broj stranica s mikrofilma),
    e. detalji obrade slike ukoliko se razlikuju od onih koji su propisane,
5. informacije o indeksiranju – točka 7.3.4.:
    a. datum i vrijeme stvaranja indeksnih datoteka,
    b. datum i vrijeme svih dodavanja u indeksnu datoteku,
    c. datum i vrijeme brisanja indeksnih datoteka,
    d. podatak o indeksnim pojmovima koji su povezani s obrisanom datotekom,
    e. identifikator dokumenta, datoteke, slike koja se briše,
6. informacije o promjenama točka 7.3.5.:
    a. vrsta promjene,
    b. ime osobe ili program koji je napravio promjenu,
    c. poveznica na prethodnu verziju informacije (gdje je prikladno),
7. informacije o digitalnim potpisima – točka 7.3.6.:
    a. identifikator datoteke,
    b. identifikator certifikata,
    c. identifikacija izdavatelja certifikata,
    d. datumski i vremenski potpis,
    e. potvrda slanja,
    f. potvrda primanja,
    g. dokaz valjanosti.

h) prepoznati su potrebni metapodaci

Točka 5.3.4. govori o osiguranju zapisivanja svih potrebnih metapodataka, te reviziji potpunosti i adekvatnosti upisanih metapodataka.

KRITIKA: U revizijske dnevnike se upisuju gore navedeni metapodaci, ali ne spominju se metapodaci koji su potrebni za autentičnost i da su pri tome upisani i povezani sa slikom.

i) prepoznate su korištene aplikacije

Točka 6.2. traži opisivanje i dokumentiranost elemenata koji čine sustav, a posebno napominju korišteni hardver, softver i mrežne elemente.

j) korištena infrastruktura (računala i mediji za pohranu)

Točka 6.2. traži opisivanje i dokumentiranost elemenata koji čine sustav, a posebno napominju korišteni hardver, softver i mrežne elemente.

k) izrada pričuvnih kopija?

Točka 5.12. navodi kako pričuvne kopije trebaju biti smještene na odvojenom spremištu i trebaju se periodički provjeravati. Također na pričuvnim kopijama se pohranjuju svi zapisi o provedenim akcijama.

3. Radi li se test na reprezentativnom uzorku?

Točka 5.4.6.1. predlaže izradu testa reprezentativnog uzorka kompletne dokumentacije koju se namjerava skenirati.

4. Jesu li popisani svi tehnički uvjeti:
a) glavna slika

Točka 3.2.4. traži popisivanje detalja odobrenih formata datoteka i kompresijskih tehnologija u dokument Politika upravljanja dokumentima. Dodatno, točka 6.7. predlaže korištenje kompresije bez gubitaka, te, u točki 5.4.8. predlaže se propisivanje korištenih procedura poboljšanja kvalitete slike te evidentiranje u Priručniku. Također, točka 6.8. napominje kako se digitaliziranoj slici ne smiju tijekom skeniranja uklanjati forme jer može doći do gubitka podataka.

b) izvedena slika

Točka 3.2.4. traži osiguranje pohrane svih relevantnih verzija glavne slike te održanje njihovih veza.

c) skener

Točka 6.2. traži opisivanje i dokumentiranje elemenata koji čine sustav, a posebno ističu korišteni hardver, softver i mrežni elementi.

KRITIKA: Ne navode se karakteristike skenera.

d) softver za prihvat slike

Točka 6.6. kao osiguranje od gubitka podataka skenirane slike napominje kako se ne smiju provoditi dodatna poboljšanja na slici nakon stvaranja slike, odnosno predlaže se pohrana originalne neprocesirane slike.

e) pokretački program

Ne spominje se.

f) aplikacija za pripremu

Ne spominje se.

g) aplikacija za indeksiranje

Ne spominje se.

h) aplikacija za kontrolu

Ne spominje se.

i) aplikacija za slanje na središnji repozitorij

Ne spominje se.

j) infrastruktura (računala i mediji za pohranu)

Točka 6.2. traži opisivanje i dokumentiranje elemenata koji čine sustav, a posebno ističu korišteni hardver, softver i mrežni elementi.

k) korišteno sistemsko vrijeme?

Točka 5.17. predlaže kontinuirano održavanje sistemskog vremena i datuma, te zapisivanje provedenih aktivnosti. Dodatno u točki 7.1.3. govore o tome kako se svaka akcija koja se upiše u revizijski trag upisuje evidentirajući datum i vrijeme unosa, i pri tome korišteni datum i vrijeme trebaju biti od povjerenja.

5. Postoje li odijeljene uloge za:

a) svaki dio procesa

Točka 4.1.3. prepoznaje odijeljenost uloga za pripremu, kontrolu kvalitete, indeksiranje i informacijsku sigurnost. Nadalje, točka 6.4. traži propisivanje i dokumentiranje uloga u sustavu. Uloge koje su prepoznate su upravitelj sustava, administrator sustava, uloga održavanja sustava, stvaratelja ili autora, uloga koja brine o pohranjenim podacima i njihovom indeksiranju, uloga koja brine o dohvatu informacija. Pri tome treba osigurati samo odobrenim uloga pristup za unošenje i ispravljanje pohranjenih informacija. Dodatno se zahtjeva od osoba koje provode ove uloge dokazivanje stručnosti.

b) nadzora

Točka 3.2.8. govori o prepoznavanju i definiranju odgovornosti osobe ili poslovne funkcije za postizanje i održavanje usklađenosti.

c) kontrole?

Točka 5.4.6.2. govori o prvoj točki kontrole koju provodi operater na skeneru kontrolirajući kvalitetu slike tijekom skeniranja, te u drugom koraku kontrole kvalitete predlaže provođenje kontrole od strane osoblja koje nije odgovorno za skeniranje.

B. Proces je nadziran tijekom digitalizacije i o tome postoje evidencije.

1. Nadzire li se proces?

Točka 4.1.3. prepoznaje potrebu zadržavanja fizičke i upravljačke odijeljenost koja postoji u sustavu kroz kontrolu logičkog pristupa. Nadzor sustava na performanse, točka 5.4.6.3., provodi se povremenim testiranjem pomoću kontrolnih uzoraka, te uz obavezan test na reprezentativnom uzorku. Nadzor medija za pohranu obavlja se zapisivanjem svih akcija zapisivanja datoteke korištenjem aplikativnog softvera, točka 6.3. Način pristupa i tumačenja revizijskih zapisa se propisuje u proceduralnim uputama, točka 7.1.5.

KRITIKA: Ne navodi se izričito nadzor cijelog procesa.

2. Jesu li provedene potrebne edukacije prije početka procesa digitalizacije?

Točka 5.2.3. govori o tome kako se usklađenost s procedurama može postići treninzima osoblja bilo specifičnim ili dnevnim, tijekom rada. Pri tome treba ugraditi procedure osiguravajući postupanje operatera sustava prema propisanim zahtjevima. Posebno točka 5.6.2. ističe provođenje treninga u slučaju ručnog indeksiranja.

3. Provode li se potrebne edukacije pri svakoj promjeni?

Točka 5.2.3. govori o tome kako se usklađenost s procedurama može postići treninzima osoblja bilo specifičnim ili dnevnim, tijekom rada. Pri tome treba ugraditi procedure osiguravajući postupanje operatera sustava prema propisanim zahtjevima.

4. Postoje li uloge nadzora?

Točka 7.1.5. govori o pristupu revizijskim zapisima od strane autoriziranog vanjskog osoblja kao na primjer revizorima.

5. Postoje li evidencije provedenih nadzora?

Ne spominje se.

6. Dokumentiraju li se sve promjene i dobiva li svaki dokument novu verziju?

Dokumentiranje svih promjena dokumenta postupanja s dokumentacijom, dodjeljivanje nove verzije nakon promjene, čuvanje prethodnih verzija sve dok se čuva digitalizirana dokumentacija na koju se ta verzija dokumenta odnosi navodi se u točkama 5.2.4., 5.18.2, i 5.19.

C. Proces je provjeravan tijekom digitalizacije i o tome postoje evidencije.

1. Provjerava li se ili kontrolira proces?

Točka 4.1.3. govori o provjeri, reviziji i ugradnji odijeljenih uloga prema potrebi.

2. Provodi li se održavanje svih elemenata procesa?

Točka 5.13.1. govori kako održavanje sustava treba provoditi isključivo kvalificirano osoblje. Sva provedena održavanja trebaju biti zapisana u dnevniku održavanja.

3. Postoje li uloge kontrole?

Točka 5.4.6.2. govori o prvoj točki kontrole koju provodi operater na skeneru kontrolirajući kvalitetu slike tijekom skeniranja, te u drugom koraku kontrole kvalitete predlaže provođenje kontrole od strane osoblja koje nije odgovorno za skeniranje.

4. Postoje li evidencije o provedenim provjerama?

Revizija Priručnika, prema točki 5.2.4., se provodi minimalno jednom godišnje a rezultat periodičke revizije treba biti dokumentiran i odobren od strane osobe koja je odgovorna za operativnost revidiranog dijela sustava. Točka 5.4.6.2. navodi kako rezultati svih provedenih kontrola kvalitete trebaju biti zapisani u dnevniku Kontrola kvalitete. Točka

5.13.1. govori kako održavanje sustava treba provoditi isključivo kvalificirano osoblje. Sva provedena održavanja trebaju biti zapisana u dnevniku održavanja. Dodatno u točki 5.13.2. navode kako nakon provedenog održavanja trebaju postojati zapisi koji pokazuju kako skener radi prema traženim zahtjevima kvalitete, te napominju kako ti zapisi služe dokazivanju kako za lošu sliku nije odgovoran skener.

3. INTEGRITET DOKUMENTA

A. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni od trenutka stvaranja?

Točka 3.2.3. navodi kako ukoliko postoje kopije elektroničkih objekata može biti važno pokazati kako nije bilo promjena bilo koje kopije. Nadalje u točki 6.10. primjećuju kako tijekom životnog vijeka digitaliziranih dokumenata može doći do raznih migracija i tijekom tih migracija treba se očuvati originalno stvoreni podaci. Predlaže se korištenje standardnih industrijskih formata ili čuvanje preglednika koji omogućavaju održavanje svakog pohranjenog formata. Potrebno je osigurati tijekom migracije da se sve digitalizirane slike, pripadni metapodaci i dnevnici zapisa migriraju bez gubitka integriteta i vodeći adekvatnu dokumentaciju o provedenoj migraciji. Kako bi se informacije očuvale tijekom cijelog perioda čuvanja, točka 6.9. predlaže provođenje redovite provjere medija za pohranu koja je usklađena s preporukama proizvođača. Također je potrebno čuvati revizijski trag, točka 7.1.6., u obliku pričuvne kopije, zatim sustav koji čuva revizijski trag treba čuvati informacije od mogućnosti promjene, te kada se radi oporavak sustava potrebno je sačuvati informacije kojima se pokazuje kako nije došlo do narušavanja autentičnosti podataka.

Međutim, najvažnija informacija o dokazivanju kako nije bilo promjena od trenutka stvaranja je preporučeno korištenje digitalnih potpisa koji sadrže kontrolni zbroj ili rezultat hash funkcije, točka 6.5.2., upisanih u samu datoteku ili na sigurnoj pohrani zajedno s ostalim originalnim podacima.

B. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni u trenutku prihvata u središnji repozitorij. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni u trenutku prihvata u središnji repozitorij?

Točka 4.2.1. kaže kako se politika informacijske sigurnosti implementira radi smanjenja rizika uspješne primjedbe autentičnosti informacije koja je elektronički pohranjena. Sigurnosni postupci trebaju uključiti izradu pričuvnih kopija, mogućnost revizije u bilo koje vrijeme, te uključivati zgrade, kontrole kvalitete, mrežnu povezanost i tako dalje. Sve promjene indeksiranih podataka trebaju biti evidentirane i raniji upisi trebaju biti sačuvani, točka 5.6.5. Integritet pohranjenih informacija, točka 6.5.1., treba biti osiguran unutar sustava uključujući slanje na i iz medija za pohranu. Kako bi se to postiglo predlaže se izrada kontrolnog zbroja prilikom izrade digitalizirane slike i zapisivanje ovog kontrolnog zbroja na revizijski trag odmah pri izradi zbroja. Dodatno u točki 6.5.2. napominju kako se za osiguranje nepromjenjivosti podataka mogu koristiti digitalni potpisa pri čemu se treba voditi računa o svim elementima koji su uključeni za izradu digitalnih potpisa kao i verifikacije pravog identiteta osobe prije dobivanja odobrenja za potpisivanje. I na kraju u točki 5.3.4. govore o tome kako se prilikom stvaranja ili uvoza digitaliziranih ili analognih dokumenata treba voditi računa da se svi relevantni metapodaci također prenesu, da su svi potrebni podaci snimljeni i da su svi digitalni i/ili analogni dokumenti pravilno interpretirani, a sadržaj metapodataka se treba revidirati po pitanju potpunosti i prikladnosti.

4. DOSTUPNOST DOKUMENTA

A. Podacima, oznakama na dokumentu i pripadajućim poveznicama s dokumentom može se ispravno pristupiti, čitati i protumačiti. Može li se ispravno pristupiti, čitati i protumačiti podatke, oznake na dokumentu i pripadajuće poveznice?

Točka 5.4.3. kaže kako se prilikom stvaranja ili uvoza digitaliziranih ili analognih dokumenata treba voditi računa da se svi relevantni metapodaci također prenesu, da su svi potrebni podaci snimljeni i da su svi digitalni i/ili analogni dokumenti pravilno interpretirani, a sadržaj metapodataka se treba revidirati po pitanju potpunosti i prikladnosti. Za očuvanje integriteta, točka 6.5.1. predlaže se korištenje kontrolnog zbroja prilikom izrade digitalizirane slike i zapisivanje ovog kontrolnog zbroja na revizijski trag odmah pri izradi zbroja. I dodatno se digitalizirana slika potpisuje digitalnim potpisom čime se osigurava nepromjenjivost i verifikacija identiteta osobe koja je šalje datoteku.

11.3. Analiza tehničkog izvještaja ISO/TR 13028:2010 i zahtjeva autentičnosti

1. POTPUNOST

A. Podaci i oznake su prisutni na dokumentu. Je li napravljena kontrola prisutnosti podataka i oznaka na digitaliziranoj slici?

Točka 6.3.3. govori o detaljima koje treba provjeravati tijekom pripreme. Priprema treba odlučiti može li papirnati original podnijeti proces skeniranja, na primjer već oštećen dokument može se dodatno oštetiti tijekom skeniranja. Zatim vodi se računa o veličini papira može li proći kroz skener, te način postupanja s rukom pisanim zabilješkama, marginalijama, bijelom korekturnom bojom, ljepljivom trakom, i tako dalje.

Nadalje, kontrola kvalitete treba biti provedena prije prihvaćanja digitaliziranih dokumenata u poslovne procese, točka 6.3.5.2. Točki 6.3.5.1. navodi kako u kontrolu kvalitete ne ulazi cijeli opseg digitaliziranih slika već dio koji se dobiva unaprijed definiranim kriterijima i frekvencijama za provjeru.

Kontrola kvalitete slike, prema Dodatku D, treba uključivati:

- je li najmanji detalj snimljen i čitljiv,
- je su li detalji snimljeni u cijelosti,
- postoji li točnost dimenzije kopije u usporedbi s originalom,
- postoje li točkice na digitaliziranoj slici koje ne postoje na originalu,
- je li original snimljen u cijelosti – jesu li svi rubovi uključeni i snimljeni,
- gustoća crnih polja,
- postojanost boje.

Dalje u Dodatku D govore o ponavljanju skeniranja ovisno o rezultatima kontrole obavljene na statističkom uzorku. Ukoliko proces kontrole kvalitete pokaže greške na više od 1% dokumentacije, sva dokumentacija obrađena nakon posljednje provjere se treba provjeriti. Ukoliko je greška na manje od 1% dokumentacije samo ona dokumentacija koja je otkrivena kontrolom se ispravlja.

KRITIKA: Predloženo rješenje je dobro za pokazivanje da je skener radio u dogovorenim granicama tolerancije kvalitete. Međutim, ništa se ne može reći o digitaliziranim slikama koje nisu provjerene.

B. Podaci i oznake su povezani s dokumentom. Postoji li poveznica između podataka i oznaka i digitalizirane slike?

Točka 6.3.4.1. govori kako postoje dvije grupe metapodataka koji se spremaju: oni koji se odnose na pojedinu sliku i proces digitalizacije i oni koji se odnose na zapise koje prenose poslovne informacije. Prepoznati metapodaci se mogu upisati u zaglavlje slike ili se voditi u posebnom sustavu i pri tome treba postojati poveznica metapodataka sa slikom na koju se odnose. Dodatni metapodaci povezani s dokumentom bi se trebali naslijediti iz ostalih sustava vođenja dokumenata.

Podaci koji se odnose na pojedinu sliku trebaju se automatski upisati, točka 6.3.4.2., su:

- jedinstvena oznaka slike,
- datum i vrijeme digitalizacije,
- ime osobe koja je obavila digitalizaciju,
- naziv uređaja koji je digitalizirao uključujući i naziv softvera,
- datum zadnje kalibracije uređaja.

Dodatno se u točkama 6.3.4.3. i 6.3.4.4. predlaže izrada dodatnih metapodataka koji opisuju sliku radi lakšeg pronalaženja.

Točka 6.5.4. navodi kako digitalizirana slika i izvorni dokument trebaju trajno biti povezani jedinstvenim identifikatorima, te kako se izvornici trebaju vratiti u prvobitni oblik nakon digitalizacijskog procesa.

Dodatak C norme govoreći o imenovanju datoteke zahtjeva unaprijed propisivanje i evidentiranje propisanog imenovanja. Pri tome predlažu kako podaci koji se nalaze u imenu datoteke trebaju biti evidentirani na dodatnoj lokaciji za slučaj preimenovanja datoteka.

KRITIKA: Prepoznati su svi metapodaci i traži se postojanje poveznice među metapodacima i digitalizirane slike na koju se odnose.

C. Sve stranice dokumenta su snimljene. Jesu li sve stranice dokumenta snimljene?

Točka 6.3.3. predlaže da se tijekom pripreme osigura provjera da su svi papiri digitalizirani. Tijekom kontrole kvalitete, 6.3.5.1., traži se verifikacija jednakosti izlazne količine i ulazne. Pored toga u Dodatku D se posebno traži kontrola korektnosti slijeda i

kompletnosti višestraničnih dokumenata. Kao način postizanja predlaže se zapisivanje količine dokumenata i količine dokumenata unutar jednog paketa.

KRITIKA: Navedeni prijedlog je dobar ukoliko je poznat točan broj stranica svakog dokumenta koji se nakon skeniranja može usporediti s brojem koji je skener zapisao. Međutim, nije jasno kako se to može obaviti tijekom pripreme, odnosno kako se tijekom pripreme osigurava da je skener točno obavio odvajanje dokumenata unutar paketa.

D. Uključeni su pripadajući dodaci. Jesu li pripadajući dodaci povezani s dokumentom? (Postoji postupanje s dodacima dokumentu kao na primjer dodatni papiri, post-it-i i slično.)

Tijekom faze pripreme, točka 6.3.3., osigurava se međusobna povezanost dokumenata kakva je pronađena. Dodatak C dodatno traži kako se treba zadržati prvotna organizacija papirnatih originala. Predlaže se organizirati digitalizirane slike u odgovarajuće mape koje predstavljaju reprezentaciju stvarne strukture originalne dokumentacije.

KRITIKA: Ukoliko se tijekom pripreme pomiješaju dokumenti nemoguće je znati koji je dokument s kojim povezan. Zato je važno zadržati pronađenu povezanost što je moguće jedino u fazi pripreme dokumentacije.

E. Poznat je podatak o stvaratelju. Je li poznat podatak o stvaratelju?

KRITIKA: U normi nema izričitog navođenja podatka o stvaratelju. Međutim, točka 6.3.4.1. govori o dodatnim metapodacima koji su povezani s dokumentom a nalaze se u sustavima vođenja dokumenata. Ukoliko se u tim metapodacima nalazi podatak o stvaratelju zapisati će se.

2. POUZDANOST PROCESA

A. Proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije.

1. Postoje li uloge koje propisuju, odobravaju i ovjeravaju proces prije početka digitalizacije?

KRITIKA: Ne navode se posebno uloge koje postoje u procesu.

2. Jesu li dokumentirani svi dijelovi procesa:

a) priprema

Točka 6.3.3. govori o pripremi.

b) skeniranje

Ne spominje se.

c) indeksiranje

Ne spominje se.

d) kontrola

Točka 6.3.5.1. govori o kontroli kvalitete slike prema kriterijima provjere navedenim u Dodatku D:

- je li najmanji detalj snimljen i čitljiv,
- je su li detalji snimljeni u cijelosti,
- postoji li točnost dimenzije kopije u usporedbi s originalom,
- postoje li točkice na digitaliziranoj slici koje ne postoje na originalu,
- je li original snimljen u cijelosti – jesu li svi rubovi uključeni i snimljeni,
- gustoća crnih polja,
- postojanost boje.

Pored kontrole kvalitete slike potrebno je obavljati i kontrolu kvalitete skenera, točka 6.3.5.1.

Dodatak D govori o kontroli metapodataka i traži provjeru zadovoljava li metapodatak standarde politike tvrtke, što učiniti u slučaju kada su metapodaci nepotpuni, provjeru relevantnosti i točnosti metapodataka, gramatičke ispravke, konzistentnost u stvaranju i čitanju metapodataka, evaluaciju korisnosti bilježenih metapodataka, kontrolu sinkronizacije

bilježenja metapodataka na više repozitorija, te popunjenost obaveznih polja. Također, potrebno je napraviti kontrolu preciznosti identifikacije datoteke.

e) ponavljanje skeniranja

Ponavljanje skeniranja je podijeljeno u dva koraka ovisno o količini pronađenih grešaka. Dodatak D kaže: ukoliko proces kontrole kvalitete pokaže greške na više od 1% dokumentacije, sva dokumentacija obrađena nakon posljednje provjere se treba provjeriti. Ukoliko je greška na manje od 1% dokumentacije samo ona dokumentacija koja je otkrivena kontrolom se ispravlja.

f) isporuka u središnji repozitorij glavnih slika

Ne spominje se.

g) izrada revizijskih dnevnika

Ne spominje se.

h) prepoznati su potrebni metapodaci

Točka 6.3.4.1. govori o dvije grupe metapodataka koji se spremaju te o dodatnim metapodacima koji su povezani s dokumentom a koji su naslijeđeni iz ostalih sustava vođenja dokumenata. Dodatno se u točkama 6.3.4.3. i 6.3.4.4. predlaže izrada dodatnih metapodataka koji opisuju sliku radi lakšeg pronalaženja, te u točki 6.5.4. traži se metapodatak o povezanosti digitalizirane slike i izvornog dokumenta.

i) prepoznate su korištene aplikacije

Ne spominje se.

j) korištena infrastruktura (računala i mediji za pohranu)

Ne spominje se.

k) izrada pričuvnih kopija?

Točka 6.4.2. govori o izradi, čuvanju, sigurnosti i testiranju pričuvnih kopija. Procedure izrade pričuvnih kopija i mediji za pohranu trebaju biti određeni, dokumentirani i primijenjeni. Izrada pričuvnih kopija digitaliziranih slika i pripadnih metapodataka trebaju biti uključeni u redovite procedure tvrtke. Nivo sigurnosti pričuvnih kopija treba osiguravati autentičnost. Pričuvne kopije trebaju biti testirane kako bi osigurale integritet pohranjenih datoteka.

3. Radi li se test na reprezentativnom uzorku?

U Dodatku D se navodi testiranje skenera na uzorku koji predstavlja dokumentaciju koja se skenira.

4. Jesu li popisani svi tehnički uvjeti:

a) glavna slika

Točka 6.2.1. govori kako se primijenjeni tehnički standardi upisuju u projektnu dokumentaciju i uključuju format datoteka i kompresiju. Zatim točka 6.2.3. govori o korištenju tehničkih specifikacija koje omogućavaju najveću kvalitetu, korištenje formata otvorenog izvora ili otvorenih standarda ili koji su u širokoj upotrebi, bez ugniježđenih objekata i poveznica na druge objekte, formati bi se trebali moći čitati koristeći dostupne programske dodatke, glavne slike bi trebale biti izrađene prema najvišim tehničkim standardima i držati se na neovisnim sustavima pohrane korištenjem sigurnih uvjeta čuvanja i najviših tehničkih standarda čuvanja.

b) izvedena slika

Točka 6.2.3. kaže kako izvedene kopije mogu biti u formatima koji su najprilagođeniji poslovnoj upotrebi. Točka 5.2. dodaje kako se izvedene kopije trebaju izraditi tijekom procesa digitalizacije.

c) skener

Ne spominje se.

d) softver za prihvat slike - poboljšanje slike

Točka 5.2. govori o korištenju tehnika poboljšanja slike koje dovode u pitanje autentičnosti digitalizirane slike:

- oštrenje slike,
- izrezivanje dijelova sjena,
- zamućivanje,
- uklanjanje mrlja,
- uklanjanje točkica.

e) pokretački program

Ne spominje se.

f) aplikacija za pripremu

Ne spominje se.

g) aplikacija za indeksiranje

Ne spominje se.

h) aplikacija za kontrolu

Ne spominje se.

i) aplikacija za slanje na središnji repozitorij

Ne spominje se.

j) infrastruktura (računala i mediji za pohranu)

Ne spominje se.

k) korišteno sistemsko vrijeme?

Ne spominje se.

5. Postoje li odijeljene uloge za:

a) svaki dio procesa

Točka 6.2.1. navodi kako se uloge trebaju dokumentirati u projektnoj dokumentaciji i govori o ulogama koji podržavaju digitalizaciju, proces planiranja, kontrole i izvršenja digitalizacije te uloge kontrolu kvalitete.

b) nadzora

Točka 6.2.1. navodi kako se uloge trebaju dokumentirati u projektnoj dokumentaciji i govori o ulogama koji podržavaju digitalizaciju, proces planiranja, kontrole i izvršenja digitalizacije te uloge kontrolu kvalitete.

c) kontrole?

Točka 6.2.1. navodi kako se uloge trebaju dokumentirati u projektnoj dokumentaciji i govori o ulogama koji podržavaju digitalizaciju, proces planiranja, kontrole i izvršenja digitalizacije te uloge kontrolu kvalitete.

B. Proces je nadziran tijekom digitalizacije i o tome postoje evidencije.

1. Nadzire li se proces?

Predlaže se nadzor pristupa medijima za pohranu tijekom perioda pohrane digitaliziranih zapisa, točka 6.4.1.1., na način da se prepozna i zapiše neovlašteni pokušaj pristupa. Nadalje, točka 6.3., traži od sustava upravljanja osiguranje kontrolu procesa

identifikacije, indeksiranja, klasifikacije, sigurnosti, kontrole pristupa, upravljanje pravima i očuvanja podataka. Točka 6.3.5.2. govori o potrebi provođenja revizije procedure kontrole kvalitete.

Također, točka 6.2.2.1., govorio o redovitom pregledu digitalizacijskog pristupa kako bi zadovoljavao pravne zahtjeve, relevantnost i učinkovitost.

KRITIKA: Norma ne govori o nadzoru tijekom digitalizacije.

2. Jesu li provedene potrebne edukacije prije početka procesa digitalizacije?

Predlaže se provođenje obuke operatera, točka 6.3.5.1., te provođenje treninga za osoblje koje stvara, upravlja i radi s digitaliziranim dokumentima, točka 6.3.5.2, pri čemu treba propisati i održavati periodičnost nivo treninga.

3. Provode li se potrebne edukacije pri svakoj promjeni?

Ne spominje se.

4. Postoje li uloge nadzora?

Točka 6.2.1. navodi kako se uloge trebaju dokumentirati u projektnoj dokumentaciji i govori o ulogama koji podržavaju digitalizaciju, proces planiranja, kontrole i izvršenja digitalizacije te uloge kontrolu kvalitete.

5. Postoje li evidencije provedenih nadzora?

Ne spominje se.

6. Dokumentiraju li se sve promjene i dobiva li svaki dokument novu verziju?

Ne spominje se.

C. Proces je provjeravan tijekom digitalizacije i o tome postoje evidencije.

1. Provjerava li se ili kontrolira proces?

Točka 6.4.2. govori o procedurama izrade pričuvnih kopija i korištenih medija za pohranu. Kao jedan od načina kontrole procesa izrade pričuvnih kopija predlaže se da digitalizirane slike i pripadni metapodaci budu uključeni u redovite procedure tvrtke zadovoljavajući nivo sigurnosti koji osigurava autentičnost i testiranjem pričuvnih kopija kako bi se osigurao integritet pohranjenih podataka.

KRITIKA: Norma ne govori o kontroli procesa.

2. Provodi li se održavanje svih elemenata procesa?

Točka 6.2.3. govorio o podršci nezavisnih stručnjaka, stručnjaci koji su neovisni o proizvođačima, koji bi stalno trebali održavati sustav i migraciju. Posebno u Dodatku D navodi se potreba periodičkog testiranja performansi skenera, provjeri zadovoljavanja određenih tolerancijama, provođenje kontrole i održavanja prema preporukama proizvođača te kontrole uređaja pomoću kontrolnog uzorka.

KRITIKA: Ne spominje se održavanje ostalih elemenata procesa.

3. Postoje li uloge kontrole?

Točka 6.2.1. navodi kako se uloge trebaju dokumentirati u projektnoj dokumentaciji i govori o ulogama koji podržavaju digitalizaciju, proces planiranja, kontrole i izvršenja digitalizacije te uloge kontrolu kvalitete.

4. Postoje li evidencije o provedenim provjerama?

Točka 6.3.5.2. traži zapisivanje rezultata kontrole kvalitete.

KRITIKA: Ne spominje se zapisivanje ostalih evidencija o provedenim provjerama tijekom procesa digitalizacije.

3. INTEGRITET DOKUMENTA

A. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni od trenutka stvaranja?

Točka 6.4.1.1. traži zaštitu od promjene digitaliziranih slika tijekom perioda čuvanja na medijima za pohranu, te evidentiranju neovlaštenih pokušaja pristupa. Pričuvne kopije se trebaju redovito održavati unutar redovitih procedura tvrtke osiguravanjem autentičnost i integriteta, točka 6.4.2. Na zahtjev, točka 6.5.2., digitalizirane slike s mogu prikazati u originalnom formatu. I dodatno, točka 6.5.5., digitalizirane datoteke se trebaju propisno čuvati tijekom cijelog perioda sve dok su potrebne.

KRITIKA: Iako se iz navedenih zahtjeva može zaključiti kako nije došlo do promjene jednom kada su podaci uvezeni u medije za pohranu, nema podatka o tome jesu li podaci promijenjeni prije tog trenutka.

B. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni u trenutku prihvata u središnji repozitorij. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni u trenutku prihvata u središnji repozitorij?

Ne spominje se.

4. DOSTUPNOST DOKUMENTA

A. Podacima, oznakama na dokumentu i pripadajućim poveznicama s dokumentom može se ispravno pristupiti, čitati i protumačiti. Može li se ispravno pristupiti, čitati i protumačiti podatke, oznake na dokumentu i pripadajuće poveznice?

Točka 6.5.5. govori o propisnom čuvanju digitaliziranih slika tijekom cijelog perioda sve dok su potrebne.

11.4. Analiza predloženog modela procesa stvaranja autentičnih digitalnih kopija u obliku originala i zahtjeva autentičnosti

1. POTPUNOST

A. Podaci i oznake su prisutni na dokumentu. Je li napravljena kontrola prisutnosti podataka i oznaka na digitaliziranoj slici?

Točka 8.5.7. obavlja završnu kontrolu svih podataka i metapodataka povezanih s digitaliziranom slikom. Samo paketi koji su dobili status „OK“ se šalju dalje na pohranu.

B. Podaci i oznake su povezani s dokumentom. Postoji li poveznica između podataka i oznaka i digitalizirane slike?

Poveznica podataka i oznaka s dokumentom nalazi se u prepoznatim i evidentiranim metapodacima koji su popisani u točki 8.15.

C. Sve stranice dokumenta su snimljene. Jesu li sve stranice dokumenta snimljene?

U fazi kontrole obavlja se usporedba broja stranica s brojem stranica iz evidencije u fazi sređivanja gradiva, točka 8.5.7.

D. Uključeni su pripadajući dodaci. Jesu li pripadajući dodaci povezani s dokumentom? (Postoji postupanje s dodacima dokumentu kao na primjer dodatni papiri, post-it-i i slično.)

Točka 8.5.2., faza pripreme, vodi računa o uključenosti pripadnih dodataka. Dodatna usporedba je u fazi kontrole gdje se obavlja kontrola očekivanih broja stranica i skeniranih.

E. Poznat je podatak o stvaratelju. Je li poznat podatak o stvaratelju?

Točka 8.5.7. govori o postojanju podatka o stvaratelju za sređenu dokumentaciju

2. POUZDANOST PROCESA

A. Proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije.

1. Postoje li uloge koje propisuju, odobravaju i ovjeravaju proces prije početka digitalizacije?

Proces se prvotno testira na primjerenom uzorku, točka 8.5.1., prilikom čega se evidentiraju rezultati testiranja. Izrađuje se uputa za cijeli proces i elemente koji se nalaze u tom procesu te uloge, točka 8.7. Nezavisna uloga odobrava proces na osnovu priloženog rezultata testiranja. Dodatno, nezavisna uloga ovjerava početak digitalizacije.

2. Jesu li dokumentirani svi dijelovi procesa:

a) priprema

Točka 8.5.2. opisuje fazu pripreme.

b) skeniranje

Točka 8.5.3. opisuje fazu skeniranja.

c) indeksiranje

Točka 8.5.6. opisuje fazu indeksiranja.

d) kontrola

Kontrola se provodi u nekoliko faza. U fazi skeniranja, točka 8.5.4., operater provodi vizualnu kontrolu. Zatim u fazi indeksiranja, točka 8.5.6., operater provodi dodatnu vizualnu kontrolu. Treća kontrola je kontrola prema definiranim upitima, točka 8.5.7.

e) ponavljanje skeniranja

Točka 8.5.8. govori o ponavljanju skeniranja.

f) isporuka u središnji repozitorij glavnih slika

Nakon obavljenih kontrola, paketi koji su dobili status „OK“ šalju se u sustav za dugoročno očuvanje, točka 8.5.8.

g) izrada revizijskih dnevnika

U revizijski trag, točka 8.18. upisuju se svi podavi nastali u digitalizacijskom procesu.

h) prepoznati su potrebni metapodaci

Svi prepoznati metapodaci popisani su u točki 8.15.

i) prepoznate su korištene aplikacije

Točka 1.16. govori o korištenim aplikacijama i zahtjevima za te aplikacije.

j) korištena infrastruktura (računala i mediji za pohranu)

Točka 8.8. govori o korištenoj infrastrukturi te njezinom propisivanju i evidentiranju.

k) izrada pričuvnih kopija?

U točki 8.17. govori se o izradi pričuvnih kopija.

3. Radi li se test na reprezentativnom uzorku i čuva li se rezultat testa?

Analizom gradiva koje je odabrano za digitalizaciju izrađuje se testni uzorak, točka 8.5.1, koji može zadovoljavajuće predstavljati ukupno gradivo koje se namjerava skenirati. Korak odabira testnog uzorka, opravdanosti za takav odabir i provođenje digitalizacije, se evidentira i zapisan se čuva tijekom cijelog perioda čuvanja dokumenata na koje se testni uzorak odnosi.

4. Jesu li popisani svi tehnički uvjeti:

a) glavna slika

Karakteristike glavne slike su opisane u točki 8.11.

b) izvedena slika

Karakteristike izvedene slike se nalaze navedene u točki 8.5.8.

c) skener

Točka 8.9 govori o karakteristikama skenera.

d) softver za prihvat slike

Softver za prihvat slike je opisan u točki 8.10.

e) pokretački program

Pokretački program je opisan u točki 8.10.

f) aplikacija za pripremu

Točka 1.16. govori o korištenim aplikacijama i zahtjevima za te aplikacije.

g) aplikacija za indeksiranje

Točka 1.16. govori o korištenim aplikacijama i zahtjevima za te aplikacije.

h) aplikacija za kontrolu

Točka 1.16. govori o korištenim aplikacijama i zahtjevima za te aplikacije.

i) aplikacija za slanje na središnji repozitorij

Točka 1.16. govori o korištenim aplikacijama i zahtjevima za te aplikacije.

j) infrastruktura (računala i mediji za pohranu)

Točka 8.8. traži da se svi elementi infrastrukture održavaju u skladu s preporukama proizvođača.

k) korišteno sistemsko vrijeme?

Korišteno vrijeme i datum je opisano u točki 8.13.

5. Postoje li odijeljene uloge za:

a) svaki dio procesa

Točka 8.8. dijeli uloge na procesne, organizacijske, nadzorne, kontrolne i uloge održavanja.

b) nadzora provedbe procesa

Točka 8.8. dijeli uloge na procesne, organizacijske, nadzorne, kontrolne i uloge održavanja.

c) kontrolu procesa?

Točka 8.8. dijeli uloge na procesne, organizacijske, nadzorne, kontrolne i uloge održavanja.

B. Proces je nadziran tijekom digitalizacije i o tome postoje evidencije.

1. Nadzire li se proces?

Točka 8.8. govori kako tijekom cjelokupnog procesa digitalizacije na dnevnom nivou koordinatori nadziru i kontroliraju rad operatera, te tjedno podnose izvještaje o obrađenim paketima, njihovim vremenima i operaterima koji su na njima radili. Na mjesečnom nivou osoba koja je zadužena za proces izrađuje kompletan izvještaj. Dva puta godišnje, ili bar dva puta u toku perioda digitalizacije odabrane dokumentacije, nadzorno tijelo provodi nadzor cijelog sustava, pri čemu provjerava sve izvještaje, rezultat testiranja uzorka dokumentacije te urednost provođenja procesa, odijeljenost uloga i educiranost djelatnika, te izrađuje izvještaj za upravu o zatečenom stanju.

2. Jesu li provedene potrebne edukacije prije početka procesa digitalizacije?

Edukacije se provode prije početka procesa digitalizacije, točka 8.8., ali i tijekom cjelokupnog procesa digitalizacije pri svakoj promjeni.

3. Provode li se potrebne edukacije pri svakoj promjeni?

Edukacije se provode prije početka procesa digitalizacije, točka 8.8., ali i tijekom cjelokupnog procesa digitalizacije pri svakoj promjeni.

4. Postoje li uloge nadzora?

Uloge nadzora su popisane u točki 8.8.

5. Postoje li evidencije provedenih nadzora?

Točka 8.8. govori o evidencijama na dnevnom, tjednom, mjesečnom nivou i dva puta tijekom godine.

6. Dokumentiraju li se sve promjene i dobiva li svaki dokument novu verziju?

Točka 8.7. govori o izradi uputa te evidenciji promjena i vođenju svih verzija dokumenata.

C. Proces je provjeravan tijekom digitalizacije i o tome postoje evidencije.

1. Provjerava li se ili kontrolira proces?

Koordinatori operatera na pripremi, skeniranju i indeksiranju provjeravaju dnevno provođenje procesa te evidentiraju utrošeno vrijeme i obavljeni posao, a jednom tjedno šalju izvještaj, točka 8.8. Kontrola rada skenera se provodi dnevno od strane operatera te prema preporukama proizvođača od strane nezavisnog stručnog i ovlaštenog servisera, točka 8.8.

2. Provodi li se održavanje svih elemenata procesa?

Točka 8.8. govori o održavanju skenera od strane nezavisnog stručnog servisera te o održavanju informacijske infrastrukture koja uključuje računala, računalne mreže, baze podataka i izradu pričuvnih kopija treba biti propisano i provođeno u skladu s preporukama proizvođača, a provode ih osobe zadužene za njihovo održavanje i serviseri.

3. Postoje li uloge kontrole?

Uloge kontrole su popisane u točki 8.8.

4. Postoje li evidencije o provedenim provjerama?

Tijekom cjelokupnog procesa digitalizacije vode se evidencije o održavanju infrastrukture, održavanju skenera, provedenim kontrolama, kako je objašnjeno u točkama 8.8. te 8.5.7.

3. INTEGRITET DOKUMENTA

A. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni od trenutka stvaranja?

Izradom hash rezultata datoteke u trenutku digitalizacije i zapisivanje u revizijski dnevnik provjerava se što je nastalo tijekom digitalizacije. Nakon kontrole i prilikom slanja XML datoteke za metapodatke koji su dobili status „OK“ izrađuje se hash rezultata XML datoteke i upisuje se u revizijski dnevnik. Oba ova dva hash rezultata čuvaju datoteku i metapodatke od promjene, odnosno ukoliko se promjena dogodila hash rezultati će biti različiti što se u koraku periodičke usporedbe može pokazati.

B. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni u trenutku prihvata u središnji repozitorij. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni u trenutku prihvata u središnji repozitorij?

Nakon završenog procesa digitalizacije, u zatvorenom sustavu digitalizacije, izrađuju se hash rezultati slika i podataka u XML datoteci. Ovi hash rezultati se uspoređuju u procesu slanja kako bi se potvrdilo da je sve što je poslano u središnji repozitorij tamo zaista stiglo u nepromijenjenom obliku. Dodatno se potpisuju digitalnim potpisom koji sadrži digitalni certifikat. Potvrdom primanja i validnosti digitalnog potpisa potvrđuje se ispravnost slanja.

4. DOSTUPNOST DOKUMENTA

A. Podacima, oznakama na dokumentu i pripadajućim poveznicama s dokumentom može se ispravno pristupiti, čitati i protumačiti. Može li se ispravno pristupiti, čitati i protumačiti podatke, oznake na dokumentu i pripadajuće poveznice?

Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom se zapisuju u samu datoteku, ali se zapisuju i u bazu podataka. Tijekom koraka kontrole sve slike i metapodaci koji su dobili status „OK“ potvrđuju kako je ovaj zahtjev ispunjen.

11.5. Rezultat analize

Rezultat komparativne analize prikazan je u tablici (tablica 11) u kojoj je ubilježen broj 1 ukoliko se neki element spominje u dokumentima, odnosno 0 ukoliko se ne spominje.

Tablica 11. Rezultat komparativne analize

ZAHTJEV AUTENTIČNOSTI	**PREDLOŽENI MODEL**	**ISO/TR 15801**	**ISO/TR 13028**
1. POTPUNOST			
A. Podaci i oznake su prisutni na dokumentu. Je li napravljena kontrola prisutnosti podataka i oznaka na digitaliziranoj slici?	1	1	0
B. Podaci i oznake su povezani s dokumentom. Postoji li poveznica između podataka i oznaka i digitalizirane slike?	1	0	1
C. Sve stranice dokumenta su snimljene. Jesu li sve stranice dokumenta snimljene?	1	0	0
D. Uključeni su pripadajući dodaci. Jesu li pripadajući dodaci povezani s dokumentom? (Postoji postupanje s dodacima dokumentu kao na primjer dodatni papiri, post-it-i i slično.)	1	1	1
E. Poznat je podatak o stvaratelju. Je li poznat podatak o stvaratelju?	1	0	0

2. POUZDANOST PROCESA			
A. Proces u kojem je dokument nastao je propisan, odobren i ovjeren prije početka digitalizacije.			
1. Postoje li uloge koje propisuju, odobravaju i ovjeravaju proces prije početka digitalizacije?	1	1	0
2. Jesu li dokumentirani svi dijelovi procesa:			
a) priprema	1	1	1
b) skeniranje	1	1	0
c) indeksiranje	1	1	0
d) kontrola	1	1	1
e) ponavljanje skeniranja	1	1	1
f) isporuka u središnji repozitorij glavnih slika	1	1	0
g) izrada revizijskih dnevnika	1	1	0
h) prepoznati su potrebni metapodaci	1	0	1
i) prepoznate su korištene aplikacije	1	1	0
j) korištena infrastruktura (računala i mediji za pohranu)	1	1	0
k) izrada pričuvnih kopija?	1	1	1
3. Radi li se test na reprezentativnom uzorku?	1	0	1
4. Jesu li popisani svi tehnički uvjeti:			
a) glavna slika	1	1	1
b) izvedena slika	1	1	1
c) skener	1	0	0
d) softver za prihvat slike	1	1	0
e) pokretački program	1	0	0
f) aplikacija za pripremu	1	0	0
g) aplikacija za indeksiranje	1	0	0
h) aplikacija za kontrolu	1	0	0
i) aplikacija za slanje na središnji repozitorij	1	0	0
j) infrastruktura (računala i mediji za pohranu)	1	1	0
k) korišteno sistemsko vrijeme?	1	1	0
5. Postoje li odijeljene uloge za:			
a) svaki dio procesa	1	1	1
b) nadzora	1	1	1
c) kontrole?	1	1	1
B. Proces je nadziran tijekom digitalizacije i o tome postoje evidencije.			
7. Nadzire li se proces?	1	0	0
8. Jesu li provedene potrebne edukacije prije početka procesa digitalizacije?	1	1	1
9. Provode li se potrebne edukacije pri svakoj promjeni?	1	1	0
10. Postoje li uloge nadzora?	1	1	1
11. Postoje li evidencije provedenih nadzora?	1	0	0
12. Dokumentiraju li se sve promjene i dobiva li svaki dokument novu verziju?	1	1	0
C. Proces je provjeravan tijekom digitalizacije i o tome postoje evidencije.			

5. Provjerava li se ili kontrolira proces?	1	1	0
6. Provodi li se održavanje svih elemenata procesa?	1	1	0
7. Postoje li uloge kontrole?	1	1	1
8. Postoje li evidencije o provedenim provjerama?	1	1	0
3. INTEGRITET DOKUMENTA			
A. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni od trenutka stvaranja dokumenta. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni od trenutka stvaranja?	1	1	0
B. Podaci, oznake na dokumentu i pripadajuće poveznice s dokumentom nisu promijenjeni u trenutku prihvata u središnji repozitorij. Postoji li dokaz da podaci, oznake na dokumentu i pripadajuće poveznice nisu promijenjeni u trenutku prihvata u središnji repozitorij?	1	1	0
4. DOSTUPNOST DOKUMENTA			
A. Podacima, oznakama na dokumentu i pripadajućim poveznicama s dokumentom može se ispravno pristupiti, čitati i protumačiti. Može li se ispravno pristupiti, čitati i protumačiti podatke, oznake na dokumentu i pripadajuće poveznice?	1	1	1
UKUPNO	45	32	17

11.6. Zaključak

Napravljena je komparativna analiza predloženog *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* i dvije prepoznate norme tehničkih izvještaja ISO/TR 15801:2009 Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost i ISO/TR 13028:2010 Informacije i dokumentacije - Implementacijske smjernice za digitalizaciju koje govore o stvaranju autentičnih digitaliziranih slika. Analiza pokazuje različite stupnjeve povezanosti. Za postizanje predložene definicije autentičnosti postoji 45 zahtjeva koje je potrebno zadovoljiti. Tehnički izvještaj ISO/TR 15801:2009 zadovoljava 32 zahtjeva. S druge strane tehnički izvještaj ISO/TR 13028:2010 zadovoljava 17 zahtjeva. Ovi rezultati pokazuju kako je, za punu primjenu ovdje izrađenog i predloženog modela, uz korištenje spomenutih normi potrebno ugraditi dodatne kontrole i njihove evidencije kojima se osigurava dovoljna količina podataka kojima se može pokazati da je stvorena digitalizirana slika autentična digitalna kopija. Korištenjem predloženog modela ostvaruje se temeljna podloga za ovjeravanje

ispisanog dokumenta kao jednakovrijednog izvorniku. Detaljniji opis uvjeta za ispis jednakovrijednom izvorniku navodi se u poglavlju 12.

12. UVJETI ZA ISPIS JEDNAKOVRIJEDAN IZVORNIKU

Digitalizacijom prema predloženom *Modelu procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* može se postići da se svi digitalizirani dokumenti mogu smatrati autentičnima i da se nakon digitalizacije analogni originali mogu nesmetano uništiti. Nakon uništenja izvornih dokumenata ostat će dostupne autentične digitalizirane kopije u obliku originala tih dokumenata. Pod kojim se uvjetima kasnije mogu digitalni i digitalizirani dokumenti ispisati iz repozitorija kao dokumenti koji će se po svojim svojstvima moći smatrati jednakovrijednima uništenim izvornicima?

Prema Rječniku stranih riječi termin *ekvivalent* označava „isto značenje, jednaku ili istu vrijednost, stvar iste vrijednosti ili zamjenu za vrijednost, odštetu, naknadu“[281]. Riječ potječe od latinske riječi *aequivalens* gdje *aequi* znači jednako, dok *valere* znači vrijediti. Rječnik daje primjer mehaničkog ekvivalenta topline. To je „količina rada koja je jednaka količini topline potrebne da se 1 kg vode (kilogram-kalorija) zagrije za 1°C“[282]. Hrvatski leksikon daje sljedeće tumačenje: "ekvivalent (lat.), stvar, pojam, čin iste praktične vrijednosti, veličina po vrijednosti jednaka kojoj drugoj veličini. U matematici za skup A kažemo da je ekvivalentan skupu B kada je ispunjeno da svi elementi iz skupa A se mogu preslikati u različite elemente skupa B i oba skupa imaju jednak broj elemenata“[283]. Prema tome ekvivalent i jednakovrijedan su sinonimi.

Kako odrediti svojstva po kojima bi se dokument ispisan na papiru izjednačio sa svojstvima dokumenta u digitalnom ili digitaliziranom obliku? Iz procesa digitalizacije može se vidjeti da osim digitalizirane slike sam dokument opisuju određeni metapodaci, kao što su to stvaratelj, metapodaci iz procesa digitalizacije, metapodaci koji opisuju dokument iz procesa klasifikacije i prihvata dokumenta. Prilikom ispisa svi ovi podaci trebaju biti prisutni, bilo na slici, bilo kao dodatni dokument s cjelokupnim popisom neovisno o tome nalaze li se ti podaci na samoj slici ili ne. Dakle, prilikom ispisa dokumenta potrebno je ispisati i popratne metapodatke koji se nalaze u sustavu. Isto to vrijedi i za dokument koji je izvorno nastao u digitalnom obliku.

Ostaje otvoreno pitanje kako vjerovati ispisanom dokumentu. Kako vjerovati izvoru koji je dokument ispisao, odnosno kako biti siguran u izvornost ispisanog dokumenta. Tu nam može pomoći ukoliko se prilikom ispisa iskoristi tehničko rješenje mikroprint. Iz poglavlja o

[281] Domović, Ž., Klaić, N., & Anić, Š. (1998). Rječnik stranih riječi : tuđice, posuđenice, izraci, kratice i fraze. Zagreb: Sani-plus.
[282] ibid.
[283] Ekvivalent značenje. (n.d.). Preuzeto 9. 3. 2018. iz Hrvatski leksikon.

mikroprintu jasno je da je riječ o tako malom fontu koji nije moguće drugim postupcima, na primjer skeniranja ili fotokopiranja, promijeniti. U mikroprint obliku mogu se nalaziti ispisani podaci o sustavu koji je ispisao dokument, osobi koja je dokument ispisala, te podaci koji omogućavaju pronalazak dokumenta sa svim metapodacima u tom sustavu. Dodatno se može ugraditi digitalni certifikat, ili elektronička vjerodajnica kao u primjeru eGrađani, za prijavu u sustav. Podatak o osobi koja se prijavila i ispisala dokument se upisuje kao jedan od podataka u mikroprint obliku.

13. ZAKLJUČAK

Cilj doktorske disertacije bio je izrada *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* te određivanje uvjeta za dobivanje autentičnih kopija nastalih digitalizacijom izvornika u fizičkom obliku. Ovaj cilj postignut je definiranjem zahtjeva autentičnosti, a to su potpunost dokumenta, pouzdanost procesa, integritet dokumenta i dostupnost dokumenta. Temeljem ovih zahtjeva izrađen je *Model procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije*.

Istraživačka pitanja za izradu Modela bila su:

1. Pod kojim se uvjetima digitalnu kopiju dokumenta može smatrati jednakovrijednom izvorniku?

Digitalna kopija dokumenta koja je izrađena korištenjem predloženog *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* može se smatrati jednakovrijednom izvorniku jer je izrađena zadovoljavanjem zahtjeva za autentičnošću koji uključuju: propisane, ovjerene i odobrene procedure i upute korištenih koraka digitalizacije, karakteristike skenera, glavne slike, pokretačkog programa i softvera za digitalizaciju, potrebnih metapodataka kojima se objašnjava kontekst digitaliziranog dokumenta, korištenih aplikacija i repozitorija podataka, provedbenih, kontrolnih i nadzornih uloga i revizijskih tragova provedenih aktivnosti unutar procesa digitalizacije.

2. Postoji li korelacija između definiranih uvjeta i normi koje se odnose na pojedine sastavnice zapisa i procesa sa zapisom?

Za postizanje predložene definicije autentičnosti Modelom se definira 45 zahtjeva koje je potrebno zadovoljiti. Komparativnom analizom predloženog *Modela procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* i tehničkih izvještaja ISO/TR 15801:2009 Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost i ISO/TR 13028:2010 Informacije i dokumentacije - Implementacijske smjernice za digitalizaciju utvrđeno je da postoje određene zajedničke ili slične značajke kao i razlike između definiranih uvjeta u Modelu i prepoznatih normi. Tehnički izvještaj ISO/TR 15801:2009 zadovoljava 32 zahtjeva, a ISO/TR 13028:2010 zadovoljava 17 zahtjeva.

3. Pod kojim se uvjetima digitalni i digitalizirani dokument može ispisati kao dokument koji se po svojim svojstvima smatra jednakovrijednim izvorniku?

Digitaliziranu sliku prate metapodaci koji određuju kontekst. Prilikom ispisa digitaliziranog dokumenta potrebno je ispisati i ove metapodatke. Isto vrijedi i za dokument koji je nastao digitalno, odnosno pored njegovog ispisa potrebno je ispisati i kontekstualne metapodatke. Pored ovog uvjeta potrebno je dodati uvjet kojim se postiže vjerodostojnost ispisanog dokumenta. Taj uvjet se ispunjava ispisivanjem u mikroprint obliku podataka o sustavu koji je ispisao dokument, podatka o osobi koja je dokument poslala na ispis i podatka koji omogućava pronalazak dokumenta u sustavu.

Znanstveni doprinos na metodološkoj razini predstavlja razvijeni *Model procesa stvaranja autentičnih digitalnih kopija u obliku originala postupkom digitalizacije* te definirani uvjeti za izradu autentičnih kopija digitalizacijom. Na teorijskoj razini doprinos je u razvoju percepcije pojma autentičnosti. Doprinos na praktičnoj razini može se vidjeti kroz daljnju upotrebu i primjenu konkretnih zahtjeva i predloženog Modela.

14. LITERATURA

1. Angeles, C. N. (n.d.). Standards and Procedure in Digitization and Digital Preservation. Preuzeto 30.. 9. 2016. iz https://paarl.wikispaces.com/file/view/Standards+and+Procedure+in+Digitization+and+Digital+Preservation.pdf
2. Barrister, S. M. (2006.). Proof of the authenticity of a Document in electronic format Introduced as evidence. Preuzeto 30. 9. 2016. iz ARMA International Educational Foundation: http://www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/Proof_of_authenticity_of_a_document.pdf
3. Butcher, K., Crown, L., & Gentry, E. J. (5. 2006.). The International System of Units (SI) – Conversion Factors for General Use. Preuzeto 23. 3. 2017. iz NIST: https://www.gpo.gov/fdsys/pkg/GOVPUB-C13-f10c2ff9e7af2091314396a2d53213e4/pdf/GOVPUB-C13-f10c2ff9e7af2091314396a2d53213e4.pdf
4. Buyers Laboratory Inc., NJ, USA. (2006.). Digital Imaging REVIEW, vol. 28. NO. 10. Preuzeto 16. 3. 2017. iz Fujitsu: http://www.fujitsu.com/downloads/COMP/fcpa/reviews/market-roundup-1006.pdf
5. Camera & Imaging Products Association. (2010.). Standard of the Camera & Imaging Products Association, CIPA DC-008-Translation-2012, Exchangeable image file format for digital still cameras: Exif Version 2.3. Preuzeto 24. 3. 2017. iz http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf
6. CANON. (2007.). Canon CAPTUREPERFECT 3.1 Operation Manual. Preuzeto 24. 3. 2017. iz manualslib the ultimate manuals library: https://www.manualslib.com/manual/24880/Canon-Captureperfect-3-1.html
7. CARNet CERT i LS&S. (2007.). RFID identifikacija, CCERT-PUBDOC-2007-01-179. Preuzeto 21. 3. 2017. iz https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-01-179.pdf
8. Dalby, S. (December 2004). Authenticity/Authentication Definitions and Sources. Preuzeto 30. 9. 2016. iz InterPARES 2 Project:

http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity_definitions-sources.pdf

9. Deegan, M., & Tanner, S. (2002.). Digital futures : strategies for the information age. New York : London: Neal-Schuman Publishers, Library Association Publishing,.
10. Domović, Ž., Klaić, N., & Anić, Š. (1998). Rječnik stranih riječi : tuđice, posuđenice, izraci, kratice i fraze. Zagreb: Sani-plus.
11. Duranti, L. (1995). Reliability and Authenticity: The Concepts and Their Implications. Preuzeto 1. 2018. iz Archivaria: https://archivaria.ca/index.php/archivaria/article/download/12063/13035
12. Duranti, L. (2005.). Authenticity and Authentication in the Law, InterPares 2 Project. Preuzeto 30.. 9. 2016. iz http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf
13. Đurek, I. (8. 6. 2002.). DIGITALIZACIJA SVJETLA. Preuzeto 20. 3. 2017. iz Filos: http://www.filos.com/mkrzak/Djurek1.doc
14. EasyCalculation.com. (n.d.). LPI To DPI Converter. Preuzeto 9.. 2. 2018. iz EasyCalculation.com: https://www.easycalculation.com/unit-conversion/lpi-to-dpi-converter.php
15. eIDAS, UREDBA (EU) br. 910/2014 EUROPSKOG PARLAMENTA I VIJEĆA. (23. 7. 2014.).
16. Ekvivalent značenje. (n.d.). Preuzeto 9. 3. 2018. iz Hrvatski leksikon.
17. Fundamental principles of digitization of documentary heritage. (n.d.). Preuzeto 30.. 9. 2016. iz http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/digitization_guidelines_for_web.pdf
18. Golowczynski, M. (20. 1. 2016.). Digital camera sensors explained. Preuzeto 20. 3. 2017. iz WHAT DIGITAL CAMERA: http://www.whatdigitalcamera.com/technical-guides/technology-guides/sensors-explained-11457
19. Government of Alberta. (1. 3. 2013.). Digitization Standard Process. Preuzeto 30. 9. 2016. iz Government of Alberta: http://imtdocs.alberta.ca/A000015_Digitization_Standard_v3.pdf
20. Government of Alberta. (1. 3. 2013.). Digitization Technical Requirements, Standard number A000013. Preuzeto 30. 9. 2016. iz http://imtdocs.alberta.ca/A000013_Digitization_Standards_Technical_v3.pdf

21. HNB. (1. 2. 2015.). Novac»Novčanice»Nevažeće novčanice»10 kuna. Preuzeto 23. 3. 2017. iz HNB: URL: https://www.hnb.hr/-/10-kuna, objavljeno 13.6.2015.
22. HRN ISO 11799:2004 – Informacije i dokumentacija – Zahtjevi za pohranu dokumenata arhivske i knjižnične građe. (2004).
23. HRN ISO/IEC 27001:2006 Sustavi upravljanja informacijskom sigurnošću - Zahtjevi. (2006).
24. InterPares. (n.d.). Authenticity Task Force Report. Preuzeto 30.. 9. 2016. iz http://interpares.org/book/interpares_book_d_part1.pdf
25. ISO 15489-1:2001 - Informacije i dokumentacija - Upravljanje zapisima - 1. dio: Općenito. (2001).
26. ISO 19005-1:2005 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 1. dio: Korištenje PDF 1.4 (PDF/A-1). (2005).
27. ISO 19005-2:2011 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 2. dio: Korištenje ISO 32000-1 (PDF/A-2). (2011).
28. ISO 19005-3:2012 Upravljanje dokumentima – elektronički format dokumenta za dugoročno očuvanje – 3. dio: Korištenje ISO 32000-1 s podrškom za sadržane datoteke (PDF/A-3). (2012).
29. ISO/TR 13028:2010 Informacije i dokumentacije - Implementacijske smjernice za digitalizaciju. (2010).
30. ISO/TR 15498-2:2001 Informacije i dokumentacija – Upravljanje zapisima – Drugi dio: Smjernice. (2001).
31. ISO/TR 15801:2009 Upravljanje dokumentima - Elektronički pohranjeni podaci - Preporuke za pouzdanost i vjerodostojnost. (2009).
32. ISO-14524 Ddigital camera contrast chart. (n.d.). Preuzeto 9. 3. 2017. iz Sine Image: http://www.sineimage.com/en/ImageTest/Test_Charts/ISO_Test_Charts/ISO-14524.html
33. ISO-15739 Digital camera noise test chart. (n.d.). Preuzeto 9. 3. 2017. iz Sine Image: http://www.sineimage.com/en/ImageTest/Test_Charts/ISO_Test_Charts/38.html
34. ISO-16067-1 Scanner Test Chart. (n.d.). Preuzeto 9. 3. 2017. iz APPLIED IMAGE Inc: https://www.appliedimage.com/files/wFsNSe/QA-61_spec_v1-08.pdf
35. ISO-21550 Dynamic Range. (n.d.). Preuzeto 9. 3. 2017. iz PRECISION OPTICAL IMAGING: http://www.precisionopticalimaging.com/products/products.asp?type=21550

36. Janich & Klass Computertechnik GmbH. (2010.). User Manual, DpuScan 5, Document Scanning and Document Processing. Preuzeto 24. 3. 2017. iz Dpuscan: http://www.dpuscan.de/pdf/DpuScan-User-Manual.pdf
37. Janich & Klass Computertechnik GmbH. (n.d.). Getting Started. Preuzeto 24. 3. 2017. iz Dpuscan: URL:http://www.dpuscan.de/pdf/GettingStarted.pdf
38. Janich & Klass Computertechnik GmbH. (n.d.). We made Document Capture Easy and Efficient: DpuScan 4.0, The universal Scan Sotfware for Color and black/white. Preuzeto 24. 3. 2017. iz Dpuscan: http://www.dpuscan.de/pdf/DpuScan-Brochure-english.pdf
39. Katedra za materijale u grafičkoj tehnologiji. (n.d.). RFID tehnologija. Preuzeto 21. 3. 2017. iz Grafički fakultet – Sveučilište u Zagrebu: http://materijali.grf.unizg.hr/media/RFID%20tehnologija.pdf
40. Khanna, N., Mikkilinenib, A. K., Chiub, G. T., Allebacha, J. P., & Delpa, E. J. (2007.). Forensic Classification of Imaging Sensor Types. Preuzeto 14. 3. 2017. iz SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents: https://engineering.purdue.edu/~prints/public/papers/ei07-nitin1.pdf
41. Kirasić, D. (n.d.). XML tehnologija i primjena u sustavima procesne informatike. Preuzeto 20. 3. 2017. iz IEEE Hrvatska sekcija: http://www.ieee.hr/_download/repository/mipro_xml_tekst.pdf
42. Kriteriji za određivanje razine osiguranja kvalitete autentifikacije za Nacionalni identifikacijski i autentifikacijski sustav (NIAS), verzija 1.2. (6. 12. 2013.). Preuzeto 24. 3. 2017. iz Projekt e-Građani: https://gov.hr/UserDocsImages//e-Gradjani_dok//NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2).pdf
43. Leksikografski zavod Miroslav Krleža. (n.d.). Digitaliizacija. Preuzeto 13. 1. 2018. iz Hrvatska enciklopedija: http://www.enciklopedija.hr/natuknica.aspx?id=68025
44. Lista prihvaćenih vjerodajnica, e-Građani. (n.d.). Preuzeto 24. 3. 2017. iz Središnji državni portal: https://gov.hr/e-gradjani/lista-prihvacenih-vjerodajnica/1667
45. Lumis. (7. 5. 2015.). Koja je razlika između načina rada CMOS i CCD senzora? Preuzeto 17. 3. 2017. iz Lumis: https://lumis.hr/clanci/tehnologija/koja-je-razlika-izmedu-nacina-rada-cmos-i-ccd-senzora/
46. McKenna, G., & De Loof, C. (2009.). Digitisation : standards landscape for European museums, archives, libraries, ATHENA project.

47. MEĐUNARODNO ARHIVSKO VIJEĆE. (2001.). ISAD (G) - OPĆA MEĐUNARODNA NORMA ZA OPIS ARHIVSKOGA GRADIVA. (Drugo izdanje). Zagreb. Preuzeto 15. 3. 2017. iz http://zagreb.arhiv.hr/hr/pdf/
48. Metcalf, K. D. (3. 1945.). The Promise of Microprint, A Symposium Based on The Scholar and the Future of the Research Library. Preuzeto 23. 3. 2017. iz COLLEGE AND RESEARCH LIBRARIES: https://www.ideals.illinois.edu/bitstream/handle/2142/35340/crl_06_02_170_opt.pdf?sequence=2
49. Mihaljević, M., Mihaljević, M., & Stančić, H. (2015). Arhivistički rječnik. Zagreb: Zavod za informacijske studije Odsjeka za informacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.
50. Nikitin, P. V., Rao, K. V., & Lazar, S. (2007.). An Overview of Near Field UHF RFID. Preuzeto 21. 3. 2017. iz https://www2.ee.washington.edu/people/faculty/nikitin_pavel/papers/RFID_2007.pdf
51. O sustavu e-Građani. (n.d.). Preuzeto 23. 3. 2017. iz Središnji državni portal: https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584
52. Peterson, A. K. (2004.). Standards Related to Digital Imaging of Pictorial Materials. Preuzeto 30. 9. 2016. iz Library of Congress, Washington, D.C.: http://www.loc.gov/rr/print/tp/DigitizationStandardsPictorial.pdf
53. Piasecki, S. J. (1995). Legal Admissibility of Electronic Records as Evidence and Implications for Records Management. Preuzeto 30. 9 2016 iz American Archivist: http://americanarchivist.org/doi/pdf/10.17723/aarc.58.1.h715312706n38822
54. Piql AS. (n.d.). Creating the ultimate digital insurance, Behind the curtains, Rev. 150306. Preuzeto 9. 11. 2016. iz https://slidex.tips/download/creating-the-ultimate-digital-insurance
55. Piql AS. (n.d.). Piql Archival Storage Format, Product Data Sheet, Rev. 150306. Preuzeto 9. 11. 2016. iz https://www.piql.com/
56. Ponovna uporaba informacija. (n.d.). Preuzeto 20. 1. 2018. iz Institut za javne financije: http://www.ijf.hr/hr/o-institutu/pravo-na-pristup-informacijama/652/ponovna-uporaba-informacija/673/
57. Pravilnik o evidencijama u arhivima. (26. 7. 2002.). (NN 90/2002, NN 106/2007).
58. Pravilnik o korištenju arhivskoga gradiva. (23. 6. 1999.). (NN 67/1999).
59. Pravilnik o predaji arhivskoga gradiva arhivima. (12. 7. 2002.). (NN br. 90/02).

60. Pravilnik o sadržaju i načinu vođenja muzejske dokumentacije o muzejskoj građi. (16. 9. 2002.). (NN 108/2002).
61. Pravilnik o uvjetima i načinu ostvarivanja uvida u muzejsku građu i muzejsku dokumentaciju. (21. 12. 2001.). (NN 115/2001).
62. Pravilnik o uvjetima smještaja, opreme, zaštite i obrade arhivskog gradiva, broju i strukturi stručnog osoblja arhiva. (11. 5. 2004.). (NN 65/04).
63. Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva. (26. 7. 2002.). (NN 90/2002).
64. Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan ARHIVA. (19. 5. 2004.). (NN 63/04).
65. Pravilnik o zaštiti knjižnične građe. (22. 4. 2005.). (NN 52/2005).
66. PRECISION OPTICAL IMAGING. (n.d.). Preuzeto 9. 3. 2017. iz http://www.precisionopticalimaging.com/products/products.asp?type=21550
67. Public Record Office Victoria. (January 2010). Evidence and Electronic Public Records. Preuzeto 30. 9. 2016. iz State of Victoria, Australia: http://studylib.net/doc/18578486/evidence-and-electronic-public-records
68. Rajh, A., & Šimundža-Perojević, Z. (2015.). Digitalizacija, prihvat i migracija gradiva u sustav upravljanja zapisima sa ciljevima ostvarivanja temeljnih funkcija HALMED-a i očuvanja gradiva. (S. Babić, Ur.) Radovi 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, 21.-23. listopada 2015., Topusko, str. 213-228.
69. Rajh, A., & Šimundža-Perojević, Z. (2016.). Koncepti rada s metapodatcima nastalima u procesima digitalizacije. (S. Babić, Ur.) Radovi 49. savjetovanja hrvatskih arhivista Arhivi i domovinski rat, Plitvice 26.-28. listopada 2016., str. 389-404.
70. ScandAll PRO V2.0 User's Guide. (6. 2012.). Preuzeto 24. 3. 2017. iz PFU LIMITED: URL: http://origin.pfultd.com/downloads/IMAGE/manual/p2ww-2860-03enzo.pdf
71. ScanTastik. (n.d.). High Speed Scanners. Preuzeto 9. 3. 2018. iz http://www.scantastik.com/high-speed-scanners.htm
72. SkyRFID inc. (n.d.). RFID Tag Maximum Read Distance. Preuzeto 21. 3. 2017. iz http://skyrfid.com/RFID_Tag_Read_Ranges.php
73. Smiley, S. (2016.). Active RFID vs. Passive RFID: What's the Difference. Preuzeto 21. 3. 2017. iz RFID INSIDER TRACKING THE RFID INDUSTRY: http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid
74. Stančić, H. (2005). Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata, Doktorska disertacija. Zagreb.

75. Stančić, H. (2009). Digitalizacija. U H. Stančić, Digitalizacija. Zagreb: Zavod za informacijske studije Odsjeka za informacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.
76. Technical Standards for Digital Conversion Of Text and Graphic Materials. (3. 7. 2007.). Preuzeto 30. 9. 2016. iz The Library of Congress: http://memory.loc.gov/ammem/about/techStandards.pdf
77. The Library of Congress Technical Standards for Digital Conversion Of Text and Graphic Materials. (7. 3. 2007.). Preuzeto 30. 9. 2016. iz http://memory.loc.gov/ammem/about/techStandards.pdf
78. The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project – Authenticity Task Force Report. (n.d.). Dohvaćeno iz http://www.interpares.org/book/index.htm
79. UCONN College of Liberal Arts and Sciences, Biology Central Services. (n.d.). Scanning and scanners. Preuzeto 20. 3. 2017. iz Scanner Resolutions: http://www.bcs.uconn.edu/Illustration/content/Scanners_Resolution.pdf
80. Učestala pitanja i odgovori, verzija 1.0. (2014.). Preuzeto 24.. 3. 2017. iz Projekt e-Građani: https://www.gov.hr/UserDocsImages//e-Gradjani_dok/korisnicka_dokumentacija//2014-06-24-FAQ-e-Gradjani.pdf
81. UNIS. (n.d.). Preuzeto 20. 3. 2017. iz https://www.unis.hr/pogodnosti.html
82. UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. (27. 4. 2016.). (L 119/1), Službeni list Europske unije.
83. Valkaj, T. (24. 6. 2017.). Provjerite rok trajanja vaših certifikata za fiskalizaciju. Preuzeto 10. 1. 2018. iz Narodni list: URL: http://www.narodni-list.hr/posts/338405001
84. VIDEOJET. (31. 3. 2015.). New Videojet Continuous Inkjet Printers Meet Micro Printing Needs. Preuzeto 23. 3. 2017. iz Recent Press Release: http://www.videojet.com/us/homepage/general/news/new-videojet-continuous-inkjet-printers-meet-micro-printing-needs.html
85. Vlada Republike Hrvatske. (4. 2017.). Prijedlog Zakona o arhivskom gradivu i arhivima. Preuzeto 10.. 3. 2018. iz e-Savjetovanja: https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=5123

86. VOI - Verband Organisations- und Informationssysteme e.V. (March 2010). Legal Requirements for Document Management in Europe. Dohvaćeno iz http://www.tech-arrow.com/wp-content/uploads/2015/01/legal-requirements-for-dms-in-eu1.pdf
87. Xerox. (2013). Specialty Imaging Text. Preuzeto 22. 3. 2017. iz The sensible way to affordably secure your documents: https://www.xerox.com/digital-printing/latest/FFSBR-47U.pdf
88. Xerox. (n.d.). Xerox Scientists Develop Microtext Font; Digitally Printing Tiny Words And Numbers Will Help Make, Documents More Secure. Preuzeto 22. 3. 2017. iz Innovation Home › Innovation Stories: https://www.xerox.com/innovation/news-stories/microtext/enus.html
89. Zakon o arhivskom gradivu i arhivima. (29. 09. 1997.). (NN 105/97, 64/00, 65/09, 125/11, 46/17).
90. Zakon o autorskom pravu i srodnim pravima. (8. 7. 2017.). (NN 167/03, 79/07, 80/11, 125/11, 141/13, 127/14, 62/17).
91. Zakon o elektroničkoj ispravi. (9. 12. 2005.). (NN 150/05).
92. Zakon o elektroničkoj trgovini. (6. 3. 2014.). (NN 173/03, 67/08, 36/09, 130/11, 30/14).
93. Zakon o elektroničkom potpisu. (6. 3. 2014.). (NN 10/02, 80/08, 30/14).
94. Zakon o knjižnicama. (25. 6. 2009.). (NN 105/97, 05/98, 104/00, 69/09).
95. Zakon o muzejima. (21. 10. 2015.). (NN 110/15).
96. Zakon o pravu na pristup informacija. (9. 8. 2015.). (NN 25/13, 85/15).
97. Zakon o zaštiti osobnih podataka. (12. 6. 2003.). (NN 103/03, 118/06, 41/08, 130/11, 106/12).

Sve internetske poveznice su bile ispravne u trenutku predaje rada.

15. POPIS SLIKA

Slika 1. Hijerarhijski model razina sređivanja 98
Slika 2. Model stvaranja slike digitalnim fotoaparatom 102
Slika 3. Blok točaka RGB i CMYK 102
Slika 4. Proces stvaranja slike kod plošnog skenera 103
Slika 5. Kontrolni uzorak ISO-15739 za testiranje šuma digitalnog fotoaparata..... 116
Slika 6. Kontrolni uzorak ISO-14524 za testiranje kontrasta digitalnog fotoaparata 116
Slika 7. Kontrolni uzorak ISO-16067-1 za test skenera..... 116
Slika 8. Kontrolni uzorak ISO 21550 za provjeru raspona tonske dinamike..... 116
Slika 9. RFID sustav..... 133
Slika 10. RFID odzivnik..... 134
Slika 11. Tijek procesa stvaranja i pohrane Piql trake 143
Slika 12. Digitalni okvir podataka. Desno je uvećani dio okvira..... 144
Slika 13. Okvir podataka na mikrofilmskom svitku 144
Slika 14. Proces čitanja i "sklapanja" originalne datoteke 145
Slika 15. Model metapodataka nakon pripreme podataka 147
Slika 16. Raspored na svitku..... 148
Slika 17. Raspored okvira 149
Slika 18. Novčanica od 10 kn..... 161
Slika 19. Primjer XML datoteke 166
Slika 20. Vodeći list 170
Slika 21. Dokumentacijska cjelina..... 185
Slika 22. Digitalizirana kopija..... 186
Slika 23. Zatvoreni sustav digitalizacije..... 193

16. POPIS TABLICA

Tablica 1. Tehničke specifikacije prihvatljivih formata 111
Tablica 2. Biografski podaci 112
Tablica 3. Bibliografski podaci 113
Tablica 4. Zahtjevi po tipovima dokumenta 117
Tablica 5. Kompresija i ton boje po tipovima datoteke 125
Tablica 6. Popis korištenih oznaka za tip datoteke TIFF 137
Tablica 7. Lista prihvaćenih vjerodajnica 158
Tablica 8. Funkcije poboljšanja slike i učinak 198
Tablica 9. Izvadak iz EXIF standarda 201
Tablica 10. Obrazac s pitanjima za usporedbu autentičnosti 209
Tablica 11. Rezultat komparativne analize 242

17. POPIS DIJAGRAMA

Dijagram 1. Kretanje fizičkog papira od stvaranja do uništenja 24
Dijagram 2. Proces digitalizacije 31
Dijagram 3. Proces uništenja..... 34

Životopis

Edvin Buršić rođen je 23. svibnja 1975. u Puli gdje završava osnovnu i upisuje srednju školu koju završava u Sjedinjenim Američkim Državama. Fakultetsko obrazovanje stječe u Zagrebu na Prirodoslovno-matematičkom fakultetu 2000. godine na smjeru Računarstvo. Svoje daljnje obrazovanje produbljuje raznim radionicama i seminarima, kao što su komunikacijske vještine, govorničke vještine, timski rad te administracija mreža, Windows Servera 2003, SQL Servera 2005, te administrator specijalist za rad s Kodak Archive Writerom. Doktorski studij upisuje 2012. godine na Filozofskom fakultetu na Odsjeku za komunikacijske i informacijske znanosti.

Radni vijek započinje u Financijskoj agenciji godine 2002. kao programer u programskom jeziku 4. generacije jezika LINC II i rad s bazom DMS II te održavanju sustava u Centru NKS. Na mjesto Voditelja Odjela za projektiranje i podršku arhivskih sustava u Arhivsko dokumentacijskom centru prelazi 2007.godine, gdje je zadužen za obavljanje arhivskih poslova kao što su izrada elektroničkih web arhiva i portabilnih arhiva, obrada papirnate dokumentacije u elektroničku te izrada mikrofilmskih svitaka obrađene dokumentacije, skeniranje velikih volumena dokumentacije, unos podataka i digitalizacija, pohrana izvorne dokumentacije, održavanje pomoćnih sustava i slično.

Godine 2010. prelazi u Arhivsko dokumentacijski centar nadalje radeći kao viši specijalist za tehnologiju na poslovima tehnologa, prodajnog predstavnika, kontakta s klijentima, pisanja ponuda, suradnje s pravnom službom na pisanju ugovora, pisanje zahtjeva za nabavom potrošnog materijala i održavanja opreme u suradnji sa službom nabave, certificiranje prostora prema zahtjevu Hrvatskog državnog arhiva, praćenje uspješnosti radnika, poslovima reinženjeringa postojećih sustava, pisanje natječaja za razne nove projekte u suradnji s upravom i nadležnim direktorima, obuka tj. uvođenje u rad novih djelatnika na poslovima arhiviranja, te držanja prezentacija rada Centra na polju digitalizacije i mikrofilmiranja širom Republike Hrvatske.

Svoj rad u smjeru arhivistike produbljuje sudjelovanjem na godišnjem savjetovanju Hrvatskog arhivističkog društva i Državnog arhiva, te izlaganjima na temu digitalnih vodenih žigova i sigurnosti pohrane arhivskih zapisa u Cloud okruženju. Kao istraživač sudjeluje kao dio europskog istraživačkog tima na međunarodnom projektu InterPARES Trust – Trust and

Digital Records in an Increasingly Networked Society od 2013. do 2018. godine, http://interparestrust.org.

POPIS RADOVA:

1. Stančić, Hrvoje; Al-Hariri, Adam; Buršić, Edvin. Archival Approach to IaaS Cloud Services // Central European Conference on Information and Intelligent Systems (CECIIS 2014): proceedings / Hunjak, Tihomir; Lovrenčić, Sandra; Tomičić, Igor (ur.). Varaždin : Faculty of Organization and Informatics Varaždin, University of Zagreb, 2014. 216-222 (predavanje, međunarodna recenzija, objavljeni rad, znanstveni).
2. Stančić, Hrvoje; Al-Hariri, Adam; Buršić, Edvin. Osiguranje povjerenja u pohranu u IaaS-u // (neobjavljeni rad, stručni).
3. Stančić, Hrvoje; Al-Hariri, Adam; Buršić, Edvin. Trust in Storage in Infrastructure-as-a-Service // (predavanje, neobjavljeni rad).
4. Stančić, Hrvoje; Rajh, Arian; Buršić, Edvin. Using Archival Information Packages for production of sustainable archival collections of digitised records // (predavanje, neobjavljeni rad, znanstveni).