Sveučilište u Zagrebu

Filozofski fakultet

Hrvoje Brzica

KONCEPT USPOSTAVE ELEKTRONIČKOGA ARHIVA U JAVNOJ UPRAVI

DOKTORSKI RAD

Zagreb, 2018.

Sveučilište u Zagrebu

Filozofski fakultet

Hrvoje Brzica

KONCEPT USPOSTAVE ELEKTRONIČKOGA ARHIVA U JAVNOJ UPRAVI

DOKTORSKI RAD

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

Zagreb, 2018.

University of Zagreb

Faculty of Humanities and Social Sciences

Hrvoje Brzica

THE CONCEPT OF ESTABLISHMENT OF ELECTRONIC ARCHIVE IN PUBLIC ADMINISTRATION

DOCTORAL THESIS

Supervisor:
Ph. D. Hrvoje Stančić, full professor

Zagreb, 2018.

ZAHVALE

Na početku, želim zahvaliti svojoj dragoj obitelji, supruzi Romani i kćerki Beli na velikoj podršci, razumijevanju i ljubavi koja nije izostala u trenucima odricanja za ovaj doktorski rad. Posebno sam zahvalan supruzi što me nagovorila na upisivanje ovog doktorskoj studija. Nadalje, želim izraziti zahvalnost svojemu mentoru dr. sc. Hrvoju Stančiću, red. prof. što me je uključio u međunarodni znanstveno-istraživački InterPARES Trust projekt na kojemu sam stekao mnoge korisne znanstvene spoznaje. Zahvaljujem mu na uputama, savjetima i smjernicama koje mi je pružio tijekom doktorskog studija i same izrade ovoga doktorskoga rada. Zahvaljujem i kolegama s kojim sam tijekom doktorskog studija radio na zajedničkim znanstvenim radovima i izlaganjima: Borisu Hercegu (prijatelju i kolegi iz Fine), doc. dr. sc. Arianu Rajhu i doc. dr. sc. Tihomiru Katuliću. Također želim zahvaliti svim kolegama s kojima sam sudjelovao u istraživanjima na projektu InterPARES Trust.

INFORMACIJE O MENTORU

Dr. sc. Hrvoje Stančić, red. prof. 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 ožujka 2018. je u zvanju redovnoga profesora.

Autor je knjige Digitalizacija, koautor knjige Heritage Live. Upravljanje baštinom uz pomoć informacijskih alata, urednik pet knjiga, a objavio je, samostalno ili u koautorstvu, više od 80 znanstvenih i stručnih radova, te je vodio izradu 11 disertacija. Od 2007. aktivno je uključen u organizaciju odsječke bienalne međunarodne konferencije INFuture – The Future of Information Sciences.

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 hrvatskog istraživačkog konzorcija na međunarodnom projektu InterPARES Trust – Trust and Digital Records in an Increasingly Networked Society (2013.-2019.).

U Ministarstvu kulture RH član je radne skupine za izradu nacionalne strategije za digitalizaciju kulturne baštine. Član je Hrvatskog informacijskog i dokumentacijskog društva (HIDD), član Predsjedništva Hrvatskog arhivističkog društva (HAD) te član Centre for the International Study of Contemporary Records and Archives (CISCRA) na Sveučilištu Britanske Kolumbije, Vancouver, Kanada.

SAŽETAK

Cilj ove doktorske disertacije je izrada modela informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata u području javne uprave. Za potrebe izrade modela obrađen je referentni teorijski model za dugotrajnu pohranu elektroničkih informacijskih objekata – OAIS. Opisane su odgovornosti i sastavnice te funkcionalni entiteti navedenog modela. Obrađena su teorijska saznanja s području infrastrukture javnog ključa (PKI) zbog tehnologija i koncepata koji podržavaju povjerenje u elektroničke zapise: digitalni certifikat, elektronički potpis, napredni elektronički potpis, certifikacijski (CA) i registracijski autoritet (RA), elektronički vremenski žig i dr. Uredbom eIDAS (Uredba (EU) br. 910/2014) je za područje Europske Unije stavljena van snage do tada važeća EU Direktiva 1999/93/EC o okviru Zajednice za elektroničke potpise. Utjecaj Uredbe eIDAS je vrlo dalekosežan za pravno reguliranje elemenata za dugotrajno očuvanje elektronički potpisanih zapisa. Navedena uredba je propisala i koncept kvalificiranog pružatelj usluga povjerenja (za izdavanje certifikata, vremenskih žigova i dr.). Posebno su detaljno obrađeni formati naprednog elektroničkog potpisa: XAdES, CAdES i PADES. Takvi formati potpisa omogućavaju očuvanje u dugom roku pa su iz tog razloga posebno zanimljivi. Detaljno su obrađeni procesi izrađivanja i validacije naprednog elektroničkog potpisa. Prepoznat je pojam dokaza postojanja, tj. PoE (engl. Proof of Existence) elektroničkog potpisa kao ključan za ovaj rad. U proučavanju područja dugoročnog očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima obrađene su četiri strategije očuvanja: uklanjanje elektroničkih potpisa, bilježenje traga o elektroničkim potpisima u metapodacima, bilježenje valjanosti o elektroničkim potpisima u blokchainu te očuvanje elektroničkih potpisa. Očuvanje elektroničkih potpisa je često implicitno definirano u zakonskim propisima te je stoga bilo i izazov za ovaj istraživački rad.

Detaljno je obrađena tematika elektroničke javne uprave (pojam, faze, mobilna javna uprava i sektori). Da bi se bolje shvatila važnost arhiva u elektroničkoj javnoj upravi obrađen je kontekst elektroničke javne uprave u Europskoj Uniji i Republici Hrvatskoj. Sudjelovao sam na InterPARES Trust istraživačkom projektu na temu analize elektroničkih javnih usluga. Analizirani su različiti aspekti javnih e-usluga, a sa stanovišta ovog rada su posebno zanimljivi rezultati s područja dugoročnog očuvanja elektroničkih zapisa te su i izneseni u ovom radu. Osim toga, istražena je dostupnost servisa i komponenata temeljenih na infrastrukturi javnog ključa u RH koji se mogu učinkovito iskoristiti za izgradnju

infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata. Konačno je dana i analiza uspješnosti elektroničkih javnih uprava po više metodologija.

Napravljena je detaljna analiza različitih aspekata elektronički potpisanih dokumenata (interoperabilnost, pravna uređenost, rokovi čuvanja, norme za dugotrajnu pohranu). Obrađen je i pojam elektroničke isprave u smislu zamjene za papirnate službene dokumente izdane od javne uprave. Analizirani su hrvatski i strani zakoni s tog područja. Kao priprema za izradu modela dugotrajne pohrane elektronički potpisanih dokumenata obavljena je analiza uspješnih implementacija e-arhiva iz Hrvatske, Njemačke, Italije, Austrije, Litve i Estonije. Obrađeni je i jedan referentni model za dugotrajnu pohranu te su analizirani rezultati istraživačkog E-ARK projekta. S obzirom na saznanja iz analize uspješnih praksi i referentnih modela izradio sam model informacijskog sustava za pohranu elektronički potpisanih dokumenta. Razrađeni model se temelji na OAIS referentnom modelu. Vrlo bitan dio u izradi navedenog modela je razrada pojma očuvanja dokaza postojanja. Predlaže se korištenje standarda RFC 6283 (XMLERS) za zapis očuvanja dokaza postojanja. Osim toga, ključno u izradi modela je korištenje usluga kvalificiranih pružatelja usluga povjerenja za certifikate i za vremenske žigove. Kvalificirani vremenski žig poprima i značenje arhivskog vremenskog žiga. Izrađeni model podrazumijeva produženje potpisa prije isteka prikladnosti korištenih algoritama. Osnovna namjera produženja potpisa jest osigurati provjerljivost cjelovitosti i autentičnosti već potpisanih dokumenata. Osim toga i vremenski žigovi s vremenom mogu izgubiti svoju prikladnost pa se pravovremeno treba dohvaćati novi vremenski žig. Predloženo je rješenje i za dugotrajno očuvanje elektroničke isprave na način da tehnološka implementacija podrži pravni okvir. Predloženi su i formati dokumenata za ovaj model te korištenje formata naprednog elektroničkog potpisa. Predloženi su formati iz AdES obitelji potpisa: XAdES, CAdES i PAdES. Na kraju rada je dan prijedlog uspostave infrastrukture za dugotrajno očuvanje potpisanih elektroničkih dokumenata u Republici Hrvatskoj.

Ključne riječi: OAIS, e-uprava, e-usluge, PKI, elektronički potpis, elektronički arhiv, elektronički dokument, ERS, XMLERS.

SUMMARY

The aim of this PhD thesis is to develop a model of the information system for the long term storage of electronically signed documents within public administration domain. For the purpose of building the model, the referent theoretical model for the long term storage of electronic information objects - OAIS is elaborated. The responsibilities, components and the functional entities of the mentioned model are described. Theoretical findings in connection with public key infrastructure (PKI) are covered because of the technologies and concepts that support the confidence in electronic records: digital certificate, electronic signature, advanced electronic signature, certificate authority (CA), registration authority (RA), electronic timestamp etc.

The EU Directive 1999/93/EC on a Community framework for electronic signatures was derrogated in the EU area by eIDAS regulation (EU Regulation no. 910/2014). The influence of the eIDAS regulation is far-reaching for the legal regulation of the elements for the long-term preservation of electronically signed records. The regulation laid out the concept of the qualified trust server provider (for the certificate issuance, timestamps, etc.). Certain formats of advanced electronic signature are thoroughly covered. Such signature formats enable long-term preservation what makes these formats particularly interesting. The processes of development and validation of advanced electronic signature are described in detail. The term Proof of Existence (PoE) of electronic signature is recognized as key for this thesis. Studying the area of the long-term integrity and authenticity preservation of electronic records with electronic signatures four strategies of preservation are covered: the removal of electronic signatures, keeping track of electronic signatures within the metadata, recording electronic signature validity within the blokchain and the preservation of electronic signatures. The preservation of electronic signatures was a challenge for this thesis because it is often implicitly defined within legal regulations.

The concept of electronic public administration is thoroughly covered (the term, phases, mobile public administration, sectors). To have a better understanding of the importance of archives in the electronic public administration the context of electronic public administration in the European Union and in the Republic of Croatia is described. The author took part at InterPARES Trust research project that was based on the analysis of electronic public services. Different aspects of public e-services are analyzed, form the point of this work the results from the area of electronic records long-term preservation are especially interesting

and as such are elaborated in this thesis. Furthermore, the availability of services and components based on the public key infrastructure in the Republic of Croatia that can be efficiently used for signing and long term-storage of electronically signed document infrastructure development is investigated. Finally the analysis of efficacy of electronic public administrations according to numerous methodologies is presented. A detailed analysis of different aspects of electronically signed documents (interoperability, legal regulation, preservation time period, long-term storage standards) is made. The term *electronic document* as a substitute for official paper documents issued by public administration is elaborated. Croatian and foreign legal regulations are analyzed. As a preparation for the long-term storage of electronically signed documents model an analysis of successful e-archive implementations from Croatia, Germany, Italy, Austria, Lithuania and Estonia is made. One referent model for the long-term storage is elaborated and the results of the E-ARK research project are analyzed.

Based on the findings from the analysis of successful practices and referent models the author built a model of the information system for storage of electronically signed documents. The developed model is based on OAIS reference model. An important part of the above mentioned model development is the elaboration of preservation of the proof of existence term. The use of RFC 6283 (XMLERS) standard for the Evidence Record Syntax is recommended. On top of that the use of qualified trust service providers for certificates and for timestamps is key for this model development. Qualified timestamp also takes the meaning of an archive timestamp. The developed model implies signature renewal before an expiration of the validity of the algorithms used. The main purpose of the signature renewal is to insure the verification of completeness of already signed documents. Additionally, timestamps can lose their validity as time passes so new timestamps must be acquired in time. The solution for the electronic document long-term preservation is suggested so that technological implementation supports legal regulation. Document formats for this model are suggested as well as the usage of the advanced electronic signature format. The formats from the AdES family of signatures are proposed: XAdES, CAdES, PAdES. At the end of this thesis the suggestion to set up an infrastructure for the long-term storage of electronically signed documents in the Republic of Croatia is given**.**

Key words: OAIS, e-government, e-services, PKI, electronic signature, electronic archive, electronic document, ERS, XMLERS.

SADRŽAJ

1. UVOD

Današnji brzi razvoj tehnologija i rastuća potreba za promjenom i optimizacijom postojećih procesa rada u svim područjima ljudske djelatnosti nameću potrebu za novim, optimiziranim tehnološkim rješenjima. Jedno od takvih područja je svakako područje javne uprave. Javne uprava umnogome svojim učinkom/neučinkom utječe na kvalitetu života i rada fizičkih i pravnih osoba. Time se dolazi do potrebe optimizacije i digitalizacije poslovnih procesa u javnoj upravi i prijelazu na e-upravu, tj. elektroničku javnu upravu. Elektronička javna uprava ima više komponenti pomoću kojih se može mjeriti njezin napredak te planirati njezino unaprjeđenje i daljnji razvoj. Hrvatska nije izoliran slučaj što se tiče e-uprave pa tako ima svoj tempo napretka i planove kako doći do zacrtanih ciljeva. Europska Unija je ta koja, kao jedna od vodeći u svijetu na tom području, svojih strategijama i planovima umnogome utječe i na hrvatske planove za razvoj u tom području. Iz navedenih razloga potrebno je toj tematici posvetiti dužnu pažnju u ovoj doktorskoj disertaciji. Hrvatska je napravila mnoge iskorake u području elektroničke javne uprave zadnjih godina (od elektroničkih identiteta, izgradnje novih e-usluga i dr.). Izazov je i ovog rada istražiti koliko je u tome uspjela zadnjih godina. Javna uprava u komunikaciji s fizičkim i pravnim osobama isporučuje velik broj dokumenata. To mogu biti razna rješenja, potvrde, zahtjevi i dr. U današnje vrijeme postoji opravdana potreba s isporuke u papirnatoj verziji prijeći na suvremene kanale isporuke (web, mobilne tehnologije,…). Izradom i isporukom dokumenta putem modernih tehnologija se dolazi do problematike elektroničkog dokumenta te raznih područja u radu s njim. Postoji pravni aspekt njegovog korištenja, problematika distribucije te konačno pohrane. Iz navedenog razloga problematika elektroničkog dokumenta zaslužuje temeljitiju razradu u ovom radu. Pravna problematika elektroničkog dokumenta u Hrvatskoj i svijetu zaslužuje, također, primjeren dio u ovom radu. Pohrana elektroničkog dokumenta i drugih zapisa te posebno dugotrajna pohrana je tematika koja se sve izrazitije nameće. Postoji puno različitih aspekata dugotrajne pohrane elektroničkih dokumenata i ostalih zapisa, a ovaj rad će se usmjeriti u proučavanje tematike dugotrajne pohrane za javnu upravu. U svijetu postoje već mnoge različite implementacije dugotrajne pohrane elektroničkih zapisa pa će se ova disertacija usmjeriti na uspješne prakse implementacije elektroničkih arhiva u javnim upravama. Osim toga, u ovom radu će se voditi računa o referentnim modelima koji su kao najbolji prepoznati u svijetu. Bitan dio ovog rada su i međunarodno prihvaćeni standardi i formati u području dugotrajne pohrane elektroničkih zapisa. Kako je tema ovog rada koncept uspostave elektroničkog arhiva u javnoj upravi, nameće se pitanje korištenje i dugotrajno pohranjivanje elektronički

potpisanih zapisa. Današnji koncepti očuvanja gradiva podrazumijevaju definiranje više bitnih pojmova: od autentičnosti, zaštite integriteta, neporecivosti i drugih. Zahtjeve navedenih pojmova će se u ovom radu nastojati riješiti već postojećim konceptima infrastrukture javnog ključa. Digitalni certifikati, vremenski žigovi i elektronički potpis su vrlo zanimljivi za ovaj rad pa će se detaljnije i obraditi. Jedan od centralnih izazova ove doktorske disertacije je kako dugotrajno sačuvati dokaze postojanja elektronički potpisanih zapisa pa će se većina istraživačkog radu usmjeriti na to područje. Motivacija za izradu ovog rada je i izrada koncepta na osnovu kojeg se može uspostaviti elektroničkih arhiv u javnoj upravi u Republici Hrvatskoj kojeg za sada nema, a nameću se funkcionalne i pravne potrebe za njim.

1.1 CILJEVI ISTRAŽIVANJA

U okviru i na temelju definirane teme ovog doktorskog rada, ciljevi istraživanja ove doktorske disertacije su:

- Detaljno obraditi OAIS[1] - referentni teorijski model za dugotrajnu pohranu elektroničkih informacijskih objekata.
- Dati uvid u pravnu stečevine Europske Unije i Republike Hrvatske na području infrastrukture javnog ključa i pouzdanih pružatelja usluga prije i nakon donošenja Uredbe (EU) br. 910/2014[2] (u nastavku teksta Uredba eIDAS) te njihov utjecaj na dugotrajnu pohranu elektronički potpisanih dokumenata.
- Obraditi tematiku komponenti temeljenih na infrastrukturi javnog ključa (PKI) koje su nužne za model informacijskog sustava za potpisivanje i dugotrajnu pohranu elektroničkih dokumenata.
- Detaljno obraditi tematiku naprednog elektroničkog potpisa.
- Istražiti problematiku elektroničke isprave u smislu zamjene za papirnate službene dokumente izdane od javne uprave s posebnim težištem na područje zakonodavnog okvira.

[1] ISO (2003.), ISO 14721:2003 - Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model; http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284 (07.08.2016.)

[2] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

- Istražiti pravni okvir za područje dugotrajne pohrane elektroničkih dokumenata u javnoj upravi RH.
- Istražiti elektroničke javne servise s različitih aspekata (međuostalim i s aspekta dugotrajne pohrane podataka).
- Istražiti uspješnost elektroničkih javnih uprava u Hrvatskoj i svijetu s aspekta povezanosti s uspješnom implementacijom e-arhiva te za potrebe dokazivanja hipoteze H-3.
- Napraviti detaljnu analizu uspješnih implementacija i referentnih modela za e-arhive u svijetu.
- Izraditi model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata u područjima javne uprave i gospodarstva.
- Izraditi prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave.

1.2 HIPOTEZE ISTRAŽIVANJA

Hipoteze ove doktorske disertacije na osnovu kojih će biti obavljeno istraživanje su:
H-1 U RH postoji odgovarajući zakonodavni okvir za implementaciju elektroničke isprave zasnovan na infrastrukturi javnog ključa.
H-2 Infrastruktura javnog ključa (PKI) predstavlja dobar temelj za izgradnju i implementaciju informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata.
H-3 Neki od dostupnih servisa i komponenata temeljenih na infrastrukturi javnog ključa u RH mogu se učinkovito iskoristiti za izgradnju infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave.
H-4 Uspostava informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata osigurava pohranu i dugotrajno čuvanje e-gradiva uz zadovoljavanje zahtjeva autentičnosti, neporecivosti, zaštite integriteta i upotrebljivosti.

Nakon cjelokupnog istraživanja i izvođenja zaključaka, dokazane hipoteze, ali i one opovrgnute omogućit će izradu koncepta elektroničkog arhiva u javnoj upravi. Navest će se koji standardi i formati se predlažu za takav koncept, arhitekturu te funkcionalni i nefunkcionalni zahtjevi željenog modela. Na temelju provedenog istraživanja izradit će se prijedlog uspostave e-arhiva za područje javne uprave.

1.3 METODOLOGIJA RADA

Prilikom izrade ove doktorske disertacije koristit će se metode analize, sinteze, apstrakcije, konkretizacije, deskripcije, komparacije, te metoda modeliranja. Činjenice i procesi će se opisivati metodom deskripcije, te obrađivati metodama analize i sinteze. Prilikom usporedbe podataka koristit će se primjerene komparativne metode. Koristit će se dostupna znanstvena i stručna literatura, objavljeni magistarski i doktorski radovi, zbornici radova s međunarodnih i domaćih znanstvenih i stručnih skupova. Intenzivno će se koristiti i izvori s interneta radi dobivanja najnovijih podataka vezanih uz tematiku ove doktorske disertacije. Obavit će se i anketiranje čiji rezultati će biti obrađeni i izloženi u ovom radu.

1.4 KOMPOZICIJA RADA

Ovaj rad ima jedanaest poglavlja. Prvo poglavlje je uvodno te se u njemu ukratko objašnjava osnovna problematika teme rada, ciljevi i hipoteze istraživanja, korištena metodologija rada, kompozicija rada i znanstveni doprinos.

U poglavlju 2 će se obraditi OAIS referentni model. Detaljno će se obraditi pojam elektroničkih informacijskih objekata. Zatim će se navesti odgovornosti i sastavnice ovog referentnog modela. Detaljno će se obraditi funkcionalni entiteti OAIS arhiva te će se na kraju dati opis perspektiva i primjene OAIS referentnog modela.

Potom će se u poglavlju 3 obraditi teorijska saznanja o području infrastrukture javnog ključa (PKI), te tehnologije i koncepte koji podržavaju povjerenje u elektroničke zapise. Za početak će se detaljno obraditi tematika kriptografije (simetrične i asimetrične). Među ključnim tehnologijama i konceptima za obraditi su: elektronički potpis, napredni elektronički potpis, digitalni certifikati, certifikacijski (CA) i registracijski autoriteti (RA), neporecivost, elektronički vremenski žig i dr.

Poglavlje 4 će donijeti analizu područja naprednog elektroničkog potpisa, elektroničkog pečata i drugih bitnih pojmova vezanih uz elektroničke potpise. Posebno je bitno u ovom radu obraditi formate elektroničkog potpisa s naglaskom na napredne formate i formate koji

omogućavaju očuvanje u dugom roku. Detaljno će se obraditi procesi izrađivanja i validacije naprednog elektroničkog potpisa.

U poglavlju 5 će se opisati postojeće strategije dugoročnog očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima.

Detaljno će se obraditi problematika elektroničke javne uprave (pojam, faze, mobilna javna uprava i sektori) u poglavlju 6. Da bi se bolje shvatila važnost arhiva u elektroničkoj javnoj upravi obradit će se kontekst elektroničke javne uprave u Europskoj Uniji i Republici Hrvatskoj. Motivacija za detaljnije obrađivanje ove tematike jest i sudjelovanje na InterPARES istraživačkom projektu na temi analize elektroničkih javnih usluga na kojoj sam i ja radio. Rezultati navedene analize će biti prikazani kroz ovaj rad. Osim toga, u svom magistarskom radu iz 2007.[3] „Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge“ sam već detaljno obradio područje javne uprave i napravio određene uvide i analize. S tog stanovišta će biti zanimljivo usporediti stanje e-uprave iz 2007. s kasnijim stanjem. Kada se obrade konteksti e-uprave u EU i Hrvatskoj, u poglavlju 7 će biti dana i analiza uspješnosti elektroničkih javnih uprava po više metodologija. Osim saznanja iz istraživačkog projekta InterPARES Trust[4] (eng. International Research on Permanent Authentic Records in Electronic Systems) o e-servisima i njihovim različitim aspektima (međuostalim i problematici dugotrajne pohrane podataka) za mene su bitna saznanja i općenite tendencije sadašnjeg razvoja e-uprave. Za hrvatsku elektroničku javnu upravu je potrebno istražiti dostupnih servisa i komponenata temeljenih na infrastrukturi javnog ključa u RH mogu se učinkovito iskoristiti za izgradnju infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata (H-3). Smatram da su područja elektroničke javna uprava i problematika e-arhiva neodvojiva i cilj je ovog dijela istraživanja pokazati vezu napretka u elektroničkoj javnoj upravi te uspješnosti u implementaciji e-arhiva. Uostalom, i sama tema ovog rada je izrada koncepta uspostave elektroničkog arhiva u javnoj upravi.

U poglavlju 8 će se analizirati aspekti elektronički potpisanih dokumenata (interoperabilnost, pravna uređenost, rokovi čuvanja, norme za dugotrajnu pohranu). Bitno je obraditi i pojam

[3] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, Hrvoje Brzica, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf (17.03.2018.)
[4] InterPARES Trust, https://interparestrust.org/

elektroničke isprave u smislu zamjene za papirnate službene dokumente izdane od javne uprave s posebnim težištem na područje zakonodavnog okvira. U okviru analize istražit će se hrvatski i strani zakoni. Posebna pažnja će biti dana relevantnim hrvatskim zakonima i pravilnicima.

Poglavlje 9 će obuhvatiti detaljnu analiza praksi i modela dugotrajne pohrane u Hrvatskoj i svijetu. Prikazat će se i već spomenuti rezultati dobiveni istraživanjima na InterPARES Trust projektu. Kao priprema za izradu modela informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata u područjima javne uprave i gospodarstva napravit će se istraživanje najboljih svjetskih praksi, te njihova komparacija. Neki od sustava koji će se analizirati su:

- Model dugotrajne pohrane elektronički potpisanih dokumenata njemačkog ureda za informacijsku sigurnost BSI (njem. Bundesamt für Sicherheit in der Information),
- Estonski nacionalni elektronički arhivi,
- HALMED (Hrvatska),
- Elektronički arhivski informacijski sustav – Litva – EAIS (lit. Elektroninio archyvo informacinė sistema),
- Arhivski sustavi njemačkog zdravstva,
- i dr.

Bit će obavljeno i anketiranje relevantnih institucija te će prikupljeni rezultati biti obrađeni evaluacijom i u pismenoj interpretaciji.

Nakon toga će u poglavlju 10 uslijediti faza sintetiziranja znanja stečenih proučavanjem postojeće literature, prakse i iskustva drugih zemalja, te postojećeg stanja u Hrvatskoj. Na temelju toga će se krenuti s izradom hrvatskog modela informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata u područjima javne uprave i gospodarstva. Tijekom izrade modela koristit će se i navedene spoznaje dobivene osobnim istraživanjima unutar međunarodnog znanstveno-istraživačkog projekta InterPARES Trust[5]. Na kraju će se dati prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave.

[5] InterPARES Trust, https://interparestrust.org/ (21.03.2018.)

Na kraju će u poglavlju 11 biti dani konačni zaključci ovog rada.

1.5 ZNANSTVENI DOPRINOS

Očekivani znanstveni doprinos istraživanja u ovoj doktorskoj disertaciji:

- Analiza stanja u pravnom području dugotrajne pohrane elektroničkih dokumenata u javnoj upravi RH.
- Analiza uspješnosti elektroničkih javnih uprava s aspekta povezanosti s uspješnom implementacijom e-arhiva.
- Rezultati istraživanja projekta InterPARES Trust iz područja analize elektroničkih javnih servisa na kojima sam i sam sudjelovao.
- Kritički osvrt na zakonodavni okvir temeljen na komparativnoj analizi postojećeg hrvatskog zakonodavnog okvira za elektroničku ispravu i sličnih zakona u svijetu čime će se dobiti uvid u moguća ograničenja ovakvog zakonodavnog rješenja, te moguće implikacije na praktične implementacije elektroničke isprave.
- Analiza konkretnih implementacija sustava za potpisivanje i arhiviranje elektroničkih dokumenata u svijetu te referentnih modela.
- Model informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata u područjima javne uprave i gospodarstva.
- Prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave.

2. OAIS – REFERENTNI MODEL ZA ELEKTRONIČKI ARHIV

U ovom poglavlju će prvo biti opisana problematika postojanog očuvanja autentičnosti elektroničkog gradiva. Obradit će se pojam elektroničkog informacijskog objekta i njegove aspekte.

Detaljno će biti obrađen OAIS referentni model za dugoročno očuvanje artefakata. Fokus ovog rada je dugoročno očuvanje elektronički potpisanih zapisa pa će se u ovom poglavlju OAIS model promatrati kao model za pohranu digitalnih zapisa ili konkretnije kao arhiv koji služi za očuvanje i dohvat digitalnih zapisa.

Obradit će se osnovnih šest zadataka (odgovornosti) koje ima arhiv organiziran prema OAIS modelu.

OAIS referentni model se će obraditi i kroz tri dijela koja su međusobno povezana: okoline u kojoj OAIS arhiv djeluje, funkcionalnih entiteta i informacijskih objekata. Postoji šest osnovnih funkcionalnih entiteta OAIS modela i jedan pridruženi koji služi kao potpora svim osnovnim entitetima.
Na kraju poglavlja će biti ukratko opisane perspektive i primjene OAIS referentnog modela.

2.1 AUTENTIČNOST ELEKTRONIČKIH INFORMACIJSKIH OBJEKATA

Napredak u tehnologijama daje velik broj prednosti i unaprjeđenja u svakodnevnom životu i radu, ali sa sobom povlači i nove izazove. Tako je i s informacijskom tehnologijom. Informacijska tehnologija se koristi, međuostalim, i za stvaranje elektroničkog gradiva. Kod elektroničkog gradiva je svojstveno da pretraživanje i pregledavanje postaje upitno nakon kraćeg vremena čuvanja. Elektroničko gradivo za korisnika tijekom vremena može postati nepouzdano, nevjerodostojno. Dakle, takvo gradivo može izgubiti autentičnost. Moderna se arhivistika uz pitanja vezana za područja tradicionalne arhivistike bavi i odgovorima na sasvim konkretna, moderna pitanja[6]:

- Kako dugoročno očuvati digitalizirano i digitalno gradivo?

[6] Odsjek za informacijske i komunikacijske znanosti Filozofskog fakulteta u Zagrebu, Arhivistika i dokumentalistika, http://inf.ffzg.unizg.hr/index.php/hr/odsjek/katedre/arhivistika-i-dokumentalistika (03.08.2016.)

- Kako očuvati autentičnost[7], integritet, vjerodostojnost, pouzdanost i iskoristivost elektroničkog gradiva (građe) tijekom mnogih i stalnih tehnoloških promjena?

Navedenu problematiku postojanog očuvanja autentičnosti elektroničkog gradiva je najbolje promatrati kroz pojam elektroničkog informacijskog objekta i njegove aspekte.

Informacijski objekt predstavlja bilo koje gradivo koje pruža informaciju bez obzira nalazio se on u analognom ili digitalnom (elektroničkom) obliku, pri čemu su računala samo jedna od metoda i tehnika njegove obrade[8]. Elektronički informacijski objekt[9], pak, predstavlja onaj objekt koji je nastao uz pomoć informacijske tehnologije, bez obzira je li to njegov izvorni oblik ili je riječ o gradivu u klasičnom obliku koje je preneseno u elektroničku okolinu postupkom digitalizacije.

S obzirom na očuvanje elektroničkih informacijskih objekata na dulji vremenski rok, svaki takav objekt možemo promatrati kroz tri razine njegovih karakteristika[10]:

1. Fizička razina je razina zapisa elektroničkog informacijskog objekta na neki medij. Problemi očuvanja na ovoj razini se javljaju kao problemi trajnosti medija, te zapisa na njima. Što se tiče elektroničkog gradiva, potrebno je očuvati stabilnim medij na koji se sprema elektroničko gradivo, te zapise koji se na mediju nalaze.
2. Logička razina određuje način na koji će sadržaj biti fizički organiziran i zapisan. Ova razina zanemaruje vrstu medija i način zapisa na njega. Međutim, ova razina mora biti prisutna i na fizičkoj razini. Navedeno podrazumijeva da informacije o logičkoj razini trebaju biti i fizički zabilježene.
3. Konceptualna razina može biti na različite načine organizirana na logičkoj razini, te o tome ovisi i njezina interpretacija. Tako isti tekst može biti zabilježen kao .pdf, .txt ili .doc dokument. Očuvanje elektroničkih informacijskih objekata na konceptualnoj razini mora uvažiti mogućnost postojanja više logičkih zapisa iste konceptualne razine.

---

[7] Hrvatski leksikon, autentičnost (lat. iz grč.), istinitost, izvornost, vjerodostojnost; http://www.hrleksikon.info/definicija/autenticnost.html (07.08.2016.)

[8] Stančić, H. (2004.), Očuvanje elektroničkih informacijskih objekata: arhivi, knjižnice, muzeji – zajednička koncepcija, u: Katić, Tinka (ur.), Zbornik 7. seminara Arhivi, knjižnice, muzeji, Hrvatsko knjižničarsko društvo, Zagreb, str. 26-35.

[9] isto

[10] Thibodeau, K. (2002.), Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, u: The State of Digital Preservation: An International Perspective, Council on Library and Information Resources (CLIR), Washington, D.C., SAD, str. 4-31.; https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10 (07.08.2016.)

Što se tiče klasičnih dokumenata, njihova autentičnost se provjerava na originalnom dokumentu. Provjera autentičnosti elektroničkih informacijskih objekata je daleko kompliciranija nego kod klasičnih dokumenata. Ono što komplicira provjeru autentičnosti elektroničkih informacijskih objekata je sama složenost takvih objekata i metoda kojim se nastoji očuvati dugoročna čitljivost takvih objekata. Postoji razlika i kod elektroničkih informacijskih objekata u složenosti provjere autentičnosti. Složenost je manja kada je u pitanju statično gradivo (npr. tekstualni dokumenti i slike), a veća je kod multimedijskog sadržaja, te elektroničkog gradiva kojem se kontinuirano mijenja sadržaj (npr. baze podataka). Bitna stavka u očuvanju autentičnosti elektroničkih informacijskih objekata je primjena primjerenih metoda za očuvanje elektroničkog objekta kroz vrijeme (npr. čuvanjem računalnih programa i operacijskih sustava, tj. okoline u kojoj je objekt stvoren). Dodatni izazovi koji se javljaju u čuvanju u dugom roku kod elektroničkih informacijskih objekata su osvježavanje medija na kojima se objekti pohranjuju, te same migracije takvih objekata. Tu je potrebno obratiti pažnju koliko je uopće autentičnost objekata nakon promjene medija na kojem je objekt bio izvorno zapisan. Uz ovakvu migraciju je potrebno očuvati i kontekstualne informacije.

Osim navedenog, vrlo bitan je pristup informacijskom objektu radi utvrđivanja autentičnosti. Kod klasičnog dokumenta autentičnost dokumenta se provjerava tako da su istovremeno fizički prisutni i osoba i dokument na istom mjestu. Za razliku od klasičnog dokumenta, elektroničkom informacijskom objektu se može pristupiti i preko udaljenog pristupa (engl. remote). Prilikom pristupa s udaljenog mjesta potrebno je osigurati nepromjenjivost prilikom prijenosa objekta putem računalne mreže od pošiljatelja do primatelja. Pošiljatelj u ovom smislu može biti institucija koja čuva elektroničke informacijske objekte, a primatelj krajnji korisnik takve institucije.

Thibodeau spominje[11] inherentni paradoks vezan uz očuvanje elektroničkih informacijskih objekata. U jednu ruku ima za zadatak dostaviti povijest u budućnost u nepromijenjenom, autentičnom stanju. Međutim, u drugu ruku, dohvat takvog sadržaja iz prošlosti neizbježno zahtijeva određene izmjene. Ovaj paradoks može biti riješen samo kroz razradu referentnog modela za digitalno očuvanje. Takav referentan model treba objasniti organizaciju, djelovanje i suradnju elektroničkih arhiva. Referentni model za otvoreni arhivski informacijski sustav (OAIS) razvio je Consultative Committee for Space Data Systems (CCSDS) pri američkoj agenciji NASA 1999. godine. Ovaj model je artikuliran kao međunarodni ISO standard –

[11] isto, str. 28

OAIS referentni model[12], te je pokriven i standardom ISO 14721:2003 - Space data and information transfer systems - Open archival information system -- Reference model.

Ovaj standard je revidiran kao ISO 14721:2012[13]. OAIS model je 2002. godine postao ISO standardom (ISO 14721), a deset godina kasnije (2012.) je objavljena trenutno važeća verzija standarda. OAIS referentni model osigurava okvir u kojem se balansira potreba za očuvanje elektroničkih informacijskih objekata nepromijenjenim, te potreba za usavršavanjem IT tehnologija sve u svrhu usavršavanja servisa za očuvanje informacijskih objekata. S druge strane OAIS (engl. Open Archival Information System) referentni model je previše generaliziran za direktnu implementaciju sustava za očuvanje autentičnosti elektroničkog gradiva kroz dulji vremenski period. Dakle, potrebna je i nadogradnja kako bi cijeli proces bio uspješan. OAIS nije statičan te se konstantno razvija kroz organizacije koje ga proširuju, kako bi bio prilagođen zahtjevima većeg broja organizacija i usluga pruženih putem Weba i oblaka (engl. Cloud). Dugoročno očuvanje elektroničkih informacijskih objekata pretpostavlja izgradnju sustava koji bi trebao biti nezavisan o promjenama računalnog programa, te operacijskih sustava i računala. Vodeći računa o navedenim postavkama, ulazni podaci bi trebali biti prilagođeni samom sustavu u koji ulaze, a taj sustav bi trebao biti postojanijih karakteristika.
OAIS referentni model je predstavljao osnovu za razvoj nekih projekata kao što je to InterPARES projekt[14]. Rezultati InterPARES projekta su dodatno specificirali OAIS polazišna načela.

2.2 ODGOVORNOSTI OAIS ARHIVA

OAIS je razvijen za dugoročno očuvanje bilo koje vrste artefakata, kako onih u digitalnom, tako i onih u fizičkom obliku. U ovom radu će se OAIS model promatrati kao model za pohranu digitalnih zapisa, tj. arhiv koji služi za očuvanje i dohvat digitalnih zapisa.

Osnovnih šest zadataka, a time i odgovornosti, koje ima arhiv organiziran prema OAIS modelu (str. 3-1)[15]su:

[12] ISO (2003.), ISO 14721:2003 - Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model; http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284 (07.08.2016.)
[13] ISO (2012.), ISO 14721:2012, http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683 (07.08.2016.)
[14] InterPARES Trust, https://interparestrust.org/ (21.03.2018.)
[15] Consultative Committee for Space Data Systems (2012.), Reference model for an open archival information system (OAIS) - 062012 - Magneta book, str. 3-1, http://public.ccsds.org/publications/archive/650x0m2.pdf (07.08.2016.)

1. Pregovaranje o preuzimanju i samo preuzimanje odgovarajućih podataka od stvaratelja podataka. Potrebno je donijeti odluke o vrsti podataka koje se u elektroničkom obliku namjeravaju čuvati. Vrste podataka mogu biti: sadržaj, format zapisa, medij, količine i dr. Ovaj zadatak podrazumijeva motiviranje aktera koji izrađuju podatke za prosljeđivanje u arhiv, ali u obliku koji je vrlo blizak onome kojeg arhiv koristi. Kao dobro rješenje se čini motivacija prosljeđivanja podataka točno određenog tipa i strukture u za to certificirani arhiv.

2. Ostvarivanje dovoljne kontrole nad preuzetim podacima u stupnju koji je potreban za očuvanje na dulji vremenski rok. Ovaj zadatak se odnosi na dobivanje dovoljnih prava radi postupaka nad podacima koje zahtjeva priprema za dugoročno čuvanje.

3. Odlučivanje, samostalno ili u dogovoru s drugima, koje skupine trebaju postati ciljnim korisničkim skupinama, te stoga trebaju biti u mogućnosti razumjeti podatke, čime definiraju svoju bazu znanja. Ovaj zadatak podrazumijeva definiranje grupe korisnika koji mogu razumjeti određeni skup podataka. Takva grupa korisnika dolazi iz istog okruženja kao i stvaratelj podataka koji se treba potruditi da ciljana grupa korisnika može razumjeti izrađene podatke.

4. Osiguravanje da se zaprimljeni podatak kod primatelja može rastumačiti bez dodatnih pojašnjavanja. Dakle, korisnik bi zaprimljene podatke trebao biti u stanju samostalno rastumačiti bez pomoći stvaratelja. Uz sličnost s trećim zadatkom postoji i razlika. Razlika se ogleda u potrebi da se jednom obrađeni i ubačeni podaci trebaju i kroz vrijeme dopunjavati određenim objašnjenjima da bi i kasnije bili čitljivi. Tu se radi o potrebi praćenja stručne terminologije, posebice ako su korisnici drugi informatički sustavi. U tom slučaju je potrebno obavljati prilagodbu formata i protokola.

5. Praćenje dokumentiranih politika i procedura koje osiguravaju da su podaci očuvani od svih mogućih slučajnosti uključujući diseminaciju podataka, osiguravajući da se nikad ne briše objekt koji sadrži dio prihvaćene strategije. Dakle, ne bi trebalo biti ad-hoc brisanja. Ovaj zadatak korisniku osigurava provjeru autentičnosti podataka. Korisnik može zatražiti usporedbu s elektroničkim originalom.

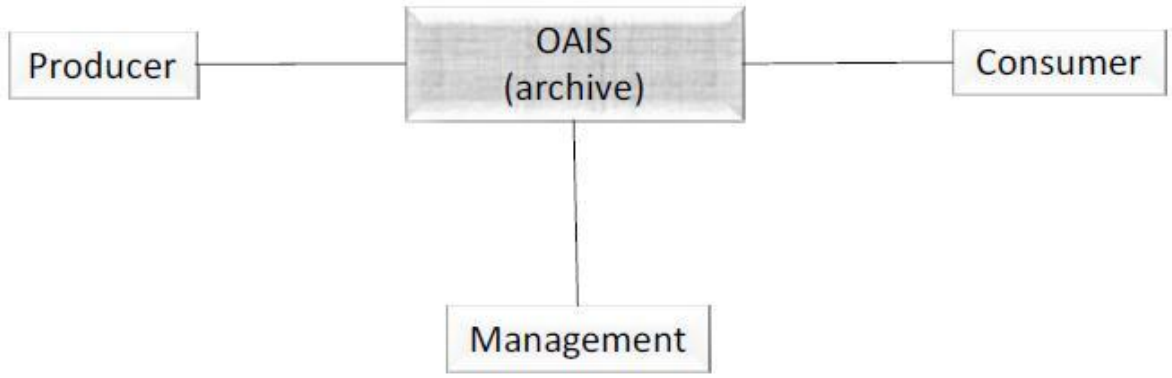
6. Osigurati da očuvani podaci budu dostupni određenim korisničkim skupinama i omogućiti da podaci budu diseminirani kao kopije originalno zaprimljenih podatkovnih

objekata s dokazom autentičnosti. Ovim zadatkom se ispunjava glavna funkcija dugoročnog očuvanja elektroničkog gradiva, zatim mogućnost diseminacije korisnicima koji za to imaju prava, ali na način da su podaci čitljivi kroz vrijeme.

2.3 SASTAVNICE OAIS REFERENTNOG MODELA

OAIS referentni model se sastoji od tri dijela koja su međusobno povezana[16]:

1. Okoline u kojoj OAIS arhiv djeluje
2. Funkcionalnih entiteta
3. Informacijskih objekata



Slika 1. Okruženje OAIS referentnog modela, preuzeto iz Consultative Committee for Space Data Systems (2012.)[17]

1. Okoline u kojoj OAIS arhiv djeluje:

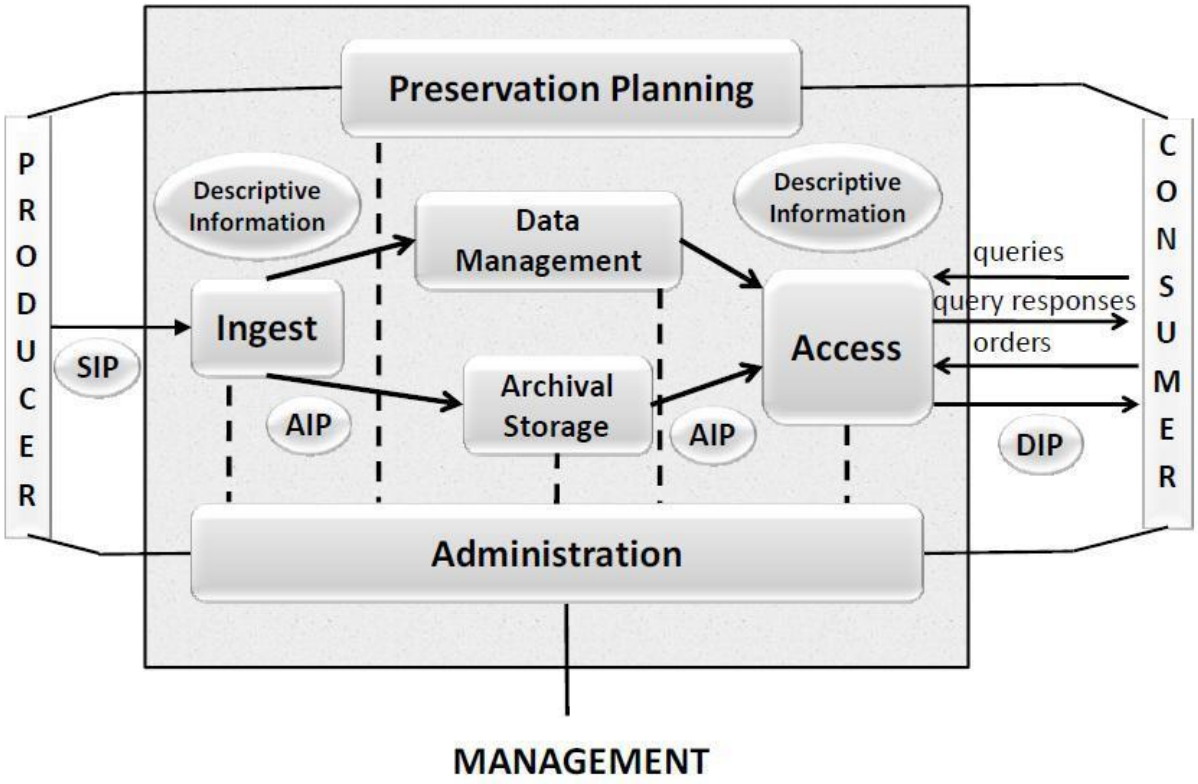
1. Proizvođači (engl. Producers) – proizvođači informacija mogu biti pojedinci, organizacije ili sustavi. Proizvođači arhivu povjeravaju informacije radi njihovog dugoročnog očuvanja.
2. Korisnici (engl. Consumers) - proizvođači informacija iz OAIS arhiva mogu biti pojedinci, organizacije ili sustavi.
3. Upravitelji (engl. Management) - upravitelji OAIS arhiva koji su zaduženi za upravljanje OAIS politikama. OAIS politike nastoje osigurati dugoročno očuvanje informacija. Osim

[16] Isto, str. 2-2
[17] Isto, str. 2-2, slika 2-1

toga, odgovornosti upravitelja su i razrada strategije upravljanje, te nadzor arhiva, provjera sigurnosnih ugroza i dr.

2. Funkcionalni entiteti – zajednički osiguravaju ulogu dugoročnog očuvanja u OAIS arhivu. Entiteti su sljedeći[18]:

1. Prihvat (engl. Ingest),
2. Arhivska pohrana (engl. Archival storage)
3. Upravljanje podacima (engl. Data management),
4. Administracija (engl. Administration),
5. Planiranje procesa očuvanja (engl. Preservation planning) i
6. Pristup (engl. Access).



Slika 2. OAIS funkcionalni entiteti, preuzeto iz Consultative Committee for Space Data Systems (2012.)[19]

Corado i Moulaison navode[20] da OAIS arhiv ima još jedan funkcionalan entitet – **zajedničke usluge** (engl. Common services). Zajedničke usluge podrazumijevaju: operacijski sustav,

[18] Isto, str. 4-2
[19] Isto, str. 4-1, slika 4-1
[20] Corrado, M. C., Moulaison, H. L. (2014.),

datotečni sustav, usluge mrežne infrastrukture, mrežnu infrastrukturu, telekomunikacijske sustava te mehanizme za autorizaciju i autentikaciju. Zajedničke usluge imaju za funkciju potpore svim procesima, koji se odvijaju u OAIS arhivu.

3. Informacijskih objekti – informacijski objekt (engl. Information object) je već spomenut u ovom radu. Stančić[21] ga definira kao objekt koji predstavlja bilo koje gradivo koje pruža informaciju bez obzira nalazio se on u analognom ili digitalnom (elektroničkom) obliku, pri čemu su računala samo jedna od metoda i tehnika njegove obrade.

Informacijski paket (engl. Information package) je strukturirani paket, tj. struktura koja logički objedinjuje više vrste informacijskih objekata.

Informacijski paketi mogu biti:

- **SIP** (engl. Submission Information Package) - Dostavljeni informacijski paket - on sadrži strukturirane informacije koje proizvođač informacija dostavlja OAIS arhivu. Struktura je takva da je već unaprijed dogovorena. Na taj način proizvođač može isporučiti OAIS arhivu informacije u onom obliku koji je najpogodniji za unos u elektroničkom formatu. Uz osnovne informacije se unose i potrebne popratne informacije.
- **AIP** (engl. Archival Information Package) - Arhivski informacijski paket - sadrži potpunu strukturu informacijskog paketa. Svi strukturni zahtjevi trebaju biti zadovoljeni jer se na taj način osigurava dugoročno očuvanje u OAIS arhivima. Ovom informacijskom paketu se dodaje opisna informacija paketa (engl. Package Description). Opisna informacija paketa služi za opisivanje paketa kao cjeline.
- **DIP** (engl. Dissemination Information Package – DIP) - Diseminacijski informacijski paket - paket koji se isporučuje na zahtjev korisnika OAIS arhiva. Diseminacijski informacijski paket sadrži dijelove ili cjelinu arhivskog informacijskog paketa. Za njega je bitno što sadrži i informaciju o pakiranju pa korisnik može razlučiti koja je tražena informacije i odvojiti je od ostalih (npr. opisnih informacija).

Digital preservation for libraries, archives, & museums, izdavač: Rowman & Littlefield, Plymouth, str. 48

[21] Stančić, H. (2004.), Očuvanje elektroničkih informacijskih objekata: arhivi, knjižnice, muzeji – zajednička koncepcija, u: Katić, Tinka (ur.), Zbornik 7. seminara Arhivi, knjižnice, muzeji, Hrvatsko knjižničarsko društvo, Zagreb, str. 26-35.

2.4 FUNKCIONALNI ENTITETI OAIS ARHIVA

U ovom poglavlju bit će dan pregled glavnih zahtjeva koje je nužno zadovoljiti u pogledu implementacije e-Arhiva. RFC 4810 popisuje zahtjeve koje trebaju zadovoljiti servisi za dugoročnu pohranu [22]. RFC 4810 pojašnjava i sljedeće termine:

Servis dugoročne pohrane, LTA (engl. Long-Term Archive Service) – to je servis koji je odgovoran za čuvanje podataka na dugi rok.

Politika dugoročne pohrane (engl. Long-Term Archive Policy) – to je skup pravila koji definira operativne karakteristike servisa dugoročne pohrane.

Zahtjevi za dugoročnu pohranu prema RFC 4810:

1. **Omogućavanje učitavanja, dohvata i brisanja arhiviranih podatkovnih objekata** (engl. Enable Submission, Retrieval, and Deletion of Archived Data Objects) - Treba biti moguće autenticirati zahtjeve i odgovore, npr. LTA servisu treba omogućiti prikazivanje autorizacijske odluke. To se može postići pomoću transportnih sigurnosnih mehanizama.

2. **Djelovanje u skladu s politikama dugoročne arhive** (engl. Operate in accordance with a long-term archive policy) – politike servisa dugoročne pohrane sadrže više komponenata. Slijede primjeri nekoliko:
    - politika održavanja arhiviranog podatkovnog objekta,
    - autorizacijska politika,
    - politika servisa.

3. **Omogućavanje upravljanja arhiviranim podatkovnim objektima** (engl. Enable Management of Archived Data Objects) – servis dugoročne pohrane mora dozvoliti klijentima na zahtjev sljedeće osnovne operacije:
    - određivanje roka arhiviranja za zaprimljene podatkovne objekte,
    - produljivanje ili skraćivanje roka arhiviranja,
    - određivanje metapodataka povezanih s arhiviranim objektima,

[22] Wallace C., Pordesch U., Brandner R.(2007.), RFC 4810, Long-Term Archive Service Requirements, https://tools.ietf.org/html/rfc4810 (06.12.2016.)

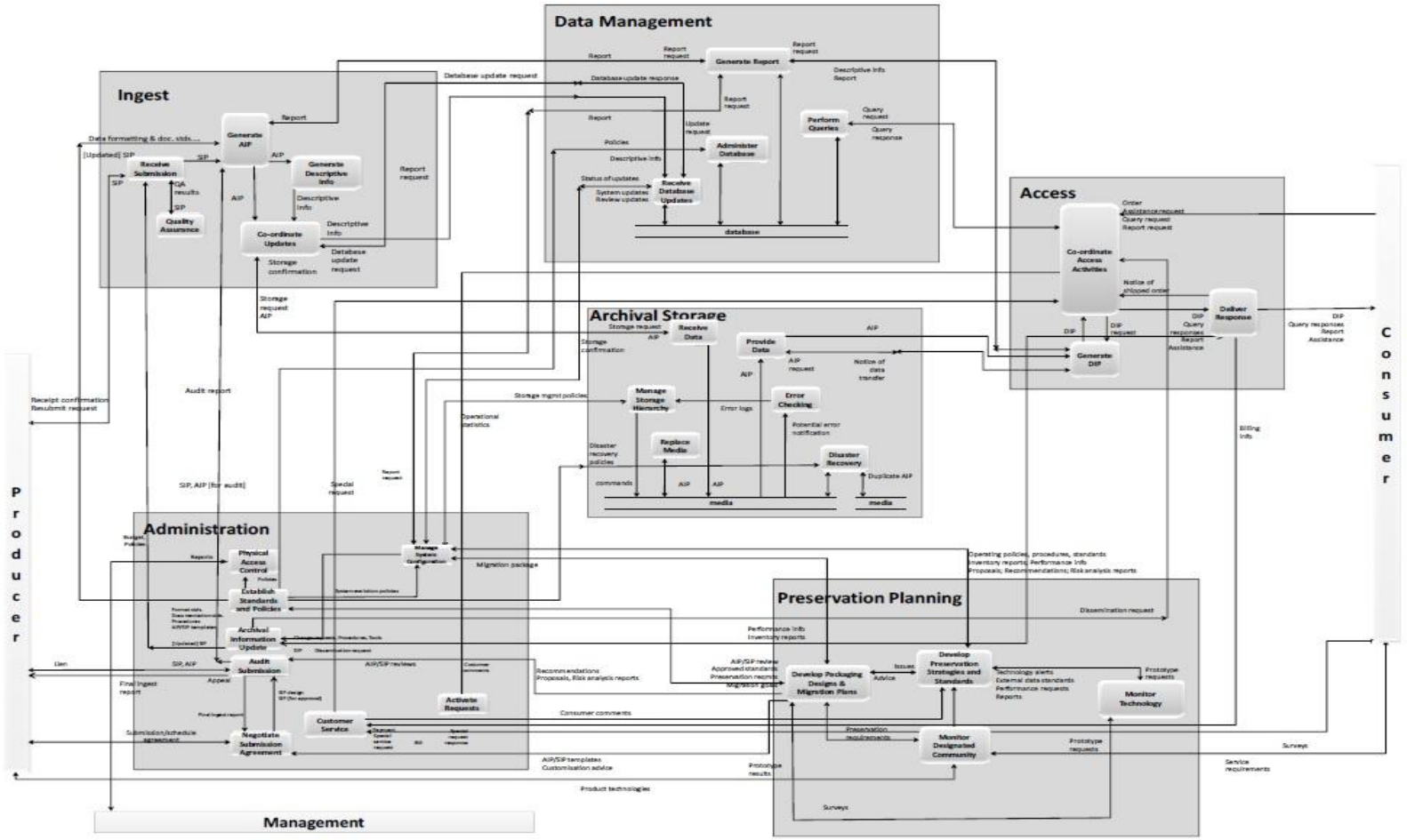
- određivanje politike arhiviranja koja će se primjenjivati nad zaprimljenim podacima.

4. **Osiguravanje evidencijskog dokaza kojim se omogućava prikazivanje statusa integriteta** (engl. Provide Evidence Records that Support Demonstration of Data Integrity) – servis dugoročne pohrane treba biti u mogućnosti osigurati evidencijski dokaz koji se može iskoristiti za demonstriranje integriteta podataka za koji je servis odgovoran. Navedeno treba osigurati od trenutka kada je podatak zaprimljen do trenutka isteka roka arhiviranja za navedeni podatak.

5. **Podrška povjerljivosti podataka (**engl. Support Data Confidentiality**) –** servis dugoročne pohrane treba dati podršku zaprimanja kriptiranih podataka na način da se naknadne aktivnosti očuvanja provode na originalnim, nekriptiranim podacima.

6. **Omogućavanje načina da se podaci i evidencijski dokazi mogu transferirati između servisa** (engl. Provide Means to Transfer Data and Evidence from One Service to Another) – treba se osigurati transferiranje podataka između više servisa bez gubitaka informacija.

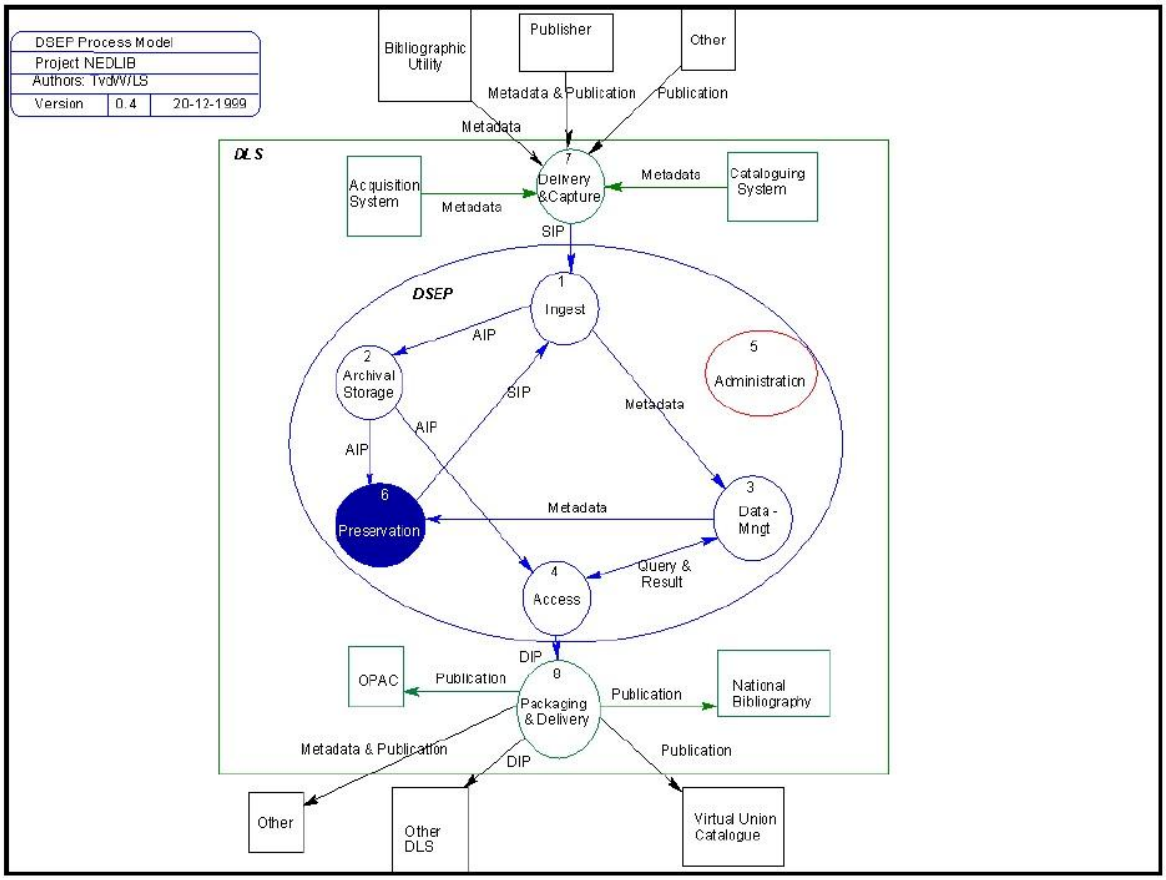
Na sljedećoj slici se nalazi prikaz kompozicije šest osnovnih funkcionalnih entiteta OAIS funkcionalnog modela.



Slika 3. Kompozicija OAIS funkcionalnih entiteta, preuzeto iz Consultative Committee for Space Data Systems (2012.)[23]

[23] Isto, str. A-2, slika A-1

Zanimljivo je pogledati sliku modela (slika 4) kao jedan od ranijih doprinosa prethodnoj slici kompozicije OAIS funkcionalnih entiteta kojeg Lee[24] spominje prilikom razrade doprinosa ranijih projekata na OAIS referentni model.



Slika 4. DSEP model, preuzeto iz Lee, C. A. (2005.)[25]

Lee spominje NEDLIB projekt[26]. NEDLIB (engl. Networked European Deposit Library) je inciran kao CoBRA+, trajni odbor europskih nacionalnih knjižnica (CENL, engl. Committee of the Conference of European National Libraries). Projekt je pokrenut 1.1.1998. i s trajanjem do kraja 2000. Osam nacionalnih knjižnica u Europi, jedan nacionalni arhiv, dvije ICT organizacije i tri velika izdavača su sudjelovali u projektu. Projekt je vodila Nacionalna knjižnica Nizozemske (nl. Koninklijke Bibliotheek, engl. National Library of the Netherlands).

[24] Lee, C. A. (2005.), Defining digital preservation work: a case study of the development of the reference model for an open archival information system, str. 131. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/39372/dissertation_callee.pdf?sequence=2&isAllowed=y (20.11.2016.)
[25] Isto, str. 131
[26] NEDLIB project, http://www.dlib.org/dlib/september99/vanderwerf/09vanderwerf.html (20.11.2016.)

NEDLIB je imao za cilj razviti arhitekturalnu okosnicu i osnovne alate za izgradnju depozitnog sustava za elektroničke publikacije, DSEP (engl. Deposit Systems for Electronic Publications).

OAIS referentni model je relevantan za depozitne knjižnice. Mogućnosti takvog modela da može osigurati solidan temelj za standardizaciju unutar elektroničkih arhiva i podrži arhivističke zahtjeve je bio presudan za NEDLIB partnere. Oni su se odlučili za mapiranje DSEP sustava na OAIS, te da detaljno primjene OAIS model unutar DSEP modela za depozitne knjižnice. NEDLIB projekt je na taj način pridonio DSEP implementaciji zadovoljavajući OAIS standard.

Doprinos NEDLIB projekta OAIS projektu[27] je bio u tome što je potaknut DSEP funkcionalnostima, OAIS definirao odvojene entitete za upravljanje podacima (engl. Data-Management Entity) za vizualizaciju metapodataka funkcija obrade.

U nastavku poglavlja slijede zahtjevi po šest osnovnih OAIS funkcionalnih entiteta, te za zajedničke servise.

Stančić u svojoj doktorskoj disertaciji „Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekat“[28] detaljno opisuje OAIS funkcionalne entitete. Vrijedan doprinos navedene disertacije je, međuostalim, i prijevod na hrvatski termina entiteta i funkcija za OAIS model koji će biti korišteni i u sljedećim poglavljima.

2.4.1 Prihvat

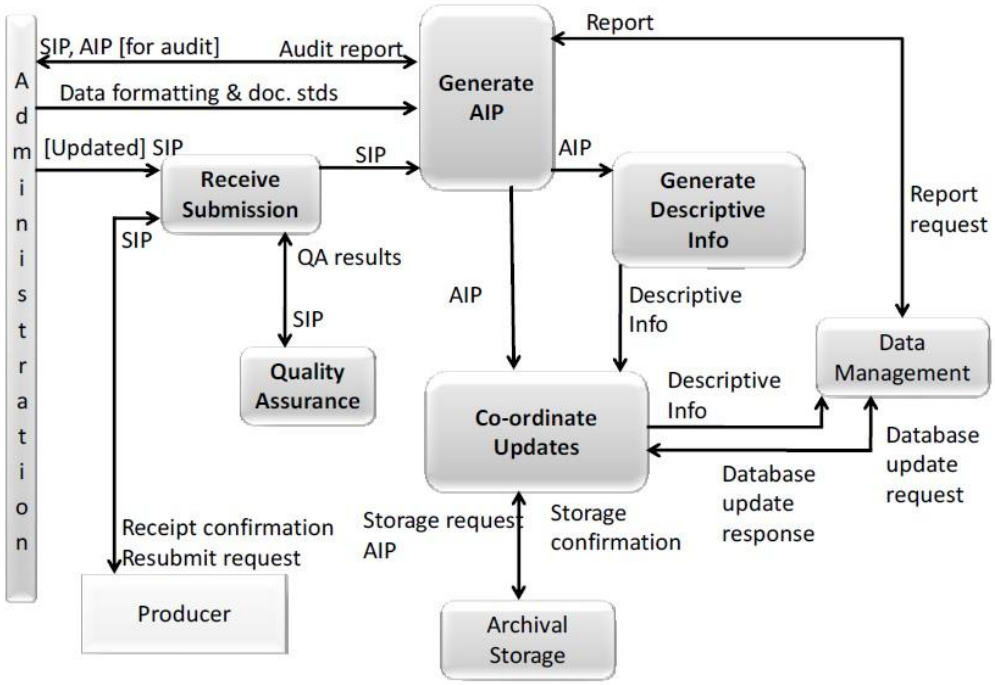
Prihvat (engl. Ingest) je OAIS entitet koji ima funkcije: od proizvođača zaprimiti SIP paket, provjeriti ispravnost i kvalitetu takvog paketa, te obaviti aktivnosti pripremanja paketa za arhiviranje u OAIS arhivu. Entitet prihvat komunicira s OAIS entitetima arhivske pohrane i entitetom za upravljanje podataka. Vrlo je bitan za komunikaciju s

[27] Lee, C. A. (2005.), Defining digital preservation work: a case study of the development of the reference model for an open archival information system, str. 130. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/39372/dissertation_callee.pdf?sequence=2&isAllowed=y (20.11.2016.)

[28] Stančić, H. (2005.), Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata, Doktorska disertacija, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb

proizvođačem zbog rješavanja preuzimanja informacija u OAIS arhiv i njihovog dugoročnog očuvanja.

U nastavku slijedi slika koja ilustrira funkcije prihvata u OAIS referentnom modelu.



Slika 5. Funkcije prihvata, preuzeto iz Consultative Committee for Space Data Systems (2012.)[29]

Funkcija primanja dostavljenih podataka (engl. Receive Submission Function) – funkcija koja osigurava prostor spremišta ili uređaje za primanje SIP paketa od proizvođača.

Funkcija stvaranja arhivskog informacijskog paketa (engl. Generate AIP Function) – ova funkcija transformira dostavljene SIP u AIP pakete.

Funkcija osiguranja kvalitete (engl. Quality Assurance Function) – ova funkcija provjerava ispravnost prijenosa dostavljenih paketa. Dodatno, utvrđuje pogreške u prijenosu ili čitanju s medija ako ih ima.

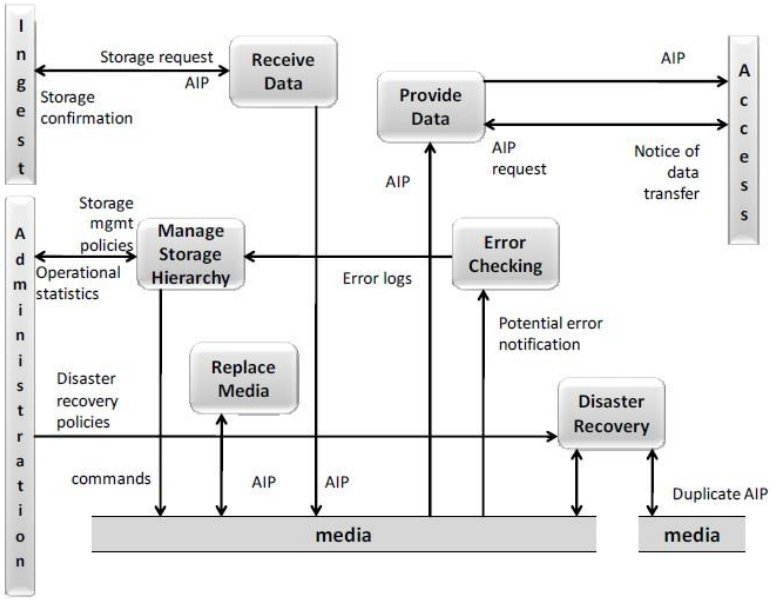
[29] Consultative Committee for Space Data Systems (2012.), Reference model for an open archival information system (OAIS) - 062012 - Magneta book, str. 4-5, slika 4-2, http://public.ccsds.org/publications/archive/650x0m2.pdf (07.08.2016.)

Funkcija koordinacije ažuriranja (engl. Coordinate Updates Function) – funkcija prebacivanja AIP paketa u OAIS entitet arhivske pohrane, te pripadajuće opisne informacije u OAIS entitet upravljanja podacima.

Funkcija stvaranja opisnih informacija (engl. Generate Descriptive Information Function) – funkcija koja iz AIP paketa i drugih izvora izvodi opisne informacije (npr. metapodaci tekstualnog tipa) te takve opisne informacije prosljeđuje funkciji za koordinaciju ažuriranja.

2.4.2 Arhivska pohrana

Arhivska pohrana (engl. Archival storage) je entitet OAIS arhiva koji služi za arhivsku pohranu i dugoročno očuvanje. Ovaj entitet provodi sve potrebne aktivnosti da bi pohranjene informacije bile dugoročno očuvane i dostupne korisnicima arhiva. Aktivnosti za omogućavanje dugoročnog očuvanja su migracija podataka (zbog formata zapisa), osvježavanje medija i dr. Entitet arhivske pohrane komunicira s unutarnjim funkcionalnim elementima OAIS arhiva, tj. ne komunicira direktno sa okolinom OAIS arhiva.



Slika 6. Funkcije arhivske pohrane, preuzeto iz Consultative Committee for Space Data Systems (2012.)[30]

[30] Isto, str. 4-8, slika 4-30

Funkcija primanja podataka (engl. Receive Data Function) – funkcija koja prima AIP i zahtjev za njegovom pohranom od entiteta prihvat. Zaprimljeni paket se dalje prosljeđuje u skladište podataka.

Funkcija upravljanja hijerarhijskim sustavom pohrane (engl. Manage Storage Hierarchy Function) – funkcija koja sprema sadržaj AIP paketa na odgovarajući medij. Za odluku na koji tip medija će sadržaj biti spremljen je presudna učestalost korištenja. S obzirom na učestalost sadržaj može biti spremljen u sljedeće vrste pohrane: izravni (engl. on-line), poluizravni (engl. near-line) ili neizravni (engl. off-line).

Funkcija pribavljanja podataka (engl. Provide Data Function) – funkcionalni entitet pristupa upućuje ovoj funkciji nalog za pribavljanje AIP paketa, a ova funkcija obavlja zadani nalog.

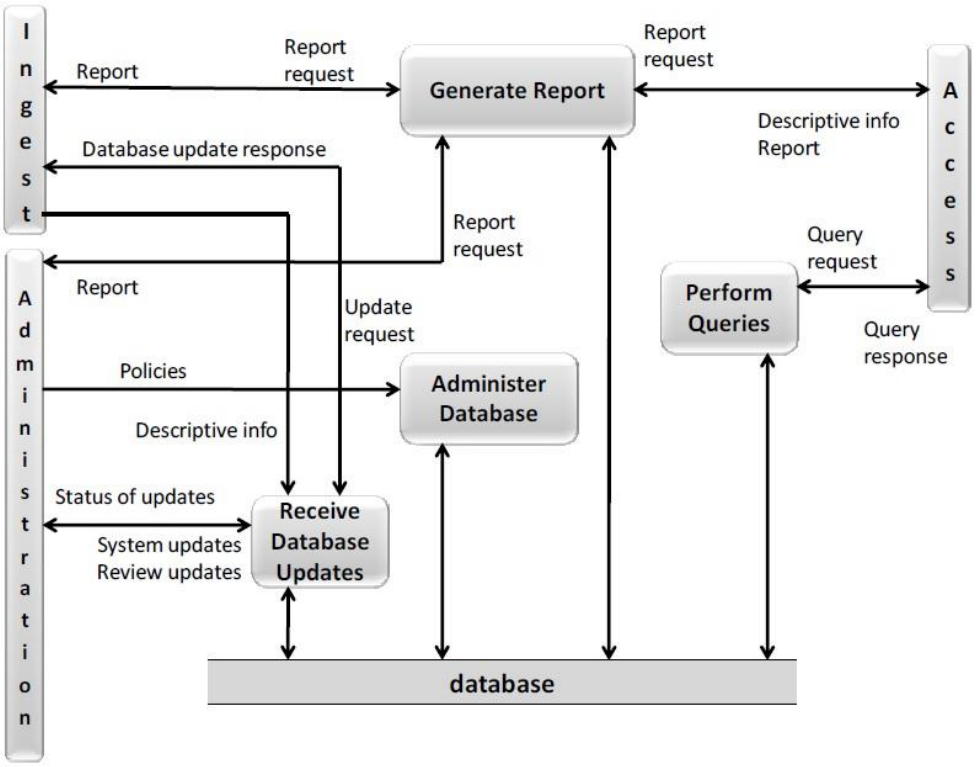
Funkcija ispitivanja pogrešaka (engl. Error Checking Function) – funkcija koja ispituje kvalitetu (fizičku) zapisa prilikom rada (čitanje, zapisivanje, prijenos) s informacijskim objektom. O definiranoj statističkoj razini pogrešaka ovisi hoće li se funkciji upravljanja hijerarhijskim sustavom pohrane dojaviti da je potrebno aktivirati funkciju zamjene medija.

Funkcija obnavljanja u slučaju uništenja (engl. Disaster Recovery Function) – ova funkcija služi sprječavanju gubitaka podataka od kvara na sustavu, požara , poplave i sl. Funkcija obnavljanja u slučaju uništenja izrađuje i održava sigurnosne kopije. Sigurnosne kopije prema definiranim politikama i procedurama trebaju biti spremljene na fizički udaljenim mjestima. Politike i procedure određuje entitet administracije.

Funkcija zamjene medija (engl. Replace Media Function) – ova funkcija provodi postupak migracije AIP paketa vodeći računa o načelu nepromjenjivosti informacije o sadržaju i informacije o opisu zaštite. Za razliku od sadržaja, informacija o pakiranju se smije mijenjati uz pridržavanje pravila da ne smije doći do gubitka informacija.

2.4.3 Upravljanje podacima

Upravljanje podacima (engl. Data management) je OAIS entitet koji je zadužen za održavanje baza podataka koje u sebi čuvaju metapodatke za opisivanje arhiviranih informacijskih objekata. Medapodaci su nužni za alate OAIS arhiva čija je uloga pretraživanje informacija i njihov dohvat. Funkcije ovog OAIS entiteta su i: izrada izvješća kroz postavljanje upita nad bazom podataka, pohranjivanje i izmjene informacija o pristiglim paketima, te brisanje informacija iz sustava. Ovaj entitet služi i za održavanje administrativnih podataka OAIS arhiva.



Slika 7. Funkcije upravljanja podacima, preuzeto iz Consultative Committee for Space Data Systems (2012.)[31]

Funkcija administriranja baze podataka (engl. Administer Database Function) – ova funkcija ima za zadatak održavati integritet baze podataka vodeći se politikama OAIS arhiva. Integritet baze podataka promatramo kroz sistemske i opisne informacija. Sistemske informacije se odnose na interne provjere konzistentnosti baze. Opisne informacije se spremaju zajedno s AIP paketima.

[31] Isto, str. 4-10, slika 4-4

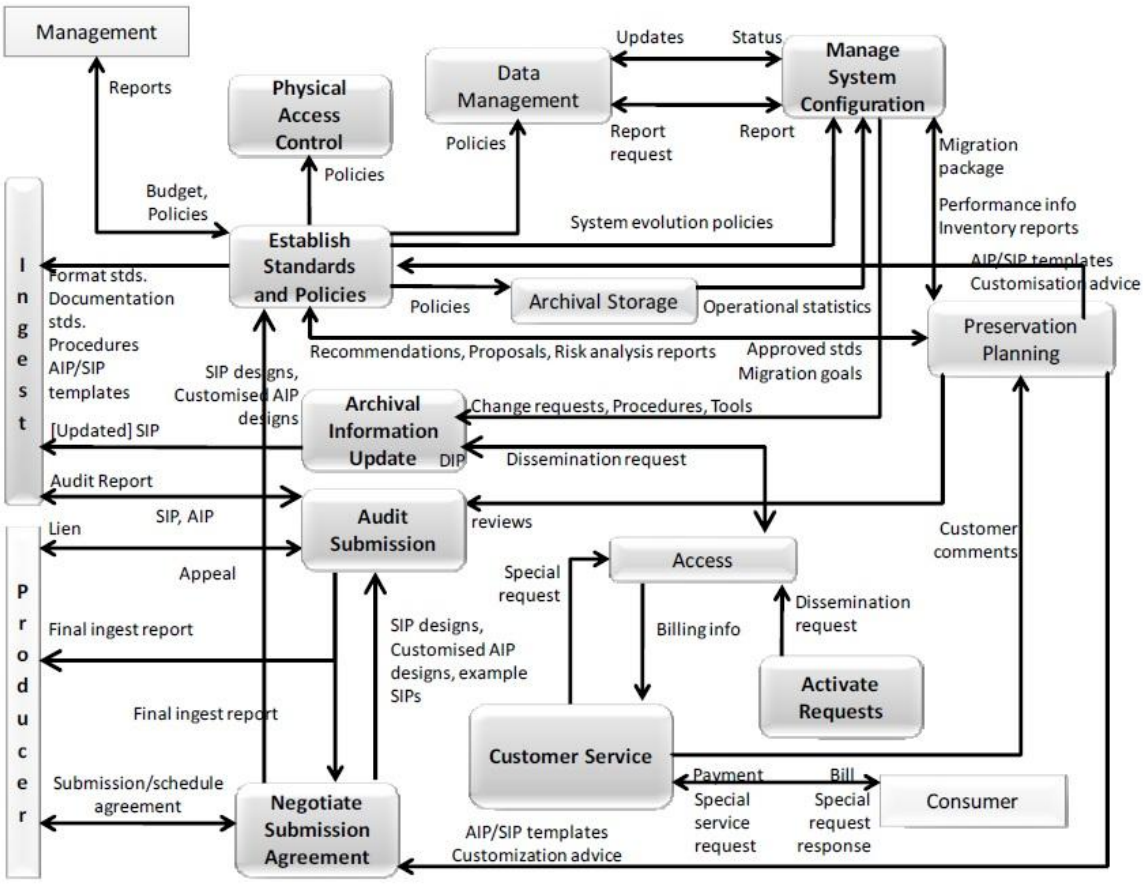
Funkcija primanja ažuriranih podataka (engl. Receive Database Updates Function) - funkcija koja komunicira s funkcijom koordinacije ažuriranja segmenta zaduženog za prihvat te s entitetom administracije (od njega dobiva ažurirane sistemske podatke i revidirane podatke).

Funkcija provođenja upita (engl. Perform Queries Function) – ova funkcija na temelju upita koje dobiva od entiteta zaduženog za pristup pretražuje vlastitu bazu podataka. Rezultate pretrage vraća kroz skupove opisnih informacija.

Funkcija stvaranja izvještaja (engl. Generate Report Function) – funkcija koja stvara izvještaje o korištenju baze podataka. Izvještaji mogu vraćati podatke po različitim kategorijama (npr. po korištenju opisnih informacija, po pronađenim traženim pojmovima i dr.).

2.4.4 Administracija

Funkcionalni OAIS entitet administracije (engl. Administration) ima ulogu pružanja podrške aktivnostima OAIS arhiva. Entitet Administracije koordinira aktivnosti ostalih pet funkcionalnih OAIS entiteta (ovaj entitet je poveznica svih drugih entiteta u OAIS modelu). Administracija komunicira sa svim akterima u OAIS okruženju: proizvođačima, korisnicima te s upraviteljima.



Slika 8. Funkcija Administracije, preuzeto iz Consultative Committee for Space Data Systems (2012.)[32]

Funkcija pregovaranja o ugovoru vezanim za dostavljanje informacijskih paketa (engl. Negotiate Submission Agreement Function) - vrlo je bitna funkcija u OAIS modelu arhiva. Funkcija pregovaranja ima za cilj postizanje dogovora kako standardizirati informacijske pakete sa stvarateljima. Ovim dogovorom se osigurava kompatibilnost unutarnje strukture dostavljenih paketa s unutarnjom strukturom AIP paketa. Postoji povezanost ove funkcije s entitetom zaduženog za planiranje procesa očuvanja (dobivanje savjeta, te uzoraka dostavljenih paketa).

Funkcija upravljanja konfiguracijom sustava (engl. Manage System Configuration Function) - funkcija koja je zadužena za stalno praćenja stanja u arhivu te promjena u OAIS okruženju. Ova funkcija je zadužena za praćenje, planiranje i predviđanje promjena

[32] Isto, str. 4-11, slika 4-5

u postavkama arhiva. Bitna uloga ove funkcije je i očuvanje zapisa o promjenama u sustavu jer se na osnovu njih može dokazivati autentičnost podataka.

Funkcija utemeljenja standarda i politika (engl. Establish Standards and Policies Function) - ova funkcija ima sljedeće odgovornosti: stvaranje i provođenje standarda i politika, te njihovo održavanje. Standardi i politike se propisuju na razini cijelog arhiva. Politike se propisuju za sljedeće postupke u OAIS arhivima: upravljanje pohranom, administracije baze podataka, migracije podataka i dr.

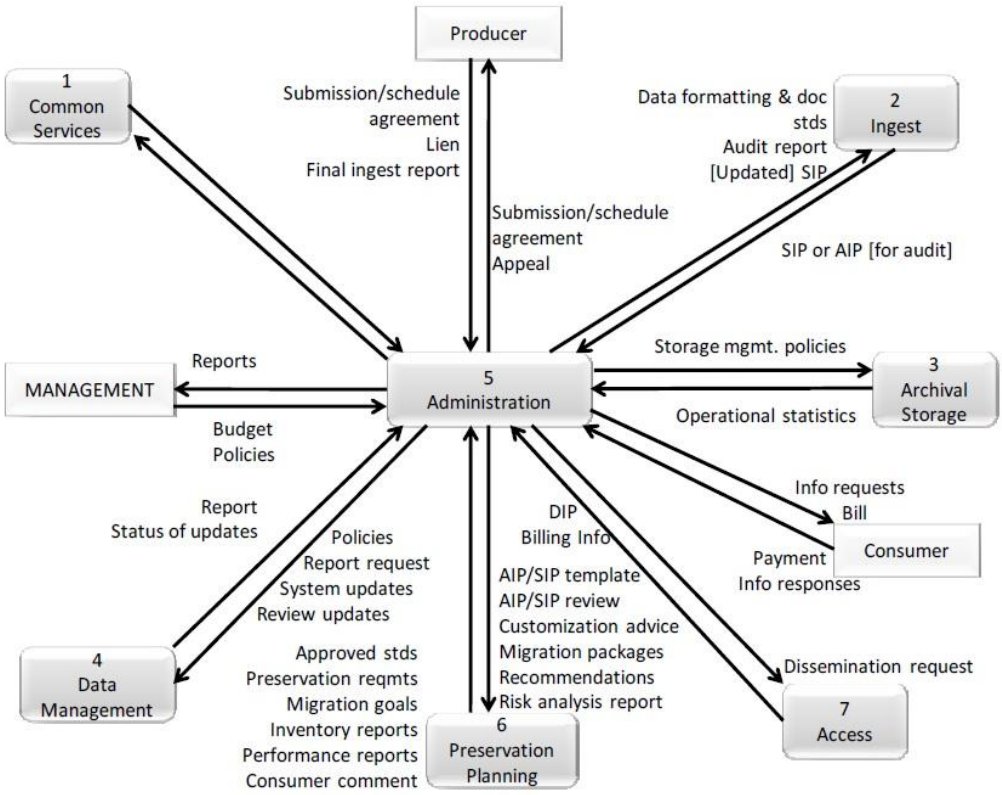
Funkcija ažuriranja arhivskih informacija (engl. Archival Information Update Function) - ova funkcija osigurava mehanizme za ažuriranja AIP paketa. Funkcija upravljanja konfiguracijom sustava šalje ovoj funkciji zahtjev za promjenom, a ova funkcija prosljeđuje zahtjev entitetu pristupa. Entitet pristupa definira upit u odgovarajućem obliku te ga šalje dalje u entitet upravljanja podacima (funkcija provođenja upita). Entitet upravljanja podacima po dobivanju skupova opisnih informacija vraća povratnom linijom rezultate. U entitet prihvata se vraća ažurirani ili novi informacijski paket.

Funkcija pregleda dostavljenih podataka (engl. Audit Submission Function) - to je funkcija koja pregledava i provjerava dostavljene podatke. Funkcija provjerava je li sadržaj dostavljenih informacijskih paketa u skladu s propisanim standardima, te jesu li dostavljene informacije prikladne za unos u OAIS arhiv. Rezultat navedene akcije mogu biti potvrde o ispravnosti i prihvaćanju gradiva koje se šalju entitetu prihvata. Entitet prihvata uzima u obzir zaprimljene potvrde i s obzirom na rezultat potvrde transformira ili ne pakete u AIP.

Funkcija kontrole fizičkog pristupa (engl. Physical Access Control Function) - to je funkcija kontroliranja fizičkog pristupa OAIS arhivu, te njegovih dijelova. Kontrola fizičkog pristupa se provodi elektroničkim zaštitnim mehanizmima na vratima prostorija. Potrebno je uspostaviti i održavati baze djelatnika s podacima o fizičkim pravima pristupa. Potrebno je pratiti propisane politike (drži ih funkcija utemeljenja standarda i politika).

Funkcija aktiviranja zahtjeva (engl. Activate Requests Function) - ova funkcija se obavlja periodično, zahtjevi se pokreću na propisane događaje. Periodički se odvija i provjera sadržaja u arhivu. Provjerava se postoje li i dalje svi podaci potrebni za aktiviranje zahtjeva.

Funkcija korisničkog servisa (engl. Customer Service Function) - ova funkcija održava bazu podataka o korisnicima i njihovim korisničkim računima. Funkcija ima za zadatak korisnicima slati korisničke račune za pojedine usluge OAIS arhiva. Poslije slanja korisničkih računa korisnicima potrebno je pratiti njihovu realizaciju/aktiviranje korištenja usluga. Pod ovom funkcijom su i odgovori na upite korisnika. Slika 9 prikazuje kontekstni dijagram entiteta administracije te zorno ilustrira povezanost ovog entiteta sa svim drugim entitetima u OAIS referentnom modelu, te akterima iz OAIS okruženja.

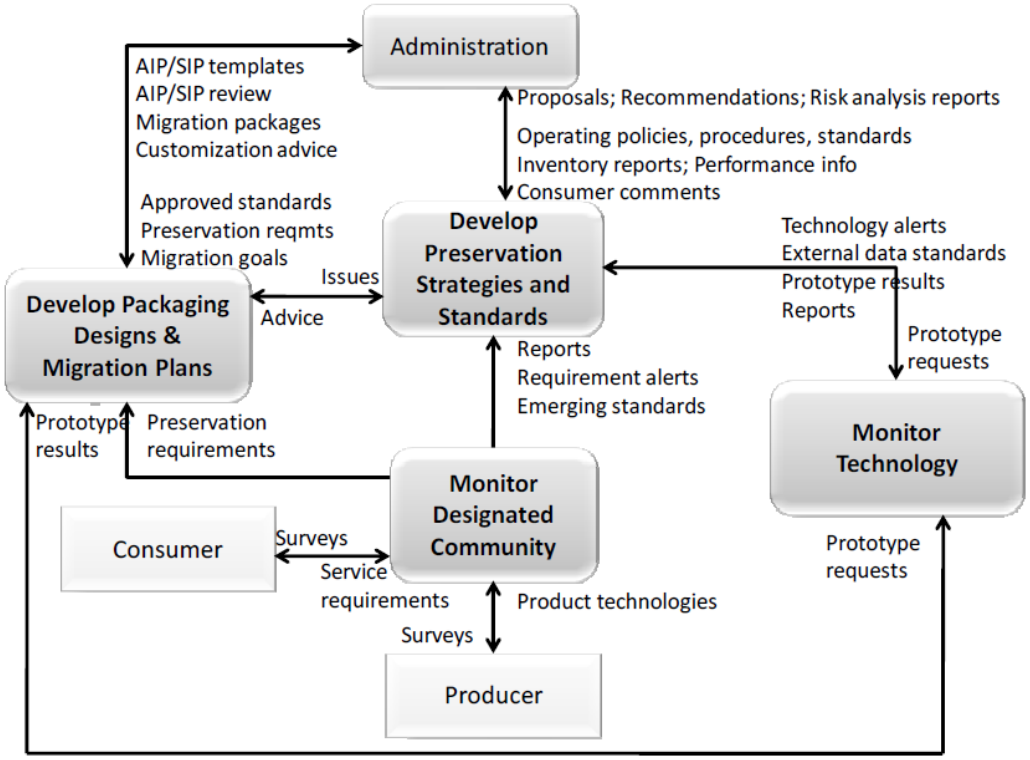


Slika 9. Kontekstni dijagram entiteta Administracije, preuzeto iz Consultative Committee for Space Data Systems (2012.)[33]

[33] Isto, str. 4-19, slika 4-9

2.4.5 Planiranje procesa očuvanja

Planiranje procesa očuvanja (engl. Preservation planning) kao OAIS entitet ima zaduženje skrbi o strategiji dugoročnog očuvanja. Daju se prijedlozi revizije strategije s obzirom na okolnosti u kojim sa nalaze akteri u okruženju OAIS arhiva. Pod praćenje okolnosti u okruženju OAIS arhiva spadaju praćenje stanja tehnološkog razvoja, te praćenje potreba određenih korisničkih skupina.



Slika 10. Funkcija Planiranja procesa očuvanja, preuzeto iz Consultative Committee for Space Data Systems (2012.)[34]

Funkcija praćenja ciljnih korisničkih skupina (engl. Monitor Designated Community Function) - kao što i naziv navodi, funkcija prati okruženje okoline OAIS arhiva. Fokus praćenja su promjene korisničkog interesa, te tehnološke promjene. Neke promjene su miješane prirode, tj. dotiču se i korisničkog interesa i tehnologije, npr. povećanjem mrežne propusnosti povećava se i mogućnost razvijanja novih usluga za krajnje korisnike koje do tada nije bilo moguće razviti.

[34] Isto, str. 4-14, slika 4-6

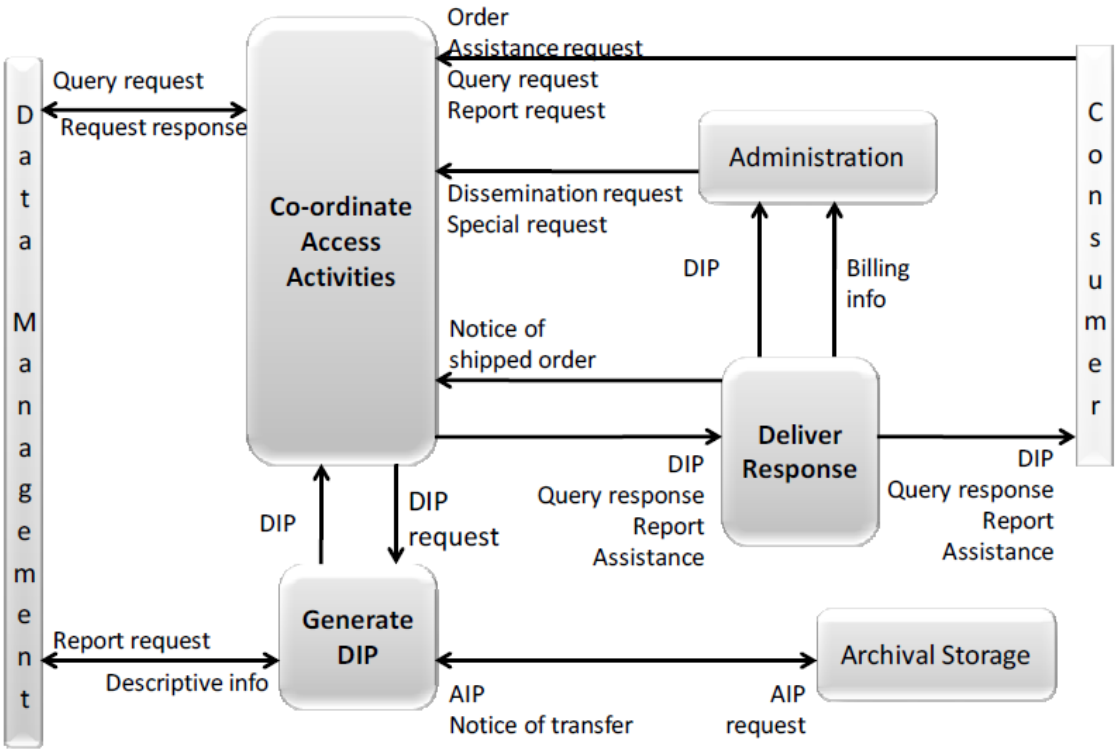
Funkcija praćenja tehnologije (engl. Monitor Technology Function) - prati promjene u tehnologijama (hardver, programske komponente) i standardima koji su nužni za održavanje nezastarijevanje podataka i mogućnosti za njihovo čitanje u arhivu. Po zamjećivanju rizika potrebno je isti dojaviti funkciji razvoja strategija i standarda za proces očuvanja. Cilj navedene dojave je dobivanje povratne informacije ili uputa za razvoj prototipa. Funkcija praćenja tehnologija potom izrađuje prototip nove komponente u OAIS arhivu sukladan zaprimljenim uputama. Prototip se šalje funkciji razvoja dizajna paketa i planiranja migracije.

Funkcija razvoja strategija i standarda za proces očuvanja (engl. Develop Preservation Strategies and Standards Function) - ova funkcija zaprima izvještaja od ostalih funkcija, te provodi postupak odlučivanja o tome hoće li se ili ne mijenjati aktualne strategije i standardi unutar arhiva. Ažurirane strategije i standardi se potom u vidu preporuka šalju funkciji razvoja dizajna paketa i planiranja migracija i entitetu administracije (funkcija utemeljenja standarda i politika).

Funkcija razvoja dizajna paketa i planiranja migracije (engl. Develop Package Designs and Migration Plans Function) - ova funkcija zaprima upute i preporuke od već spomenutih funkcija: funkcije utemeljenja standarda i politika u segmentu administracije, funkcije razvoja strategija i standarda za proces očuvanja, funkcije praćenja tehnologije i funkcije praćenja ciljnih korisničkih skupina. Na osnovu zaprimljenih uputa i preporuka dizajnira nove pakete. Slično se događa i s planovima migracije zapisa.

2.4.6 Pristup

Pristup (engl. Access) je OAIS funkcionalni entitet koji ima funkcije koje osiguravaju korisničkim skupinama pristup informacijama kao što su: pretraživanje, pronalaženje i sl. Pristup preuzima AIP od entiteta arhivske pohrane, pretvara ga u DIP, prosljeđuje ga funkciji koordinacije pristupnih aktivnosti. Nakon toga ga u suradnji sa funkcijom upravljanja šalje korisniku kojem takav podatak treba.



Slika 11. Funkcije Pristupa, preuzeto iz Consultative Committee for Space Data Systems (2012.)[35]

Funkcija koordinacije pristupnih aktivnosti (engl. Coordinate Access Activities Function) - odgovorna je za predstavljanje sučelja za korisnike za pretraživanje i pristupanje podacima OAIS arhivu. Postoje različiti tipovi pretraživanja i pristupanja podacima: klasični upiti, specifični zahtjevi za izvještajima, zahtjevi za očuvanim zapisima i opći zahtjevi za pomoć.

Funkcija stvaranja diseminacijskog informacijskog paketa (engl. Generate Dissemination Information Package (DIP) Function) - ova funkcija pribavlja AIP-e iz entiteta arhivske pohrane, te opisne informacije iz entiteta upravljanja podacima. Od pribavljenih podataka iz obadva izvora stvara DIP paket. DIP paket se nakon toga dostavlja funkciji koordinacije pristupnih aktivnosti.

Funkcija isporuke odgovora (engl. Deliver Response Function) - ova funkcija prima DIP paket, te zaprimljeni paket isporučuje korisnicima. Funkcija isporuke odgovora

[35] Isto, str. 4-16, slika 4-7

komunicira s entitetom administracijom radi naplate usluga.

2.4.7 Zajedničke usluge

Na razini OAIS arhiva postoje usluge koje su zajedničke svim entitetima, te one predstavljaju podršku svim funkcijama u arhivu. Takve usluge se zovu zajedničke usluge[36] (engl. Common Services).

Usluge operacijskog sustava (engl. Operating System Services) – omogućavaju izvođenje aplikacija, te administriranje OAIS arhiva. Ove usluge uključuju sljedeće:

- Kernel operacije,
- Naredbe i alate koji uključuju mehanizme za operacije na operaterskoj razini (npr. usporedba, ispisivanje i prikazivanje sadržaja datoteka, editiranje datoteka),
- Ekstenzije u realnom vremenu (npr. za aplikacije koje zahtijevaju deterministično izvođenje),
- Upravljanje sustavom,
- Sigurnosne usluge operacijskog sustava (npr. kontrole pristupa sistemskim podacima).

Mrežne usluge (engl. Network services) – ove usluge omogućavaju mehanizme za mrežnu podršku, te pristup OAIS arhivima koji su međusobno umreženi. Osim toga, omogućava se i interoperabilnost među heterogenim umreženim sustavima. Ove usluge uključuju sljedeće:

- Aplikativna programska sučelja (API) i specifikacije protokola,
- Transparentni pristup datotekama bilo gdje u heterogenoj mreži,
- Podrška za osobna i mikro računala,
- Pozivi udaljenih procedura (RPC),
- Mrežne sigurnosne usluge (npr. za neporecivost, zaštitu integriteta i sl.).

Sigurnosne usluge (engl. Security services) – to su usluge koje omogućavaju zaštitu sustava u cjelini, ali i određivanje razine zaštite pojedine komponente ili specifičnih informacija.

[36] Consultative Committee for Space Data Systems (2012.), Reference model for an open archival information system (OAIS) - 062012 - Magneta book, str. 4-3, http://public.ccsds.org/publications/archive/650x0m2.pdf (27.11.2016.)

Sigurnosne usluge su sljedeće:

- Usluge autentikacije,
- Usluge dozvole pristupa,
- Usluge zaštite integriteta,
- Usluge zaštite povjerljivosti podataka,
- Usluge neporecivosti.

2.5 PERSPEKTIVE I PRIMJENE OAIS REFERENTNOG MODELA

OAIS referenti model je jako složen i apstraktan. Zbog toga se iz njega teško može odmah implementirati konkretan arhiv. Dakle, OAIS se ne može strogo preslikati na konkretnu implementaciju jer ne određuje kako izraditi neki konkretni elektronički arhiv. OAIS po entitetima pruža samo teoretsku razradu o strukturi i komunikaciji. Ne nude se, dakle, informacije ili sugestije o tehnologijama koje bi se mogle upotrijebiti u implementaciji takvog arhiva ili pojedinih njegovih komponenti.

Lavoie u dokumentu Uvoda u referentni OAIS model navodi[37] da je OAIS apstraktni model ili domenski specifična ontologija koja se sastoji od skupa međusobno povezanih koncepata. Navedene koncepte su izradili stručnjaci ili tijela sastavljena od stručnjaka nastojeći ohrabriti čistu komunikaciju. Ovaj referentni model ima za cilj definirati osnovne funkcionalne komponente sustava dedicirane dugoročnom očuvanju digitalnih informacija. Lavoie dalje navodi da referentni model može biti primijenjen na dugoročno očuvanje objekata u bilo kojoj formi uključujući fizičke objekte. Dakle, referentni model ne uvjetuje tip informacija koje bi trebale biti sačuvane. Tako primjerice informacija koja se čuva u ovakvom modelu može biti i običan kamen. Dakle, riječ je o apstraktnom modelu, a ne implementaciji i konkretnim tehnologijama i tehničkim detaljima.
OAIS je originalno razvijen od strane CCSDS organizacije, tijela kojem je namjena nadgledanje svemirskih agencija. Međutim digitalno očuvanje je postala samostalna disciplina, a OAIS je postao standardni model za izradu sustava za digitalno očuvanje za

[37] Lavoie, B. (2014.), The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition), DPC Technology Watch Series Report 14-02, str. 3; https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file (28.11.2016.)

mnoge institucije i organizacije[38]. Sukladnost s OAIS referentnim modelom je postao temeljni uvjet dizajna elektroničkih arhiva za mnoge nacionalne arhive i organizacije koje se bave upravljanjem zapisa. Primjeri su mnogi:

- NARA - Nacional Archives and Record Administration, SAD[39],
- Kongresna biblioteka (engl. Library of Congress), SAD [40],
- Nacionalna biblioteka Britanije (engl. British Library), VB[41],
- Nacionalna biblioteka Francuske (fra. Bibliothèque nationale de France), FRA[42],
- Koninklijke Bibliotheek (nl. National Library of the Netherlands), NIZ[43],
- ….

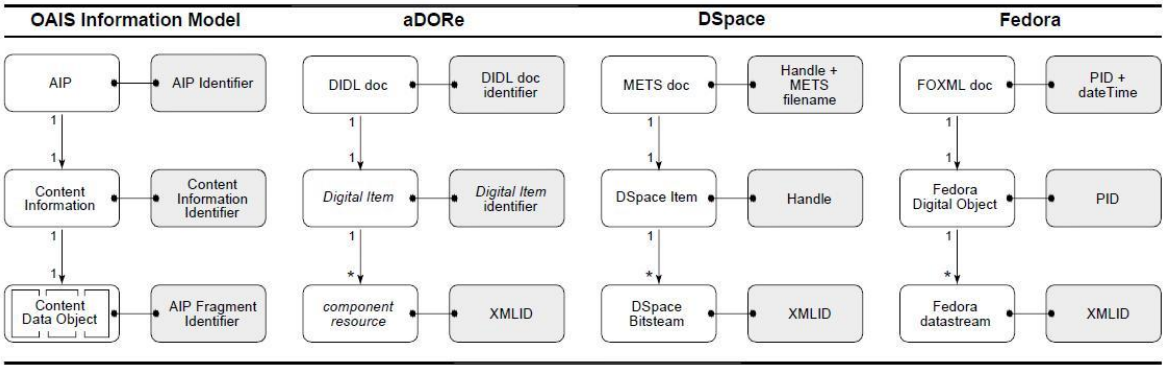
Bekaert i Van de Sompel donose[44] vrlo zanimljivo mapiranje koncepata OAIS referentnog modela na sustave aDORe, DSpace i Fedora. Danas postoji velik broj razvijenih i prilagođenih različitih digitalnih repozitorija i arhivskih sustava, heterogenih s obzirom na tipove medija.

Primjeri takvih informacijskih sustava koje su Bekaert i Van de Sompel uzeli u razmatranje su:

- aDORe, arhitektura arhiva dizajniranog i implementiranog u instituciji Research Library of the Los Alamos National Laboratory[45],
- DSpace, sustav elektroničkog arhiva izgrađen zajedničkim radom MIT Libraries i Hewlett-Packard (HP) tvrtke[46],
- Fedora, aplikativno rješenje otvorenog koda razvijano zajedničkim radom Cornell University i University of Virginia[47].

[38] OAIS, wikipedia, https://en.wikipedia.org/wiki/Open_Archival_Information_System#Adoption (28.11.2016.)
[39] Nacional Archives and Record Administration, SAD, https://www.archives.gov/ (28.11.2016.)
[40] Library of Congress, https://www.loc.gov/ (28.11.2016.)
[41] British Library, http://www.bl.uk/ (28.11.2016.)
[42] Bibliothèque nationale de France, http://www.bnf.fr/fr/acc/x.accueil.html (28.11.2016.)
[43] Koninklijke Bibliotheek (nl. National Library of the Netherlands), https://www.kb.nl/en (28.11.2018.)
[44] Jeroen, B., Van de Sompel, H. (2005.), Access Interfaces for Open Archival Information Systems based on the OAI-PMH and the OpenURL Framework for Context-Sensitive Services, Digital Library Research & Prototyping Team, Los Alamos National Laboratory, Dept. of Architecture and Urbanism, Faculty of Engineering, Ghent University, http://www.ukoln.ac.uk/events/pv-2005/pv-2005-final-papers/032.pdf (28.11.2016.)
[45] Bekaert, J., Liu, X., Van de Sompel, H. (2005.), aDORe - A Modular and Standards-Based Digital Object Repository at the Los Alamos National Laboratory, Los Alamos National Laboratory, https://pdfs.semanticscholar.org/09f9/ad95b839780705725b6afb2f56e91436c0d9.pdf (28.11.2016.)
[46] Dspace, https://dspace.mit.edu/ (28.11.2016.)
[47] Fedora, http://fedorarepository.org/about (28.11.2016.)

Svi ti sustavi mogu pohranjivati različite vrste digitalnog sadržaja, te osiguravaju alate za spremanje, upravljanje i pristup digitalnom sadržaju. Navedeni sustavi imaju slične ciljeve, ali svaki od njih donosi svoju perspektivu kako osigurati zacrtane ciljeve.
Autori su istražili kako se specifična svojstva podatkovnih modela koji pokrivaju aDORe, DSpace i Fedora sustave mogu mapirati na koncepte OAIS informacijskog modela. Naglasak je bio na svojstvima koja su ključna za pristupna sučelja, upravljanje identifikatorima i verzije digitalne imovine. Istražena mapiranja su ilustrirana na slici 12.



Slika 12. Mapiranje OAIS koncepta na aDORe, Dspace i Fedora sustave, preuzeto iz Jeroen, B., Van de Sompel, H. (2005.)[48]

U aDORe okruženju se objekti predstavljaju pomoću MPEG-21 DID apstraktnog modela te se serijaliziraju koristeći MPEG-21 DIDL sintaksu. U MPEG-21 modelu, digitalni sadržaj se naziva digitalni artikl (engl. Digital Item) te je informacija od primarnog interesa za krajnjeg korisnika u MPEG-21 okruženju. XML dokument koji pakira i serijalizira digitalni artikl naziva se DIDL dokument. ADORe digitalni artikl se mapira u OAIS informacije o sadržaju (engl. Content Information). DIDL XML dokumenti koji pakiraju digitalne artikle se mapiraju u OAIS AIP pakete.

DSpace Data Model je takav model u kojem je svaki DSpace artikl (engl. DSpace Item) predstavljen kao XML dokument kroz Metadata Encoding and Transmission Standard (METS) sintaksu. U ovakvom modelu DSpace artikl koji predstavlja odgovarajući sadržaj

[48] Jeroen, B., Van de Sompel, H. (2005.), Access Interfaces for Open Archival Information Systems based on the OAI-PMH and the OpenURL Framework for Context- Sensitive Services, Digital Library Research & Prototyping Team, Los Alamos National Laboratory, Dept. of Architecture and Urbanism, Faculty of Engineering, Ghent University, http://www.ukoln.ac.uk/events/pv-2005/pv-2005-final-papers/032.pdf , str. 6, slika 3 (28.11.2016.)

se mapira u OAIS informacije o sadržaju (engl. Content Information). METS XML dokument koji predstavlja i serijalizira sadržaj kao pohranjiv paket se u OAIS smislu može usporediti s AIP paketom.

Složeni digitalni sadržaj pohranjen u Fedora repozitoriju je predstavljen kroz Fedora Digital Object Model i kodiran koristeći FOXML sintaksu. Digitalni artikli se označavaju kao Fedora digitalni objekti, te se mapiraju u OAIS konceptu u OAIS informacije o sadržaju (engl. Content Information). Serijalizacija Fedora digitalnih objekata u FOXML se naziva FOXML dokument. Ova serijalizacija mapira FOXML u OAIS AIP paket.

2.6 ZAKLJUČAK

Arhivistika se bavi pitanjima vezanim za područja tradicionalne arhivistike, ali i konkretnim, modernim pitanjima[49]: Kako dugoročno očuvati digitalizirano i digitalno gradivo? Kako očuvati autentičnost, integritet, vjerodostojnost, pouzdanost i iskoristivost elektroničke građe tijekom mnogih i stalnih tehnoloških promjena?

S obzirom na dugoročno očuvanje elektroničkih informacijskih objekata, svaki takav objekt se može promatrati kroz tri razine njegovih karakteristika: fizičku, logičku i konceptualnu. Kod klasičnih dokumenata autentičnost se provjerava na originalnom dokumentu, a provjera autentičnosti elektroničkih informacijskih objekata je daleko kompliciranija. Kod provjere autentičnosti elektroničkih informacijskih objekata kompliciranа je sama složenost takvih objekata i metoda kojim se nastoji očuvati dugoročna čitljivost takvih objekata. Thibodeau[50] navodi inherentni paradoks vezan uz očuvanje elektroničkih informacijskih objekata. S jedne strane ima za zadatak dostaviti povijest u budućnost u nepromijenjenom, autentičnom stanju, a s druge strane dohvat takvog sadržaja iz prošlosti neizbježno zahtijeva određene izmjene. Ovaj paradoks može biti riješen samo kroz razradu referentnog modela za digitalno očuvanje koji definira organizaciju, djelovanje i suradnju elektroničkih arhiva. Takav referentni model za otvoreni arhivski informacijski sustav (OAIS) je razvio Consultative Committee for Space Data

[49] Odsjek za informacijske i komunikacijske znanosti Filozofskog fakulteta u Zagrebu, Arhivistika i dokumentalistika, http://inf.ffzg.unizg.hr/index.php/hr/odsjek/katedre/arhivistika-i-dokumentalistika (03.08.2016.

[50] Thibodeau, K. (2002.), Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, u: The State of Digital Preservation: An International Perspective, Council on Library and Information Resources (CLIR), Washington, D.C., SAD, str. 28, https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10 (07.08.2016.)

Systems (CCSDS) pri američkoj agenciji NASA-i 1999. godine. Ovaj model je artikuliran kao međunarodni ISO standard (OAIS referentni model) te je prvotno pokriven i ISO standardom ISO 14721:2003 (Space data and information transfer systems - Open archival information system - Reference model). OAIS referentni model je predstavljao osnovu za razvoj nekih projekata kao što je InterPARES projekt. OAIS je razvijen za dugoročno očuvanje bilo koje vrste artefakata (bilo u digitalnom ili fizičkom obliku).

OAIS referentni model se sastoji od tri dijela koja su međusobno povezana: okoline u kojoj OAIS arhiv djeluje, funkcionalnih entiteta i informacijskih objekata. Okoline u kojoj OAIS arhiv djeluje su: proizvođači, korisnici i upravitelji.

Funkcionalni entiteti OAIS modela osiguravaju ulogu dugoročnog očuvanja u OAIS arhivu i ima ih šest: prihvat, arhivska pohrana, upravljanje podacima, administracija, planiranje procesa očuvanja i pristup.

Corado i Moulaison navode[51] da OAIS arhiv ima još jedan funkcionalan entitet, a to su zajedničke usluge koje podrazumijevaju: operacijski sustav, datotečni sustav, usluge mrežne infrastrukture i dr.

Informacijski objekt Stančić definira[52] kao objekt koji predstavlja bilo koje gradivo koje pruža informaciju bez obzira nalazio se on u analognom ili digitalnom (elektroničkom) obliku, pri čemu su računala samo jedna od metoda i tehnika njegove obrade. Informacijski paket je strukturirani paket, tj. struktura koja logički objedinjuje više vrste informacijskih objekata. Informacijski paketi mogu biti: SIP (Dostavljeni informacijski paket), AIP (Arhivski informacijski paket) i DIP (Diseminacijski informacijski paket).

RFC 4810 iz 2007. (Long-Term Archive Service Requirements) [53] popisuje zahtjeve koje trebaju zadovoljiti servisi za dugoročnu pohranu, a donosi i termin servisa dugoročne pohrane ili LTA (engl. Long-Term Archive Service).

Lavoie u dokumentu Uvoda u referentni OAIS model navodi[54] da je OAIS apstraktni model ili domenski specifična ontologija koja se sastoji od skupa međusobno povezanih koncepata.

---

[51] Corrado, M. C., Moulaison, H. L. (2014.), Digital preservation for libraries, archives, & museums, izdavač: Rowman & Littlefield, Plymouth, str. 48

[52] Stančić, H. (2004.), Očuvanje elektroničkih informacijskih objekata: arhivi, knjižnice, muzeji – zajednička koncepcija, u: Katić, Tinka (ur.), Zbornik 7. seminara Arhivi, knjižnice, muzeji, Hrvatsko knjižničarsko društvo, Zagreb, str. 26-35.

[53] Wallace C., Pordesch U., Brandner R.(2007.), RFC 4810, Long-Term Archive Service Requirements, https://tools.ietf.org/html/rfc4810 (06.12.2016.)

OAIS je originalno razvila CCSDS organizacija (tijelo za nadgledanje svemirskih agencija), ali je kroz vrijeme OAIS postao standardni model za izradu sustava za digitalno očuvanje za mnoge institucije i organizacije. Sukladnost s OAIS referentnim modelom je postao temeljni uvjet dizajna elektroničkih arhiva za mnoge nacionalne arhive i organizacije koje se bave upravljanjem zapisa. Primjeri su mnogi među nacionalnim i kongresnim bibliotekama: Nizozemske, Britanije, Francuske, SAD-a,….

Bekaert i Van de Sompel donose[55] vrlo zanimljivo mapiranje koncepata OAIS referentnog modela na sustave: aDORe (arhitektura arhiva dizajniranog i implementiranog u instituciji Research Library of the Los Alamos National Laboratory), DSpace (sustav elektroničkog arhiva izgrađen zajedničkim radom MIT Libraries i Hewlett-Packard) i Fedora (aplikativno rješenje otvorenog koda razvijano zajedničkim radom Cornell University i University of Virginia).

[54] Lavoie, B. (2014.), The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition), DPC Technology Watch Series Report 14-02, str. 3; https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file , str. 3. (28.11.2016.)

[55] Jeroen, B., Van de Sompel, H. (2005.), Access Interfaces for Open Archival Information Systems based on the OAI-PMH and the OpenURL Framework for Context-Sensitive Services, Digital Library Research & Prototyping Team, Los Alamos National Laboratory, Dept. of Architecture and Urbanism, Faculty of Engineering, Ghent University, http://www.ukoln.ac.uk/events/pv-2005/pv-2005-final-papers/032.pdf (28.11.2016.)

3. INFRASTRUKTURA JAVNOG KLJUČA (PKI)

Razvoj informacijskih i komunikacijskih tehnologija je doveo do toga da se razmjena povjerljivih podataka odvija svakodnevno. Kod korištenja usluga elektroničkog bankarstva, slanja elektroničke pošte i drugih usluga koje podrazumijevaju korištenje i razmjenu povjerljivih podataka izuzetno je bitno da ne može doći do neovlaštenog pristupa podacima koji se razmjenjuju. Kako bi se razmjena povjerljivih podataka između dvije strane učinila sigurnijom, podaci se modificiraju na način da ih osoba kojoj informacije nisu namijenjene ne može protumačiti u slučaju da dođe do takvih podataka.
Infrastruktura javnog ključa, PKI[56] (engl. *Public Key Infrastructure*), je složen sustav koji se temelji na asimetričnoj kriptografiji. Ideja o infrastrukturi javnog ključa je nastala sedamdesetih godina 20. stoljeća. Tada je postojala simetrična kriptografija, tj. kriptografija temeljena na tajnom ključu. Najveći problem simetrične kriptografije je bio kako na siguran način razmijeniti tajni ključ putem nesigurnog kanala. Znanstvenici W.Diffie i M.Hellman su 1976. objavili znanstveni rad *"New Directions in Cryptography*"[57]. Autori su u tom radu iznijeli ideju razmjene tajnog ključa temeljenu na asimetričnoj kriptografiji. Asimetrična kriptografija[58] je kriptografija temeljena na javnom i privatnom ključu. Asimetrična kriptografija je bila temelj i za pojavu digitalnih certifikata, te za elektroničko potpisivanje podataka. Kako su se sve više razvijale informacijsko-komunikacijske tehnologije, npr. internet kao nesigurni kanal, tako je i rasla potreba većeg korištenja infrastrukture javnog ključa koja omogućuje sigurnu komunikaciju.

Nadalje, u ovom poglavlju će se opisati PKI standardi (X.509, PKCS i ostali). Detaljno će biti opisana i PKI arhitektura, tj. arhitektura javnog ključa. Navest će se funkcionalnosti infrastrukture javnog ključa (registracija, inicijalizacija i dr.).

U zasebnom potpoglavlju će biti detaljno opisane osnovne komponente PKI infrastrukture: certifikacijska služba (CA, engl. Certification Authority), registracijska

[56] PKI (engl. public key infrastructure), http://searchsecurity.techtarget.com/definition/PKI (06.03.2015.)
[57] Diffie, W., E., Hellman, M. (1976.), New Directions in Cryptography,IEEE Transactions on information theory, vol. IT22, no. 6, http://www-ee.stanford.edu/~hellman/publications/24.pdf (28.11.2016.)
[58] Asymmetric cryptography (public-key cryptography), http://searchsecurity.techtarget.com/definition/asymmetric-cryptography (6.3.2015.)

služba (RA, engl. Registration Authority), repozitorij ili baza valjanih i opozvanih certifikata (engl. Certificate/CRLRepository) i dr.

Na kraju ovog poglavlja će se opisati pojmovi digitalnih certifikata i vremenskih žigova. Certifikati i vremenski žigovi su izuzetno bitni za ovaj rad kao PKI elementi nužni za realizaciju dugotrajne pohrane elektronički potpisanih zapisa tako da će biti opisano područje njihove primjene i pravni okvir za njihovo korištenje (s naglaskom na ključne uredbe Europske unije čiju stečevinu preuzima i Republika Hrvatska).

3.1 KRIPTOGRAFIJA

Kriptografija[59] je znanost o primjeni kompleksne matematika za povećanje sigurnosti elektroničkih transakcija. Ova znanost se može podijeliti na kriptoanalizu i kriptologiju.

Kriptoanaliza[60] (od grčkog kryptós (skriveno) i analýein (razmrsiti)) je grana kriptografije koja predstavlja proučavanje metoda za saznavanje šifriranih informacija, bez posjedovanja tajnih podataka koji su obično potrebni da bi se pristupilo tim informacijama. Dakle, pod ovim se obično podrazumijeva pronalaženje tajnog ključa, tj. analiziranje novih algoritama i testiranje njihovih ranjivosti.

Kriptologija[61] (od grčkog kryptós (skriveno) i logos - znanje, znanost) je grana kriptografije koja se bavi izučavanjem i definiranjem metoda za zaštitu informacija, te izučavanjem i pronalaženjem metoda za otkrivanje šifriranih informacija. Kriptoanalizom se bave stručnjaci koji analiziraju nove algoritme, te testiraju njihove ranjivosti. Kriptologijom se bave znanstvenici koji pronalaze nove kriptografske algoritme.

Kriptografija je bitno utjecala na mnoge ratne sukobe u povijesti. Knjiga D.Khana "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet"[62] daje prikaz povijesti upotrebe kriptografije kroz ratne sukobe uključivši i drugi svjetski rat. Korištenje kriptografije je do 60-ih godina prošlog stoljeća, tj. do pojave suvremenih informacijsko-komunikacijskih tehnologija bilo vezano uz vojne i

[59] Kutičić, D., Infrastruktura javnog ključa - PKI, Otvoreni sustavi i sigurnost, http://security.foi.hr/wiki/index.php/Infrastruktura_javnog_klju%C4%8Da_-_PKI (04.03.2015.)
[60] Kriptoanaliza, http://hr.wikipedia.org/wiki/Kriptoanaliza (04.03.2015.)
[61] Kriptologija, http://hr.wikipedia.org/wiki/Kriptologija (04.03.2015.)
[62] Kahn, D. (1996.), The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised edition, New York, Scribner, http://math.boisestate.edu/~liljanab/MATH509Spring2012/IndexCoincidence.pdf (04.03.2015.)

obavještajne svrhe. Do tada je postojao i nedostatak javnosti raspoložive literature. Ta nedostupnost literature nije značila da se ova znanost ne razvija, već samo da se pažljivo skrivala unutar raznih vojnih i obavještajnih službi koje su se bavile ovakvim istraživanjima. Međutim, i u tome su postajali neki izuzeci, a to su dva znanstvena članka koja su nastala kao rezultat aktivnog djelovanja autora članaka u području kriptografije u prvom i drugom svjetskom ratu. William F. Friedman je 1920. objavio članak "The Index of Coincidence and Its Applications in Cryptography"[63], a Claude E. Shannon je 1949. objavio članak "The Communication Theory of Secrecy Systems"[64] objavljen 1949. Ova dva članka su i dala neke od temelja za razvoj kriptografije. Od 60-tih godina prošlog stoljeća dolazi do ozbiljnog korištenja informacijsko-komunikacijskih tehnologija u korporacijama. Korporacije su imale namjeru štititi svoje podatke na računalima, te komunikaciju između računala. Iz tog razloga dolazi i do širenje primjene kriptografije i kriptografskih metoda i izvan dosadašnje primjene – vojne i obavještajne. Američka korporacija IBM je 1971. prva u privatnom sektoru objavila rezultate kriptografskog istraživanja. Tim IBM-ovih znanstvenika pod vodstvom H.Feistela je razvio kriptografski algoritam simetrične kriptografije – Lucifer[65]. Na osnovu tog algoritma je 1977. razvijen američki standard DES[66] (engl. Data Encryption Standard) algoritam simetrične kriptografije. On je jedan od najpoznatijih i najraširenijih algoritama u području kriptografije tajnog ključa (engl. secret key cryptography). DES algoritam je postao najpoznatiji kriptografski algoritam ikada, te se i danas koristi za aktivnosti kriptiranja u poslovne svrhe. Tek je 2001. odabran novi američki standard – AES (eng. Advanced Encryption Standard)[67]. Ta specifikacija za kriptiranje elektroničkih podataka je utemeljena od strane američkog Nacionalnog instituta standarde i tehnologije (NIST[68] – National Institute of Standards and Tehnology). Rijndael je algoritam koji je NIST odabrao kao kandidat za Advanced Encryption Standard (AES). Rijndeal je razvijen od strane dvojice belgijskih kriptografskih znanstvenika - Joan Daemena i Vincent Rijmen. Rijndael je vrsta algoritama s različitim ključevima i veličinama blokova. AES je postao

[63] Friedman, W. F. (1987.), The Index of Coincidence and Its Applications in Cryptography, A Cryptographic series, Riverbank Publication No. 22, Riverbank Labs, 1920. Reprinted by Aegean Park Press
[64] Shannon, C.E. (1949.), Communication Theory of Secrecy Systems, Bell System Tehnical Journal, v. 28, n.4, str. 656-715, http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf (04.03.2015.)
[65] Smith, J.L. (1971.), The Design of Lucifer, a Cryptographic Device for Data Communications, IBM Research Report RC3326, Yorktown Heights, New York, 1971.
[66] DES – Data Encryption Standard, http://hr.wikipedia.org/wiki/Data_Encryption_Standard (04.03.2015.)
[67] AES – Advanced Encryption Standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard (04.03.3015.)
[68] NIST – National Institute of Standards and Technology, http://www.nist.gov/ (04.03.2015.)

američki federalni standard 2002. poslije odobrenja američkog Ministarstva trgovine, te je uključen u ISO/IEC 18033 standard[69].

Američki znanstvenici W. Diffie i M. Hellman su 1976. objavili znanstveni rad "New Directions in Cryptography"[70]. Taj rad je predstavio sasvim novi koncept kriptografije - asimetričnu kriptografiju. Za razliku od simetrične kriptografije, asimetričnom kriptografijom je bilo moguće kriptirati poruku jednim, a dekriptirati drugim ključem. Za ovaj rad je bitno i što je definirao siguran način razmjene ključeva koji se može primijeniti u simetričnoj kriptografiji. Diffie i Hellman su dobro osmislili koncept asimetrične kriptografije, međutim nisu objasnili način kako taj koncept realizirati. Pozitivan odjek navedenog rada je bio što su potaknuta mnoga istraživanja u pravcu realizacije koncepta asimetrične kriptografije. Vrlo brzo su znanstvenici R. L. Rivest, A.Shamir i L.M.Adleman pronašli način praktične realizacije koncepta asimetrične kriptografije, te su navedeno i objavili u radu iz 1977. godine "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"[71]. Vrijednost ovog rada je i što je ponudio i koncept stvaranja elektroničkog potpisa. Na temelju saznanja iz navedenih radova je i zasnovana infrastruktura javnih ključeva. Dakle, napredak informacijsko-komunikacijskih tehnologija je doveo do njihove široke upotrebe među ljudima. Ljudi su u sve većoj mjeri počeli koristili elektroničku komunikaciju (npr. elektroničku poštu) za međusobnu komunikaciju. Takva komunikacija je uz velik broj prednosti imala i jednu veliku manu – bila je nesigurnija od obične komunikacije pismima. Elektronička poštu je bilo moguće presresti i pročitati na relativno jednostavan način. Osim toga, elektronička poruka je putem mogla biti i promijenjena. Prekretnica se dogodila kada je Amerikanac P.Zimmermann napravio program koji je na jednostavan način omogućavao kriptiranje i elektroničko potpisivanje elektroničke pošte. Program je nazvao PGP[72] (engl. Pretty Good Privacy). Autor je prvotno imao namjeru prodavati PGP, ali je američka vlada kanila zabraniti upotrebu ovakvog kriptografskog alata za široku primjenu iz razloga zaštite američke nacionalne sigurnost. Međutim, Zimmermann je 1991. preko *Usenet bulletin board* (jedna od mreža

[69] ISO (2005.), ISO/IEC 18033-3, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=37972 (04.03.2015.)
[70] Diffie, W., E., Hellman, M. (1976.), New Directions in Cryptography,IEEE Transactions on information theory, vol. IT22, no. 6, http://www-ee.stanford.edu/~hellman/publications/24.pdf (28.11.2016.)
[71] Rivest, R.L., Shamir A., Aldeman, L.M. (1977.), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, str. 120-126
[72] PGP, Pretty Good Privacy, http://en.wikipedia.org/wiki/Pretty_Good_Privacy (07.03.2015.)

na internetu) dao PGP program na besplatno korištenje[73]. Tim potezom je kriptografija za osobnu upotrebu postala dostupna širokoj masi ljudi, međutim širu primjenu nije imala. S druge strane, infrastruktura javnog ključa može ljudima osigurati sigurne komunikacije kako za poslovne, tako i za privatne svrhe.

A. Menezes, P. van Oorschot, S. Vanstone u svojoj knjizi "*Handbook of Applied Cryptography*"[74] opisuju i funkcije kriptografije. Oni daju definiciju kriptografije koja je temeljena na njenoj namjeni. Ta definicija definira kriptografiju kao istraživanje matematičkih tehnika vezanih za područja sigurnosti informacija kao što su: povjerljivost (*engl. confidentiality*), integritet podataka (*engl. data integrity*), autentikacija entiteta (*engl. entity authentication*) i autentikacija podrijetla podataka (*engl. data origin authentication*). Ovakva definicija pokriva tri od četiri funkcije kriptografije.

U nastavku slijedi opis funkcija kriptografije:

1. Povjerljivost (*engl. confidentiality*) je prvotna funkcija kriptografije. Ovom funkcijom se osigurava da je sadržaj podataka dostupan samo onome kome su podaci namijenjeni.
2. Integritet podataka (*engl. data integrity*) je funkcija kriptografije koja osigurava nepromjenjivost podataka. Promjene podataka mogu biti zamjena jednih podataka drugim, dodavanje ili uklanjanje podataka. Integritet se može osigurati tako da se omogući otkrivanje bilo kakve neovlaštene promjene podataka.
3. Autentikacija (*engl. authentication*) je funkcija vezana za razmjenu podataka. Autentikacija je identifikacija subjekata razmjene podataka i samog podatka. Elementi autentičnosti podataka su njihovo podrijetlo, vrijeme nastajanja i vrijeme slanja.
4. Neporecivost (*engl. non-repudiation*) je funkcija koja treba onemogućiti negiranje učinjenih aktivnosti od strane bilo kojeg učesnika u njima.

U praksi postoje više različitih tehnika kojima se mogu ostvariti osnovne funkcije kriptografije. Oba tipa kriptografije - i simetrična i asimetrična mogu pružiti sve četiri opisane funkcije. PKI - Infrastruktura javnih ključeva je sustav koji pokriva sve funkcionalnosti kriptografije.

[73] Giacomello, G. (2005.), National Governments and Control of the Internet: A Digital Challenge, New York, str. 43.
[74] Menezes, A., van Oorschot, P., Vanstone, S. (1997.), Handbook of Applied Cryptography, CRC Press, str. 4.

3.1.1 Simetrična kriptografija

Simetrična kriptografija (naziva se i još i kriptografija tajnim ključem) je najstariji poznati oblik kriptografije[75]. Ključ kojim se kriptira poruka i ključ dekriptiranja su jednaki, te predstavljaju tajni ključ. Tajni ključ poznaju samo sudionici sigurne komunikacije.

Slika 13. Simetrična kriptografija

Na slici 13 je prikazan primjer komunikacije između dvije osobe (A i B). Osobe A i B u komunikaciji koriste simetričnu kriptografiju. E je poruka kriptirana tajnim ključem K, a D je poruka dekriptirana tim istim tajnim ključem. Autor kriptirane poruke (osoba A) mora osigurati siguran kanal, te način dijeljenja tajnog ključa s osobom B kojoj je poruka namijenjena.

Prednosti simetrične kriptografije su jednostavnost i brzina izvođenja. Nedostatak je kada je potrebno većem broju osoba poslati kriptiranu poruku ili kada treba osigurati sigurnu komunikaciju. Ako je poruka kriptirana jednim tajnim ključem, tada je rizik što je on poznat svim osobama koji imaju prava pristupa kriptiranoj poruci. U tom slučaju postoji velika vjerojatnost krađe ključa ili presretanja poruke. Nedostaci tajnog ključa u simetričnoj kriptografiji se pojavljuju i kada se unutar zaštićene komunikacije uključuju novi sudionici koji dotadašnjim sudionicima nisu poznate, te još nije uspostavljeno povjerenje. Nedostatak je i što s porastom broja korisnika raste broj ključeva (npr. 5 korisnika – 10 ključeva).

$$broj\ ključeva\ za\ N\ korisnika = N * (N-1) /2$$

Simetrični algoritmi se mogu podijeliti u dvije grupe: *stream*-algoritam i *blok*-algoritam. *Stream*-algoritmi rade na načelu da se kriptiranje poruke obavlja bit po bit. Kod blok algoritama kriptiranje se obavlja po blokovima podataka. Dakle, uzimaju se blokovi od više bitova (64, 128, 196, 256 ...), te se kriptiraju kao cjelina. Dekriptiranje se najčešće

[75] Konheim, A. G. (2007.), Computer security and cryptography, Wiley

obavlja inverznim kriptiranjem - algoritam je isti, ali se podključevi kriptiranja koriste obrnutim redoslijedom[76].

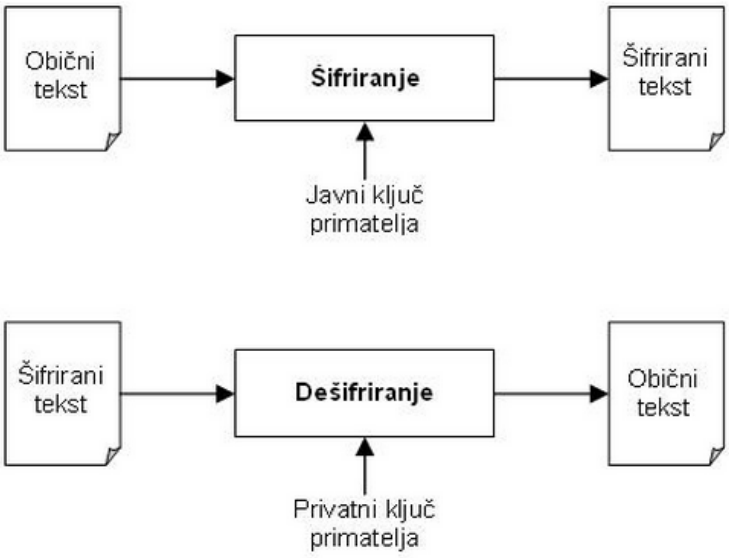
Simetrični kriptografski algoritmi koji su danas najrašireniji u internet protokolima su DES[77] (*engl. Data Encryption Standard*), te IDEA[78] (*engl. International Data Encryption Algorithm*). DES je razvijen od IBM-a 1977. godine, te se koristi tajnim ključem duljine 56 bitova. Za današnju snagu računala, te brzinu procesiranja ova duljina tajnog ključa postala je prekratka. Duljina od samo 56 bitova predstavlja najkritičniji dio ovog algoritma, te je 2001. zbog toga DES algoritam zamijenio novi simetrični algoritam – AES[79] (*engl. Advanced Encryption Standard*). Simetrični algoritam IDEA razvio je ETH Zurich[80] 1991. godine, te koristi ključ duljine 128 bitova. AES podržava ključeve duljine 128, 192, te 256 bitova. Osim navedenih algoritama koriste se još i Twofish, Blowfish, CAST5, RC4 i TDES.

3.1.2 Asimetrična kriptografija

Asimetrična kriptografija (naziva se još i kriptografijom javnim ključem) se za razliku od simetrične koristi s dva različita ključa od kojih se jedan koristi za kriptiranje a drugi za dekriptiranje. Kao što je već navedeno, W.Diffie i M.Hellman su 1976. objavili rad *"New Directions in Cryptography"*[81]. u kojem su iznijeli ideju razmjene tajnog ključa temeljenu na asimetričnoj kriptografiji. Algoritmi asimetrične kriptografije temelje se na matematičkom problemu faktorizacije velikih prirodnih brojeva na proste faktore. Svaka od strana u komunikaciji ima par ključeva - javni ključ i privatni ključ. Javni ključ je javan, te služi za kriptiranje. Privatni ključ je tajan, poznat je samo vlasniku ključa, te služi za dekriptiranje poruka. Javni ključ se može jednostavno odrediti na temelju poznatog privatnog ključa.

---

[76] Rueppel, R.A. (1992.), Stream Ciphers, Contemporary Cryptology - The Science of Information Integrity, edited by G.J.Simmons, New York, IEEE Press, str. 65.-134.
[77] U.S. Department of commerce, NIST (1999.), DES - Data Encryption Standard; http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[78] Teiwes, S., Hartmann, P., Kuenzi, D. (2001.), RFC 3058 - Use of the IDEA Encryption Algorithm in CMS, http://www.faqs.org/rfcs/rfc3058.html (21.03.2018.)
[79] Federal Information (2001.), AES - Advanced Encryption Standard, http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[80] ETH Zurich, https://www.ethz.ch/en.html (09.03.2015.)
[81] Diffie, W., E., Hellman, M. (1976.), New Directions in Cryptography,IEEE Transactions on information theory, vol. IT22, no. 6, http://www-ee.stanford.edu/~hellman/publications/24.pdf (28.11.2016.)



Slika 14. Asimetrična kriptografija

Određivanje privatnog ključa na temelju poznatog javnog ključa nije baš jednostavno. To je matematički vrlo zahtjevna operacija, te je uglavnom samo teoretski izvediva. Za obavljanje takve matematičke operacije je potrebna ekstremno skupa i moćna računalna oprema. Zbog toga su asimetrični kriptografski algoritmi cijenjeni kao vrlo sigurni. Zbog izrazite matematičke složenosti su asimetrično algoritmi i puno sporiji od simetričnih algoritama, te su neodgovarajući za kriptiranje veće količine podataka. Asimetrični algoritmi se koriste u većini slučajeva za elektroničko potpisivanje, te za razmjenu tajnog ključa simetrične kriptografije. Prednost asimetrične kriptografije je i ta što je broj ključeva koje treba razmijeniti uvijek isti bez obzira koliko ima sudionika u komunikaciji. Nasuprot navedenom, u simetričnoj kriptografiji postoji problem složenosti razmjene ključeva. Danas postoje mnogobrojni algoritmi asinkrone kriptografije. Od nastanka asimetrične kriptografije su mnogi asimetrični algoritmi prestali vrijediti zbog velike upornosti znanstvenika iz područja kriptoanalize, ali su isto tako su mnogi i prestali vrijediti zbog stalnog entuzijazma kriptoanalitičara.

U nastavku slijedi popis najpoznatijih asimetričnih algoritama:

- ECC ili kriptografija eliptične krivulje (engl. *Elliptic Curve Cryptography*) je algoritam koji je do sada pokazao veliku otpornost na napade[82]. Ovaj algoritam je danas prisutan (opcionalno) u mnogim protokolima. Međutim, više je namijenjen

[82] Halderman, B., Moore, H., Wustrow, N. (2014.), Elliptic Curve Cryptography in Practice; Financial Cryptography and Data Security, Springer; https://eprint.iacr.org/2013/734.pdf (18.03.2015.)

za korištenje u aplikacijama koje ne zahtijevaju veliku interoperabilnost. Radi dobro s matematičkom jedinicom koja se nalazi u procesorima. ECC algoritam je manje složeniji od RSA koji će biti sljedeći opisan, te se za određenu sigurnosnu razinu mogu koristiti i ključevi kraće duljine.

- RSA[83] je algoritam nazvan prema znanstvenicima Rivest, Shamir, Adleman s američkog sveučilišta Massachusetts Institute of Technology (MIT). Ovaj algoritam je primjenjiv i za kriptiranje i za dekriptiranje, za elektroničko potpisivanje te provjeru potpisa. Trenutno je za ovaj algoritam preporuka da bi duljina ključeva trebala biti najmanje 1024 bitova (iz razloga osiguravanja sigurnosti). RSA je danas obavezan u mnogim protokolima.
- DSA[84] (*engl. Digital Signature Algorithm*) je asimetrični kriptografski algoritam koji je napravljen za potrebe elektroničkog potpisivanja, provjere elektroničkog potpisa te za osiguravanje integriteta podataka.
- SHA-1[85] (*engl. Secure Hash Algorithm*) je revizija algoritma SHA koji je napravljen za korištenje algoritama DSA i RSA. Ovaj algoritam radi po načelu sličnom kao za algoritam MD5 hash funkcije. Algoritmi za izradu elektroničkog potpisivanja se uvijek koriste usko povezano s hash algoritmima, tj. hash algoritmi su sastavni dio elektroničkog potpisa i integriteta podataka.

Lenstra i Verheul su 2001. u svom članku „*Selecting cryptographic key sizes*“[86] dali preporuke koliko bi dugi ključevi trebali biti da bi se zadovoljila sigurnost. Osim toga su dali predviđanje vremenskog roka u kojem bi ključevi bili sigurni. U dolje navedenoj tablici je dan prikaz preporučenih duljina ključa (u bitovima) za kriptografske algoritme. Uz to, je u tablici dana procjena vremena koje je potrebno računalu za razbijanje šifre u jednoj MIPS (engl. *million instructions per second*) godini. MIPS godina je količina operacija računanja u godinu dana koje se mogu izvesti na računalu koje može odraditi milijun instrukcija u sekundi.

[83] RSA, http://en.wikipedia.org/wiki/RSA_(cryptosystem) (18.03.2015.)
[84] DSA, http://en.wikipedia.org/wiki/Digital_Signature_Algorithm (18.03.2015.)
[85] SHA-1, http://en.wikipedia.org/wiki/SHA-1 (19.03.2015.)
[86] Lenstra, A.K., Verheul, E.R. (2001.), Selecting cryptographic key sizes, Journal of Cryptology 14, str. 255-293.

Tablica 1. Procjena vremena koje je potrebno računalu za razbijanje šifre u jednoj MIPS godini, preuzeto iz Lenstra, A.K., Verheul, E.R. (2001.)[87]

God.	Dužina simetričnog ključa	Veličina klasičnog asimetričnog ključa	Duljina ECC ključa	MIPS godina	Najniži troškovi hardvera za jedan dan napada (US $)
1982.	56	417	105	$5,00 * 10^5$	$3,98 * 10^7$
1990.	63	622	117	3,51 * 107	$6,93 * 10^7$
2000.	70	952	132	$7,13 * 10^9$	$1,39 * 10^8$
2010.	78	1369	146	$1,45 * 10^{12}$	$2,77 * 10^8$
2020.	86	1881	161	$2,94 * 10^{14}$	$5,55 * 10^8$
2030.	93	2493	176	$5,98 * 10^{16}$	$1,11 * 10^9$
2040.	101	3214	191	$1,22 * 10^{19}$	$2,22 * 10^9$
2050.	109	4047	206	$2,47 * 10^{21}$	$4,44 * 10^9$

Iz *podataka* iz tablice 1 se može zaključiti da kriptosustavi koji su temeljeni na eliptičkim krivuljama (ECC) imaju višestruko manju duljinu ključa od drugih asimetričnih kriptoalgoritama (trenutno i do desetak puta), ali pružaju gotovo istu sigurnost kao kriptosustavi temeljeni na asimetričnim algoritmima (npr. RSA). Po navedenoj projekciji se može očekivati da će u budućnosti taj omjer biti još povoljniji za ECC. Ta je informacija bitna za primjene kod kojih je prostor za pohranu ključeva ograničen (npr. pametne kartice, *engl. smart cards*). Iz navedenog razloga će ECC ili kriptografija eliptične krivulje biti sve više u fokusu znanstvenika kriptografa.

3.2 PKI STANDARDI

3.2.1 X.509

Standard koji se koristi za zapis digitalnih certifikata je X.509. Danas je u upotrebi standard X.509 v3[88]. Prva verzija X.509 standard (X.509 v1) je nastala 1988 godine. Ova verzija standarda je sadržavala polja s informacijama o subjektu kome digitalni certifikat pripada, te informacije o certifikacijskoj službi (engl. Certificate Authority) koji je izdao taj digitalni certifikat.

[87] Lenstra, A.K., Verheul, E.R. (2001.), Selecting cryptographic key sizes, Journal of Cryptology 14, str. 269, str. 255-293, tablica 1

[88] Housley, R., Polk, W., Ford, W., Solo, D. (2002.), Internet X.509 Public Key Infrastructure, IETF, https://www.ietf.org/rfc/rfc3280.txt

Polja koja se navode u prvoj verziji X.509 standarda su:

- verzija certifikata,
- serijski broj certifikata,
- algoritam koji je certifikacijska služba koristila za elektronički potpis,
- naziv subjekta,
- naziv izdavatelja,
- period valjanosti certifikata,
- javni ključ koji certifikat povezuje sa subjektom,
- elektronički potpis izdavatelja.

Druga verzija ovog standarda (X.509 v2) proširuje prethodnu verziju s dva polja:

- jedinstvenim identifikatorom izdavatelja certifikata - ovo polje sadrži opcionalni niz bitova, te se time osigurava jedinstvenost imena izdavatelja vjerodajnice. Dodavanjem ovog polja je omogućeno da se ime certifikacijske službe nanovo koristi u budućim vremenima.
- jedinstvenim identifikatorom subjekta – i ovo polje sadrži opcionalan niz bitova kako bi ime subjekta bilo jedinstveno (slična namjena kao za jedinstveni identifikator izdavatelja certifikata).

Pet godina kasnije je objavljen RFC za PEM (engl. Internet Privacy Enhanced Mail)[89]. PEM uključuje specifikacije za infrastrukturu javnih ključeva temeljenu na X.509 v1 certifikatima. Naime, pokazalo se da prve dvije verzije standarda digitalnog certifikata (X.509 v1 i v2) nisu u dovoljnoj mjeri odgovarajuće. Pokazala se potreba za dodatnim poljima u koja bi se zapisivale informacije potrebne za PEM realizaciju. Iz tog razloga je 1996. objavljen X.509 v3 standard kao format digitalnih certifikata. X.509 v3 proširuje X.509 v2 s poljem koje sadrži ekstenzije. Navedene ekstenzije su uključile podatke poput:

- dodatnih informacija o identitetu subjekta,
- dodatne informacije o ključu,
- informacije vezane uz hijerarhiju infrastrukture javnih ključeva,

[89] Linn, J. (1993.), Privacy Enhancement for Internet Electronic Mail, IETF, http://www.ietf.org/rfc/rfc1421.txt (21.03.2018.)

- ograničenja kretanja certifikata i dr.

3.2.2 PKIX

Radna skupina za sustav infrastrukture javnog ključa temeljenog na X-509 (PKIX, engl. Public-Key Infrastructure X.509) pod nazivom PKIX-WG je ustanovljena 1995. od strane IETF (engl. Internet Engineering Task Force) organizacije da bi razvila potrebne internetske standarde koji će podržati infrastrukturu javnog ključa temeljenu na X.509 protokolu[90].

Da bi opisao infrastrukturu javnog ključa, PKIX koristi termine PKI (engl. Public Key Infrastructure) i PMI (engl. Privilege Management Infrastructure). PMI upravlja atributima certifikata, a PKI javnim ključevima.

PKIX ima pet standardizacijskih područja[91] pod kojima su navedeni generalni zahtjevi:

1. Profili X.509 digitalnih certifikata i liste opozvanih certifikata

Ovo područje opisuje osnovna polja certifikata i dodatke da bi bili podržani za digitalne certifikate i liste opozvanih certifikata. Navedene su osnovne i produžene validacije putanja certifikata. Na kraju, ovo područje pokriva i podržane kriptografske algoritme. Osnovna namjena ovog područja je standardizirati usvajanje korištenja X.509 certifikata unutar internet aplikacija i područja (www, elektronička pošta, korisnička autentikacija, IPSEC).

2. Funkcije upravljanja

Na početku područja su navedene pretpostavke i ograničenja protokola. Nadalje su opisane strukture podataka korištene za poruke za upravljanje PKI infrastrukturom, te se definiraju odgovarajuće funkcije. Na kraju, ovo područje pokriva i jednostavni protokol za prijenos PKI poruka. Ovaj protokol je izrađen kao podrška online interakciji između komponenti PKI infrastrukture. Detaljnije o ovim funkcijama će biti opisano u poglavlju „FUNKCIONALNOSTI INFRASTRUKTURE JAVNOG KLJUČA“.

3. Operativni protokoli

U ovom području se opisuje kako se protokoli: LDAP v2[92], FTP i HTTP mogu koristiti kao operativni protokoli.

[90] Oppliger, R. (2002.), Internet and Intranet Seucurity, Artech House, str. 345.
[91] Vacca, J.R. (2004.), Public Key Infrastructure, Building Trusted Applications and Webservices, Taylor & Francis Group, str. 58.

Protokol koji je izrađen za komunikaciju s certifikacijskom službom o statusu certifikata je nazvan OCSP (engl. On-line Certificate Status Protocol). OCSP je izrađen za korištenje HTTP protokola kao pristupne metode.

4. Politike certifikata i Pravilnik o postupcima certificiranja (CPS, engl. Certificate Practice Statements)

Namjena ovog dokumenta je uspostaviti jasnu relaciju između politika certifikata i CPS-ova. To je dokument koji izdaje certifikacijska služba te koji opisuje svoje prakse za izdavanje i upravljanje digitalnim certifikatima. U tom dokumentu su definirani procesi uključeni u generiranje, izdavanje, upravljanje, pohranu, dostavu i povlačenje javnih ključeva.

5. Servisi vremenskog žiga (engl. Timestamping services) i servisi validacije/potvrde podataka (DVCS, engl. Data Validation and Certification Services)

Servisi vremenskog žiga definiraju povjerljivu treću stranu (engl. trusted third–party) koja izrađuje tokene vremenskog žiga iz razloga da se osigura povjerenje da je datum nastao baš u određenoj vremenskoj točki. DVCS servisi osiguravaju potvrdu posjedovanja podataka i tvrdnju o posjedovanju podataka, te validaciju elektronički potpisanih dokumenata i certifikata.

Bitni RFC (engl. Request For Comments) dokumenti vezani uz PKIX standardizacijska područja su navedeni u tablici 2:

[92] Yeong, W., Howes, T., Kille, S. (1995.), Lightweight Directory Access Protocol, https://www.ietf.org/rfc/rfc1777.txt (21.03.2018.)

Tablica 2. Tablica RFC dokumenata za PKIX standardizacijska područja, preuzeto iz Vacca, J.R. (2004.)[93]

PKIX standardizacijsko područje	**RFC-ovi**
Profili X.509 digitalnih certifikata i liste opozvanih certifikata	RFC 2459
Protokoli upravljanja	RFC 2510
Operativni protokoli	RFC 2559 RFC 2585 RFC 2560
Politike certifikata i Pravilnik o postupcima certificiranja za certifikate (CPS, engl. Certificate Practice Statements)	RFC 2527
Servisi vremenskog žiga (engl. Timestamping services) i servisi validacije/potvrde podataka (DVCS, engl. Data Validation and Certification Services)	RFC 3161 (Time Stamp Protocol) , te zasada eksperimentalni status za DCVS (RFC 3029)

3.2.3 PKCS

Standardi kriptografije javnog ključa (engl. PKCS, Public Key Cryptography Standards) su skup standarda koji je imao snažan utjecaj na korištenje kriptografije javnog ključa u praksi. PKCS standardi su skup standarda, nazvani PKCS #1 do #15. Ti standardi pokrivaju RSA kriptiranje, RSA potpis, kriptiranje lozinkom, sintaksu kriptografske poruke i dr. PKCS standarde objavljuje istraživački centar RSA Laboratories[94] od 1991. godine. PKCS standardi su bili temelj za mnoge druge formalne i de facto standarde kao što su S/MIME, PKIX, SSL i dr.

[93] Vacca, J.R. (2004.), Public Key Infrastructure, Building Trusted Applications and Webservices, Taylor & Francis Group, str. 59
[94] RSA Laboratories, http://www.emc.com/emc-plus/rsa-labs/index.htm (05.04.2015.)

Standarde uobičajeno zajednički definira i usuglašava veći broj organizacija, te je stoga PKCS informativni standard jer ga kontrolira RSA. Međutim, PKCS standardi su široko prihvaćeni u industriji, te imaju svoje ekvivalente kao IETF ili IEEE standarde.

U nastavku slijedi popis PKCS standarda (uz bitnije standarde će biti dan i detaljniji opis):

PKCS #1[95] - RSA Cryptography Standard

Ovaj standard opisuje kako se podaci kriptiraju koristeći RSA kriptosustav javnog ključa. Njegova svrha je u izradi elektroničkog potpisa i digitalne omotnice, te će biti opisan u PKCS #7. PKCS #1 standard definira matematičke definicije i svojstva koja RSA javni i privatni ključ moraju imati. Sintaksa javnog ključa se koristi i u digitalnim certifikatima (X.509). Standardi PKCS #2 i PKCS #4 su uključeni u PKCS #1 specifikaciju. PKCS #1 je definiran i kao RFC 3447.

PKCS #3[96] - Diffie-Hellman Key Agreement Standard

Ovaj standard opisuje metode za implementiranje Diffie-Hellman sporazuma o ključu, pri čemu dvije strane, bez ikakvog prethodnog dogovora, mogu uspostaviti tajni ključ koji potom mogu koristiti. Predviđena namjena ovog standarda je u protokolima za uspostavljanje sigurnih konekcija, kao što su zahtijevane za OSI transportni i mrežni sloj.

PKCS #5 - Password-Based Cryptography Standard. PKCS #5 je definiran i kao RFC 2898.

PKCS #6 - Extended-Certificate Syntax Standard

PKCS #7[97] - Cryptographic Message Syntax Standard

PKCS #7 opisuje generalnu sintaksu za podatke na koje je kriptografija primjenjiva, kao što su elektronički potpisi i digitalna omotnica. Sintaksa podržava rekurziju, tako da primjerice jedna omotnica može biti ugniježđena unutar druge. Drugi atributi kao što je potpisno vrijeme mogu biti autenticirani uz sadržaj poruke. PKCS #7 je definiran i kroz RFC 2315.

PKCS #8 - Private-Key Information Syntax Standard . Definiran je i kroz RFC 5208.

PKCS #9 - Selected Attribute Types . Definiran je i kroz RFC 2985.

---

[95] RSA (2012.), PKCS #1 v2.2: RSA Cryptography Standard, http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf (21.03.2018.)
[96] RSA (1993.), PKCS #3: Diffie-Hellman Key-Agreement Standard, ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-3.asc (21.03.2018.)
[97] RSA (1993., 2.), PKCS #7: Cryptographic Message Syntax Standard, ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-7.asc (21.03.2018.)

PKCS #10[98] - Certification Request Syntax Standard

Ovaj standard opisuje sintaksu za zahtjeve za certifikatom, koji se šalje certifikacijskoj službi. Na osnovu navedenog zahtjeva CA izrađuje digitalni certifikat u X.509 formatu. Certifikacijski zahtjev sadrži DN (engl. distinguished name), javni ključ i opcionalno skup atributa. Skup atributa mogu biti informacije tipa poštanske adrese na koju će izrađeni certifikat biti isporučen za slučaj da se certifikat ne može isporučiti na adresu elektroničke pošte. PKCS #10 je definiran i kroz RFC 2986.

PKCS #11[99] - Cryptographic Token Interface Standard

PKCS #11 specificira API, nazvan Cryptoki za uređaje koji sadrže kriptografsku informaciju i izvode kriptografske funkcije. Cryptoki je neovisan o platformi, te je namijenjen uređajima kao što su HSM (engl. hardware security modules) i pametne kartice (engl. smart cards). Navedeni API definira najčešće kriptografske tipove objekata (RSA ključevi, X.509 certifikati, DES/Triple DES ključevi i dr.) i funkcije tog API-ja služe za korištenje, kreiranje, promjenu i brisanje navedenih objekata.

PKCS #12[100] - Personal Information Exchange Syntax Standard.

Ovaj standard definira prijenosni format za pohranu i transportiranje korisničkih privatnih ključeva, certifikata, raznih tajni i dr. PKCS #12 je definiran i kroz RFC 7292.

PKCS #13 - Elliptic Curve Cryptography Standard

PKCS #14 – Pseudo-random Number Generation

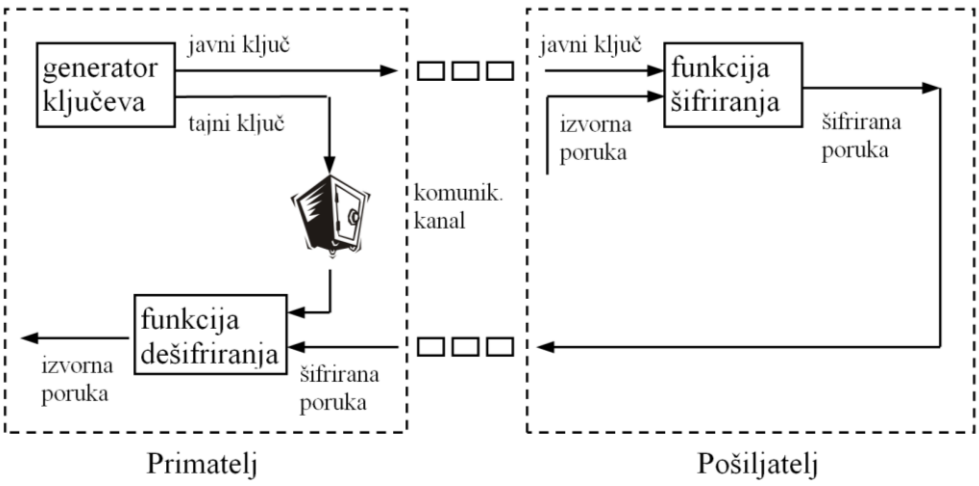
PKCS #15 - Cryptographic Token Information Format Standard

3.3 PKI ARHITEKTURA

Infrastruktura javnoga ključa (PKI) je složena informacijska infrastruktura, te služi za upravljanje elektroničkim identitetima. Uporaba asimetrične kriptografije je u temelju rada PKI infrastrukture. Asimetrična kriptografija zapravo počiva na paru matematički povezanih ključeva – javnog i privatnog ključa, koji su generirani da bi se zajedno

[98] RSA (1993., 3.), PKCS #10: Certification Request Syntax Standard, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.doc (21.03.2018.)
[99] RSA (2004.), PKCS #11 v2.20: Cryptographic Token Interface Standard, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf (21.03.2018.)
[100] Moriarty, K., Nystrom, M., Parkinson, S., Rusch, A., Scott, M. (2004.), PKCS #12: Personal Information Exchange Syntax v1.1, http://tools.ietf.org/html/rfc7292 (21.03.2018.)

koristili[101]. Privatni ključ može koristiti samo vlasnik jer je tajan. Javni ključ je dostupan svima[102]. Samo osoba koja ima tajni ključ ju može dekriptirati, kao što je navedeno na slici 15. Međutim, svatko tko ima javni ključ može kriptirati poruku.



Slika 15. Postupak šifriranja i dešifriranja upotrebom javnog i tajnog ključa, preuzeto iz Stančić, H. (2001.)[103]

Kada osoba elektronički potpiše poruku svojim tajnim ključem svatko može javnim ključem provjeriti je li ta osoba potpisala dokument. U ovom slučaju se javlja problematika provjere stoji li prava osoba iza elektroničkog potpisa. Tu problematiku se može riješiti uspostavom certifikacijske službe (CA) koja izdaje digitalne certifikate. Certifikacijska služba je samo jedan od niza komponenata koji sačinjavaju PKI infrastrukturu.

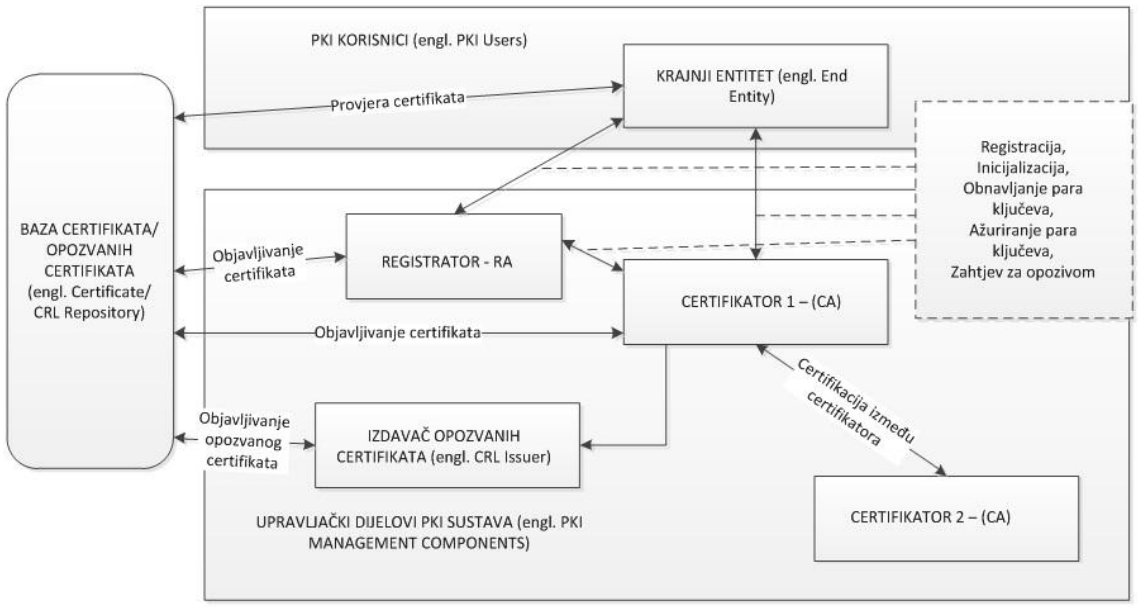
Osnovne komponente PKI infrastrukture su:

- krajnji entitet ili korisnici PKI sustava,
- certifikacijska služba (CA),
- registracijska služba (RA, engl. Registration Authority),

[101] Jacobs, J., Clemmer, L., Dalton, M., Rogers, R., Posluns, J. (2003.), SSCP Study Guide, Syngress Publishing, str. 330-331.
[102] Isto
[103] Stančić, H. (2001.), Upravljanje znanjem i globalna informacijska infrastruktura, Magistarski rad, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb, str. 48

- repozitorij ili baza valjanih i opozvanih certifikata (engl. Certificate/CRLRepository),
- izdavač liste opozvanih certifikata (engl. CRL Issuer),

Na slici 16 je dan prikaz PKIX sustava (sustava infrastrukture javnog ključa temeljenog na X.509).



Slika 16. Sustav infrastrukture javnog ključa temeljenog na X.509, preuzeto iz Stallings, W. (2006.)[104]

Radi boljeg uvida u složenost problematike dugoročnoga očuvanja arhivskoga gradiva koje sadrži elektroničke potpise, a što je i jedna od tema ovog rada, u narednim potpoglavljima i poglavlju „4. NAPREDNI ELEKTRONIČKI POTPIS KAO PODLOGA ZA DUGOROČNO OČUVANJE ELEKTRONIČKIH ZAPISA“ će se pojasniti osnovne pojmove infrastrukture javnoga ključa (PKI): digitalnog certifikata, kvalificiranog digitalnog certifikata, certifikacijske službe, registracijske službe, ali i druge PKI elemente nužne za realizaciju dugotrajne pohrane takve arhivske građe: elektroničkog potpisa, naprednog elektroničkog potpisa, pouzdane arhivske službe, vremenskog žiga, pouzdanog vremenskog žiga, vremenskog pečata i dr.

[104] Stallings, W. (2006.), Cryptography and Network Security, Principles and Practices, 5th Edition, Pearson Education, str. 438

3.4 FUNKCIONALNOSTI INFRASTRUKTURE JAVNOG KLJUČA

Funkcionalnosti PKI infrastrukture su[105]:

- **Registracija** – ovo je proces registracije korisnika pri certifikacijskoj službi te je to korak koji je potrebno obaviti prije izdavanja certifikata korisniku. Registracijom počinje proces upisa (engl. enrolling) u infrastrukturi javnog ključa. Registracija uobičajeno uključuje određene offline ili online procedure za zajedničku (engl. mutual) autentikaciju. Registracijom korisnik dobiva svoj korisnički identitet/digitalnu vjerodajnicu. Funkcija certifikacije službe je povezivati korisnički identitet s njegovim javnim ključem. Navedeno povezivanje se ostvaruje elektroničkim potpisivanjem korisnikovog javnog ključa privatnim ključem certifikacijske službe.
- **Inicijalizacija** – prije nego što sustav korisnika može djelovati sigurno, nužno je instalirati programsku opremu s ključevima koja će biti u odgovarajućoj relaciji s ključevima spremljenim unutar infrastrukture. Klijent treba na siguran način biti inicijaliziran s javnim ključem i drugim provjerenim informacijama certifikacijske službe (CA), da bi se mogao koristiti u ispravnoj putanji certifikata (engl. certificate paths).
- **Certifikacija** – to je proces u kojem certifikacijska služba izdaje certifikate za korisnikov javni ključ, te ga isporučuje na korisnikov sustav i/ili ga sprema u repozitorij certifikata. Kao repozitorij u koji se objavljuju liste objavljenih certifikata je de facto prihvaćen LDAP (engl. Lightweight Directory Access Protocol) koji je razvijen kao komplement X.500[106] protokolu za Internet.
- **Oporavak para ključeva** – par ključeva je korišten kao podrška izradi i provjeri elektroničkog potpisa, kriptiranju i dekriptiranju ili i jednom i drugom. Kada se par ključeva koristi za kriptiranje/dekriptiranje, bitno je osigurati mehanizam za oporavak ključeva za dekriptiranje kada pristup kriptiranom materiju nije više moguć. U suprotnom, nije moguće oporaviti kriptirane podatke. Razlozi gubitka pristupa deskripcijskom ključu mogu biti: zaboravljena lozinka, zaboravljen PIN, oštećen disk, oštećeni hardverski tokeni i dr.

[105] Stallings, W. (2006.), Cryptography and Network Security, Principles and Practices, 5th Edition, Pearson Education, str. 438
[106] X.500, http://en.wikipedia.org/wiki/X.500 (06.04.2015.)

- **Obnova para ključeva** – svi ključevi trebaju se regularno obnavljati, tj. biti zamijenjeni s novim parom ključeva. Time se korisniku mogu izdati novi certifikati. Obnova je potrebna kada životni tijek certifikata istječe, te kao rezultat opoziva certifikata.
- **Zahtjev za opozivom** – autorizirana osoba prijavljuje certifikacijskoj službi neregularnu situaciju, te može zahtijevati opozivanje certifikata. Razlozi za opoziv certifikata mogu biti: kompromitiranje privatnog ključa, gubitak uređaja s certifikatom, promjena imena i dr.
- **Međusobna certifikacija** (engl. Cross certification) – dva CA razmjenjuju informacije i uspostavljaju međusobnu certifikaciju. Na taj način jedna certifikacijska služba može izdavati certifikate koji sadrže CA potpisni ključ korišten za izdavanje certifikata od strane druge certifikacijske službe.
- **Objava liste opozvanih certifikata** – lista opozvanih certifikata (CRL, engl. Certificate Revocation List) je potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim. Objavom liste opozvanih certifikata se omogućava online provjera statusa valjanosti certifikata. Primjer takve online provjere opozvanosti certifikata je i provjera pomoću online preuzete CRL. U slučaju da se online provjera statusa certifikata obavlja preko CRL, tada se provjerava samo zadnje izdana CRL.

  OCSP protokol (engl. Online Certificate Status Protocol) je internetski protokol korišten za dobivanje statusa opoziva certifikata. Ovaj protokol je opisan u RFC 6960[107]. OCSP je napravljen kao alternativa listi opozvanih certifikata, i to posebno zbog rješavanja problema povezanih s korištenjem CRL liste unutar PKI infrastrukture (npr. CRL zna biti velika, te je time opterećenje za veličinu elektronički potpisanog dokumenta).

[107] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, S. (2013.), X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP, https://tools.ietf.org/html/rfc6960 (21.03.2018.)

3.5 PKI ELEMENTI ZA DUGOTRAJNU POHRANU

3.5.1 Certifikacijska služba (CA)

Unutar infrastrukture javnog ključa (PKI) funkciju izdavanja i opozivanja digitalnih certifikata ima certifikacijska služba (CA). Certifikacijska služba je nadležna za ovjeru identiteta. CA je organizirana kao hijerarhija unutar koje je korijenski CA (engl. Root CA) najviši entitet koji vjeruje sam sebi. Korijenskom CA vjeruju svi hijerarhijski niži entiteti. Namjena ovakve hijerarhije je da svaki identificirani entitet dobije ovjeru svog javnog ključa (tj. elektronički zapis), te se time potvrđuje njegov identitet. Potvrđivanje identiteta se obavlja tako da certifikacijska služba potpisuje digitalni certifikat određenog entiteta svojim privatnim ključem. Identitet tog entiteta bi se kasnije trebao moći provjeriti s javnim ključem CA. Kada entitet zatraži ovjeru, CA provjerava s registracijskim autoritetom (RA) informacije o identitetu. U slučaju da RA potvrdi vjerodostojnost informacija o entitetu - CA izdaje digitalni certifikat.

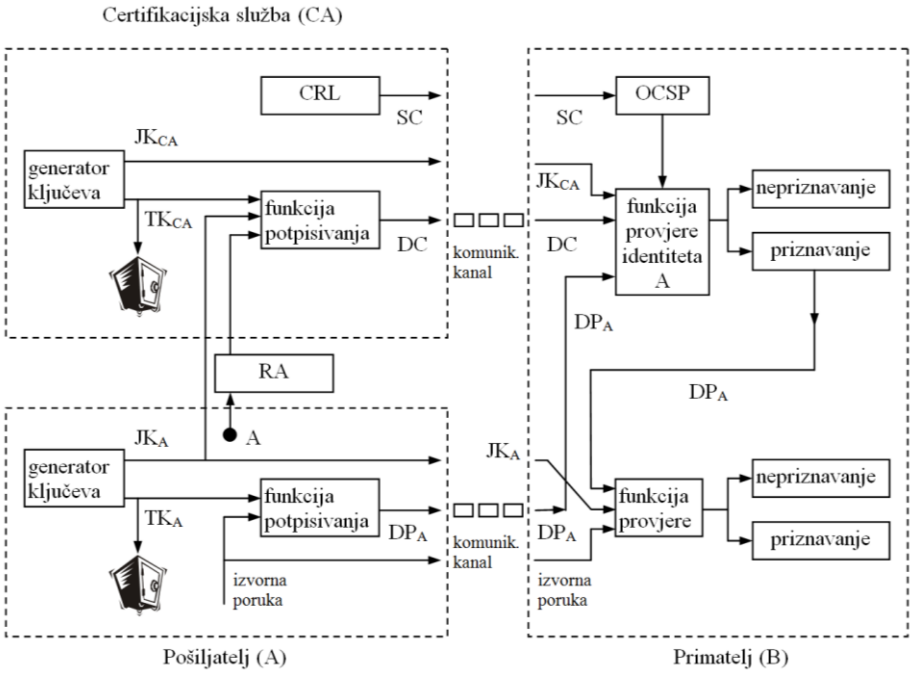
Digitalni certifikati moraju biti dostupni svim korisnicima PKI infrastrukture. Korisnici mogu biti subjekti certifikata, ali i aplikacije i treće strane koje koriste certifikate. Za svrhu distribuciju certifikata krajnjim korisnicima postoji repozitorij ili spremnik digitalnih certifikata koji predstavlja sustav ili skup distribuiranih sustava koji pohranjuju certifikate i liste opozvanih certifikata[108].

Kao repozitoriji ili spremnici digitalnih certifikata se uglavnom podrazumijevaju X.500 imenički servisi. Repozitoriji certifikata mogu biti i jednostavnije strukture (npr. datoteke na serveru kojima se može pristupiti preko FTP ili HTTP protokola). X.500 imenički servisi su vrlo pogodni kao spremnici digitalnih certifikata, jer se X.509 format certifikata dobro uklapa u X.500 servise. Kao protokol za pristup repozitoriju certifikata se najčešće koristi LDAP (engl. Lightwaight Directory Access Protocol)[109].

Certifikacijska služba treba održavati i informacije o stanju digitalnih certifikata, te objavljivati informacije o nevažećim certifikata. Jedan od načina je putem liste opozvanih

[108] Housley, R., Polk, W., Ford, W., Solo, D. (2002.), Internet X.509 Public Key Infrastructure, IETF, https://www.ietf.org/rfc/rfc3280.txt (21.03.2018.)
[109] Sermersheim, J. (2006.), Lightweight Directory Access Protocol (LDAP): The Protocol, https://tools.ietf.org/html/rfc4511 (21.03.2018.)

certifikata, CRL (engl. Certificate Revocation List)[110]. Valjanost certifikata se osim liste opozvanih certifikata može provjeriti i protokolom za online provjeru certifikata, OCSP (engl. Online Certificate Status Protocol). OCSP omogućuje klijentima određivanje statusa opoziva korištenih certifikata[111]. OCSP klijent izrađuje zahtjev za provjerom statusom certifikata, te ga šalje OCSP poslužitelju. OCSP klijent omogućuje potvrđivanje certifikata tek kada dobije pozitivan odgovor od OCSP poslužitelja (tijek provjere je prikazan na slici 17).



A – ime pošiljatelja
CA – certifikacijska služba
CRL – lista opozvanih certifikata
DC – digitalni certifikat
DP_A – digitalni potpis A
JK_A – javni ključ pošiljatelja
JK_{CA} – javni ključ CA
OCSP – protokol za online provjeru certifikata
RA – registracijska služba
SC – status certifikata
TK_A – tajni ključ pošiljatelja
TK_{CA} – tajni ključ CA

Slika 17. Postupak rada certifikacijske službe prilikom provjere elektronički potpisane poruke i digitalnoga certifikata, preuzeto iz Stančić, H. (2001.), str. 51[112]

[110] Lista opozvanih certifikata je jedna od najvažnijih komponenti infrastrukture javnog ključa jer se putem nje provjerava valjanost digitalnog certifikata. CRL je potpisan privatnim ključem CA, pa je samim time krivotvorenje liste opozvanih certifikata gotovo nemoguće.
PKI 101, What is a CRL?, URL: http://www.pki101.com/CRLWhat.html (07.04.2015.)
[111] Myers, M. et al. (1999), X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP, Network Working Group, The Internet Society, URL: http://www.ietf.org/rfc/rfc2560.txt (14.04.2014.)
[112] Stančić, H. (2001.), Upravljanje znanjem i globalna informacijska infrastruktura, Magistarski rad, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb, str. 51

U Republici Hrvatskoj je FINA (Financijska agencija)[113] jedna od certifikacijskih službi koje održavaju registar digitalnih certifikata, a da pri tome ima dozvolu Ministarstva gospodarstva[114]. Prvi pravilnik o administriranju korisnika i certifikata FINA-PKI[115], kao i certifikacijska politika (engl. Certification Policy) FINA-PKI izrađeni su uz nadzor Ministarstva gospodarstva. Europska komisija je 17. travnja 2014. godine objavila pouzdanu listu certifikacijskih službi koji izdaju kvalificirane certifikate[116] i na njoj se po prvi put pojavio certifikat iz Republike Hrvatske, tj. certifikat Financijske agencije. Od tog se datuma FINA može smatrati pouzdanim i priznatim izdavateljem digitalnih certifikata i unutar Europske unije. Na stranicama Ministarstva gospodarstva Republike Hrvatske je za Finu navedeno i sljedeće: „NCARH (nacionalni CA za Republiku Hrvatsku) je uspostavljen u cilju ostvarivanja povjerenja pri razmjeni podataka i elektroničkih dokumenata u elektroničkom poslovanju na nacionalnoj razini. Po svojoj funkciji NCARH namijenjen je za spajanje PKI domena u Hrvatskoj te za povezivanje s PKI domenama u inozemstvu. Tehničko i informatičko održavanje te operativnu podršku u radu NCARH u ime i za račun Ministarstva temeljem ugovora obavlja Financijska agencija (FINA).“

U tablici 3 je dan prikaz evidentiranih podataka o jednom davatelju usluga certificiranja u Republici Hrvatskoj (FINA) sa stranica Ministarstva gospodarstva:

Tablica 3. Podaci o evidentiranom davatelju usluga certificiranja u Republici Hrvatskoj (Fini) na dan 8. prosinca 2015., preuzeto sa stranica Ministarstva gospodarstva RH[117]

Evidencijski broj:	**HR-QC-2008-07-16-1**
Vrste certifikata koje se izdaju i status usluge:	QC, C, QTS, aktivan
Naziv davatelja usluga certificiranja:	Financijska agencija
Adresa davatelja usluga certificiranja:	Ulica grada Vukovara 70, Zagreb, HR
Osobni identifikacijski broj davatelja usluga certificiranja:	85821130368
Ime i prezime ovlaštene osobe za zastupanje davatelja usluga certificiranja:	Anđelka Buneta
Osnovna djelatnost:	• Agencija prikuplja, priprema i objedinjuje podatke o poslovnim subjektima, te vodi odgovarajuće

[113] FINA, FINA RDC (Registar Digitalnih Certifikata), URL: http://rdc.fina.hr/ (07.04.2015.)
[114] Ministarstvo gospodarstva RH, Evidencija davatelja usluga certificiranja u Republici Hrvatskoj, http://mingo.fina.hr/index.html (07.04.2015.)
[115] FINA (2.), Pravilnik o administriranju korisnika i certifikata v1.0, http://demo-pki.fina.hr/dokumentacija/pak.pdf (31.03.2003).
[116] Europska komisija, List of Trusted List information as notified by Member States, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1788 (07.04.2014.)
[117] Ministarstvo gospodarstva, http://mingo.fina.hr/index.html (8.12.2015.)

	registre; • Agencija vodi i druge registre, evidencije i zbirke podataka za potrebe države i drugih subjekata; • Agencija obavlja sljedeće komercijalne djelatnosti: vodi nacionalni sustav za izdavanje javnih ključeva - Registar digitalnih certifikata (RDC), operativno vođenje drugih javnih i komercijalnih registara; • Agencija može obavljati i druge djelatnosti koje služe obavljanju djelatnosti iz prethodnih stavaka.
Elektronička adresa davatelja usluga certificiranja:	e-mail: mailto:pr@fina.hr
Broj telefona:	01/6127-111
Broj faksa:	01/6128-089
Elektronička adresa i telefonski brojevi službe za odnose sa strankama:	e-mail: mailto:info@fina.hr, tel: 0800 0080
Datum upisa u Evidenciju:	16. srpnja 2008.
Datum promjene ili dopune Evidencije:	8. prosinca 2015.
Datum prestanka obavljanja usluge certificiranja i opoziva svih certifikata za koje davatelj nije osigurao nastavak obavljanja usluge kod drugog davatelja usluga i adresa liste opozvanih certifikata:	-
Datum brisanja iz Evidencije ili oznaka o neispunjavanju uvjeta /oznaka o eventualnim arhivskim podacima važećim do upisa promjene za sve ili tip usluge:	-
Oznaka o dobrovoljnoj akreditiranosti:	-
Granica vrijednosti transakcija za koje davatelj usluga certificiranja odgovara:	• Certifikati standardne razine sigurnosti: do 8.000 kn • Certifikati srednje razine sigurnosti: do 80.000 kn • Certifikati visoke razine sigurnosti: do 400.000 kn • Napredni vremenski žig: do 20.000 kn
Oznaka poslovne banke u kojoj se vodi poslovni račun:	Hrvatska poštanska banka d.d. Zagreb, VBDI: 2390001
Popis normi koje davatelj usluge primjenjuje u svom poslovanju:	HRN ETSI/EN 319 401, HRN ETSI/EN 319 411-2, HRN ETSI/EN 319 411-3, HRN ETSI/EN 319 412-5, HRS ETSI/TS 102 023, HRS ETSI/TS 101 861, ETSI TS 119 312, ISO/IEC 9001:2008, ISO/IEC 27001:2013

Osim Fine, na stranicama Ministarstva gospodarstva su na dan 28. prosinca 2017. kao davatelji usluga certificiranja u Republici Hrvatskoj navedeni i AKD[118] i Zagrebačka banka[119].

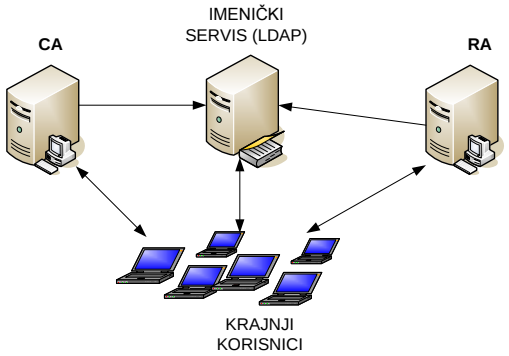
[118] Agencija za komercijalnu djelatnost d.o.o., http://www.akd.hr/ (21.03.2018.)
[119] Zagrebačka banka, https://www.zaba.hr/ (21.03.2018.)

3.5.2 Registracijska služba (RA)

Registracijska služba, RA (engl. Registration Authority) u infrastrukturi javnog ključa predstavlja autoritet za provjeru zahtjeva entiteta za izdavanjem digitalnih certifikata koji potvrđuje valjanost zahtjeva certifikacijskoj službi. Registracijska služba nije obavezna komponenta PKI infrastrukture. U zavisnosti od izvedbe PKI infrastrukture, certifikacijska služba može delegirati registracijskoj službi neke od administrativnih funkcija. U slučaju da RA ne postoji, tada CA mora sama obavljati sve funkcije koje bi inače obavljala RA.

Registracijski autoritet pruža informaciju certifikacijskoj službi da bi certifikacijska služba mogla izdati digitalni certifikat[120]. Registracijski autoritet provjerava sadržaj certifikata za certifikacijski autoritet te obavlja identifikaciju samih entiteta kao i autentikaciju entiteta koji se prijavljuje za izdavanje digitalnih certifikata. Dodatno, RA obavlja još neke administrativne zadatke (kao pomoć CA). RA može provjeravati i ostale atribute certifikata entiteta, te provjeriti posjeduje li entitet zaista privatni ključ koji odgovara javnom ključu koji će se nalaziti na digitalnom certifikatu. RA može i generirati par ključeva za entitet i posredovati između entiteta i CA prilikom informiranja o kompromitiranju privatnog ključa. Registracijski autoritet, s druge strane, ne može obavljati izdavanje certifikata i lista opozvanih certifikata.

Imenički servis distribuira certifikate i liste opozvanih certifikata u realnom vremenu. Imenički servis ima funkciju repozitorija, te se za komunikaciju CA i RA s njim koristi LDAP protokol. Certifikacijska služba objavljuje certifikate u repozitorij, a korisnici ih dohvaćaju putem klijentske aplikacije preko LDAP protokola (prikazano na slici 18).



Slika 18. Uloga imeničkog sustava u provjeri digitalnih certifikata

[120] Search Security, Registration Authority (RA), http://searchsecurity.techtarget.com/definition/registration-authority (08.04.2015)

3.5.3 Certifikati za elektronički potpis

Chokhani[121] definira digitalni certifikat (engl. Digital certificate) kao elektronički zapis koji služi za potvrdnu identifikaciju entiteta. Entitet može biti fizička osoba, pravna osoba ili organizacija, te uređaj. Digitalni certifikati su strukture podataka koje vežu javni ključ entiteta sa setom informacija koje identificiraju entitet, odnosno povezuje odgovarajući privatni ključ entiteta. Ova veza se potvrđuje elektroničkim potpisom certifikacijske službe koja je izdala certifikat. Najrašireniji format digitalnih certifikata je X.509 v3 koji je vrlo složen, ali i standardiziran, pa je mogućnost pogreške implementacije smanjena korištenjem standarda[122]. Prema Uredbi (EU) br. 910/2014[123] (u Uredba eIDAS) digitalni certifikat se naziva i certifikat za elektronički potpis. Uredba eIDAS je certifikat za elektronički potpis definirala na sljedeći način: „certifikat za elektronički potpis" znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe. Detaljnije o povijesti razvoja EU i hrvatske regulative koja se tiče elektroničkog potpisa će biti više napisano u poglavlju 4.1 Elektronički potpis.

Sadržaj digitalnog certifikata je sljedeći[124]:

- informacije kojima se identificira entitet (fizička osoba, pravna osoba ili organizacija, uređaj) koji posjeduje certifikat,
- javni ključ korisnika,
- vremenski period valjanosti certifikata,
- informacije o organizaciji koja izdaje certifikat,
- elektronički potpis koji potvrđuje identitet organizacije koja je izdala certifikat,

[121] Chokhani, S. et al.(2003.), Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework, Network Working Group, The Internet Society, http://www.ietf.org/rfc/rfc3647.txt (08.04.2015.)
[122] Ferguson, N., Schneier, B., Kohno, T. (2010.), Criptography Engineering: Deisign Principles and Practical Applicarion, Wiley Publishing, str. 279.
[123] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)
[124] Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, e-potpis, materijal predmeta Sigurnost elektroničkog poslovanja, http://www.fer.unizg.hr/_download/repository/7_sigurnost_potpis.pdf (08.04.2015.)

- digitalni zapis koji potvrđuje da je određeni entitet vlasnik određenog javnog ključa,
- javni zapis koji entitet distribuira zainteresiranim stranama, kako bi se identitet entiteta mogao provjeriti.

Bitno je napomenuti da je sadržaj certifikata (sva polja) elektronički potpisan što znači da bi promjena bilo kojeg polja učinila potpis nevažećim (a time bi i certifikat bio nevažeći).

Europska komisija je koristila pojam kvalificiranog certifikata (engl. Qualified Certificate) za opis određene vrste digitalnoga certifikata koji je relevantan za europsko zakonodavstvo. Tako RFC dokument „*Internet X.509 Public Key Infrastructure. Qualified Certificates Profile*“ Qualified Certificates Profile[125] pruža detaljnu specifikaciju izdavanja kvalificiranog certifikata. Takav certifikat jamči pouzdanu identifikaciju osobe kao entiteta pri korištenju javnih usluga unutar kojih se poštuje načelo neporecivosti. Prema Uredbi eIDAS[126] kvalificirani certifikat se naziva i kvalificirani certifikat za elektronički potpis. Kvalificirani certifikat izdaje certifikacijska služba koja mora udovoljiti specifičnim zahtjevima definiranima unutar EU Uredbe. Uredba eIDAS je kvalificirani certifikat za elektronički potpis definirala na sljedeći način: „kvalificirani certifikat za elektronički potpis” znači certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I. Prilog I Uredbe eIDAS detaljno specificira sadržaj takvog certifikata i zahtjeve koji takvi certifikati trebaju zadovoljavati. U nastavku je naveden sadržaj Priloga I[127] Uredbe eIDAS:

„Kvalificirani certifikati za elektroničke potpise sadržavaju:

(a) naznaku, barem u obliku prikladnom za automatiziranu obradu, da je certifikat izdan kao kvalificirani certifikat za elektroničke potpise;

[125] Santesson, S., Polk, W., Barzin, P., Nystrom, M. (2001.), Internet X.509 Public Key Infrastructure. Qualified Certificates Profile, Network Working Group, The Internet Society, http://www.ietf.org/rfc/rfc3039.txt (08.04.2015.)
[126] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)
[127] Isto, članak 3. Definicije, L 257/111

(b) skup podataka koji nedvojbeno predstavlja kvalificiranog pružatelja usluga povjerenja koji izdaje kvalificirane certifikate uključujući barem državu članicu u kojoj pružatelj ima poslovni nastan i

— za pravnu osobu: naziv i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji,

— za fizičku osobu: ime osobe;

(c) barem ime potpisnika, ili pseudonim; ako se koristi pseudonimom, on se mora jasno naznačiti;

(d) podatke za validaciju elektroničkog potpisa koji odgovaraju podacima za izradu elektroničkog potpisa;

(e) podatke o početku i završetku roka valjanosti certifikata;

(f) identifikacijsku oznaku certifikata koja mora biti jedinstvena za kvalificiranog pružatelja usluga povjerenja;

(g) napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluga povjerenja koji izdaje certifikat;

(h) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredan elektronički potpis ili napredan elektronički pečat iz točke (g);

(i) lokaciju usluga koje se mogu koristiti za ispitivanje statusa valjanosti kvalificiranog certifikata;

(j) ako su podaci za izradu elektroničkog potpisa koji su povezani s podacima za validaciju elektroničkog potpisa smješteni u kvalificiranom sredstvu za izradu elektroničkog potpisa, odgovarajuću naznaku navedenog, barem u obliku prikladnom za automatiziranu obradu.“

Uredba eIDAS u uvodnim odredbama navodi i razloge njezina donošenja te ciljeve koje time želi postići. Točka 60.[128] nabraja razloge zbog kojih su u Prilogu I. detaljno navedeni sadržaj i zahtjevi nad kvalificiranim certifikatima za elektroničke potpise:

„(60) Pružatelji usluga povjerenja koji izdaju kvalificirane certifikate za elektroničke pečate trebali bi primjenjivati neophodne mjere kako bi bili u mogućnosti utvrditi identitet fizičke osobe koja zastupa pravnu osobu kojoj je izdan kvalificirani certifikat za

[128] Isto, članak 3. Definicije, L 257/80

elektronički pečat, ako je takva identifikacija potrebna na nacionalnoj razini u kontekstu sudskog ili upravnog postupka.“

Dakle, Europska unija je kroz Uredbu eIDAS željela što više osigurati pravnu sigurnost u elektroničkom poslovanju i širenje elektroničkog poslovanja. U točkama 1. i 2.[129] uvodnih odredbi navedene težnje se i izrijekom navode:

„(1) Izgradnja povjerenja u online okruženje ključna je za gospodarski i socijalni razvoj. Zbog nedostatka povjerenja, posebno zbog osjećaja pravne nesigurnosti, potrošači, poduzeća i tijela javne vlasti oklijevaju provoditi transakcije elektroničkim putem te koristiti odnosno uvoditi nove usluge.

(2) Ovom Uredbom nastoji se povećati povjerenje u elektroničke transakcije na unutarnjem tržištu pružanjem zajedničkog temelja za sigurnu elektroničku interakciju između građana, poduzeća i tijela javne vlasti, povećavajući time djelotvornost javnih i privatnih online usluga, elektroničkog poslovanja i elektroničke trgovine u Uniji.“

Usporedbe radi u nastavku teksta donosi se sadržaj dijela Uredbe 1999/93/EC (koja se Uredbom eIDAS stavlja izvan snage) koji propisuje da unutar kvalificiranog certifikata moraju biti sadržane sljedeće informacije[130]:

a. podatak da se certifikat izdaje kao kvalificirani certifikat,
b. podatak o identifikaciji certifikacijske službe (izdavatelja) i državi u kojoj je uspostavljen,
c. podatak o nazivu (imenu ili pseudonimu) potpisnika,
d. podatak o specifičnom atributu potpisnika koji se po potrebi može dodati, u ovisnosti o namjeni kvalificiranoga certifikata,
e. podaci za provjeru potpisa koji odgovaraju podacima o potpisivanju koji su pod nadzorom potpisnika,
f. podatak o početku i kraju valjanosti certifikata,
g. identifikacijski kod certifikata,
h. napredni elektronički potpis certifikacijske službe koja izdaje kvalificirani certifikat,

[129] Isto, članak 3. Definicije, L 257/73
[130] Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)

i. ograničenja za korištenje certifikata, ako postoje,

j. limit vrijednosti transakcija za koje se certifikat može koristiti, ako postoji.

Stavke Uredbe eIDAS (Uredba (EU) br. 910/2014) i 1999/93/EC vezane za kvalificirani certifikat su slične na prvi pogled, ali Uredba eIDAS daje jasnija zahtjeve postavljene nad certifikatima za elektroničke potpise te opis sadržaja. Brzica, Herceg, Katulić i Stančić[131] su u svom radu „Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata“ opisali jedan od problema koje je svojim donošenjem Uredbe eIDAS riješila. Radi se o problematici definiranja pojma pravne osobe u dosadašnjem Zakonu o elektroničkom potpisu. Autori definiraju problem na sljedeći način:

„Zakonom o elektroničkom potpisu (ZEP) definirana su pravila primjene neporecivoga elektroničkog potpisa, koji se u navedenom zakonu izvodi primjenom kvalificiranoga certifikata. Zakon se u svojim odredbama poziva na odredbe Direktive 1999/93/EC, unutar koje su raspisane opće smjernice te pojmovi povezani s kvalificiranim certifikatom. Međutim, komparativnom analizom utvrdili smo da postoji znatna razlika između Direktive 1999/93/EC i Zakona o elektroničkom potpisu Republike Hrvatske u dijelu s odredbama povezanima s kvalificiranim certifikatom. Osnovni pojam koji Direktiva poznaje jest „potpisnik“ (engl. signatory). Hrvatsko zakonodavstvo taj pojam svodi na pojam fizičke osobe. Definicija potpisnika kao fizičke osobe u hrvatskom zakonodavstvu onemogućuje bilo kakvu automatizaciju izradbe neporecivoga elektroničkog potpisa, već s ga može izvesti isključivo fizička osoba. Definicija potpisnika u ZEP-u se nalazi u čl. 2. točka 3: „Potpisnik – znači osobu koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koji djeluje u svoje ime ili u ime fizičke i pravne osobe koju predstavlja.“ S druge strane definicija potpisnika u Direktivi koja se također nalazi u čl. 2. točka 3 kaže: „Signatory“ means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. Razmatrajući definiciju potpisnika s obzirom na odredbe koje se odnose na kvalificirani certifikat (Aneks I Direktive /v. poglavlje 3.1.3. ovoga rada/ i čl. 11 ZEP-a), osim

[131] Brzica, H., Herceg, B., Katulić, T., Stančić, H. (2014.), Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata, Arh. vjesn. 57, str. 129-157, https://scholar.google.com/citations?view_op=view_citation&hl=ja&user=OCjAcywAAAAJ&citation_for_view=OCjAcywAAAAJ:2osOgNQ5qMEC (24.07.2017.)

nedosljednosti između točaka b, c i d Aneksa u odnosu na točke 2., 3. i 4. čl. 11., primjećuje se već spomenuta razlika gdje točka 3. čl. 11. kroz tražene podatke uvjetuje potpisnika kao fizičku osobu.“.

Dakle, u vidu bilo kakve automatizacije izrađivanja naprednog elektroničkog potpisa dosadašnji hrvatski Zakon o elektroničkom potpisu nije osiguravao da napredne elektroničke potpise izrađuje npr. računalo već ga je mogla izvesti isključivo fizička osoba.

Uredba eIDAS navodi u stavci (g) Priloga I. da kvalificirani certifikati za elektroničke potpise sadržavaju:

„(g) napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluga povjerenja koji izdaje certifikat“.

Kada povežemo navedenu stavku s točkom 59 Uredbe eIDAS dolazimo do rješenja u kojemu se elektronički pečati mogu primjenjivati za pravne osobe u onoj mjeri u kojoj se elektronički potpisi primjenjuju fizičke osobe. Slijedi točka 59 iz Uredbe eIDAS[132]:

„(59) Elektronički pečati trebali bi služiti kao dokaz da je elektronički dokument izdala pravna osoba, jamčeći na taj način izvornost i cjelovitost dokumenta.“

Elektronički pečat će detaljnije biti opisan u poglavlju 4.2 Elektronički pečat.

Autori gore spomenutog člana su u dijelu koji obrađuje problematiku definiranja pojma pravne osobe u dosadašnjem Zakonu o elektroničkom potpisu ne znajući o pripremi Uredbe eIDAS niti za pripremu pojma elektronički pečat predložili sljedeće poboljšanje zakonske regulative[133]:

„Članak 11 ZEP-a u okviru odredbi koje se odnose na potpisnika kvalificiranoga certifikata (točka 3) treba izmijeniti tako da glasi (podcrtani dio treba dodati): 3. identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako

[132] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/80, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[133] Brzica, H., Herceg, B., Katulić, T., Stančić, H. (2014.), Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata, Arh. vjesn. 57, str. 129-157, https://scholar.google.com/citations?view_op=view_citation&hl=ja&user=OCjAcywAAAAJ&citation_for_view=OCjAcywAAAAJ:2osOgNQ5qMEC (24.07.2017.)

ga osoba ima, datum rođenja, prebivalište, odnosno boravište ili naziv, sjedište i OIB pravne osobe ukoliko je riječ o pravnoj osobi kao potpisniku).

U postojeći članak 5. ZEP kao stavak 2. treba dodati: Odredbe stavka 1. ovoga članka odnose se i na elektronički potpis zasnovan na kvalificiranom certifikatu kojem je potpisnik pravna osoba. Iza članka 11. treba dodati članak 11.a, sadržaj kojega bi trebao glasiti:

Članak 11.a

Kvalificirani certifikat za pravnu osobu sadržava sve elemente propisane člankom 11. ovoga Zakona.

U smislu ovoga zakona kvalificirani certifikat za pravnu osobu koristi se za izradbu naprednoga elektroničkog potpisa u skladu s Pravilnikom o izradi elektroničkog potpisa i s ograničenom primjenom i to za:

1. izdavanje elektroničkih dokumenata iz područja opskrbnog lanca:

a. e-narudžbenica,

b. e-odgovor na narudžbu,

c. e-otpremnica,

d. e-primka,

e. e-povratnica,

f. e-račun,

g. e-odobrenje,

h. e-terećenje.

2. izdavanje potvrde fizičkim i pravnim osobama koje izdaju tijela državne

uprave te lokalne i regionalne (područne) samouprave,

3. potvrde primitka upisa ili promjene podataka u registre tijela državne uprave

te lokalne i regionalne (područne) samouprave,

4. ostale primjene definirane Pravilnikom o izradi elektroničkog potpisa.“

Autori su navedenim prijedlogom poboljšanja zakonske regulative htjeli dati doprinos u rješavanju ograničenja koja su prepoznali u područjima elektroničkog poslovanja i

elektroničke javne uprave s kojim su se susretali (opskrbni lanac, razne potvrde državne uprave i dr.). Realizaciju tih prijedloga je kroz Uredbu eIDAS preuzeo elektronički pečat. Treba napomenuti da ne postoje nikakva saznanja da su autori navedenim prijedlozima utjecali u bilo kojoj mjeri na Uredbu eIDAS.

Sve dosada spomenuto u vezi certifikata za elektronički potpis je usko vezano za ostvarivanje bitnog svojstva elektroničkog potpisa, tj. **neporecivosti** (engl. non-repudiation). Neporecivost zapisa sprječava entitetu mogućnost poricanja sadržaja potpisa, poricanje provedbe neke akcije te time i preuzimanja odgovornosti. Svojstvo neporecivosti sprječava poricanje obavljenih radnje u računalnom svijetu. Neporecivost se uglavnom povezuje s činom potpisivanja elektroničkim potpisom. U hrvatskom zakonodavstvu se neporecivost vezuje uz potpisivanje s naprednim elektroničkim potpisom o čemu će biti više napisano u poglavlju 4.1 Elektronički potpis.

3.5.4 Elektronički vremenski žig

Vremenski žig (engl. Time Stamp) je potvrda Službe za izradu vremenskoga žiga, TSA (engl. Time Stamping Authority). S vremenskim žigom kao izdanom potvrdom se potvrđuje da su podaci postojali u određenom trenutku[134].

Napredni vremenski žig (engl. Trusted Digital Time Stamp) je vremenski žig koji omogućava sigurno određivanje trenutka elektroničkog potpisivanja te praćenje promjena do kojih je dolazilo tijekom vremena[135].

Hrvatski zakon o elektroničkom potpisu koji je stavljen izvan snage Uredbom eIDAS (Uredba (EU) br. 910/2014) je vremenski žig definirao kao[136] elektronički potpisanu potvrdu izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu, a napredan vremenski žig kao elektronički potpisanu potvrdu ovjerovitelja koja ispunjava uvjete za napredan elektronički potpis. Vremenski žig se primjenjuje kao

[134] Wallace C., Pordesch U., Brandner R.(2007.), RFC 4810, Long-Term Archive Service Requirements, https://tools.ietf.org/html/rfc4810 (06.12.2016.)
[135] Ćosić, J., Bača, M. (2010.), (Im)Proving Chain of Custody and Digital Evidence Integ¬rity with Time Stamp, MIPRO – Proceedings of the 33rd International Convention, str. 1227-1228, URL: http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (14.04.2014.)
[136] Hrvatski sabor (2002.), Zakon o elektroničkom potpisu, NN 10/02, http://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html , Članak 2. (21.03.2018.)

dodatak elektroničkom potpisu te se njegovim dodavanjem elektroničkom potpisu potvrđuje da je potpis izrađen u točno određenom trenutku. Time se omogućava provjera točnog trenutka nastanka elektroničkoga potpisa. Postojanje pouzdanog vremenskog žiga je važno zbog dokazivanja integriteta elektroničkog zapisa tijekom vremena njegova čuvanja.

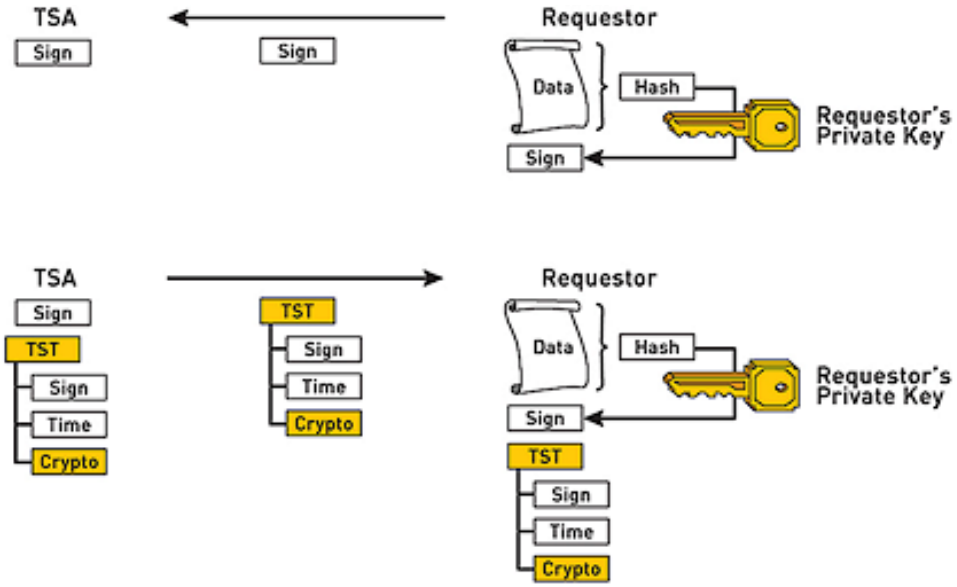
Uredba eIDAS daje složeniju definiciju vremenskog žiga[137] nego opozvani hrvatski Zakon o elektroničkom potpisu, a osim toga mijenja termin u **elektronički vremenski žig**:
„33. „elektronički vremenski žig" znači podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme;". U navedenoj definiciji se ne koristi više termin elektronički potpisane potvrde izdavatelja već se spominju samo podaci u elektroničkom obliku.

Sličan je slučaj i s definicijom naprednog vremenskog žiga, odnosno **kvalificiranim elektroničkim vremenskim žigom** (što je novi termin u skladu s Uredbom eIDAS). Definicija iz opozvanog hrvatskog Zakona govori o takvom vremenskom žigu kao potpisanoj potvrdi ovjerovitelja koji ispunjava određene zahtjeve. Uredba eIDAS definira sljedeće:
„ 34. „kvalificirani elektronički vremenski žig" znači elektronički vremenski žig koji ispunjava zahtjeve navedene u članku 42."
U članku 42. se među navedenim zahtjevima ne spominje potpisana potvrda ovjerovitelja već navodi da se temelji na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom. Osim toga navodi da je takav vremenski žig potpisan pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.
Međutim, može se iščitati da i navedeni hrvatski Zakon i Uredba eIDAS podrazumijevaju isto kada navode ovjerovitelja, odnosno kvalificiranog pružatelja usluga povjerenja. Radi se o Službi za izradu vremenskog žiga, tj. TSA[138] (engl. Time-Stamping Authority) ili

[137] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/85, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)
[138] Pinkas, D. et al. (2003.), RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs), https://tools.ietf.org/html/rfc3628 (25.07.2017.)

QTSA (engl. Qualified Time-Stamping Authority), ako se radi o pružatelju usluga kvalificiranog vremenskog žiga. Zahtjevi nad takvom Službom su definirani u RFC 3628.

Na slici 19 je prikazan proces generiranja vremenskog žiga za potpisane podatke. Za aplikacije koje koriste elektronički potpisane podatke, tražitelj potpisuje digitalni hash sa svojim privatnim ključem i šalje elektronički potpis na TSA. TSA veže zaprimljene podatke s vremenskim žigom koristeći kriptografske funkcije te ga vraća tražitelju. Kada tražitelj zaprimi vremenski žig od TSA, on može opcionalno potpisati vremenski žig sa svojim privatnim ključem. Tražitelj sada ima dokaz da su podaci postojali u vrijeme izdano od TSA. Prilikom provjere vremenskog žiga kod ovlaštenog verifikatora, osigurava se i dokaz da je elektronički potpis postajao prilikom izrade elektroničkog potpisa, tako da se ne može osporiti njegovo stvaranje od strane potpisnika.



Slika 19. Generiranje vremenskog žiga za potpisane podatke, preuzeto s wikipedije[139]

Bitno je navesti kako je Uredba eIDAS definirala pravni učinak elektroničkih vremenskih žigova (u članku 41.[140]):

[139] Wikipedia, http://en.wikipedia.org/wiki/ANSI_ASC_X9.95_Standard (15.04.2015.)
[140] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Europski parlament, članak 3. Definicije, L 257/106, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

„ 1. Elektroničkom vremenskom žigu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve kvalificiranog elektroničkog vremenskog žiga.
2. Za kvalificirani elektronički vremenski žig predmnijeva se točnost datuma i vremena koje pokazuje te cjelovitost podataka s kojima su datum i vrijeme povezani.
3. Kvalificirani elektronički vremenski žig izdan u jednoj državi članici priznaje se kao kvalificirani elektronički vremenski žig u svim državama članicama.“

Dakle, vodi se dosta računa o tome da bi se elektronički vremenski žig mogao koristiti kao dokaz u sudskim postupcima i to u različitim državama članicama Europske unije. Osim toga, elektroničkim vremenskim žigom se omogućuje povjerenje u elektronički potpis i poslije isteka certifikata potpisnika (zbog isteka valjanosti ili zbog opoziva). Na taj način se omogućuju pretpostavke za dugoročno arhiviranje elektronički potpisanih dokumenata.

3.6 ZAKLJUČAK

Cilj ovog poglavlja je bio opisati što detaljnije infrastrukturu javnog ključa (PKI) iz razloga nalaženja temelja za izgradnju i implementaciju informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata. Osim toga cilj je bio opisati servise i komponente temeljene na infrastrukturi javnog ključa u Republici Hrvatskoj koji se mogu učinkovito iskoristiti za izgradnju infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave.
Za početak je obrađena tematika kriptologije koja se kao grana kriptografije bavi izučavanjem i definiranjem metoda za zaštitu informacija te izučavanjem i pronalaženjem metoda za otkrivanje šifriranih informacija. Kriptografija ima sljedeće funkcije: povjerljivost, integritet podataka, autentikacija te neporecivost. Opisane su simetrična i asimetrična kriptografija te i jedna i druga kriptografija mogu pružiti sve četiri navedene funkcije. PKI infrastruktura je sustav koji pokriva sve funkcionalnosti kriptografije.

Simetrična kriptografija ili kriptografija tajnim ključem je najstariji poznati oblik kriptografije. Kod nje su ključ kojim se kriptira poruka i ključ dekriptiranja jednaki te predstavljaju tajni ključ. Samo sudionici sigurne komunikacije poznaju tajni ključ. Simetrični kriptografski algoritmi, danas najrašireniji u internet protokolima su DES i IDEA.

Asimetrična kriptografija ili kriptografija javnim ključem se koristi s dva različita ključa od kojih se jedan koristi za kriptiranje a drugi za dekriptiranje. Prednost asimetrične kriptografije nad simetričnom je što je broj ključeva koje treba razmijeniti uvijek isti bez obzira na broj sudionika komunikacije. Najpoznatiji asimetrični algoritmi su: ECC ili kriptografija eliptične krivulje, RSA, DSA i SHA-1. Kriptosustavi koji su temeljeni na eliptičkim krivuljama (ECC) imaju višestruko manju duljinu ključa od drugih asimetričnih kriptoalgoritama, ali pružaju gotovo istu sigurnost kao drugi kriptosustavi (npr. RSA). Zbog toga je ECC vrlo primjenjiv za sustave kod kojih je prostor za pohranu ključeva ograničen (npr. pametne kartice).

U ovom poglavlju su obrađeni i PKI standardi. Standard koji se koristi za zapis digitalnih certifikata je X.509. Danas je u upotrebi standard X.509 v3. Radna skupina za sustav infrastrukture javnog ključa temeljenog na X-509 (PKIX) pod nazivom PKIX-WG je ustanovila IETF organizacija da bi razvila potrebne internetske standarde koji će podržati infrastrukturu javnog ključa temeljenu na X.509 protokolu. PKIX ima pet standardizacijskih područja pod kojima su navedeni generalni zahtjevi: profili X.509 digitalnih certifikata i liste opozvanih certifikata, funkcije upravljanja, operativni protokoli, politike certifikata i pravilnik o postupcima certificiranja, servisi vremenskog žiga i servisi validacije/potvrde podataka.

Standardi kriptografije javnog ključa (PKCS) su skup standarda koji je snažan uticao na korištenje kriptografije javnog ključa u praksi. PKCS standardi su skup standarda te su nazvani PKCS #1 do #15. PKCS standardi pokrivaju RSA kriptiranje, RSA potpis, kriptiranje lozinkom, sintaksu kriptografske poruke i dr.

Infrastruktura javnoga ključa (PKI) je složena informacijska infrastruktura koja služi za upravljanje elektroničkim identitetima. U temelju rada PKI infrastrukture je uporaba asimetrične kriptografije. Funkcionalnosti PKI infrastrukture su: registracija, inicijalizacija, certifikacija, oporavak para ključeva, obnova para ključeva, zahtjev za opozivom, međusobna certifikacija i objava liste opozvanih certifikata.

Unutar PKI infrastrukture funkciju izdavanja i opozivanja digitalnih certifikata ima certifikacijska služba (CA). Certifikacijska služba je nadležna za ovjeru identiteta. Registracijska služba (RA) u PKI infrastrukturi javnog ključa predstavlja autoritet za provjeru zahtjeva entiteta za izdavanjem digitalnih certifikata koji potvrđuje valjanost zahtjeva certifikacijskoj službi, ali nije obavezna komponenta. CA može delegirati

registracijskoj službi neke od administrativnih funkcija. Na stranicama Ministarstva gospodarstva Republike Hrvatske su na dan 28. prosinca 2017. kao davatelji usluga certificiranja u Republici Hrvatskoj navedeni: FINA, AKD i Zagrebačka banka.

Uredba eIDAS je certifikat za elektronički potpis definirala na sljedeći način[141]: „certifikat za elektronički potpis" znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe. Veza javnog ključa entiteta sa setom informacija koje identificiraju entitet se potvrđuje elektroničkim potpisom certifikacijske službe koja je izdala certifikat. Najraširenija format digitalnih certifikata je X.509 v3. Certifikat za elektronički potpis je tehnološka podloga za ostvarivanje bitnog svojstva elektroničkog potpisa, tj. neporecivosti. Neporecivost zapisa sprječava entitetu mogućnost poricanja sadržaja potpisa te poricanje provedbe neke akcije.

Na kraju ovog poglavlja je obrađen i vremenski žig. To je potvrda Službe za izradu vremenskoga žiga (TSA). Funkcija vremenskog žiga kao izdane potvrde je potvrditi da su podaci postojali u određenom trenutku. Uredba eIDAS mijenja termin vremenskog žiga u elektronički vremenski žig te vodi dosta računa o tome da bi se elektronički vremenski žig mogao koristiti kao dokaz u sudskim postupcima i to u različitim državama članicama Europske unije. Elektronički vremenski žig je bitan iz razloga što omogućuje povjerenje u elektronički potpis i poslije isteka certifikata potpisnika (zbog isteka valjanosti ili zbog opoziva). Navedeno je vrlo bitna činjenica za ovaj rad jer se omogućuju pretpostavke za dugoročno arhiviranje elektronički potpisanih dokumenata.

[141] Isto, članak 3. Definicije, L 257/84

4. NAPREDNI ELEKTRONIČKI POTPIS KAO PODLOGA ZA DUGOROČNO OČUVANJE ELEKTRONIČKIH ZAPISA

U ovom poglavlju će prvo biti opisan elektronički potpis. Za elektronički potpis će se dati definicije te pregled izmjene EU i hrvatske regulative od 2014. godine. Posebno će se detaljno obraditi Uredbu eIDAS (Uredba (EU) br. 910/2014) te napraviti usporedba s do tada važećom EU Direktivom 1999/93/EC. Prilikom obrade ovog područja će se posebno voditi računa o naprednom elektroničkom potpisu koji je izuzetno bitan za ovaj rad. Nadalje će biti obrađen elektronički pečat koji je Uredba eIDAS propisala te će se navesti njegova svrha te razlike naspram elektroničkog potpisa.

Detaljno će biti obrađeni formati elektroničkog potpisa koji spadaju u kategoriju naprednog elektroničkog potpisa te će biti dana njihova kratka usporedba. CAdES, XAdES i PAdES su formati naprednog elektroničkog potpisa (engl. AdES, Advanced Electronic Signatures) koji su sukladni s Uredbom eIDAS te će se ovaj rad, međuostalim, referencirati i na pripadne ETSI tehničke specifikacije kojim se ovi formati opisuju.

ETSI norma EN 319 102-1 je za ovaj rad bitna iz razloga što detaljno propisuje procese izrađivanja i validacije naprednog elektroničkog potpisa. Ova norma je jedna od ekstenzija Uredbe eIDAS te je bitna u samom propisivanju detalja samih procesa izrade i validacije. Norma ETSI EN 319 102-1 definira četiri klase potpisa koje su međusobno uvećavajuće te će se svaka biti detaljno opisana u potpoglavlju izrađivanja naprednog elektroničkog potpisa.

Na kraju ovog poglavlja će se detaljno opisati proces validacije naprednog elektroničkog potpisa, od sheme validacije osnovnog elektroničkog potpisa, gradivnih blokova prikazane sheme do statusa koje sam validacijski proces može generirati. U potpoglavlju validacije naprednog elektroničkog potpisa će se opisati, što je jako bitno za ovaj rad, mogućnost validacije elektroničkog potpisa u dugom roku.

4.1 ELEKTRONIČKI POTPIS

Elektronički potpis (engl. Electronic Signature) predstavlja ekvivalent vlastoručnom potpisu u elektroničkom obliku. Hrvatski zakon iz 2002. je elektronički potpis

definirao[142] kao skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanog elektroničkog dokumenta. Elektronički potpis sadrži podatke u elektroničkom obliku koji su vezani za elektroničke dokumente (npr. računi, ugovori i dr.), te transakcije. On služi kao sredstvo za potvrdu i provjeru autentičnosti. Pogrešno je sliku vlastoručnog potpisa smatrati elektroničkim potpisom. To je digitalizirani, a ne elektronički potpis (ili digitalni). Elektronički potpis predstavlja drugačiji niz znakova kod svakog potpisivanja. Kada bi to bio uvijek isti niz, elektronički potpis bi se mogao tada neovlašteno kopirati na neki drugi dokument u elektroničkom svijetu. Jedino korištenjem kriptografskih transformacija podataka se primatelju podataka može osigurati provjeru podrijetla i integriteta potpisanih podataka. Za izradu i provjeru elektroničkog potpisa je potrebna infrastruktura javnoga ključa (PKI).

Unutar Europske unije je pitanje elektroničkog potpisa bilo vrlo bitno za pravni okvir elektroničkog poslovanja. Krajem 1999. je iz tog razloga donesena Direktiva o elektroničkom potpisu 1999/93/EC[143]. Tom direktivom se htjelo stvoriti jedinstveni zakonodavni okvir za primjenu elektroničkoga potpisa na području zemalja članica Europske unije. Rezultat toga je bilo to da se elektronički potpis mogao upotrebljavati u elektroničkom poslovanju s istom pravnom snagom kao i vlastoručni potpis s običnog, papirnatog dokumenta. Direktiva 1999/93/EC je razlikovala dva tipa elektroničkog potpisa: elektronički potpis (osnovni ili radni) i napredni elektronički potpisa.

Napredni elektronički potpis je bio definiran kao potpis zasnovan na kvalificiranom certifikatu. Da bi neki elektronički zapis očuvao svojstvo neporecivosti neophodno je osigurati[144]:

1. digitalni identitet potpisnika,
2. opoziv prava potpisa u realnom vremenu,

[142] Hrvatski sabor (2002.), Zakon o elektroničkom potpisu, NN 10/02, http://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html , Članak 2. (21.03.2018.)
[143] Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)
[144] Brzica, H., Herceg, B., Stančić, H. (2013), Long-term Preservation of Validity of Electronically Signed Records, u: Gilliland, A. et al. (ur.), INFuture2013: Information Governance, Zagreb : Odsjek za informacijske i komunikacijske znanosti Filozofskoga fakulteta Sveučilišta u Zagrebu, str. 150, https://bib.irb.hr/datoteka/662133.403_Brzica_Herceg_Stancic_LTP_of_Validity_of_Electronically_Signed_Records.pdf (21.03.2018.)

3. vremensku ovjeru elektroničkog potpisa nakon provjere liste opozvanih certifikata čime se osigurava valjanost elektroničkoga potpisa u trenutku potpisivanja,
4. dugoročno i sigurno očuvanje arhiviranog zapisa koji je elektronički potpisan kao i osiguranje mogućnosti provjere elektroničkoga potpisa.

Elektronički potpis, je prema EU Direktivi 1999/93/EC, morao zadovoljiti sljedeće zahtjeve kako bi postao napredni elektronički potpis (engl. Advanced Electronic Signature) [145]:

1. jedinstveno je povezan s potpisnikom,
2. njime je moguće jedinstveno identificirati potpisnika,
3. stvoren je načinima koje potpisnik kontrolira i koji nisu dostupni drugima,
4. povezan je s podacima koje potpisuje tako da se svaku naknadnu izmjenu može detektirati.

Elektroničke transakcije koje su zaštićene primjenom digitalnih certifikata i elektroničkog potpisa zadovoljavaju zahtjeve elektroničkog poslovanja[146]:

1. autentifikaciju – proces kojim korisnik dokazuje da je zaista onaj za kojeg se predstavlja.
2. integritet – sigurnost da podaci u prijenosu ili obradi nisu uništeni ili promijenjeni.
3. tajnost – kriptiranje podataka koji će biti pohranjeni ili poslani mrežom štiti čitanje sadržaja od neovlaštenih osoba.
4. neporecivost – onemogućavanje poricanja (negiranja) akcije koje je osoba poduzela ili autorizirala. Ova mogućnost je realizirana kroz napredni elektronički potpis.

Osim elektroničkog potpisa i naprednog elektroničkog potpisa Direktiva 1999/93/EC je uvela i pojam kvalificiranog digitalnog certifikata.

[145] Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)
[146] FINA, Elektroničko poslovanja – e-poslovanje, http://www.fina.hr/Default.aspx?sec=940 (15.04.2015.)

Sljedeći bitan zakonodavni događaj vezan za elektronički potpis vezan za Europsku uniju i Republiku Hrvatsku se dogodio u srpnju 2014. Naime, tada su Europski parlament i Vijeće donijeli Uredbu eIDAS (Uredba (EU) br. 910/2014)[147]. Uredba eIDAS je uredba o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ. Uredba eIDAS je stupila na snagu 17. rujna 2014. Početak pune primjene je bio od 1. srpnja 2016., a prijelazno razdoblje za pružatelje usluga (TSP, engl. Trust Service Providers) do 1. srpnja 2017. Uredba je zakonodavni akt za sve članice Europske unije tako i za Republiku Hrvatsku. Sve članice Europske unije su dobile zadatak prilagoditi spomenutu Uredbu sa svojim nacionalnim zakonodavstvom.

Hrvatski Sabor je donio Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ[148]. Spomenuti hrvatski zakon je na snazi od 8. srpnja 2017., a time je izvan snage stavljen Zakon o elektroničkom potpisu iz 2002.

U Uredbi eIDAS u članku definicija je dana i definicija elektroničkog potpisa[149]: „Elektronički potpis znači podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje“.
Navedena definicije je gotovo istovjetno onoj iz starog hrvatskog Zakona o elektroničkom potpisu: „Elektronički potpis je skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanog elektroničkog dokumenta“. U ovoj

[147] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)
[148] Hrvatski sabor (2017.), Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, NN 62/17 , http://narodne-novine.nn.hr/clanci/sluzbeni/2017_06_62_1430.html (23.07.2017.)
[149] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

definiciji se spominju i identifikacije potpisnika i elektronički dokumenti, a u Uredbi eIDAS je navedeno obrađeno kroz ostatak Uredbe.

Bitno je spomenuti da Uredba eIDAS strogo razdvaja namjene elektroničkog potpisa i elektroničkog pečata koji će detaljnije biti razrađeni u sljedećem poglavlju. Iz navedenog razloga potpisnik se u Uredbi definira kao fizička osoba koja izrađuje elektronički potpis.

Dakle, autor elektroničkog potpisa može biti samo fizička osoba. S druge strane autor elektroničkog pečata može biti samo pravna osoba, a elektronički pečat služi za osiguravanje izvornosti i cjelovitosti podataka.

Za izradu elektroničkog potpisa služi certifikat za elektronički potpis (opisan u poglavlju 3.5.3 Certifikati za elektronički potpis), a za izradu elektroničkog pečata služe certifikati za elektroničke pečate (bit će detaljnije opisano u poglavlju 4.2 Elektronički pečat).

Od bitnih definicija iz Uredbe eIDAS vezanih za elektroničke potpise treba spomenuti i napredan elektronički potpis i kvalificirani elektronički potpis.

Napredan elektronički potpis Uredba definira kao elektronički potpis koji ispunjava zahtjeve navedene u članku 26., a kvalificirani elektronički potpis definira kao napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.

Članak 26. definira zahtjeve za napredne elektroničke potpise[150]:

„Napredan elektronički potpis mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način je povezan s potpisnikom;

(b) omogućava identificiranje potpisnika;

(c) izrađen je korištenjem podataka za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom; i

(d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.“

Kvalificirano sredstvo za izradu elektroničkog potpisa ili QSCD (engl. Qualified Electronic Signature Creation Device), dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu elektroničkog potpisa te zaštićuju elektronički potpis od krivotvorenja i sl.

U članku 25. Uredbe eIDAS su opisani i pravni učinci elektroničkih potpisa:

[150] Isto, članak 3. Definicije, L 257/84

„1. Elektroničkom potpisu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalificirani elektronički potpis.
2. Kvalificirani elektronički potpis ima jednak pravni učinak kao vlastoručni potpis.
3. Kvalificirani elektronički potpis koji se temelji na kvalificiranom certifikatu izdanom u jednoj državi članici priznaje se kao kvalificirani elektronički potpis u svim ostalim državama članicama.“

Ako napravimo usporedbu s Direktivom 1999/93/EZ, ona je u članku 5.[151] navodila da zemlje članice EU neće uskratiti elektroničkom potpisu (u smislu osnovnog, a ne naprednog) mogućnost ostvarivanja pravnih učinaka i upotrebe kao dokaza u pravnim postupcima samo zato što:

1. je potpis dan u elektroničkom obliku,
2. potpis nije baziran na kvalificiranom certifikatu,
3. potpis nije baziran na kvalificiranom certifikatu izdanom od strane ovlaštenoga certifikacijskog tijela,
4. potpis nije učinjen putem posebnog uređaja za stvaranje elektroničkoga potpisa

Iz navedene usporedbe se može zaključiti da Direktiva 1999/93/EZ i Uredba eIDAS određuju gotovo isto područje, ali Uredba je napravila korak više u pojednostavljenu primjene kvalificiranog elektroničkog potpisa kao naprednog elektroničkog potpisa uz određene uvjete (primjena kvalificiranih sredstava za izradu elektroničkog potpisa i temeljenje na kvalificiranom certifikatu za elektroničke potpise). Dakle, svaki kvalificirani elektronički potpis je ujedno i napredan elektronički potpis. S druge strane, svaki napredni elektronički potpis ne mora biti kvalificirani elektronički potpis. Navedeni zaključak je bitan iz razloga pravnog učinka (Uredba eIDAS, članak 25., stavka 2. u Uredbi): „Kvalificirani elektronički potpis ima jednak pravni učinak kao vlastoručni potpis“. Međutim, elektroničkim potpisima koji nisu kvalificirani se ne smiju uskratiti pravni učinak i dopuštenost u sudskim postupcima (Uredba eIDAS, članak 25., stavka 1.).

[151] Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)

U Direktivi 1999/93/EC postoji velik broj navedenih tehničkih detalja pa se navedena direktiva mogla smatrati i tehnološkim propisom jer jasno upućuje na izradu potpisa i naprednog elektroničkog potpisa primjenjujući tehnologiju infrastrukture javnog ključa.

Uredba eIDAS izričito navodi, pak, načelo tehnološke neutralnosti kao jedno od svojih polazišta[152]:

„(27) Ova Uredba trebala bi biti tehnološki neutralna. Pravni učinci koji se njome osiguravaju trebali bi biti ostvarivi bilo kojim tehničkim sredstvima pod uvjetom da su zahtjevi ove Uredbe ispunjeni.“.

Bez obzira na pozivanje na načelo tehnološke neutralnosti, Uredba se slično kao i Direktiva 1999/93/EC poziva na nužnost korištenja infrastrukture javnog ključa na paneuropskoj razini, međuostalim, i zbog osiguravanja prekogranične interoperabilnosti elektroničkih transakcija:

„(7) Europski parlament je u svojoj rezoluciji od 21. rujna 2010. o dovršetku formiranja unutarnjeg tržišta za elektroničku trgovinu (1) naglasio važnost sigurnosti elektroničkih usluga, naročito elektroničkih potpisa, i potrebu za stvaranjem infrastrukture javnog ključa (Public Key Infrastructure – PKI) na paneuropskoj razini, te je pozvao Komisiju da uspostavi europski portal tijelâ za validaciju radi osiguravanja prekogranične interoperabilnosti elektroničkih potpisa i povećavanja sigurnosti transakcija koje se obavljaju putem interneta.“

Što se tiče dugoročnog čuvanja elektroničkih potpisa Uredba eIDAS u članku 34. definira kvalificiranu usluga čuvanja kvalificiranih elektroničkih potpisa[153]:

„1. Kvalificiranu uslugu čuvanja kvalificiranih elektroničkih potpisa može pružati samo kvalificirani pružatelj usluga povjerenja koji koristi postupke i tehnologije koje mogu produljiti pouzdanost kvalificiranog elektroničkog potpisa na razdoblje koje je dulje od razdoblja tehnološke valjanosti.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificiranu uslugu čuvanja kvalificiranih elektroničkih potpisa. Ako dogovori za kvalificiranu uslugu

[152] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/76, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[153] Isto, članak 3. Definicije, L 257/103

čuvanja kvalificiranih elektroničkih potpisa udovoljavaju tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1.
Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.“
U članku 48. stavci 2. se navodi da Komisiji pomaže Odbor (odbor u smislu uredbe (EU) br. 182/2011.[154]) . Nadalje, navodi se primjena članka 5. Uredbe (EU) br. 182/2011. Koja se odnosi na postupak ispitivanja. Naime, kada se primjenjuje postupak ispitivanja za akte koji se donose na prijedlog Komisije, Odbor donosi mišljenje većinom. Kada je mišljenje odbora pozitivno, Komisija donosi nacrtom predviđeni provedbeni akt.

Osim o elektroničkom potpisu navedena Uredba eIDAS definira i razrađuje i druge elemente potrebne za osiguravanje većeg širenja i uporabe elektroničkog poslovanja, a bitni su i za ovaj rad te će biti spomenuti u drugim poglavljima ovog rada: elektronički pečat, elektronički vremenski žig, elektronički dokumenti, očuvanje elektroničkih potpisa i pečata i dr.

4.2 ELEKTRONIČKI PEČAT

U poglavlju 4.1 Elektronički potpis je navedeno da autor elektroničkog potpisa može biti samo fizička osoba. S druge strane autor elektroničkog pečata može biti samo pravna osoba, a elektronički pečat služi za osiguravanje izvornosti i cjelovitosti podataka.

Uredba eIDAS za elektronički pečat navodi i sljedeće odredbe[155]:
„(58) Kada je za transakciju potreban kvalificirani elektronički pečat pravne osobe, kvalificirani elektronički potpis ovlaštenog predstavnika pravne osobe trebao bi biti jednako prihvatljiv.
(59) Elektronički pečati trebali bi služiti kao dokaz da je elektronički dokument izdala pravna osoba, jamčeći na taj način izvornost i cjelovitost dokumenta.

[154] Europski parlament i Vijeće (2011.), Uredba br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32011R0182&from=HR (07.08.2017.)
[155] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/80, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

(65) Osim autentikacije dokumenta koji je izdala pravna osoba, elektronički pečati mogu se koristiti i za autentikaciju bilo koje digitalne imovine pravne osobe, kao što su softverski kod ili poslužitelji.“

Gore navedenim odredbama Uredbom eIDAS se pokazuje težnja primjene elektroničkog pečata za potrebe elektroničkog poslovanja u domeni pravne osobe za osiguravanje izvornosti i cjelovitosti podataka.

Uredba eIDAS, nadalje, čitavim nizom definicija[156] opisuje sve bitne termine vezane uz elektroničke pečate. Autor pečata znači pravna osoba koja izrađuje elektronički pečat, a sam elektronički pečat je definiran kao podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.

Napredan elektronički pečat je definiran kao elektronički pečat koji ispunjava zahtjeve navedene u članku 36.:

„Napredan elektronički pečat mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način je povezan s autorom pečata;

(b) omogućava identificiranje autora pečata;

(c) izrađen je korištenjem podataka za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata; i

(d) povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka.“

Kvalificirani elektronički pečat je definiran kao napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat.

Certifikat za elektronički pečat je definiran kao elektronička potvrda koja povezuje podatke za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe.

Kvalificirani certifikat za elektronički pečat znači certifikat za elektronički pečat koji izdaje kvalificirani pružatelj usluge povjerenja i koji ispunjava zahtjeve određene u Prilogu III[157] Uredbe eIDAS.

[156] Isto, , članak 3. Definicije, L 257/85
[157] Isto, članak 3. Definicije, L 257/113

Kvalificirano sredstvo za izradu elektroničkog pečata (QSCD) dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu elektroničkog pečata, zaštićuje elektronički pečat od krivotvorenja i.t.d.

4.3 FORMATI ELEKTRONIČKIH POTPISA

Elektroničke potpise se može izrađivati prema različitim standardima. Međuostalim, to mogu biti sljedeći standardi: CMS (PKCS#7), XMLDSig, CAdES, XAdES i PAdES. Zadnja tri navedena standarda imaju definirane i profile koji su namijenjeni dugoročnom arhiviranju te će iz navedenog razloga biti detaljnije razrađeni u ovom radu. CAdES, XAdES i PAdES su formati naprednog elektroničkog potpisa (engl. AdES, Advanced Electronic Signatures). Turner u svom članku „Advanced Electronic Signatures for eIDAS“[158] opisuje što su napredni elektronički potpisi i kakvo je njihovo značenje, prema Uredbi eIDAS, za države članice EU.
S tehničke točke gledišta napredni elektronički potpisi koje priznaje Europska unija i koji su sukladni s Uredbom eIDAS mogu biti implementirani kroz sljedeća tri formata elektroničkog potpisa: XAdES (XML), CAdES i PAdES (PDF). Ova tri standarda su razvijena od strane ETSI instituta (engl. European Telecommunications Standards Institute).

U nastavku slijede potpoglavlja koja opisuju formate elektroničkog potpisa i naprednog elektroničkog potpisa

4.3.1 CMS

CMS je široko korišten standard definiran od strane IETF organizacije (engl. Internet Engineering Task Force) za kriptografski zaštićene poruke. CMS ima sintaksu omotnice za zaštitu podataka koja koristi ASN.1[159] (engl. Abstract Syntax Notation One) sintaksu i

[158] Turner, D. M. (2016.), Advanced Electronic Signatures for eIDAS, Cryptomathic, https://www.cryptomathic.com/news-events/blog/advanced-electronic-signatures (09.08.2017.)
[159] ASN, http://www.itu.int/en/ITU-T/asn1/Pages/asn1_project.aspx (15.08.2017.)

može biti korištena za elektronički potpis, autenticiranje ili kriptiranje bilo koje forme digitalnih podataka.

CMS je izveden iz sintakse PKCS#7[160] standarda te omogućava višestruke omotnice. Primjerice jedna omotnica može biti ugniježđena unutar druge. Drugi atributi kao što je potpisno vrijeme mogu biti autenticirani uz sadržaj poruke.

CMS elektronički potpis osigurava elektronički potpis u BER (engl. Basic Encoding Rules) ili DER (engl. Distinguished Encoding Rules) kodiranoj ASN.1 strukturi. Infrastruktura javnog ključa (PKIX) podržava CMS standard.

Mnogi kriptografski standardi koriste CMS kao kriptografsku komponentu:

- S/MIME (engl. Secure/Multipurpose Internet Mail Extensions),
- Protokoli za osiguravanje elektroničke pošte (kriptiranje mail-ova),
- PKCS#12 kao standard koji služi kao spremište X.509 certifikata skupa s njegovim privatnim ključem ili za grupiranje certifikata u lanac (engl. certificate chain),
- Protokol stavljanja vremenskog žiga.

4.3.2 XMLDSig

XML potpis definira XML sintaksu za elektroničke potpise[161]. Definiran je u W3C preporuci – Sintaksa i procesiranje XML potpisa. XML potpis je znan i pod nazivima: XMLDSig[162], XML-DSig i XML-Sig. XML potpis se može primijeniti na bilo koji digitalni sadržaj (podatkovni objekt), uključujući XML. XML potpis se može primijeniti na sadržaj jednog ili više izvora.

Odvojeni (engl. Detached) potpis je XML potpis koji se koristi za potpisivanje resursa izvan XML dokumenta.

Omotani (engl. Enveloped) ili omotavajući (engl. Enveloping) potpisi su XML potpisi kojim se potpisuju podaci unutar istog XML dokumenta. Potpis se nalazi unutar

[160] RSA (1993., 2.), PKCS #7: Cryptographic Message Syntax Standard, ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-7.asc (21.03.2018.)
[161] CIS – Centar informacijske sigurnosti (2011.), XML digitalni potpis, http://www.cis.hr/files/dokumenti/CIS-DOC-2011-07-020.pdf (15.08.2017.)
[162] XMLDSig, http://www.w3.org/TR/xmldsig-core/ (15.08.2017.)

dokumenta (omotani potpis) ili potpis omeđuje dokument koji potpisuje (omotavajući dokument).

Jednim XML potpisom moguće je potpisati više dokumenata.

4.3.3 XAdES

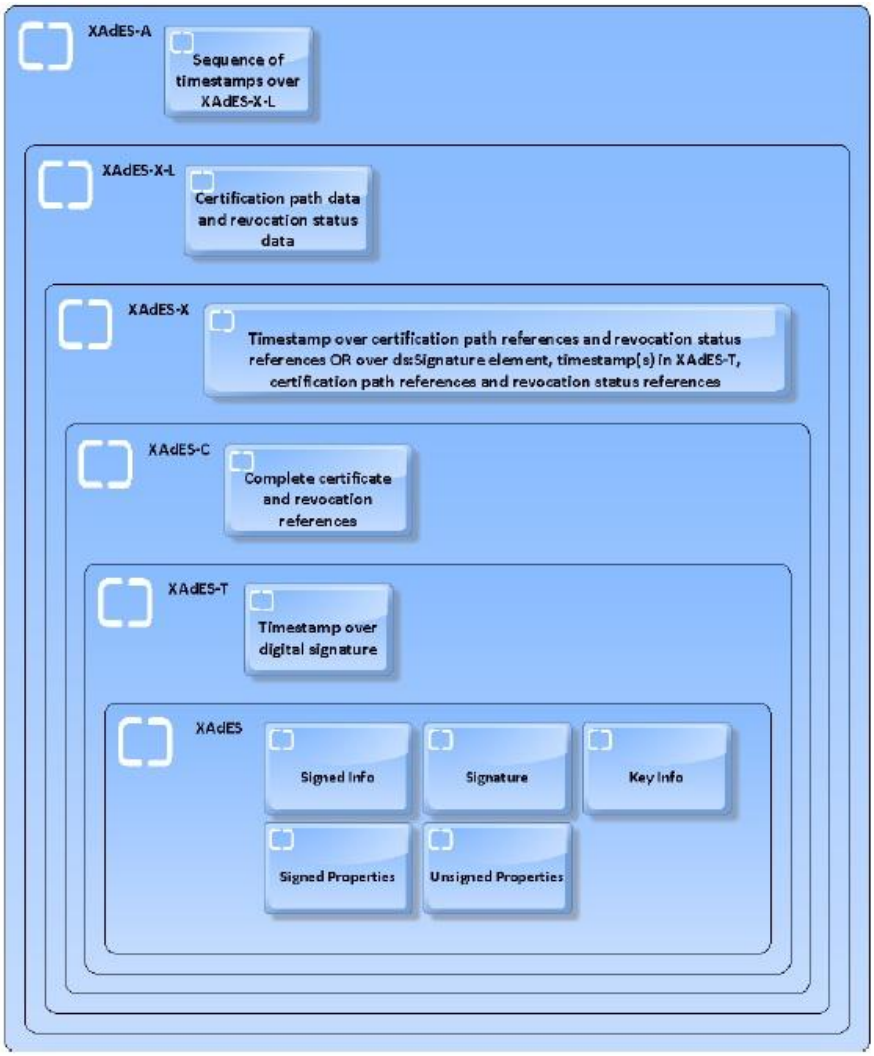
XAdES[163] (XML napredni elektronički potpis) – Osigurava osnovnu autentikaciju i zaštitu integriteta te zadovoljava pravne zahtjeve za naprednim elektroničkim potpisom kao što je definirano u EU direktivi 1999/93/EC i Uredbi eIDAS. XAdES ETSI tehnička specifikacija je definirana kao TS 101 903[164]. Na njoj je definiran XAdES Baseline Profile – ETSI TS 103 171[165].

XAdES ETSI tehnička specifikacija definira šest profila koji se razlikuju po razini zaštite koju nude, ali svaki profil uključuje i prethodni:

- XAdES – osnovna forma (engl. basic form) – osnovi profil. U skladu je sa zakonskim zahtjevima iz Uredbe eIDAS za napredni elektronički potpis,
- XAdES-T (engl. timestamp) – dodano polje vremenskog žiga radi osiguravanja neporecivosti,
- XAdES-C (engl. complete) - Ovaj profil je nadogradnja na XAdES-T potpis i uključuje dodatne podatke potrebne za provjeru:
    - Redoslijeda referenci na cijelom skupu CA certifikata koji se koriste za provjeru elektroničkog potpisa do (ali ne uključujući) potpisnikovog certifikata
    - Potpunog skupa referenci za opoziv podataka koji su korišteni u validaciji potpisnikovog i CA certifikata,
- XAdES-X (engl. extended) - dodavanje vremenskih žigova na reference uvedenim u XAdES-C radi zaštite od mogućeg budućeg kompromisa među certifikatima u lancu,

[163] XAdES, http://www.w3.org/TR/XAdES/ (21.08.2017.)
[164] ETSI (2010), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), ETSI TS 101 903 V1.4.2 (2010-12), Technical Specification, http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf (21.08.2017.)
[165] ETSI (2012.), ETSI TS 103 171 V2.1.1 (2012-03), http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf (21.08.2017.)

- XAdES-X-L (engl. extended long-term) – dodavanje važećih certifikata i popisa opozvanih certifikata na potpisani dokument kako bi se omogućila provjera u budućnosti, čak i ako njihov originalni izvor nije dostupan,
- XAdES-A (engl. archival) – dodana mogućnost periodičnog dodavanja vremenskih žigova na arhivirane dokumente.



Slika 20. Struktura XAdES specifikacijske forme, preuzeto iz Brzica, H., Herceg, B., Stančić, H. (2013)[166]

Baseline profili su definirani Normom ETSI EN 319 102-1[167] te je to imalo za svrhu od više različitih razina AdES formata izdvojiti manji skup razina radi olakšavanja

[166] Brzica, H., Herceg, B., Stančić, H. (2013), Long-term Preservation of Validity of Electronically Signed Records, u: Gilliland, A. et al. (ur.), INFuture2013: Information Governance, Zagreb : Odsjek za informacijske i komunikacijske znanosti Filozofskoga fakulteta Sveučilišta u Zagrebu, https://bib.irb.hr/datoteka/662133.403_Brzica_Herceg_Stancic_LTP_of_Validity_of_Electronically_Signed_Records.pdf, str. 158 (21.03.2018.)

interoperabilnosti elektronički potpisanih dokumenata. Definirane su četiri razine koje opisuje Baseline profili, a njima se nastojalo ukloniti poteškoće u prekograničnom korištenju naprednih elektroničkih potpisa (vrijedi za XAdES, CAdES i PAdES).

Postoje četiri razine elektroničkih potpisa koje definiraju Baseline profili:

- B-B (engl. Basic) – osnovna razina
- B-T (engl. Timestamp) – dodan je vremenski žig na B razinu
- B-LT (engl. Long Term) – na T razinu su dodani podaci za provjeru certifikata
- B-LTA (engl. Long Term with Archive timestamps) – omogućeno je periodičko dodavanje arhivskih vremenskih žigova na LT razinu

4.3.4 CAdES

CAdES[168] (CMS napredni elektronički potpis) je skup proširenja za CMS (eng. Cryptographic Message Syntax) potpisane podatke.

CADES definira šest profila (slično kao XAdES). CAdES profili se razlikuju po razini zaštite koju nude, ali svaki profil uključuje i prethodni: CAdES - osnovna forma (engl. basic form), CAdES-T (engl. timestamp), CAdES-C (engl. complete), CAdES-X (engl. extended), CAdES-X-L (engl. extended long-term) and CAdES-A (engl. archival).

CAdES ETSI tehnička specifikacija je TS 101 733[169].

Kao i za XAdES tako i za CAdES postoje četiri razine Baseline profila elektroničkih potpisa: B, T, LT i LTA.

---

[167] ETSI (2016.), Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation ; ETSI EN 319 102-1 V1.1.1 (2016-05); http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf (22.08.2017.)

[168] CAdES - CMS Advanced Electronic Signatures (CAdES), http://tools.ietf.org/html/rfc5126 (21.08.2017.)

[169] ETSI (2013.), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES); ETSI TS 101 733 V2.2.1 (2013-04); http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf (21.08.2017.)

4.3.5 PAdES

PDF (eng. Portable Document Format) je vrlo raširen format dokumenta. PDF pruža mehanizam elektroničkog potpisa, a korisnicima omogućuje stvaranje, razmjenu i prikaz elektroničkih dokumenata neovisno o okruženju.

ISO (eng. International Organization for Standardization) je objavila standard ISO 32000-1:2008[170]. ISO propisuje da se elektronički potpis može ugraditi u PDF dokument (u obliku elektroničkog potpisa), u svrhu provjere autentičnosti identiteta autora i potvrde integriteta dokumenta sadržaja. Ovaj format je namijenjen developerima softvera koji izrađuju PDF datoteke, softvera koji učitavaju postojeće PDF datoteke i tumače njihov sadržaj radi prikaza ili interakcije. ISO 32000-1:2008 ne određuje procese za konverziju papira ili elektroničkih dokumenata u PDF format niti fizičke metode spremanja PFD dokumenata. Norma ISO 32000-1:2008 zadovoljava Uredbu eIDAS.

Postoji još jedan standard vezan i za PDF i za napredni elektronički potpis, a to je PAdES (napredni elektronički potpis za PDF). PAdES je razvijen u 2009. od strane ETSI organizacije u suradnji sa stručnjacima za PDF format.

PAdES standard je definiran kroz ETSI tehničku specifikaciju 102 778[171].

Navedena PAdES specifikacija definira 5 dijelova:

- dio 1 - Pregled (engl. Overview) - opće značajke PDF potpisa,
- dio 2 - Osnovni profil (engl. Basic form) - zahtjevi su već navedeni u ISO 32000-1,
- dio 3 – Poboljšani profil (engl. Enhanced) - uključuje ekvivalent za BES i EPES kao što je navedeno u CAdES-u i XAdES-u,
- dio 4 – Dugoročni profil (engl. Long Term) - LVT (eng. Long Term Validation),
- dio 5 – Profil za XML Sadržaj (engl. XML Content) - Profili za XAdES potpis XML sadržaja u PDF datoteci

Šesti dio navedene specifikacije je definiran 2010.[172]:

[170] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (21.08.2017.)
[171] ETSI (2009.), ETSI TS 102 778-1 V1.1.1 (2009-07); Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES; http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf (21.08.2017.)

- dio 6 - Vizualno prikazivanje elektroničkih potpisa (engl. Visual Representations of Electronic Signatures)

Kao i za XAdES tako i za PAdES postoje četiri razine Baseline profila elektroničkih potpisa: B, T, LT i LTA. PAdES Baseline profil je definiran kroz ETSI TS 103 172[173].

PAdES standard je usklađen i s Uredbom eIDAS te je 2016. kao PAdES Baseline standard naveden - ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)[174]. Uredba eIDAS smješta specifikacije za napredni elektronički potpis za PDF pod PAdES format. Dakle, PAdES je elektronički potpis izrađen za PDF napredni elektronički potpis.

Navedeni standard se sastoji od dva dijela:

- dio 1: Gradivni blokovi i PAdES Baseline potpisi (engl. Building blocks and PAdES baseline signatures)
- dio 2: Dodatni PAdES potpisni profili (engl. Additional PAdES signatures profiles)

Turner u svom članku „PAdES and Long Term archival (LTA)"[175] navodi da je LTA razina koja je vrlo slična s prijašnjim profilom nazvanim LTV (engl. Long Term Validation) odgovarajuća za elektronički potpisane dokumente koji su spremljeni na dugi rok. S navedenom LTA razinom tokeni vremenskog žiga su ugrađeni u PAdES potpis koji omogućava u dugom roku integritet i dostupnost za potpisane dokumente. Unutar LTA razine su ugrađene i razine: B, L i LT. Potpisi koji odgovaraju LTA razini moraju imati barem jedan dokument s primijenjenim vremenskim žigom u svom profilu. Prije nego se atribut dokumenta s vremenskim žigom generira i uključi u potpisni profil, svi validacijski materijali koji su potrebni za provjeru potpisa moraju biti uključeni. Ovi materijali

---

[172] ETSI (2010, 2.), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures ETSI TS 102 778-6 V1.1.1 (2010-07) - Technical Specification http://www.etsi.org/deliver/etsi_ts/102700_102799/10277806/01.01.01_60/ts_10277806v010101p.pdf (21.08.2017.)

[173] ETSI (2013., 2.), Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile; ETSI TS 103 172 V2.2.2 (2013-04); http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf (22.08.2017.)

[174] ETSI (2016., 2.), ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES); http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf (21.08.2017.)

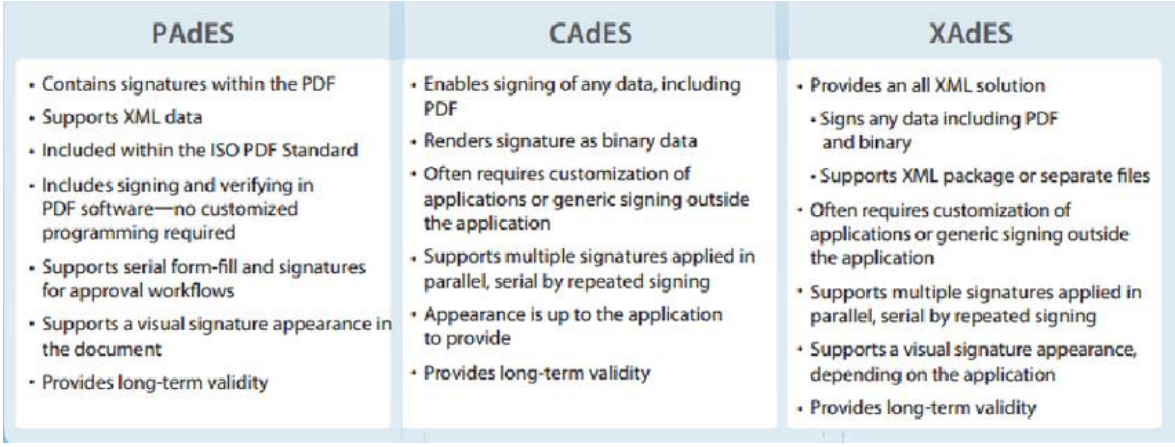
[175] Turner, D. M. (2017.), PAdES and Long Term archival (LTA); https://www.cryptomathic.com/news-events/blog/pades-and-long-term-archival-lta (17.03.2017.)

uključuju sve certifikate i OCSP ili CRL statusne informacije koje se odnose na ove certifikate. Sljedeće informacije je potrebno validirati:

- potpisni certifikat,
- sve atribute certifikata koji se nalaze u potpisu,
- sve potpisne certifikate vremenskih žigova koji su već uključeni u potpisu.

Turner time zaključuje da korištenje PAdES Baseline LTA standarda osigurava valjanost i integritet potpisanog dokumenta kojem će se trebati pristupiti daleko u budućnosti.

Na slici 21 je prikazana usporedba PAdES, CAdES i XAdES formata (iz dokumenta „The AdES family of standards: CAdES, XAdES, and PAdES: Implementation guidance for using electronic signatures in the European Union“).



Slika 21. Usporedba PAdES, CAdES i XAdES formata, preuzeto iz Adobe (2009.)[176]

Slika prikazuje usporedbu značajki tri formata naprednog elektroničkog potpisa. Može se vidjeti da je PAdES format primjenjiv samo na PDF dokumente što je ograničavajuće. S druge strane XAdES i CAdES dopuštaju potpisivanje bilo kojeg tipa podataka pa i PDF datoteka i binarnih podataka.

PAdES ima tu prednost što ne zahtijeva prilagođenu aplikaciju za potpisivanje i verificiranje dokumenata. Sva tri formata osiguravaju LTV. Najprirodnije je odabrati format naprednog elektroničkog potpisa prema formatu dokumenta koji se potpisuje. PDF dokumenti se tako potpisuju s PAdES formatom. XML dokumenti se potpisuju s XAdES

[176] Adobe (2009.), The AdES family of standards: CAdES, XAdES, and PAdES: Implementation guidance for using electronic signatures in the European Union, Adobe Systems Incoporated, https://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf , str. 7, slika 1 (21.08.2017.)

formatom. CAdES format naprednog elektroničkog potpisa se najčešće koristi za potpisivanje dokumenata čija je struktura definirana s ASN.1 sintaksom (kodirani u BER i DER formatu).

Kod usporedbe ova tri standarda bitno je uzeti u obzir broj potpisnika i broj dokumenata koje treba potpisati. Sva tri formata su dobar izbor za potpisivanje jednog dokumenta od strane jednog potpisnika. Što se tiče stavljanja paralelnih potpisa, PAdES standard ne dozvoljava paralelne potpise. Paralelno potpisivanje znači kada jedan potpisnik potpiše dokument pa dokument potpiše drugi potpisnik i.t.d. PAdES dozvoljava serijsko potpisivanje, a to je kada jedan potpisnik potpiše dokument pa drugi potpisnik potpiše i dokument i prvi potpis. XAdES omogućava najveću slobodu oko potpisivanja i omogućava i paralelno i serijsko potpisivanje i to na više dokumenata. CAdES omogućava i serijsko i paralelno potpisivanje, ali ne može potpisati više dokumenata.

4.4 IZRAĐIVANJE NAPREDNOG ELEKTRONIČKOG POTPISA

U ovom potpoglavlju će biti detaljnije objašnjeno sam proces izrade naprednog elektroničkog potpisa. Navedeni opis procesa će se prenijeti iz ETSI norme ETSI EN 319 102-1 čiji je finalni draft donesen u svibnju 2016. godine. Navedena norma je jedna od ekstenzija Uredbe eIDAS te je kao takva vrlo bitna u samom propisivanju detalja samih procesa izrade i validacije naprednih elektroničkih potpisa u smislu olakšanja prekograničnog korištenja elektroničkih potpisanih zapisa (propisano na razini Europske unije).

Kao ilustracija koliko je navedena norma bitna slijedi popis nekoliko nacionalnih normi unutar EU koji su se u svojoj normi ili samo referencirali na ETSI EN 319 102-1 ili su napravili zaseban dokument sa zaglavljem i kopirali izvornu ETSI normu u novi dokument:

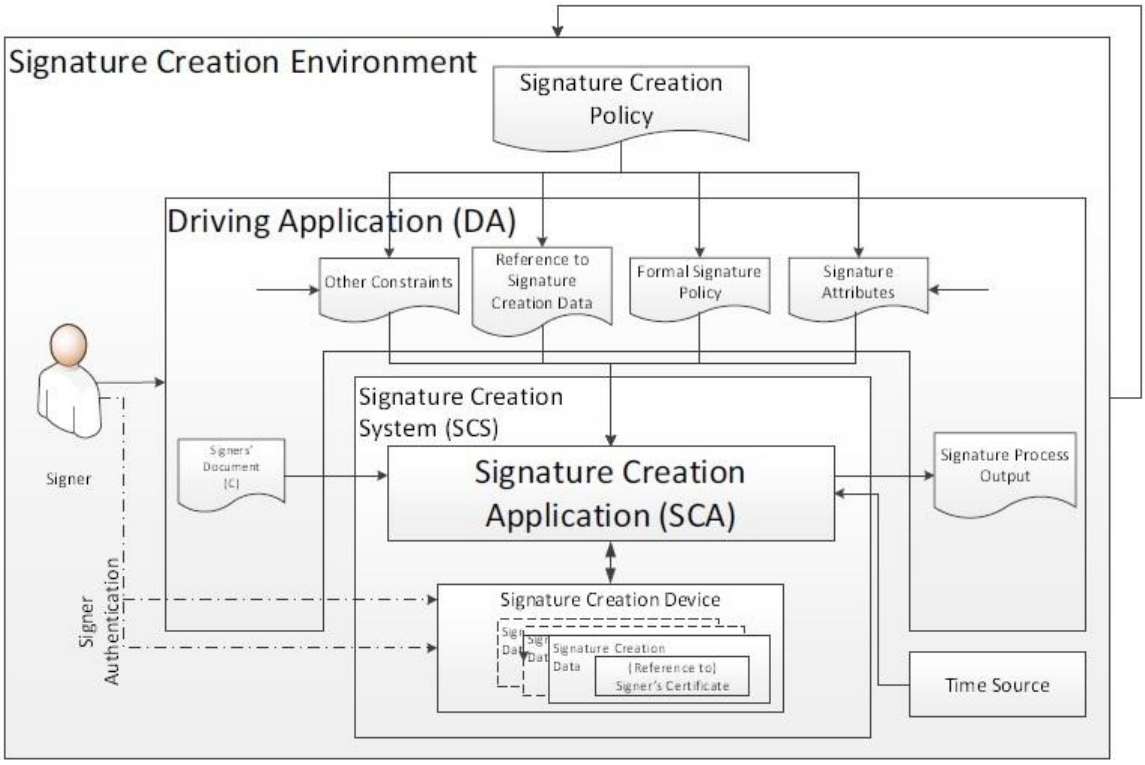
- Hrvatska
    - Samo referenca na ETSI normu[177]
    - Oznaka: HRN EN 319 102-1 V1.1.1:2016
    - Naslov (HR): Elektronički potpisi i infrastrukture (ESI) -- Postupci za kreiranje i vrednovanje AdES elektroničkih potpisa -- 1. dio: Kreiranje i vrednovanje (EN 319 102-1 V1.1.1:2016)

[177] HZN (2016.), HRN EN 319 102-1 V1.1.1:2016, http://31.45.242.218/HZN/Todb.nsf/cd07510acb630f47c1256d2c006ec863/b421b900bcd6bbcbc1257f800030ef69?OpenDocument&AutoFramed (23.08.2017.)

- Austrija
    - Zaseban dokument sa zaglavljem u kojem je kopirana izvorna norma[178]
    - Oznaka: ÖVE/ÖNORM EN 319 102-1 V1.1.1:2016
- Danska
    - Samo referenca na ETSI normu[179]
    - Oznaka: DS/EN 319 102-1 V1.1.1:2016
- Estonija
    - Samo referenca na ETSI normu[180]
    - Oznaka: EVS-EN 319 102-1 V1.1.1:2016
- Litva
    - Samo referenca na ETSI normu[181]
    - Oznaka LST EN 319 132-1 V1.1.1:2016

Slijedi slika i opis funkcionalnog modela za izradu elektroničkog potpisa koju koristi norma ETSI 319 132-1 V1.1.1:2016[182].

[178] Austrian Standards Institute (2016.), ÖVE/ÖNORM EN 319 102-1 V1.1.1 https://shop.austrian-standards.at/Preview.action?preview=&dokkey=577183&selectedLocale=en (23.08.2017.)
[179] Dansk Standard, DS/EN 319 102-1 V1.1.1:2016, https://webshop.ds.dk/en-gb/standard/35-040-character-sets-and-information-coding/ds-en-319-102-1-v1-1-12016 (21.03.2018.)
[180] Eesti Standardikeskus (2016.), EVS-EN 319 102-1 V1.1.1:2016, https://www.evs.ee/tooted/evs-en-319-102-1-v1-1-1-2016 (21.03.2018.)
[181] Lietuvos Standartizacijos Departamentas (2016.), http://lsd.lt/index.php?-1664611101 (23.08.2017.)
[182] ETSI (2016.), Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation ; ETSI EN 319 102-1 V1.1.1 (2016-05); http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf, str. 12 (22.08.2017.)



Slika 22. Funkcionalni model za izradu elektroničkog potpisa, preuzeto iz ETSI (2016.)[183]

Prikazani funkcionalni model ne razlikuje hardverske i softverske implementacije te ne određuje prirodu bilo kojih ulaza/izlaza ili tokova informacija između različitih komponenti.

Okruženje izrade elektroničkog potpisa, SCE (engl. Signature Creation Environment) je sačinjeno od:

- Potpisnika koji želi izraditi elektronički potpis.
- Pokretačke aplikacije, DA (engl. Driving Application) koja predstavlja korisničko okruženje (npr. poslovnu aplikaciju) koju potpisnik koristi za pristupanje funkcionalnostima potpisivanja.
- Sustava za izradu elektroničkog potpisa, SCS (engl. Signature Creation System) koji implementira funkcionalnosti potpisivanja.

Potrebno je napomenuti da za stvaranje elektroničkog potpisa nije uvijek nužno potreban ljudski potpisnik. Ponekad potpisivanje može biti i automatizirani proces implementiran u pokretačkoj aplikaciji (DA).

[183] Isto, str. 12, slika 1

Sustav za izradu elektroničkog potpisa (SCS) se sastoji od:

- Aplikacije za izradu elektroničkog potpisa, SCA (engl. Signature Creation Application (SCA)
- Uređaja za izradu elektroničkog potpisa, SCDev (engl. Signature Creation Device)

Sam postupak potpisivanja se sastoji od sljedećih koraka:

- sustav za izradu elektroničkog potpisa, SCS zaprima dokument koji treba potpisati skupa s drugim potrebnim podacima dobivenim od DA,
- SCS komponira dokument i druge dobivene podatke u Podatke za potpisivanje, DTBS (engl. Data To Be Signed),
- zatim formatira DTBS u Formatirane podatke za potpisivanje, DTBSF (engl. Data To Be Signed (Formatted)),
- SCS izrađuje elektronički potpis oko DTBSF,
- formatira se rezultat u Potpisani podatkovni objekt, SDO (engl. Signed Data Object) u skladu s očekivanim formatom elektroničkog potpisa (npr. CAdES, XAdES ili PAdES). SDO se sastoji od vrijednosti potpisa (engl. Signature Value) i atributa potpisa. SDO može sadržavati i Potpisnikov dokument, SD (engl. Signer's Document) i Prikaz potpisnikovog dokumenta, SDR (engl. Signer's Document Representation) kao i dodatne podržavajuće nepotpisane atribute. Potpisnikov dokument (SD) je dokument na kojem se generira potpis i na koji je povezan. SD je odabran ili sastavljen od strane potpisnika ili DA. U određenim slučajevima tijekom procesa potpisivanja umjesto kompletnog Potpisnikovog dokumenta može biti prikazan Prikaz potpisnikovog dokumenta. Kad god DA ne osigurava SDR, SCA treba izračunati SDR iz SD primjenjujući algoritam određen propisanom politikom stvaranja potpisa (engl. Signature Creation Policy).
- SCS zatim vraća SDO i pokazatelj statusa u DA.

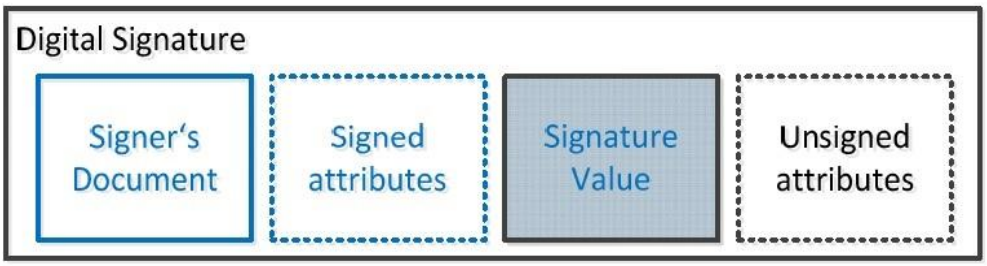
U slučaju greške, SCS treba vratiti dodatne informacije te time omogućiti da DA ili potpisnik propisno postupaju s prijavljenom greškom.

Neke klase naprednih elektroničkih potpisa uključuju i dodatne podatke potrebe za validaciju potpisa. Ovi dodatni podaci se zovu validacijski podaci te su rezultat procesa produženja (engl. augmentation) potpisa. Validacijski podaci trebaju uključivati:

- certifikate javnog ključa, PKCs (engl. Public Key Certificates),
- statusne informacije o opozivu za svaki PKC. Statusne informacije mogu biti Liste opozvanih certifikata, CRL (engl. Certificate Revocation Lists) ili Online statusne informacije certifikata, OCSP (engl. Online certificate status information),
- vremenske tvrdnje (engl. Time-assertions) primijenjene na elektronički potpis.

Validacijski podaci mogu uključivati i druge dodatne podatke koji su nužni ili korisni za validacije. Validacijski podaci mogu biti prikupljeni od strane potpisnika i/ili verifikatora.

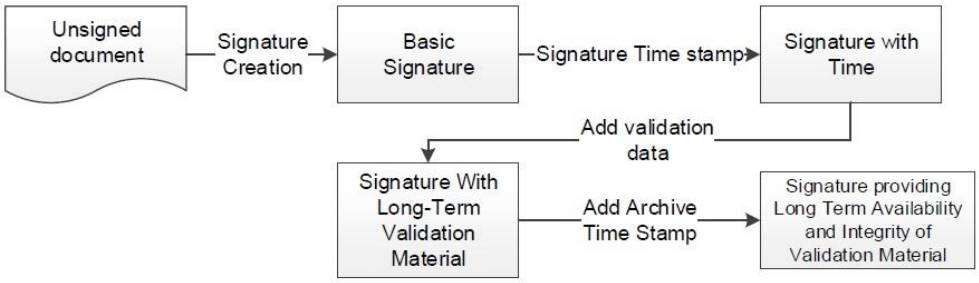
Sljedeća slika iz norme ETSI 319 132-1 V1.1.1:2016 prikazuje osnovnu strukturu elektroničkog potpisa.



Slika 23. Osnovna struktura elektroničkog potpisa, preuzeto iz ETSI (2016.)[184]

Prikazana struktura se sastoji od potpisnikovog dokumenta (engl. Signer's Document) i potpisanih atributa (engl. Signed attributes) te vrijednosti potpisa (engl. Signature value) i nepotpisanih atributa (engl. Unsigned attributes). Potpisnikov dokument i potpisani atributi su uključeni u izračun vrijednosti potpisa.

Slika 24 prikazuje životni ciklus elektroničkog potpisa.



Slika 24. Životni ciklus elektroničkog potpisa, preuzeto iz ETSI (2016.)[185]

[184] Isto, str. 19, slika 3

Koraci u životnom ciklusu elektroničkog potpisa na slici su definirani kao klase potpisa. Proces izrade instance klase potpisa temeljene na potpisu druge klase slijedi ovakav životni ciklus te se zove produženje potpisa (engl. Signature Augmentation), a tim procesom upravlja politika produženja potpisa (engl. Signature augmentation policy). Svaka od prikazanih klasa potpisa odgovara kombinaciji atributa dodanih potpisu s ciljem usavršavanja sposobnosti potvrđivanja potpisa u budućnosti, kada je odgovarajući certifikat potreban za uspješnu provjeru valjanosti možda istekao ili opozvan ili korišteni algoritmi nisu dovoljno jaki da bi bili pouzdani.

U nastavku slijedi opis iz norme ETSI 319 132-1 V1.1.1:2016[186] klasa potpisa:

- **Osnovni elektronički potpis (engl. Basic Signature)** je potpis koji može biti validiran sve dok odgovarajući certifikati nisu istekli ili nisu opozvani.
- **Elektronički potpis s vremenom (engl. Signature with Time)** je potpis koji osigurava da je potpis postojao u danom trenutku. Ovaj potpis se može koristiti za validiranje potpisa kada je certifikat opozvan.
- **Elektronički potpis s dugoročnim potvrdnim materijalom (engl. Signature with Long-Term Validation Material)** je potpis koji osigurava dugoročnu dostupnost validacijskog materijala ugrađujući u potpis materijal ili reference za potvrđivanje potpisa.
- **Elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala (engl. Signature providing Long Term Availability and Integrity of Validation Material)** može pomoći potvrditi potpis povrh mnogih događaja koji ograničavaju njegovu valjanost, npr. slabosti korištenih kriptografskih algoritama ili isteka potvrdnih podataka.

Osnovni elektronički potpis se izrađuje za potrebe sprječavanje jednostavnih zamjena, napada te za određivanje certifikata koji će se koristiti za potvrdu potpisa. Rezultat procesa izrade osnovnog elektroničkog potpisa je potpisani podatkovni objekt, tj. SDO (engl. Signed Data Object) koji sadrži:

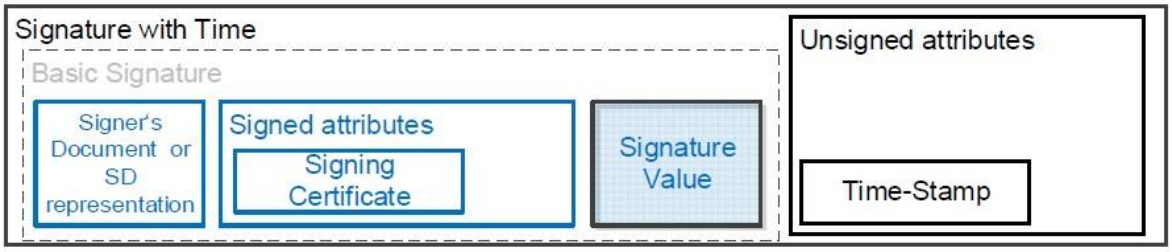
- vrijednost potpisa (engl. Signature Value),
- referencu na potpisni certifikat ili kopiju potpisnog certifikata kao potpisani atribut,
- opcionalne potpisane ili nepotpisane atribute (npr. identifikator politike potpisa)

[185] Isto, str. 19, slika 4
[186] Isto, str. 19

Slika 25 prikazuje strukturu osnovnog elektroničkog potpisa.

Slika 25. Struktura osnovnog elektroničkog potpisa, preuzeto iz ETSI (2016.)[187]

Proces izrade elektroničkog potpisa s vremenom kao rezultat vraća potpis koji uključuje osnovni elektronički potpis s dodanim nepotpisanim atributima uključujući i vremenski žig potpisa. Slika 26 prikazuje strukturu elektroničkog potpisa s vremenom te opis procesa stvaranja.



Slika 26. Elektronički potpis s vremenom, preuzeto iz ETSI (2016.)[188]

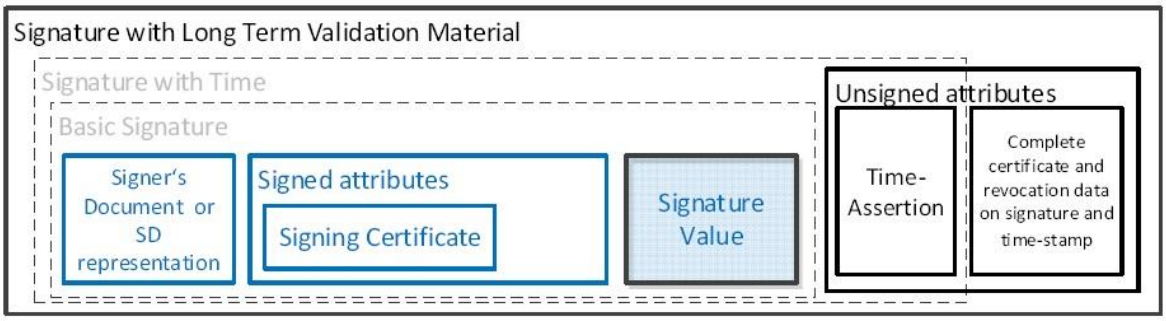
Proces produženja potpisa (engl. Signature augmentation) u ovom slučaju teče na sljedeći način:

1. zahtijeva se jedan ili više vremenskih žigova dobivenih od odgovarajućih TSA kako je definirano u politici potpisa ili u lokalnoj konfiguraciji,
2. izrađuje se potpisni atribut koji uključuje dobiveni vremenski žig,
3. dodaje se izrađeni potpisni atribut kao nepotpisani u SDO.

Vremenski žig osigurava početni korak prema osiguravanju dugoročne valjanosti. Vremenski žig treba izraditi prije nego se certifikat opozove ili istekne. U slučaju da se to ne može postići, validacija izrađenog potpisa može pasti.

[187] Isto, str. 20, slika 6
[188] Isto, str. 23, slika 7

Slika 27 prikazuje strukturu elektroničkog potpisa s dugoročnim potvrdnim materijalom te opis samog procesa stvaranja.



Slika 27. Elektronički potpis s dugoročnim potvrdnim materijalom, preuzeto iz ETSI (2016.)[189]

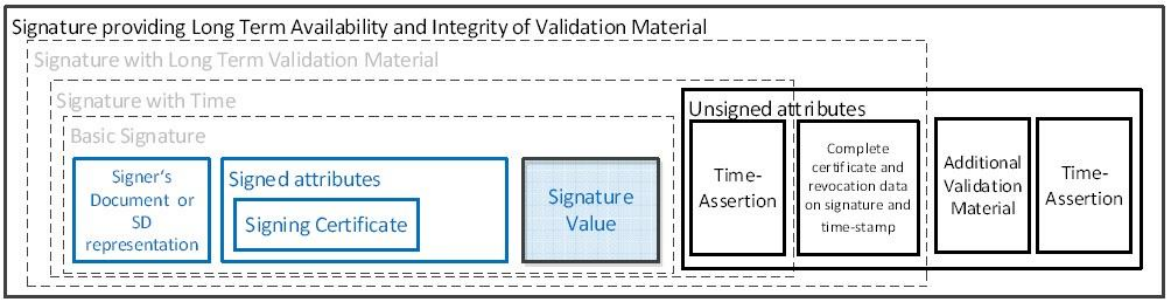
Kod procesa stvaranja ovog potpisa je bitno napomenuti da validacijski algoritam za potpis može procijeniti njegovu valjanost samo dok su podaci potrebni za potvrdu još uvijek dostupni verifikatorima na mreži. U slučaju kad je nesigurno da će potvrdni podatak biti dostupan na mreži verifikatorima ili neki verifikatori ne mogu pristupiti podacima, tada je nužno ugraditi takve podatke u sam potpis. Elektronički potpis s dugoročnim potvrdnim materijalom uključuje potvrdne podatke nužne za provjeru potpisa i nakon isteka valjanosti potvrde za potpis. Navedeno je posebno bitno zbog utvrđivanja statusa opoziva svih certifikata krajnjeg entiteta uključenih u potpis (potpisni certifikat, certifikati vremenskih žigova, certifikati atributa i dr.).

Sam proces izrade elektroničkog potpisa s dugoročnim potvrdnim materijalom će kao rezultat vratiti status potvrđivanja potpisa zajedno s izrađenim potpisom. Kada se dodaje atribut koji sadrži dugoročni potvrdni materijal, proces produženja (engl. augmentation) potpisa teče na sljedeći način:

1. validiranje elektroničkog potpisa s vremenom u svom sadašnjem stanju,
2. dodavanje potpisu svih materijala i referenci koji su korištene tijekom validacije i koji još nisu prisutni u potpisu,
3. vraćanje produženog (engl. augmentated) potpisa s informacijom o validaciji statusa i izvješću o validaciji osiguranim od aplikacije za validaciju potpisa, SVA (engl. Signature Validation Application).

[189] Isto, str. 24, slika 8

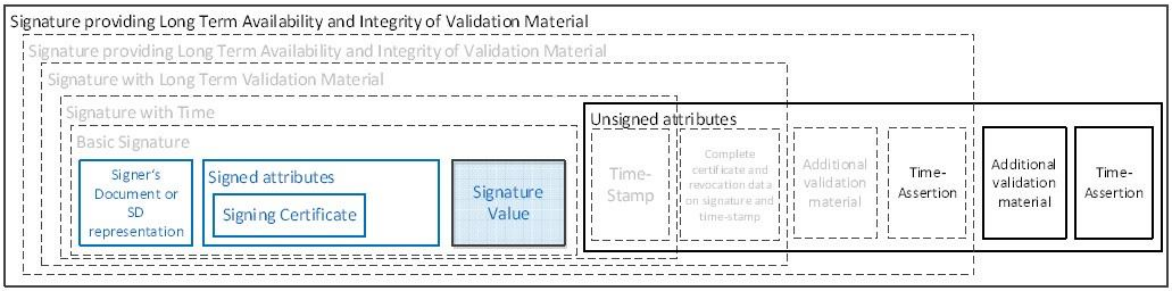
Na koncu slijedi slika 28 koja prikazuje strukturu elektroničkog potpisa koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala te opis samog procesa stvaranja.



Slika 28. Elektronički potpis koji osigurava dugoročnu dostupnost i integritet validacijskog materijala, preuzeto iz ETSI (2016.)[190]

Algoritmi, ključevi i drugi kriptografski podaci koji su korišteni u trenutku potpisivanja s vremenom postaju sve slabiji. Kriptografske funkcije korištene u potpisivanju s vremenom postaju sve ranjivije. Certifikati koji potvrđuju postojeće vremenske tvrdnje (engl. Time-Assertions) mogu isteći ili mogu biti opozvani. Iz navedenih razloga je potrebno potpisnikov dokument, elektronički potpis kao i sve atribute sadržane u elektroničkom potpisu s dugoročnim potvrdnim materijalom zaštititi primjenom jednog ili više vremenskih tvrdnji. Vremenske tvrdnje vezuju podatke za određeno vrijeme dokazujući time da su tadašnji podaci postojali u točno određeno vrijeme. Dodatne vremenske tvrdnje se dodaju u elektronički potpis ili nepotpisane atribute da bi se osigurala dugoročna dostupnost i integritet potvrdnog materijala. Takvi atributi se zovu i atributima za dugoročna dostupnost i integritet potvrdnog materijala. Sama izrada vremenskih tvrdnji se treba ponoviti prije nego što zaštita učinjena prethodnom vremenskom tvrdnjom postane slaba. To znači da bi se kod izrade nove vremenske tvrdnje trebalo koristiti jačim kriptografskim algoritmima i većom dužinom ključeva u odnosu na prethodne vremenske tvrdnje. U slučaju da se proces dodavanja vremenskih tvrdnji ponavlja, u elektroničkom potpisu se može pojaviti više instanci vremenskih tvrdnji. Na slici 29 je prikazan elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala s ugrađene dvije vremenske tvrdnje.

[190] Isto, str. 25, slika 9

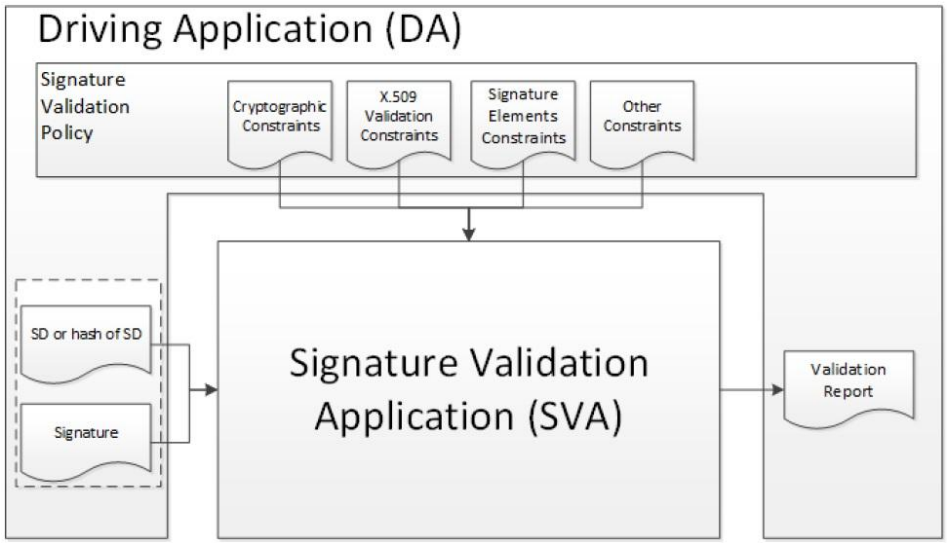


Slika 29. Elektronički potpis koji osigurava dugoročnu dostupnost i integritet validacijskog materijala nakon ponavljanja, preuzeto iz ETSI (2016.)[191]

4.5 VALIDACIJA NAPREDNOG ELEKTRONIČKOG POTPISA

U ovom potpoglavlju će biti detaljnije objašnjeno sam proces validacije naprednog elektroničkog potpisa. Kao što je bio slučaj oko izrade potpisa u prethodnom poglavlju „Izrađivanje naprednog elektroničkog potpisa“, opis procesa validacije će se prenijeti iz ETSI norme ETSI EN 319 102-1 čiji je finalni draft donesen u svibnju 2016. godine.

Navedena ETSI norma predstavlja i konceptualni model validacije naprednog elektroničkog potpisa na slici 30.



Slika 30. Konceptualni model validacije naprednog elektroničkog potpisa, preuzeto iz ETSI (2016.)[192]

[191] Isto, str. 25, slika 10

ETSI norma ETSI EN 319 102-1 nadalje objašnjava sam postupak validacije[193]. U navedenom modelu se softver dijeli po funkcijama validacije potpisa u dva dijela:

- Aplikacija za validaciju potpisa, SVA (engl. Signature Validation Application) i
- Pokretačke aplikacije, DA (engl. Driving Application).

Aplikacija za validaciju potpisa zaprima AdES elektronički potpis te druge ulazne podatke od pokretačke aplikacije. SVA aplikacija validira elektronički potpis sukladno politici validacije potpisa te skupu validacijskih pravila te kao rezultat postupka validacije daje status provjere i izvješće o validaciji. Izvješće o validaciji osigurava detalje tehničke validacije svakog pravila koji može biti bitan za DA aplikaciju u interpretaciji rezultata. Sve dok DA ne zatraži od SVA obavljanje procesa validacije, validacija starta s validacijskim procesom za elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala. Jedan od prvih koraka ovog procesa validacije je pozivanje procesa validacije elektroničkog potpisa s vremenom te pozivanje procesa validacije elektroničkog potpisa s dugoročnim potvrdnim materijalom. Navedeni procesi validacije potom pozivaju proces za validaciju osnovnog elektroničkog potpisa. Ovakva validacija slijedi životni ciklus elektroničkog potpisa sa slike 24 iz ovog rada (slika životnog ciklusa elektroničkog potpisa) i provjerava status elektroničkog potpisa temeljenog na validacijskom procesu za prvu klasu elektroničkog potpisa, tj. osnovnom elektroničkom potpisu. U slučaju da ovaj postupak dovede do konačnog pozitivnog ili negativnog rezultata validacije, validacija se zaustavlja. U slučaju da validacijski proces za osnovni elektronički potpis ne dovede do konačnog zaključka, validacija nastavlja s validacijskim procesima za uvećavajuće potpisne klase. To su: elektronički potpis s vremenom, elektronički potpis s dugoročnim potvrdnim materijalom te elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala. Validacija se nastavlja sa sljedećom klasom do konačnog zaključka ili do nedostupnosti procesa validacije za sljedeću uvećanu klasu. Tijekom procesa validacije primjenjuje se nekoliko validacijskih blokova: format elektroničkog potpisa, ispravnost potpisnog certifikata, kriptografska validacija i dr. Status validacije iz validacijskog bloka može biti jedan od sljedećih:

- Uspješan na validaciji (engl. PASSED),
- Neuspješan na validaciji (engl. FAILED),
- Neodređen (engl. INDETERMINATE).

Status cjelokupne validacije jedne potpisne klase može imati sljedeće značenje:

---

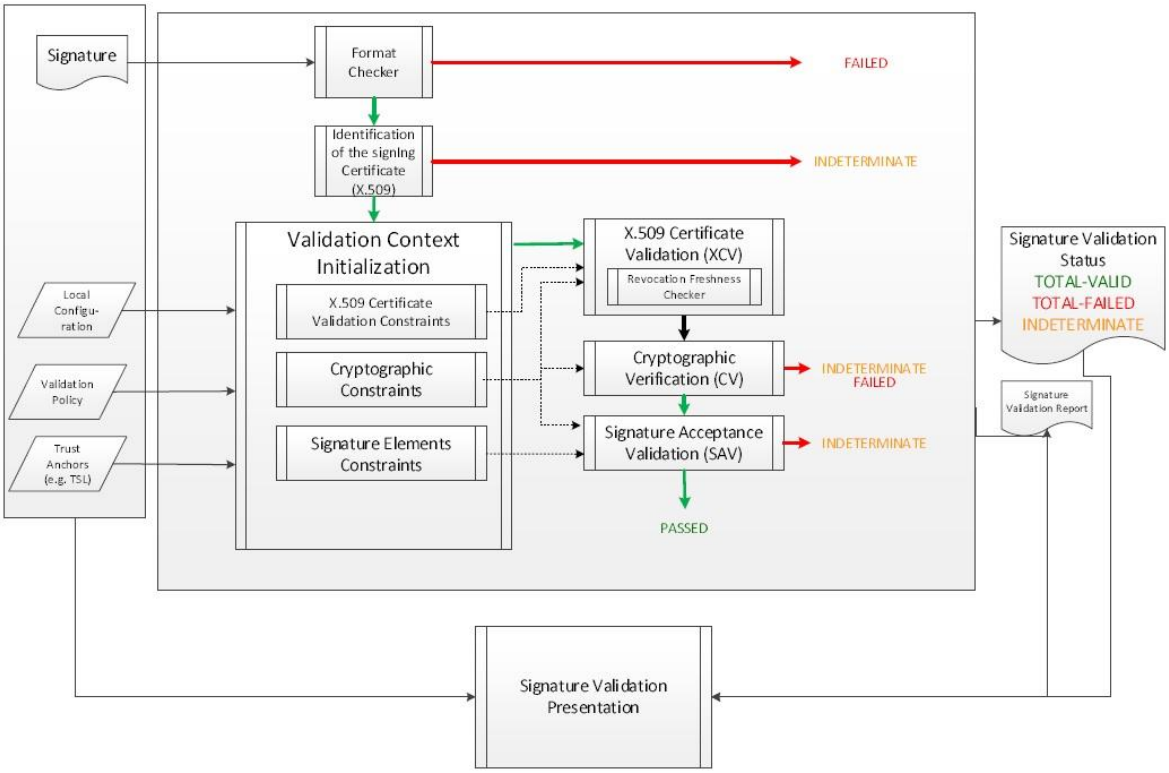
[192] Isto, str. 28, slika 11
[193] Isto, str. 27

- U potpunosti uspješan na validaciji (engl. TOTAL-PASSED) – kada je kriptografska provjera potpisa uspješna. Kriptografska provjera uključuje i provjeru hash vrijednosti zasebnih podatkovnih objekata koji su potpisani indirektno.
- U potpunosti neuspješan na validaciji (engl. TOTAL-FAILED) – kada je kriptografska provjera potpisa neuspješna ili je dokazano da je izrada potpisa učinjena nakon opoziva potpisnog certifikata. Status cjelokupne validacije može biti ovakav i kada potpis nije sukladan nekom od osnovnih standarda pa ga validacijski blokovi ne mogu niti obraditi.
- Neodređen (engl. INDETERMINATE) – rezultati obavljenih provjera ne omogućavaju zaključivanje je li status potpisa TOTAL-PASSED ili TOTAL-FAILED.

Izlazni rezultat SVA aplikacije treba biti obrađen od strane DA aplikacije da bi mogao biti predstavljen verifikatoru elektroničkog potpisa i za druge svrhe. Postoje različiti načini implementacije procedura za validaciju potpisa:
- aplikacija (ili dio aplikacije) na uređajima kao što je PC s korisničkim sučeljem,
- web servis,
- web aplikacija,
- command-line alat,
- programske biblioteke koje se mogu ugraditi u druge aplikacije.

SVA aplikacija prilikom podržavanja validacije za elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala mora podržati i validacije drugih potpisnih klasa: elektroničkog potpisa s dugoročnim potvrdnim materijalom, elektroničkog potpisa s vremenom i osnovnog elektroničkog potpisa.

ETSI norma ETSI EN 319 102-1 navodi i shemu validacije osnovnog elektroničkog potpisa (na slici 31). Ova shema je bitna zato što u pojednostavljenom obliku prezentira osnovne gradivne blokove koji se koriste za izradu algoritama za validacije različitih potpisnih klasa.



Slika 31. Validacija osnovnog elektroničkog potpisa, preuzeto iz ETSI (2016.)[194]

Slijedi kratak opis funkcionalnosti gradivnih blokova koji su potrebni za validaciju elektroničkog potpisa kako su navedeni u ETSI normi ETSI EN 319 102-1[195].

Provjera formata (engl. Format Checker) provjerava odgovara li potpis koji se provjerava, barem primjenjivom osnovnom formatu u smislu omogućavanja obrade njegovog unutarnjeg sadržaja kriptografskim verifikacijskim blokom. Ova provjera još ne uključuje provjeru sukladnosti s određenim profilom potpisa ili sa specifičnim stupnjem potpisa kao što je npr. PAdES-B-LTA.

Identifikacija potpisnog certifikata (engl. Identification on the signing certificate) je blok odgovoran za identificiranje potpisnog certifikata koji će biti korišten za validaciju potpisa.

Inicijalizacija konteksta validacije (engl. Validation context initialization) je gradivni blok koji inicijalizira validacijska pravila (X.509 validacijska pravila, kriptografska pravila, pravila za potpisne elemente) i parametre koji će biti korišteni za validaciju potpisa.

[194] Isto, str. 37, slika 12
[195] Isto, str. 37

Provjera informacija o opozivu (engl. Revocation freshness checker) – ovaj gradivni blok provjerava je li postojeća informacija o opozivu dovoljno „svježa“ u dano validacijsko vrijeme. Traženo vrijeme svježine informacije o opozivu je definirano kao maksimalna prihvaćena razlika između validacijskog vremena te vremena izdavanja informacije o opozivu. Funkciju ovog gradivnog bloka koriste drugi validacijski blokovi kada provjeravaju status opoziva certifikata. Ova provjera je bitna kada se provjerava osnovni potpis bez pouzdane vremenske tvrdnje, a vrijeme koje postoji nije dovoljno pouzdano. U ovakvim slučajevima potpis se može izraditi netom prije provjere potpisa, ali točno vrijeme tada nije poznato. Ako je informacija o opozivu prestara tada certifikat može biti opozvan prije izrade potpisa što onda nije naznačeno u podacima o opozivu.

Validacija X.509 certifikata (engl. X.509 certificate validation) je gradivni blok koji provjerava potpisni certifikat u validacijsko vrijeme. Ako validacijsko vrijeme nije previđeno kao ulaz, validacija će biti izvedena s trenutnim vremenom.

Kriptografska verifikacija (engl. Cryptographic verification) je gradivni blok koji provjerava integritet potpisanih podataka obavljanjem kriptografskih provjera. U većini slučajeva kriptografska verifikacija zahtijeva samo potpisni certifikat, a ne cijeli validirani lanac.

Validacija prihvaćanja potpisa, SAV (engl. Signature Acceptance Validation) je gradivni blok koji pokriva dodatnu verifikaciju koja se izvodi na samom potpisu ili na atributima potpisa. Ovaj proces može uključivati i ostale provjere određene politikom provjere valjanosti potpisa. Provjere koje nisu na popisu unutar politike provjere valjanosti potpisa nisu obavezne za implementaciju unutar ovog bloka.

Gradivni blok za prezentaciju validacije potpisa (engl. Signature validation presentation building block) je opcionalan gradivni blok u procesu validacije potpisa. Verifikator može koristiti ovaj gradivni blok za provjeru rezultata procesa validacije potpisa. Kada se koristi u procesu validacije potpisa, ovaj gradivni blok će korisniku prezentirati sljedeće:

- podatke koji su obuhvaćeni potpisom,
- podatke koji identificiraju potpisnika,
- datum i vrijeme u kojem je određen status validacije,
- sve atributa potpisa koji su uključeni u potpis te prikazivanje informacije koji su atributi potpisani a koji nisu,
- informacije o korištenoj politici validacije potpisa,
- konačni status validacije potpisa (TOTAL-PASSED, TOTAL-FAILED ili

INDETERMINATE),

- u slučaju statusa TOTAL-FAILED, prikazuje se razlog zbog kojeg je potpis proglašen neispravnim,
- u slučaju statusa INDETERMINATE se posebno označava dio validacijskog izvješća koji preporuča korake koje treba poduzeti da bi se eventualno došlo do konačne odluke o statusu validacije,
- validacijsko izvješće.

Lipp u svojem članku „Signature Validation – a Dark Art“[196] na konferenciji Information Security Solutions Europe 2015 Conference daje kritički osvrt na proces validacije elektroničkog potpisa kako ga propisuje ETSI Standard EN 319 102-1. Navodi da navedena norma pokriva izradu i validaciju elektroničkog potpisa, ali i da su neki eksperti koji su do sada bili uvjereni da su razumjeli što treba učiniti kada se validira potpis ostali zbunjeni. Lipp navodi da ETSI Standard EN 319 102-1 specificira procedure za izradu naprednog elektroničkog potpisa te za provjeru kada je napredni elektronički potpis tehnološki valjan.

Navodi, nadalje, da Uredba (EU) br. 910/2014[197] (Uredba eIDAS) u članku 26. određuje uvjete za validaciju kvalificiranog elektroničkog potpisa:

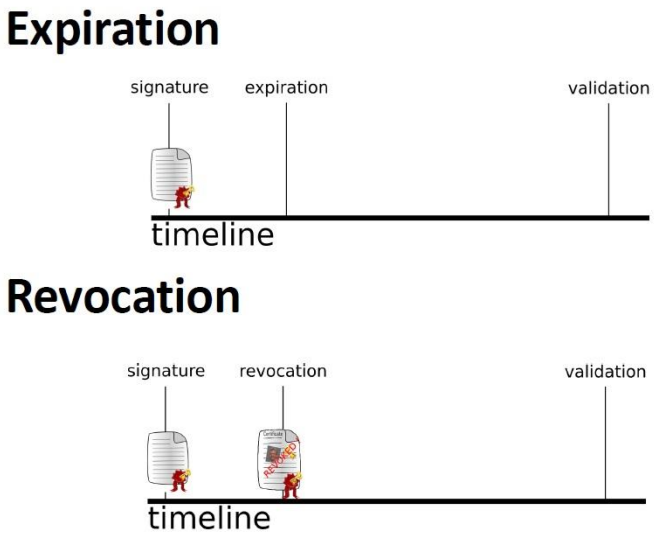
- certifikat ili kvalificirani certifikat je valjan u trenutku potpisivanja,
- ne navodi se ništa oko statusa nije istekao (engl. not expired) ili nije opozvan kasnije (engl. not revoked later),
- certifikat treba biti valjan samo u trenutku potpisivanja.

Lipp je navedeno izložio kroz prezentaciju na Information Security Solutions Europe konferenciji u Berlinu 2015. U navedenoj prezentaciji je dao sljedeći prikaz događaja isteka certifikata (engl. Expiration) i opoziva (engl. Revocation)[198].

[196] Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

[197] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[198] Lipp, P. (2015., 2.), Signature Validation - a black art? TU Graz, prezentacija s konferencije Information Security Solutions Europe konferencije, Berlin, https://www.eema.org/wp-content/uploads/lipp.pdf , str. 12.-13, (25.12.2017.)



Slika 32. Istek i opoziv certifikata, preuzeto iz Lipp, P. (2015., 2.)[199]

Moguć je sljedeći odnos valjanosti certifikata i valjanosti elektroničkog potpisa po Uredbi eDAS kako je navedeno u tablici 4.

Tablica 4. Mogući odnos valjanosti certifikata i valjanosti elektroničkog potpisa po Uredbi eIDAS, preuzeto iz Lipp, P. (2015., 2.)[200]

	eIDAS	X.509
Istek certifikata	valjan potpis	istekao
Opoziv	valjan potpis	opozvan

Dakle, prethodnom tablicom je prikazana mogućnost da Uredba eIDAS pokriva i slučajeve kada je certifikat istekao ili je opozvan, a potpis učinjen takvim certifikatom se proglašava valjanim.

Ovakve situacije su moguće kada je elektronički potpis izrađen u vrijeme prije:

- opoziva certifikata,
- isteka certifikata,
- nego što su korišteni kriptografski algoritmi postali slabi,
- nego što je dužina ključeva postala premala.

Elektronički potpis sadrži vrijeme izrade te je potrebno poznavati status certifikata u vrijeme potpisivanja. Dakle, potrebno je osigurati vrijeme potpisa, tj. vremenske tvrdnje

[199] Isto, str. 12
[200] Isto, str. 13

(engl. Time-assertions). Navedeno se osigurava s vremenskim žigom unutar potpisa (engl. signature time-stamp) koji jamči da je potpis postojao u vrijeme vremenskog žiga. U ovom slučaju navedeno možemo nazvati i **dokaz postojanja, PoE (engl. Proof of Existence)**. Lipp nadalje objašnjava da ETSI norma ETSI EN 319 102-1 utvrđuje mogućnost da validacijski algoritmi odrađuju validacije u dugom roku kada postoje vremenski žigovi. Da bi se to odradilo potrebno je validirati vremenske žigove (potencijalno koristeći validacijske blokove za potpise iz prošlosti ako je potrebno). Osim toga potrebno je obaviti izvlačenje (engl. extract) svih objekata zaštićenih vremenskim žigom koristeći informaciju od blokova za potpise iz prošlosti (engl. past-signature-validation building block) koji će za to iskoristiti sve PoE-ove izvučene u prethodnom koraku.

Nadalje, potrebno je voditi računa da vremenski žig sadrži elektronički potpis. Za taj elektronički potpis je potreban certifikat i validacija potpis. Tu se isto može dogoditi istek certifikata ili njegov opoziv. Proces se dalje odvija rekurzivno. Isto načelo rekurzije vrijedi za certifikate CRL lista i OCSP servisa. Oni isto mogu isteći i biti opozvani.

Lipp zaključno u svom članku daje preporuke izbjegavanja potrebe za dugoročnom validacijom potpisa. U slučaju kada je dugoročna validacija potpisa nužna, predlaže validiranje potpisa neposredno nakon izrade te njihovo sigurno arhiviranje zajedno s validacijskim rezultatom, validacijskim izvješćem i materijalom korištenim za validiranje.

4.6 ZAKLJUČAK

U ovom poglavlju je posebna pažnja dana proučavanju zakonske podloge u EU i Hrvatskoj što se tiče naprednog elektroničkog potpisa. Dvije su EU Uredbe posebno bitne za razumijevanje ove tematike. Krajem 1999. je donesena Direktiva o elektroničkom potpisu 1999/93/EC kojom se u Europskoj uniji namjeravalo stvoriti jedinstveni zakonodavni okvir za primjenu elektroničkoga potpisa na području svih zemalja članica. Nadalje, u srpnju 2014. je na razini EU donesena Uredba eIDAS (910/2014) kojoj je puni naziv Uredba o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ. Uredba eIDAS strogo razdvaja namjene elektroničkog potpisa i elektroničkog pečata. Potpisnik se u Uredbi definira kao fizička osoba koja izrađuje elektronički potpis. S druge strane autor elektroničkog pečata može biti samo pravna osoba, a elektronički pečat služi za osiguravanje izvornosti i cjelovitosti podataka. Ova uredba je pojednostavila primjenu kvalificiranog elektroničkog potpisa kao naprednog elektroničkog potpisa uz određene

uvjete. Svaki kvalificirani elektronički potpis je ujedno i napredan elektronički potpis, ali svaki napredni elektronički potpis ne mora biti kvalificirani elektronički potpis. Uredba eIDAS definira da kvalificirani elektronički potpis ima jednak pravni učinak kao vlastoručni potpis.

Elektronički potpisi se mogu izrađivati prema različitim formatima. U ovom poglavlju su obrađeni sljedeći standardi: CMS (PKCS#7), XMLDSig, CAdES, XAdES i PAdES. Zadnja tri formata su napredni elektronički potpisi koji su sukladni s Uredbom eIDAS te su iz navedenog razlog detaljnije obrađeni. CMS je široko korišten standard definiran od strane IETF organizacije za kriptografski zaštićene poruke. CMS ima sintaksu omotnice za zaštitu podataka i može biti korištena za elektronički potpis, autenticiranje ili kriptiranje bilo koje forme digitalnih podataka. XML potpis definira XML sintaksu za elektroničke potpise. Što se tiče pitanja koji format dokumenta potpisati s kojim naprednim elektroničkim potpisom odgovor je da je najbolje odabrati format naprednog elektroničkog potpisa prema formatu dokumenta koji se potpisuje. PDF dokumente je najbolje potpisivati s PAdES formatom naprednog elektroničkog potpisa, XML dokumente s XAdES formatom, a CAdES format se najčešće koristi za potpisivanje dokumenata čija je struktura definirana s ASN.1 sintaksom (to su dokumenti kodirani u BER i DER formatu). PAdES ima tu prednost što ne zahtijeva prilagođenu aplikaciju za potpisivanje i verificiranje dokumenata. XAdES, CAdES i PAdES osiguravaju LTV (engl. Long Term Validation). XAdES format naprednog elektroničkog potpisa omogućava najveću slobodu oko potpisivanja i omogućava i paralelno i serijsko potpisivanje i to na više dokumenata.

Turner u svom članku „PAdES and Long Term archival (LTA)“ navodi[201] da je LTA (engl. Long Term Archival) razina odgovarajuća za elektronički potpisane dokumente koji su spremljeni na dugi rok. Navodi i da se tokeni vremenskog žiga s navedenom LTA razinom mogu ugraditi u PAdES potpis te se na taj način omogućava u dugom roku integritet i dostupnost za potpisane dokumente.

U ETSI normi EN 319 102-1 je detaljnije objašnjen sam proces izrade naprednog elektroničkog potpisa. Sama norma propisuje detalje samih procesa izrade i validacije naprednih elektroničkih potpisa u smislu olakšanja prekograničnog korištenja elektroničkih

[201] Turner, D. M. (2017.), PAdES and Long Term archival (LTA); https://www.cryptomathic.com/news-events/blog/pades-and-long-term-archival-lta (17.03.2017.)

potpisanih zapisa što je propisano na razini Europske unije. Tako su definirane četiri klase potpisa: osnovni elektronički potpis, elektronički potpis s vremenom, elektronički potpis s dugoročnim potvrdnim materijalom i elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala. Detaljno je opisan i proces validacije naprednog elektroničkog potpisa uz navođenje sheme validacije osnovnog elektroničkog potpisa te gradivnih blokova sheme. Statusi koje sam validacijski proces može generirati su: TOTAL-PASSED, TOTAL-FAILED i INDETERMINATE.

Lipp je u svojem članku „Signature Validation – a Dark Art“ [202] na Information Security Solutions Europe konferenciji u Berlinu 2015 dao kritički osvrt na sam proces validacije naveden u ETSI EN 319 102-1. Objašnjava da je norma u pogledu validacije zbunila i neke eksperte zbog slučajeva kada elektronički potpis vrijedi, a certifikat kojim je potpis učinjen je istekao ili je opozvan. U članku pojašnjava da ETSI norma ETSI EN 319 102-1 utvrđuje mogućnost da validacijski algoritmi odrađuju validaciju potpisa u dugom roku kada postoji vremenski žig koji jamči da je potpis postojao u vrijeme vremenskog žiga. Radi se o dokazu postojanja, tj. PoE (engl. Proof of Existence). Lipp zaključno u svom članku daje preporuke izbjegavanja potrebe za dugoročnom validacijom potpisa zbog rekurzivne potrebe validacije potpisa (timestamp, CRL i OCSP,...). U slučaju kada je dugoročna validacija potpisa nužna, Lipp predlaže validiranje potpisa neposredno nakon izrade te njihovo sigurno arhiviranje zajedno s validacijskim rezultatom, validacijskim izvješćem i materijalom korištenim za validiranje.

[202] Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

5. DUGOROČNO OČUVANJE INTEGRITETA I AUTENTIČNOSTI ELEKTRONIČKIH ZAPISA S ELEKTRONIČKIM POTPISIMA

Za proučavanje područja dugoročnog očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima posebno je bitan rad autora Jean-François Blanchette-a „The digital signature dilemma“[203] iz 2006. godine. U navedenom se radu tvrdi da su razlike između tehničkih, pravnih i arhivskih odgovora na problem dugoročnog očuvanja elektronički potpisanih dokumenata utemeljena na divergentnim shvaćanjima elektroničke autentičnosti (fizičko nasuprot kontekstualnog). Blanchette navodi temeljnu dilemu s kojom se suočavaju arhivisti tražeći očuvanje čitljivosti potpisanih dokumenta i njihovih kriptografskih potpisa nakon dužeg roka[204]. U nastavku Blanchette navodi saznanja iz više zemalja koja su nastala na navedenoj dilemi (SAD, Australija i Kanada). Za ovaj rad su posebno bitna saznanja iz Kanade kako ih je opisao autor[205]. Naime, 1999. godine su kanadske vlasti najavile ambiciozne planove o stavljanju svih federalnih vladinih servisa online do 2005. godine, a kao ključni element za stvaranje navedenih planova je bila uspostava infrastrukture javnog ključa kanadske vlade. Knjižnica i arhiv Kanade[206] je bila jedan od nositelja tih planova. Sa stanovišta arhivista[207], bez obzira na sigurnosnu ulogu, elektronički potpisi nakon njihovog prijenosa u arhiv imaju manju funkciju. Naime, tada je kanadski nacionalni arhiv bio stava da neće pokušati zadržati sposobnost ponovnog potvrđivanja elektroničkog potpisa nakon prijenosa elektronički potpisanih dokumenata pod njegovu kontrolu, niti će sačuvati tragove elektroničkog potpisa koji se generiraju u federalnom PKI sustavu.

Dakle, sa stajališta arhivskih institucija suočenih s potrebom da se razviju pravila vezana uz očuvanje elektronički potpisanih dokumenata pojavila su se tri moguća rješenja[208]:

1. Očuvanje elektroničkih potpisa (engl. Preservation of the digital signatures): Ovo rješenje pretpostavlja zahtjevnu implementaciju za potrebne mehanizme za očuvanje i validiranje elektroničkih potpisa što ne adresira istodobnu potrebu za očuvanjem razumljivosti dokumenata,

[203] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 1 (06.02.2018.)
[204] Isto, str. 8
[205] Isto, str. 13
[206] Library and Archives Canada, http://www.bac-lac.gc.ca/eng/Pages/home.aspx (06.02.2018.)
[207] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 14 (06.02.2018.)
[208] Isto, str. 14

2. Uklanjanje elektroničkih potpisa (engl. Elimination of the signatures): Ovo rješenje zahtijeva najmanje prilagodbe u arhivskim institucijama, ali osiromašuje opis dokumenta jer eliminira potpis kao jedan tehnički element koji se koristi za osiguranje autentičnosti dokumenata,
3. Bilježenje traga o elektroničkim potpisima u metapodacima (engl . Recording the trace of the signatures as metadata): Ovo rješenje zahtijeva malo tehničkih sredstava i za bilježenje potpisa i za bilježenje rezultata provjere. Međutim, na ovaj način elektronički potpisi gube svoj poseban status kao primarni oblik dokaza iz kojeg se može zaključiti o autentičnosti elektronički potpisanog dokumenta.

Iako je prvo predloženo rješenje (očuvanje elektroničkih potpisa) često implicitno definirano u zakonskim propisima, Blanchette zaključuje da je zadnje rješenje (bilježenje traga o elektroničkim potpisima u metapodacima) u najvećoj mjeri komforno s arhivskom praksom i teorijom. Osim toga, Blanchette upućuje i na rezultate InterPARES[209] projekta koji ukazuju da su integritet, sigurnost i trajna dostupnost ključni rezultati arhivske evidencije te da se to prvenstveno osigurava proceduralnim i deskriptivnim metapodacima. Što se tiče bilježenja traga o elektroničkim potpisima u metapodacima Blanchette nastavlja[210] „Arhivski metapodaci moraju podržati kontinuiranu autentičnost zapisa opisujući zapise kako su primljeni od stvaratelja zapisa, a uz to se mora dokumentirati cijeli proces očuvanja“.

Najviše sam ipak pažnje posvetio prvom predloženom rješenju, tj. očuvanju elektroničkih potpisa. Razlog je evidentan napredak u korištenju infrastrukture javnog ključa od vremena pisanja članka „The digital signature dilemma“. Osim toga, samo zakonodavstvo Europske Unije je kroz Uredbu eIDAS[211] otvorilo prostor industriji i javnoj upravi za napredak u izradi servisa javne uprave te općenito elektroničkih servisa iz razloga podizanja konkurentnosti EU gospodarstva. Navedeni elektronički servisi se, međuostalim, temelje i na PKI tehnologijama. Vezano uz rješenje očuvanja elektroničkih potpisa na dugi rok, kasnije u ovom radu, će se obraditi ključni slučajevi korištenja (engl. Use cases)

[209] InterPARES Trust, https://interparestrust.org/ (06.03.2018.)
[210] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 14 (06.02.2018.)
[211] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (06.02.2018.)

elektroničkih arhiva, mahom u Europskoj Uniji, koji se temelje na infrastrukturi javnog ključa.

Nastavno na novije rezultate InterPARES Trust projekta[212], Stančić na prezentaciji perspektiva InterPARES Trust projekta[213] u Hagu 2016. godine iznosi tezu i o četvrtom rješenju za dugoročno očuvanje integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima. Naime, radi se o bilježenju podatke o valjanosti elektroničkih potpisa u blokchainu[214] (engl. Record the digital signatures validity information to the blockchain).

Dakle, četiri rješenja (ili strategije) dugoročnog očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima koja se obrađuju u ovom radu su:

1. Očuvanje elektroničkih potpisa,
2. Uklanjanje elektroničkih potpisa,
3. Bilježenje traga o elektroničkim potpisima u metapodacima,
4. Bilježenje valjanosti o elektroničkim potpisima u blokchainu.

Prve tri strategije su navedene u spomenutom članku od Blanchette, a četvrta strategija je navedena u Stančićevom izlaganju o perspektivama InterPARES Trust projekta.
U kontekstu dugoročnog očuvanja elektroničkih potpisanih zapisa bitno je spomenuti i pojam Pouzdane arhivske služba, TAS (engl. Trusted Archive Service). Koncept TAS servisa uveden je u kontekstu Europske standardizacijske inicijative za elektronički potpis, EESSI (engl. European Electronic Signature Standardization Initiative), a fokus je bio na standardizaciji koja ima za cilj provođenje zahtjeva europske direktive za elektroničke potpise i europske standarde[215]. Koncept se odnosi na stvaranje nove vrste komercijalnih usluga koja će ponuditi osnivanje novih ustanova i zanimanja kako bi jamčila dugoročni

[212] InterPARES Trust, https://interparestrust.org/ (06.02.2018.)
[213] Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague, https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf (06.02.2108.)
[214] Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague, https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf, slide 19. (06.02.2108.)
[215] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 9 (06.02.2018.)

integritet elektronički potpisanih dokumenata. Dumortier i Eynde[216] navode da pouzdana arhivska služba (TAS) ima funkciju osiguravanja mogućnosti validacije arhiviranog elektronički potpisanog dokumenta godinama nakon dana pohrane istog u arhiv čak i ako se aplikacijsko rješenje kojim je izvedena ovjera vremena nastanka elektroničkog dokumenta više ne koristi ili je zastarjela. TAS mora osigurati održavanje aplikativnog rješenja za uvid u arhiv te aplikacije za validaciju elektroničkog potpisa. Sve se to treba osigurati zajedno s pripadajućom platformom, tj. s hardverom i operacijskim sustavom. Ako se ne može osigurati takva pripadajuća platforma, potrebno je osigurati bar najmanje emulaciju takvog okruženja. Time se može osigurati mogućnost validacije autentičnosti dokumenata i uvid u arhivirane dokumente, te što je jako bitno, i validaciju pripadajućeg elektroničkog potpisa kroz duže vremensko razdoblje. Isti autori, nadalje, predlažu da TAS mora prihvatiti samo dokumente u formatu koji se i dalje može razumjeti te da svaki TAS mora stoga objaviti popis podržanih formata dokumenata, a takav popis može biti iscrpan ili vrlo ograničen. Svaki put kada TAS zaprima novi dokument mora se provjeriti format prije nego što se prihvati za arhiviranje.

Volarević i Stančić u kontekstu dugoročnoga arhiviranja elektronički potpisanih zapisa navode da[217]:„možda neće biti dovoljno samo da elektronički potpis označimo vremenskim žigom dok potpis još vrijedi, odnosno prije isteka certifikata, a da se potom sam vremenski žig ne obnavlja, jer je za dugoročno arhiviranje potreban samo dokaz da je potpis postojao u jednome trenutku, u jednome obliku i da je tada bio valjan, ali ne i mogućnost da taj isti potpis ponovno provjerimo. U ovome slučaju potrebno je periodički obnavljati arhivski vremenski žig kao što je to predviđeno normom ETSI EN 319 102-1.“. Dakle, navedeno „možda“ odnosi se upravo na strategiju očuvanja elektroničkog potpisa te je za tu strategiju potrebno periodički obnavljati arhivski vremenski žig. Za ostale tri strategije očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima nije potrebno periodički obnavljati arhivski vremenski žig.

Prva navedena strategija (Očuvanje elektroničkih potpisa) je već detaljno obrađena u poglavlju 4. Napredni elektronički potpis kao podloga za dugoročno očuvanje

[216] Dumortier, J., Van Den Eynde, S., Electronic Signatures and Trusted Archival Services, http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf , str. 7. (07.02.2018.)
[217] Volarević, I., Stančić, H. (2016.), Norme za elektroničke vremenske žigove i mogućnosti njihove primjene u arhivskoj struci, Arhivi i domovinski rat, Zagreb, str. 433 (str. 425-435), http://www.bib.irb.hr/850052 (08.02.2018.)

elektroničkih zapisa, a obrađivat će se i u poglavlju 10. Model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata. Iz navedenog razloga se ova strategija u ovom poglavlju neće zasebno obrađivati. Kao uvod u obradu naprednog elektroničkog potpisa detaljno je obrađena i infrastruktura javnog ključa (PKI) u poglavlju 3.

Ostale tri strategije dugoročnog očuvanja integriteta i autentičnosti elektroničkih zapisa s elektroničkim potpisima će biti opisane u nastavku ovog poglavlja.

5.1 UKLANJANJE ELEKTRONIČKIH POTPISA

Američki nacionalni arhivi[218] (engl. National Archives) su 2000. godine izdali Smjernice za upravljanje zapisima za agencije za provedbu tehnologija elektroničkog potpisa[219] (engl. Records Management Guidance for Agencies Implementing Electronic Signature Technologies). U navedenim Smjernicama se nude dva pristupa arhiviranja elektronički potpisanih zapisa[220]. U prvom pristupu agencije mogu odlučiti zadržati mogućnost ponovnog potvrđivanja elektroničkog potpisa. informacije potrebne za provjeru valjanosti elektroničkog potpisa (tj. javni ključ koji se koristi za potvrdu potpisa, certifikat koji se odnosi na taj ključ, CRL,…) moraju se čuvati dokle god je elektronički potpisan zapis arhiviran. Obje kontekstualne i strukturne informacije o zapisu moraju biti čuvane. Drugi pristup se temelji na održavanju odgovarajuće dokumentacije o valjanosti elektroničkog potpisa koje je generirana u vrijeme potpisivanja ili blizu njega. Ovakav pristup može biti poželjan za arhiviranje zapisa koji se zadržavaju trajno ili dugoročno. Ovaj pristup je manje ovisan o tehnologiji i mnogo se lakše podržava s obzirom da tehnologije evoluiraju s vremenom. Za ovaj pristup elektronički potpis ne treba biti čitljiv tijekom vremena zbog bitnog mijenjanja zapisa ili kao posljedica tehnološke zastarjelosti. Agencije moraju osigurati da se za trajne zapise tiskaju ime potpisnika i datum kada je potpis izvršen na elektroničkom prikazu ili ispisu. Dakle, u ovom slučaju se elektronički potpis može ukloniti.

[218] Nacional Archives, https://www.archives.gov/ (08.02.2018.)
[219] Nacional Archives and Record Administration (2000.), Records Management Guidance for Agencies Implementing Electronic Signature Technologies, https://www.archives.gov/files/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf (08.02.2018.)
[220] Nacional Archives and Record Administration (2000.), Records Management Guidance for Agencies Implementing Electronic Signature Technologies, https://www.archives.gov/files/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf, str. 8 (08.02.2018.)

Blanchette u svom članku „Definiranje elektroničke autentičnosti: Interdisciplinarni put“[221] (engl. Defining Electronic Authenticity: An Interdisciplinary Journey) navodi i slučaj Kanadskog nacionalnog arhiva koji je 2001. godine izdao dokument „Smjernice za zapise izrađene pomoću infrastrukture javnog ključa infrastrukturi pomoću šifriranja i elektroničkih potpisa“[222] (engl. Guidelines For Records Created Under a Public Key Infrastructure Using Encryption And Digital Signatures). Nacionalni arhiv Kanade propisuje da neće zadržati sposobnost ponovnog potvrđivanja elektroničkog potpisa nakon prijenosa potpisanog zapisa pod njegovu kontrolu niti očuvati tragove elektroničkog potpisa koji se generiraju u federalnom PKI sustavu. Blanchette u navedenom članku spominje i finalni izvještaj InterPARES projekta iz 2002. godine[223] u kojem se zaključuje da su „elektronički potpisi i infrastruktura javnih ključeva (PKI) primjeri tehnologija koje su razvijene i implementirane kao sredstva autentifikacije za elektroničke zapise koji se prenose *arros space*. Iako su se arhivisti i informatički stručnjaci pouzdali u autentifikacijske tehnologije kako bi se osigurala vjerodostojnost zapisa te tehnologije nikada nisu namjeravale biti održive kao sredstvo osiguranja autentičnosti elektroničkih zapisa tijekom vremena.“

Dakle, može se zaključiti da su se Smjernice Američkog nacionalnog arhiva iz 2000., Smjernice Kanadskog nacionalnog arhiva iz 2001., te finalni izvještaj InterPARES projekta iz 2002. godine dosta neafirmativno odnosile prema infrastrukturi javnog ključa kao podlozi za dugoročno očuvanje elektronički potpisanih zapisa. Brisanje elektroničkih potpisa i bilježenje informacije o valjanosti elektroničkog potpisa u nekom obliku prije trenutka brisanja potpisa i arhiviranja zapisa za navedene smjernice i InterPARES finalni izvještaj čine se kao sasvim zadovoljavajuće rješenje. Strategijom uklanjanja elektroničkog potpisa se neću više baviti u radu već ću u većoj mjeri posvetiti obradi ostale tri strategije (očuvanje elektroničkih potpisa, bilježenje traga o elektroničkim potpisima u metapodacima, bilježenje valjanosti o elektroničkim potpisima u blokchainu).

[221] Blanchette, J.F. (2004.), Defining Electronic Authenticity: An Interdisciplinary Journey, International Conference on Dependable Systems and Networks, IEEE Computer Society Press, str. 231 (228-232.), http://kavehh.com/my%20Document/Essex/Digital%20signature/blanchettejf_authenticity.pdf (10.02.2018.)
[222] National Archives of Canada (2001.), Guidelines For Records Created Under a Public KeyInfrastructure Using Encryption And Digital Signatures (10.02.2018.)
[223] InterPARES (2002.), The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, http://www.interpares.org/book/index.htm (10.02.2018.)

5.2 BILJEŽENJE TRAGA O ELEKTRONIČKIM POTPISIMA U METAPODACIMA

Bralić, Kuleš i Stančić navode[224] da trenutno većina arhiva ovisi o povjerenju u potvrđivanje zastarjelih elektroničkih potpisa. Tu se mora vjerovati arhivu (ili drugoj instituciji) koja čuva dokument na kojem je potpis bio valjan u vrijeme arhiviranja te da se dokument nije poslije toga mijenjao. Navedene informacije o valjanosti elektroničkog potpisa se mogu spremati u metapodatke.

Boudrez[225] tvrdi da zapisi o valjanosti elektroničkog potpisa u metapodacima mogu zamijeniti elektronički potpis za one elektroničko potpisane zapise čije je razdoblje očuvanja trajno (engl. permanent retention period).

Płoszajski navodi[226] da se metapodaci koriste za opisivanje digitalnih podataka već neko vrijeme. Navodi da su prvi standardi metapodataka nastali devedesetih godina prošlog stoljeća. Tako je Dublin Core[227] dizajniran za opis web resursa još 1995. godine. Dublin Core shema[228] je mali skup rječničkih pojmova koji se mogu koristiti za opisivanje web resursa (video, slike, web stranice i dr.). Osim toga, mogu se opisivati i fizički resursi poput knjiga ili CD-ova te predmeta poput umjetnina.
Płoszajski, nadalje, piše[229] o očuvanju digitalnih objekata. Jedna od mogućih aktivnosti nad njima je prikupljanje opisnih informacija o svakom digitalnom objektu. Takve se informacije nazivaju metapodaci. Navedeni autor piše u kontekstu digitalizacije kulturne baštine gdje se stvaraju metapodaci nakon stvaranja odgovarajućih digitalnih objekata. U takvom slučaju metapodaci trebaju sadržavati informacije o izvornom objektu i o stvorenom digitalnom objektu (npr. parametri digitalne slike, korištene opreme, podataka i vremena stvaranja i dr.). Metapodaci trebaju sadržavati pravne informacije o pristupu na

[224] Bralić, V., Kuleš, M., Stančić, H. (2017.), A model for long-term preservation of digital signature validity: TrustChain, Konferencija INFuture 2017: Integrating ICT in Society, https://bib.irb.hr/datoteka/906471.TrustChainV11-final.pdf , str. 2 (18.02.2018.)
[225] Boudrez, F. (2007.), Digital signatures and electronic records, Archival Science, ISSN: 1389-0166, str. 190 (179-193)
[226] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 15 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[227] Dublin Core Metadata Initiative, http://dublincore.org/ (19.02.2018.)
[228] Dublin Core, https://en.wikipedia.org/wiki/Dublin_Core (19.02.2018.)
[229] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 16 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)

digitalni objekt i dopuštene i/ili zabranjene transformacije. Metapodaci se nazivaju prema prirodi informacija, npr. opisne, tehničke, administrativne, prava pristupa i dr.

Što se tiče metapodataka i bilježenja traga o elektroničkim potpisima u njima, postoji više tipova metapodataka namijenjenih tome. McDonough[230] navodi METS[231] (engl. Metadata Encoding and Transmission Standard) kao standard za metapodatke koji služi za kodiranje opisnih, administrativnih i strukturnih metapodataka u vezi s objektima unutar digitalne knjižnice. Izrađen je pomoću jezika XML sheme. Standard se održava kao dio MARC standarda Kongresne knjižnice, a razvija se kao inicijativa Federacije digitalnih knjižnica, DLF (engl. Digital Library Federation). Wikipedija METS definira[232] kao XML shemu dizajniranu u svrhu:

- Izrada primjeraka XML dokumenta koji izražavaju hijerarhijsku strukturu digitalnih bibliotekarskih objekata,
- Snimanje naziva i mjesta datoteka koje sadrže te objekte,
- Snimanje povezanih metapodataka. METS se stoga može koristiti kao alat za modeliranje objekata u stvarnom svijetu, kao što su određeni tipovi dokumenata.

U okviru OAIS referentnog modela METS dokument se može upotrijebiti u ulozi SIP-a (Dostavljenog informacijskog paketa), AIP-a (Arhivskog informacijskog paketa) ili DIP-a (Diseminacijski informacijski paket). McDonough navodi[233] da je postojala želja da METS olakša razmjenu i interoperabilnost digitalnih bibliotekarskih objekata preko digitalnih bibliotekarskih sustava i pružanja podrške dugoročnom očuvanju digitalnih bibliotekarskih objekata. Krier i Strasser[234] navode da je METS u potpunosti razvijena shema za aministrativne podatke. Ona administrativne podatke razdvaja u četiri dijela: tehničke metapodatke (engl. tehnical metadata) za format datoteke i izradu, metapodatke za intelektualna prava (engl. intellectual property and rights metadata), metapodatke za vlasništvo i pristupna prava (engl. intellectual property and rights metadata, about data ownership and access rights), izvorne metapodatke (engl. source metadata) koji se široko

[230] McDonough, J., METS: Standardized Encoding for Digital Library Objects, University of Illinois, https://www.ideals.illinois.edu/bitstream/handle/2142/177/METS.pdf?sequence=2 , str. 2 (18.02.2018.)
[231] Digital Library Federation (2010.), METS Reference Manual, https://web.archive.org/web/20130516023805/http://www.loc.gov/standards/mets/METSPrimerRevised.pdf (18.02.2018.)
[232] METS, Metadata Encoding and Transmission Standard, https://en.wikipedia.org/wiki/Metadata_Encoding_and_Transmission_Standard (18.02.2018.)
[233] McDonough, J., METS: Standardized Encoding for Digital Library Objects, University of Illinois, https://www.ideals.illinois.edu/bitstream/handle/2142/177/METS.pdf?sequence=2 , str. 3 (18.02.2018.)
[234] Krier, L., Strasser, C. (2014.), Data Management for Libraries: A LITA Guide StrasserData Management for Libraries: A LITA Guide, Chicago, str. 44. (18.02.2014.)

primjenjuju za datoteke digitalizirane iz originalnog analognog izvora, te metapodatke digitalne provenijencije (engl. digital provenance metadata) koja služi za bilježenje bilo kakvih promjena na datoteci tijekom životnog ciklusa u procesa očuvanja. Ako se datoteka migrira na napredniji datotečni format, tada je vrlo bitno zabilježiti ne samo da je datoteka mijenjana, od koga i kada, već je bitno ažurirati i metapodatke. Popis slijeda mjerodavnosti (engl. chain of custody) digitalnih objekata treba biti dio administrativnih metapodataka. Krier i Strasser[235], nadalje tvrde da je drugi ključ očuvanja integriteta digitalnih objekata uključivanje informacije o stabilnosti (engl. fixity information). Informacija o stabilnosti može podržati provjeru integriteta podataka na stupnju objekata podataka koristeći kontrolne zbrojeve i elektroničke potpise koji upozoravaju na bilo koju promjenu napravljenu na datoteci na stupnju bitova. Informacija o stabilnosti osigurava da se podaci nisu mijenjali u privremenom razdoblju vremena i osigurava dokaz integriteta podataka.

METS profili se koriste za[236]:

- Glazbu,
- Materijale za ispis (knjige, pamfleti itd.),
- Snimljene događaje (audio ili video),
- PDF dokumente,
- Bibliografske zapise,
- Fotografije,
- CD-ove,
- kolekcije.

U nastavku slijedi primjer AIP objekta gdje su informacije o pristupnim pravima omotane u METS dokumentu pomoću sheme METSRights.

[235] Krier, L., Strasser, C. (2014.), Data Management for Libraries: A LITA Guide StrasserData Management for Libraries: A LITA Guide, Chicago, str. 44. (18.02.2014.)
[236] METS, Metadata Encoding and Transmission Standard, https://en.wikipedia.org/wiki/Metadata_Encoding_and_Transmission_Standard (19.02.2018.)

```
<RightsDeclaration >
   Any re -use of these materials in publication may
   only be done with the explicit permission of the
   Charles L. Dodgson Estate. Please contact the
   Fales Library staff if you wish to use any of
   these materials.
</RightsDeclaration >
...
<RightsHolder RIGHTSHOLDERID =" FALESRH01">
  <RightsHolderName >The Estate of Charles L.
     Dodgson (Lewis = Carroll )</ RightsHolderName >
  <RightsHolderComments >
     The estate of Charles Dodgson is represented by
     AP Watt agency of London. All permissions issues must
     be addressed to them.
  </RightsHolderComments >
  <RightsHolderContact >
     ...
  </RightsHolderContact >
</RightsHolder >
...
<Context CONTEXTCLASS =" GENERAL PUBLIC">
   <Permissions OTHER =" false" PRINT =" false" DELETE =" false" MODIFY =" false"
      DUPLICATE =" false" COPY =" false"
      DISPLAY ="true" DISCOVER =" true"/>
   <Constraints CONSTRAINTTYPE =" QUALITY">
   <ConstraintDescription >
      Users may only access digital copies of photographic
      materials digitized at 50 dpi or less.
   </ConstraintDescription >
   </Constraints >
</Context > <Context CONTEXTCLASS =" REPOSITORY MGR">
   <Permissions OTHER =" false" PRINT =" true"
     DELETE =" true" MODIFY =" true"
     DUPLICATE ="true" COPY =" true"
     DISPLAY ="true" DISCOVER =" true"/>
</Context >
```

Slika 33. Primjer METS AIP objekta, preuzeto iz Płoszajski, G. (2017.)[237]

DIP može izvući METSRights metapodatke iz AIP-a kako bi korisnicima pružio detalje o uvjetima pristupa.

Płoszajski zaključuje[238] se se standardi metapodataka kontinuirano razvijaju. Dobivaju nove inačice, kao npr. standard VRA Core[239] koji služi za opis slika i djela u umjetnosti, a stvoren je krajem devedesetih godina. VRA Core je dobio verziju 4.0 u 2007. godini. ISO 19115 standard DIF[240] koji se koristi u zemljinim znanostima (engl. earth sciences) u 2010. godini dobiva verziju 6.0. Već spomenuti METS stvoren je 2001, a 2015. godine dobiva verziju 11.0 XML sheme. Kao rezultat sve toga, metapodacima koji se temelje na različitim verzijama mora se osigurati suživot u dugoročnim elektroničkim arhivama, a arhivi moraju biti u stanju upravljati imovinom s metapodacima koji se temelje na različitim standardnim verzijama. Brojni rječnici i ontologije podataka razvijeni su kao dio standarda metapodataka koji pomažu u pripremi dosljednih metapodataka, npr.

[237] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 19 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[238] Isto, str. 15
[239] VRA, Visual Resources Association, http://www.vraweb.org/index.html (19.02.2018.)
[240] DIF, Directory Interchange Format, Global Change Master Directory, http://www.gcmd.nasa.gov/add/difguide/index.html (19.02.2018.)

PREMIS[241]. Isti autor, nadalje, zaključuje[242] da su standardi koji zaslužuju više pozornosti u kontekstu dugoročnog arhiviranja:

- METS, koji se može koristiti za stvaranje paketa SIP, a namijenjen je sadržavanju metapodataka o pravima,
- PREMIS, koji definira obilježja prava koja se odnose na očuvanje aktivnosti i skuplja informacije tijekom pohrane digitalnih objekata u arhivu.

PREMIS ima veliki značaj[243] među standardima metapodataka za očuvanje podataka. Naziv PREMIS označava **PRE**servation**M**etadata: **I**mplementation **S**trategies. Izvorno to je naziv međunarodne radne skupine osnovane 2003. godine za dizajn metapodaka za digitalno očuvanje. Izrada metapodataka u PREMIS standardu se temelji se na modelu podataka i semantičkim jedinicama. Model podataka definira pet međusobno povezanih entiteta: intelektualni entitet, objekt, događaj, agent i prava. Intelektualni entitet definira se kao "skup sadržaja koji se promatra kao jedna intelektualna jedinica za potrebe upravljanja i opisa". Verzija 3.0 PREMIS standarda je objavljena 2015. godine.

PREMIS metapodaci se mogu koristiti za čuvanje hash vrijednosti i elektroničke potpise. Konzorcij W3C je 2013. godine objavio dokument „Sintaksa i obrada XML potpisa“[244] (engl. XML Signature Syntax and Processing). U navedenom dokumentu se navodi da se provjera XML potpisa sastoji se od dvije faze:

1. Validacije potpisa
2. Validacije reference

U članku „Metapodaci za autentičnost: hash funkcije i elektronički potpisi“[245] (engl. Metadata for authenticity: hash functions and digital signatures) se ističe a popularnost standarda metapodataka kao što je METS, koji omogućuje referenciranje i ugrađivanje metapodataka i digitalnih datoteka u jednu XML datoteku. PREMIS standard određuje da se elektronički potpisi primjenjuju samo na datoteke i sljedove bitova radi očuvanja te

[241] PREMIS Data Dictionary for Preservation Metadata, http://www.loc.gov/standards/premis/ (19.02.2018.)
[242] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 45 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[243] Isto, str. 15
[244] W3C (2013.), XML Signature Syntax and Processing Version 1.1 , Recommendation, https://www.w3.org/TR/xmldsig-core/ (19.02.2018.)
[245] Paradigm.ac.uk, Metadata for authenticity: hash functions and digital signatures, http://www.paradigm.ac.uk/workbook/metadata/authenticity-xml.html (19.02.2018.)

stoga nije potrebna mogućnost potpisa agregacije datoteka. Unatoč tome, preporuka W3C konzorcija ostaje de facto standard za kodiranje elektroničkih potpisa te su korisne njezine definicije pravila obrade elektroničkih potpisa i semantičkih jedinica potrebnih za pohranu. PREMIS posuđuje[246] neke elemente iz W3C preporuke u definiranju semantičkih jedinica potrebnih za pohranu metapodataka o elektroničkim potpisima. Navedeni metapodaci uključuju:

- Vrijednost samog elektroničkog potpisa,
- Naziv algoritma hash funkcije i algoritma elektroničkog potpisa koji se koristi za izradu potpisa,
- Parametre povezane s navedenim algoritmima,
- Lanac certifikata (ako se certifikati koriste za vezanje subjekta potpisnika na njegov javni ključ) potrebnih za provjeru potpisa.

U nastavku slijedi prikaz PREMIS metapodaka koji uključuju gore navedene podatke o elektroničkom potpisu.

```
<premis:object>
  <--!other metadata-->
    <premis:signatureInformation>
      <premis:signatureInformationEncoding>BASE 64</premis:signatureInformationEncoding>
      <premis:signer>Susan Thomas</premis:signer>
      <premis:signatureMethod>DSA-SHA1</premis:signatureMethod>
      <premis:signatureValue>qUADDMHZkyebvRdLs+6Dv7RvgMLRlUaDB4Q9yn9XoJA79a2882ffTg==
      </premis:signatureValue>
      <premis:signatureValidationRules>Add reference to repository documentation detailing signature
      validation rules</premis:signatureValidationRules>
      <premis:signatureProperties>2006-11-01T10:15:16</premis:signatureProperties>
    </premis:signatureInformation>
  <--!other metadata-->
</premis:object>
```

Slika 34. PREMIS metapodaci za bilježenje podataka o elektroničkim potpisima, preuzeto s Paradigm.ac.uk[247]

Arhivi koji koriste elektroničke potpise moraju sigurno pohraniti svoje privatne i javne ključeve. PREMIS također preporučuje[248] da arhivi pohranjuju definicije algoritama i

[246] Paradigm.ac.uk, Metadata for authenticity: hash functions and digital signatures, http://www.paradigm.ac.uk/workbook/metadata/authenticity-xml.html (19.02.2018.)
[247] Isto
[248] Isto

relevantnih standarda koji se koriste u kontekstu pohrane elektroničkih potpisa kako bi se te metode mogle ponovno implementirati ako bude potrebno.

Bitno je napomenuti da PREMIS u METS-u može imati ulogu PDI-a (engl. Preservation Description Information) u AIP-u. Dakle, METS XML se može koristiti kao serijalizacija PREMIS-a, tj. METS XML je dobar medij za PREMIS set metapodataka. Na ovaj način se mogu kombinirati. Primjer korištenja PREMIS-a kao PDI unutar METS XML strukture je Archivematica[249].

Rajh i Šimundža-Perojević navode primjer korištenja PREMIS-a u METS XML strukturi u sustavu HALMED-a (Hrvatska Agencija za lijekove i medicinske proizvode)[250]. Autori navode da PREMIS treba implementirati na razini objekta ugradnjom PREMIS metapodataka u XML (npr. u METS XML). HALMED je definirao svoje PREMIS entitete i njihova svojstva.

Od verzije 2.2 Fedora[251] digitalni repozitorijski softver pruža mogućnost izračuna, pohranjivanja i provjere hash vrijednosti za sve datoteke i metapodatke kojima se upravlja u repozitoriju. Fedora podržava snimanje jedne vrijednosti pomoću jednog od sljedećih algoritama: MD5, SHA-1, SHA-256, SHA-384 i SHA-512[252]. Dobiveni metapodaci održavaju se kao dio FOXML-a (Fedora nativni XML standard, koji se može izvesti u METS) i izgleda kao na slici 35.

[249] Archivematica, https://wiki.archivematica.org/Improvements/aipreadme (03.09.2018.)
[250] Rajh, A., Šimundža-Perojević, Z. (2018.), Lessons learned from internal and external digitisation processes implemented at the Croatian Agency for Medicinal Products and Medical Devices, izlaganje na konferenciji Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja (Radenci, 11. – 13.4.2018.), https://www.researchgate.net/publication/326836150_Lessons_learned_from_internal_and_external_digitisation_processes_implemented_at_the_Croatian_Agency_for_Medicinal_Products_and_Medical_Devices (03.09.2018.)
[251] Fedora, http://fedorarepository.org/ (19.02.2018.)
[252] Paradigm.ac.uk, Metadata for authenticity: hash functions and digital signatures, http://www.paradigm.ac.uk/workbook/metadata/authenticity-xml.html (19.02.2018.)

```
<--!other metadata-->
 <foxml:datastream CONTROL_GROUP="M" ID="thumbnail" STATE="A" VERSIONABLE="true">
   <foxml:datastreamVersion CREATED="2007-02-07T15:32:05.802Z" ID="thumbnail.0"
   LABEL="Thumbnail image of Louis in the Sun" MIMETYPE="image/jpeg" SIZE="0">
     <foxml:contentDigest DIGEST="8316de8d1432a3df74c4f1c4f530187e469a1bff" TYPE="SHA-
     1"/>
     <foxml:contentLocation REF="http://shuttle.paradigm.ac.uk:8080/fedora/get/paradigm:401/
     thumbnail/2007-02-07T15:32:05.802Z" TYPE="INTERNAL_ID"/>
   </foxml:datastreamVersion>
 </foxml:datastream>
<--!other metadata-->
```

Slika 35. FEDORA metapodaci za bilježenje hash vrijednosti, preuzeto s Paradigm.ac.uk[253]

Płoszajski u kontekstu standarda za metapodatke i OAIS informacijskih paketa (SIP, AIP i DIP) spominje[254] da se generalno paketi sastoje od:

- Digitalnih objekata (datoteka sa sadržajem i datoteka s metapodacima),
- Metapodataka s opisom samog paketa.

Metapodaci koji se tiču paketa trebali bi imati barem informacije o strukturi paketa: npr. popis datoteka, format datoteka, struktura kataloga i slično te informacije o atributima datoteka kao što su kontrolni zbrojevi. Neki takvi sustavi metapodataka postali su standardi. To obično znači da su definirani detaljno i točno te da imaju sintaksu pod kontrolom XML sheme koju održava organizacija odgovorna za standard. Razvijeno je nekoliko takvih standarda metapodataka koji služe za definiranje paketa[255]:

- METS - već je više puta spomenut u ovom radu,
- XFDU[256] – XML formatirana podatkovna jedinica, izrađena je za prostorne podatke (ISO standard 13527 iz 2003. godine),
- LOTAR[257] – Radna grupa za metapodatke i arhivske pakete (engl. Metadata for Archival Package Workgroup),
- E-ARK[258] – Europsko arhiviranje zapisa i očuvanje znanja (engl. European Archival Records and Knowledge Preservation),

[253] Isto
[254] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 47 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[255] Isto, str. 47
[256] ISO (2008., 2.), XFDU, XML Formatted Data Unit, Structure and Construction Rules, CCSDS 661.0-B-1. Blue Book, ISO 13527:2010, https://public.ccsds.org/Pubs/661x0b1.pdf (19.02.2018.)
[257] LOTAR: Long Term Archiving and Retrieval. Metadata for Archival Package Workgroup, http://www.lotar-international.org/lotar-workgroups/metadata-for-archival-package.html (19.02.2018.)

5.3 BILJEŽENJE VALJANOSTI O ELEKTRONIČKIM POTPISIMA U BLOKCHAINU

Strategija bilježenja valjanosti o elektroničkim potpisima u blokchainu je nova strategija. Blokchain[259] kao tehnologija je nastala 2008. godine. Izumio ga je Satoshi Nakamoto[260] za upotrebu u kriptovaluti Bitcoin[261] kao svoju javnu knjigu transakcija. Danas se blokchain pojam usko veže uz kriptovalute, npr. Bitcoin i Ethereum[262]. Satoshi Nakamoto je funkcioniranje Bitcoina objasnio i u čuvenom članku „Bitcoin: A Peer-to-Peer Electronic Cash System“[263].

Ideja blokchain tehnologije je decentralizirani sustav za zapisivanje različitih vrsta podataka iako su najpoznatije financijske transakcije vezane uz kriptovalute. U ovom radu će se blokchain obraditi u smislu mogućnosti upisivanja podataka o valjanosti elektroničkih potpisa. Blokchain je kompleksan sustav koji prati sve transakcije (financijske ili druge prirode). Svi akteri u sustavu mogu zapisivati transakcije ako slijede propisana pravila. Ovdje je bitno napomenuti da je sustav strogo decentraliziran, tj. nitko nije odgovoran za takav sustav. Dakle, nema neke centralne točke koja upravlja blokchainom. Bitcoin je tako suprotnost današnjem financijskom sustavu u kojem centralne banke upravljaju svime. Nasuprot tome blokchain sustav je mreža servera koji se ponašaju kao replicirane baze podataka. Dakle, svaki server sadrži sve podatke o specifičnim transakcijama. Bitan je pojam bloka (engl. block) koji se sastoji od velikog broja transakcija. Kada se više blokova nižu jedan za drugim čine lanac blokova (engl. blokchain). Blokchain se u svojem radu koristi konceptom glavne knjige (engl. ledger). Računala u blokchain sustavu (mreži) koji pogađaju kombinacije kako bi se otkrili hashevi zovu se čvorovi (engl. nodes). Otkrivanje hasheva je i smisao ovih akcija što će u ovom radu biti objašnjeno za potrebe čuvanja valjanosti o elektroničkim potpisima. Kada se otkrije hash, odobrava se obavljanje transakcije, a čvorovi šalju informacije o tome po cijelom sustavu te svaki server bilježi informacije o transakciji kod sebe (zbog toga je riječ o distribuiranoj glavnoj knjizi). Time svi akteri u blokchain sustavu dobivaju informacije o svim transakcijama čije promjene je kasnije nemoguće sakriti baš zbog najšireg mogućeg distribuiranja podataka o njima. Iz tog razloga je blokchain danas sve prihvaćeniji za

---

[258] E-ARK - European Archival Records and Knowledge Preservation, http://www.eark-project.com/about/work-packages/9-about/32-wp4intro (19.02.2018.)
[259] Blokchain, https://en.wikipedia.org/wiki/Blockchain (10.02.2018.)
[260] Satoshi Nakamoto, https://en.wikipedia.org/wiki/Satoshi_Nakamoto (10.02.2018.)
[261] Bitcoin, https://www.bitcoin.com/ (10.02.2018.)
[262] Ethereum, https://www.ethereum.org/ (12.02.2018.)
[263] Nakomoto, S.(2008.), Bitcoin: A Peer-to-Peer Electronic Cash System, http://nakamotoinstitute.org/bitcoin/#selection-7.4-9.38 (12.02.2018.)

financijske transakcije, a predstavlja izazov i za transakcije drugog tipa kao što je čuvanje informacija o valjanosti elektroničkih potpisa što je i tema ovog rada. Mogućnosti korištenja blokchain tehnologije je vrlo široka. Ova tehnologija se može iskoristiti za bilježenje svih promjena prilikom prodaja i kupovina nekretnina. Ovime se blokchain koristi za bilježenje svih kupoprodajnih nekretninskih transakcija. Postoje već slučajevi pokretanja izrade zemljišnih knjiga utemeljenih na blokchain tehnologiji, npr. švedski katastar[264] (šve. Lantmäteriet), grad London[265] ili Honduras[266].

Proces pogađanja hasheva se zove rudarenje (engl. mining). Rudarenje ima ovdje preneseno značenje jer se „rudari" primjerice Bitcoin kriptovaluta uz utrošak vremena i korištenje struje za pokretanje računala. U procesu rudarenja Bitcoina čvor koji je pogodio ciljanu kombinaciju će biti nagrađen s nekoliko tokena, tj. Bitcoina. Iz navedenog razloga se proces rudarenja temelji na korištenju snažnih računala koja rješavaju složene matematičke algoritme koji su ključ za autentifikaciju transakcija preko blokchaina. Rudarenje u blokchain sustavima postaje svakim danom sve zahtjevnije tako da su se počela koristiti i superračunala koja su projektirana za rad na nuklearnom oružju jer imaju ogroman kapacitet. U želji za lakom zaradom nisu rijedak slučaj niti zlouporabe kao ona u Federalnom nuklearnom centru u Sarovu, u zapadnoj Rusiji[267]. Naime, znanstvenici iz navedenog nuklearnog centra su razotkriveni od ruske tajne službe i uhićeni jer su vojna superračunala iz nuklearnog centra koristili za rudarenje kriptovaluta.

Budući da je blokchain baza podataka (ili datoteka koja sadrži svaku transakciju ikada izvršenu) podijeljena između svih čvorova koji su u sustavu tako svi akteri mogu znati npr. koliko je jedinica neke kriptovalute bilo na nekoj adresi u bilo kojem trenutku. Ovakav tip blokchaina je javan. S druge strane, blokchain se može izgraditi i kao privatan. U privatnom blokchainu pristup nemaju svi akteri već samo akter koji je ovlašten za navedeno i ima određeno sredstvo (token) s kojim onda može zapisivati transakcije.

[264] Qz.com, Sweden's blockchain-powered land registry is inching towards reality, https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/ (12.02.2018.)
[265] Citymetric.com, Forget privatisation: the Land Registry needs blockchain, https://www.citymetric.com/politics/forget-privatisation-land-registry-needs-blockchain-2233 (12.02.2018.)
[266] In.reuters.com, Honduras to build land title registry using bitcoin technology, https://in.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515 (12.02.2018.)
[267] Vecernji.hr, Rusi uhitili znanstvenike kada su otkrili za što koriste superračunala, https://www.vecernji.hr/vijesti/ruski-znanstvenici-atomska-bomba-bitcoin-kriptovaluta-1225724 (11.02.2018.)

Ovakva vrsta blokchaina je primjenjiva u tvrtkama, ustanovama koje žele napraviti distribuirani sustav u svojoj organizaciji (ili više povezanih organizacija) za bilježenje transakcija kojima ne smije pristupiti javnost. Privatni tip blokchaina je zanimljiviji za bilježenje valjanosti o elektroničkim potpisima nego javni. Razlog zašto je korištenje privatnog blokchaina perspektiva za veće organizacije je u pojmu „jedne točke neuspjeha" (engl. single point of failure). Naime, ako su u nekoj organizaciji na središnjem serveru pohranjeni svi bitni podaci, a dogodi se greška – to znači nedostupnost ili gubitak podataka i posljedično veliku štetu za kompaniju. Do sada su kompanije u svijetu navedeno rješavale konceptom visoke dostupnosti (engl. high availability), tj. više moćnih servera koji u različitim načinima rada preuzimaju funkcije jedan od drugog. Osiguravanje koncepta visoke dostupnosti za tvrtke iziskuje izuzetno velike troškove ulaganja.

Lemieux 2015. godine u svom članku „Blockchain Technology for Recordkeeping"[268] iznosi tezu da blokchain tehnologija, sa svojim opsežnim potencijalnim aplikacijama, mogla dramatično promijeniti zapisivanje podataka. U zaključku članka Lemieux navodi[269]: „Blokchain tehnologija bi mogla promijeniti postojeću paradigmu za vjerodostojne zapise; umjesto korištenja pouzdane treće strane (kao što su državni registri) za pouzdane podatke se korisnici mogu okrenuti prema blokchainu. Mogu se, također, fragmentirati komponente potrebne za utvrđivanje autentičnosti (npr. metapodaci i elektronički potpisi) samih zapisa". Osim afirmativnih izjava za blokchain tehnologiju Lemieux, nadalje, poziva i na oprez: „Najveća opasnost zapravo ne dolazi od ranjivosti ove tehnologije, već od slijepog povjerenja u blokchain, od blokchain developera, zakonodavaca, provođenja zakona, te odnosa javnosti prema ovoj tehnologiji."

Stančić je 2016. godine na prezentaciji InterPARES Trust projekta u Hagu iznio tezu o bilježenju valjanosti o elektroničkim potpisima u blokchainu[270] kao četvrtu tezu nakon tri već postojeće koje je ranije definirao Blanchette[271].

---

[268] Lemieux, V. L. (2015.), Blockchain Technology for Recordkeeping, The University of British Columbia, Vancouver, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjo45yquaHZAhWH_ywKHarXDBwQFgg9MAI&url=https%3A%2F%2Fwww.researchgate.net%2Fprofile%2FVictoria_Lemieux%2Fpublication%2F309414363_Blockchain_for_Recordkeeping_Help_or_Hype%2Flinks%2F580f539408ae009606bb62f6%2FBlockchain-for-Recordkeeping-Help-or-Hype.pdf&usg=AOvVaw3BACiNT3YaeubXd3zG54iJ (12.02.2018.)

[269] Isto

[270] Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague,

Na konferenciji INFuture 2017 u Zagrebu su Bralić, Kuleš i Stančić prezentirali model za očuvanje valjanosti elektroničkog potpisa u blokchainu[272]. Autori navedenog modela navode problematiku kada se mora vjerovati arhivu (ili drugoj instituciji) koji čuva elektronički potpisani dokument čiji je potpis važio u vrijeme arhiviranja, a potrebno je imati i povjerenje da se dokument nije mijenjao od arhiviranja. Jedno od uobičajenih rješenja kojim se povećava povjerenje u takve arhive (ili druge institucije) je korištenje servisa vremenskog žiga. Time se znatno produljuje vijek trajanja potpisa, ali kako autori naglašavaju[273], nije trajno rješenje. Bralić, Kuleš i Stančić iz spomenutih razloga u istom članku predlažu poboljšanje ove situacije sa sustavom koji se temelji na tehnologiji blokchain koja bi mogla ukloniti potrebu povjerenja arhivima (i drugim sličnim institucijama) i to pohranjivanjem kontrolnih hasheva ili elektroničkih potpisa u nepromjenjiv i javno čitljiv blokchain. Koristeći takav sustav, svaka zainteresirana strana može potvrditi da je elektronički potpisan i arhiviran dokument doista ostao nepromijenjen i da je njegov potpis važeći u trenutku stvaranja zapisa u blokchainu. Taj sustav su Bralić, Kuleš i Stančić nazvali TrustChain[274]. Autori TrustChain model razvijaju kao dio istraživačke studije TRUSTER Preservation Model (EU31) na međunarodnom istraživačkom projektu InterPARES Trust te predstavlja jedno je od nekoliko rješenja problema dugoročnog očuvanja elektronički potpisanih dokumenata koje razmatra navedena istraživačka skupina.

U zaključku navedenog članka autori navode[275] da se predloženi sustav oslanja na uključenost skupine pouzdanih institucija koje su zainteresirane za provedbu takvog sustava. Jednom kad se takva skupina identificira i implementira sustav, može se staviti na raspolaganje bilo kojoj zainteresiranoj strani. Bralić, Kuleš i Stančić kao najveći nedostatak TrustChain modela navode to što rješava samo problem dugoročnog očuvanja dokumenata s važećim elektroničkim potpisima, a ne daje izravno rješenje za postojeće potpisane dokumente čiji su potpisni certifikati već istekli. Takvi elektronički potpisani

---

https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf, slide 19 (06.02.2108.)

[271] Blanchette, J. F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 14 (06.02.2018.)

[272] Bralić, V., Kuleš, M., Stančić, H. (2017.), A model for long-term preservation of digital signature validity: TrustChain, Konferencija INFuture 2017: Integrating ICT in Society, https://bib.irb.hr/datoteka/906471.TrustChainV11-final.pdf (18.02.2018.)

[273] Isto, str. 2

[274] Isto, str. 2

[275] Isto, str. 14

dokumenti bi se trebali ponovo potpisati prije nego što se njihovi zapisi zapišu u TrustChain, ili se trebaju razviti i povezati sa sustavom TrustChaina odvojena rješenja za spremanje validiranih potpisa.

Thompson također piše očuvanju elektroničkih potpisa u blokchainu[276] te postavlja pitanje nudi li PKI s blokchain pogonom bolju strategiju za očuvanje elektroničkog potpisa od PKI kontroliranog od strane CA. Nadalje, odgovara da to ovisi o tome koje metapodatke profesionalci odabiru za arhivsko pohranjivanje te o vremenu očuvanja. Korištenje blokchaina može biti povoljnije za zapise sa trajnim razdobljem očuvanja. To je zato što je hash vrijednost kao značajka blokchain lanca, postoji kao metapodatak o potpisu koji ne zahtijeva specifičan softver za buduće provjere. Nadalje, zapis blokchaina ne zahtijeva centraliziranu provjeru kao što to čini CA. Thompson zaključuje[277] da blokchain nudi uzbudljive mogućnosti razvoja za knjižnice, arhive i upravljanje zapisima, ali i da blokchain zajednica još uvijek ne može sagledati kakvi su krajnji ishodi razvoja sustava temeljenih na ovoj platformi te da bi informacijski stručnjaci trebali biti razboriti prije konačnog prihvaćanja tih tehnologija.

5.4 ZAKLJUČAK

Blanchette je 2006. u svom članku „The digital signature dilemma“[278] naveo tri moguće strategije za očuvanje elektroničkih zapisa s elektroničkim potpisima:[279]:

1. Očuvanje elektroničkih potpisa,
2. Uklanjanje elektroničkih potpisa,
3. Bilježenje traga o elektroničkim potpisima u metapodacima.

Blanchette kao najprihvatljiviju strategiju navodi bilježenje traga o elektroničkim potpisima u metapodacima jer je u najvećoj mjeri komforno s arhivskom praksom i teorijom.

[276] Thompson, T. (2017.), The preservation of digital signatures on the blockchain, The University of British Columbia iSchool Student Journal Vol. 3 (Spring 2017), http://ojs.library.ubc.ca/index.php/seealso/article/view/188841/186525 , str. 13. (10.02.2018.)
[277] Isto, str. 14
[278] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 1 (06.02.2018.)
[279] Isto, str. 14

Stančić na prezentaciji perspektiva InterPARES Trust projekta u Hagu 2016. godine predlaže i četvrtu strategiju, a radi se o bilježenju podataka o valjanosti elektroničkih potpisa u blokchainu[280].

Vezano uz problematiku strategija za dugoročno očuvanje elektronički potpisanih zapisa je bitan i pojam Pouzdane arhivske službe, TAS (engl. Trusted Archive Service). Pouzdana arhivska služba ima za funkciju osiguravanje mogućnosti validacije arhiviranog elektronički potpisanog dokumenta godinama nakon dana pohrane takvog zapisa u arhiv. Mogućnost validacije je potrebna čak i ako se aplikacijsko rješenje kojim je izvedena ovjera vremena nastanka elektroničkog dokumenta više ne koristi ili je zastarjela[281].

Strategija očuvanja elektroničkih potpisa je detaljno obrađena u poglavlju 4. Napredni elektronički potpis kao podloga za dugoročno očuvanje elektroničkih zapisa, a obrađivat će se i u poglavlju 10. Model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata pa nije posebno obrađena u ovom poglavlju.
Što se tiče strategije uklanjanja elektroničkih potpisa ona je bila aktualna početkom ovog stoljeća i to posebno u Sjevernoj Americi (SAD i Kanada). Takvu strategiju predviđaju (uz mogućnost bilježenja u metapodatke ili neki drugi oblik elektroničkog zapisa i ispisa) Smjernice Američkog nacionalnog arhiva[282] iz 2000., Smjernice Kanadskog nacionalnog arhiva[283] iz 2001. te finalni izvještaj InterPARES projekta[284] iz 2002. godine. Nacionalni arhiv Kanade u navedenim Smjernicama eksplicitno propisuje da neće zadržati sposobnost ponovnog potvrđivanja elektroničkog potpisa nakon prijenosa potpisanog zapisa pod njegovu kontrolu niti očuvati tragove elektroničkog potpisa koji se generiraju u federalnom PKI sustavu.

[280] Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague, https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf, str. 19 (06.02.2108.)
[281] Dumortier, J., Van Den Eynde, S., Electronic Signatures and Trusted Archival Services, http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (07.02.2018.)
[282] Nacional Archives and Record Administration (2000.), Records Management Guidance for Agencies Implementing Electronic Signature Technologies, https://www.archives.gov/files/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf (08.02.2018.)
[283] National Archives of Canada (2001.), Guidelines For Records Created Under a Public KeyInfrastructure Using Encryption And Digital Signatures (10.02.2018.)
[284] InterPARES (2002.), The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, http://www.interpares.org/book/index.htm (10.02.2018.)

Kao jedna o prvih tvrdnji u razradi strategije bilježenja traga o elektroničkim potpisima u metapodacima navodi se Boudrezova[285] o tome da zapisi o valjanosti elektroničkog potpisa u metapodacima mogu zamijeniti elektronički potpis za one elektroničko potpisane zapise čije je razdoblje očuvanja trajno. Nadalje se u razradi navedene strategije obrađuju standarde i inicijative za metapodatke: Dublin Core, METS, VRA Core, DIF, PREMIS, FEDORA, XFDU, LOTAR, e-ARK.

Płoszajski zaključuje[286] da su standardi metapodataka koji zaslužuju više pozornosti u kontekstu dugoročnog arhiviranja METS i PREMIS. METS se može koristiti za stvaranje paketa SIP, a namijenjen je sadržavanju metapodataka o pravima, a PREMIS definira obilježja prava koja se odnose na očuvanje aktivnosti i skuplja informacije tijekom pohrane digitalnih objekata u arhivi. PREMIS metapodaci se mogu koristiti za čuvanje hash vrijednosti i elektroničke potpise. te je dan jedan primjer kako se u PREMIS metapodatkovnom objektu pohranjuju elementi elektroničkog potpisa. Za FEDORA metapodatkovni objekt je dan primjer spremanja hash vrijednosti.

Płoszajski u kontekstu standarda za metapodatke i OAIS informacijskih paketa (SIP, AIP i DIP) navodi[287] da se generalno paketi sastoje od: digitalnih objekata (datoteka sa sadržajem i datoteka s metapodacima) i metapodataka s opisom samog paketa. Kao standardi koji podržavaju OAIS informacijske pakete navodi: METS, XFDU, LOTAR i E-ARK.

Strategija bilježenja valjanosti o elektroničkim potpisima u blokchainu je nova strategija kao i sama blokchain tehnologija. Lemieux iznosi tezu[288] da bi blokchain tehnologija mogla promijeniti postojeću paradigmu za vjerodostojne zapise te bi se umjesto korištenja

[285] Boudrez, F. (2007.), Digital signatures and electronic records, Archival Science, ISSN: 1389-0166, str. 190 (179-193)
[286] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 45 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[287] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 47 (15.-61), http://www.springer.com/978-3-319-51800-8 (19.02.2018.)
[288] Lemieux, V. L. (2015.), Blockchain Technology for Recordkeeping, The University of British Columbia, Vancouver, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjo45yquaHZAhWH_ywKHarXDBwQFgg9MAI&url=https%3A%2F%2Fwww.researchgate.net%2Fprofile%2FVictoria_Lemieux%2Fpublication%2F309414363_Blockchain_for_Recordkeeping_Help_or_Hype%2Flinks%2F580f539408ae009606bb62f6%2FBlockchain-for-Recordkeeping-Help-or-Hype.pdf&usg=AOvVaw3BACiNT3YaeubXd3zG54iJ (12.02.2018.)

pouzdane treće strane korisnici mogli okrenuti prema blokchainu. U tu svrhu adresira blokchain i kao mogućnost za zapisivanje valjanosti elektroničkih potpisa. Na konferenciji INFuture 2017 u Zagrebu su Bralić, Kuleš i Stančić prezentirali model za očuvanje valjanosti elektroničkog potpisa u blokchainu[289], TrustChain, kao rezultat istraživanja na projektu InterPARES Trust. Oni predlažu model u kojem bi se pohranjivali kontrolni hashevi ili elektronički potpisi u nepromjenjiv i javno čitljiv blokchain, a svaka zainteresirana strana bi mogla potvrditi da je elektronički potpisan i arhiviran dokument doista ostao nepromijenjen i da je njegov potpis važeći u trenutku stvaranja zapisa u blokchainu. Nedostatak ovog sustava je što nema izravnog rješenja za postojeće potpisane dokumente čiji su potpisni certifikati već istekli. Thompson zaključuje[290] da blokchain donosi velike razvojne mogućnosti za biblioteke, arhive i upravljanje zapisima, ali da s druge strane treba biti oprezan i pažljivo odlučiti u koju svrhu koristiti ovu tehnologiju jer se još ne mogu sagledati krajnji ishodi razvoja takvih sustava.

6. ELEKTRONIČKA JAVNA UPRAVA

U ovom poglavlju će za početak biti obrađena općenita materija vezana za elektroničku javnu upravu: pojam elektroničke uprave, faze elektroničke javne uprave. Zatim će biti obrađena tematika mobilne javne uprave i sektori elektroničke javne uprave.

Posebna pažnja će se posvetiti elektroničkoj javnoj upravi u Europskoj uniji. Bit će navedene strategije, akcijski planovi te općenito kontekst razvoja e-Uprave unutar EU. Posebno bitno za napredak e-Uprave u Uniji je interoperabilnost, računalstvo u oblaku i zaštita podataka.

Na kraju poglavlja će biti dan pregled konteksta razvoja elektroničke javne uprave u Hrvatskoj (strategije, akcijski planovi, uredbe i zakoni) te će se detaljno opisati infrastruktura e-Uprave u Republici Hrvatskoj.

[289] Bralić, V., Kuleš, M., Stančić, H. (2017.), A model for long-term preservation of digital signature validity: TrustChain, Konferencija INFuture 2017: Integrating ICT in Society, https://bib.irb.hr/datoteka/906471.TrustChainV11-final.pdf , str. 2 (18.02.2018.)
[290] Thompson, T. (2017.), The preservation of digital signatures on the blockchain, The University of British Columbia iSchool Student Journal Vol. 3 (Spring 2017), http://ojs.library.ubc.ca/index.php/seealso/article/view/188841/186525 , str. 13. (10.02.2018.)

6.1 OPĆENITO O ELEKTRONIČKOJ JAVNOJ UPRAVI

6.1.1 Pojam elektroničke javne uprave

Danas postoji velik broj inačica pojma elektronička uprava u engleskom jeziku. Za pojam e-Government mogu se pobrojati inačice[291]: electronic government, e-gov, digital government, online government, digital governance, Egovernance, E-governance, electronic governance i dr. Po velikom broju različitog nazivlja za isti pojam se može zaključiti da se radi o području koje se propulzivno mijenja i prilagođava novim potrebama i okolnostima. Od samih definicija se mogu iznijeti par relevantnih definicija.

Gartner grupa definira elektroničku javnu upravu kao kontinuiranu optimizaciju isporuke javnih usluga, izborno sudjelovanje, te transformiranje unutarnjih i vanjskih odnosa u upravi korištenjem novih tehnologija i interneta[292]. Ramadoss i Palanisamy daju sljedeću definiciju[293] (E-governance) kao primjenu elektroničkih sredstava za poboljšanje interakcija vlasti i građana te za povećanje upravne učinkovitosti i učinkovitosti u poslovanju javne uprave. Navedeni autori u istom članku navode i da je to primjena informacijske tehnologije na procese javne uprave koji trebaju omogućiti pametno (engl. smart) upravljanje (SMART – **S**imple, **M**oral, **A**ccountable, **R**esponsive, **T**ransparent). Dakle, ne može se jednostavno izjednačiti elektroničku javnu upravu s procesima digitalizacije procesa ili automatiziranjem usluga javne uprave već je potrebno promatrati e-upravu kroz sveukupnu optimizaciju procesa komunikacije javne uprave s krajnjim korisnicima.

Pregled stanja elektroničke javne uprave UN-a za 2016.[294] (The 2016 United Nations E-Government Survey) je izdan u trenutku kada se mnoge zemlje pripremaju za

[291] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, Hrvoje Brzica, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf, str. 8 (17.03.2018.)
[292] Gartner Group (2000.), Key Issues in E-Government Strategy and Management, Research Notes
[293] Ramadoss, B., Palanisamy, R. (2004.), Issues and challenges in electronic governance planning, https://www.researchgate.net/publication/220082762_Issues_and_challenges_in_e-governance_planning (31.12.2017.)
[294] UN, Department of Economic and Social Affairs (2016.), UN E-Government Survey 2016, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016 (31.12.2017.)

implementaciju Agende 2030 za održivi razvoj. Ovaj Pregled stanja daje novu analizu potencijala elektroničke javne uprave za podršku Agendi 2030 i njezinih 17 ciljeva održivog razvoja. Agenda 2030 navodi[295] da širenje informacijske i komunikacijske tehnologije i globalne povezanosti ima velik potencijal za ubrzavanje ljudskog napretka, za premošćivanje digitalnih podjela i razvijanje društva znanja, kao i znanstvene i tehnološke inovacije u različitim područjima kao što su medicina i energetika. Glavna skupština UN-a je prepoznala u nekoliko slučajeva da informacijske i komunikacijske tehnologije promiču održivi razvoj i podržavaju javne politike i usluge. Istaknuto je da su takve tehnologije omogućile proboj[296] u javnoj upravi i osiguravanju javnih servisa, edukacije, zdravstva i zapošljavanja te u poslovanju, poljoprivredi i znanosti omogućivši tako pristup velikom broju ljudi podacima i uslugama koji su možda ranije bili izvan dohvata ili nedostupni. Generalna skupština UN-a je uz to posebno naglasila potencijal elektroničke javne uprave u promicanju transparentnosti, odgovornosti, učinkovitosti i angažmana građana u pružanju javnih usluga. Pregledi stanja elektroničke javne uprave omogućavaju analizu napretka u korištenju elektroničke javne uprave te mogućnosti u realizaciji međunarodno deklariranih razvojnih ciljeva.

Seifert navodi[297] da elektronička javna uprava ima u puno točaka kontakata s pravnim stečevinama. Takve dodirne točke su: privatnost, pravo na pristup povjerljivom sadržaju, javnost pristupa za informacije javne uprave, informacijsku sigurnost te isporuku javnih usluga. Takva javna uprava se može postići kroz napore u poboljšavanju upravljanja i učinkovitosti javnih informacija i to pomoću tehnoloških resursa. Na taj način se elektronička javna uprava može promatrati kao proces.

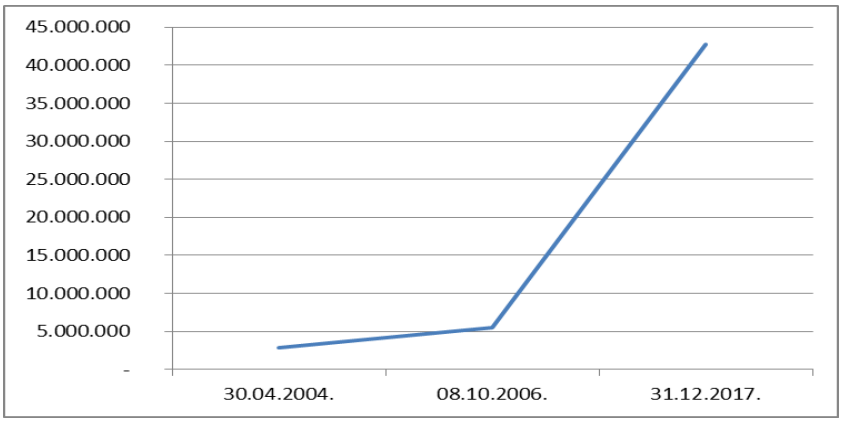
Vrijednost elektroničke javne uprave je što uključuje upotrebu informacijsko komunikacijskih tehnologija (internet, višekanalne isporuke,..) za poboljšavanje isporuke javnih usluga krajnjim korisnicima. Osim toga, tako transformirana javna uprava ima široke mogućnosti spajanja javnih tijela izravno s građanima i drugim krajnjim korisnicima te osigurava isporuku usluga 24/7 (24 sata na dan/sedam dana u tjednu).

[295] UN, Department of Economic and Social Affairs (2015.), Transforming our world: the 2030 Agenda for Sustainable Development, Paragraf 15., https://sustainabledevelopment.un.org/post2015/transformingourworld (31.12.2017.)
[296] Isto, Paragraf 16.
[297] Seifert, J. W. (2003.), A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance, str. 4

U svom magistarskom radu „Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge“[298] zaključujem da se elektronička javna uprava može promatrati kroz transformaciju postojećeg načina rada državne uprave radi kvalitetnijeg služenja svrsi, te kroz učinkovitu isporuku transformiranih usluga okruženju (građanima, poslovnim subjektima i drugim tijelima javne uprave) kroz informacijsku infrastrukturu.

Svakog dana se na internetu povećava broj tema koje obrađuju pojam elektroničke javne uprave. Halachmi u članku “E-Government Theory and Practice: The Evidence from Tennessee (USA)” iznosi podatak da je rezultat pretrage pojma „e-Government“ na tražilici Google na dan 30. travnja 2004. vratio 2.8 milijuna poveznica, dok je pretraga s ključnom riječi globalno zagrijavanje (engl. Global Warming) rezultirala s manje od 700.000 poveznica[299]. U svom magistarskom radu sam iznio podatak da je dana 8. listopada 2006. na tražilice Google na pretragu upita e-Government dobio 5.55 milijuna poveznica[300]. Isto sam pretraživanje obavio i 31. Prosinca 2017. te je s pretragom ključne riječi e-Government kroz tražilicu Google dobio oko 42.70 milijuna poveznica. Manje je bitno za ovaj rad, ali svakako je možda zanimljiv podatak za neke druge znanstvene discipline da je Google pretraživanje ključne riječi Global Warming na dan 31. prosinac 2017. rezultiralo s oko 734 milijuna poveznica. U nastavku je dan prikaz porasta broja poveznica dobivenih pretragom ključne riječi e-Government u Google tražilici kroz godine.

[298] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, Hrvoje Brzica, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf, str. 8 (17.03.2018.)
[299] Halachmi, A., E-Government Theory and Practice: The Evidence from Tennessee (USA), National Center for Public Productivity, Rutgers University, str. 2.
[300] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, Hrvoje Brzica, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf, str. 8 (17.03.2018.)



Slika 36. Prikaz porasta broja poveznica dobivenih pretragom ključne riječi e-Government u Google tražilici kroz godine

6.1.2 Faze elektroničke javne uprave i razine zrelosti usluga

Napredak elektroničke javne uprave nije proces koji se može obaviti u jednom koraku ili fazi. Taj proces ima evolucijska svojstva te se odvija kroz nekoliko faza ili koraka. Faze razvoja elektroničke javne uprave se nadopunjuju. Nove faza ima uporišne elemente koji su realizirani u prethodnoj fazi. U svijetu je u prvom desetljeću 21. stoljeća bilo više modela faza u razvoju elektroničke javne uprave: Svjetske banke, UN-a (Ujedinjenih naroda), te Gartner grupe. Sva ovi modeli pokrivaju otprilike ista područja. Pojedine aktivnosti iz ovih modela se nalaze u ranijim ili kasnijim fazama.

Dokument Svjetske banke „The E-Government Handbook for Developing Countries“ iz 2002.[301] za usmjeravanje elektroničke javne uprave za zemlje u razvoju obuhvaća dobre prakse elektroničkih javnih uprava u svijetu, a osim toga intencija izvješća je davanje smjernica u razvoju. Navedeni dokument definira tri faze u razvoju elektroničke javne uprave:

1. Objava informacija na internetu (engl. Publish)
2. Interakcija (engl. Interact)
3. Transakcija (engl. Transact)

[301] World bank (2002.), The E-Government Handbook for Developing Countries, infoDev and The Center for Democracy & Technology, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN007462.pdf , str. 3 (10.01.2018.)

Faza objave informacija na internetu pokriva objavu informacija javne uprave na internetu. Objavljuju se zakoni, propisi, javni dokumenti i obrasci. Faza interakcije uključuje dvosmjernu komunikaciju između građana i javne uprave. Minimalno nudi kontakt informacije (mail, međuostalim) namijenjene upitima. U fazi transakcije izrađuju se web stranice javne uprave na kojima se može obavljati transakcija putem interneta. Primjeri ovakvih usluga su elektroničko plaćanje, dobivanje građevinske dozvole. S današnjeg stanovišta ovaj model nije dovoljno ambiciozan unatoč jer je više bio namijenjen zemljama u razvoju.

Nakon toga se pojavilo izvješće UN-a koje je ambicioznije u pogledu zacrtanih ciljeva razvoja. Izvješće UN-a za 2005. o globalnom stanju elektroničke javne uprave[302] daje ambicioznije ciljeve u modelu razvoja. Model UN-a ima pet faza:

1. Početna prisutnost (engl. Emerging Presence)
2. Istaknuta prisutnost (engl. Enhanced Presence)
3. Interaktivna prisutnost (engl. Interactive Presence)
4. Transakcijska prisutnost (engl. Transactional Presence)
5. Umrežena prisutnost (engl. Networked Presence)

Faza početne prisutnosti osigurava prikazivanje osnovnih informacija na internetu. Tijela javne uprave u načelu ovakve informacije stavljaju na stranice u obliku statičkog sadržaja uz poveznice na druge bitne sadržaje (druga javna tijela, institucije i sl.).

U drugoj fazi, tj. fazi istaknute prisutnosti je na stranicama javne uprave puno bogatiji sadržaj (zakoni, propisi, izvješća i obrasci). Takve stranice se mogu i pretraživati od strane krajnjih korisnika (pretražuju se baze podataka te repozitoriji javnih dokumenata).

Faza interaktivne prisutnosti (treća faza) obuhvaća usluge koje uključuju interakciju korisnika s javnom upravom. Primjeri takvih usluga su popunjavanje sa stranica skinutih elektroničkih obrazaca. Tijela javne uprave u ovoj fazi daju mogućnost da ih se kontaktira putem telefona, ali i slanjem popunjenih obrazaca elektroničkom poštom, običnom poštom ili faksom. Četvrta faza (Transakcijska prisutnost) podrazumijeva dvosmjernu

[302] United Nations, Department of Economic and Social Affairs (2005.), Global e-government readiness report 2005, New York, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf (11.01.2018.)

komunikaciju između građana i uprave. Dakle, korisnik kontaktira tijela javne uprava, a tijelo javne uprave vraća informacije korisniku. Ovdje su smještene elektroničke javne usluge koje je moguće koristiti od 0 do 24. Primjeri takvih usluga su: dobivanje potvrda o nekažnjavanju, plaćanje poreza i sl. Ova faza uključuje mogućnosti plaćanja poreza preko Interneta, zahtjeve za dozvolama, dobivanje različitih potvrda i uvjerenja. Izuzetno je bitno za ovu uslugu osigurati sigurnu komunikaciju preko interneta jer se radi o osjetljivim transakcijama.

Zadnja, peta faza (Umrežena prisutnost) obuhvaća najnaprednije usluge elektroničke javne uprave. U ovoj fazi se povezuju tijela javne uprave međusobno te s korisnikom. Dakle, tijela javne uprave se integriraju između sebe zbog razmjene podataka. Na ovaj način omogućavaju i građanima ulogu u donošenju odluka, savjetovanje oko nacrta zakona i sl.

Vrlo sličan model kao UN ima i Gartner grupa. Gartner grupa je još 2000. godine objavila model razvoja elektroničke javne uprave u članku „Gartner's Four Phases of E-Government Model“[303]. Ovaj model je kroz svoje nadogradnje je i danas vrlo aktualan. Gartnerov model ima četiri faze:

1. Prisutnost (engl. Presence)
2. Interakcija (engl. Interaction)
3. Transaction (engl. Transakcija)
4. Transformacija (engl. Transformation)

Može se zaključiti da su model UN-a i model Gartner grupe vrlo slični. Razlika je u tome što je izvješće UN-a u svom modelu Gartnerovu fazu web prisutnosti razdijelilo na faze Početne prisutnosti i Istaknute prisutnosti.

Kako bi se lakše moglo usporedno pratiti razvoj elektroničke javne uprave po zemljama, Europska komisija je napravila razlikovanje elektroničkih javnih usluga na one za građane i na one za poslovne subjekte. Takve se usluge grupiraju prema problemima koje rješavaju tako da nema grupiranja usluga po institucijama. Detaljnije o definiranim elektroničkim javnim uslugama će biti navedeno u poglavlju 6.2 Elektronička javna uprava u Europskoj Uniji. Sukladno zadanim smjernicama Europske komisije su utvrđene razine zrelosti (ili

[303] Di Maio, B. (2000.), Gartner's Four Phases of E-Government Model, Gartner Group, November 2000, str. 1

razine informatiziranosti) po kojima se mjeri dostupnost javnih usluga na internetu. Svaka elektronička javna usluga definirana je različitim razinama zrelosti ili informatiziranosti.

Navedene razine zrelosti se mjere od 1 do 5 te imaju određeno značenje[304]:

1. Informacija: na mreži je dostupna samo informacija o usluzi (npr. opis postupka).
2. Jednosmjerna interakcija: dostupnost formulara u e-obliku za pohranjivanje na računalu, prazne formulare moguće je otisnuti na pisaču.
3. Dvosmjerna komunikacija: interaktivno ispunjavanje formulara i prijava uz autentifikaciju, ispunjavanjem formulara pokreće se pojedina usluga.
4. Transakcija: cijela usluga je dostupna na mreži, popunjavanje formulara, autentifikacija, plaćanje i isporuka potvrda, narudžbe ili drugi oblici potpune usluge putem mreže.
5. Ciljana usluga (proaktivnost/automatizacija): obavljanje usluge je proaktivno /automatizirano na način da se od korisnika traži samo potvrda ili suglasnosti.

Prvotno su definirane razine informatiziranosti koje se mjere na skali od 0 do 4. Te su razine definirane još 1994. Bangemannovim izvještajem[305], a značenje im je navedeno u tablici 5.

Tablica 5: Razine informatiziranosti elektroničkih javnih usluga definirane Bangemannovim izvještajem

Razina informatiziranosti	Naziv razine	Opis
0	Nema informacije	Informacija o usluzi nije dostupna na mreži ili pružatelj usluge nema web stranicu
1	Informacija	Na mreži je dostupna samo informacija o usluzi (npr. opis postupka)
2	Jednosmjerna interakcija	Dostupnost formulara u elektroničkom obliku za pohranjivanje na računalu. Prazne formulare moguće je i otisnuti na pisaču
3	Dvosmjerna komunikacija	Interaktivno ispunjavanje formulara i prijava uz autentifikaciju. Ispunjavanjem formulara pokreće

[304] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630, str. 27 (10.01.2018.)
[305] Bangemann, M. et al. (1994.), Europe and the global information society, Bangemann report recommendations to the European Council, High-Level Group on the Information Society, http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (10.01.2018.)

		se pojedina usluga
4	Transakcija	Cijela usluga je dostupna na mreži, popunjavanje formulara, autentifikacija, plaćanje i isporuka potvrda, narudžbe ili drugi oblici potpune usluge

Akcijski plan Europske komisije za razvoj elektroničke javne uprave[306] predstavljen u travnju 2006. godine (i2010 eGovernment Action Plan) proširuje razina informatiziranosti sa stupnjem 5. Ovaj stupanj definira obavljanje iterativnih usluga. To su usluge koje se zakonski svake godine ponavljaju, npr. prijava poreza putem interneta. Ovakva vrsta usluga automatski se obavlja, a korisnici primaju obavijest o izvršenju putem web aplikacija, mobilnih uređaja i sl.

Tablica 6: Peta razina informatiziranosti elektroničkih javnih usluga koja je dopunila Bangemannov izvještaj

Razina informatiziranosti	**Naziv razine**	**Opis**
5	Iteracija	Usluge koje se ponavljaju (npr. prijava poreza), automatsko izvršavanje, automatsko obavještavanje korisnika o izvršenju usluge

U izvješću eGovernment Benchmark 2016 Background Report[307] pripremljenom za Europsku komisiju navedeni su sljedeći nazivi za razine 0-5:

- Offline (0, Nema informacije)
- Information online but not through portal (1, Informacija)
- Information online and through portal (2, Jednosmjerna interakcija)
- Service online but not through portal (3, Dvosmjerna komunikacija)
- Service online and through portal (4, Transakcija)
- Automated service (5, Iteracija)

Više konkretnih rezultata o istraživanjima na temelju navedenih pet razina informatiziranosti/zrelosti javnih usluga bit će navedeno u sljedećim poglavljima ovog rada.

[306] Europska komisija (2006.), i2010 eGovernment Action Plan, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24226j (10.01.2018.)
[307] Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856 (21.03.2018.)

6.1.3 Mobilna javna uprava i važnost razvoja infrastrukture

Elektronička javna uprava ima velike koristi od inovativnog oblika informiranja i poboljšanih načina komuniciranja s krajnjim korisnicima. Posebno se to odnosi na korištenje interneta i poboljšavanje osnovnih funkcija javne uprave. Navedene funkcije se sve više mogu unaprijediti i korištenjem mobilnih i bežičnih tehnologija te korištenjem novog kanala isporuke za javne usluge, mobilnu javnu upravu (m-upravu). Kushchu i Kuscu[308] definiraju mobilnu javnu upravu (m-upravu) kao strategiju i njezine implementacije uključujući upotrebu bežične i mobilne tehnologije, usluga, aplikacija i uređaja za poboljšanje koristi za strane uključene u elektroničku javnu upravu, uključujući građane, tvrtke i sva vladina tijela. Kushchu i Kuscu u svom članku „Mobile Government" napominju[309] da dolazeće razdoblje m-uprave donosi nekoliko pitanja. Jedno od zanimljivijih je: hoće li m-uprava zamijeniti aktivnosti e-uprave? Navedeni autori odmah daju odgovor da se unatoč svom značaju, m-uprava ne može promatrati kao zamjena za e-upravu te da će u mnogim slučajevima biti komplementarna naporima e-uprave. Nadalje, navode da konvencionalna elektronička javna uprava osigurava servise kroz žičane mreže s interaktivnim i relativno inteligentnim aplikacijama te da vrijednost mobilne javne uprave dolazi iz aplikacija koje podržavaju mobilnost građana, poduzeća i internih procesa javne uprave.

Kushchu i Kuscu opisuju[310] i značajke mobilne javne uprave:

- Velika pristupačnost i dostupnost – m-uprava potiče veće korištenje vladinih usluga kroz poboljšanu pristupačnost i dostupnost. Građani mogu koristiti mobilne javne servise ne samo u bilo koje vrijeme već i od bilo kuda.
- Mobilni uređaji su uvijek uključeni što je velika razlika naspram osobnih računala jer su mobilni uređaji većinom uvijek uključeni. Uobičajeno ovakvi uređaji mogu biti u neaktivnom stanju zbog nekorištenja, ali aplikacije mogu „probuditi" uređaj.
- Mobilni uređaji su dizajnirani tako da se mogu prenositi uokolo. Kako ih korisnici uvijek nose sa sobom, mobilne aplikacije mogu biti dizajnirane da osiguraju svježe informacije za korisnika.

[308] Kushchu, I., Kuscu, H. (2003.), From E-government to M-government: Facing the Inevitable, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan045367.pdf (21.03.2018.)
[309] Kushchu, I., Kuscu, H., Mobile Government, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040049.pdf , str. 1 (31.12.2017.)
[310] Kushchu, I., Kuscu, H., Mobile Government, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040049.pdf , str. 4 (31.12.2017.)

- Bolja preciznost i prilagodba ciljanim korisnicima i isporuci sadržaja – osobno računalo može biti dijeljeno između više različitih korisnika, ali mobilni uređaji su dizajnirani za korištenje od strane jednog korisnika. To znači da osobni podaci mogu doći do istog korisnika u bilo kojem trenutku putem tog određenog uređaja.
- Veća i šira korisnička baza – mobilna javna uprava doseže veći broj korisnika kroz mobilne uređaje što često daleko premašuje korisničku zajednicu žičanog interneta. Mobilna javna uprava dolazi do raznih publika, uključujući korisnike koji nisu imali niti edukaciju niti iskustvo u radu s osobnim računalima, ali su zato aktivni korisnici mobilnih komunikacija.

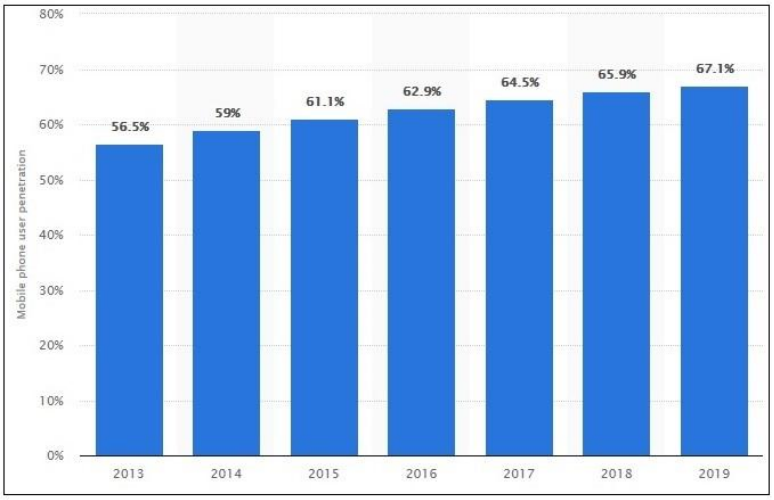
Kushchu i Kuscu navode[311] i glavna pitanja za mobilnu javnu upravu:

- Pokretači mobilne javne uprave – postoje različiti tehnološki i netehnološki pokretački faktori za mobilnu javnu upravu:
    - Povećava se i poboljšava mobilna infrastruktura i penetracija mobilnih uređaja u svijetu.
    - Mobilne internetske tehnologije evoluiraju, standardi i protokoli omogućavaju rad bržim i boljim aplikacijama i prilagodbu potrebama krajnjih korisnika.
- Tranzicija iz elektroničke javne uprave u mobilnu javnu upravu
    - Korištenje m-uprave je neizbježno – glavne značajke koje utječu na usvajanje m-uprave su: velik je tehnološki napredak u mobilnim tehnologijama, povećavaju se koristi koje krajnji korisnici mogu imati iz razvoja usluga m-uprave, povećavaju se očekivanja građana za boljim i praktičnijim uslugama javne uprave.
    - Mobilna javna uprava će biti komplementarna s elektroničkom javnom upravom – neke usluge m-uprave su replikacije usluga e-uprave na mobilnim uređajima. Sinergija između e-uprave i m-uprave može biti od posebnog interesa za one zemlje koje su već uložile znatna ulaganja u implementaciju e-uprave.
- Implementacijski izazovi
    - Izgradnja bežičnih i mobilnih mreža i popratne infrastrukture
    - Povećanje mobilne penetracije i povećavanje pristupačnosti

[311] Isto, str. 5

- Zaštita privatnosti i osiguravanje sigurnosti za podatke i transakcije
- Reguliranje i razvijanje pravnih aspekata mobilnih aplikacija i korištenja servisa

Budući da penetracija mobilnih uređaja (posebno pametnih telefona, engl. smartphones) postaje sve bitnija za napredak m-uprave (te općenito e-uprave) zanimljivo je pogledati kretanje udjela korištenja mobilnih uređaja u svjetskoj populaciji od 2013. do 2019. godine (uz projekciju) na slici 37 sa statističkog portala Statista.



Slika 37. Kretanje udjela korištenja mobilnih uređaja u svjetskoj populaciji od 2013. do 2019. godine (uz projekciju), preuzeto sa Statista.com [312]

Vidljivo je da se svake godine postotak povećava, ali s tendencijom usporavanja rasta (2014. je rast korištenja mobilnih uređaja bio 2,5 %, a projekcija za 2019. je da će rast biti 1,2 %). Ipak, postotak za današnjih oko 65% korisnika mobilnih uređaja znači da dvoje od troje ljudi na svijetu koristi takav uređaj što je vrlo visoko i povoljno kao baza za m-upravu.

Zanimljivu statistiku (top lista zemalja svijeta po penetraciji pametnih telefona) je objavljena na Wikipediji (uz napomenu da su brojke preuzeli iz Newzoo Global Mobile Market izvještaja iz travnja 2017.). Taj izvještaj se temelji na modelu koji uzima u obzir ekonomsku razvijenost zemlje, demografiju, online populaciju i nejednakosti). Navedena statistika (za top 20 zemalja) će biti prikazana u tablici 7.

[312] Statista.com (2018.), Mobile phone user penetration as percentage of the population worldwide from 2013 to 2019*, https://www.statista.com/statistics/470018/mobile-phone-user-penetration-worldwide/ (01.01.2018.)

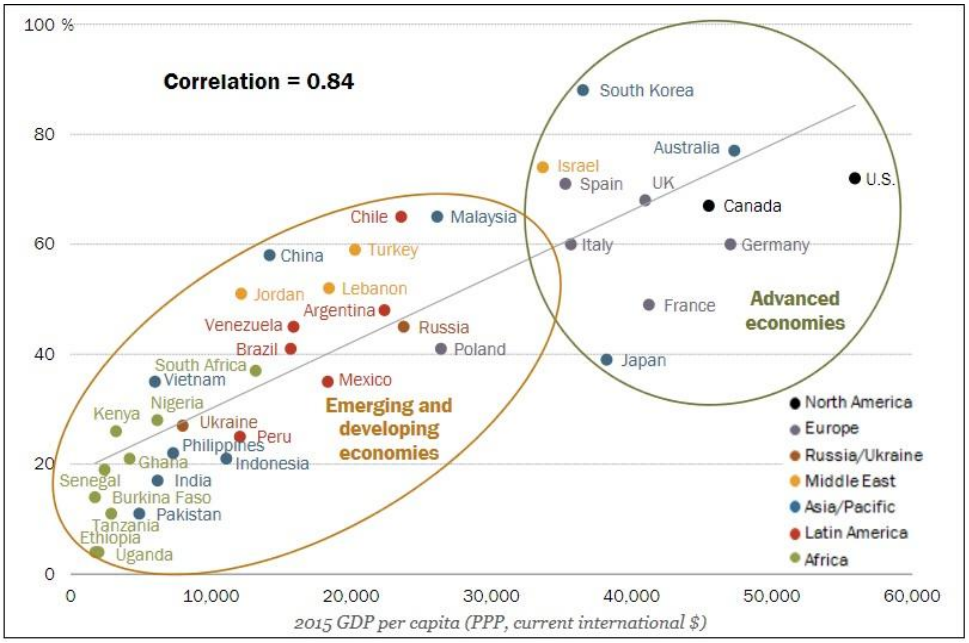
Tablica 7. Top lista zemalja svijeta po penetraciji pametnih telefona, preuzeto s wikipedije[313]

Mjesto	Zemlja	Stanovnika	Penetracija pametnih telefona	Apsolutni broj korisnika pametnih telefona
1	UAE	9,398,000	80.6%	7,573,000
2	Švedska	9,921,000	72.2%	7,167,000
3	Švicarska	8,454,000	71.7%	6,061,000
4	Južna Koreja	50,705,000	71.5%	36,262,000
5	Tajvan	23,564,000	70.4%	16,596,000
6	Kanada	36,626,000	69.8%	25,556,000
7	SAD	326,474,000	69.3%	226,289,000
8	Nizozemska	17,033,000	68.8%	11,720,000
9	Njemačka	80,636,000	68.8%	55,492,000
10	Ujedinjeno Kraljevstvo	65,511,000	68.6%	44,953,000
11	Australija	24,642,000	67.7%	16,671,000
12	Belgija	11,444,000	67.3%	7,706,000
13	Španjolska	46,070,000	66.8%	30,771,000
14	Azerbejdžan	9,974,000	66.4%	6,619,000
15	Italija	59,798,000	65.8%	39,323,000
16	Francuska	64,939,000	65.3%	42,399,000
17	Saudijska Arabija	32,743,000	65.2%	21,337,000
18	Portugal	10,265,000	65.0%	6,672,000
19	Češka	10,555,000	64.8%	6,835,000
20	Malezija	31,164,000	64.1%	19,967,000

Iz tablice 7 se da zaključiti da su većina ovih zemalja i najrazvijenije zemlje svijeta s dostupnom mobilnom infrastrukturom i velikom kupovnom moći. Wikipedia na istoj stranici donosi i istraživanje iz 2016. godine od Pew istraživačkog centra (engl. Pew Research Center)[314] kod kojeg je poredak malo drugačiji, ali među prvih deset opet su vrlo razvijene zemlje (1. Južna Koreja 88%, 2. Australija 77%, 3. Izrael 74%, 4. SAD 72%, 5. Španjolska 71%, 6. Novi Zealand 70%, 7. Velika Britanija 68%, 8. Kanada 67%, 9. Čile 65%, 10. Malezija 65%).

[313] Wikipedia.org, List of countries by smartphone penetration, https://en.wikipedia.org/wiki/List_of_countries_by_smartphone_penetration (01.01.2018.)
[314] Pew Research Center, http://www.pewresearch.org/ (03.01.2018.)

Nastavno na taj zaključak vrlo je zanimljiva studija iz veljače 2016. koju je izradio Jacob Poushter (Pew Research Center)[315]. Studija nosi naziv „Broj vlasnika pametnih telefona i internet korisnika se nastavlja penjati, ali razvijene ekonomije još imaju više razine korištenja tehnologije“ (engl. Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use). Autor je u nazivu studije već opisao glavni trend zadnjih godina prikazan i na Wikipediji (Newzoo Global Mobile Market izvještaj). Na slici 38 je dan prikaz postotka vlasništva nad pametnim telefonima po zemljama svijeta. Izrazitije je posjedovanje u razvijenim gospodarstvima. Navedena studija je dala zaključak da postoji velika korelacija između bogatstva zemlje i vlasništva nad pametnim telefonima (0,84). Što je zemlja bogatija i pametni telefoni su cjenovno dostupniji.

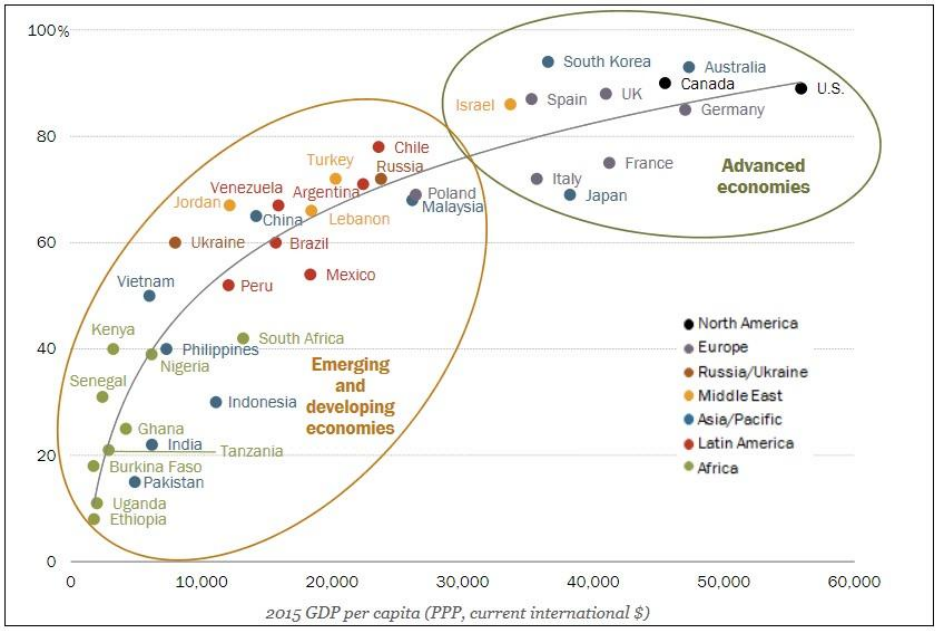


Slika 38. Vlasništvo pametnih telefona je izraženije u razvijenim gospodarstvima, preuzeto iz Poushter, J. (2016.)[316]

[315] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ (01.01.2018.)

[316] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ , str. 17 (01.01.2018.)

Osim toga, ova studija daje prikaz odnosa veličine BDP-a i pristupa interneta po zemljama u svijetu (što je bitno i za širenje e-uprave i m-uprave). Studija zaključuje da postoji vrlo jaka korelacija (0,87) između bogatstva zemlje (mjereno BDP-om) i pristupa internetu. Siromašnije zemlje kao što su u Južnoj i Jugoistočnoj Aziji imaju daleko manju razinu pristupa interneta u usporedbi s zemljama u razvoju u Južnoj Americi te posebno s razvijenim zemljama u Europi, Sjevernoj Americi i Australiji i Oceaniji.



Slika 39. Jaka veza između veličine BDP-a i pristupa internetu, preuzeto iz Poushter, J. (2016.)[317]

Više o korelaciji penetracije pametnih uređaja i pristupa internetu i uspješnosti elektroničke javne uprave će biti dano u poglavlju 6.1.4 Sektori elektroničke javne uprave.

S obzirom na upravo prikazane postotke pristupa internetu iz 2016. zanimljivo se danas čini i istraživanje iz 2006. koje sam naveo u svom magistarskom radu[318], a preneseno je svojevremeno sa stranice „Internet World Stats – Usage and Population Statistics“. donose istraživanje o korištenju Interneta u svijetu, populacijskoj statistici, te postocima korištenja

[317] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/, str. 9 (01.01.2018.)

[318] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, Hrvoje Brzica, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf (17.03.2018.)

po kontinentima[319]. S obzirom na istraživanje iz 2006., 3. siječnja 2017. sam nanovo povukao podatke sa iste stranice (podatke koji su objavljeni 30. lipnja 2017.)[320] te sam napravio komparativnu tablicu s poljima: korisnici interneta, udio internetskih korisnika, rast korištenja.

Tablica 8. Komparativna tablica rasta korisnika interneta iz napravljena po podacima iz izvješća „Internet World Stats – Usage and Population Statistics" iz 2006. i 2017. godine

Kontinent /Regija	Broj korisnika interneta (2006.)	Broj korisnika interneta (30.06.2017.)	Udio (%) internetskih korisnika (2006.)	Udio (%) internetskih korisnika (30.06.2017.)	Rast korištenja 2000-2006	Rast korištenja 2000-2017
Afrika	32.765.700	388.376.491	3.6 %	31.2 %	625,8 %	8.503,1%
Azija	394.872.213	1.938.075.631	10.8 %	46.7 %	245,5 %	1.595,5%
Europa	308.712.903	659.634.487	38.2 %	80.2 %	193,7 %	527,6%
Srednji Istok	19.028.400	404.269.163	10.0 %	62.4 %	479,3 %	2.137,4%
Sjeverna Amerika	229.138.706	146.972.123	69.1 %	58.7 %	112,0 %	4.374,3%
Južna i srednja Amerika	83.368.209	320.059.368	15.1 %	88.1 %	361,4 %	196,1%
Australija i Ocean.	18.364.772	28.180.356	54.1 %	69.6 %	141,0 %	269,8%
UKUPNO:	1.086.250.903	3.885.567.619	16.7 %	51.7 %	200,9 %	976,4%

Iz podataka iz 2006. je vidljivo da su najrazvijenije svjetske regije (Sjeverna Amerika, Europa i Australija) imale tada velike udjele internet korisnika što već tada dovoljno govori o prepoznavanju važnosti tehnološke platforme za uspješan gospodarski razvoj, a samim time i za elektroničku javnu uprave. Europa 2006. nije po penetraciji interneta bila dostigla Sjevernu Ameriku, ali je od tada ubrzano radila na razvoju infrastrukture (posebno širokopojasnog interneta i mobilnih mreža) te na zajedničkim okosnicama za elektroničku javnu upravu (što će biti obrađeno u poglavlju 6.2 Elektronička javna uprava u Europskoj Uniji). Iz podataka iz 2017. se može potvrditi trend koji je Poushter[321] opisao studijom naziva „Broj vlasnika pametnih telefona i internet korisnika se nastavlja penjati, ali razvijene ekonomije još imaju više razine korištenja tehnologije". Dakle, vidljivo je da i

[319] Internet World Stats (2006.), Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (18.09.2006.)
[320] Internet World Stats (2018.), Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (03.01.2018.)
[321] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ (01.01.2018.)

nerazvijeni kontinenti i regije imaju velike skokove u penetraciji internet infrastrukture (npr. Afrika, Srednji Istok), ali da je to još daleko od penetracije koju imaju primjerice Sjeverna Amerika i Europa.

6.1.4 Sektori elektroničke javne uprave

Elektronička javna uprava podrazumijeva širok raspon usluga. Usluge mogu biti od upita za status pojedinog upravnog akta pa do zahtjeva i preuzimanja službene isprave. Usluge uključuju i prijave poreza, ostvarivanje socijalnih prava, javne nabave, upise u škole i fakultete i dr. Postoje elektroničke javne usluge koje su namijenjene za građane i one koje su namijenjene za poslovne subjekte, a postoje i elektroničke javne usluge koje koriste sami zaposlenici javne uprave. Dakle, možemo govoriti o različitim sektorima u koje se svrstavaju elektroničke javne usluge. Sektori elektroničke javne uprave se definiraju prema odnosu između sudionika elektroničke javne uprave. Seifert u izvješću „A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance" navodi da se elektroničke javne usluge mogu svrstati u četiri sektora[322]:

- G2C (engl. Government to Citizens) – to je sektor u kojem su elektroničke usluge javne uprave koje su namijenjene građanima. Ove usluge su u kategoriji omogućavanja lakše interakcije građana i vlade. To je i vrlo bitan cilj e-uprave. U ovom sektoru se omogućavaju transakcije za građane, a to mogu biti: dobivanje raznih dozvola i isprava, prijava poreza. Za građane je bitno da uslugu obave što jednostavnije i da uštede na vremenu. Javna uprava ima interes unaprijediti svoje poslovne procese da može biti kvalitetniji servis građanima. U olakšavanju pružanja ovakvih usluga je i formiranje „One stop shop" ekstenzija javne uprave gdje se na jednom mjestu građanima želi omogućiti dostupnim više usluga radi olakšavanja interakcije. To je jedinstveno mjesto na kojem građani mogu obavljati više usluge, a bitne su usluge koje zahtijevaju suradnju više tijela javne uprave. Građanima je prednost to što onda ne trebaju kontaktirati svako tijelo javne uprave zasebno.

[322] Seifert, J. W. (2003.), A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance, https://fas.org/sgp/crs/RL31057.pdf , str. 6 (21.03.2018.)

- G2B (engl. Government to Business) – je sektor elektroničke javne uprave koji obuhvaća usluge javne uprave poslovnim subjektima. To su vrlo bitne usluge koje su u fokusu javnosti zbog interesa poslovnog sektora da se smanje troškovi poslovanja i da se brže i kvalitetnije obave usluge s javnim sektorom. Vrlo bitne usluge u ovom sektoru su javne nabave kojim se mogu postići velike uštede za javni sektor. Postoje i usluge javnih dražbi koji su prilika javnom sektoru za unovčenjem svojih nekretnina i drugih vrijednosti, a poslovnom sektoru za kupovinu po povoljnim cijenama.
- G2E (engl. Government to Employees) – to je sektor u kojem se nalaze elektroničke usluge koje koriste djelatnici javne uprave. Ovakvim uslugama se moderniziraju i optimiziraju poslovni procesi javne uprave. Olakšava se delegiranje radnih zadataka djelatnicima (engl. workflow management). U ovom sektoru su i usluge koje se nude preko web portali javne vlasti kojima djelatnici javne uprave pristupaju radi pristupa bazama znanja (engl. Knowledge management). Ovakvi web portali omogućavaju optimizaciju poslovnih procesa i tokova podataka unutar tijela javne vlasti. Time se mogu smanjiti troškovi, ali se i povećava interna efikasnost unutar javnih tijela.
- G2G (engl. Government to Government) – ovaj sektor elektroničke javne uprave je vrlo bitan za funkcioniranje cjelokupne e-uprave kao ključan faktor. Ovdje su smješteni servisi koji razmjenjuju podatke između tijela javne vlasti. Podaci se razmjenjuju elektroničkim putem između javnih djelatnika na više razina (državna, regionalna, lokalna). Tijela javne uprave na taj način ostvaruju suradnju unutar iste transakcije koju treba obaviti, a moguće je i zajedničko korištenje baza podataka (npr. porezne uprave). Dakle, ovdje je bitno učiniti napore za optimizacijom, tj. reinženjeringom poslovnih procesa. Osim toga, potrebno je omogućiti upravljanje podacima i dokumentima za više zaposlenika unutar jednog ili više tijela javne uprave. Kao i u poslovnom sektoru i ovdje su bitni ERP (engl. Enterprise Resource Planning) sustavi[323] za upravljanje javnim resursima, novčanim transakcijama i dr.

[323] Panian Ž. (2005.), ERP sustav – Poslovno-upravljački sustav koji povezuje sve dijelove i faze poslovanja, uključujući planiranje, proizvodnju, prodaju i marketing, Informatički enciklopedijski rječnik @-L, Europapress holding Zagreb, str. 197.

6.2 ELEKTRONIČKA JAVNA UPRAVA U EUROPSKOJ UNIJI

6.2.1 Kontekst razvoja elektroničke javne uprave i Digitalna agenda

Strategiju Europa 2020 (Europska strategija za pametan, održiv i uključiv rast)[324] je Europska komisija (u daljnjem tekstu EK) objavila u ožujku 2010. godine. Navedenu strategiju EK donosi u trenucima ekonomske recesije i neizvjesnosti gospodarskog rasta. Namjera donošenja te strategije je bila napraviti Europsku uniju otporniju na krize i napraviti od unije pametnu, održivu i uključivu ekonomiju koja isporučuje visoke razine zaposlenosti, produktivnosti i socijalne kohezije. Europa 2020 postavlja tri prioriteta[325]:

- Pametni rast (engl. Smart growth) - razvijanje gospodarstva utemeljenog na znanju i inovacijama,
- Održivi rast: promicanje učinkovitije, zelene i konkurentnije ekonomije,
- Uključivi rast: poticanje gospodarstva s visokim zapošljavanjem koje pruža socijalnu i teritorijalnu koheziju.

EU kroz Europu 2020 definira gdje želi biti 2020. Dakle, do navedene godine Europska komisija predlaže sljedeće glavne ciljeve EU:

- 75 % populacije od 20 do 64 godine bi trebala biti zaposlena,
- 3% EU BDP-a bi trebalo investirati u istraživanje i razvoj,
- trebali bi biti dostignuti "20/20/20"[326] klimatsko/energetski ciljevi,
- Postotak učenika koji odustaju u školovanju u ranoj fazi bi trebao pasti ispod 10%, a barem 40% mlađe generacije bi trebalo steći više ili visoko obrazovanje,
- 20 milijuna manje ljudi bi trebalo biti u riziku od siromaštva.

Kako bi se osiguralo da svaka država članica EU prilagodi strategiju Europa 2020 za svoje prilike, EK je predložila da se ciljevi EU uključe u nacionalne ciljeve i planove.
Europska komisija predlaže sedam glavnih inicijativa za kataliziranje napretka u okviru postavljenih prioriteta[327]:

[324] Europska komisija (2010.), Europa 2020, Europska strategija za pametan, održiv i uključiv rast, https://mzo.hr/sites/default/files/migrated/europa-2020.pdf (12.01.2018.)
[325] Isto, str. 3
[326] Europska komisija, 2020 climate & energy package, https://ec.europa.eu/clima/policies/strategies/2020_en (13.01.2018.)

1. Unija inovacija - s ciljem unapređenja okvirnih uvjeta i dostupnosti financiranja za istraživanje i inovacije kako bi se osigurala mogućnost transformacije inovativnih ideja u proizvode i usluge koje stvaraju rast i radna mjesta.
2. Mladi u pokretu - s ciljem povećanja učinka obrazovnih sustava i olakšanja ulaska mladih na tržište rada.
3. Digitalna agenda za Europu - s ciljem bržeg širenja brzog interneta te korištenja prednosti jedinstvenog digitalnog tržišta za kućanstva i tvrtke.
4. Resursno učinkovita Europa - s ciljem razdvajanja ekonomskog rasta od korištenja resursa, podrške prijelazu na ekonomiju koja koristi male razine ugljena, povećanja korištenja obnovljivih izvora, modernizacije sektora transporta i promicanja energetske učinkovitosti.
5. Industrijska politika za globalizacijsko doba - s ciljem unapređenja poslovnog okruženja, prvenstveno za male i srednje poduzetnike, te razvoja snažne i održive globalno konkurentne industrijske osnove.
6. Program za nove vještine i radna mjesta - s ciljem modernizacije tržišta rada te osnaživanja ljudi razvojem njihovih vještina tijekom cijeloga života s ciljem povećanog sudjelovanja radne snage te boljeg slaganja ponude i potražnje, uključujući i mobilnost radne snage.
7. Europska platforma protiv siromaštva - s ciljem jamčenja društvene i teritorijalne povezanosti na način da svi imaju koristi od prednosti rasta i radnih mjesta te da se ljudima koji pate od siromaštva i socijalne isključenosti omogući dostojanstven život i aktivno sudjelovanje u društvu.

Treća inicijativa, Digitalna agenda za Europu[328] (u daljnjem tekstu Digitalna agenda) je strateški kontekst koji je u narednom razdoblju najviše odredio smjer razvoja elektroničke javne uprave za zemlje EU i zemlje kandidate. Inicijativa Digitalna agenda je pokrenuta u svibnju 2010. godine. Digitalna agenda propisuje 101 mjeru koje su grupirane u 7 prioritetnih područja djelovanja na razini Europske unije.

[327] Europska komisija (2010.), Europa 2020, Europska strategija za pametan, održiv i uključiv rast, https://mzo.hr/sites/default/files/migrated/europa-2020.pdf , str. 6 (12.01.2018.)
[328] Europska komisija (2010., 2.), Digital agenda for Europe, Rebooting Europe's economy, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (12.01.2018.)

Digitalna agenda ima više stupova. Prvi stup Digitalne agende je Jedinstveno digitalno tržište[329] (engl. Digital Single Market). Ovaj stup sadrži 21 mjeru kojom se nastoji potaknuti promet s internetskim sadržajima i uspostaviti jedinstveni okvir za elektronička plaćanje. Osim toga, nastoji se osigurati zaštita potrošača u digitalnom okruženju. Ključna aktivnost za razvoj jedinstvenog digitalnog tržišta je osiguravanje prekograničnih usluga elektroničke javne uprave. Digitalna agenda je popis ciljeva koji bi (uz primjenu tehnologije) trebali unijeti pozitivne promjene u živote ljudi. Digitalna agenda ima za ciljeve sljedeće:

- stvoriti jedinstveno digitalno tržište,
- unaprijediti okvir za interoperabilnost između informacijsko-komunikacijskih produkata i usluga,
- potaknuti povjerenje i sigurnost poslovanja na internetu,
- osigurati brzi i ultrabrzi pristup internetu,
- povećati istraživanje i inovacije,
- unaprijediti digitalnu pismenost.

Digitalna agenda propisuje da države članice EU trebaju podržati inovativna, prekogranična rješenja elektroničke javne uprave. Posebno se to odnosi na osiguravanje sljedećih rješenja:

- Punu interoperabilnost usluga elektroničke javne uprave. Potrebno je premostiti sljedeće barijere: pravne, organizacijske, tehničke i semantičke te podržati uvođenje najnovije verzije IPv6[330] internet protokola,
- Točke jedinstvenog kontakta trebaju biti punopravni centri za elektroničke javne uprave i trebaju pružati usluge koje osiguravaju zahtjeve koji su zadani u Direktivi o uslugama,
- Zajednička lista ključnih prekograničnih usluga. Ona će odgovarati uslugama određene svrhe: poduzetnici trebaju moći uspostaviti i obavljati poslovne aktivnosti bilo gdje u Europskoj uniji, studenti bi trebali moći studirati, a umirovljenici bi trebali moći biti u mirovini bilo gdje u EU.

[329] Europska komisija, Jedinstveno digitalno tržište, https://ec.europa.eu/commission/priorities/digital-single-market_en (12.01.2018.)
[330] IPv6, Internet protokol verzija 6, https://hr.wikipedia.org/wiki/IPv6 (13.01.2018.)

Bitno je napomenuti da Europska komisija daje ocjenu napretka u postizanju ciljeva Digitalne agende u zemljama Europske unije predstavljajući rezultate u okviru godišnjih izvješća naslovljenih s „Digital Agenda Scoreboard“, tj. semafor Digitalne agende[331].

Na osnovu propisanih strategija se definiraju i akcijski planovi za razvoj elektroničke javne uprave. Akcijski plan za elektroničku javnu upravu za razdoblje 2016. - 2020.[332] ima sljedeće prioritete:

1. Digitalizacija procesa javne uprave,
2. Unapređenje prekogranične interoperabilnosti javne uprave,
3. Osiguranja digitalne interakcije javne uprave i krajnjih korisnika.

Cilj provedbe ovog akcijskog plana je da se do 2020. postigne sljedeće:

- napraviti javne uprave otvorenim, učinkovitim i uključivim,
- građanima i poduzećima pružati personalizirane elektroničke javne usluge, a po potrebi i prekogranične

Strategiji Europa 2020 su prethodili druge strategije, akcijski planovi i vizije. Europska komisija je u lipnju 2013. objavila dokument „A vision for public services“[333]. Cilj ovog dokumenta je stvaranje okvira dugoročne vizije modernog i otvorenog javnog sektora te načina na koji javne usluge mogu biti isporučene u otvorenoj upravi. Osnova otvorene uprave su informacijsko komunikacijske tehnologije. Dakle, cilj je bio pripremiti okvir za pružanje jednoznačnih javnih usluga građanima i poslovnim subjektima koje će se moći koristiti od 0-24.

Akcijski plan Europske komisije koji je prethodio planu za razdoblje 2016. - 2020 je bio onaj za razdoblje 2011.-2015.[334]. EK je navedeni plan predložila kao put ostvarivanja ambiciozne vizije napretka elektroničke javne uprave sadržane u deklaraciji donesenoj na

[331] Europska komisija, Digital Agenda Scoreboard, https://ec.europa.eu/digital-single-market/en/digital-scoreboard (13.01.2018.)
[332] Europska komisija (2016.), EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268 (13.01.2018.)
[333] Europska komisija (2013.), A vision for public services, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3179 (13.01.2018.)
[334] Europska komisija (2010., 3.), The European eGovernment Action Plan 2011-2015, Harnessing ICT to promote smart, sustainable & innovative Government, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF (13.01.2018.)

5. ministarskoj razini „Deklaracija iz Malmöa“[335]. Akcijski plan 2011.-2015. promovira novu generaciju usluga elektroničke javne uprave te navodi četiri politička prioriteta za sve europske javne uprave za petogodišnje razdoblje (navedeni prioriteti su ustanovljeni u Deklaraciji iz Malmöa):

1. Osnaživanje građana i tvrtki putem usluga elektroničke javne uprave,
2. Poticanje mobilnosti na jedinstvenom tržištu za omogućavanje i unaprjeđivanje poslovanja, studiranja, življenja, boravka i umirovljenja bilo gdje u Europskoj uniji,
3. Omogućavanje učinkovitosti i djelotvornosti uz korištenje elektroničke javne uprave (smanjivanje administrativnih barijera, poboljšavanje organizacijskih procesa i promicanje održive, ekološki usmjerene ekonomije s niskom razinom ugljičnih plinova),
4. Osiguravanje ključnih preduvjeta za provedbu prioriteta. Pravni preduvjeti su otvorenost specifikacija i interoperabilnost. Tehnički preduvjeti su: elektronička identifikacija (eID), elektronički potpisi (engl. eSignature), elektronički dokumenti (engl. eDocuments), autentični izvori (engl. Authentic Sources), elektronička sigurnost (engl. eSafe), te jednokratna prijava (engl. SSO, Single Sign On).

Akcijski plan 2011.-2015. postao je temelj razvoja velikih infrastrukturnih projekata kao podloga za stvaranje inovativnih prekograničnih rješenja: STORK, e-SENS, SPOCS, PEPPOL, epSOS, eCODEX. Slijede kratki opisi navedenih projekata.

STORK[336] (engl. **S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed) – cilj projekta je stvoriti u Europskoj uniji interoperabilan, prekogranični sustav koji će služiti za verifikaciju elektroničkih identiteta. Nacionalni sustav elektroničkog identiteta pojedine države bi se trebao moći koristiti u svima zemljama članicama EU.

e-SENS[337] (engl. **e**lectronic **S**imple **E**uropean **N**etworked **S**ervices) – cilj projekta je konsolidirati rješenja koja su napravljena u prethodnima projektima. Time bi se izradilo univerzalno rješenje koje će se moći koristiti u različitim područjima elektroničke javne uprave (e-Documents, e-Delivery, e-ID, e-Signature, ….) .

[335] Malmö Declaration on eGovernment (2009.), 5th Ministerial eGovernment Conference, Malmö, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf (13.01.2018.)
[336] STORK, Secure Identity Across Borders Linked, https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu (13.01.2018.)
[337] e-SENS, Electronic Simple European Networked Services, https://www.esens.eu/ (13.01.2018.)

SPOCS[338] (engl. **S**imple **P**rocedures **O**nline for **C**ross- border **S**ervices) - cilj projekta je bio uvesti jednostavne prekogranične usluge (već je implementirano u razdoblju 2009.-2012.).

PEPPOL[339] (**P**an-**E**uropean **P**ublic **P**rocurement **O**n**L**ine) – cilj projekta je osigurati infrastrukturu za elektroničku javnu nabavu za europske operatere.

epSOS[340] (engl. **S**mart **O**pen **S**ervices for **e**uropean **p**atients) – cilj projekta je izgradnja infrastrukture za prekograničnu razmjenu medicinskih podataka (npr. medicinski podaci o pacijentu) između zdravstvenih sustava unutar EU.

eCODEX[341] (engl. justice **C**ommunication via **O**nline **D**ata **Ex**change) – cilj projekta je osiguravanje pristupa građanima i poslovnim subjektima pravosuđu u drugim državama unutar EU.

Navedeni projekti se već koriste ili će se koristiti u daljnjem razvoju elektroničke javne uprave u Hrvatskoj što će detaljnije biti opisano u poglavlju 6.3 Elektronička javna uprava u Republici Hrvatskoj.

Dakle, u svrhu podrške razvoju pametne, održive i uključive ekonomije Akcijski plan 2011.-2015. određuje da zemlje članice Europske unije do 2015. godine trebaju osigurati sljedeće:

- pružanje ključnih prekograničnih usluge u vidu elektroničkih usluga. Time se želi osigurati poduzetnicima uspostavu i vođenje posla bilo gdje unutar Europe te omogućiti građanima studiranje, rad, prebivanje i umirovljenje gdje god željeli u Europskoj uniji,
- da najmanje 50% građana i 80% poduzetnika Europske unije koristi usluge elektroničke javne uprave.

[338] SPOCS, Simple Procedures Online for Cross- Border Services, http://www.eu-spocs.eu/ (13.01.2018.)
[339] PEPPOL, Pan-European Public Procurement Online, https://peppol.eu/ (13.01.2018.)
[340] epSOS, Smart Open Services for european patients, http://www.epsos.eu/ (13.01.2018.)
[341] eCODEX, justice Communication via Online Data Exchange, https://www.e-codex.eu/ (13.01.2018.)

Rezultati ocjene Akcijskog plana za elektroničku javnu upravu za razdoblje 2011.-2015.[342] pokazuju da je taj plan pozitivno utjecao na razvoj europske e-uprave (sveukupno i po državama članicama). Navedeni plan je unaprijedio usklađenost nacionalnih strategija e-uprave te osigurao razmjenu najboljih praksi i interoperabilnosti rješenja među državama članicama. Zaključno, Akcijski plan 2011.-2015. je doveo do razvoja tehnoloških rješenja ključnih za lakši pristupa elektroničkim javnim uslugama te njihovim lakšim korištenjem. Međutim, tu akcijski planovi i deklaracije EU za elektroničku javnu upravu nisu stali. Nakon Deklaracija elektroničke javne uprave iz Malmöa (2009.), u listopadu 2017. je objavljena nova deklaracija o elektroničkoj javnoj upravi „Deklaracija iz Tallina“[343].

Deklaracija iz Tallina (potpisana na ministarskoj razini EU i EFTA članica) označava političku predanost država članica za ostvarivanjem vizije navedene u Akcijskom planu 2016.-2020. te uključuje posebne mjere kako bi se osigurala usklađenost s njezinim načelima. Jedna od ključnih obveza je ubrzavanje priprema za provedbu propisa o elektroničkoj identifikaciji i povjerenju u usluge elektroničkih transakcija na unutarnjem tržištu (Uredba eIDAS). Ona obuhvaća i razmjenu identiteta između organizacija javnog sektora. Ideja je da se građani i poslovni subjekti koji su se identificirali za određenu javnu uslugu u jednoj zemlji trebaju biti pokriveni time kada se drugom uslugom i istoj zemlji ili nekoj drugoj zemlji EU. Ističe se važnost pridržavanja standarda Uredbe eIDAS i primjene nekad načela „once-only“, tj. jedna prijava i jedan zahtjev za više elektroničkih javnih usluga. Uredba eIDAS označava usluge elektroničke identifikacije, provjere autentičnosti i povjerenja te obuhvaća, između ostalog, aspekte kao što su elektronički potpisi, vremenske oznake, elektronički transferi sredstava i javne usluge.

6.2.2 Interoperabilnost

Za početak potrebno je definirati pojam interoperabilnosti. Panian[344] definira interoperabilnost kao sposobnost nekog proizvoda ili sustava da surađuje i interagira s drugim proizvodima, odnosno sustavima. Specifičnije, sposobnost hardvera i softvera

[342] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630, str. 11 (10.01.2018.)
[343] Tallinn Declaration on eGovernment (2017.), Ministerial eGovernment Conference, Tallin, https://ec.europa.eu/newsroom/document.cfm?doc_id=47559 (13.01.2018.)
[344] Panian Ž. (2005.), Informatički enciklopedijski rječnik @-L, Europapress holding Zagreb, str. 296.

različitih proizvođača da razmjenjuju i dijele podatke. Strahonja i Šimić[345] navode da je interoperabilnost svojstvo organizacija te njihovih informacijskih sustava i poslovnih procesa da surađuju i djeluju usklađeno radi ostvarenja određenog cilja, bez obzira na organizacijsko vlasništvo nad procesima, lokaciju izvršavanja te razinu tehnološke potpore.

Ujedinjeno Kraljevstvo je 2000. godine razvila sofisticiranu interoperabilnu okosnicu e-GIF[346] (engl. e-Government Interoperability Framework). Navedena britanska okosnica je bitna iz razloga jer je među prvima definirala određene skupove tehničkih standarda i politika za osiguravanje interoperabilnosti sustava koji isporučuje elektroničke javne usluge. Usklađenost s e-GIF okosnicom je bila obavezna u javnom sektoru Velike Britanije.

Slijede najbitnije postavke e-GIF okosnice:

- Glavne specifikacije korištenih na Internetu za sve informacijske sustave javnog sektora trebaju biti univerzalno prihvaćene,
- Potrebno je prihvatiti XML kao primarni standard za integraciju podataka i prezentacijske alate,
- Web preglednici su ključno korisničko sučelje. Kroz tehnologije temeljene na web preglednicima trebaju biti dostupni svi informacijski sustavi javnog sektora. U slučaju da je platforma preglednik i druga sučelja su dozvoljena,
- Metapodaci su temelj za informacijske resurse javne uprave,
- Potrebno je razviti i prihvatiti standarde za metapodatke elektroničke javne uprave e-GMS (engl. e-Government Metadata Standard).

E-GIF je bila jedna od referentnijih interoperabilnih okosnica u svijetu. Imala je utjecaj na razvoj mnogih drugih nacionalnih okosnica (novozelandski NZ GIF[347], australski Information Interoperability Framework[348] i dr).

[345] Strahonja, V., Šimić, D. (2010.), Kako EU strategiju za interoperabilnost (EIS) i EU okvir za interoperabilnost (EIF) propagirati u Hrvatskoj i SEE regiji?, 8. Europska konferencija o poslovnim procesima, https://bib.irb.hr/datoteka/579053.2010-04-15_BPC2010_Strahonja_Simic.pdf (16.01.2018.)
[346] e-GIF, https://en.wikipedia.org/wiki/E-GIF (16.01.2018.)
[347] New Zealand e-Government Interoperability Framework (2005.), https://www.oasis-open.org/committees/download.php/13081/e-GIF%20v3.0%20draft%2023-05-2005.pdf (16.01.2108.)
[348] Australian Government Information Interoperability Framework, https://www.finance.gov.au/archive/policy-guides-procurement/interoperability-frameworks/information-interoperability-framework/ (16.01.2018.)

Europska unija je prvotno je kroz svoj program IDABC (engl. Interoperable Delivery of European eGovernment Services to Public Administrations)[349] napravila okosnicu za interoperabilnost između tijela javne uprave. IDABC je pokrenut 2004. godine u programu Europske unije koji je promicao pravilnu uporabu informacijskih i komunikacijskih tehnologija (IKT) za prekogranične usluge u Europi. Za postizanje ciljeva kao što je interoperabilnost IDABC je izdao preporuke, razvio rješenja i pružio usluge koje omogućuju nacionalnim i europskim upravama da komuniciraju elektronički dok nude moderne javne usluge tvrtkama i građanima. U kontekstu IDABC-a tada je izdana prva europska verzija interoperabilnosti verzije, EIF (engl. European Interoperability Framework). Novi Europski okvir za interoperabilnost (EIF) dio je Priopćenja[350] (COM (2017) 134) Europske komisije usvojenog u ožujku 2017. godine. Navedeni okvir daje specifične smjernice o tome kako uspostaviti interoperabilne elektroničke javne usluge. EIF nudi javnim upravama 47 konkretnih preporuka o tome kako poboljšati upravljanje njihovim aktivnostima interoperabilnosti, uspostaviti međusobne organizacijske odnose, pojednostaviti procese koji podržavaju elektroničke usluga te osigurati da i postojeći i novi propis ne ugroze napore za interoperabilnost. Novi EIF je donijet u kontekstu prioriteta Europske komisije za stvaranje jedinstvenog digitalnog tržišta u Europi. Javni sektor u Europskoj uniji čini preko četvrtinu ukupne zaposlenosti i predstavlja približno petinu BDP-a Unije. Nove preporuke se usmjeravaju na otvorenost i upravljanje informacijama, prenosivosti podataka, interoperabilnosti upravljanja te integriranim pružanjem usluga.

Navedene preporuke o interoperabilnosti uzimaju u obzir različite politike Europske unije kao što su:

- Direktiva o ponovnoj uporabi informacija javnog sektora[351] (engl. Directive on the reuse of Public Sector Information),
- Direktiva INSPIRE[352] (engl. INSPIRE Directive),
- Uredbe eIDAS,
- Europska Cloud inicijativa[353] (engl. European Cloud initiative),

[349] Europska komisija, IDABC - Interoperable Delivery of European eGovernment Services to Public Administrations, Business and Citizens, http://ec.europa.eu/idabc/ (16.01.2018.)
[350] Europska komisija (2017.),European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF (16.01.2018.)
[351] Europska komisija (2014.),Directive on the reuse of Public Sector Information, http://europa.eu/rapid/press-release_IP-14-840_en.htm (16.01.2018.)
[352] Europska komisija, INSPIRE Directive, http://inspire.ec.europa.eu/about-inspire/563 (16.01.2018.)

- Akcijski plan elektroničke javne uprave 2016.-2020. (engl. EU eGovernment Action Plan 2016-2020).

Među preporukama se navode i Inicijative koje su u planu kao Jedinstveni Digitalni Gateway[354] (engl. Single Digital Gateway). EIF komunikacija je popraćena Akcijskim plan za interoperabilnost[355] koji ukazuje na prioritete koji će podržati provedbu Europskog okvira za interoperabilnost od 2016. do 2020. godine. Europska komisija će za provedbu i praćenje okvira koristiti ISA² programa[356] (engl. ISA² programme). Države članice će usklađivati nacionalne planove s europskim Akcijskim planom za interoperabilnost. Europska komisija će ocjenjivati novi EIF do kraja 2019. godine. Program ISA² podržava razvoj digitalnih rješenja koja omogućuju javnim upravama, tvrtkama i građanima u Europi da imaju koristi od interoperabilnih prekograničnih i međusektorskih javnih usluga. Revizijom europskog okvira za interoperabilnost ispunjava se dio Strategije Jedinstvenog digitalnog tržišta (engl. Digital Single Market strategy).

Konceptualni EIF model je temeljen na 4 sloja interoperabilnosti[357]:

1. Pravna interoperabilnost (engl. Legal Interoperability) – to je usklađenost pravnih sustava zemalja članica. Zakoni usklađeni s EU direktivama su osnova za zakonitu razmjenu podataka,
2. Organizacijska interoperabilnost (engl. Organisational Interoperability) – ona pokriva definiranje poslovnih ciljeva, modeliranje poslovnih procesa te kolaboraciju i razmjenu informacija između tijela javne uprave koja imaju različite procese i različite interne ustroje,
3. Semantička interoperabilnost (engl. Semantic Interoperability) – to je interoperabilnost koja pokriva značenja i tumačenja informacija izmijenjenih između više aplikacija. Semantička interoperabilnost je preduvjet za višejezičnu isporuku usluge krajnjim korisnicima.

---

[353] Europska komisija (2016., 2.), European Cloud initiative, http://europa.eu/rapid/press-release_IP-16-1408_en.htm (16.01.2018.)
[354] Single Digital Gateway, http://ec.europa.eu/growth/content/commission-launches-consultation-single-digital-gateway-1_en (16.01.2018.)
[355] Europska komisija (2017., 2.), Akcijski plan za interoperabilnost 2016.-2020., http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN (16.01.2018.)
[356] ISA² programme, https://ec.europa.eu/isa2/home_en (16.01.2018.)
[357] Bovalis, K. (2017.), European Interoperability Framework, Inspire 2017, https://ec.europa.eu/isa2/sites/isa/files/docs/publications/2017-09-07_eif_inspire.pdf (16.01.2018.)

4. Tehnička interoperabilnost (engl. Technical Interoperability) - ova interoperabilnost pokriva tehničke standarde koji služe za povezivanje računalnih sustava i različitih usluga. Tehnička interoperabilnost pokriva velik broj ključnih područja: interkonekcijske servise, integriranje podataka i poslužiteljske strane, otvorena sučelja, prezentaciju podataka, razmjenu podataka, sigurnost….

EIF ima za svrhu omogućiti povezivanje drugih nacionalnih okvira interoperabilnosti između sebe zbog povezanih elektroničkih javnih usluga i prekogranične suradnje. Za Europsku uniju je za tu svrhu bitna infrastruktura sTESTA[358] (engl. secured Trans European Services for Telematics between Administrations). Tom infrastrukturom je Europska unija dobila mogućnost sigurne razmjene podataka između nacionalnih elektroničkih javnih uprava.

6.2.3 Računalstvo u oblaku

Američki Nacionalni institut za standarde i tehnologije, NIST (engl. National Institute of Standards and Technology) definira[359] računalstvo u oblaku (engl. Cloud computing) kao model za omogućavanje sveprisutnog, prikladnog, na zahtjev (engl. on demand) mrežnog pristupa zajedničkom skupu konfigurabilnih računalnih resursa (npr., mreža, poslužitelja, pohrane, aplikacija i usluga) koje se mogu brzo rezervirati i pustiti s minimalnim naporom upravljanja ili interakcijom pružatelja usluga. NIST dodaje da je računalni oblak skupina zajedničkih resursa i servisa na računalima te ostalim uređajima koji na zahtjev postaju dostupni za krajnjeg korisnika preko internet infrastrukture, a da pri tome korišteni resursi te servisi ne moraju biti u vlasništvu njihovog krajnjeg korisnika.

Kao osnovne značajke računalstva u oblaku NIST navodi[360]:

- Samoposluživanje na zahtjev (engl. On-demand self-service.) - Korisnik može na jednostran način odrediti računalne resurse te potrebe tipa vremena pružanja usluge

[358] STESTA, Secure Trans European Services for Telematics between Administrations, http://ec.europa.eu/idabc/en/document/2097.html (17.01.2018.)
[359] Mell, P., Grance, T. (2011.), The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf , str. 2 (17.01.2018.)
[360] Isto, str. 2

i mrežne pohrana. Sve se to može izvesti automatski (bez ljudske interakcije sa pružateljem usluge),

- Široki pristup mreži (engl. Broad network access) - Mogućnosti korištenja su dostupne preko mreže. Korištenje se odvija putem standardnih mehanizama koji promiču korištenje heterogenih tankih ili debelih klijentskih platformi (npr. mobitela, tableta, prijenosnih računala i radnih stanica),
- Grupiranje resursa (engl. Resource pooling) - Računalni resursi pružatelja usluge grupirani su na način da mogu poslužiti više potrošača pomoću modela s više korisnika, s različitim fizičkim i virtualnim resursima. Navedeni virtualni resursi su dinamički dodijeljeni i preraspodijeljeni prema zahtjevu korisnika. Postoji osjećaj nezavisnosti lokacije po tome što korisnik nema kontrolu ili znanje o preciznoj lokaciji navedenih resursa. Korisnik lokaciju može odrediti na višoj razini apstrakcije (npr. zemlja, država ili podatkovni centar). Primjeri takvih grupiranih resursa uključuju: pohranu, procesiranje, memoriju i propusnost mreže,
- Brza elastičnost (engl. Rapid elasticity) - resursi se mogu elastično dodijeliti i otpustiti. Ponekad se dodjela/otpuštanje resursa obavlja automatski kako bi se stanje brzo uskladilo s potražnjom. Korisnicima se dostupni resursi često čine neograničeni te im mogu biti dodijeljeni u bilo kojem trenutku u bilo kojoj količini,
- Mjerena usluga (engl. Measured service) – sustavi računalnog oblaka automatski kontroliraju i optimiziraju korištenje resursa i to iskorištavanjem mjernih sustava na nekoj razini apstrakcije koja odgovara vrsti usluge (npr. pohrana, obrada, propusnost i aktivni korisnički računi). Obično se to radi na načelu "plati po korištenju" (engl. pay-per-use) ili "naplati po upotrebi" (engl. charge-per-use). Korištenje resursa može se pratiti, kontrolirati i prijaviti pružajući pri tome transparentnost i za pružatelja i korisnika korištene usluge.

Što se tiče modela usluga (engl. Service Models) za računalne oblake postoji SPI model. SPI model[361] (SaaS, PaaS, IaaS) je akronim za najčešće modele usluge računalstva u oblaku: softver kao usluga (engl. Software as a Service), platforma kao usluga (engl. Platform as a Service) i infrastruktura kao usluga (engl. Infrastructure as a Service).

[361] SPI model (SaaS, PaaS, IaaS), http://searchcloudcomputing.techtarget.com/definition/SPI-model (18.01.2018.)

Softver kao usluga, SaaS (engl. **S**oftware **a**s **a** **S**ervice) – korisniku se pruža mogućnost korištenje aplikacija pružatelja usluga koji se izvodi na infrastrukturi oblaka. Aplikacijama se može pristupiti s različitih klijentskih uređaja kao što su tanki klijenti (npr. web preglednik, u tom slučaju se navodi URL na webu) ili sučelje aplikacije. Korisnik ne upravlja niti kontrolira osnovnu infrastrukturu za oblak, uključujući mrežu, poslužitelje, operativne sustave, pohranu te čak niti pojedinačne aplikacije. Moguća je iznimka ograničenih korisničkih postavki konfiguracije aplikacije.

Platforma kao usluga, PaaS (engl. **P**latform **a**s **a** **S**ervice) – mogućnost koja se pruža korisniku je implementacija na infrastrukturi oblaka koja je stvorena ili kupljena od potrošača stvorenih pomoću programskih jezika, knjižnica, usluga i alata koje podržava pružatelj usluge. Korisnik ne upravlja niti kontrolira osnovnu infrastrukturu oblaka, uključujući mrežu, poslužitelje, operativne sustave ili pohranjivanje, ali ima kontrolu nad implementiranim aplikacijama i mogućim postavkama konfiguracije za okruženje aplikacijskog hostinga.

Infrastruktura kao usluga, IaaS (engl. **I**nfrastructure **a**s **a** **S**ervice) – korisniku je pružena mogućnost pružanja obrade, skladištenja, mreža i drugih osnovnih računalnih resursa na kojima korisnik može implementirati i pokrenuti proizvoljni softver koji može uključivati operacijske sustave i aplikacije. Korisnik ne upravlja niti kontrolira temeljnu infrastrukturu računalnog oblaka već ima kontrolu nad operacijskim sustavima, pohranom i aplikacijama. Korisnik eventualno ima ograničenu kontrolu nad odabranim komponentama umrežavanja (npr. vatrozidima glavnog računala).

Sljedeći su modeli implementacije računalnih oblaka[362]:

- Privatni oblak (engl. Private cloud) – računalni oblak čija je infrastruktura osigurana isključivo za jednu organizaciju koja uključuje više potrošača (npr. različite poslovne jedinice). Može biti u vlasništvu, vlastitom upravljanju i upravljanju od strane organizacije, treće strane ili nekih njihovih kombinacija, a može biti u prostorijama organizacije ili izvan nje.

[362] Mell, P., Grance, T. (2011.), The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf , str. 3 (17.01.2018.)

- Zajednica u oblaku (engl. Community cloud) – infrastruktura oblaka je osigurana isključivo za određenu zajednicu potrošača iz organizacija koje imaju zajedničku brigu (npr. misija, sigurnosni zahtjevi, različite politike,...). Može biti u vlasništvu, i upravljanju od strane jedne ili više organizacija u zajednici, treće strane ili neke njihove kombinacije, a može biti unutar njihovih prostora ili izvan.
- Javni oblak (engl. Public cloud) – infrastruktura oblaka je osigurana za otvorenu upotrebu za javnost. Može biti u vlasništvu i upravljanju od strane poslovne, akademske ili državne organizacije ili neke njihove kombinacije. Ona postoji u prostorijama pružatelja usluge računalnog oblaka.
- Hibridni oblak (engl. Hybrid cloud) - infrastruktura oblaka je spoj dva ili više oblaka različitih modela (privatna, zajednička ili javna) koja ostaju jedinstveni entiteti, ali su povezana standardiziranom ili vlasničkom tehnologijom koja omogućava prenosivost podataka i aplikacija (npr. balansiranje opterećenja između oblaka).

Što se tiče Europske unije, Europska komisija je 2012. godine usvojila je Strategiju za oslobađanje potencijala računalstva u oblaku. Time je iskazala namjeru uključivanja računalstva u oblaku u uvođenje interoperabilnih usluga za građane, tvrtke i tijela javne uprave. Osim toga, plan je uključiti i platforme i infrastrukturu koje će se koristiti na većem prostoru. Važne su za širenje računalstva u oblaku i Studija Europske komisije o ekonomskom utjecaju računalstva u oblaku u Europi[363]. Navedena studija ističe ekonomske prednosti objedinjavanja računalnih oblaka i slobodnog protoka podataka unutar Europske unije. Studija pokazuje da bi široka primjena računalnih oblaka mogla doprinijeti kumulativnom ukupnom prihodu od 449 milijardi eura u BDP-u Europske unije te bi navedeno imalo veliki utjecaj na zapošljavanje i stvaranje novih poslova. Provedba sigurnosne certifikacije i uklanjanje zahtjeva za lokalizacijom podataka mogla bi povećati prihod za dodatnih 19 milijardi eura između 2015. i 2020. godine[364].

Zanimljiva je i platforma austrijskog Ministarstva za održivost i turizam, Elektroničkog sustava za upravljanje podacima - EDM (njem. Elektronisches Datenmanagement –

[363] Europska komisija, Measuring the economic impact of cloud computing in Europe, Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe (10.01.2017.)
[364] Europska komisija (2014., 2.), Study on measuring the economic impact of cloud computing in Europe — SMART 2014/0031, http://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:173873-2014:TEXT:EN:HTML (18.01.2018.)

Umwelt)[365]. Navedena platforma je dobila EuroCloud nagradu 4 zvjezdice StarAudit certifikat[366] (njem. 4-star StarAudit Certificate). EDM podupire tvrtke i javnu upravu u provedbi ekološki relevantnih zahtjeva. Ovaj događaj je važan iz razloga što je to prva certificirana usluga u oblaku za elektroničku javnu upravu u Europi. Implementacija EDM platforme je pokrenuta 15 godina ranije, a svrha izrade ove platforme je bila obrada ekološki relevantnih izvješća kako bi se spriječila suvišna registracija i obrada podataka. Puštanjem u produkcijski rad, EDM postaje neophodan izvor informacija u mnogim područjima koja se odnose na okoliš. Mnoštvo zakonskih obveza sada se rješava uz pomoć 23 aplikacije koje su integrirane u zajednički informacijski sustav.

6.2.4 Zaštita podataka

Zaštiti podataka se u Europskoj uniji daje velika važnost. Europska unija još 1995. godine donosi direktive o zaštiti podataka (95/46/EC)[367]. Direktivu 2003/98/EZ Europskog parlamenta i Vijeća iz studenog 2003. o ponovnoj uporabi informacija javnog sektora je EU donijela kao pravni akt za zaštitu podataka[368]. Direktiva 2003/98/EZ je donesena da bi propisala okvir zaštite podataka u zemljama članicama EU što su iste trebale striktno primijeniti kroz svoja nacionalna zakonodavstva. Navedena direktiva navodi da se unutar tijela javne vlasti osobni podaci moraju zaštititi. Zaštita se odnosi na slučajno ili nezakonito uništavanje, nezakonitu obradu, zatim na promjenu podataka te njihovo nedopušteno objavljivanje. Posebno je bitno zaštititi podatke prilikom prijenosa podataka putem mreže. Europska komisija je na tragu potrebe ujednačavanja pravila unutar Unije, 2012. predložila veliku reformu pravila Europske unije o zaštiti podataka[369] iz 1995. Time se nastojalo dodatno ojačati prava na privatnost na internetu te potaknuti europsko digitalno gospodarstvo. Težnja je bila napraviti jedinstveni pravni okvir te riješiti rascjepkanost u nacionalnim regulativama i smanjiti skupa administrativna opterećenja.

[365] First Cloud Certification in Europe for E-Government-Platform of the BMNT, EuroCloud, https://eurocloud.org (01.08.2018.)
[366] EuroCloud, eurocloud.org (01.09.2018.)
[367] Europski parlament i Vijeće (1995.), Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, azop.hr/images/dokumenti/168/direktiva_9546ez.doc (20.01.2018.)
[368] Europski parlament i Vijeće (2003.), Direktiva 2003/98/EZ Europskog parlamenta i Vijeća iz studenog 2003. o ponovnoj uporabi informacija javnog sektora, https://data.gov.hr/sites/default/files/library/CELEX-32003L0098-HR-TXT.pdf (20.01.2018.)
[369] Europski parlament i Vijeće (2012.), Prijedlog uredbe o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kretanja takvih podataka (opća uredba o zaštiti podataka) (COM(2012) 11)

Procjena je bila da će poduzeća uštedjeti blizu 2,3 milijarde eura po godini. Osim toga navedena inicijativa je imala za težnju učvrstiti povjerenje potrošača u usluge na internetu te time dati poticaj rastu, otvaranju novih radnih mjesta i inovacijama.

Katulić u svom članku „Stiže Opća uredba o zaštiti podataka“[370] konstatira da Europa napokon ima novi pravni okvir zaštite osobnih podataka. Naime, nakon dugogodišnjih konzultacija i zakonodavne procedure usvojen je prijedlog novog temeljnog propisa koji zamjenjuje Direktivu o zaštiti osobnih podataka iz 1995. godine. Taj propis je donesen u obliku uredbe naziva „Opća uredba o zaštiti podataka“[371], GDPR (engl. General Data Protection Regulation). Važnost njezinog donošenja kao uredbe je što se treba direktno primjenjivati u svim državama članicama EU bez potrebe za implementacijom u zasebna nacionalna zakonodavstva. Katulić u navedenom članku primjećuje[372] kako je Uredba sastavni dio pravne i političke poruke Bruxellesa, kako državama članicama, tako i drugim partnerima, ponajviše Sjedinjenim Državama, čija poduzeća predvode u poslovnom iskorištavanju osobnih podataka osoba koje žive na području Unije. Naime, europski zakonodavac ovom Uredbom podiže standarde zaštite osobnih podataka i time se ponovo pozicionira kao predvodnik zaštite ljudskih prava na svjetskoj razini. GDPR Uredba je stupila na snagu 24.05.2016., a početak primjene Uredbe je previđen za 25.05.2018. Ovime se stavlja izvan snage Direktiva 95/46/EC.

Glavni ciljevi su: usklađivanje zakona o zaštiti podataka u cijeloj Europi, zaštita i osnaživanje osobnih podataka svih građana EU te promjena načina pristupa zaštiti podataka u organizacijama. Novost su i jako velike propisane kazne koje se mogu naplatiti zbog neusklađivanje s Uredbom. Novčane kazne mogu biti do 20 milijuna eura ili čak do 4 % ukupnog godišnjeg prometa na svjetskoj razini. Nacionalna regulatorna tijela unutar članica EU bit će biti nadležna za osiguravanje primjene Uredbe. U Hrvatskoj je AZOP[373] tijelo koje je nadležno za nadzor provođenja. AZOP ima i dosadašnja ovlaštenja, primjerice narediti voditelju zbirke da ukloni nepravilnosti ili obriše prikupljene podatke koji su bez valjanog pravne osnove prikupljeni u zbirku.

[370] Katulić. T. (2016.), Stiže Opća uredba o zaštiti podataka, https://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (29.05.2016.)
[371] Europski parlament i Vijeće (2016.), 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 te o stavljanju izvan snage direktive 95/46/EZ (Opća uredba o zaštiti podataka) (20.01.2018.)
[372] Katulić. T. (2016.), Stiže Opća uredba o zaštiti podataka, https://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (29.05.2016.)
[373] Agencija za zaštitu osobnih podataka, AZOP, http://azop.hr/ (21.01.2018.)

GDPR Uredba propisuje prava korisnika te načela obrade osobnih podataka. Prava ispitanika su sljedeća:

- Pravo na prenosivost podataka - korisnik ima pravo zatražiti i dobiti osobne podatke koji se odnose na njega u nekoj instituciji ili tvrtki te ima pravo prenijeti podatke u drugu instituciju ili tvrtki,
- Pravo na pristup podacima i njihov ispravak - korisnik ima pravo dobiti od institucije ili tvrtki potvrdu obrađuju li se njegovi osobni podaci te koja je svrha obrade i predviđeno razdoblje za pohranu. Osim toga, korisnik može zatražiti i ispravak podataka,
- Pravo na zaborav - korisnik ima pravo od tvrtke/institucije zahtijevati brisanje osobnih podataka koji se na njega odnose,
- Slanje izvješća o povredi osobnih podataka - u slučaju dolaska do povrede osobnih podataka tvrtke/institucije moraju najkasnije 72 sata nakon saznanja o toj povredi poslati izvješće odgovarajućem nadzornom tijelu i korisniku.

Načela obrade osobnih podataka definirana Uredbom su:

- Zakonitost, poštenost i transparentnost,
- Cjelovitost i povjerljivost,
- Točnost,
- Potrebno je ograničiti svrhu prikupljanja i obrade podataka na nužnu,
- Ograničavanje vremena pohrane (podaci se smiju čuvati samo onoliko vremena koliko je potrebno radi zadovoljenja svrhe),
- Potrebno je smanjiti količine podataka (smiju se prikupljati i obrađivati samo oni podaci koji su nužni za obavljanje procesa za čije potrebe se prikupljaju).

Uredba propisuje i potrebu da određene organizacije imenuju službenika za zaštitu podataka, DPO (engl. Data Protection Officer). DPO se imenuje i ukoliko obradu obavlja tijelo javne vlasti ili javno tijelo. Izuzetak su sudovi koji djeluju u okvirima sudske nadležnosti. Službenik za zaštitu podataka može obavljati funkciju i za grupu tvrtki. Uvjet je to je da je službenik za zaštitu podataka lako dostupan iz mjesta svog poslovanja.

GDPR Uredba je za organizacije unutar EU postavila i zahtjev Provedbe analize utjecaja zaštite osobnih podataka, DPIA (engl. **D**ata **P**rotection **I**mpact **A**ssessment). Članak 35. Uredbe propisuje da je DPIA postupak koji organizacija mora provesti kad postoji vjerojatnost da će neka vrsta obrade osobnih podataka predstavljati velik rizik za prava i slobode pojedinaca. To se najviše odnosi na podatke koji se koriste kroz nove tehnologije, a potrebno je uzeti u obzir prirodu, opseg, kontekst i svrhu obrade. Markovinović[374] navodi da se rizici provedbom DPIA-e neće smanjiti sami od sebe, ali će se identificirati prijetnje te će se predlagati načini ublažavanja rizika u ranoj fazi uvođenja novih tehnika i metoda obrade osobnih podataka. Markovinović, nadalje, navodi[375] da je za učinkovitu provedbu ovakve aktivnosti potrebno, između ostaloga, dokumentirati:

- vrste prikupljanih osobnih podataka;
- način prikupljanja, korištenja, prenošenja i pohranjivanja podataka;
- način i razlog dijeljenja podataka među poslovnim entitetima;
- mjere sigurnosti koje se primjenjuju za sprječavanje neovlaštenog pristupa podacima u svakom koraku obrade.

Međutim da postoje i nerazumijevanja i dvojbe oko provođenja GDPR Uredbe navodi i Tannam[376] pozivajući se na neovisnu globalnu anketu koju je naručila tvrtka WatchGuard Technologies. Spomenuta anketa je pokazala koliko je organizacija nespremno za nadolazeće propise o GDPR Uredbi. Kriteriji Uredbe utvrđuju da svaka tvrtka koja pohranjuje ili obrađuje osobne podatke o državljanima Europske unije mora dokazati sukladnost. Ovo istraživanje više od 1.600 organizacija pokazalo je da postoji široka zbrka oko pitanja o vrstama podataka koje spadaju pod ovu Uredbu. Među ispitanicima je 37% reklo da ne zna je li njihova organizacija dužna pridržavati se ili ne navedene Uredbe, a 28% ispitanika ispitanih organizacija smatra da nemaju nikakvih zahtjeva koji bi oni trebali poštovati. Istraživanje je pokazalo da jedan od sedam ispitanika koji ne smatraju da se propisi ove Uredbe primjenjuju na njih, zapravo prikupljaju osobne podatke od građana EU.

[374] Markovinović, N. (2017.), Kako učinkovito provesti Data Protection Impact Assessment (DPIA)?, https://gdpr2018.eu/kako-ucinkovito-provesti-data-protection-impact-assessment-dpia/ (09.10.2017.)
[375] Isto
[376] Tannam, E. (2017.), Confusion remains around GDPR compliance, https://www.siliconrepublic.com/enterprise/gdpr-compliance-watchguard-survey (14.07.2017.)

Katulić zaključno o Uredbi navodi[377] da Europska unija smatra kako su privatnost i zaštita osobnih podataka temeljna ljudska prava. Europska unija smatra kako osobni podaci za SAD predstavljaju samo digitalno dobro koje se može i treba uspješno monetizirati. S druge strane Amerikanci o ovoj Uredbi ne misle ništa dobro te je čak smatraju zaprekom slobodi govora. Dakle, može se reći da je ovdje riječ o dubokoj pravnoj i kulturnoj podjeli.

6.3 ELEKTRONIČKA JAVNA UPRAVA U REPUBLICI HRVATSKOJ

6.3.1 Kontekst razvoja elektroničke javne uprave u Republici Hrvatskoj

U svom magistarskom radu „Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge“[378] dajem pregled zakonskih osnova i strategija za razvoj hrvatske e-Uprave do 2007. godine. Jedan od prvih konkretnijih strateških planova za ubrzavanje procesa informatizacije i restrukturiranje državne uprave, povećanje konkurentnosti hrvatskih poduzeća i povećanje efikasnosti usluga građanima je bio Program e-Hrvatska 2007. Navedeni program je imao zacrtane sljedeće ciljeve:

- Informatizaciju školstva, te razvijanje sustava obrazovanje i kontinuiranog obrazovanja putem interneta,
- Informatizaciju zdravstva, te stvaranje online pristupa zdravstvenim uslugama,
- Za razdoblje od 2004. do 2007. bila je planirana uspostava i umrežavanje sustava tijela javne uprave. Osim toga su bile planirane elektroničke usluge za građane i poduzeća za sljedeća područja: javne uprave, zdravstva, školstva i pravosuđa.

Operativni plan provedbe programa e-Hrvatska 2007. za 2004.[379] prati zacrtane smjernice odrednice Akcijskog plana Europske komisije - eEurope 2005. Naime, pokazalo se da poslije donošenja navedenog programa nisu uspostavljeni odgovarajući mehanizmi praćenja. Posljedica je bila spora i neusklađena provedba. Svrha Operativnog plana

[377] Katulić, T. (2016.), Stiže Opća uredba o zaštiti podataka, https://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (29.05.2016.)
[378] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf, str. 121 (17.03.2018.)
[379] Središnji državni ured za e-Hrvatsku (2004.), Operativni plan provedbe programa e-Hrvatska 2007. za 2004. godinu, http://digured.srce.hr/arhiva/10/10/www.vlada.hr/Download/2004/07/12/Operativni_plan_eHR2004_V1_5.pdf (21.01.2018.)

provedbe programa e-Hrvatska 2007. Za 2004 je bila uspostavljanje okvira za provedbu i praćenje Programa e-Hrvatska 2007. Praćenje se nastojalo omogućiti na razini aktivnosti i projekata te provedbenih mjera kako bi se osigurala učinkovita provedba programa. Važnost ovih Programa i operativnih planova bivšeg Ureda za e-Hrvatsku je bila što su zahvaljujući njima prvi puta su pokrenute aktivnosti u područjima:

- e-Uprave,
- e-Pravosuđa,
- e-Obrazovanja,
- e-Zdravstva,
- e-Poslovanja.

Operativni plan provedbe programa e-Hrvatska 2007. za 2006. godinu[380] se nastavlja pratiti stanje elektroničkih javnih usluga iz definiranih područja: e-Uprave, e-Pravosuđa, e-Obrazovanja, e-Zdravstva i e-Poslovanja. Ovaj operativni planu se vodi i Inicijativom Europske komisije i2010 iz 2005. godine koja u informacijskoj i komunikacijskoj tehnologiji prepoznaje pokretača razvoja i zapošljavanja kroz tri prioritetna smjera razvoja: razvoj zajedničkog informacijskog prostora kroz stvaranje digitalnih sadržaja i usluga, inovativnost i tehnologijski razvoj te uključivanje svih društvenih slojeva u informacijsko društvo.

Operativni plan provedbe programa e-Hrvatska za 2009.[381] godine nastavlja na tragu prethodnih godišnjih programa e-Hrvatske, a važan je i što se 2009. godine Središnji državni ured za e-Hrvatsku uključio se u projekt Europske komisije "eGovernment Benchmarking" kojim se mjeri stupanj razvoja elektroničke uprave u zemljama EU. Iste godine je Vlada Republike Hrvatske usvojila prvu sveobuhvatnu Strategiju razvoja elektroničke uprave za razdoblje 2009.-2012.[382] koja definira viziju i strategiju ostvarenja korisnički usmjerene uprave. U navedenoj strategiji su navedena četiri temelja elektroničke uprave i ciljevi koji su usmjereni njihovoj izgradnji. Kao temelji su navedeni: računalna i

[380] Središnji državni ured za e-Hrvatsku (2006.), Operativni plan provedbe programa e-Hrvatska 2007. za 2006. godinu, http://digured.srce.hr/arhiva/434/8002/www.e-hrvatska.hr/ehrvatska/modules/Downloads/upload/Operativni_plan_provedbe_Programa_e-Hrvatska_2007_za_2006.pdf (21.01.2018.)
[381] Središnji državni ured za e-Hrvatsku (2009., 2.), Operativni plan provedbe programa e-Hrvatska 2009., http://digured.srce.hr/arhiva/434/42111/e-hrvatska.hr/sdu/hr/e-hrv/contentParagraph/011111111111111/document2/Plan_provedbe_e-Hrvatska_2009.pdf (21.01.2018.)
[382] Središnji državni ured za e-Hrvatsku (2009.), Strategija razvoja elektroničke uprave za razdoblje 2009.-2012., http://digured.srce.hr/arhiva/10/31637/strategija_e_Uprave_HRV_final.pdf (21.01.2018.)

komunikacijska infrastruktura, podatkovno/informacijska i dokumentacijska osnovica, dostupnost elektroničkih usluga te ljudski potencijali.

U 2010. godini je Republika Hrvatska pristupila Programu Interoperabilna rješenja za europsku javnu upravu, ISA[383] (engl. **I**nteroperability **S**olutions for European Public **A**dministrations) od 2010. do 2015. godine koja je za cilj imala unaprijediti suradnju i komunikaciju između europskih javnih uprava elektroničkim putem te omogućiti korištenje zajedničkih rješenja.

Godinu dana kasnije Središnji državni ured za e-Hrvatsku započinje koordinaciju provedbe Digitalne agende za Europu 2020, a Vlada Republike Hrvatske usvaja Odluku o utvrđivanju ciljeva razvoja elektroničke uprave u tijelima državne uprave za razdoblje od 2011. do 2015. godine[384]. Naglasak navedene odluke je na:

- razvoju osobnih elektroničkih usluga, uključujući usluge kao što su praćenje statusa vlastitog predmeta u javnoj upravi,
- omogućavanje pristupa putem interneta informacijama o zakonima i drugim pravnim aktima, politikama i financiranju,
- omogućavanje elektroničkog pristupa osobnim podacima koje o fizičkim osobama vode tijela državne uprave te omogućavanju informiranja elektroničkim putem, kad su njihovi podaci predmet automatske obrade i razmjene podataka.

Krajem 2011. godine je Hrvatski Sabor donio je Zakon koji uključuje ukidanje Središnjeg državnog ureda za e-Hrvatsku i prebacivanje svih poslova koji se tiču informatizacije državne uprave na Ministarstvo uprave.

Zakon o državnoj informacijskoj infrastrukturi[385] je donesen u srpnju 2014. Njime se nastojala uvesti promjena načina rada u javnoj upravi te promijeniti njen odnos prema građanima i poduzetnicima. Konačan cilj je bio osigurati elektroničke javne usluge za

[383] ISA, Interoperability Solutions for European Public Administrations, https://ec.europa.eu/isa2/home_en (21.01.2018.)
[384] Središnji državni ured za e-Hrvatsku (2011.), Odluka o utvrđivanju ciljeva razvoja elektroničke uprave u tijelima državne uprave za razdoblje od 2011. do 2015. godine, https://uprava.gov.hr/UserDocsImages/eHrvatska/5-Odluka%20Vlade%20RH%20o%20ciljevima%20e-Uprave%202011-2015.pdf (21.01.2018.)
[385] Sabor Republike Hrvatske (2014.), Zakon o državnoj informacijskoj infrastrukturi, https://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1840.html (21.01.2018.)

građane i poslovne subjekte temeljene na integriranom informacijskom sustavu države. Navedenim zakonom se teži rješavanju tri ključna problema e-Uprave:

1. Nadležnost za upravljanje i koordiniranje razvoja e-Uprave – želi se osigurati takav razvoj državne informacijske infrastrukture koji će djelovati kao jedinstveni sustav za pružanje usluga prema građanima i poslovnim subjektima,
2. Stvaranje virtualnog jedinstvenog upravnog mjesta,
3. Obveznost korištenja podataka u temeljnim registrima (načelo samo jedanput, engl. only once) – svrha je rasteretiti građane od fizičkog nošenja dokumenata između institucija.

Ministarstvo uprave Republike Hrvatske 2015. godine donosi Nacrt Strategije eHrvatska 2020. Navedeni dokument je izrađen s namjerom podizanja konkurentnosti gospodarstva pomoću informacijske i komunikacijske tehnologije te pružanjem visokokvalitetnih elektroničkih javnih usluga društvu. Vlada Republike Hrvatske je zadužila Ministarstvo uprave za izradu Strategije e-Hrvatska 2020 vezano na 2. tematski cilj (Digitalni rast) čime se osigurava pristup sredstvima u iznosu od 750 mil. kuna iz Europskog regionalnog razvojnog fonda za financijsku perspektivu 2014-2020. Iz navedenih sredstava se planirao realizirati Centar dijeljenih usluga te razviti elektroničke javne usluge u područjima: zdravstva, upravljanja zemljištem, turizma i kulture te digitalizacije sustava Hrvatske gospodarske komore. Strategija e-Hrvatska 2020[386] je donesena u svibnju 2017. te daje pregled razvoja informatizacije i elektroničkih usluga u javnom sektoru te ciljeve daljnjeg razvoja. Ova Strategija je u uskoj vezi s Digitalnom agendom za Europu. Glavni cilj donesene Strategije je osigurati povezivanje informacijskih sustava tijela javne uprave iz svih sektora na način da se građanima pruži što veći broj kompleksnih e-usluga i smanji opterećenje građana u interakciji s javnom upravom. Aktivnosti će se provesti sukladno Akcijskom planu za provedbu Strategije[387] i što je vrlo bitno plan je financirati se prvenstveno iz Europskih fondova te iz nacionalnih sredstava. U Akcijskom planu je navedeno konkretnih 126 projekata s ključnim aktivnostima, indikatorima uspješnosti, početkom i završetkom provedbe te planiranim iznosima projekata po izvorima financiranja (EU fondovi, državni proračun,..) i po godinama.

[386] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 , str. 27 (10.01.2018.)
[387] Ministarstvo uprave (2017., 2.), Akcijski plan za provedbu Strategije e-Hrvatska 2020, https://uprava.gov.hr/UserDocsImages//e-Hrvatska//Akcijski%20plan%20za%20provedbu%20Strategije%20e-Hrvatska%202020.pdf (21.01.2018.)

6.3.2 Infrastrukturne sastavnice i usluge

Za potrebe razvoja i podrške elektroničke javne uprave u Hrvatskoj Ministarstvo uprave se oslanja na više organizacija i firmi: Financijsku agenciju, APIS, CARNET, AKD, HAKOM, CERT.hr i druge.

Financijska agencija[388] (**FINA**) je trgovačko društvo u državnom vlasništvu koje pruža financijske i elektroničke usluge. FINA ima veliku nacionalnu pokrivenost te izrađuje i održava informatičke sustave za bitne poslove od nacionalne važnosti (od jednostavnih financijskih transakcija do složenih poslova u elektroničkom poslovanju). FINA obavlja i poslove izrade i održavanja mreže tijela državne uprave (**HITRONet**) čija je funkcija povezivanje tijela državne uprave u zajedničku računalno-komunikacijsku mrežu. Da bi se HITRONet priključio na sTESTA mrežu Europske unije potrebno je bilo ispuniti sve tehničke preduvjete za povezanost s tom mrežom. Od lipnja 2009. godine HITRONet je uspješno povezan sa sTESTA[389] mrežom.
FINA osim toga pruža podrške sustavu državnih i javnih financija, podrške sustavu državnih registara i informacijskih servisa za potrebe tijela državne uprave, regionalne uprave i lokalne samouprave. FINA je registrirani davatelj usluge certificiranje elektroničkog potpisa, a Uredbom Vlade RH o davatelju usluga certificiranja elektroničkih potpisa za tijela državne uprave Finini certifikati su izjednačeni s vlastoručnim potpisom i u tijelima javne uprave.

Agencija za podršku informacijskih sustava i informacijske tehnologije d.o.o. (**APIS IT**)[390] je agencija koja pruža usluge razvoja i podrške informatičkim sustavima za Republiku Hrvatsku i Grad Zagreb. APIS će imati bitnu ulogu vezanu uz **uspostavu Centra dijeljenih usluga (CDU)** što će biti jedna od bitnih sastavnica projekta stvaranja zajedničke državne informatičke infrastrukture.

[388] FINA – Financijska agencija, http://www.fina.hr (21.01.2018.)
[389] sTESTA- Secure Trans European Services for Telematics between Administrations, http://ec.europa.eu/idabc/en/document/2097.html (21.01.2018.)
[390] APIS - Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, https://www.apis-it.hr/ (21.01.2018.)

CARNet[391] (engl. Croatian Academic and Research Network) je Hrvatska akademska i istraživačka mreža - nastala 1991. godine kao projekt Ministarstva znanosti i tehnologije Republike Hrvatske. CARNet javna je ustanova koja djeluje u sklopu Ministarstva znanosti i obrazovanja u području informacijskih i komunikacijskih tehnologija i njihovih primjena u obrazovanju u rasponu od mreža i internetske infrastrukture te preko elektroničkih javnih usluga do sigurnosti i korisničke podrške. CARNetove usluge u jednakoj su mjeri dostupne obrazovnim ustanovama (od osnovnoškolskog obrazovanja do visokog obrazovanja pa do znanstveno-istraživačkih centara i instituta) i pojedinačnim korisnicima.

Agencija za komercijalnu djelatnost, **AKD**[392] – je tvrtka specijalizirana u području identifikacijske industrije koja svoje proizvode i usluge isporučuje državnom i korporativnom sektoru stavljajući posebni naglasak na elektroničke identifikacijske dokumente građana, sve vrsta kartičnih proizvoda i proizvoda zaštićenih od krivotvorenja te pripadajućih i cjelovitih IT sigurnosnih rješenja. Ministarstvo unutarnjih poslova je izdavanjem **elektroničke osobne iskaznice** (eID) s identifikacijskim certifikatom u suradnji s AKD-om, koji je ujedno vjerodajnica najviše razine, omogućilo pristupanje svim elektroničkim uslugama.

Hrvatski nacionalni CERT[393], **CERT.hr** (engl. Computer Emergency Response Team) ima sjedište u CARNetu i odgovoran je za sprječavanje i zaštitu od računalnih prijetnji sigurnosti javno-informativnih sustava u Republici Hrvatskoj.

Osim nacionalnog CERT-a postoji i ZSIS CERT. **ZSIS CERT**[394] je pri Zavodu za sigurnost informacijskih sustava te je nadležan za državna tijela, tijela jedinica lokalne i područne samouprave. Osim toga pod nadležnost ZSIS CERT-a spadaju i pravne osobe s javnim ovlastima, ali i pravne i fizičke osobe koje u svom poslovanju imaju doticaj s klasificiranim i neklasificiranim podacima.

[391] CARNet – Croatian Academic and Research Network, Hrvatska akademska istraživačka mreža, https://www.carnet.hr/ (21.01.2018.)
[392] AKD - Agencija za komercijalnu djelatnost, http://www.akd.hr (21.01.2018.)
[393] CERT.hr, http://cert.hr/ (21.01.2018.)
[394] ZSIS CERT, https://www.zsis.hr/default.aspx?id=16 (21.01.2018.)

Hrvatska regulatorna agencija za mrežne djelatnosti (**HAKOM**[395]) je nacionalna regulatorna agencija za obavljanje regulatornih i drugih poslova u okviru djelokruga i mjerodavnosti propisanih Zakonom o elektroničkim komunikacijama, Zakonom o poštanskim uslugama i Zakonom o regulaciji tržišta željezničkih usluga.

Zakon o državnoj informacijskoj infrastrukturi je bio podloga za uspostavljanje **jedinstvenog Centra dijeljenih usluga**, **CDU ili SSC** (engl. Shared Service Centre). CDU treba poslužiti kao jedinstveno strateško mjesto upravljanja i koordiniranja razvoja državne informacijske infrastrukture. Osim toga, potrebno je standardizirati procese u samim tijelima javne uprave te u međusobnoj komunikaciji (standardizacija). Navedeni Zakon definira ustrojstvo **Registra ProDII**[396] (Javni registar za koordinaciju projekata izgradnje državne informacijske infrastrukture). U Registru ProDII se trebaju unijeti svi informatički projekti u tijelima javne uprave radi bolje koordinacije i racionalizacije raznih ulaganja u informacijsku infrastrukturu Republike Hrvatske.

Vlada Republike Hrvatske je 10. lipnja 2014. u produkcijski rad pustila **platformu e-Građani**. Autentikacija korisnika u sustavu e-Građani oslanja se na Nacionalni identifikacijski i autentifikacijski sustav - NIAS. Korisnici uslugama pristupaju preko Središnjeg državnog portala (gov.hr). Treća sastavnica platforme e-Građani je Osobni korisnički pretinac, OKP.

Problem raspršenosti informacija i elektroničkih javnih usluga po velikom broju stranica i poveznica se riješio uvođenjem sustava **Središnjeg državnog portala** (**gov.hr**[397]) koji integrira informacije i elektroničke javne usluge na jednom mjestu. Portal gov.hr pruža informacije o svim uslugama javne uprave (pokriva životne situacije), a osim toga integrira sve web stranice tijela javne uprave na jednom web mjestu na standardizirani način. Portal gov.hr udomljava i održava APIS IT. Usluge i informacije su podijeljene po kategorijama: zdravlje, rad, državljanstvo i isprave, pravna država i sigurnost, promet i vozila, financije i porezi, obitelj i život, hrvatski branitelji, obrazovanje, stanovanje i okoliš, poslovanje, aktivno građanstvo i slobodno vrijeme.

[395] HAKOM - Hrvatska regulatorna agencija za mrežne djelatnosti, https://www.hakom.hr (21.01.2018.)
[396] Hrvatski sabor (2014.), Zakon o državnoj informacijskoj infrastrukturi, https://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1840.html , čl. 6. (21.01.2018.)
[397] Središnji državni portal, gov.hr, https://gov.hr/ (21.01.2018.)

Nacionalni identifikacijski i autentifikacijski sustav (**NIAS**)[398] je jedinstveno mjesto verifikacije elektroničkog identiteta za pristupa elektroničkim javnim uslugama. NIAS je informacijsko sustav koji osigurava identifikaciju i autentifikaciju korisnika na nacionalnoj razini, a razvija ga i udomljava FINA. NIAS omogućava uključivanje više tipova vjerodajnica različitih razina sigurnosti. Razine sigurnosti mogu biti od najniže razine (2 – zaporka ili PIN), srednje razine (3 - soft certifikat ili uređaj za OTP, soft certifikat ili uređaj za OTP, hard certifikat) do najviše razine (4 - kvalificirani hard certifikat). Dostupne vjerodajnice navedene su u Listi prihvaćenih vjerodajnica[399].

Na dan 21. siječanj 2018. NIAS sustav je imao devetnaest prihvaćenih vjerodajnica:

- Razina 4 (2 vjerodajnice) - FinaCertRDC certifikat (FINA), Elektronička osobna iskaznica – eOI (MUP, AKD),
- Razina 3 (10 vjerodajnica) - FinaSoft certifikat (FINA), mToken za e-Građane (CARNet), Pametna kartica s certifikatom (HZZO), HPB token / mToken (HPB), ZABA token/m-token (ZABA), PBZ mToken/čitač kartice (PBZ), RBA token/mtoken i CAP čitač (RBA), SMS jednokratni pin (KentBank), OTP token/mobilni token (OTP), Erste mToken/Display kartica (Erste),

- Razina 2 (7 vjerodajnica) - e-Građani ePass (FINA), Korisničko ime i lozinka - AAI@EduHr (Srce), ePošta (HP), HT Telekom ID (HT), Korisničko ime i lozinka (HZMO, REGOS, HZZ).

Osobni korisnički pretinac (OKP) omogućava korisnicima zaprimanje poruka od tijela javne uprave. Putem Osobnog korisničkog pretinca (uz važeći OIB i korištenjem odgovarajuće vjerodajnice) korisnici mogu pregledati i upravljati porukama koje je zaprimio iz tijela javne uprave. Putem OKP-a korisnik može i pristupiti željenim elektroničkim javnim uslugama. Primjer poruka iz Osobnog korisničkog pretinca su: istek osobne iskaznice, putovnice, vozačke dozvole ili registracije vozila; obavijesti od REGOS-a, HZMO-a i HZZ-a, obavijesti o početku i završetku blokade računa, stanje uplata dopunskog zdravstvenog osiguranja, obavijest o verifikaciji podataka u državnim maticama i dr.

[398] NIAS - Nacionalni identifikacijski i autentifikacijski sustav, https://nias.gov.hr/ (21.01.2018.)
[399] Središnji državni portal, Lista prihvaćenih vjerodajnica na NIAS sustavu, https://gov.hr/e-gradjani/lista-prihvacenih-vjerodajnica/1667 (21.01.2018.)

Slijedi popis nekoliko zanimljivijih usluga koje se mogu obaviti putem sustava e-Građani:

- e-Zahtjev za izdavanje ePutovnice – usluga iz kategorije Pravna država i sigurnost. Omogućeno je predavanje zahtjeva za ePutovnicu (podnositelj zahtjeva treba posjedovati eOsobnu iskaznicu)
- e-Prijava boravišta hrvatskih državljana – usluga iz kategorije Pravna država i sigurnost koja je korisna pri promijeni mjesta boravka.
- Uvjerenje da se ne vodi kazneni postupak – usluga iz kategorije Pravna država i sigurnost. Ova usluga je posebno korisna prilikom traženja posla ili drugih zahtjeva kada se traži Potvrda o nekažnjavanju.
- e-Zahtjev za izdavanje vozačke dozvole – usluga iz kategorije Promet i vozila. Moguće je preko interneta zatražiti izdavanje vozačke dozvole (potrebna je eOsobna iskaznica).
- E-radna knjižica (Elektronički zapis o radno pravnom statusu) – usluga iz kategorije Rad. Pomoću ove usluge je moguće pronaći podatke o dosadašnjem stažu.
- e-Matične knjige – usluga iz kategorije Obitelj i život koja omogućava izdavanje rodnog lista.
- Zahtjev za izdavanje Europske kartice – usluga iz kategorije Zdravlje.
- e-Zapis o statusu studenta – usluga iz kategorije Odgoj i obrazovanje. Ova usluga daje studentima mogućnost izdavanja potvrda o studiranju koja se često traži prilikom natječaja za stipendije ili prilikom potrage za studentskim poslovima.
- e-Dnevnik za roditelje – usluga iz kategorije Odgoj i obrazovanje. Pomoću ove usluge roditelji mogu pregledavati ocjene svoje djece u osnovnim i srednjim školama.

6.4 ZAKLJUČAK

Po velikom broju različitog nazivlja za pojam e-Government, tj. elektronička javna uprava se može zaključiti da se radi o području koje se propulzivno mijenja i prilagođava novim potrebama i okolnostima. U svom magistarskom radu „Razvojne mogućnosti elektroničke

javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge“[400] zaključujem da se elektronička javna uprava može promatrati kroz transformaciju postojećeg načina rada državne uprave radi kvalitetnijeg služenja svrsi, te kroz učinkovitu isporuku transformiranih usluga okruženju (građanima, poslovnim subjektima i drugim tijelima javne uprave) kroz informacijsku infrastrukturu.

Pregledi stanja elektroničke javne uprave omogućavaju analizu napretka u korištenju elektroničke javne uprave te mogućnosti u realizaciji međunarodno deklariranih razvojnih ciljeva. Izvješće UN-a za 2005. o globalnom stanju elektroničke javne uprave[401] daje ambiciozne ciljeve u modelu razvoja elektroničke javne uprave te ima pet faza: početna prisutnost, istaknuta prisutnost, interaktivna prisutnost, transakcijska prisutnost i umrežena prisutnost (obuhvaća najnaprednije usluge elektroničke javne uprave.). Model razvoja e-Uprave UN-a i model Gartner grupe vrlo slični. Razlika je u tome što je izvješće UN-a u svom modelu Gartnerovu fazu web prisutnosti razdijelilo na faze Početne prisutnosti i Istaknute prisutnosti. Sukladno zadanim smjernicama Europske komisije su utvrđene razine zrelosti (ili razine informatiziranosti) po kojima se mjeri dostupnost javnih usluga na internetu. Navedene razine zrelosti se mjere od 1 do 5: informacija, jednosmjerna interakcija, dvosmjerna komunikacija, transakcija, ciljana usluga (proaktivnost/ automatizacija).

Osnovne funkcije javne uprave se mogu unaprijediti i korištenjem mobilnih i bežičnih tehnologija te korištenjem novog kanala isporuke za javne usluge, mobilnu javnu upravu (m-upravu). Kushchu i Kuscu u svom članku „Mobile Government“ navode[402] da se unatoč svom značaju, m-uprava ne može promatrati kao zamjena za e-upravu te da će u mnogim slučajevima biti komplementarna naporima e-uprave. Jacob Poushter (Pew Research Center)[403]. daje zaključak da postoji velika korelacija između bogatstva zemlje i

[400] Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf , str. 8 (17.03.2018.)
[401] United Nations, Department of Economic and Social Affairs (2005.), Global e-government readiness report 2005, New York, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf (11.01.2018.)
[402] Kushchu, I., Kuscu, H., Mobile Government, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040049.pdf , str. 1 (31.12.2017.)
[403] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ (01.01.2018.)

vlasništva nad pametnim telefonima. Što je zemlja bogatija i pametni telefoni su cjenovno dostupniji. Studija zaključuje i da postoji vrlo jaka korelacija između bogatstva zemlje (mjereno BDP-om) i pristupa internetu. Siromašnije zemlje kao što su u Južnoj i Jugoistočnoj Aziji imaju daleko manju razinu pristupa interneta u usporedbi s zemljama u razvoju u Južnoj Americi te posebno s razvijenim zemljama u Europi, Sjevernoj Americi i Australiji i Oceaniji. Europa 2006. nije po penetraciji interneta bila dostigla Sjevernu Ameriku, ali je od tada ubrzano radila na razvoju infrastrukture (posebno širokopojasnog interneta i mobilnih mreža) te na zajedničkim okosnicama za elektroničku javnu upravu.

Sektori elektroničke javne uprave se definiraju prema odnosu između sudionika elektroničke javne uprave. Seifert[404] navodi da se elektroničke javne usluge mogu svrstati u četiri sektora: G2C (engl. Government to Citizens), G2B (engl. Government to Business), G2E (engl. Government to Employees) i G2G (engl. Government to Government).

Europska unija strategijom Europa 2020 (donesene 2010. godine) postavlja tri prioriteta: pametni, održivi i uključivi rast. Inicijativa Digitalna agenda za Europu[405] je strateški kontekst koji je od donošenja strategije Europa 2020 najviše odredila smjer razvoja elektroničke javne uprave za zemlje EU i zemlje kandidate. Digitalna agenda propisuje 101 mjeru koje su grupirane u 7 prioritetnih područja djelovanja na razini Europske unije. Europska komisija daje ocjenu napretka u postizanju ciljeva Digitalne agende u zemljama Europske unije predstavljajući rezultate u okviru godišnjih izvješća naslovljenih s „Digital Agenda Scoreboard“, tj. semafor Digitalne agende. Akcijski plan 2011.-2015. (temeljen na Deklaraciji elektroničke javne uprave iz Malmöa iz 2009.) je doveo do razvoja tehnoloških rješenja ključnih za lakši pristupa elektroničkim javnim uslugama te njihovim lakšim korištenjem. U listopadu 2017. je objavljena nova deklaracija o elektroničkoj javnoj upravi „Deklaracija iz Tallina“ koja označava političku predanost država članica za ostvarivanjem vizije navedene u Akcijskom planu 2016.-2020. (naglasak je, međuostalim, na implementaciji Uredbe eIDAS i „once-only“ načela).

[404] Seifert, J. W. (2003.), A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance, https://fas.org/sgp/crs/RL31057.pdf , str. 4
[405] Europska komisija (2010., 2.), Digital agenda for Europe, Rebooting Europe's economy, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (12.01.2018.)

EIF je europski okvir za interoperabilnost koji daje specifične smjernice o tome kako uspostaviti interoperabilne elektroničke javne usluge. EIF nudi javnim upravama 47 konkretnih preporuka. Za Europsku uniju je u području interoperabilnosti jako bitna infrastruktura sTESTA kojom je dobivena mogućnost sigurne razmjene podataka između nacionalnih elektroničkih javnih uprava.

Europska komisija je 2012. godine usvojila je Strategiju za oslobađanje potencijala računalstva u oblaku. Time je iskazala namjeru uključivanja računalstva u oblaku u uvođenje interoperabilnih usluga za građane, tvrtke i tijela javne uprave. Studija Europske komisije o ekonomskom utjecaju računalstva u oblaku u Europi[406] ističe ekonomske prednosti objedinjavanja računalnih oblaka i slobodnog protoka podataka unutar Europske unije te navodi da bi široka primjena računalnih oblaka mogla doprinijeti kumulativnom ukupnom prihodu od 449 milijardi eura u BDP-u Europske unije.

Katulić[407] konstatira da Europa napokon ima novi pravni okvir zaštite osobnih podataka. Naime, radi se o uredbi naziva „Opća uredba o zaštiti podataka“[408], GDPR. Glavni ciljevi GDPR uredbe su: usklađivanje zakona o zaštiti podataka u cijeloj Europi, zaštita i osnaživanje osobnih podataka svih građana EU te promjena načina pristupa zaštiti podataka u organizacijama.

Što se tiče elektroničke javne uprave u Hrvatskoj, dan je pregled zakonskih osnova i strategija za razvoj hrvatske e-Uprave od 2004. do 2017. Strategija e-Hrvatska 2020[409] je donesena u svibnju 2017. te daje pregled razvoja informatizacije i elektroničkih usluga u javnom sektoru te ciljeve daljnjeg razvoja. Ova Strategija je u uskoj vezi s Digitalnom agendom za Europu. Glavni cilj donesene Strategije je osigurati povezivanje informacijskih sustava tijela javne uprave iz svih sektora na način da se građanima pruži što veći broj kompleksnih e-usluga i smanji opterećenje građana u interakciji s javnom

[406] Europska komisija (2014., 2.), Study on measuring the economic impact of cloud computing in Europe — SMART 2014/0031, http://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:173873-2014:TEXT:EN:HTML (18.01.2018.)
[407] Katulić. T. (2016.), Stiže Opća uredba o zaštiti podataka, https://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (29.05.2016.)
[408] Europski parlament i Vijeće (2016.), 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 te o stavljanju izvan snage direktive 95/46/EZ (Opća uredba o zaštiti podataka) (23.07.2017.)
[409] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 , str. 27 (10.01.2018.)

upravom. Za potrebe razvoja i podrške elektroničke javne uprave u Hrvatskoj, Ministarstvo uprave se oslanja na više organizacija i firmi: Financijsku agenciju, APIS, CARNET, AKD, HAKOM, CERT.hr i druge.

Vlada Republike Hrvatske je u lipnja 2014. u produkcijski rad pustila platformu e-Građani. Autentikacija korisnika u sustavu e-Građani oslanja se na Nacionalni identifikacijski i autentifikacijski sustav - NIAS. Korisnici uslugama pristupaju preko Središnjeg državnog portala, gov.hr. Treća komponenta platforme e-Građani je Osobni korisnički pretinac, OKP.

Dakle, da rezimiram, u ovom poglavlju su prikazani teorijski pojmovi elektroničke javne uprave, faze elektroničke javne uprave, pojam mobilne e-uprave te sektori e-uprave. Posebna je pažnja dana kontekstu razvoja elektroničke javne uprave u Europskoj Uniji i Republici Hrvatskoj. Smatram da je obrada ovog područja bitna za shvaćanje konteksta elektroničkog arhiva kao jednog bitnog dijela u napretku Republike Hrvatske u području e-uprave unutar Europske Unije. Iz tog razloga su obrađene strategije i agende Europske Unije i dana je poveznica s hrvatskom e-upravom i mjestu Republike Hrvatske na ljestvicama razvijenosti u mjerenjima EU. Osim toga, istraživanje razvijenosti e-uprave u Hrvatskoj koje slijedi u poglavlju 7. Analiza uspješnosti elektroničkih javnih uprava je napravljeno kao samostalni nastavak istraživanja u kojima sam sudjelovao na InterPARES Trust projektu u sklopu istraživanja e-servisa.

7. ANALIZA USPJEŠNOSTI ELEKTRONIČKIH JAVNIH UPRAVA

U ovom poglavlju će biti detaljno obrađene metodologije UN-a i Europske unije. Nakon proučavanja navedenih metodologija će biti dane i analize uspješnosti elektroničkih javnih uprava iz izvješća UN-a i Europske unije, tj. Europske komisije. Na kraju poglavlja će se dati i analiza uspješnosti hrvatske elektroničke javne uprave.

7.1 SVJETSKE METODOLOGIJE

U ovom potpoglavlju će biti obrađene najbitnije svjetske metodologije i izvješća koja se po tim metodologijama izrađuju. Metodologija Europske unije će se obraditi u idućem potpoglavlju.

UN je kroz izvješće „World Public Sector Report - e-government at the crossroads“ iz 2003. koje obrađuje svjetski javni sektor[410] predložio načela za uspješno planiranje i izgradnju elektroničke javne uprave. U navedenom izvješću je navedeno petnaest načela (Guiding Principles for Successful E-Government) koja su podijeljena u tri kategorije:

Tablica 9. Petnaest načela podijeljenih u tri kategorije iz UN izvješća World Public Sector Report - e-government at the crossroads

I.	Nužni razlozi za stvaranje usluga elektroničke javne uprave:
1.	Javljanje potrebe za stvaranjem elektroničkih usluga za društvo
2.	Potreba za povećanjem djelotvornosti postojećih javnih usluga
II.	Sposobnost javne uprave da koristi IKT za svoje aktivnosti
3.	Sposobnost financiranja projekata do kraja
4.	Postojanje odgovarajućih vještina javnih zaposlenika
5.	Postojanje koordinacije unutar i između državnih tijela radi izbjegavanja dupliciranja posla te radi osiguravanja kvalitetnog međudjelovanje javnih tijela
6.	Postojanje pravnih okvira za realizaciju elektroničkih javnih usluga
7.	Postojanje nužne informacijsko komunikacijske infrastrukture
8.	Odlučno političko vodstvo u stvaranju elektroničkih usluga te dugoročna predanost tom cilju
9.	Uključenost javnosti
10.	Planovi za izgradnju i nadogradnju ljudskih resursa i tehnološke infrastrukture

[410] United Nations, Department of Economic and Social Affairs (2003.), World Public sector Report 2003, E-Government at the Crossroads, https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/World%20Public%20Sector%20Report%20series/World%20Public%20Sector%20Report.2003.pdf , str. 8 (03.01.2018.)

11.	Izgradnja partnerstva između javne uprave, privatnog sektora i civilnih organizacija
12.	Kontinuirano nadgledanje i procjenjivanje razvoja i rada elektroničkih javnih usluga
III.	Nužni razlozi koji bi trebali privući korisnike korištenju elektroničke javne uprave
13.	Korisnici bi trebali moći jednostavno pristupiti javnim uslugama i na jednostavan način ih koristiti
14.	Pozitivna percepcija korisnika i korist od korištenja javnih usluga
15.	Privatnost i sigurnost korištenja usluge

Može se reći da su tada definirana načela i danas vrlo odgovarajuća. Iz njih je vidljivo da se kao bitni preduvjeti uspješne izgradnje i razvoja elektroničke javne uprave uglavnom navode:

- dobro definirani ciljevi,
- koordinacija i suradnja tijela javne uprave s korisnicima i međusobno,
- dobro osmišljeno zakonodavstvo,
- dobro razrađene dugoročne strategija razvoja e-uprave i tehnološke infrastrukture.

UN od 2001. godine na godišnjoj razini objavljuje Pregled (engl. Survey) efikasnosti elektroničkih javnih uprava u isporuci osnovnih ekonomskih i socijalnih usluga korisnicima u pet sektora: obrazovanje, zdravstvo, rad i zapošljavanje, financije i socijalna skrb te okoliš. UN agencija za ekonomske i socijalne poslove, UNDESA[411] (engl. UN Department of Economic and Social Affairs) je 2005. definirala prva četiri sektora, a peti sektor (okoliš) je UNDESA dodala 2012. Navedeni UN-ov Pregled identificira predloške u razvoju elektroničke javne uprave i procjenjuje po zemljama u kojem području su dosegli IKT potencijal te gdje mogu još napredovati. Ovaj Pregled je globalno izvješće koje procjenjuje razvitak elektroničkih javnih uprava svih članica UN-a.

Podaci iz UN Pregleda bi državama trebala omogućiti preuzimanje pozitivnih iskustava od drugih (da se identificiraju dobre strane, snage, ali i izazovi u području elektroničke javne uprave te da se oblikuju strategije i javne politike za razvoj i unapređenja e-uprave). Pregled sadrži: analitički dio, podatke o elektroničkim javnim upravama država te anekse s rangiranjem zemalja po uspješnosti. Analiziraju se tri dimenzije uz pomoć kojih građani i poslovni subjekti mogu imati koristi od elektroničkih javnih usluga i informacija: 1. koliko

[411] UNDESA, Department of Economic and Social Affairs, https://www.un.org/development/desa/en/ (04.01.2018.)

je telekomunikacijska infrastruktura odgovarajuća, 2. Sposobnost stanovništva da koristi informacijsko komunikacijske tehnologije i 3. Dostupnost online usluga i sadržaja.

Razvoj elektroničke javne uprave se prati preko **EGDI indeksa** (engl. **E-Government Development Index**). To je kompozitni indeks koji je temeljen na ponderiranom prosjeku tri indikatora koji su prethodno normalizirani. Trećinu predstavlja Infrastrukturni indeks telekomunikacija (TTI, engl. Telecommunication Infrastructure Index), trećinu Indeks ljudskog kapitala (HCI, engl. Human Capital Index) te trećinu Indeks online usluga (OSI, engl. Online Service Index). Formula za izračunavanje EDGI indeksa je sljedeća:

$$EDGI = \frac{1}{3} \times (OSI_{normalizirani} + TTI_{normalizirani} + HCI_{normalizirani})$$

Komponente EDGI indeksa se izračunavaju na sljedeći način:

- **OSI - Indeks online usluga** - se utvrđuje se na temelju odgovora na upitnik. Ovaj upitnik se sastoji od nekoliko skupova pitanja. Skupovi pitanja su sljedeći:
  - koncept cjelovitosti državne uprave,
  - višekanalna dostupnost usluga,
  - uklanjanje digitalnih podjela,
  - porast upotrebe usluga,
  - otvorenost uprave,
  - e-participacija.

- **TTI - Infrastrukturni indeks telekomunikacija –** se izračunava sljedećom formulom:

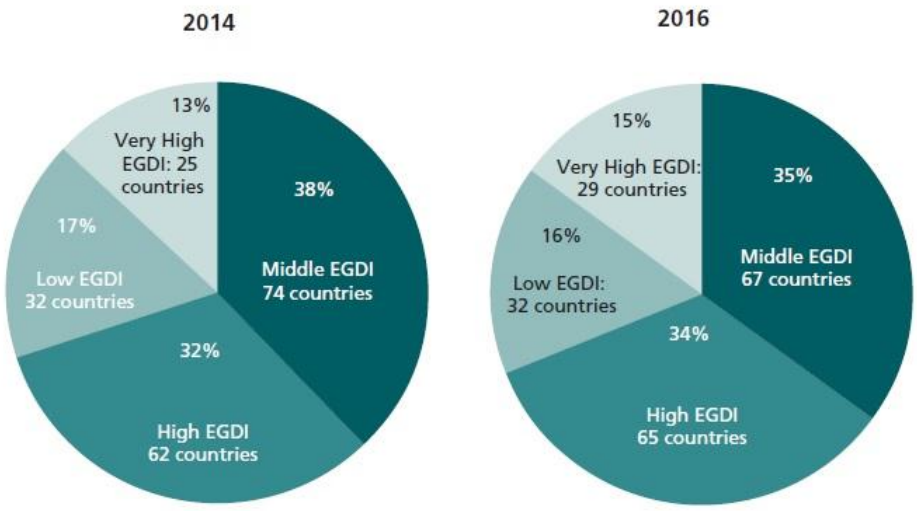
  TII = 1/5 × broj internetskih korisnika na 100 stanovnika +
  1/5 × broj fiksnih telefonskih priključaka na 100 stanovnika +
  1/5 × broj pretplata mobilne telefonije na 100 stanovnika +
  1/5 × broj priključaka bežičnog širokopojasnog interneta na 100 stanovnika +
  1/5 × broj priključaka fiksnog širokopojasnog interneta na 100 stanovnika

- **HCI - Indeks ljudskog kapitala** – izračunava se sljedećom formulom:

  HCI = 1⁄3× stupanj obrazovanja kod odraslih osoba +
  2⁄9× ukupan broj osoba koje pohađaju školovanje +
  2⁄9 × očekivano trajanje školovanja u godinama +

2⁄9 × prosječna starost osoba koje završavaju školovanje

Na slici 40 su prikazane zemlje grupirane po EDGI indeksu u 2016. uspoređujući sa stanjem indeksa iz 2014.



Slika 40. Usporedba stanja EDGI indeksa u UN Pregledima iz 2014. i 2016. godine, preuzeto iz United Nations, Department of Economic and Social Affairs (2016.)[412]

U 2016. je bilo više zemalja s vrlo visokim EDGI indeksom (većim od 0,75), tj. 29 zemalja je imalo takav indeks (za razliku od 2014. kada je takav indeks imalo 25 zemalja). Međutim, u 2016. godini se povećao i broj zemalja s visokim EGDI indeksom (vrijednost je između 0,5 i 0,75) za 3 zemlje (sa 62 na 65 zemalja). Broj zemalja s srednjim EDGI indeksom (vrijednost je u rasponu 0,25-0,5) je pao u 2016. za 7 (sa 74 na 67 zemalja). Broj zemalja s niskim EDGI indeksom (vrijednost je manja od 0,25) je ostao isti (32 zemlje). Usporedba ova dva grafa pokazuje da EDGI indeks globalno napreduje po zemljama.

U tablici 10 je navedeno prvih 15 zemalja po EDGI indeksu kako je navedeno u UN Pregledu za 2016. godinu.

[412] United Nations, Department of Economic and Social Affairs (2016.), UN E-Government Survey 2016, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016, str. 108 (31.12.2017.)

Tablica 10. Svjetski lideri u elektroničkoj javnoj upravi s vrlo visokim EDGI indeksom, preuzeto iz United Nations, Department of Economic and Social Affairs (2016.)[413]

	Zemlja	OSI	HCI	TII	EGDI
1.	**Ujedinjeno Kraljevstvo**	1,0000	0,9402	0,8177	**0,9193**
2.	**Australija**	0,9783	1,0000	0,7646	**0,9143**
3.	**Južna Koreja**	0,9420	0,8795	0,8530	**0,8915**
4.	**Singapur**	0,9710	0,8360	0,8414	**0,8828**
5.	**Finska**	0,9420	0,9440	0,7590	**0,8817**
6.	**Švedska**	0,8768	0,9210	0,8134	**0,8704**
7.	**Nizozemska**	0,9275	0,9183	0,7517	**0,8659**
8.	**Novi Zeland**	0,9420	0,9402	0,7136	**0,8653**
9.	**Danska**	0,7754	0,9530	0,8247	**0,8510**
10.	**Francuska**	0,9420	0,8445	0,7502	**0,8456**
11.	**Japan**	0,8768	0,8274	0,8277	**0,8440**
12.	**SAD**	0,9275	0,8815	0,7170	**0,8420**
13.	**Estonija**	0,8913	0,8761	0,7329	**0,8334**
14.	**Kanada**	0,9565	0,8572	0,6717	**0,8285**
15.	**Njemačka**	0,8406	0,8882	0,7342	**0,8210**

Hrvatska je u Pregledu za 2016. godinu smještena na 37. mjestu s EDGI indeksom od 0,7162 što je svrstava u zemlje s visokim indeksom. Komponenti indeksi za Hrvatsku za 2016. su sljedećih vrijednosti: OSI = 0,7464, TII = 0,5974, HCI = 0,8050. Kod EDGI indeksa za Hrvatsku za 2016. se može zaključiti da bi EDGI bio puno bolji kada bi se popravila telekomunikacijska infrastruktura u zemlji, a postoji mogućnost i za velik napredak u razvoju i unaprjeđenju online usluga. Zanimljivo je da je 2012. godine Hrvatska bila na 30. mjestu, a 2014. na 47. mjestu s EDGI indeksom od 0,6282.

Spremić i ja[414] smo dali usporedni prikaz uspješnosti e-uprava u svijetu kroz četiri javno objavljene studije (Accenture, Waseda, Economist Intelligence Unit i UN Pregled koji je već spomenut). Obrađene studije daju podatke za 2005. godinu.

Accenture[415] je globalna konzultantska kompanija čija su područja interesa razna (industrija, komunikacije i visoka tehnologija, banke, osiguranja, energetika i javna uprava). Accenture je objavila studije koje nastoje kvantitativno izmjeriti vrijednosti koje elektroničke javne usluge nude građanima. U istraživanju su uključene dvije glavne

[413] United Nations, Department of Economic and Social Affairs (2016.), UN E-Government Survey 2016, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016, str. 111 (31.12.2017.)
[414] Spremić, M, Brzica, H. (2008.), Comparative Analysis of e-Government Implementation Models and Progressive Services, WSEAS transactions on business and economics, http://www.wseas.us/e-library/transactions/economics/2008/27-124.pdf , str. 254-263 (20.01.2018.)
[415] Accenture, https://www.accenture.com (22.01.2018.)

komponente. Prva komponenta obuhvaća procjenu zrelosti i korisnosti usluga te procjenu upravljanja kroz nekoliko ključnih kategorija. Druga komponenta obuhvaća anketiranje oko 9000 osoba u analiziranim zemljama radi istraživanja percepcije i iskustava korisnika pri radu s elektroničkim uslugama javne uprave.

Waseda University Institute of e-Government[416] – je institut s japanskog sveučilišta Graduate School of Global Information and Telecommunication Studies. Izvješće daje pregled stanju elektroničkih javnih uprava u svijetu. Izvješće obrađuju šest područja kroz 28 indikatora.

Economist Intelligence Unit[417] je poslovno analitičarska grupacija unutar Economist Group koji je izdavač poslovnih tjednika i časopisa. Brojne korporacije, banke, sveučilišta i državne institucije koriste poslovne analize ove grupacije. Economist Intelligence Unit u kooperaciji s IBM Institute for Business Value od 2000. objavljuje analize e-spremnosti svjetskih ekonomija.

Usporedni prikaz je napravljen na način da je napravljeno bodovanje poredaka po zasebnim studijama (prvo mjesto donosi deset, a deseto mjesto 1 bod). U zadnjem stupcu je prikazan poredak prvih deset zemalja po broju bodova kroz četiri izvještaja. U zagradi je prikazan ukupan broj bodova za pojedinu zemlju. Ovaj usporedni prikaz smo napravili pod pretpostavkom da sve četiri studije imaju jednakovrijedne metodologije pa je bodovanje obavljeno linearno. Dakle, nema težinskih faktora pojedinih studija ili njihovih komponenti.

[416] Institute of e-Government Waseda University, https://www.waseda.jp/inst/cro/other-en/2017/03/08/3270/ (22.01.2018.)
[417] Economist Intelligence Unit, http://www.eiu.com/home.aspx (22.01.2018.)

Tablica 11. Usporedni prikaz po deset najuspješnijih elektroničkih javnih uprava u svijetu kroz četiri studije za 2005. godinu, preuzeto iz Spremić, M, Brzica, H. (2008.)[418]

	Accenture	Waseda	UN	Economist	Usporedni poredak
1.	Kanada	SAD	SAD	Danska	**SAD (38)**
2.	SAD	Kanada	Danska	SAD	**Danska (27)**
3.	Danska, Singapur	Singapur	Švedska	Švedska	**Kanada (22)**
4.		Japan	Ujedinjeno Kraljevstvo	Švicarska	**Singapur (20)**
5.	Australija, Francuska, Japan	Južna Koreja	Južna Koreja	Ujedinjeno Kraljevstvo	**Švedska (16)**
6.		Njemačka	Australija	Finska, Hong Kong	**Ujedinjeno Kraljevstvo, Australija (15)**
7.		Tajvan	Singapur		
8.	Norveška, Finska	Australija	Kanada	Nizozemska	**Japan (13)**
9.		Ujedinjeno Kraljevstvo	Finska	Norveška	**J. Koreja (12)**
10.	Nizozemska	Finska	Norveška	Australija	**Finska (11)**

Naveden je i poredak preostalih zemalja obrađenih u usporednom prikazu: 11.) Švicarska (7), 12.) Norveška i Francuska (6), 14.) Njemačka i Hong Kong (5), 16.) Tajvan i Nizozemska (4).

Iz ovog usporednog prikaza za 2005. godinu i prethodno navedene tablice poretka svjetskih lidera u elektroničkoj javnoj upravi iz UN Pregleda za 2016. može se zaključiti da se radi o uglavnom istim zemljama (uz nešto izmijenjen poredak) koje su istodobno i najrazvijenije zemlje svijeta. Može se dodatno zaključiti da su navedene zemlje prepoznale značaj ulaganja u telekomunikacijsku infrastrukturu te razvoja informacijskog društva.

7.2 METODOLOGIJA EUROPSKE UNIJE

Europska unija ima svoje zasebne metodologije kojima prati napredak u elektroničkoj javnoj upravi za zemlje članice i zemlje kandidate za članstvo. Jedan od bitnijih indikatora u uspješnosti e-Uprave je indeks **DESI**, Indeks digitalnog gospodarstva i društva (engl.

[418] Spremić, M, Brzica, H. (2008.), Comparative Analysis of e-Government Implementation Models and Progressive Services, WSEAS transactions on business and economics, http://www.wseas.us/e-library/transactions/economics/2008/27-124.pdf , str. 254-263 (20.01.2018.)

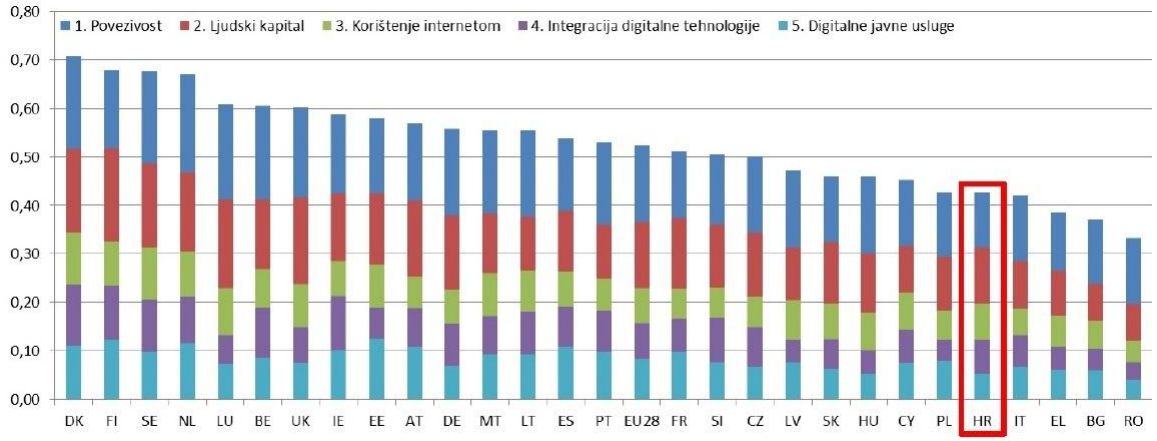
Digital **E**conomy and **S**ociety **I**ndex). Indeks DESI je definiran nastavno na donošenje Digitalne agende 2020 te nastojanja da se ustanovi jedinstveno digitalno tržište. Kroz taj indeks se mjeri napredak u ostvarivanju ciljeva Digitalne agende u zemljama članicama i zemljama kandidatima za članstvo. Europska komisija je na svojim web stranicama pod kategorijom Jedinstveno digitalno tržište[419] (engl. Digital Single Market) objavila Digitalni semafor[420] (engl. Digital Scoreboard). Digitalni semafor mjeri učinke Europe i država članica u širokom rasponu područja od povezivanja i digitalnih vještina do digitalizacije tvrtki i javnih usluga. Osim DESI indeksa, Digitalni semafor objavljuje podatke u sklopu Europskog izvješća o digitalnom napretku, **EDPR** (engl. **E**uropean **D**igital **P**rogress **R**eport).

DESI je složeni indeks koji u obzir uzima više indikatora kojima se prati napredak zemalja članica u ostvarivanju ciljeva Digitalne agende. Indeks DESI se izračunava pomoću pet komponenti od kojih svaka sudjeluje u indeksu s određenim postotkom:

1. Povezanost brzim internetom (engl. Connectivity) – 25%
2. Ljudski kapital (engl. Human Capital) – 25%
3. Korištenje interneta (engl. Use of internet) – 15%
4. Integracija digitalne tehnologije (engl. Integration of Digital Technology) – 20%
5. Elektroničke javne usluge (engl. Digital Public Services) – 15 %

EK u okviru Digitalnog semafora objavljuje podatke i grafikone za DESI indeks na svojim stranicama. Slijedi grafikon za DESI 2017. indeks (s pripadnim komponentama) po zemljama članicama (obrađeni su podaci za 2016. godinu). Slika 41 je preuzeta iz „Izvješća o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska“ .

[419] Digital Single Market, https://ec.europa.eu/digital-single-market/ (13.01.2018.)
[420] Digital Scoreboard, https://ec.europa.eu/digital-single-market/digital-scoreboard (13.01.2018.)



Slika 41. Indeks digitalnoga gospodarstva i društva (DESI) 2017. (poredak), preuzeto iz Europska komisija (2017., 3.) [421]

DESI 2017 donosi da Danska, Finska, Švedska i Nizozemska imaju najnaprednije digitalne ekonomije u EU, a slijede ih Luksemburg, Belgija, Velika Britanija i Irska. Rumunjska, Bugarska, Grčka i Italija imaju najniže rezultate za DESI 2017. Europska komisija navodi da su se u 2016. godini sve zemlje članice poboljšale u pogledu DESI indeksa. Najviše su napredovale Slovačka i Slovenija od zadnje godine (više od 0,04 za razliku od prosjeka EU koji se poboljšao za 0,028). S druge strane, u Portugalu, Latviji i Njemačkoj bilo je jako mali napredak (ispod 0,02).

Što se tiče Hrvatske, u promatranom kontekstu je stagnirala. Nalazi se na 23. mjestu od 28 zemalja. Napravila je minimalan napredak od zadnje godine (DESI je porastao s 0,40 na 0,43), ali je pala s 23. na 24. mjesto jer su ostale države napredovale brže. Izvješće o digitalnom razvoju Europe (EDPR) 2017. za profil Hrvatske navodi rezultate dobivene istraživanjem[422]: hrvatski se građani internetom služe više od prosjeka EU, njihove digitalne vještine neprestano se poboljšavaju (sa 17. mjesta u poretku 2015. se dogodio pomak na 13. mjesto u poretku za 2016. godinu). Što se tiče poslovnog sektora, upotreba digitalnih tehnologija je otprilike na razini prosjeka EU, a usluge u oblaku se koriste više od prosjeka (16 %, te 9. mjesto u poretku). Promet malih i srednjih poduzeća koji prodaju usluge i proizvode na internetu u porastu je i iznad je prosjeka Unije. Elektronički javni servisi se postupno poboljšavaju te su rezultati Hrvatske u području dostupnosti otvorenih podataka iznad prosjeka Europske unije. Problem je što se broj korisnika elektroničkih

[421] Europska komisija (2017., 3.), Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska, ec.europa.eu/newsroom/document.cfm?doc_id=44293, str.1 (15.01.2018.)
[422] Europska komisija (2017., 3.), Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska, ec.europa.eu/newsroom/document.cfm?doc_id=44293, str.2 (15.01.2018.)

javnih usluga povećava vrlo sporo. U smislu digitalizacije su rezultati jako loši i to u području povezivosti. Ograničen je širokopojasni pristup i pokrivenost u ruralnim područjima. Uz to su cijene fiksnog širokopojasnog pristupa vrlo visoke. Održani su izbori u Hrvatskoj (2015. i 2016. godine) što je dovelo do dodatne stagnacije u razvoju elektroničke javne uprave.

Nadalje, za proučavanje napretka elektroničke javne uprave u Europskoj uniji su bitna godišnja izvješća o usporednim analizama e-Uprava, eGovernment Benchmark Report (u nastavku Studija). Ova se Studija na godišnjoj razini izrađuje za Europsku komisiju od strane sljedećih konzultantskih kompanija i fakulteta: Capgemini[423], IDC[424], Sogeti[425] i Politecnico di Milano[426]. U ovom radu će se obrađivati metodologija kako je opisana u Studiji za 2016. godinu (engl. eGovernment Benchmark 2016[427]). Studija za 2016. prikazuje stanje napretka elektroničkih javnih usluga u Europi od 2015. Elektroničke javne usluge su ocijenjene u 34 zemalja sudionica istraživanja, uključujući sve tadašnje članice Europske unije (28). Studija upotrebljava metodu Mystery Shopping, pri čemu kvalitetu i količinu elektroničkih javnih usluga mjere procjenitelji koji djeluju kao korisnik. Kako bi se optimiziralo praćenje rezultata istraživanja, rezultati se bilježe kroz dvije vrste studija, od kojih se svaki obraća različitoj publici. Jedna studija je Pozadinska studija (engl. Background report) koja ima za cilj pružiti učinkovitu studiju o elektroničkoj javnoj upravi. U kraćoj Studiji o uvidu (engl. Insight report) pružaju se ključni nalazi i preporuke. Objavljivanje obje Studije dolazi sa skupom otvorenih, strojno čitljivih podataka. Takvi strojno čitljivi podaci su pogodni za daljnja istraživanja od strane akademske i znanstvene zajednice. Studija za 2016. obuhvaća sve procjene životnih događaja koje su nastale 2015. godine. Internetska stranica Europske komisije također uključuje podatke prikupljene u procjenama životnih događaja u 2012., 2013. i 2014. Studija 2016. je objavljena u zanimljivom trenutku: kada se zaključuje Akcijski plan e-Uprave 2011.-2015. i počinje provedba Akcijskog planu za eGovernment 2016-2020. Vrjednovanje (engl. Benchmarking) je važan aspekt Otvorene metode koordinacije, OMC[428] (engl. Open

[423] Capgemini, https://www.capgemini.com/ (14.01.2018.)
[424] IDC, https://www.idc.com/ (14.01.2018.)
[425] Sogeti, https://www.sogeti.com/ (14.01.2018.)
[426] Politecnico di Milano, https://www.polimi.it/ (14.01.2018.)
[427] Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856 (21.03.2018.)
[428] OMC, Open Method of Coordination, https://ec.europa.eu/culture/policy/strategic-framework/european-coop_en (14.01.2018.)

Method of Coordination) koju članice Europska unije koriste u razmjeni dobrih praksi. OMC metoda se unutar EU koristi i za oblikovanje politika i shema financiranja.

Studija elektroničke javne uprave (engl. eGovernment Benchmark) nadzire performanse e-Uprave u Europi već više od desetljeća. Europska komisija je za 2016. pokrivala 34 zemlje i svake godine donosi novu Studiju o tranziciji na suvremeni javni sektor. Od 2001. godine metoda je ažurirana nekoliko puta kako bi bila u skladu s tehnološkim i organizacijskim razvojem. Okosnica (engl. framework) za izradu nadziranje performansi e-Uprave je strukturiran oko četiri glavna prioritetna područja Akcijskog plana 2011.-2015.: Osnaživanje korisnika, Digitalno jedinstveno tržište, Učinkovitost i djelotvornost te Preduvjeti. Navedena prioritetna područja nisu samo pokazatelji. Naime, napredak na svakom prioritetnom području mjeri se s jednim ili više indikatora, takozvanim mjerila najviše razine (engl. top level benchmarks).

Dakle, Studija se sastoji od četiri mjerila najviše razine koja pokrivaju važne političke prioritete Europske unije[429]:

1. Usmjerenost korisniku (engl. User Centricity) - označava do koje mjere je usluga omogućena online,
2. Transparentnost (engl. Transparency) - ukazuje na to koliko su javne uprave transparentne u pogledu: a) vlastitih odgovornosti i uspješnosti, b) procesu pružanja usluga i c) uključenih osobnih podataka,
3. Prekogranična mobilnost (engl. Cross Border Mobility) - pokazuje koliko europskih korisnika može koristiti elektroničke javne usluge u drugoj zemlji,
4. Ključni čimbenici (engl. Key enablers) - označava opseg korištenja pet tehničkih preduvjeta za elektroničku javnu upravu.

Većina mjerila najviše razine sastoji se od više pokazatelja. Da bi se procijenili svi indikatori najviše razine, trenutačna mjerila koriste već spomenutu metodu Mystery Shopping. Procjenitelji po Mystery Shopping metodi djeluju kao potencijalni korisnici i slijede detaljan, objektivni popis za provjeru evaluacije (engl. evaluation checklist). Nakon vježbe Mystery Shopping-a, svi rezultati se provjeravaju i potvrđuju od država članica. U ovom intenzivnom kolaboracijskom procesu sudjeluju predstavnici zemalja. Države

[429] Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856, str. 20 (14.01.2018.)

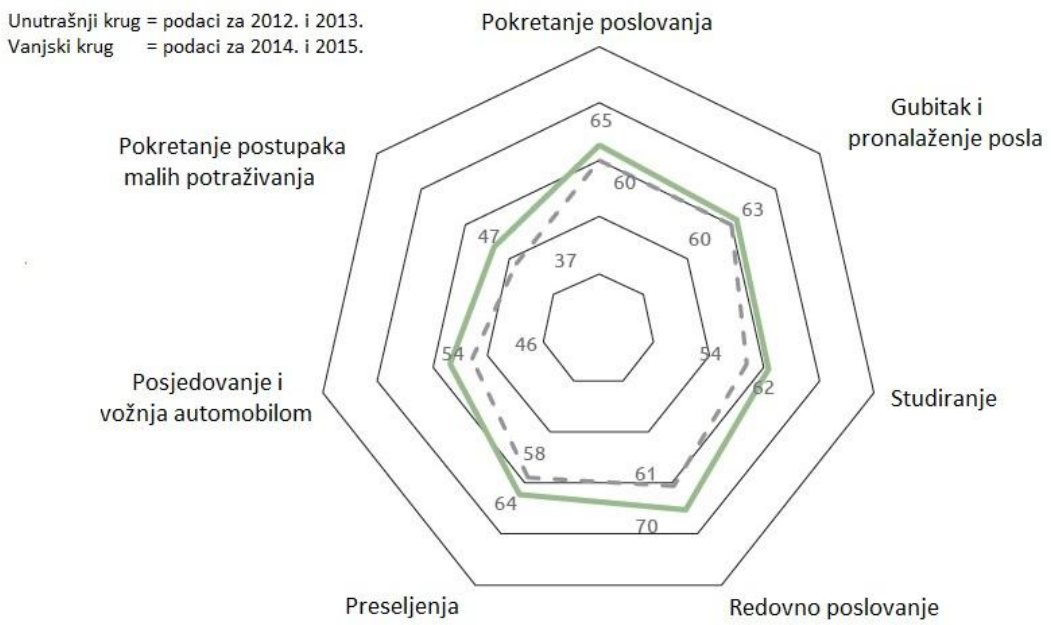
članice uključene su na početku i na kraju evaluacije. Na početku su uključene radi potvrđivanja uzorka i ključnih karakteristika usluga koje se ocjenjuju, a na kraju trebaju potvrditi rezultate istraživanja u suradnji s odgovornim organizacijama u zemlji i eventualno ispraviti očigledne pogrešne rezultate. Postoji jedna iznimka - određivanje jednostavnosti i brzine korištenja, što je osobna procjena procesa životnog događaja od strane istraživača. Iz tog razloga se rezultati tog mjerenja ne mogu provjeravati i potvrđivati od država članica. Predmet istraživanja je skup od sedam životnih događaja.

Sedam definiranih životnih događaja su:

1. Pokretanje poslovanja i ranih poslova trgovanja (engl. Starting up a business and early trading operations),
2. Redovno poslovanje (engl. Regular business operations),
3. Gubitak i pronalaženje posla (engl. Losing and finding a job),
4. Preseljenje (engl. Moving),
5. Pokretanje postupka malih potraživanja (engl. Starting a small claims procedure),
6. Posjedovanje i vožnja automobilom (engl. Owning and driving a car),
7. Studiranje (engl. Studying).

Navedenih sedam životnih događaja skupa predstavljaju gotovo sve domene javne uprave. Svaki životni događaj procjenjuje se jednom svake dvije godine. Za 2015. godinu su procijenjena četiri životna događaja: redovno poslovanje, preseljenja, posjedovanje i vožnja automobila i pokretanje postupka malih potraživanja. Ovime je dovršen drugi ciklus mjerenja. Kako su svi životni događaji dvaput procijenjeni bila je moguća puna analiza napretka po zemljama i za cijelu EU.

Slika 42 pokazuje napredak koji je napravio svaki od sedam životnih događaja s obzirom na prethodnu godinu, ilustriran prosjekom svih mjerila najviše razine u ovoj procjeni. Unutrašnji krug se odnosi na 2012. i 2013. godinu, a vanjski krug se odnosi na 2014. i 2015. godinu.

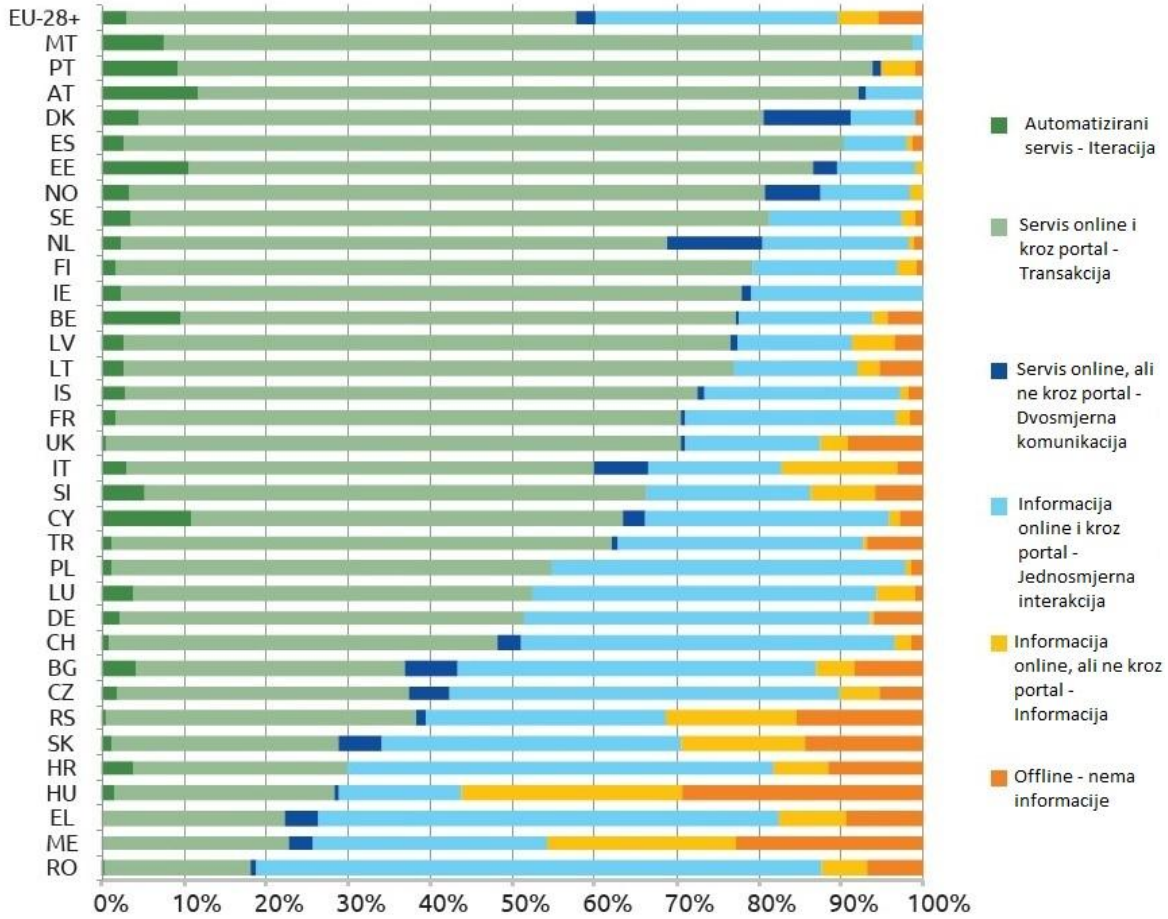


Slika 42. Agregirani EU28+ rezultati za životne događaje u Studiji elektroničke javne uprave 2016., preuzeto iz Capgemini et al. (2016.)[430]

Za sve životne događaje, prosječni rezultat je poboljšan u drugom mjerenju u usporedbi s prvim mjerenjem. Najviši rezultat je za događaje iz poslovnog života, odnosno Pokretanje poslovanja (65%) i Redovne poslovanje (70%). Pokretanje postupaka malih potraživanja procijenjeno je najniže u 2012./2013. i još uvijek ima najniži apsolutni rezultat u 2014./2015. Međutim, za ovaj životni događaj postignut je najveći napredak (porast od 10 postotnih bodova). S druge strane, rezultat za životni događaj Gubitak i pronalaženje posla bio relativno visok u prvom mjerenju, ali je u drugom mjerenju napredak bio ograničen (samo 3%).

U Studiji 2016 su, nadalje, objavljeni rezultati istraživanja dostupnosti javnih usluga po zemljama (preko životnih događaja, za razdoblje 2014.-2015. za zemlje članice i članice kandidate, tj. EU28+). Na slici 43 su prikazani rezultati navedenog te su različitim bojama označene razine dostupnosti (informatiziranosti po Bangemannovom izvještaju).

[430] Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856, str. 22 (14.01.2018.)



Slika 43. Rezultati istraživanja dostupnosti javnih usluga u Studiji elektroničke javne uprave 2016, preuzeto iz Capgemini et al.[431]

Za EU28 + prosjek je da se 60% svih usluga e-uprave nudi potpuno online (tamne i svijetlo zelene i tamno plava trake). To je povećanje od 7 postotnih bodova u odnosu na rezultate prošle godine. Za 34,5% svih usluga korisnici nisu mogli potpuno pristupiti uslugama, ali su barem neki podaci bili dostupni putem portala (svijetlo plava traka) ili su bile dostupne, ali ne kroz portal (narančasta traka). Još uvijek 5,5% usluga nije ponuđeno u elektroničkom obliku. Međutim, taj je postotak smanjen za 3,5% u odnosu na prošlu godinu. U tablici 12 su uparene razine dostupnosti elektroničkih javnih usluga iz Studije elektroničke uprave 2016 (kako su navedene na slici 43 u kazalu) te razine informatiziranosti/zrelosti iz Bangemannovog izvještaja.

[431] Isto, str. 27

Tablica 12. Uparivanje razine dostupnosti elektroničkih javnih usluga iz Studije elektroničke javne uprave 2016 te razine informatiziranosti/zrelosti iz Bangemannovog izvještaja

Razina dostupnosti (Studija 2016)	**Razina informatiziranosti/ zrelosti (Bangemann) - opis**	**Razina informatiziranosti/ zrelosti (Bangemann) - broj**
Automatizirani servis (engl. Automated service)	Iteracija	5
Servis online i kroz portal (engl. Service online and through portal)	Transakcija	4
Servis online, ali ne kroz portal (engl. Service online but not through portal)	Dvosmjerna komunikacija	3
Informacija online i kroz portal (engl. Information online and through portal)	Jednosmjerna interakcija	2
Informacija online, ali ne kroz portal (engl. Information online but not through portal)	Informacija	1
Offline	Nema informacije	0

U Studiji elektroničke javne uprave 2016 postoji objašnjena i metoda za klastere zemalja po kontekstu i performansama elektroničke javne uprave[432] (engl. Method for clustering countries on eGovernment context and performance). Prvi korak analize ima za cilj mjerenje zrelosti (engl. maturity) zemlje. Apsolutni pokazatelji koji se koriste za mjerenje zrelosti izvedbe elektroničke javne uprave su penetracija i digitalizacija. Penetracija predstavlja korištenje elektroničkih javnih usluga, a mjeri se pomoću pokazatelja Eurostata[433]. Iz navedenog razloga sljedeće zemlje ne mogu biti uključene: Švicarska, Srbija i Crna Gora. Digitalizacija mjeri učinkovitost i djelotvornost javne administracije u unutarnjim postupcima. Podaci za digitalizaciju se dobivaju pomoću već spomenute istraživačke metode Mystery Shopping. Drugi korak analize procjenjuje kako vanjski

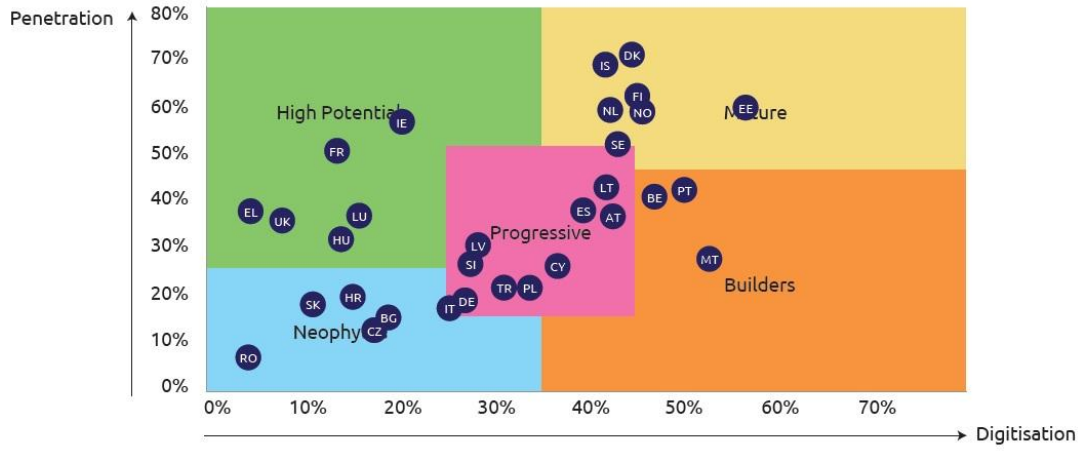
[432] Isto, str. 60

[433] Eurostat, Statistički ured Europskih zajednica prikuplja i objavljuje statističke podatke iz država članica, država izvan Europske unije te od međunarodnih organizacija kako bi informirao institucije Europske unije i omogućio praćenje učinaka politika Zajednice.
https://hr.wikipedia.org/wiki/Statistički_ured_Europskih_zajednica (15.01.2018.)

čimbenici oblikuju specifičan kontekst pojedinih zemalja. Tri su kategorije ovih kontekstualnih ili relativnih pokazatelja: 1. Opskrba države: širenje usluga e-uprave, uključujući ulaganja i napore u inovacijama, difuziju i kvalitetu usluga. 2. Potrebe elektroničke javne uprave: spremnost građana da koriste online usluge. 3. Okoliš: socio-demografski podaci, ICT spremnost i struktura upravljanja. Postoji više različiti klastera koji se mogu dobiti ovom analizom. Za ovaj rad su bitni klasteri zemalja temeljenih na faktorima izvedbe elektroničke javne uprave (engl. Clusters of countries based on eGovernment performance factors). Do raspodjele zemalja po ovim klasterima se dolazi pomoću rezultata analize učinka elektroničke javne uprave izmjerene s dva apsolutna pokazatelja: penetracije i digitalizacije. Postoji 5 klastera zemalja temeljenih na faktorima izvedbe elektroničke javne uprave:

1. Početnici (engl. Neophytes),
2. S visokim potencijalom (engl. High Potentials),
3. Progresivni (engl. Progressive),
4. Napredni (engl. Builders),
5. Zreli (engl. Mature).

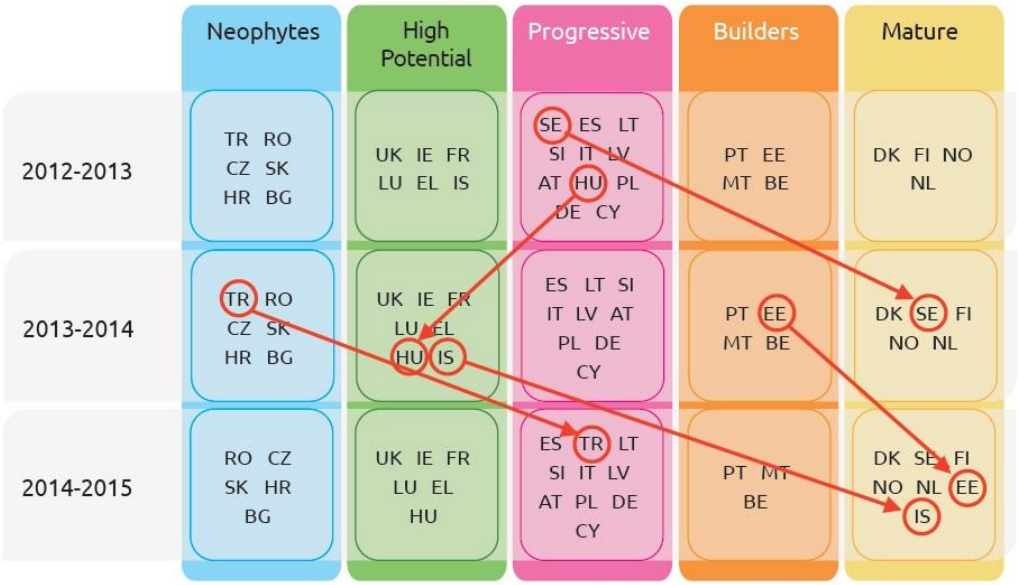
Na slici su prikazani klasteri zemalja temeljenih na faktorima izvedbe elektroničke javne uprave i njihove performanse za 2014. i 2015. godinu[434]. Prikazane su dvije osi (penetracija i digitalizacija). Svaki klaster ima raspone postotaka penetracije i digitalizacije. Unutar svakog klastera su smještene zemlje po svojim performansama.



Slika 44. Klasteri zemalja temeljenih na faktorima izvedbe elektroničke javne uprave i njihove performanse za 2014. i 2015. godinu, preuzeto uz Capgemini et al. (2016., 2.)

[434] Capgemini et al. (2016., 2.), eGovernment Benchmark 2016, Final insight report – volume 1, https://www.capgemini.com/wp-content/uploads/2017/07/egovernment_benchmark_2016.pdf , str. 65 (15.01.2018.)

Hrvatska se u 2014. i 2015. nalazila u klasteru Početnika zajedno s Rumunjskom, Slovačkom, Češkom i Bugarskom. Zrele zemlje su mahom na sjeveru Europe (Danska, Švedska, Finska, Norveška, Nizozemska, Estonija i Island). Pozadinska Studija donosi i vrlo zanimljiv dinamički prikaz kretanja zemalja po klasterima u razdoblju 2012.-2015. godine[435].



Slika 45. Dinamički prikaz kretanja zemalja po klasterima u razdoblju 2012.-2015, preuzeto iz Capgemini et al. (2016.)

U prikazanoj analizi, klasteri se vremenski ne zadržavaju na okupu već se zemlje ovisno o svom napretku miču u druge klastere. grupe nisu dinamične. Postoje i različiti putovi izvedbe, tj. nemaju sve zemlje jednak put izvedbe. Island, koji ima jednu od najviših razine penetracije, poboljšavao je razinu digitalizacije tijekom godina sve do dostizanja klastera Zrelih. Estonija je s druge strane već 2012. Imala veliku razinu digitalizacije, a do 2015. je povećavala i penetraciju te je na taj način dosegnula klaster Zrelih. Hrvatska se u promatranom razdoblju lagano pomiče naprijed. Dok se penetracija gotovo neznatno poboljšala, razina digitalizacija se poveća oko 10%. Uglavnom, velik je prostor za napredak Hrvatske i u razvoju elektroničkih javnih usluga i u razini digitalizacije.

[435] Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856, str. 96 (21.03.2018.)

Studija 2016 o uvidu donosi retrospektivu za razdoblje 2012.-2015. te sedam digitalnih izazova za javnu upravu u narednom vremenu. U retrospektivi se navodi[436] da je europska digitalna dijagonala ubrzala napredak elektroničke javne uprave. Online dostupnost javnih usluga je za EU28+ dosegla 81% (što je 9% više nego 2013.), a online iskoristivost je 83% (što je 4% više nego 2013.). S druge strane lakoća i brzina korištenja elektroničkih javnih usluga je imala slab pomak, samo 1% od 2013. Što se tiče transparentnosti, zaključuje se da je potrebno više unaprijediti transparentnost procesa samih servisa, osobnih podataka i javnih tijela diljem Europe. Ovo mjerilo se poveća za 8% (na 56% u 2015.). Što se tiče prekogranične mobilnosti, zaključeno je da su prekogranični servisi nužnost za uspostavljanje jedinstvenog digitalnog tržišta u punoj mjeri. Mjerilo prekogranične mobilnosti se povećalo za 11%, a mobilnosti poslovanja za 13% (na 64%). Što se tiče isporuka aplikacija u mobilnom kanalu iznesen je podataka da samo 1 od 3 stranice javne uprave ima isporuku i kroz mobilni kanal.

Izneseno je i sedam digitalnih izazova:

1. Servisi trebaju biti elektronički po definiciji (engl. Digital by default),
2. Samo-jednom načelo (engl. Once-only principe),
3. Uključivost i dostupnost (engl. Inclusiveness and accessibility),
4. Otvorenost i transparentnost (engl. Opennes & transparency),
5. Prekograničnost po definiciji (engl. Cross-border by default),
6. Interoperabilnost po definiciji (engl. Interoperability by default),
7. Pouzdanost i sigurnost (engl. Trustworthiness & security).

7.3 ANALIZA USPJEŠNOSTI ELEKTRONIČKE JAVNE UPRAVE U REPUBLICI HRVATSKOJ

Strategija e-Hrvatska 2020 (objavljena u svibnju 2017.) navodi[437] da je stanje u Republici Hrvatskoj još takvo da je još uvijek velika većina elektroničkih javnih usluga na razini zrelosti 2 (jednosmjerna interakcija). Razlog tome je taj što do ljeta 2014. godine (tj. do puštanja u rad sustava e-Građani) nije bilo jedinstvenog mjesta u virtualnom svijetu za

[436] Capgemini et al. (2016., 2.), eGovernment Benchmark 2016, Final insight report – volume 1, https://www.capgemini.com/wp-content/uploads/2017/07/egovernment_benchmark_2016.pdf , str. 38 (15.01.2018.)
[437] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 , str. 25 (10.01.2018.)

interakciju s građanima i poslovnim subjektima. Do tada je svako tijelo javne uprave koje je htjelo pružati personalizirane usluge moralo razviti i svoj sustav izdavanja mehanizama za verifikaciju elektroničkog identiteta.

Međutim, stanje se mijenja ubrzano na bolje. Na dan 21. siječanj 2018. godine. sam proveo istraživanje broja objavljenih usluga koje su dostupne preko sustava e-Građani. Navedenog datuma su bile dostupne 46 elektroničke javne usluge iz kategorije e-Građani[438] i 92 elektroničke javne usluge pod kategorijom Ostale e-usluge u Republici Hrvatskoj. Broj integracija novih usluga na sustav e-Građani se svakim danom sve više povećava. Primjer je nova usluga e-Zahtjev za izdavanje ePutovnice koja je puštena u rad 1. siječnja 2018. godine[439].

Što se tiče pozicije Hrvatske ona je u Pregledu UN-a za 2016. Godinu (već je spomenuto u ovom radu) smještena na 37. mjestu s EDGI indeksom od 0,7162 što je svrstava u zemlje s visokim indeksom. Komponenti indeksi za Hrvatsku za 2016. su sljedećih vrijednosti: OSI = 0,7464, TII = 0,5974, HCI = 0,8050. Kod EDGI indeksa za Hrvatsku za 2016. se može zaključiti da bi situacija bila puno bolja (EDGI bi imao veću vrijednost) kada bi se popravila telekomunikacijska infrastruktura u zemlji te mogućnost njezinog korištenja (TII=0,5974 što može biti i puno bolje). Postoji i mogućnost za velik napredak u razvoju i unaprjeđenju online usluga (OSI=0,7464). U UN Pregledu za 2012. Godinu, Hrvatska je bila na 30. mjestu, a 2014. Tek na 47. mjestu s EDGI indeksom od 0,6282.

Što se tiče Digitalnog semafora Europske komisije i DESI indeksa, Hrvatska je u Studiji za 2016. (obrađeni su rezultati za 2015. uz usporedbu s razdobljem od 2012.) stagnirala. Hrvatska se nalazila na 23. mjestu od 28 zemalja što znači pad za jedno mjesto (s 23. na 24.). Napravila je minimalan napredak od zadnje godine (DESI je porastao s 0,40 na 0,43), ali su ostale države napredovale brže. Kao jedan od razloga stagnacije u Izvješće se navodi da su održani izbori u Hrvatskoj (2015.) što je dovelo do dodatne stagnacije u razvoju elektroničke javne uprave.

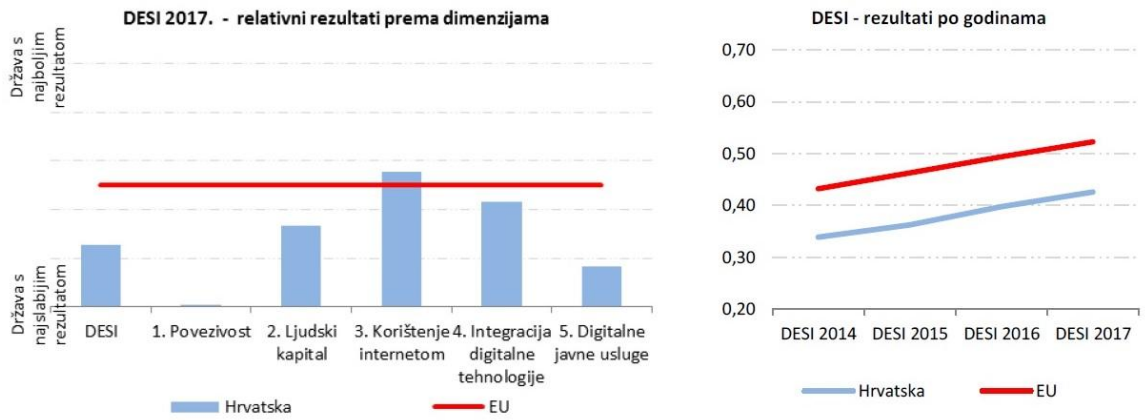
[438] Središnji državni portal, Elektroničke javne usluge iz kategorije e-Građani i kategorije Ostale e-Usluge u Republici Hrvatskoj, https://pretinac.gov.hr/KorisnickiPretinac/eGradani.html (21.01.2018.)
[439] Jutarnji list, Hrvati od danas dobivaju e-putovnice Nema više čekanja na šalteru, isprava stiže na kućnu adresu, evo što sve treba učiniti i koliko će to koštati, https://www.jutarnji.hr/vijesti/hrvatska/hrvati-od-danas-dobivaju-e-putovnice-nema-vise-cekanja-na-salteru-isprava-stize-na-kucnu-adresu-evo-sto-sve-treba-uciniti-i-koliko-ce-to-kostati/6892977/ (21.01.2018.)

Studija Europske komisije za 2016. Hrvatsku smješta u klaster početnika. Hrvatska se od početka istraživanja nalazila u klasteru početnika, a 2014. i 2015. se situacija isto nije popravila. Klaster zemalja početnika zajedno s Hrvatskom čine Rumunjska, Slovačka, Češka i Bugarska. Za promatrano razdoblje 2012.-2015. Hrvatska se po DESI indeksu lagano pomiče naprijed. Penetracija (korištenje elektroničkih javnih usluga) se gotovo neznatno poboljšala, ali se razina digitalizacije povećala za oko 10% (digitalizacija mjeri učinkovitost i djelotvornost javne administracije u unutarnjim postupcima). Europska komisija u Studiji za 2016. Zaključuje da je velik prostor za napredak Hrvatske i u sferi penetracije i u razini digitalizacije.

Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska[440] donosi još novije podatke za Hrvatsku s konkretnim preporukama. Izvješće navodi da Hrvatska pripada skupini manje uspješnih zemalja[441] u smislu digitalnog razvoja. Kao manje uspješne zemlje su navedene: Rumunjska, Bugarska, Grčka, Italija, Hrvatska, Poljska, Cipar, Mađarska i Slovačka. Kao okolnost manje uspješnosti se navodi i u održanim izborima u 2015. godini što je dovelo do razdoblja mirovanja u strateškim smjernicama i aktivnostima. Nadalje, vlada koja je preuzela vlast nakon izbora u rujnu 2016. radi na osnivanju Središnjeg državnog ureda za razvoj digitalnog društva. Bitne zadaće tog ureda bit će: pružanje podrške vladi RH u razvoju infrastrukture informacijskih i komunikacijskih tehnologija, podrška pri razvoju elektroničkih javnih usluga. Osim toga želi se popularizirati razvoj digitalnog društva među građanima, poslovnim subjektima i u tijelima javnog sektora.

Na slici 46 je naveden prikaz DESI 2017. indeksa za Hrvatsku i Europsku uniju po DESI dimenzijama te kretanje veličine DESI indeksa po godinama za RH i EU.

[440] Europska komisija (2017., 3.), Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska, ec.europa.eu/newsroom/document.cfm?doc_id=44293 (15.01.2018.)
[441] Isto, str. 2



Slika 46. DESI 2017. relativni rezultati prema dimenzijama, preuzeto iz Europska komisija (2017., 3.)[442]

Izvješće o digitalnom razvoju Hrvatske 2017. navodi da je u dimenziji povezivosti Hrvatska ostvarila određeni napredak u pogledu uspješnosti, ali je i dalje na dnu ljestvice Unije. Prema pokazatelju dostupnosti fiksnih širokopojasnih mreža Hrvatska se nalazi neznatno ispod prosjeka Unije, ali nije postignut napredak u pogledu njihove iskorištenosti. Naime, samo je 70% kućanstava pretplaćeno na fiksne širokopojasne mreže. Isto tako, dostupnost širokopojasnih mreža velike brzine poboljšala se u apsolutnom smislu kao i iskorištenost takvih mreža (povećanje sa 3% na 10% svih mreža), ali su oba pokazatelja i dalje daleko ispod prosjeka Unije. Slabim rezultatima u području iskorištenosti širokopojasnih mreža pridonose ograničena potražnja za širokopojasnim mrežama velike brzine te financijska nepristupačnost. Bitno je napomenuti da je Hrvatska zemlja s najskupljom pretplatom za samostalni fiksni širokopojasni pristup u cijeloj Europskoj uniji (navedena pretplata iznosi čak 2,9% prosječnog bruto dohotka dok je prosjek Europske unije od 1,2% prosječnog bruto dohotka). U Hrvatskoj se povećava iskorištenost mobilnih širokopojasnih usluga, ali je zato pokrivenost 4G mrežama skromna (Hrvatska u tom pogledu zauzima 25. mjesto). Na razini EU je usvojena Direktiva 2014/61/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina. Hrvatska je u srpnju 2016. donijela „Strategiju razvoja širokopojasnog pristupa u Republici Hrvatskoj za razdoblje 2016. – 2020."[443]. Navedena strategija navodi da su glavni ciljevi koji se moraju ispuniti do 2020.

[442] Isto, str. 2
[443] Vlada Republike Hrvatske (2016.), Strategija razvoja širokopojasnog pristupa u Republici Hrvatskoj za razdoblje 2016. – 2020, http://www.mppi.hr/UserDocsImages/Strategija-sirokopojasni-pristup2016-2020-usvojeno%20na%20VRH.pdf (21.01.2018.)

usmjereni su na: univerzalnu pokrivenost mrežama sljedeće generacije s brzinama većima od 30 Mbps te zastupljenost brzina većih od 100 Mbps u najmanje 50% kućanstava. Tek se u prosincu 2016. donosi Zakon o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina[444]. Za očekivati je da će se u narednom razdoblju povećati iskorištenost širokopojasnih priključaka u Republici Hrvatskoj.

Što se tiče dimenzije ljudskog kapitala, Hrvatska tu napreduje. Broj korisnika interneta i digitalne vještine se neprestano poboljšavaju. Izvješće o digitalnom razvoju 2017 navodi da 55% Hrvata ima barem osnovne digitalne vještine (prosjeka Unije je 56%). U pogledu radne snage za IKT sektor za 2016. navedeni su podaci da samo 2,7% radne snage čine IKT stručnjaci. Još zabrinjavajuće je da je udio osoba s diplomom iz znanosti, tehnologije i matematike (STEM područje) iznosio samo 1,6% u dobnoj skupini od 20 do 29 godina. Općenito je u Hrvatskoj veliki problem sa pronalaskom i zapošljavanjem stručnjaka za IKT. Prema posljednjim procjenama stručnjaka[445], postoji deficit od 2000 programera u Hrvatskoj godišnje. Vlasnici privatnih firmi navode da nemaju dovoljno ljudi za provedbu svih projekata koje traže investitori. Naime, novca stvarno ima, ali nedostaju ljudi koji će taj novac pretvoriti u gotove projekte.

Što se tiče sklonosti pojedinaca da se služe uslugama na internetu Hrvatska napreduje, ali drugi napreduju brže tkao da je Hrvatska pala u poretku sa 13. na 14. mjesto. Međutim, ovo je dimenzija DESI indeksa u kojem Hrvatska postiže najbolje rezultate i nalazi se iznad prosjeka Unije.

U području integracije digitalnih tehnologija u poduzećima Hrvatska ima dobre rezultate. Hrvatska poduzeća koriste usluge u oblaku više od prosjeka, ali je korištenje e-računa slabo. Europska komisija za hrvatsko gospodarstvo navodi da bi bilo još korisnije kad bi hrvatska poduzeća imala na raspolaganju ciljanu strategiju digitalizacije.

Što se tiče dimenzije e-upravi, Hrvatska je u prošloj godini postigla određeni napredak, ali je i ovdje pala s 25. na 26. mjesta. Broj korisnika usluge e-uprave polako se povećava, ali

[444] Sabor Republike Hrvatske (2016.), Zakon o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina, https://narodne-novine.nn.hr/clanci/sluzbeni/2016_12_121_2623.html (21.01.2018.)
[445] T-Portal, Pogledajte koliko zarađuju programeri u Hrvatskoj i koji programski jezik je najisplativiji, https://www.tportal.hr/tehno/clanak/pogledajte-koliko-zaraduju-programeri-u-hrvatskoj-i-koji-programski-jezik-je-najisplativiji-foto-20180116 (17.01.2018.)

nije postignut napredak u pogledu isporuke usluga. Navedeno se objašnjava time što zbog političke situacije u protekloj godini nije bilo mnogo aktivnosti u pogledu usluge e-uprave (izbori i politička nestabilnost).

Izvješće o digitalnom razvoju Hrvatske 2017. Zaključno navodi da se daljnjim razvojem i provedbom strategije e-uprave te uključujući alata e-poslovanja može pridonijeti uspješnijem okruženju e-uprave. Uspješan razvoj elektroničke javne uprave u Hrvatskoj bi mogao donijeti znatne uštede građanima, poslovnim subjektima i javnoj upravi.

7.4 ZAKLJUČAK

U ovom poglavlju su detaljnije obrađena izvješća i metodologije mjerenja UN-a i Europske unije. UN od 2001. godine na godišnjoj razini objavljuje Pregled (engl. Survey) efikasnosti elektroničkih javnih uprava u isporuci osnovnih usluga korisnicima u pet sektora: obrazovanje, zdravstvo, rad i zapošljavanje, financije i socijalna skrb te okoliš. UN je u izvješću (Pregled) iz 2003.[446] predložio načela za uspješno planiranje i izgradnju elektroničke javne uprave. U navedenom izvješću je navedeno petnaest načela koja su podijeljena u tri kategorije: nužni razlozi za stvaranje usluga elektroničke javne uprave, sposobnost javne uprave da koristi IKT za svoje aktivnosti te nužni razlozi koji bi trebali privući korisnike korištenju elektroničke javne uprave. UN razvoj elektroničke javne uprave prati preko EGDI indeksa. To je kompozitni indeks koji je temeljen na ponderiranom prosjeku tri indikatora koji su prethodno normalizirani. Trećinu predstavlja Infrastrukturni indeks telekomunikacija (TTI), trećinu Indeks ljudskog kapitala (HCI) te trećinu Indeks online usluga (OSI). Usporedba grafova za EDGI indeks za 2016. i 2014. godinu je pokazala da EDGI indeks globalno napreduje po zemljama, tj. povećava se broj zemalja s vrlo visokom i visokom razinom EDGI indeksa, a smanjuje se broj zemalja sa srednjom i niskom razinom. Svjetski lideri u elektroničkoj javnoj upravi s vrlo visokim EDGI indeksom za 2016. godinu su po redu: Ujedinjeno Kraljevstvo, Australija, Južna Koreja, Singapur, Finska, Švedska, Nizozemska, Novi Zeland, Danska, Francuska, Japan, SAD, Estonija, Kanada i Njemačka. Hrvatska je u Pregledu za 2016. godinu smještena na 37. mjestu te je u kategoriji zemalja s visokim indeksom.

[446] United Nations, Department of Economic and Social Affairs (2003.), World Public sector Report 2003, E-Government at the Crossroads, https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/World%20Public%20Sector%20Report%20series/World%20Public%20Sector%20Report.2003.pdf , str. 8 (03.01.2018.)

Europska unija ima svoje metodologije kojima prati napredak u elektroničkoj javnoj upravi za zemlje članice i zemlje kandidate za članstvo. Jedan od bitnih indikatora u uspješnosti e-Uprave je indeks DESI, Indeks digitalnog gospodarstva i društva. Kroz taj indeks se mjeri napredak u ostvarivanju ciljeva Digitalne agende u zemljama članicama i zemljama kandidatima za članstvo. Europska komisija je na svojim web stranicama objavila Digitalni semafor (engl. Digital Scoreboard) koji mjeri učinke Europe i država članica u širokom rasponu područja od povezivanja i digitalnih vještina do digitalizacije tvrtki i javnih usluga. Osim DESI indeksa, Digitalni semafor objavljuje podatke u sklopu Europskog izvješća o digitalnom napretku, tj. EDPR. Indeks DESI se izračunava pomoću pet komponenti od kojih svaka sudjeluje u indeksu s određenim postotkom. DESI 2017. (podaci za 2016.) navodi da Danska, Finska, Švedska i Nizozemska imaju najnaprednije digitalne ekonomije u EU, a slijede ih Luksemburg, Belgija, Velika Britanija i Irska. Rumunjska, Bugarska, Grčka i Italija imaju najniže rezultate za DESI 2017. Nadalje, za proučavanje napretka elektroničke javne uprave u Europskoj uniji su bitna godišnja izvješća o usporednim analizama e-Uprava, eGovernment Benchmark Report (Studija). Studija upotrebljava metodu Mystery Shopping, pri čemu kvalitetu i količinu elektroničkih javnih usluga mjere procjenitelji koji djeluju kao korisnik. Jedna studija je Pozadinska studija (engl. Background report) koja ima za cilj pružiti učinkovitu studiju o elektroničkoj javnoj upravi. U drugoj, kraćoj Studiji o uvidu (engl. Insight report) pružaju se ključni nalazi i preporuke. Studija 2016. je objavljena u zanimljivom trenutku: po zaključenju Akcijskog plana e-Uprave 2011.-2015. i početku provedbe Akcijskog planu za eGovernment 2016.-2020. Vrjednovanje (engl. Benchmarking) je važan aspekt Otvorene metode koordinacije, OMC koju članice Europska unije koriste u razmjeni dobrih praksi. Predmet vrjednovanja je skup od sedam životnih događaja. Sedam definiranih životnih događaja su: pokretanje poslovanja i ranih poslova trgovanja, redovno poslovanje, gubitak i pronalaženje posla, preseljenje, pokretanje postupka malih potraživanja, posjedovanje i vožnja automobilom te studiranje. U Studiji 2016. su objavljeni rezultati istraživanja dostupnosti javnih usluga po zemljama za razdoblje 2014.-2015. za EU28+. Prosjek je da se 60 % svih usluga e-uprave nudi potpuno online (povećanje od 7% u odnosu na rezultate prošle godine). U Studiji 2016. postoji objašnjena i metoda za klastere zemalja po kontekstu i performansama elektroničke javne uprave. Prvi korak analize ima za cilj mjerenje zrelosti zemlje. Apsolutni pokazatelji koji se koriste za mjerenje zrelosti izvedbe elektroničke javne uprave su penetracija i digitalizacija. Penetracija predstavlja korištenje

elektroničkih javnih usluga, a mjeri se pomoću pokazatelja Eurostata. Digitalizacija mjeri učinkovitost i djelotvornost javne administracije u unutarnjim postupcima (koristi se metoda Mystery Shop). Postoji 5 klastera zemalja temeljenih na faktorima izvedbe elektroničke javne uprave: Početnici, S visokim potencijalom, Progresivni, Napredni i Zreli. Zrele zemlje su mahom na sjeveru Europe (Danska, Švedska, Finska, Norveška, Nizozemska, Estonija i Island).

Što se tiče pozicije Hrvatske ona je u Pregledu UN-a za 2016. godinu smještena na 37. mjestu (u kategoriji je zemalja s visokim indeksom). Kod EDGI indeksa za Hrvatsku za 2016. se može zaključiti da bi situacija bila puno bolja (EDGI bi imao veću vrijednost) kada bi se popravila telekomunikacijska infrastruktura u zemlji te mogućnost njezinog korištenja (TII je 0,5974). Što se tiče Digitalnog semafora Europske komisije i DESI indeksa, Hrvatska je u Studiji za 2016. (obrađeni rezultati za 2015. uz usporedbu s razdobljem od 2012. što je već spomenuto u ovom radu) stagnirala. (pad s 23. na 24. mjesto). Kao jedan od razloga stagnacije u Izvješću se navode održani izbori u 2015. i politička nestabilnost što je dovelo do dodatne stagnacije u razvoju elektroničke javne uprave. Studija 2016. Hrvatsku smješta u klaster početnika. Europska komisija u Studiji za 2016. po DESI indeksu zaključuje da je velik prostor za napredak Hrvatske i u sferi penetracije i u razini digitalizacije. Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska[447] donosi još novije podatke za Hrvatsku. Izvješće navodi da Hrvatska pripada skupini manje uspješnih zemalja u smislu digitalnog razvoja. Izvješće o digitalnom razvoju Hrvatske 2017. navodi da je u dimenziji povezivosti Hrvatska ostvarila određeni napredak u pogledu uspješnosti, ali je i dalje na dnu ljestvice Unije. Slabim rezultatima u području iskorištenosti širokopojasnih mreža pridonose ograničena potražnja za širokopojasnim mrežama velike brzine te financijska nepristupačnost. Bitno je napomenuti da je Hrvatska zemlja s najskupljom pretplatom za samostalni fiksni širokopojasni pristup u cijeloj Europskoj uniji. U srpnju 2016. je donesena „Strategija razvoja širokopojasnog pristupa u Republici Hrvatskoj za razdoblje 2016.-2020."[448] čiji su glavni ciljevi koji se moraju ispuniti do 2020. usmjereni na: univerzalnu pokrivenost mrežama sljedeće generacije s brzinama većima od 30 Mbps te zastupljenost brzina većih

[447] Europska komisija (2017., 3.), Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska, ec.europa.eu/newsroom/document.cfm?doc_id=44293 (15.01.2018.)
[448] Vlada Republike Hrvatske (2016.), Strategija razvoja širokopojasnog pristupa u Republici Hrvatskoj za razdoblje 2016. – 2020, http://www.mppi.hr/UserDocsImages/Strategija-sirokopojasni-pristup2016-2020-usvojeno%20na%20VRH.pdf (21.01.2018.)

od 100 Mbps u najmanje 50% kućanstava. Što se tiče dimenzije ljudskog kapitala, Hrvatska tu dobro napreduje. Broj korisnika interneta i digitalne vještine se neprestano poboljšavaju. Što se tiče sklonosti pojedinaca da se služe uslugama na internetu i u području integracije digitalnih tehnologija u poduzećima Hrvatska ima dobre rezultate.

Što se tiče dimenzije e-upravi, Hrvatska je u prošloj godini postigla određeni napredak, ali je i ovdje pala s 25. na 26. mjesta. Broj korisnika usluge e-uprave polako se povećava, ali nije postignut napredak u pogledu isporuke usluga. Navedeno se objašnjava time što zbog političke situacije u protekloj godini (izbori i politička nestabilnost) nije bilo mnogo aktivnosti u pogledu usluge e-uprave.

8. ASPEKTI ELEKTRONIČKI POTPISANIH DOKUMENATA

U ovom poglavlju će biti obrađeno više aspekata elektronički potpisanih dokumenata. Prvo će se obraditi interoperabilnost s naglaskom na rezultate EU razvojnih projekata na tom području. Pravna uređenost područja elektroničkih dokumenata u Republici Hrvatskoj će se temeljiti na zakonskoj uređenosti elektroničke isprave. Poslije Hrvatske će se dati i pregled stanja pravne uređenosti u korištenju elektroničkih dokumenata po odabranim zemljama u svijetu. Potpoglavlje Rokovi čuvanja dokumenata u Republici Hrvatskoj će dati kratak prikaz rokova čuvanja za samo manji dio propisane dokumentacije. Na kraju poglavlja će biti dan prikaz normi za dugoročno očuvanje elektroničkih dokumenata.

8.1 INTEROPERABILNOST ELEKTRONIČKIH DOKUMENATA

Elektronički dokumenti su jako bitan element komunikacije elektroničkim putem. Različite su svrhe za koje se elektronički dokumenti mogu koristiti: razmjena, pohrana, obrađivanje različitih vrsta informacija i podataka. Prilikom različitih aktivnosti nad dokumentima, potrebno ih je potpisati radi osiguravanja njihove autentičnosti i integriteta. Pravni okvir potpisivanja elektroničkih dokumenata u Europskoj uniji je pokriven Uredbom eIDAS[449]. Kao prvi stup Digitalne agende Europske unije je navedeno Jedinstveno digitalno tržište. Jedinstveno digitalno tržište sadrži 21 mjeru kojima se nastoji ostvariti više ciljeva: potaknuti promet s internetskim sadržajima, uspostaviti jedinstveni okvir za elektronička plaćanje te osigurati zaštitu potrošača u digitalnom okruženju. Jedna od ključnih aktivnosti za razvoj jedinstvenog digitalnog tržišta je i osiguravanje prekograničnih elektroničkih javnih usluga. Uz to je vezana i prekogranična interoperabilnost elektroničkih dokumenata (što uključuje i elektronički potpisane dokumente). Europski okvir za interoperabilnost, EIF[450] (engl. European Interoperability Framework) daje specifične smjernice o uspostavljanju interoperabilnih elektroničkih javnih usluga. EIF nudi javnim upravama Europske unije 47 konkretnih preporuka za uspostavljanje i poboljšavanje aktivnosti.

[449] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (21.01.2018.)

[450] Europska komisija (2017.),European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF (29.01.2018.)

Preporuke EIF-a se fokusiraju na sljedeća područja: otvorenost i upravljanje informacijama, interoperabilnost upravljanja, prenosivost podataka te integrirano pružanje usluga.

Konceptualni EIF model je temeljen na 4 sloja interoperabilnosti:
1. Pravna interoperabilnost – odnosi se na usklađenost pravnih sustava zemalja članica,
2. Organizacijska interoperabilnost – odnosi se na interoperabilnost između tijela javne uprave koja imaju različite procese i različite interne ustroje,
3. Semantička interoperabilnost – je interoperabilnost koja pokriva značenja i tumačenja informacija izmijenjenih između više aplikacija te je preduvjet za višejezičnost,
4. Tehnička interoperabilnost - ova interoperabilnost pokriva tehničke standarde koji služe za povezivanje računalnih sustava i različitih usluga te će biti u fokusu ovog poglavlja vezanog uz elektroničke dokumente.

Tehničku interoperabilnost je potrebno osigurati (kad god je to moguće) uporabom formalnih tehničkih specifikacija, a EIF nudi konkretne preporuke (engl. Directives). U ovom poglavlju će biti dane najbitnije EIF preporuke vezane za elektroničke dokumente.

Preporuka 33[451] govori o tome da je potrebno koristiti otvorene specifikacije, tamo gdje su dostupne, kako bi se osigurala tehnička interoperabilnost pri uspostavi europskih javnih usluga.

Nadalje, Preporuka 41[452] navodi nužnost otvorenih podataka: „Potrebno je uspostaviti postupke i procese za integraciju otvaranja podataka za zajedničke poslovne procese, radne rutine i razvoj novih informacijskih sustava“. Vezano uz ovu preporuku spominje se i Direktiva o ponovnoj upotrebi informacija javnog sektora[453] koja pruža zajednički pravni okvir za ponovno korištenje podataka javnog sektora. Tu je naglasak na objavljivanju podataka koji se mogu strojno čitati kako bi se mogla potaknuti: transparentnost, poštena

[451] Europska komisija (2017.),European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF, str. 27 (29.01.2018.)
[452] Europska komisija (2017.), European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF, str. 33 (29.01.2018.)
[453] Europski parlament i Vijeće (2013.), Direktiva 2013/37/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o izmjeni Direktive 2003/98/EZ o ponovnoj uporabi informacija javnog sektora, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32013L0037&from=FR (29.01.2018.)

konkurencija, inovacije i gospodarstvo temeljeno na podacima. Dakle, podaci moraju biti interoperabilni kako bi se mogli pronaći, otkriti i obraditi. Iz tog razloga Preporuka 42[454] potiče objavu otvorenih podataka u strojno čitljivim, nevlasničkim formatima. Preporuka 43 upućuje[455] na jasno isticanje prava na pristup i ponovno korištenje otvorenih podataka, a pravni režimi za olakšavanje pristupa i ponovne uporabe (npr. licence) trebaju biti standardizirani što je više moguće.

Bitan projekt u osiguravanju Europskog interoperabilnog okvira je SPOCS[456] (engl. Simple Procedures Online for Cross-border Services). Osnovni cilj SPOCS projekta je bio uvesti jednostavne prekogranične usluge što je već implementirano u razdoblju 2009.-2012. Kroz SPOCS projekt su definirani i interoperabilnih gradivni blokovi (engl. Interoperability building blocks).

SPOCS ima više interoperabilnih gradivnih blokova[457]:

- Gradivni blok **Sindikacija i eServisi** (engl. Syndication & eServices) pruža semantičku interoperabilnost što omogućuje povezivanje nacionalnih i stranih dokumenata te procedura i usluga u svrhu pružanja integrirane usluge stranim pružateljima usluga,
- Gradivni blok **eDokumenti i elektronički potpisi** (engl. eDocuments and electronic signatures) omogućuju digitalnu omotnicu koja može sadržavati skupove različitih dokumenata u različitim formatima i uključuje definirane elektroničke potpise,
- Gradivni blok **eIsporuka** (engl. eDelivery) osigurava sigurnu prekograničnu isporuku s dokazima isporuke putem nacionalnih sustava eIsporuka,
- Gradivni blok **eSef** (engl. eSafe) pruža mogućnost korištenja postojećih nacionalnih eSefova za primanje, slanje i spremanje elektroničkih dokumenata. Ključno pitanje za ovaj gradivni blok je kako sigurno pohraniti i dohvatiti elektroničke dokumente. Navedeno se osigurava s PUSH i PULL interakcijom s točkama jedinstvenog kontakta, PSCs (engl. Points of Single Contact).

[454] Europska komisija (2017.), European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF, str. 34 (29.01.2018.)
[455] Isto, str. 34
[456] SPOCS, Simple Procedures Online for Cross- Border Services, http://www.eu-spocs.eu/ (29.01.2018.)
[457] Stranacher, K. (2012.), Final Report Work Package 2: eDocuments, http://www.eu-spocs-starterkit.eu/documents#d31 , str. 13. (29.01.2018.)

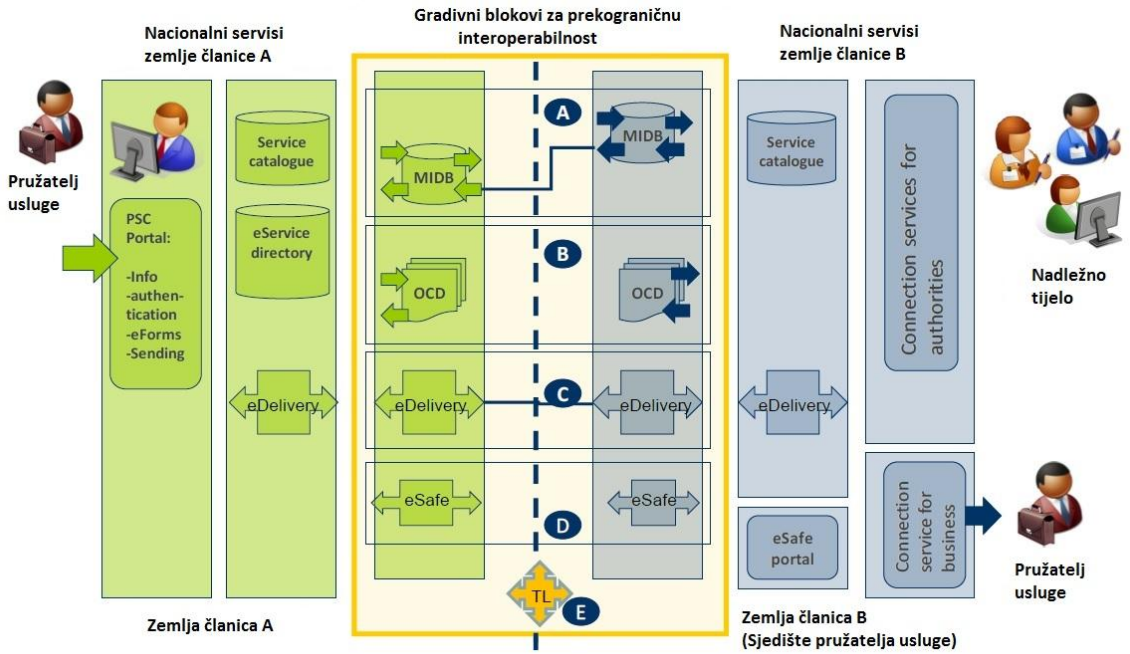
- Gradivni blok **SPOCS Liste od povjerenja** (engl. SPOCS Trusted List) osigurava siguran način za uspostavljanje povjerenja između različitih partnera i korištenih elektroničkih usluga.

Za ovaj rad je bitan gradivni blok eDokumenti i elektronički potpisi. Ovaj gradivni blok se bavi pitanjima kako predstavljati elektroničke dokumente te ih potpisivati i razmjenjivati, a sve u kontekstu prekogranične suradnje u Europskoj uniji. Direktiva 2006/123/EZ Europskog parlamenta i Vijeća od 12. prosinca 2006. o uslugama na unutarnjem tržištu[458] u članku 8. definira sljedeće „Države članice dužne su osigurati da se svi postupci i formalnosti vezani uz pristup usluzi za obavljanje djelatnosti i njihovo ostvarivanje mogu lako, na daljinu i elektroničkim putem, obaviti putem mjerodavne točke jedinstvenog kontakta s nadležnim tijelima“. Središnje točke ovih elektroničkih postupaka su elektronički dokumenti koji se razmjenjuju između uključenih strana. Uredba eIDAS navodi i sljedeće u kontekstu eDokumenata[459]: „Elektroničkom dokumentu ne smije se odbiti pravni učinak i korištenje kao dokaz u pravnim postupcima isključivo zbog toga što je u elektroničkom obliku“.

SPOCS projekt je definirao i SPOCS arhitekturalni okvir (engl. SPOCS Architectural Framework) u koji su uključeni gradivni blokovi koji su već prethodno opisani. Slika 47 prikazuje SPOCS arhitekturalni okvir.

[458] Europski parlament i Vijeće (2006.), Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123 (30.01.2018.)

[459] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)



PCS Portal – Portal jedinstvene točke kontakta
Service catalogue – Katalog servisa
eService directory – imenik elektroničkih sevisa
MIDB – Baza podataka za metapodatke
(engl. Meta-Information Database)

Gradivni blokovi:
A - Sindikacija i eServisi
B - eDokumenti i elektronički potpisi
C - eIsporuka
D - eSef
E - SPOCS Liste od povjerenja

Slika 47. SPOCS arhitekturalni okvir, preuzeto iz Stranacher, K. (2012.)[460]

Navedeni okvir se temelji na postojećim (nacionalnim) rješenjima, a gradivni SPOCS blokovi ne zahtijevaju da države članice mijenjaju svoje nacionalne infrastrukture. SPOCS specifikacija definira višeslojni format kontejnera elektroničkih dokumenata, tzv. Raznovrsni spremnik za eDokumente, OCD (engl. Omnifarious Container for Documents). OCD definira logičku strukturu koja se sastoji od sljedećih slojeva:

- Sloj nosivosti (engl. Payload layer): Ovaj sloj može sadržavati bilo kakve elektroničke podatke, tj. elektronički dokument kojeg izdaju države članice,
- Sloj metapodataka (engl. Metadata layer): sloj metapodataka sadrži metapodatke o sadržanim dokumentima i metapodatke o cijelom spremniku. Ovaj sloj omogućuje semantičku interoperabilnost,

[460] Stranacher, K. (2012.), Final Report Work Package 2: eDocuments, http://www.eu-spocs-starterkit.eu/documents#d31 , str. 13. (29.01.2018.)

- Sloj provjere autentičnosti (engl. Authentication layer): ovaj sloj dodaje mehanizam autentifikacije u OCD spremnik. Na ovaj način se može potpisati cijeli spremnik i svi povezani elementi.

Ova logička struktura može se implementirati kroz različite fizičke implementacije. Trenutačno su specificirani OCD spremnici temeljeni na ZIP i PDF ekstenziji.

ZIP spremnik je prikladniji za korištenje u pozadinskim aplikacijama i obradama (engl. back office). U sloju provjere autentičnosti se koristi XAdES format naprednog elektroničkog potpisa.

PDF spremnik je prikladniji za rad s građanima jer su upoznati s korištenjem navedenog tipa podataka. OCD temeljen na PDF formatu koristi mehanizam PDF-a s privicima[461]. Glavna PDF datoteka služi za vizualni prikaz OCD metapodataka. Sve ostale datoteke se dodaju kao privici u glavnu PDF datoteku. PAdES potpisi[462] se koriste u sloju provjere autentičnosti.

Gradivni blok eDokumenti i elektronički potpisi ima sljedeće funkcije:

- Kreiranje ZIP i PDF OCD spremnika,
- Verifikacija ZIP i PDF OCD spremnika. Postupak provjere obuhvaća osnovne korake provjere valjanosti (validacija formata, provjera valjanosti pojedinog sloja, provjera valjanosti potpisa),
- Raspakiranje ZIP i PDF OCD spremnika.

Projekt SPOCS je tijekom svog trajanja definirao i inventar standardnih dokumenta i relacija za otvorene specifikacije[463].

[461] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (31.01.2018.)
[462] ETSI (2009., 2.), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles; TS 102 778-3, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.01.02_60/ts_10277803v010102p.pdf (30.01.2018.)
[463] Roessler, T. et al. (2010.), D2.1 Inventory of standard documents and relations to open specifications, projekt SPOCS, http://www.eu-spocs-starterkit.eu/images/files/D2.1_List_of_standard_documents_and_relations_to_open_specifications.pdf (30.01.2018.)

Opisani formati i standardi podijeljeni su u sljedeće kategorije:

- Strukturirani formati (engl. Structured formats) - ti su formati strojno čitljivi i time primjenjivi za automatiziranu obradu (npr. XML),
- Nestrukturirani formati (engl. Unstructured formats) – za razliku od strukturiranih formata, nestrukturirani formati se vrlo teško strojno obrađuju. Obično se koriste za vizualni prikaz (npr. TIFF),
- Formati spremnika (engl. Container formats) – ovi formati se koriste za nošenje različitih vrsta podataka i općenito su samostalni (engl. self-contained). Ovaj format je bitan zato što ne ograničava podržavanje samo određenih formata i tehnologija za elektroničke dokumente. Primjer je MIME.

SPOCS daje i popis tehnologija/formata povezanih s eDokumentima koji su relevantni za ovaj projekt[464]. Prilikom izrade sljedećeg popisa relevantnih standarda i tehnologija za eDokumente, SPOCS projekt je osim standarda i tehnologija međunarodnih institucija i standardizacijskih tijela (ECMA - engl. European Computer Manufacturers Association, ETSI - engl. European Telecommunications Standards Institute, IETF - engl. Internet Engineering Task Force, ISO - engl. International Organization for Standardization, OASIS - engl. Organization for the Advancement of Structured Information Standards i W3C - engl. World Wide Web Consortium) uzimao u obzir i standarde zemalja članica:

- Osnovna tehnologija (engl. Basic Technology): XML, XSLT, XSD, PDF – ISO 32000, PDF-A -ISO 19005-1, TIFF,
- Tehnologija za elektroničke obrasce (engl. Technology providing forms): XFORMS, XPATH,
- Spremnik (engl. Container): XMLPersondata, XML-EDIAKT II, ODF, OOXML, XPS, MIME,
- Autentifikacijska tehnologija (engl. Authentication Technology): CMS potpisi, CAdES - TS 101 733, XMLDSIG, XAdES - TS 101 903, PAdES – TS 102 778, PDF-AS, Vidljivi potpisi,
- Ostalo: VCD (okvir, engl. Framework), MDOC (Litvanski format dokumenta za strukturirane podatke koje su namijenjene za strojno čitanje), ADOC (Litvanski

[464] Roessler, T. et al. (2010.), D2.1 Inventory of standard documents and relations to open specifications, projekt SPOCS, http://www.eu-spocs-starterkit.eu/images/files/D2.1_List_of_standard_documents_and_relations_to_open_specifications.pdf (30.01.2018.)

format dokumenta za nestrukturirane podatke koji su namijenjeni ljudima za čitanje).

SPOCS projekt nije jedini koji obrađuje tematiku eDokumenata. Formatima eDokumenata i eDokumentima se bave i neki drugi veliki projekti, npr. PEPPOL[465] (Pan-European Public Procurement OnLine) i e-CODEX[466] (engl. justice Communication via Online Data Exchange).

Projekt PEPPOL ima za cilj uspostaviti okvir interoperabilnosti za prekograničnu u elektroničkih dokumenata u području javne nabave, a eCODEX nastoji osigurati pristup građanima i poslovnim subjektima prema pravosuđima u drugim državama unutar EU. Budući da su zahtjevi projekata PEPPOL i SPOCS koji se odnose na prekograničnu uporabu eDokumenata vrlo slični, navedeni projekti su uspostavili blisku suradnju. PEPPOL je uveo takozvani Virtualni dosije tvrtke, VCD[467] (engl. Virtual Company Dossier). VCD eDokument je interoperabilno rješenje koje podržava razmjenu standardiziranih podataka tvrtke unutar paneuropske faze javne nabave.

8.2 PRAVNA UREĐENOST ELEKTRONIČKIH DOKUMENATA

8.2.1 Hrvatska

U ovom poglavlju je obrađena zakonska osnova za korištenje elektroničke isprave u Republici Hrvatskoj. Hrvatski zakon o elektroničkoj ispravi[468] (ZEI) je donesen 2005. godine. Lisičar o donošenju tog zakonu navodi sljedeće[469]: „Donošenjem Zakona o elektroničkoj ispravi 2005. godine upotpunjen je paket zakona koji uređuju pitanje elektroničkog poslovanja u Republici Hrvatskoj. Zakon o elektroničkom potpisu, koji je donesen još 2002. godine, nije mogao u potpunosti ostvariti svoju funkciju bez ZEI-a jer taj Zakon ne uređuje pitanje elektroničke isprave.“.

[465] PEPPOL, Pan-European Public Procurement Online, https://peppol.eu/ (31.01.2018.)
[466] eCODEX, justice Communication via Online Data Exchange, https://www.e-codex.eu/ (31.01.2018.)
[467] Virtualni dosije tvrtke (VCD), https://joinup.ec.europa.eu/solution/vcd-virtual-company-dossier (31.01.2018.)
[468] Hrvatski sabor (2005.), Zakon o elektroničkoj ispravi, NN 150/2005, http://www.nn.hr/clanci/sluzbeno/2005/2898.htm (01.02.2018.)
[469] Lisičar, H. (2010.), Mogućnosti uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku, Zbornik PFZ, 60, (3) 1391-1422 (2010), str.1395, https://hrcak.srce.hr/file/94423 (31.01.2018.)

Katulić Zakon o elektroničkoj ispravi dovodi u kontekst elektroničke trgovine[470] „Osiguravajući oznaku identiteta osobe i sadržaja elektroničkog dokumenta, elektronički potpis i elektronički certifikat nužan su preduvjet, pravno i tehnički, definicije i bitka pojma elektroničke isprave. Neka zakonodavstva, pa tako i hrvatsko, koriste se pojmom elektroničke isprave kako bi pripremila pravni okvir za interpretaciju sadržaja dokumenta u elektroničkom obliku i njegove pravne snage, za razliku od drugih, a osobito sustava common lawa koji u pravilu ne nalaze potrebnim stvoriti novi pravni institut samo da bi postigli izjednačavanje valjanosti dokumenata na papiru i onih u elektroničkom obliku… Uz Zakon o elektroničkom potpisu i Zakon o elektroničkoj trgovini, Zakonom o elektroničkoj ispravi definira se posebna vrsta dokumenta, elektronička isprava koja u praksi treba biti izjednačena s ispravama izdanima na papiru (pod određenim zakonskim uvjetima), čime je po mišljenju zakonodavca tada trebao biti zaokružen potreban pravni okvir kako bi elektronička trgovina bila adekvatno regulirana i zaštićena u usporedbi s tradicionalnim oblicima poslovanja.“

Lisičar, nadalje dovodi u vezu ZEI i Zakon o elektroničkom potpisu (ZEP)[471]: „Zakon o elektroničkom potpisu, koji je donesen još 2002. godine, nije mogao u potpunosti ostvariti svoju funkciju bez ZEI-a jer taj Zakon ne uređuje pitanje elektroničke isprave. Naime, ZEP-om se uređuje pravo pravnih i fizičkih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama.“. Lisičar je elektroničku ispravu promatrao u kontekstu uporabe u parničnom postupku. Danas u Republici Hrvatskoj imamo situaciji da je ZEP opozvan Uredbom eIDAS[472] (koja je i naslovljena i na stavljanje izvan snage Direktive 1999/93/EZ koja je bila temelj ZEP-a). S druge strane, ZEI je ostao na snazi, tj. mjerodavno tijelo za njega (Ministarstvo gospodarstvo[473]) nije propisalo nikakve zakonske akte nastavno na Uredbu eIDAS ili bar donijelo smjernice. Smatram da nakon svega do sada napisanog o Zakonu o elektroničkoj ispravi postoji prostor za donošenje zasebnih zakonskih akata ili barem smjernica za ZEI u

[470] Katulić, T. (2011.), Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u hrvatskom i poredbenom pravu, Zbornik PFZ, 61, (4) 1339-1378 (2011), str. 1345, http://hrcak.srce.hr/ 70481 (31.01.2018.)
[471] Hrvatski sabor (2002.), Zakon o elektroničkom potpisu, NN 10/02, http://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html , Članak 2. (21.03.2018.)
[472] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/84, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)
[473] Ministarstvo gospodarstva, https://www.mingo.hr/

kontekstu Uredbe eIDAS jer je ZEI usko vezan za elektronički potpis. Međutim, i uz navedene nedorečenosti, hrvatski ZEI je prilikom donošenja doprinio široj implementaciji i korištenju elektroničkih dokumenata u Republici Hrvatskoj te je iz navedenog razloga ZEI detaljnije obrađen u ovom poglavlju.

ZEI u članku 5.[474] definira elektroničku isprava kao ispravu koja ima pravnu valjanost kao i isprava na papiru ako: „je izrađena, otpremljena, primljena, čuvana i pohranjena primjenom dostupne informacijske tehnologije (računalni i srodni uređaji i programi),
– u potpunosti ispunjava zahtjeve sadržane u članku 6. ovoga Zakona,
– sadrži osnovnu građu utvrđenu u članku 7. ovoga Zakona,
– se može prikazati u obliku koji je sukladan obrascu utvrđenom u članku 8. ovoga Zakona.“

U kontekstu elektroničke isprave bitan je pojam i dokumentacijskog ciklusa. ZEI dokumentacijski ciklus propisuje u članku 6[475]: „Elektronička isprava mora u svim radnjama uključenim u dokumentacijski ciklus osigurati:
– jednoznačno obilježje kojim se nedvojbeno utvrđuje pojedinačna elektronička isprava,
– jednoznačno obilježje kojim se nedvojbeno utvrđuje pojedinačni stvaratelj elektroničke isprave,
– informacijsku cjelovitost i nepovredivost elektroničke isprave,
– pristup sadržaju elektroničke isprave kroz cijelo vrijeme dokumentacijskog ciklusa,
– oblik zapisa koji čitatelju omogućuje jednostavno čitanje sadržaja.“

Posebnost elektroničke isprave su i obrasci prikaza. Elektronička se isprava u procesima prikazivanja sadržaja, ali i tijekom rukovanja sadržajima koji su ugrađeni u elektroničku ispravu sastoji od dva neodvojiva dijela 7[476]: „Građa elektroničke isprave sastoji se obvezno od dva neodvojiva dijela:
– općeg dijela kojeg čini predmetni sadržaj (informacije u elektroničkom obliku) isprave. Uključuje i naslov primatelja ako je elektronička isprava namijenjena otpremi imenovanom primatelju,

[474] Hrvatski sabor (2005.), Zakon o elektroničkoj ispravi, NN 150/2005, http://www.nn.hr/clanci/sluzbeno/2005/2898.htm, članak 5 (01.02.2018.)
[475] Isto, članak 6
[476] Isto, članak 7

– posebnog djela kojeg čine jedan ili više ugrađenih elektroničkih potpisa i podaci o vremenu nastajanja (završetka izrade) elektroničke isprave, kao i druga dokumentacijska svojstva.“. Članak 8. Zakona o elektroničkoj ispravi govori o unutarnjem i vanjskom obrascu. Unutarnji obrazac prikaza sastoji se od tehničkog i programskog zapisivanja sadržaja u elektroničkom obliku i to na mediju koji je namijenjen zadržavanju ili prosljeđivanju elektroničke isprave. S druge strane, vanjski obrazac sastoji se od vizualnog prikaza sadržaja elektroničke isprave razumljivog korisniku (može se prikazati na zaslonu računalnih ili drugih elektroničkih uređaja, ali i na papiru ili drugom materijalnom predmetu). Uzevši u obzir unutrašnji obrazac, elektroničke isprave (za razliku od klasičnih skenova u digitalnom formatu) omogućavaju da se različite informacije u ispravi mogu strukturirati. Informacije se unutar unutrašnjeg obrasca mogu lakše strukturirati, a time i lakše spremati i kasnije pretraživati.

Već spomenuti OCD, tj. Raznovrsni spremnik za eDokumente iz SPOCS projekta može biti temeljen na PDF formatu koji koristi mehanizam PDF-a s privicima te naprednog elektroničkog potpisa (PAdES) za osiguravanje autentičnosti[477]. Ovaj OCD koncept može podržati zahtjeve vanjskog i unutrašnjeg obrasca po još važećem Zakonu o elektroničkoj ispravi. Kod OCD-a temeljenog na PDF-u glavna datoteka služi za vizualni prikaz OCD metapodataka (time je pokriven vanjski obrazac). Sve ostale datoteke se kao privici dodaju u glavnu OCD PDF datoteku (time se pokriva unutrašnji obrazac).

Za ovaj rad je izuzetno bitan članak 20.[478] Zakona o elektroničkoj ispravi koji propisuje čuvanje elektroničkih isprava, a i eksplicitno se propisuju zadaci elektroničkog arhiva za elektroničke isprave:

„(1) Fizička i pravna osoba kojoj je zakonom ili drugim propisima utvrđena obveza čuvanja isprava u izvornom obliku, dužna je čuvati elektroničke isprave u skladu s odredbama stavka 2. i 3. ovoga članka.

(2) Elektroničke isprave čuvaju se izvorno u informacijskom sustavu ili na medijima koji omogućuju trajnost elektroničkog zapisa za utvrđeno vrijeme čuvanja, i čine elektroničku arhivu.

(3) Elektronička arhiva mora osigurati:

[477] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (03.02.2018.)

[478] Hrvatski sabor (2005.), Zakon o elektroničkoj ispravi, NN 150/2005, http://www.nn.hr/clanci/sluzbeno/2005/2898.htm, članak 20 (03.02.2018.)

– da se elektroničke isprave čuvaju u obliku u kojem su izrađene, otpremljene, primljene i pohranjene i koji materijalno ne mijenja informaciju odnosno sadržaj isprava,
– da su elektroničke isprave u čitljivom obliku za cijelo vrijeme čuvanja dostupne osobama koje imaju pravo pristupa tim ispravama,
– da se čuvaju podaci o elektroničkim potpisima kojima su elektroničke isprave potpisane kao i podaci za ovjeru tih elektroničkih potpisa,
– da su elektroničke isprave pohranjene u takvom obliku i pomoću takve tehnologije i postupaka koji uz ugrađene elektroničke potpise pružaju razumno jamstvo za njihovu vjerodostojnost i cjelovitost za cijelo vrijeme čuvanja,
– da je za svaku elektroničku ispravu moguće vjerodostojno utvrditi podrijetlo, stvaratelja, vrijeme, način i oblik u kojem je zaprimljena u sustav na čuvanje,
– da su elektroničke isprave pohranjene u takvom obliku i pomoću takve tehnologije i postupaka koji pružaju razumno jamstvo da ne mogu biti mijenjane i da se ne mogu neovlašteno brisati,
– da postupci održavanja i zamjene medija za pohranu elektroničkih isprava ne narušavaju cjelovitost i nepovredivost elektroničkih isprava,
– da se elektroničke isprave mogu sigurno, pouzdano i vjerodostojno zadržati u razdoblju koje je utvrđeno zakonom ili drugim propisima kojima se uređuju obveze čuvanja odgovarajućih isprava na papiru.“

U Republici Hrvatskoj je članak 20. danas referentni zakonski propis za arhive elektroničkih isprava u javnoj upravi. Postoji, doduše i Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva[479] koji u članku 10. navodi sljedeće: „Gradivo u elektroničkom obliku pohranjuje se tako da se podaci izdvoje iz izvornog sustava, odnosno sustava koji omogućuje brisanje, mijenjanje i dodavanje podataka, i pohrane u sustavu koji onemogućuje brisanje, mijenjanje i dodavanje podataka, ili tako da se u sustavu u kojem se nalaze onemogući brisanje, mijenjanje i dodavanje podataka. Elektronički podaci se pohranjuju u najmanje dvije kopije, od kojih jedna treba biti u sustavu koji omogućuje pristup, pretraživanje i prikazivanje podataka koji se predaju na pohranu, a jedna izvan tog sustava.

[479] Ministarstvo kulture (2004.), Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva, https://narodne-novine.nn.hr/clanci/sluzbeni/2004_05_63_1383.html (03.02.2018.)

Prije pohrane gradiva u elektroničkom obliku u pisanom se obliku opisuje format i struktura zapisa, način na koji će se osigurati njihovo čuvanje i zaštita od neovlaštenog pristupa ili mijenjanja podataka, način na koji će se provoditi izlučivanje te oblik i način predaje nadležnom arhivu.

Pri pohrani gradiva u elektroničkom obliku obvezno se provjerava čitljivost i cjelovitost svih kopija predanih elektroničkih zapisa.“. Međutim, članak 10. navedenog pravilnika se teško može prepoznati kao relevantan za elektronički arhiv elektroničkih isprava javne uprave jer je previše načelan.

O Zakonu o elektroničkoj ispravi piše i Grbac[480] te navodi da je prema ZEI-u pravna snaga i vjerodostojnost elektroničke isprave izjednačena s ispravom u pisanom obliku, ali da zakon također predviđa slučajeve u kojima ovakva vrsta isprave neće biti podoban dokaz u pravnom prometu. Upućuje na članak 11. Stavak 2.[481] Zakona o elektroničkoj ispravi u kojem se navodi da „Za sve radnje u kojima se zakonom ili drugim propisima izričito traži javnobilježnička ovjera isprava na papiru, ne može se dostavljati elektronička isprava ili njegova preslika na papiru.“
Grbac, nadalje, daje[482] svoju ocjenu razvoja hrvatskog javnog bilježništva u području digitalizacije pravnog prometa. Ocjenjuje da Republika Hrvatska već dulji niz godina pokazuje pozitivni primjer smjelosti u slijedu elektroničkih tokova poslovanja. Grbac ističe[483] Hrvatsku javnobilježničku komoru koja vodi elektroničke registre kao što su Hrvatski upisnik oporuka (HUO) i Registar zadužnica i bjanko zadužnica (HRZ), a u pripremi je i uspostava Registra anticipiranih naredbi i punomoći te se sve knjige, imenici i upisnici javnih bilježnika vode u elektroničkom obliku. Osim toga, u poslovanju s trgovačkim društvima u Republici Hrvatskoj Grbac navodi[484] da se mogu elektronički osnivati društva s ograničenom odgovornošću (d.o.o. i j.d.o.o.) posredstvom servisa e-tvrtka i HITRO.HR[485] te naši javni bilježnici već dulji niz godina uspješno izdaju izvatke iz

[480] Grbac, M. (2016.), Tranzicija javnobilježničke službe - od tradicije do elektronifikacije, Javni bilježnik, broj 43, str.110. (107.-112.), http://www.hjk.hr/Portals/0/CasopisJB/Javni%20bilje%C5%BEnik%2043.pdf (01.02.2018.)
[481] Hrvatski sabor (2005.), Zakon o elektroničkoj ispravi, NN 150/2005, http://www.nn.hr/clanci/sluzbeno/2005/2898.htm, čl. 11 (01.02.2018.)
[482] Grbac, M. (2016.), Tranzicija javnobilježničke službe - od tradicije do elektronifikacije, Javni bilježnik, broj 43, str.110. (107.-112.), http://www.hjk.hr/Portals/0/CasopisJB/Javni%20bilje%C5%BEnik%2043.pdf (01.02.2018.)
[483] Isto, str. 111
[484] Isto, str. 111
[485] HITRO.HR, http://www.hitro.hr/Default.aspx?sec=28 (01.02.2018.)

sudskih registara. Za servis e-Tvrtku se na stranicama HITRO.HR-a navodi[486] da se dokumenti potrebni za upis osnivanja d.o.o. i j.d.o.o. u sudski registar automatski pohranjuju u digitalnu zbirku isprava Sudskoga registra.

Maganić spominje[487] više o važnosti izrade elektroničkih isprava putem servisa e-Tvrtka „Za razvoj elektroničkog pravnog prometa u Hrvatskoj posebno je važan projekt e-Tvrtka i HITRO.HR, u kojem središnju ulogu imaju javni bilježnici. Naime, sve je počelo 29. listopada 2007., kada je prvi put u povijesti hrvatskog pravnog sustava elektronički potpis javnog bilježnika na online prijavi za upis u sudski registar zamijenio potpis i pečat javnog bilježnika na papiru. Naime, Trgovačkom sudu u Varaždinu bile su upućene prve prijave za upis osnivanja društva s ograničenom odgovornošću putem interneta koje je predstavila informatička struktura FINA-e, odnosno sustav HITRO.HR. Bio je to pilot projekt koji je provelo Ministarstvo pravosuđa u suradnji s FINA-om i koji je obuhvatio sve javne bilježnike s područja nadležnosti tog suda (Međimurska i Varaždinska županija).“

Dakle, Maganić navodi e-Tvrtku i online prijavu za upis u sudski registar u kontekstu zamjene potpisa i pečata javnog bilježnika na papiru što je posljedično 2007. dovelo do slučaja konkretne zamjene papirnate isprave s elektroničkom ispravom u Republici Hrvatskoj.

8.2.2 Stanje u svijetu

U ovom poglavlju će se dati kratak pregled stanja pravne uređenosti korištenja elektroničkih dokumenata (elektroničkih isprava) po svijetu i vezano uz njih reguliranost elektroničkog potpisa. Reguliranje elektroničkog potpisa i elektroničke isprave istim zakonom je češći slučaj u svijetu. Međutim, postoje i slučajevi slični hrvatskom, tj. zasebnog zakona za područje elektroničke isprave. Lisičar[488] za hrvatski Zakon o elektroničkoj ispravi navodi da je „Ovakvo rješenje kojim se elektronički potpis i elektronička isprava uređuju u dvama odvojenim zakonima nije uobičajeno. Promatrajući zakonodavstava zemalja članica EU-a, uglavnom se nailazi na primjer jedinstvenog zakona

[486] e-Tvrtka, http://www.hitro.hr/Default.aspx?sec=72 (01.02.2018.)
[487] Maganić, A. (2013.), Javni bilježnik u elektroničkom pravnom prometu, Zbornik PFZ, 63, (2) 383-431 (2013), https://hrcak.srce.hr/file/161630 (01.02.2018.)
[488] Lisičar, H. (2010.), Mogućnosti uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku, Zbornik PFZ, 60, (3) 1391-1422 (2010), str.1395, https://hrcak.srce.hr/file/94423 (31.01.2018.)

koji uređuje pitanje tih dvaju instrumenata, a mislimo da to i jest ispravno rješenje upravo zbog njihove bliske povezanosti. Naišli smo samo na primjer Litve koja također uređuje elektroničku ispravu posebnim zakonom.“. Katulić nastavlja[489] na tom navodu sa sljedećim komparativno-pravnim zaključkom: „Komparativnopravno, pojam elektroničke isprave u smislu odredaba Zakona o elektroničkoj ispravi relativno je rijetko rješenje. Posvetiti poseban zakon regulaciji elektroničke isprave još je veći raritet. Neke od zemalja čija su zakonodavstva odlučila posebno regulirati elektroničku ispravu tako su primjerice Azerbejdžan, Filipini, Kanada i Litva.“

Adobe daje zanimljiv Globalni vodič svjetskih zakona o elektroničkom potpisu[490]. Navedenim vodičem su obrađeni zakoni za 47 zemalja u svijetu (uključujući sve najveća svjetska gospodarstva), a neki zakoni pokrivaju i područje elektroničkog dokumenta. U ovom radu će biti obrađene samo zemlje koje pokrivaju svojim zakonima i elektronički dokument (Kanada, Europska unija, SAD, Filipini, Urugvaj, Kostarika, Kuvajt).

Kanada

Kanadski Zakon o zaštiti osobnih podataka i elektroničkim dokumentima[491] (engl. Personal Information Protection and Electronic Documents Act) omogućava korištenje elektroničkog potpisa za gotovo sve vrste ugovora. Kod njega je važno dobiti prethodnu suglasnost svih strana za obavljanje poslova elektroničkim putem. Pretpostavlja se da su elektronički potpisi valjani dok se ne dokaže suprotno. Neki ugovori o nekretninama, oporuke, sporazumi o nekretninama i punomoći su isključeni iz zakona. Postoje neke varijacije među kanadskim provincijama, ali se poštuju ograničenja navedena kanadskim zakonom (primjer je Quebec[492]).

[489] Katulić, T. (2011.), Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u hrvatskom i poredbenom pravu, Zbornik PFZ, 61, (4) 1339-1378 (2011), str. 1373, http://hrcak.srce.hr/70481 (31.01.2018.)

[490] Adobe (2016.), Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability, https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf (02.02.2018.)

[491] Kanadski parlament (2000.), Personal Information Protection and Electronic Documents Act, https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html (02.02.2018.)

[492] Publications Quebec (2012.), Act to establish a legal framework for information technology, https://www.canlii.org/en/qc/laws/stat/rsq-c-c-1.1/latest/rsq-c-c-1.1.html?searchUrlHash=AAAAAQBBQW4gQWN0IHRvIGVzdGFibGlzaCBhIGxlZ2FsIGZyYW1ld29yayBmb3IgaW5mb3JtYXRpb24gdGVjaG5vbG9neSAAAAAAAAQ (02.02.2018.)

Europska Unija

Uredba eIDAS[493] koja je stupila na stanju od 1. lipnja 2016., uspostavlja nove zakonske strukture za elektroničku identifikaciju, potpise, pečate i dokumente diljem Europske Unije. Uredba eIDAS definira i napredni elektronički potpis[494] koji omogućava jedinstveni identifikator i autentifikaciju potpisnika te provjeru integriteta elektronički potpisanog dokumenta. Ova Uredba je važna iz razloga što po prvi put postoji konzistentan pravni okvir i jedinstveno tržište za priznavanje elektroničkih potpisa i identiteta u cijeloj Europskoj Uniji. Navedeno osigurava tvrtkama predvidljivo pravno okruženje u kojem će razviti i proširiti korištenje elektroničkih potpisa.

SAD

Savezna vlada SAD-a usvojila je 2000. godine Zakon o elektroničkim potpisima u globalnom i nacionalnom poslovanju, ESIGN[495] (engl. Electronic SIGNatures in global and national commerce act). Osim ESIGN zakona, svaka država ima svoj zaseban zakon o elektroničkom potpisu. Opća namjera ovog Zakona je napisana je u prvom odjeljku (101.a) i navodi: „da se ugovoru ili potpisu ne smije odbiti pravni učinak, valjanost ili ovršnost samo zato što je u elektroničkom obliku". Ova jednostavna izjava definira da su elektronički potpisi i elektronički zapisi jednako dobri kao i njihovi papirni ekvivalenti pa stoga podliježu istom pravnom proučavanju autentičnosti koje se primjenjuje na papirnate dokumente. ESIGN ne govori o elektroničkim dokumentima (engl. electronic documents) već o elektroničkim zapisima (engl. electronic records).

Filipini

Na Filipinima je 2000. godine donijet Zakon br. 8792: Zakon o priznavanju i korištenju elektroničkih poslovnih i nekomercijalnih transakcija i dokumenata[496] (engl. Republic Act

[493] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[494] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/100, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[495] U.S. Congress (2000.), ESIGN - Electronic Signatures in global and national commerce act, https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm (03.02.2018.)

[496] Filipinski Senat (2000.), Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents,

No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents). Ovaj zakon predviđa važenje elektroničkih potpisa dok se stranke mogu slobodno dogovoriti da će elektronički potpisi biti obvezujući.

Urugvaj

Urugvaj je 2009. godine donio Zakon za elektroničke dokumente i elektroničke potpise[497] (špa. Ley Documento electrónico y firma electrónica). Zakon je donekle neuobičajen jer dopušta strankama da povuku suglasnost nakon što ga daju. To znači da se stranke mogu dogovoriti o elektroničkom prijenosu poslovanja i potpisati dokument elektroničkom putem, ali to neće spriječiti niti jednu od stranaka u postupku da naknadno povuku svoj pristanak. S druge strane, postoje dokazi da se elektronički potpisi i elektronički potpisani dokumenti uobičajeno koriste u Urugvaju i podneseni su u sudskim spisima.

Kostarika

Zakon o elektroničkim potpisima, certifikatima i elektroničkim dokumentima[498] (engl. The Law of Digital Signatures, Certificates and Electronic Documents) daje pravno priznanje elektroničkim potpisima i dokumentima. Dakle, elektronički potpis se izjednačava s vlastoručnim potpisom, a elektronički dokument s fizičkim dokumentom. Elektronički potpis se registrira nakon što certifikator pošalje digitalni certifikat korisniku.

Kuvajt

Kuvajtski Zakon br.20. za elektroničke transakcije[499] donesen je 2014. godine, a obuhvaća elektroničke zapise, poruke, informacije, dokumente i potpise.

Nadalje, slijedi pregled zakonodavstava kod još dvije europske zemlje koje su zasebnim aktima regulirale područje elektroničkih dokumenata (Škotska i Srbija).

---

http://www.fda.gov.ph/attachments/article/29048/RA%208792%20E%20Commerce%20Law.pdf (02.02.2018.)

[497] Urugvajski Senat (2009.), Ley Nº 18.600 DOCUMENTO ELECTRÓNICO Y FIRMA ELECTRÓNICA, http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/D09A96E064A5815705257D1C0078B0B3/$FILE/Ley_N%C2%BA_18.600_Documento_Electr%C3%B3nico_y_Firma_Electr%C3%B3nica.pdf (02.02.2018.)

[498] Banco central de Costa Rica, The Law of Digital Signatures, Certificates and Electronic Documents, http://www.bccr.fi.cr/bccr_home_page/digital_signature/ (03.02.2018.)

[499] Kuvajtska centralna agencija za informacijsku tehnologiju (2014.), Law No. 20 of 2014. Concerning Electronic Transactions, https://www.csb.gov.kw/images/Magazine_E.pdf (03.02.2018.)

Škotska

Škotska je 2014. izdala zasebnu Pravnu regulaciju za elektroničke dokumente[500]. Ova Pravna regulacija se odnosi na Zakon o potpisu iz 1995 (engl. Requirements of Writing (Scotland) Act 1995). Regulacija propisuju uvjete za elektroničke dokumente i potpise za dokumente iz zemljišnjih knjiga.

Srbija

U Srbiji je 2017. godine donesen Zakon o elektroničkom dokumentu, elektroničkoj identifikaciji i uslugama od povjerenja u elektroničkom poslovanju (srp. Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju)[501]. Ovim zakonom je korisnicima omogućeno[502] da preko svog mobilnog telefona koriste kvalificirani elektronički potpis u transakcijama i elektroničkoj komunikaciji, a elektronički dokument je izjednačen s papirnatim dokumentom. Predviđeno je i formiranje elektroničkog spremnika (srp. elektronskog magacina) za čuvanje dokumentacije. Pravne osobe će imati elektronički pečat koji će istovremeno biti zamjena i za pečat i vlastoručni potpis. Ovim zakonom se omogućava rješenje za povezivanje različitih informacijskih sustava i institucija koje mogu razmjenjivati elektroničke dokumente ovjerene elektroničkim pečatom. Ovaj Zakon je na tragu Uredbe eIDAS koju Srbija kao zemlja kandidatkinja za članstvo u EU kroz pregovore preuzima kao pravnu stečevinu.

U nastavku slijedi pregled zakona po zemljama bivšeg Sovjetskog saveza i bivšeg Varšavskog bloka koje su pod utjecajem Direktive o elektroničkom potpisu 1999/93/EC[503] Europske Unije iz 1999. zakonski definirale korištenje elektroničkih dokumenata.

---

[500] Registri Škotske u ime škotske vlade (2014.), The electronic documents (Scotland) regulations, SSI 2014/83, http://www.legislation.gov.uk/ssi/2014/83/pdfs/ssipn_20140083_en.pdf (03.02.2018.)

[501] Narodna skupština Republike Srbije (2017.), Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, https://www.ekapija.com/dokumenti/ZAKON_o_elektronskom_dokumentu_elektronskoj_identifikaciji_i_uslugama_od_poverenja_u_elektronskom_poslovanju_231017.pdf (03.02.2018.)

[502] eKapija, Usvojen Zakon o elektronskom dokumentu - Elektronski pečat za pravna lica imaće punopravnu snagu, https://www.ekapija.com/news/1910885/usvojen-zakon-o-elektronskom-dokumentu-elektronski-pecat-za-pravna-lica-imace-punopravnu (17.10.2017.)

[503] Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)

Rusija

U Rusiji je 2011. godine stupio je na snagu savezni Zakon o elektroničkom potpisu (br. 63-FZ)[504]. Navedeni Zakon je dao smjernice o tome kako stvoriti i koristiti elektronički potpis te je definirao dužnosti stranaka u razmjeni elektroničkih dokumenata. Iste godine je donesen savezni Zakon o računovodstvu[505] (br. 402-FZ). Ovaj zakon opisuje koji se gospodarski događaji odražavaju u primarnim računovodstvenim dokumentima i koji se dokumenti mogu pripremiti u papirnatom obliku ili kao elektronički dokumenti potpisati elektroničkim potpisom. Taj Zakon je bio podloga da se pomoću EDI protokola mogu slati, primiti i prihvaćati elektronički dokumenti vezani uz obračun PDV-a. Federalna porezna služba Ruske Federacije izdala je 2012. godine Nalog br. MMV-7-6 /172 koji određuje novi oblik primarnih računovodstvenih dokumenata te se njime određuju formati elektroničkih dokumenata.

Ukrajina

Ukrajina 2003. godine donosi Zakon o elektroničkim dokumentima i elektroničkom upravljanju dokumentima[506] (engl. Law about electronic documents and electronic document management). Zakon se redovito dorađuje te je zadnji puta mijenjan u 2015. godini. Ovim se Zakonom utvrđuju osnovne organizacijske i pravne osnove upravljanja elektroničkim dokumentima i korištenja elektroničkih dokumenata.

Litva

U Litvi je Zakon o elektroničkom dokumentu[507] (engl. Electronic Documents Law) donesen 2004. godine. Ovaj Zakon definira što je elektronički dokument i što su derivati elektroničkog dokumenta.

---

[504] Docusign, eSignature Legality in Russia, https://www.docusign.com/how-it-works/legality/global/russia (15.05.2017.)
[505] Russia Briefing, Legal Environment of Electronic Document Interchange in Russia, https://www.russia-briefing.com/news/legal-environment-electronic-document-interchange-russia.html/ (24.06.2014.)
[506] Ukrajinski parlament (2003.), Law of Ukraine About electronic documents and electronic document management No. 851-IV, http://cis-legislation.com/document.fwx?rgn=11196 (03.02.2018.)
[507] Litvanski parlament, Saeima (2004.), Electronic Documents Law, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&cad=rja&uact=8&ved=0ahUKEwjl9sWM-PjYAhUSKuwKHcIZAts4ChAWCDMwAQ&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FCiti%2FElectronic_Documents_Law.doc&usg=AOvVaw0QRJjM2mPtfH3lGZSiH0Xl (03.02.2018.)

Armenija

Armenija 2004. godine donosi Zakon o elektroničkom dokumentu i elektroničkom potpisu[508] (engl. Law on electronic document and electronic signature). Ovim zakonom se uređuju okviri primjene elektroničkih dokumenata i elektroničkih potpisa, ali se eksplicitno navodi da se ne uređuju okviri uslijed korištenja digitaliziranog potpisa i takvih elektroničkih dokumenata (engl. electronic version of a person's manuscript signature and its copies).

Bugarska

U Bugarskoj je Zakon o elektroničkom dokumentu i elektroničkom potpisu[509] (engl. Law for the electronic document and electronic signature) donesen 2001. godine. Ovaj zakon definira elektronički dokument, elektronički potpis i uvjete njihovog korištenja. Osim toga propisuje i okvire osiguravanja certifikacijskih servisa.

Kazahstan

U Kazahstanu je 2003. godine donesen Zakon o elektroničkom dokumentu i elektroničkom digitalnom potpisu[510] (engl. Law on electronic documents and electronic digital signatures). Zakon se od tada više puta mijenjao te su zadnje izmjene iz 2015. godine.

Gruzija

Gruzija 2008. godine donosi Zakon o elektroničkom potpisu i elektroničkom dokumentu[511] (engl. Law on electronic signatures and electronic documents). U uvodnim odredbama se navodi da ovaj zakon uspostavlja pravni okvir za protok elektroničkih dokumenata kroz IT sustave te korištenje elektroničkih potpisa unutar takvih sustava.

[508] Armenski parlament (2004.), The law of the Republic of Armenia "on electronic document and electronic signature", http://www.parliament.am/law_docs/150105HO40eng.pdf (03.02.2018.)
[509] Bugarski parlament (2001.), Law for the electronic document and electronic signature, http://www.crc.bg/files/_en/ZED_ENG_15.01.2008.htm (03.02.2018.)
[510] Kazahstanski parlament (2003.). Law of the Republic of Kazakhstan No. 370-II of January 7, 2003, on Electronic Documents and Electronic Digital Signatures, http://www.wipo.int/wipolex/en/details.jsp?id=16138 (03.02.2018.)
[511] Gruzijski parlament (2008.), Law of Georgia on electronic signatures and electronic documents, https://matsne.gov.ge/ru/document/download/20866/4/en/pdf (03.02.2018.)

Iz navedenog prikaza zemljama bivšeg Sovjetskog saveza i bivšeg Varšavskog bloka vidljivo je da je velika većina njih zakonski pokrivala područje elektroničkog potpisa i elektroničkog dokumenta u istom zakonu.

8.3 ROKOVI ČUVANJA DOKUMENATA U REPUBLICI HRVATSKOJ

Svi dokumenti (fizički i elektronički), ako se koriste u službene svrhe, imaju propisane rokove čuvanja. U Republici Hrvatskoj su rokovi čuvanja pojedine dokumentacije propisani Pravilnikom o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva[512] (Pravilnik) kojeg je Ministarstvo kulture donijelo 2002. godine. Pravilnik u općim odredbama propisuje sljedeće:

„(1) Ovim Pravilnikom utvrđuju se kriteriji vrednovanja arhivskoga gradiva, kategorizacija stvaratelja, izradba popisa arhivskoga gradiva s rokovima čuvanja, postupak odabiranja i izlučivanja te način uništavanja izlučenoga gradiva.

(2) Odredbe ovoga Pravilnika odnose se na sve stvaratelje i imatelje javnoga arhivskoga gradiva u smislu članka 5. Zakona o arhivskom gradivu i arhivima (u daljnjem tekstu: Zakona), kao i na stvaratelje i imatelje privatnoga arhivskoga gradiva upisane u Upisnik vlasnika i imatelja privatnoga arhivskoga gradiva sukladno čl. 31. Zakona.“ Dakle, Pravilnik se referencira na Zakon o arhivskom gradivu u arhivima[513] (zadnja promjena na tom Zakonu se dogodila 2017. godine[514]). Za ovaj rad je bitan dio koji se tiče rokova čuvanja koji imaju utjecaj i na osmišljavanje i implementaciju elektroničkog arhiva u javnoj upravi.

Pravilnik u prilogu 1. daje Orijentacijski popis gradiva ograničenih rokova čuvanja[515] te za rokove čuvanja navodi: „Rokovi čuvanja računaju se od:

– godine nastanka, osnivanja, pohađanja ili polaganja ispita

– dana usvajanja financijskog rješenja (za računovodstvenu dokumentaciju)

[512] Ministarstvo kulture (2002.), Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva, Ministarstvo kulture, https://narodne-novine.nn.hr/clanci/sluzbeni/2002_07_90_1476.html (03.02.2018.)

[513] Hrvatski sabor (1997.), Zakon o arhivskom gradivu i arhivima, https://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_105_1617.html (03.02.2018.)

[514] Hrvatski sabor (2017., 2.), Zakon o izmjenama i dopunama zakona o arhivskom gradivu i arhivima, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2017_05_46_1070.html (03.02.2018.)

[515] Ministarstvo kulture (2002.), Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva, Ministarstvo kulture, https://narodne-novine.nn.hr/clanci/sluzbeni/2002_07_90_1476.html, Prilog 1, str. 7 (03.02.2018.)

– godine prestanka ugovornih i drugih obveza.“

U nastavku slijede rokovi čuvanja za neke vrste gradiva, tj. navest će se rokovi nakon koji se gradivo može izlučiti.

Nakon pedeset godina od nastanka:

- personalni listovi (dosjei) zaposlenika s prilozima i podatcima (status, kvalifikacije, ugovor o radu, osobne i obiteljske promjene, trajna porezna kartica, radni zadaci, evidencije izdanih zdravstvenih knjižica, zahtjevi za mirovinu),
- …

Nakon deset godina od godine nastanka:

- glavna financijska knjiga (kartice),
- obračun poreza na promet nekretnina,
- godišnje porezne evidencije (kartice) zaposlenika,
- …

Nakon pet godina od godine nastanka:

- knjiga analitičkog knjigovodstva (kartice),
- knjiga blagajne o dnevnom prometu gotovinom (knjiga kopija),
- ulazni i izlazni računi,
- evidencija ulaznih i izlaznih računa,
- putni računi (troškovi) za službena putovanja,
- obračuni plaćenih poreza i doprinosa (na dohodak),
- …

Nakon tri godine od godine nastanka:

- troškovnici za radove i usluge,
- dokumentacija o platnom prometu,
- obračunski listovi osobnih dohodaka,
- evidencije o prisutnosti na radu,
- …

Nakon dvije godine od godine nastanka:

- otpremnice, dostavnice, prijemni listovi, povratnice,
- izvještaji i doznake o bolovanju zaposlenika,
- rasporedi i rješenja o godišnjim odmorima,
- …

Nakon isteka jedne godine od godine nastanka:

- sporedni izborni materijal (glasački listići),
- vratarske evidencije o dolasku radnika na rad i kretanju stranaka,
- …

Postoji i Prilog 2 koji daje Orijentacijski popis gradiva trajne vrijednosti[516].

Trajno

- dokumenti o osnivanju, konstituiranju, registraciji, udruživanju, diobama, sanaciji, stečaju, likvidaciji, prestanku djelovanja i drugim statusnim promjenama,
- imovinsko-pravni dokumenti o nekretninama u posjedu (građevinska i druga tehnička dokumentacija s nacrtima, kupoprodajni i drugi ugovori, izvodi iz zemljišnih knjiga i dr.),
- matične knjige zaposlenika,
- državni proračuni i proračuni jedinica lokalne samouprave,
- evidencije o isplatama osobnih dohodaka (osobni kartoni ili isplatne liste),
- obrasci osobnih primanja za mirovinsko osiguranje (M-4),
- urbanistički i prostorni planovi,
- izumi, patenti, licence i inovacije svih vrsta (dokumentacija i evidencije),
- okružnice, upute, obavijesti, informacije, interna i javna glasila, službeni listovi, časopisi,
- …

Iz Pravilnika je naveden samo manji dio gradiva za koje su propisani rokovi čuvanja.

Hrvatsko arhivsko vijeće je 2012. donijelo Opći popis arhivskog i registraturnog gradiva s rokovima čuvanja[517]. Na navedenom popisu se nalaze kategorije ili vrste dokumentacije koja nastaje u obavljanju općih i administrativnih poslova u javnim tijelima i ustanovama. Popis navodi dokumentaciju koja nastaje kod svih stvaratelja na sličan ili isti način. Korist od ovog popisa je ta što navodi orijentacijske rokove čuvanja. Zbog lakšeg snalaženja

[516] Isto, str. 10
[517] Hrvatsko arhivsko vijeće (2012), Opći popis arhivskog i registraturnog gradiva s rokovima čuvanja, http://arhinet.arhiv.hr/_Download/PDF/Opci_popis_gradiva_s_rokovima_cuvanja.pdf (28.08.2018.)

popis je uređen hijerarhijski, a može poslužiti i za izradu klasifikacijskih planova dokumentacije.

Slijede korištene oznake o rokovima čuvanja iz navedenog popisa[518]:

- N - Rok čuvanja računa se od isteka godine u kojoj je dokumentacija nastala,
- Z - Rok čuvanja računa se od isteka godine u kojoj je spis zaključen, odnosno u kojoj je dokument (ugovor, odluka, pravilnik i sl) prestao važiti ili je zamijenjen drugim odgovarajućim dokumentom,
- D = Djelomično odabrati

  Po isteku roka čuvanja odabire se prema uputama nadležnog državnog arhiva dio dokumentacije za trajno čuvanje. U pravilu se radi o slučajevima gdje se među istovrsnim predmetima i dokumentima mogu naći oni koji se odnose na značajnije događaje, odluke, stvari ili osobe te ih se uslijed toga odabire za trajno čuvanje,
- I = Izlučiti

  Po isteku roka dokumentacija se može izlučiti u cjelini, uz pribavljano odobrenje nadležnog državnog arhiva,
- T = Trajno čuvati

  Po isteku roka dokumentacija se u cjelini odabire za trajno čuvanje.

Uzevši u obzir da tijela javne uprave svake godine stvaraju veliku količinu dokumenata, a među njima je sve više elektroničkih dokumenata (i elektronički potpisanih), dugoročna pohrana takve dokumentacije (sukladno propisanim rokovima) postavlja ozbiljan izazov za javnu upravu.

8.4 NORME ZA DUGOROČNO OČUVANJE ELEKTRONIČKIH DOKUMENATA

Ministarstvo gospodarstva Republike Hrvatske je u svibnju 2013. donijelo popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj[519]

[518] Isto, str. 3

[519] Ministarstvo gospodarstva (2013.), Popis normizacijskih dokumenata u području primjene zakona o elektroničkom potpisu i pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u

(Popis). Vrijednost Popisa je što je dao vrlo iscrpan pregled hrvatskih i europskih normizacijskih dokumenata za navedeno područje. Europska Unija je 2014. Donijela Uredbu eIDAS[520] koja je u punoj primjeni od lipnja 2016. godine. Kao što je već više puta u ovom radu spomenutu Uredba eIDAS je stavila izvan snage Direktivu 1999/93/EZ Europskog parlamenta, a Republika Hrvatska je preuzimanjem ove Uredbu stavila van snage Zakon o elektroničkom potpisu. Međutim, ovaj Popis daje pregled standarda i normi koji su i dalje važeći (nisu ovisili o opozvanim aktima) te su time zanimljivi i za ovaj rad. U nastavku je prikazan spomenuti Popis Ministarstva gospodarstva, a na temelju njega će više biti rečeno o normama koje su bitne za dugoročno očuvanje elektroničkih dokumenata.

poslovanju davatelja usluga certificiranja u Republici Hrvatskoj, (NN 89/13), https://narodne-novine.nn.hr/clanci/sluzbeni/2013_07_89_1957.html (04.02.2018.)

[520] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

Tablica 13. Popis normizacijskih dokumenata u području primjene zakona o elektroničkom potpisu i pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj[521]

Članak – Pravilnik	Oznaka hrvatskoga normizacijskog dokumenta	Naslov hrvatskoga normizacijskog dokumenta	Oznaka europskoga/međunarodnoga normizacijskog dokumenta	Naslov europskoga/međunarodnoga normizacijskog dokumenta
Čl. 12. st. 3. Čl. 40. st. 1.	HRN ISO/IEC 15408-1:2013	Informacijska tehnologija – Sigurnosne tehnike – Kriteriji za vrednovanje sigurnosti IT-a – 1. dio: Uvod i opći model	ISO/IEC 15408-1:2009	Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
Čl. 12. st. 3. Čl. 40. st. 1.	HRN ISO/IEC 15408-2:2013	Informacijska tehnologija – Sigurnosne tehnike – Kriteriji za vrednovanje sigurnosti IT-a – 2. dio: Funkcionalni zahtjevi za sigurnost	ISO/IEC 15408-2:2008	Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
Čl. 12. st. 3. Čl. 40. st. 1.	HRN ISO/IEC 15408-3:2013	Informacijska tehnologija – Sigurnosne tehnike – Kriteriji za vrednovanje sigurnosti IT-a – 3. dio: Jamstveni zahtjevi za sigurnost	ISO/IEC 15408-3:2008	Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements
Čl. 12. st. 4.			FIPS PUB 140-1, minimum level 2	Federal Information Processing Standards Publication 140-1 – Security requirements for cryptographic modules, minimum level 2
Čl. 12. st. 4.			FIPS PUB 140-2, minimum level 2	Federal Information Processing Standards Publication 140-2 – Security requirements for cryptographic modules, minimum level 2
Čl. 12. st. 4.			CWA 14169	CEN Workshop Agreement CWA 14169 – Secure signature-creation devices »EAL 4+«: 2004
Čl. 35. st. 1.			IETF/RFC 3647 (2003)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (IETF RFC 3647)
Čl. 58. st 2. Čl. 59. st. 1. Čl. 59. st. 2.			IETF/RFC 3161	Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP)
Čl. 27. st. 2. Čl. 40. st 2. Čl. 57.	HRN ISO/IEC 27001:2006	Informacijska tehnologija – Sigurnosne tehnike – Sustavi upravljanja informacijskom sigurnošću – Zahtjevi (ISO/IEC 27001:2005)	ISO/IEC 27001:2005	Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005)
Čl. 27. st. 2. Čl. 40. st 2.***	HRN ISO/IEC 27002:2006	Informacijska tehnologija – Sigurnosne tehnike – Kodeks postupaka za upravljanje informacijskom sigurnošću (ISO/IEC 27002:2005) – istovjetna normi HRN ISO/IEC 17799:2006+Ispr.1:2007	ISO/IEC 27002:2005	Information technology – Security techniques – Code of practice for information security management (ISO/IEC 27002:2005) – identical to HRN ISO/IEC 17799:2006+Ispr.1:2007

[521] Ministarstvo gospodarstva (2013.), Popis normizacijskih dokumenata u području primjene zakona o elektroničkom potpisu i pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj, (NN 89/13), https://narodne-novine.nn.hr/clanci/sluzbeni/2013_07_89_1957.html (04.02.2018.)

Članak – Pravilnik	Oznaka hrvatskoga normizacijskog dokumenta	Naslov hrvatskoga normizacijskog dokumenta	Oznaka europskoga/međunarodnoga normizacijskog dokumenta	Naslov europskoga/međunarodnoga normizacijskog dokumenta
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 101 733 V2.1.1:2012	Elektronički potpisi i infrastrukture (ESI) – Napredni elektronički potpisi u CMS-u (CAdES) (ETSI/TS 101 733 V2.1.1:2012)	ETSI/TS 101 733 V2.1.1:2012	Electronic Signatures and Infrastructures (ESI) – CMS Advanced Electronic Signatures (CAdES) (ETSI/TS 101 733 V2.1.1:2012)
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 101 903 V1.4.2:2012	Elektronički potpisi i infrastrukture (ESI) – Napredni elektronički potpisi u XML-u (XAdES) (ETSI/TS 101 903 V1.4.2:2010)	ETSI/TS 101 903 V1.4.2:2010	Electronic Signatures and Infrastructures (ESI) – XML Advanced Electronic Signatures (XAdES) (ETSI/TS 101 903 V1.4.2:2010)
Čl. 24. st. 2. Čl. 35. st. 2. Čl. 38. st. 1. Čl. 40. st. 1. Čl. 53. st.1. Čl. 54. st 2.	HRN ETSI/EN 319 401 V1.1.1:2013	Elektronički potpisi i infrastrukture (ESI) – Sveopći zahtjevi općih pravila za vjerodostojne davatelje usluga koje podržavaju elektroničke potpise (EN 319 401 V1.1.1:2013)	ETSI/EN 319 401 V1.1.1:2013	Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers supporting Electronic Signatures (EN 319 401 V1.1.1:2013)
Čl. 24. st. 2.* Čl. 35. st. 2.* Čl. 38. st. 1.* Čl. 39. st. 3. Čl. 40. st 1.* Čl. 53. st.1.* Čl. 54. st 2.*	HRN ETSI/EN 319 411-2 V1.1.1:2013	Elektronički potpisi i infrastrukture (ESI) – Opća pravila i sigurnosni zahtjevi za vjerodostojne davatelje usluga certificiranja – 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate (EN 319 411-2 V1.1.1:2013)	ETSI/EN 319 411-2 V1.1.1:2013	Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Policy requirements for certification authorities issuing qualified certificates (EN 319 411-2 V1.1.1:2013)
Čl. 24. st. 2.** Čl. 35. st. 2. ** Čl. 38. st. 1. ** Čl. 40. st 1.** Čl. 53. st.1.** Čl. 54. st 2.**	HRN ETSI/EN 319 411-3 V1.1.1:2013	Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za opća pravila i sigurnost za vjerodostojne davatelje usluga koji izdaju certifikate – 3. dio: Opća pravila za certifikacijska tijela koja izdaju certifikate s javnim ključem (EN 319 411-3 V1.1.1:2013)	ETSI/EN 319 411-3 V1.1.1:2013	Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 3: Policy requirements for Certification Authorities issuing public key certificates (EN 319 411-3 V1.1.1:2013)
Čl. 55. st. 2. Čl. 58. st. 2.	HRS ETSI/TS 102 023 V 1.2.2:2009	Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za osobe ovlaštene za otiskivanje vremena (ETSI TS 102 023 V1.2.2:2008)	ETSI/TS 102 023 V1.2.2:2008	Electronic signatures and infrastructures (ESI) -Policy requirements for time stamping authorities (ETSI TS 102 023 V1.2.2:2008)
Čl. 59. st 2.	HRS ETSI/TS 101 861 V1.4.1:2012	Elektronički potpisi i infrastrukture (ESI) – Profil vremenskoga žiga (ETSI/TS 101 861 V1.4.1:2011)	ETSI/TS 101 861 V1.4.1:2011	Electronic Signatures and Infrastructures (ESI) – Time stamping profile (ETSI TS 101 861 V1.4.1:2011)
Čl. 44. st. 3.	HRN ETSI/EN 319 412-5 V1.1.1:2013	Elektronički potpisi i infrastrukture (ESI) – Profili vjerodostojnih davatelja usluga koji izdaju certifikate – 5. dio: Proširenje za profil kvalificiranoga certifikata (EN 319 412-5 V1.1.1:2013)	ETSI/EN 319 412-5 V1.1.1:2013	Electronic Signatures and Infrastructures (ESI) – Profiles for Trust Service Providers issuing certificates – Part 5: Extension for Qualified Certificate profile (EN 319 412-5 V1.1.1:2013)
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 102 778-1	Elektronički potpisi i infrastrukture (ESI) – Profili naprednog elektroničkog potpisa u PDF-u – 1. dio: PAdES pregled – Okvirni dokument za PAdES (ETSI/TS 102 778-1 V1.1.1:2009)	ETSI/TS 102 778-1 V.1.1.1:2009	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview – a framework document for PAdES (ETSI TS 102 778-1 V.1.1.1:2009)

Članak – Pravilnik	Oznaka hrvatskoga normizacijskog dokumenta	Naslov hrvatskoga normizacijskog dokumenta	Oznaka europskoga/međunarodnoga normizacijskog dokumenta	Naslov europskoga/međunarodnoga normizacijskog dokumenta
	V.1.1.1:2009			
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 102 778-2 V.1.2.1:2009	Elektronički potpisi i infrastrukture (ESI) – Profili naprednog elektroničkog potpisa u PDF-u – 2. dio: Osnovni PAdES – Profil na osnovu ISO 32000-1 (ETSI/TS 102 778-2 V1.2.1:2009)	ETSI/TS 102 778-2 V.1.2.1:2009	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic – Profile based on ISO 32000-1 (ETSI TS 102 778-2 V.1.2.1:2009)
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 102 778-3 V1.2.1:2012	Elektronički potpisi i infrastrukture (ESI) – Napredni elektronički potpis u PDF-u – 3. dio: Poboljšani PAdES – PAdES-BES i PAdES-EPES profili (ETSI/TS 102 778-3 V1.2.1:2010)	ETSI/TS 102 778-3 V1.2.1:2010	Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles (ETSI/TS 102 778-3 V1.2.1:2010)
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 102 778-4 V1.1.2:2012	Elektronički potpisi i infrastrukture (ESI) – Profili naprednoga elektroničkog potpisa u PDF-u – 4. dio: Dugotrajni PAdES – PAdES LTV profili (ETSI/TS 102 778-4 V1.1.2:2009)	ETSI/TS 102 778-4 V1.1.2:2009	Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 4: PAdES Long Term – PAdES LTV Profile (ETSI/TS 102 778-4 V1.1.2:2009)
Čl. 6. st. 4. Čl. 10. st. 2.	HRS ETSI/TS 102 778-5 V1.1.2:2012	Elektronički potpisi i infrastrukture (ESI) – Profili naprednoga elektroničkog potpisa u PDF-u – 5. dio: PAdES za sadržaj u XML-u – Profili za potpise XAdES-a (ETSI/TS 102 778-5 V1.1.2:2009)	ETSI/TS 102 778-5 V1.1.2:2009	Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 5: PAdES for XML Content – Profiles for XAdES signatures (ETSI/TS 102 778-5 V1.1.2:2009)
Čl. 13. st.1.			Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
Čl. 13. st.2. Čl. 53. st.2.	HRS ETSI/TS 102 176-1 V2.1.1:2012	Elektronički potpisi i infrastrukture (ESI) – Algoritmi i parametri za sigurne elektroničke potpise – 1. dio: Hash funkcije i asimetrični algoritmi (ETSI/TS 102 176-1 V2.1.1:2011)	ETSI/TS 102 176-1 V2.1.1:2011	Electronic Signatures and Infrastructures (ESI) – Algorithms and Parameters for Secure Electronic Signatures – Part 1: Hash functions and asymmetric algorithms (ETSI/TS 102 176-1 V2.1.1:2011)
Čl. 24. st. 3.			CWA 14167-1	CEN Workshop Agreement CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements

Missoni[522] navodi da su od posebnog značaja za dugoročno arhiviranje elektroničkih isprava bitni sljedeći članci – pravilnici:

- Elektronički potpisi i infrastrukture (ESI) – CMS usavršeni elektronički potpisi (CAdES) (ETSI TS 101 733 V.1.7.4.:2008),
- XML usavršeni elektronički potpisi (XAdES) (ETSI TS 101 903 V1.4.1:2009),
- Elektronički potpisi i infrastrukture (ESI)-Profili PDF usavršenog elektroničkog potpisa-CMS profil na osnovu ISO 32000-1 (ETSI TS 102 778 V.1.1.1:2009),
- Elektronički potpisi i infrastrukture (ESI)-Profili PDF usavršenog elektroničkog potpisa-4. Dio: Dugotrajni PAdES – Profili PAdES-LTV (ETSI TS 102 778-4 V.1.1.1:2009),
- Profil otiska vremena (ETSI TS 101 861 V.1.3.1:2006).

Ovdje je bitno spomenuti da Popis Ministarstva gospodarstva, uz međunarodne norme, sadrži i oznake hrvatskih normi (koje je na osnovu međunarodnih normi prihvatio Hrvatski zavod za norme, HZN[523]). Primjer je prethodno spomenuta norma ETSI TS 102 778 V.1.1.1:2009 (Elektronički potpisi i infrastrukture (ESI)-Profili PDF usavršenog elektroničkog potpisa-CMS profil na osnovu ISO 32000-1). Navedena norma je prihvaćena od strane Hrvatskog zavoda za norme te je dobila sljedeću oznaku (navedeno je i u Popisu): HRS ETSI/TS 102 778-4 V1.1.2:2012.

Za dugoročnu pohranu elektroničkih dokumenata bitna je i MoReq2 specifikacija[524] (engl. **Mo**del **Req**uirements for the Management of Electronic Records, second version). MoReq2 se sastoji od formalne specifikacije zahtjeva za generički sustav upravljanja elektroničkim zapisima, praćen testnom dokumentacijom i povezanim informacijama. Europska komisija je specifikaciju objavila 2008. godine, a namijenjena je za korištenje u Europskoj Uniji. Međutim, može se koristiti i drugdje. MoReq2 se općenito smatra de facto standardom u Europi, ali nema formalni status kao standard[525]. Missoni navodi[526] da je izdana i MoReq10 specifikacija, ali da je jasno da ona nije zaživjela i da se ne koristi u

[522] Heđbeli, Ž., Missoni, E. et al. (2016.), Arhiviranje, evidencije i rokovi čuvanja dokumentacije, TEB Poslovno savjetovanje d.o.o., Zagreb, str. 39.
[523] Hrvatski zavod za norme, HZN, http://www.hzn.hr / (04.02.2018.)
[524] Europska komisija (2008.), MoReq2, Model Requirements for the Management of Electronic Records, second version, European Commision, http://moreq2.eu/attachments/article/189/MoReq2_typeset_version.pdf (04.02.2018.)
[525] MoReq2, https://en.wikipedia.org/wiki/MoReq2 (04.02.2018.)
[526] Heđbeli, Ž., Missoni, E. et al. (2016.), Arhiviranje, evidencije i rokovi čuvanja dokumentacije, TEB Poslovno savjetovanje d.o.o., Zagreb, str. 40.

praksi te da je samo jedno rješenje za upravljanje zapisima certificirano u skladu sa starijom MoReq2 specifikacijom.

Missoni, nadalje navodi[527] da je najčešće korištena referentna specifikacija za e-Arhiv ISO 14721:2003 – Open Archival Information System (OAIS). OAIS je u ovom radu detaljno obrađen u poglavlju 2. OAIS – Referentni model za elektronički arhiv.

Za dugoročno čuvanje elektroničkih dokumenata postoji norma ISO 19005-1:2005, Upravljanje dokumentima – Format elektroničke datoteke za dugoročnu pohranu (PDF/A-1)[528]. Ovaj standard je i Hrvatski zavod za norme prihvatio kao hrvatsku normu pod oznakom HRN ISO 19005:2008. PDF A-1 ima dvije mogućnosti (PDF/A-1a koji osigurava strukturu i vizualni prikaz, te PDF/A-1b koji osigurava vizualni prikaz). PDF/A-1 se temelji na PDF verziji verzije 1.4 (od tvrtke Adobe Systems Inc.[529]) koji se prvi put implementirao u proizvodu Adobe Acrobat 5. Primjenjuje se na dokumente koji sadrže kombinacije karaktera, rastera i vektorskih podataka. PDF/A-1 je danas svjetski standard za dugoročno očuvanje elektroničkih dokumenata.

Sljedeća verzija PDF/A ISO normi je PDF/A-2 - ISO 19005-2:2011[530] koja je donesena 2011. godine. Ona je temeljena na PDF specifikaciji 1.7 kako je formalizirano u ISO normi 32000-1[531] za dugoročno očuvanje statičke vizualne prezentacije elektroničkih dokumenata koji se sastoje od stranica. PDF/A-2 omogućava JPEG2000 kompresiju, transparentne elemente i PDF slojeve. PDF/A-2 omogućava ugradnju OpenType fontova i podršku za već spomenuti PAdES elektronički potpis (engl. PDF Advanced Electronic Signatures). PDF/A-2 ima i funkciju spremnika što znači da se PDF/A datoteke mogu se ugraditi u PDF /A-2 dokument.

[527] Isto, str. 40.
[528] ISO (2005., 2.), ISO 19005-1:2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1), https://www.iso.org/standard/38920.html (04.02.2018.)
[529] Adobe Systems Inc., https://www.adobe.com/ (04.02.2018.)
[530] ISO (2011.), ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2), https://www.iso.org/standard/50655.html (04.02.2018.)
[531] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (21.08.2017.)

PDF/A-3 - ISO 19005-3: 2012[532] donesena je 2012. i specificira upotrebu Portable Document Format (PDF) 1.7, kako je formalizirano u ISO 32000-1 za dugoročno očuvanje statičke vizualne prezentacije elektroničkih dokumenata koji se sastoje od stranica uz mogućnost da bilo koja vrsta drugog sadržaja može biti uključena kao ugrađena datoteka ili privitak. Missoni navodi[533] da je PDF/A-3 izabran kao format za elektronički potpis u Njemačkoj jer su u njemu uključeni podaci samog elektroničkog računa na standardan način (račun se može pregledavati na zaslonu ili otisnuti na papiru) i kao XML podatke, koji automatizirane aplikacije za obradu računa mogu preuzeti i obrađivati. Missoni u nastavku napominje[534] da ukoliko se elektronički potpisani dokumenti (npr. u .doc formatu) pretvaraju bilo u PDF ili u PDF/A formate, tada se elektronički potpisi izbrišu i dobiju se zakonski nevažeći dokumenti kojim se više ne može jamčiti integritet, autentičnost i vrijeme u kojem su izvorno nastali. Nastavno na već rečeno slijedi zaključak[535]: „Dakle, PDF i PDF/A (nastali konverzijom iz drugih formata) ne mogu prihvatiti elektroničke potpise iz izvorne elektroničke isprave i drugih elektronički potpisanih dokumenata, te se isti ne preporučaju radi dugoročnog arhiviranja elektronički potpisanih dokumenata. Ukoliko se želi zadržati izvorni elektronički potpis, treba pohraniti te (originalne) elektroničke isprave i dokumente u sustav za upravljanje zapisima – elektroničku arhivu“.

Missoni nakon toga navodi sljedeće[536] (što je vrlo bitno i za ovaj rad): „Čak i ako se elektroničke isprave ne čuvaju u specijaliziranom sustavu za upravljanje zapisima, zahvaljujući elektroničkom potpisu kojim su potpisane, njihova zakonska snaga, autentičnost i integritet i vrijeme u kome su potpisane ostaju osigurani od izmjena primijenjenom PKI tehnologijom kojom je elektronički potpis napravljen, a ako se elektronički potpis radi u skladu s jednim od ETSI standarda za napredni elektronički potpis (Advanced Electronic Signature – CAdES, XAdES ili PAdES) i profilima za dugoročno arhiviranje, moći će se vršiti i naknadno validiranje certifikata s kojim su potpisani kao i zaštita tako potpisanih dokumenata od eventualnih izmjena omogućenih

[532] ISO (2012., 2.), ISO 19005-3:2012 - Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3) (04.02.2018.)https://www.iso.org/standard/57229.html (04.02.2018.)
[533] Heđbeli, Ž., Missoni, E. et al. (2016.), Arhiviranje, evidencije i rokovi čuvanja dokumentacije, TEB Poslovno savjetovanje d.o.o., Zagreb, str. 42.
[534] Isto, str. 42.
[535] Isto, str. 42.
[536] Isto, str. 42.

budućim napretkom tehnologija i zastarijevanja primijenjenih mehanizama zaštite u trenutku potpisa“.

Budući da su u ovom radu u poglavlju 4. Napredni elektronički potpis kao podloga za dugoročno očuvanje elektroničkih zapisa već obrađeni postupci izrade naprednih elektroničkih potpisa koji se rade u skladu s ETSI standardima (XAdES, CAdES i PAdES) s pripadnim profilima za dugoročno očuvanje te postupci validacije takvih potpisa te uzevši u obzir teze koje je Missoni u vezi s njima iznio, navedeni formati naprednog elektroničkog potpisa se u ovom poglavlju neće ponovo detaljnije navoditi i obrađivati.

8.5 ZAKLJUČAK

Europski okvir za interoperabilnost, EIF (engl. European Interoperability Framework) daje specifične smjernice o uspostavljanju interoperabilnih elektroničkih javnih usluga. Bitan projekt u osiguravanju Europskog interoperabilnog okvira je SPOCS, te njezin gradivni blok eDokumenti i elektronički potpisi. SPOCS specifikacija definira višeslojni format kontejnera elektroničkih dokumenata, OCD koji se sastoji od: sloj nosivosti, sloja metapodataka i sloja provjere autentičnosti. Trenutačno su specificirani OCD spremnici temeljeni na ZIP i PDF ekstenziji. OCD temeljen na PDF formatu koristi mehanizam PDF-a s privicima (PDF 1.7 specifikacija).

Hrvatski zakon o elektroničkoj ispravi (ZEI) donesen je 2005. i po mišljenju Lisičara je zaokružio paket zakona koji uređuju područje elektroničkog poslovanja. Nakon donošenja Uredbe eIDAS i povlačenja hrvatskog Zakona o elektroničkom potpisu postoji nedorečenost vrijedi li i dalje Zakon o elektroničkoj ispravi. Smatram da je ZEI umnogome pomogao široj implementaciji i korištenju elektroničkih dokumenata u Republici Hrvatskoj. ZEI definira elektroničku ispravu, dokumentacijski ciklus, obrasce prikaza, vanjski i unutarnji obrazac (uočio sam sličnost s OCD spremnikom za eDokumente) te arhiviranje elektroničkih isprava. Kao prvu implementaciju elektroničke isprave u Republici Hrvatskoj i kao trenutak zamjene pečata i potpisa se spominje servis HITRO.HR-a e-Tvrtka za registraciju tvrtki (d.o.o. i j.d.o.o.).

Nakon Hrvatske se analizira stanje pravne uređenosti korištenja elektroničkog dokumenta po odabranim svjetskim zemljama: SAD, Rusija, Škotska, Litva, Urugvaj, Filipini … Manji dio zemalja je elektroničkom dokumentu posvetio zaseban zakon. Većina zemalja je istim zakonom pokrila i područje elektroničkog potpisa i elektroničkog dokumenta.

Za manji dio dokumentacije propisane Pravilnikom o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva navedeni su definirani rokovi čuvanja (rokovi su: 50, 10, 5, 3, 2, 1 godinu, te trajno). Javne uprave svake godine stvara, međuostalim, veliku količinu elektroničkih dokumenata (i elektronički potpisanih) pa dugoročna pohrana takve dokumentacije postaje ozbiljan izazov.

Na kraju su obrađene norme za dugoročno očuvanje elektroničkih dokumenata. Navedeni su MoReq2, PDF/A-1, PDF/A-2, PDF/A-3. Konverzijom elektronički potpisanih dokumenata u PDF/A formate se gube elektronički potpisi te se isti ne preporučaju radi dugoročnog arhiviranja elektronički potpisanih dokumenata. Kada se elektronički potpis izrađuje u skladu s ETSI standardima za napredni elektronički potpis (CAdES, XAdES ili PAdES) i profilima za dugoročno arhiviranje tada se takvi potpisi mogu naknadno validirati što je preduvjet za izgradnju arhiva za elektronički potpisane dokumente.

9. ANALIZA PRAKSE I MODELA DUGOTRAJNE POHRANE

U ovom poglavlju će biti obrađene najbolje prakse u implementaciji sustava za dugotrajnu pohranu te referentni modeli. Obradit će se njemački arhivski zdravstveni sustav (klinika Braunschweig), njemački referentni model za izradu elektroničkog arhiva. HALMED agencija će biti obrađena kao primjer dobre prakse implementacije dugotrajne pohrane dokumentacije za potrebe navedene institucije. Nadalje će biti obrađeni konkretni primjeri elektronički arhiva za javne uprave u Estoniji i Litvi te Vicenza arhivski zdravstveni sustav u Italiji. Obradit će se i E-ARK projekt na razini Europske Unije koji je pilotirao postojeće arhivske servise koji zadržavaju autentičnost i čitljivost na postojećim najboljim praksama. Osim ovih studija slučajeva obradit će se i rezultati dviju komparativnih analiza: InterPARES Trust istraživačkog projekta za analizu implementiranih elektroničkih javnih servisa i komparativna analiza unutarnje strukture i funkcija elektoničkog arhiva za složene elektroničke zapise.

9.1 InterPARES Trust - KOMPARATIVNA ANALIZA IMPLEMENTIRANIH ELEKTRONIČKIH JAVNIH SERVISA

Komparativna analiza implementiranih elektroničkih javnih servisa[537] (engl. Comparative Analysis of Implemented Governmental e-Services) je istraživačka studija (u daljem tekstu Studija) koja je obavljena unutar projekta InterPARES Trust 2014. godine. Završni izvještaj[538] (engl. Final report) navedene Studije je objavljen u svibnju 2015. godine. Kako sam bio aktivan član tima koji je radio kao doktorand na spomenutoj Studiji, ona će i ovdje biti ukratko opisana te će biti navedena neka njezina saznanja s fokusom na dugotrajno očuvanje elektronički potpisanih zapisa. Motivacija za ovo istraživanje nam je bila pronaći dovoljno informacija o elektroničkim javnim uslugama kako bi provjerili jesu li usluge izgrađene kao: odgovorne, pouzdane, točne, sigurne, transparentne i vjerodostojne te razmatraju li problematiku pitanja vezana uz privatnost, obaveze čuvanja i pravo na zaborav.

[537] InterPARES Trust Studies, Comparative Analysis of Implemented Governmental e-Services (EU09), Project List by Title, https://interparestrust.org/trust/about_research/studies (20.02.2018.)
[538] Stančić, H., Brzica, H., Adžaga, I., Garić, A., Poljičak-Sušec, M., Presečki, K., Stanković, A. (2015.), Comparative Analysis of Implemented Governmental e-Services (EU09), Final report, InterPARES Trust Project, https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisImplementedGovernmentaleServices_FinalReport.pdf (20.02.2018.)

Istraživanje smo podijelili u četiri faze: 1. Identifikacija, 2. Prikupljanje podataka, 3. Analiza i 4. Tumačenje podataka.

Studija je obuhvatila određeni broj elektroničkih usluga za osam članica Europske Unije: Belgiju, Hrvatsku, Dansku, Estoniju, Njemačku, Litvu, Švedsku i Ujedinjeno Kraljevstvo. Hrvatska je odabrana za usporedbu jer je istraživanje provedeno u Hrvatskoj te zbog dostupnosti potrebnih materijala i mogućnosti usporedbe razvoja Hrvatske s razvojem drugih zemalja. Ostalih sedam zemalja izabrano je na temelju najbolje online dostupnosti materijala potrebnih za istraživanje. Odabrane usluge su detaljno istražene po upitniku koji je formirao istraživački tim. Istraživanje usluga elektroničke javne uprave usvojilo je reprezentativni skup od 20 usluga (engl. Representative basket of 20 services) kako je opisano u dokumentu Europske komisije od prosinca 2010. godine „Digitalizacija javnih usluga u Europi: Stavljanje ambicija u akciju“[539] (engl. Digitizing Public Services in Europe: Putting ambition into action). Ovaj dokument dijeli elektroničke javne usluge u dvije glavne grupe: usluge za građane (G2C, 12 usluga) i usluge za poslovne subjekte (G2B, 8 usluga). U nastavku slijedi popis usluga koje su obrađene po navedenih osam zemljama uz navedene oznake pojedinih usluga.

Elektroničke javne usluge za građane (C1-C12):

1. Prijava poreza na dohodak (engl. Income taxes),
2. Usluga zavoda za zapošljavanje (engl. Job search),
3. Socijalne naknade (engl. Social security benefits),
4. Osobni dokumenti (engl. Personal documents),
5. Registracija vozila (engl. Car registration),
6. Građevna dozvola (engl. Application for building permission),
7. Prijave policiji (engl. Declaration to the police),
8. Javne knjižnice (engl. Public libraries),
9. Izvodi iz matičnih knjiga (engl. Birth and marriage certificates
10. Upisi na visokoškolske ustanove (engl. Enrolment in higher education),
11. Promjena boravišta (engl. Announcement of moving),
12. Health-related services (engl. Zdravstvene usluge).

[539] Capgemini et al. (2010.), Digitizing Public Services in Europe: Putting ambition into action, 9 th. Benchmark Measurement, pripremili Capgemini, IDC, Rand Europe, Sogeti i DTi za Europsku komisiju, ec.europa.eu/newsroom/document.cfm?action=display&doc_id=747 (20.02.2018.)

Elektroničke javne usluge za poslovne subjekte (B1-B8)

1. Socijalno osiguranje zaposlenika (engl. Social contribution for employees),
2. Porez na dobit (engl. Corporate tax),
3. Porez na dodanu vrijednost (engl. VAT - Value Added Tax),
4. Upis u registar poslovnih subjekata (engl. Registration of a new company),
5. Prijava podataka Državnom zavodu za statistiku (engl. Submission of data to the statistical office),
6. Custom declaration (engl. Carinska prijava),
7. Dozvole i izvještaji temeljem studija utjecaja na okoliš (engl. Environment-related permits),
8. Javna nabava (engl. Public procurement).

Rad na ovoj Studiji je bio ograničen na G2C i G2B elektroničke usluge. Ostale usluge (B2B, B2C i C2C) nisu analizirane jer se ne smatraju državnim e-uslugama. Identificiranih dvanaest G2C i osam G2B e-usluga analizirane su u svakoj od osam zemalja kako bi se utvrdile ključne komponente usluga. Navedeno je iskorišteno za izradu upitnika za elektroničke javne usluge. Upitnik se sastojao od 52 pitanja koja su bila podijeljena u 6 kategorija.

Kategorije pitanja iz upitnika bile su sljedeće:

1. Osnovne informacije o servisu (engl. Basic service information) - 11 pitanja,
2. Korisnici (engl. Users) - 7 pitanja,
3. Optimizacija poslovanja (engl. Business optimization) - 4 pitanja,
4. Tehnološka rješenja (engl. Technological solutions) - 14 pitanja,
5. Pohrana i trajna dostupnost sadržaja (engl. Storage and long-term content availability) - 10 pitanja,
6. Transparentnost rada sustava (engl. System operation transparency) - 6 pitanja.

Upitnik se nalazi u ovom radu kao Prilog 1 – Upitnik za elektroničke javne usluge.

Ključno pitanje kojim smo se kao istraživački tim vodili prilikom utvrđivanja hoćemo li se baviti s analizom neke elektroničke javne usluge ili ne – bilo je ima li usluga razinu zrelosti 2 ili više. U slučaju kad je razina zrelosti bila 1 ili 0, nismo ju smatrali dobrim kandidatom

za detaljnije istraživanje. Kao razine zrelosti usluga od 0 do 5 su uzete razine informatiziranosti elektroničkih javnih usluga definirane Bangemannovim izvještajem (u ovom radu su već navedene u tablici 5 u poglavlju 6. Elektronička javna uprava).

U drugoj fazi (Prikupljanju podataka) razvijeni upitnik je korišten za prikupljanje informacija o dvanaest G2C i osam G2B elektroničkih usluga u osam zemalja. Upitnike smo ispunili tijekom internetske istrage. Ukupno je bilo 8320 pitanja. Neka pitanja, u nedostatku izvora s interneta, nisu odgovorena.

U trećoj fazi (Analiza podataka) smo ispunjene upitnike o elektroničkim javnim uslugama prvo analizirali po zemljama, a zatim usporedno putem kategorija servisa (12 + 8).

Četvrta faza je bila faza Tumačenja podataka, a za ovaj rad su relevantna saznanja iz kategorije pitanja Pohrana i trajna dostupnost sadržaja[540] pa će ona biti i navedena u ovom radu kako slijedi. Razdoblje čuvanja podataka u sustavima istraživanih elektroničkih javnih usluga razlikuju se u ovisnosti o vrsti podataka koji se čuvaju, vrsti institucije odgovorne za podatke. Primjerice u Njemačkoj i Ujedinjenom Kraljevstvu visokoškolske institucije i sveučilišta su dužni čuvati podatke tijekom studiranja te još tri godine povrh toga. S druge strane, u Hrvatskoj i Švedskoj, evidencije o podacima zdravstvene i socijalne skrbi koje su stvorene elektroničkim uslugama trebaju se čuvati najmanje 30 godina. Nakon isteka razdoblja čuvanja podataka, takvi podaci se brišu ili uništavaju. Informacije o tome su pronađene u dostupnoj dokumentaciji sedam usluga. Zanimljivo je i istraženo ponašanje s podacima za e-uslugu prijave policiji. Naime, u tom servisu se podaci brišu nakon 30 dana, a u slučaju kada se radi o osjetljivim podacima isti se odmah brišu iz IT sustava e-usluge.

Što se tiče informacija o preferiranim dugoročnim formatima očuvanja zapisa, takve su pronađene samo u slučaju jedne e-usluge: litvanske e-usluge za socijalne doprinose zaposlenicima. U tom servisu se koriste formati: PDF/A i XAdES-A, a podaci su pohranjeni u središnjoj litavskoj elektroničkoj arhivskoj informacijskoj službi (EAIS).

[540] Stančić, H., Brzica, H., Adžaga, I., Garić, A., Poljičak-Sušec, M., Presečki, K., Stanković, A. (2015.), Comparative Analysis of Implemented Governmental
e-Services (EU09), Final report, InterPARES Trust Project, https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisImplementedGovernmentaleServices_FinalReport.pdf, str. 15-16 (20.02.2018.)

U istraženim servisima nisu pronađene informacije o sukladnosti e-usluga s dugoročnim standardima očuvanja. Također, nisu pronađeni niti podaci o mogućoj ponudi korištenja elektroničke arhive kao dodatne usluge.

U ovom istraživanju nije bilo moguće pronaći odgovor koje institucije su obavljale udomljavanje vlastitih e-usluga, ali je bilo dosta informacija o mjestima gdje su primljeni podaci pohranjeni. Takve informacije su pronađene kod 19 servisa, a primjeri pohranjivanja podataka u nadležnim institucijama su poput onih u kategorijama traženja posla, upisa u visoko obrazovanje i podnošenja podataka statističkom uredu. Primjeri pohranjivanja podataka izvan informacijskih sustava nadležnih institucija su prijave policiji u Danskoj i Njemačkoj gdje su podaci pohranjeni na posebno zaštićenim mjestima s autoriziranim pristupom. Ostali takvi pronađeni primjeri su zdravstvene usluge u Danskoj i Estoniji gdje se podaci pohranjuju u centraliziranoj nacionalnoj bazi podataka kojoj mogu pristupiti sve bolnice.

Nije bilo moguće pronaći odgovor koriste li e-usluge rješenja u oblaku i nalaze li se pružatelji usluga udomljavanja servisa u istoj zemlji, ali su pronađene informacije o korištenju rješenja u oblaku za pohranu podataka su pronađeni u kategoriji socijalnog osiguranja za zaposlenike u četiri zemlje: Hrvatskoj, Estoniji, Njemačkoj i Litvi.

Na kraju finalnog izvještaja je istraživački tim dao i neke preporuke slijedom dobivenih saznanja. Relevantna je preporuka koju je tim dao oko obaveze objave načina skladištenja i dugoročnog očuvanja podataka. Naime, prilikom istraživanja e-usluga gotovo uopće nisu postojale takve javno objavljene informacije. Na takav način, korisnici ne mogu prosuditi hoće li e-usluga biti u stanju sačuvati pohranjene podatke za zakonito traženo razdoblje od npr. 30 godina. Sada tu problematiku (a i druga pitanja oko zaštite podataka) rješava Opća uredba o zaštiti podataka[541], tj. GDPR.

[541] Europski parlament i Vijeće (2016.), 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 te o stavljanju izvan snage direktive 95/46/EZ (Opća uredba o zaštiti podataka) (20.01.2018.)

9.2 HRVATSKA – HALMED - DAIS

Stančić, Herceg i Rajh pišu o HALMED DAIS (hrv. Digitalni Arhivski Informacijski Sustav) sustavu[542]. Agencija za lijekove i medicinske proizvode u Republici Hrvatskoj, HALMED[543] provodi projekte digitalizacije registraturnog i arhivskog gradiva dokumentacije o lijeku od 2013. godine. DAIS je projekt koje je nastao na temelju prijedloga koji je Rajh predložio krajem 2008. u okviru istraživanja u svojem doktoratu „Teorijski model digitalnog arhivskog sustava u domeni regulacije tržišta lijekova“[544]. Navedeni projekt je 2011. dobio financiranje EU te ga je i vodio začetnik same ideje, Rajh, u razdoblju 2013.-2014.[545]

Rajh i Šimundža-Perojević navode podatke[546] o kompatibilnosti DAIS sustava s ISO standardima. Naime, DAIS sustav je u većoj mjeri kompatibilan s ISO standardom za otvorene arhivske informacijske sustave (OAIS) te s PDF/A. Ovaj sustav, navode autori, uz OAIS arhivsku funkciju sustava, dugoročnu pohranu zapisa podupire i procedure konverzije u arhivski PDF format i prijenos metapodataka putem XML formata za razmjenu podataka. U DAIS se od kraja 2014. godine migriraju digitalizirani zapisi. Pri tome se uz svaki dostavljani informacijski paket obavlja prijenos metapodataka iz XML

[542] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)

[543] HALMED, Agencija za lijekove i medicinske proizvode, http://www.halmed.hr/ (24.02.2018.)

[544] Rajh, A. (2010.), Teorijski model digitalnog arhivskog sustava u domeni regulacije tržišta lijekova, doktorska disertacija, Zagreb, Filozofski fakultet, 303 str. Voditelj: Stančić, H., https://www.researchgate.net/publication/310450300_Teorijski_model_digitalnog_arhivskog_sustava_u_domeni_regulacije_trzista_lijekova_Theoretical_Model_of_Digital_Archival_System_in_the_National_Competent_Body_for_Marketing_Authorization_of_Medicines (26.02.2018.)

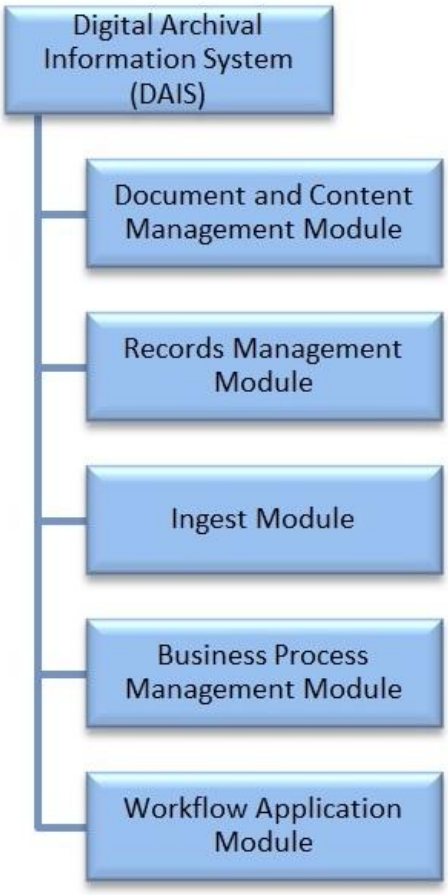
[545] Rajh, A. (2017.), Digital Archives: Towards the Next Step, INFuture 2017: The Future of Information Sciences: Integrating ICT in Society; Atanassova, Iana; Zaghouani, Wajdi; Kragić, Bruno; Kuldar, Aas; Stančić, Hrvoje; Seljan, Sanja (ur.)., Zagreb, Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, 116. (115-120.) , https://www.researchgate.net/publication/320934421_Digital_Archives_Towards_the_Next_Step_INFuture_2017_The_Future_of_Information_Sciences_Integrating_ICT_in_Society_Atanassova_Iana_Zaghouani_Wajdi_Kragic_Bruno_Kuldar_Aas_Stancic_Hrvoje_Seljan_Sanja_u (26.02.2018.)

[546] 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, 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, Topusko, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjA1or9sL_ZAhUBDuwKHRiMDJcQFgguMAE&url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F310453035_Digitalizacija_prihvat_i_migracija_gradiva_u_sustav_upravljanja_zapisima_sa_ciljevima_ostvarivanja_temeljnih_funkcija_HALMED-a_i_ocuvanja_gradiva_Digitisation_ingest_and_migration_of_archival_records_&usg=AOvVaw178pndAHhSZ8dNVMffRT91 (24.02.2018.)

dokumenta koji dolazi uz dostavljeni paket. Rajh i Šimundža-Perojević navode[547] i informaciju da je od 2015. godine HALMED krenuo s digitalizacijom i drugih serija dokumentacije (uz dokumentaciju o lijeku), a počelo se raditi i na arhiviranju izvornih elektroničkih zapisa. Osim toga, autori navode da je DAIS realiziran kroz europski IPA 2009 TAIB projekt.

Stančić, Herceg i Rajh navode[548] da se DAIS sustav sastoji od pet modula te da je razvijen na FileNet P8 platformi. Osnovni modul je modul za upravljanje dokumentima i sadržajem (engl. Document and Content Management Module, Content navigator s ROS[549] repozitorijem). Drugi modul je modul za upravljanje zapisima (engl. Records Management Modul) s FPOS[550] repozitorijem arhivskih metapodataka za dokumente koji su proglašeni zapisima. Treći modul je modul prihvata (engl. Ingest Module) i služi za prihvat SIP paketa, tj. digitaliziranih medicinskih proizvoda. Četvrti modul služi upravljanju poslovnim procesima DAIS sustava (engl. Business Process Management Module) koji sadrži modele procesa, povezanu procesnu dokumentaciju i aplikaciju za izvršavanje procesa (engl. Process Designer). Peti modul je aplikacija za upravljanje radnim zadacima (engl. Workflow Application Module). Slika 48 prikazuje arhitekturu HALMED DAIS sustava.

[547] Isto
[548] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)
[549] ROS – engl. **R**ecords-enabled content **O**bject **S**tore
[550] FPOS – engl. File Plan Object Store



Slika 48. Arhitektura HALMED DAIS sustava, preuzeto iz Stančić, H., Herceg, B., Rajh, A. (2014.)[551]

Elektronički dokument se u DAIS sustav pohranjuje na jednom mjestu, ali se može prikazati u brojnim virtualnim direktorijima pomoću metode datoteke (engl. file-in method). Integracija s arhivskim alatom, koji uključuje raspored zadržavanja (eng. retention schedule) po odobrenju Hrvatskog državnog arhiva[552], omogućuje tom alatu kontrolu poslovnih evidencija i objekata u FPOS repozitoriju. Na kraju poslovnog postupka, kada elektronički dokument treba biti arhiviran, proglašava se zapisom i zaštićuje se od izmjena korisnika. Dodatna PDF/A verzija dokumenta se automatski izrađuje nakon toga. Arhivski metapodaci i jedinstveni identifikator bilježe se u arhivskoj aplikaciji. Arhivski metapodaci i metapodaci sustava pohranjeni su u FPOS repozitoriju i prikazani u imeniku (engl. Directory) s istim jedinstvenim identifikatorom kao u arhivskom alatu. Zapisi se mogu preuzeti bilo iz DAIS-a ili iz arhivske aplikacije. Tijekom

[551] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 5 (24.02.2018.)
[552] Hrvatski državni arhiv, http://www.arhiv.hr/ (24.02.2018.)

migracije putem migracijskog modula (koristi se za migraciju složenijih sadržaja iz datotečnog sustava u DAIS) izvršava se provjera SIP provjere valjanosti. Nakon provjere SIP-a započinje postupak deklariranja zapisa. U slučaju digitaliziranih dokumenata stvaranje i prijava (engl. check-in) PDF/A verzije dokumenta izostavljeni su jer su papirni dokumenti već digitalizirani kao PDF/A datoteke. Moguće je i migracija iz DAIS-a s kontekstualnim metapodacima u XML datoteke.

Stančić, Herceg i Rajh navode[553] da HALMED koristi svoj interni elektronički potpis, ali i da i planira provođenje zakonski valjanog elektroničkog potpisa nakon šire implementacije elektroničkog potpisa u Hrvatskoj i među europskim medicinskim agencijama.

Što se tiče HALMED-a, procesi digitalizacije u toj agenciji kontinuirano napreduju. Rajh i Šimundža-Perojević navode sljedeće podatke o projektu digitalizacije[554]. Agencija je 2013. godine otpočela s projektima vanjske digitalizacije, a do danas su odrađena dva ciklusa takvih projekata te je digitalizirano gotovo 18 milijuna stranica. Stvaratelj je 2016. krenuo s internim projektom digitalizacije. Proces se sastoji od pripreme, skeniranja, indeksiranja, prihvata arhivskog paketa digitaliziranog gradiva u DAIS i deklariranja zapisa u bazi podataka Pismohrana. Digitalizirana dokumentacija koristi se radi ubrzanja osnovne djelatnosti agencije, lakše manipulacije gradivom (omogućen je paralelni rad više djelatnika) i dugoročne uštede na pohrani gradiva. Autori su naveli da su paketi usklađeni s OAIS informacijskim modelom, a da je u DAIS migrirano 42.409 komada (registratora, svežnjeva, svezaka). Na dan 26. veljače 2018. u DAIS sustavu je bilo 24,8 milijuna skenova[555].

9.3 NJEMAČKA – ARHIVSKI ZDRAVSTVENI SUSTAV

Wild je opisao primjer njemačke klinike Braunschweig[556] koja je korištenjem PDF/A standarda unaprijedila radne procese te smanjila troškove arhiviranja medicinske

[553] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 7 (24.02.2018.)
[554] Rajh, A., Šimundža-Perojević, Z. (2016.), Projekti digitalizacije dokumentacije o lijekovima u Agenciji za lijekove i medicinske proizvode, Šesti festival hrvatskih digitalizacijskih projekata, Nacionalna i sveučilišna knjižnica u Zagrebu, http://dfest.nsk.hr/2016/wp-content/uploads/2016/04/Rajh_Simundza.pdf (24.02.2018.)
[555] Informacija priopćena iz HALMED ustanove (26.02.2018.)
[556] Wild, B. (2012.), PDF/A in Healthcare, white paper, PDF Association – PDF/A Competence Center,

dokumentacije. Promjene su napravljene uključivanjem medicinskih zapisa u bolnički informacijski sustav klinike. Dodatna unaprjeđenja u sustavu njemačke klinike su napravljene uvođenjem elektroničkog zdravstvenog kartona, elektroničkog potpisa u informacijski sustav. Informacijski sustav je zatim povezan s elektroničkim arhivom. Time su smanjeni troškovi dugotrajnog arhiviranja. Ono što je označeno kao optimizacija jesu i novi načini komunikacije i kolaboracije tijekom bolničkih postupaka. Name, medicinski nalazi uz pripadajuće snimke te ostali podaci se spremaju centralno. Iz centralne lokacije se zatim tim podacima može pristupiti s više lokacija. Ovako nadograđen i optimiziran sustav je omogućio da se velik dio papirnate dokumentacije skenira i arhivira u centralizirani informacijski sustav te arhiv. Wild navodi podatak[557] da je klinika Braunschweig prije izrade ovakvog sustava trošila oko 470.000 eura na arhiviranje. Troškovi su procijenjeni na temelju 3,5 milijuna medicinskih dokumenata koje klinika proizvodi svake godine.

Razdoblje čuvanja medicinskih dokumenata može biti 30 godina ili više. Primjerice, rendegenske snimke ili slike sa CT pretraga se često trebaju čuvati na dugi rok. Kod ovakvih nalaza je bitna i pravna sigurnost pa se za elektroničke verzije nalaza mora biti potpisana kvalificiranim elektroničkih potpisom. Potpisivanjem kvalificiranim elektroničkim potpisom te korištenjem vremenskog žiga osigurava nepobitan dokaz o vremenu izrade.

Wild navodi dva procesa arhiviranje skeniranih dokumenata u klinici Braunschweig[558] (te procesi se u slučaju Braunschweig skladno nadopunjuju):

- Pretvaranje skeniranih slika u PDF/A format u skladu sa industrijskim standardom ISO 19005,
- Elektronički potpisi se ugrađuju u PDF/A, te jamče sigurnost i nepromijenjivost dokumenata u elektroničkoj arhivi.

Jedan od posebno sigurnih i jednostavnih načina je skeniranje i potpisivanje dokumenata u računalnoj obradi (engl. batch) koja se obavlja na poslužitelju.

---

https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiCnczNv77ZAhXD26QKHU7KCZIQFggsMAA&url=https%3A%2F%2Fwww.pdfa.org%2Fwp-content%2Funtil2016_uploads%2F2012%2F05%2FWP-PDFA-in-Healthcare.pdf&usg=AOvVaw0PYq9l9u_u5UJwI9zwCdCW (24.02.2018.)

[557] Isto, str. 12

[558] Isto, str. 12

Prilikom digitaliziranja medicinskih zapisa u PDF/A format, osiguravaju se sljedeće mogućnosti bitne za medicinsku dokumentaciju: skeniranje dokumenata u boji, pretraživanja teksta nakon OCR postupka, pohranjivanje podataka u datoteke relativno male veličinu. Osim toga, omogućuje se i uključivanje elektroničkog potpisa u dokument kao ugrađenog potpisa (engl. embedded signature). PDF/A-1 osigurava osnovne standarde za arhiviranje elektroničkih dokumenata, ali jedino PDF/A-2 i PDF/A-3 formati podržavaju ugrađeni binarni sadržaj i strojno čitljive podatke[559].

9.4 LITVA – EAIS

U Litvi su Zakonom o dokumentima i arhivima[560] osigurane pravne pretpostavke za postupan prijelaz od pisanih prema elektroničkim dokumentima. Glavni ciljevi navedenog zakona koji se odnose na upravljanje elektroničkim dokumentima su bili: osigurati trajan i dugoročan arhiv (26 do 100 godina), očuvanje elektroničkih dokumenata, pristup elektroničkim dokumentima, određivanje redoslijeda prijenosa u državne arhive te definiranje legitimne upotrebe Elektroničkog arhivskog informacijskog sustava, EAIS[561] (lit. Elektroninio archyvo informacinė sistema). Zakon također određuje i pojam elektroničkog dokumenta u Litvi. Stvaranje EAIS sustava je pokrenuto krajem 2011. godine. EAIS omogućava spremanje u državne arhive službenih elektroničkih dokumenata potpisanih kvalificiranim elektroničkim potpisom. Prilikom pohrane se osigurava sljedeće za pohranjene dokumente: integritet, autentičnost, neporecivost i sposobnost korištenja i pohrane u dugom roku. EAIS sustav pohranjuje i elektronički potpisane dokumente. Struktura takvih dokumenata je temeljena na XML jeziku, a potpis se izvodi pomoću XAdES potpisnog formata. Kod primjene XAdES potpisnog formata je moguće imati u istom dokumentu više potpisanih podatkovnih objekata, te više elektroničkih potpisa. Zasebno mogu biti potpisani i metapodaci (kao podstablo unutar XML datoteke metapodataka). Ovdje je bitno napomenuti da su metapodaci integralni dio elektroničkog dokumenta.

---

[559] Isto, str. 7

[560] Litvanski parlament, Seima (1995.), Law on Documents and Archives, Seimas of the Republic of Lithuania, (zadnji amadmani su iz 2008.), http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=404607 (23.02.2018.)

[561] Elektroninio archyvo informacinė sistema, Electronic Archive Information System, http://eais-pub.archyvai.lt/eais (23.02.2018.)

Usko vezano uz sustav EIAS je implementirano i rješenje za probleme interoperabilnosti u litvanskoj elektroničkoj javnoj upravi i to primjenom dviju specifikacija za složene elektroničke dokumente: ADOC i MDOC koji su već spomenuti u poglavlju 8.1 Interoperabilnost elektroničkih dokumenata. ADOC je specifikacija za opisivanje i postupanje s dokumentima čitljivim ljudima, MDOC je specifikacija za opisivanje i postupanje s dokumentima koji su strojno čitljivi.

EAIS arhitektura se sastoji od tri glavna dijela[562]:

- Javnog portala[563] koji poslužuje sve vanjske korisnike,
- Internog portala[564] koji poslužuje korisnike državnih arhiva,
- Arhiva elektroničkih dokumenata.

Dijelovi EAIS arhitekture pokriveni javnim i internim portalom se sastoje od sljedećih podsustava[565]:

- Prihvata elektroničkih dokumenata – ovaj modul osigurava funkcionalnosti prijenosa dokumenata u državne arhive u zakonski propisanom vremenu, prijenos paketa dokumenata kroz kompjutorsku mrežu ili učitavanje s fizičkog medija. Nadalje, ovaj modul provjerava integritet elektroničkih dokumenata, autentičnost i sukladnost specifikacijama. Sve navedeno se obavlja u svrhu pripremanja elektroničkih dokumenata za dugotrajnu pohranu. Zadnja funkcionalnost ovog modula je pohranjivanje dokumenata,
- Čuvanje elektroničkih dokumenata,
- Objava i prezentacija elektroničkih dokumenata,
- Administracija,
- Organizacija upravljanja dokumentima (eng. Organization of documet management),
- Besplatni alati za sljedeće funkcionalnosti: pripremu, potpisivanje, pregledavanje i verifikaciju službenih elektroničkih dokumenata,
- Elektronički servisi.

[562] Ragaisis, S., Birstunas, A., Mitasiunas, A., Stockus, A. (2012.), Electronic Archive Information System, Vilnius University, Lithuania; http://ceur-ws.org/Vol-924/paper11.pdf , str. 111 (107.-114.) (23.02.2018.)
[563] EAIS javni portal, https://eais-pub.archyvai.lt/eais/ (23.02.2018.)
[564] EAIS interni portal, https://eais-int.archyvai.lt/ (23.02.2018.)
[565] Ragaisis, S., Birstunas, A., Mitasiunas, A., Stockus, A. (2012.), Electronic Archive Information System, Vilnius University, Lithuania; http://ceur-ws.org/Vol-924/paper11.pdf , str. 111 (107.-114.) (23.02.2018.)

Mogućnost dugoročnog korištenja elektroničkih dokumenata[566] je osigurano konvertiranjem sadržaja tih dokumenata u formate namijenjene dugotrajnoj pohrani podataka – PDF/A formatima. Osim toga, elektronički dokumenti su konvertirani i u formate namijenjene pregledavanju na internetu – PNG i JPEG. U Litvanskoj elektroničkoj javnoj upravi se koriste elektronički potpisi prema XAdES-A formatu iz razloga što njihova pravna snaga treba biti dugoročno sačuvana.

Modul čuvanja elektroničkih dokumenata uključuje sredstva za fizičko očuvanje elektroničkih dokumenata: backup kopije, spremanje originalnih paketa elektroničkog dokumenta u WORM uređaje (piši jedanput – čitaj više puta, eng. **W**rite **O**nce, **R**ead **M**any), te sredstva za upravljanje rizicima.

EAIS sustav je fizički smješten na dvije geografski udaljene lokacije[567] (jedna je u Vilniusu, a druga u Šiauliai). Sustav je implementiran tako da se obavlja replikacija arhivskih podataka između glavnog i rezervnog podatkovnog centra s mogućnošću za operacijom prebacivanja jednog na drugi u slučaju grešaka ili nesreće. Zbog sigurnosnih razloga pristup skladišnom prostoru je moguć samo preko internog portala.

Uspjehu EAIS sustava u primjeni litvanske elektroničke javne uprave je pridonijelo i to što su javno dostupan besplatni softverski alati (prilagođeni propisanim specifikacijama) za pripremu, potpisivanje, pregledavanje i verifikaciju službenih elektroničkih dokumenata. Navedeni alati su dostupni kroz web sučelja ili kao desktop aplikacije.

Autentikacija vanjskih korisnika na EAIS je implementirana kroz litvanski gateway elektroničke javne uprave. Autentikacijski servis[568] je osiguran za korisnike Internet bankarstava svih banaka koje djeluju u Litvi i vlasnika osobnih digitalnih certifikata. Određene EAIS funkcije su omogućene i za neautentificirane korisnike.

[566] Ragaisis, S., Birstunas, A., Mitasiunas, A., Stockus, A. (2012.), Electronic Archive Information System, Vilnius University, Lithuania; http://ceur-ws.org/Vol-924/paper11.pdf , str. 112 (107.-114.) (23.02.2018.)
[567] Electronic Archive Information System, Office of the Chief Archivist of Lithuania, http://www.archyvai.lt/en/new/system.html (23.02.2018.)
[568] Lukšaitė, D. (2012.), The life cycle of e-documents: methodological and legal approach in Lithuania, Nordic Baltic Seminar "Practical Aspects of E-Signature and E-Documents Use in the Framework of Digital Single Market", http://www.rrt.lt/download/16522/5%20nb8%20archives%20lt-1.pdf (23.02.2018.)

Ipak, EAIS identificira dva tipa rizika[569]:

- Rizik vezan uz formate sadržaja – oni mogu tijekom vremena zastarjeti, te neće više biti podržani od aktualnih verzija softvera. Ovaj rizik se riješava konvertiranjem cijelog sadržaja u PDF/A format.
- Rizik vezan uz elektronički potpis – kriptografski algoritam koji je korišten za kreiranje elektroničkog potpisa danas može biti siguran, ali u budućnosti može doći do njegovog razbijanja. Ovaj rizik se rješava dodatnom ovjerom vremenskim žigom nad XAdES-A formatom. Prilikom navedene ovjere je potrebno voditi računa o korištenju kriptografskih algoritama primjerene jačine (te dužine ključa koji se koristi).

9.5 KOMPARATIVNA ANALIZA UNUTARNJE STRUKTURE I FUNKCIJA ELEKTRONIČKIH ARHIVA ZA SLOŽENE ELEKTRONIČKE ZAPISE

Vrlo je sa stanovišta ovog rada zanimljiva i komparativna analiza unutarnje strukture i funkcija elektroničkih arhiva za složene elektroničke zapise (engl. Comparative analysis of internal structure and functions of digital archives preserving complex electronic records) koju su napravili Stančić, Herceg i Rajh[570] 2014. godine. Komparativna analiza je uzela u obzir: elektroničke arhivske sustave odgovorne su za očuvanje digitaliziranih ili elektroničkih zapisa u austrijskim zemljišnim knjigama (BAIK), klasificirane zapise o lijekovima i medicinskim proizvodima odobrenim za tržište u Hrvatskoj (HALMED), elektroničke zdravstvene evidencije s vremenskim oznakama (klinika Braunschweig u Njemačkoj), evidencije litvanske javne uprave stvorene kao dio državnih elektroničkih javnih usluga i potpisane kvalificiranim elektroničkim potpisima (EAIS) te na kraju referentni njemački model za dugoročno očuvanje elektronički potpisanih zapisa (BSI).

Hrvatski HALMED, njemačka klinika Braunschweig i litvanski EAIS arhivski sustav su već obrađeni u ovom radu pa će u obrađivanju ove komparativne analize biti spomenuta samo zapažanja iz rada Stančića, Hercega i Rajha. BSI će biti detaljnije razrađen u

[569] Ragaisis, S., Birstunas, A., Mitasiunas, A., Stockus, A. (2012.), Electronic Archive Information System, Vilnius University, Lithuania; http://ceur-ws.org/Vol-924/paper11.pdf , str. 112 (107.-114.) (23.02.2018.)
[570] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)

sljedećem poglavlju, a zapažanja iz spomenute komparativne analize će biti dane skupa s ostalim elektroničkim arhivima.

Austrijska Federalna komora arhitekata i inženjera[571] (BAIK) osnovala je suvremenu arhivu elektroničkih dokumenata za spremanje dokumenata za potrebe zemljišnih knjiga. BAIK omogućuje siguran ulaz i uvid u podatke korisnicima i državnim tijelima (sudovima), a nudi brz i jeftin elektronički arhiv s pravnom snagom i izvornošću dokumenata sukladno propisima arhiva javnih tijela[572] (njem. Urkundenarchive von Körperschaften öffentlichen Rechts). Unutar BAIK arhiva nalaze se svi javni elektronički dokumenti namijenjen zbirci isprava zemljišnih knjiga (katastar, čestice, planovi, procjene vrijednosti). Autentičnost i uvid u arhivske građe omogućena je korištenjem elektroničkog potpisa i dokumentacije u formatu PDF/A1-b, a kao format elektroničkog potpisa uzima se isključivo XMLDSig.

Komponente BAIK arhiva su:

- Spremište za potvrde (njem. Urkundencontainer) - omogućuje pohranu i uvid dokumenata te izdavanje različitih potvrda elektroničkim putem klijentima za ostvarivanje određenih prava i uvida u zemljišnim knjigama. Koristi se elektronički potpis, a dokumenti moraju biti pohranjeni u formatu PDF/A-1b,
- Spremište za mišljenja (njem. Gutachtencontainer) - Unutar ovog spremišta pohranjuju se dokumenti (uz suglasnost klijenta) pri čemu građevinar ili klijent može dati elektronički pristup vlastitim dokumentima inženjerima. Ovi dokumenti mogu biti u bilo kojem formatu. Mišljenje koje inženjer izdaje mora biti u formatu PDF/A1-b uz uporabu elektroničkog potpisa,
- Sigurnosno spremište (njem. Sicherungscontainer) - Služi kao dio za izradu sigurnosnih kopija, odnosno kao privatni arhiv inženjera. Ovdje se pohranjuju dokumenti i podaci u različiti formatima, kako bi se osigurala njihova sigurna pohrana u različitim formatima.

Promatrana komparativna analiza temelji se na kriterijima grupiranim oko funkcionalnosti, implementiranih standarda, formata te dostupnih softverskih alata za

[571] BAIK, https://www.baik-archiv.at/urka/ (25.02.2018.)
[572] Jusline, § 91c GOG Urkundenarchive von Körperschaften öffentlichen Rechts, https://www.jusline.at/gesetz/gog/paragraf/91c (25.02.2018.)

upravljanje sačuvanim zapisima. U tablici 14 je dan prikaz komparativne analize za promatrane sustave po različitim promatranim kategorijama.

Tablica 14. Komparativna analiza unutarnje strukture i funkcija elektroničkih arhiva za složene elektroničke zapise, preuzeto iz Stančić, H., Herceg, B., Rajh, A. (2014.) [573]

Sustav	Funkcionalnosti Arhiviranja elektroničkih zapisa	Funkcionalnosti Arhiviranja elektroničkih potpisanih zapisa	Potporni moduli	Implementirani standardi	Implementirani Standardi za elektronički potpis
BAIK	DA	DA	Kontejner za dokumente, Backup kontejner	PDF A-1b	XMLDsig s implementacijom digitalnih certifikata
HALMED (DAIS)	DA	Djelomično, zapisi potpisani samo s internim potpisom	FileNet ECM s migracijskim modulom, Enterprise Record modul, backup	OAIS RM, PDF/A-1 i 2, XML	Integracija modula za interni elektronički potpis s DAIS sustavom
Klinika Braunschweig	DA	DA	OCR, klasifikacija i eksport podataka	PDF/A	Vremenski žig
EAIS	DA	DA	Modul zadržavanja, modul organizacije dokumenata	PDF/A, XML, PNG, JPEG	XAdES
BSI	DA	DA	ECM s	BSI	XMLDSig,

[573] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 14 (24.02.2018.)

			ArchiSafe, ArchiSig i kriptomoduli -ma	Tehničke smjernice 03125, MoReq2, OAIS, XAIP, PDF/A, XML	XAdES, CAdES, kvalificirani vremenski žig

Stančić, Herceg i Rajh daju zaključak[574] da je ova komparativna analize pokazala da je kod svih istraženih elektroničkih arhiva naglašen isti osnovni problem - očuvanje autentičnog sadržaja u nekom obliku. U slučaju kada je taj sadržaj pohranjen u oblik zapisa onda se njegovo očuvanje i očuvanje metapodataka može olakšati koristeći standardizirane formate datoteka kao što je PDF/A. Za PDF/A format datoteke i XML format za metapodatke autori navode da su široko priznata rješenja koja su preferirana od svih elektroničkih arhiva koji se ovdje razmatraju unutar ove analize. Autori idu i korak dalje i predlažu razvijanje sustava koji koristi OAIS informacijske pakete (SIP, AIP i DIP) uz korištenje dva već navedena standarda (PDF/A i XML). Bez obzira jesu li zapisi arhivirani u PDF/A formatu elektronički potpisani ili ne, možemo zaključiti da su analizirane institucije prepoznale otvorene standarde u implementaciji svojih elektroničkih arhivskih sustava. Stančić, Herceg i Rajh na kraju komparativne analize zaključuju[575] da proces dugoročnog očuvanja složenih elektroničkih zapisa ostaje tehnički i organizacijski izazov, ali i da bi oslanjanje na otvorene standarde, umjesto vlasničkih, moglo donijeti stabilnost u tom procesu.

9.6 E-ARK PROJEKT

E-ARK projekt[576] (hrv. Europski arhivski zapisi i očuvanje znanja, engl. European Archival Records and Knowledge Preservation) je istraživački projekt financiran od Europske Unije koji je trajao tri godine (2014.-2017.). Cilj ovog projekta je bio pilotirati postojeće arhivske servise koji zadržavaju autentičnost i čitljivost na postojećim najboljim praksama. Adresirana su sljedeća tri svojstva arhiviranja koja su se kroz projekt nastojala

[574] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 14 (24.02.2018.)
[575] Isto, str. 15
[576] E-ARK, European Archival Records and Knowledge Preservation, http://www.eark-project.com/ (06.03.2018.)

proučiti: učitavanje digitalnog sadržaja (engl. acquiring), očuvanje (engl. preserving) i omogućavanja ponovnog korištenja podataka (engl. enabling re-use of information). Projekt je imao za cilj i demonstrirati potencijalne prednosti za javnu upravu, javne agencije, javne servise, građane i poslovne subjekte omogućavajući lak i efikasan pristup arhiviranim zapisima. Koordinator E-ARK projekta je bilo Sveučilište u Brightonu (Ujedinjeno Kraljevstvo). Sudionici projekta su bile nacionalni arhivi, javne uprave, javne institucije, znanstvene ustanove i pružatelje usluga arhiviranja iz sljedećih zemalja Uuropske Unije: Austrije, Njemačke, Danske, Estonije, Španjolske, Madžarske, Norveške, Portugala, Švedske, Slovenije i Ujedinjenog Kraljevstva. E-ARK je kroz projekt nastojao harmonizirati arhivski proces na paneuropskoj razini te pružiti priručnike i preporuke za dugotrajno čuvanje digitalnih zapisa.

E-ARK projekt je istraživao sljedeće arhivske sustave i referentne modele:

- US Patent 13/219,630 Method And System For Preparing Digital Information For Long-Term Preservation[577]
- BSI TR Model 03125 (bit će detaljno obrađen i u ovom radu),
- Archivematica[578] – besplatan i open-source sustav za dugotrajno očuvanje digitalnog sadržaja,
- Riksarkivet[579] (Norveška),
- Preservica[580] - pružatelj usluga arhiviranja,
- i dr.

E-ARK projekt je kao jednu od svojih projektnih isporuka u veljači 2017. godine isporučio „Zajedničku specifikaciju za informacijske pakete“[581] (engl. Common specification for information packages). Zajednička specifikacija za informacijske pakete (u nastavku E-ARK Specifikacija) definira zahtjeve koje treba ispuniti za osiguravanje interoperabilnosti informacijskog paketa. E-ARK Specifikacija predlaže i detalje XML temeljene implementacije traženih zahtjeva za očuvanje digitalnog sadržaja. E-ARK Specifikacija polazi od OAIS referentnog modela i OAIS informacijskih paketa: SIP, AIP i DIP. E-ARK

[577] Gladney, H. (2011.), US Patent, US Patent 13/219,630 Method And System For Preparing Digital Information For Long-Term Preservation, https://patents.google.com/patent/US20130054607 (06.03.2018.)
[578] Archivematica, https://www.archivematica.org/en/ (06.03.2018.)
[579] ESSArch, http://www.essarch.org/ (06.03.2018.)
[580] Preservica, https://preservica.com/ (06.03.2018.)
[581] DLM Archival Standards Board (2017.), Common Specification for Information Packages v1.0, http://www.dasboard.eu/images/Specifications/CS/Common_Specifications_for_IPs_v10.pdf (06.03.2018.)

projekt ih imenuje: E-ARK SIP[582], E-ARK DIP[583] i E-ARK AIP[584]. Svaki od pripadnih informacijskih paketa ima svoju specifikaciju.

E-ARK specifikacija navodi da postoji sedam različitih specifikacija koje definiraju različite vrste sadržaja (engl. Content Information Type)[585]:

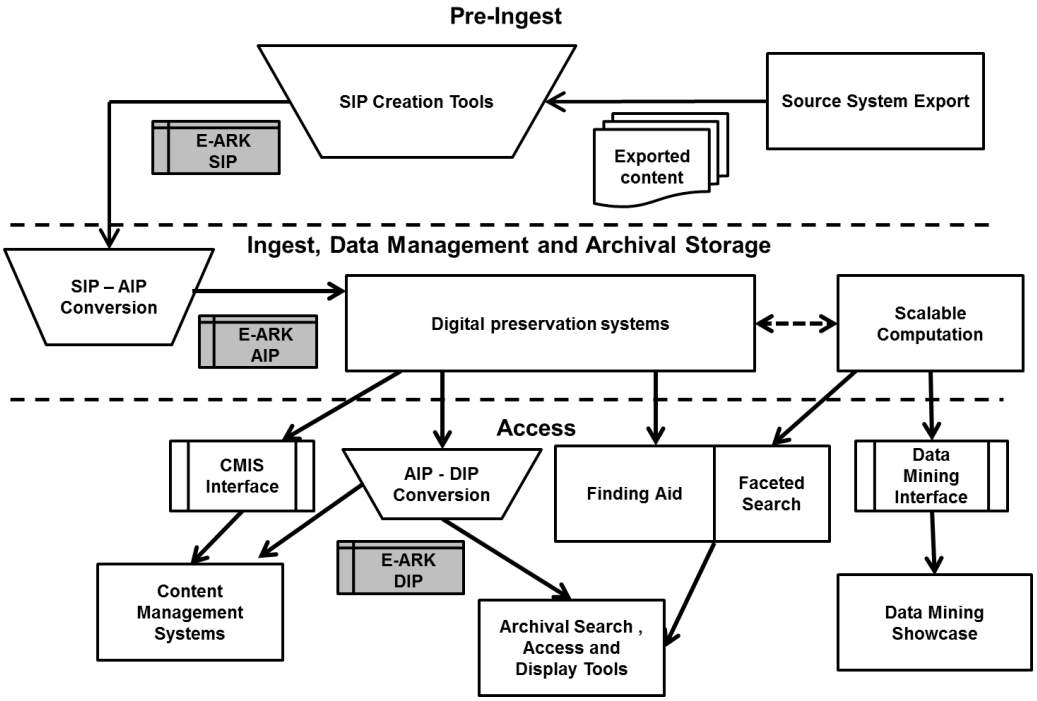
- SMURF SFSB –formati zapisa za jednostavne File-System temeljene zapise,
- SMURF ERMS – formati zapisa za ERM sustave,
- GeoVectorGML, GeoRasterGeoTIFF – formati zapisa za spremanje geoprostornih informacija,
- SIARD1, SIARD2 i SIARDDK – opisuje se korištenje opće specifikacije za arhiviranje, očuvanje i ponovno korištenje relacijskih baza podataka.

Provedba E-ARK Specifikacije se sastoji od dva osnovna elementa: fiksne fizičke strukture informacijskog paketa i točne uporabe metapodataka u METS i PREMIS formatima[586].

Svrha METS odjeljka s opisnim podacima jest ugraditi ili uputiti na datoteke koje sadrže opisne metapodatke. E-ARK specifikacija preporučuje i zagovara upotrebu standarda PREMIS metapodataka za snimanje metapodataka za očuvanje i tehničkih metapodataka o digitalnim objektima. Opisi događaja trebaju biti uključeni u PREMIS metapodatke što je više moguće. Detaljne informacije o pravima trebaju biti isključivo uključene u PREMIS.

Na slici 49 je dana E-ARK arhitektura koju je projekt isporučio kao jednu od isporuka. Iz slike arhitekture je vidljivo da je E-ARK preuzeo OAIS funkcionalne entitete, a da je za informacijske pakete (AIP, SIP i DIP) dodan prefiks E-ARK

[582] E-ARK SIP, http://www.dasboard.eu/images/Specifications/SIP/General_SIP-Specification_v1.4.pdf (06.03.2018.)
[583] E_ARK DIP, http://www.dasboard.eu/images/Specifications/DIP/DIP_10_v2.pdf (06.03.2018.)
[584] E-ARK AIP, http://www.dasboard.eu/images/Specifications/AIP/DASBOARD_E-ARK_AIP_1_0.pdf (06.03.2018.)
[585] Common Specification for Information Packages v1.0, DLM Archival Standards Board, 2017., http://www.dasboard.eu/images/Specifications/CS/Common_Specifications_for_IPs_v10.pdf (06.03.2018.)
[585] E-ARK SIP, http://www.dasboard.eu/images/Specifications/SIP/General_SIP-Specification_v1.4.pdf, str. 9. (06.03.2018.)
[586] DLM Archival Standards Board (2017.), Common Specification for Information Packages v1.0, http://www.dasboard.eu/images/Specifications/CS/Common_Specifications_for_IPs_v10.pdf, str. 9 (06.03.2018.)
[586] E-ARK SIP, http://www.dasboard.eu/images/Specifications/SIP/General_SIP-Specification_v1.4.pdf, str. 24. (06.03.2018.)



Slika 49. E-ARK arhitektura, preuzeto s www.eark-project.com [587]

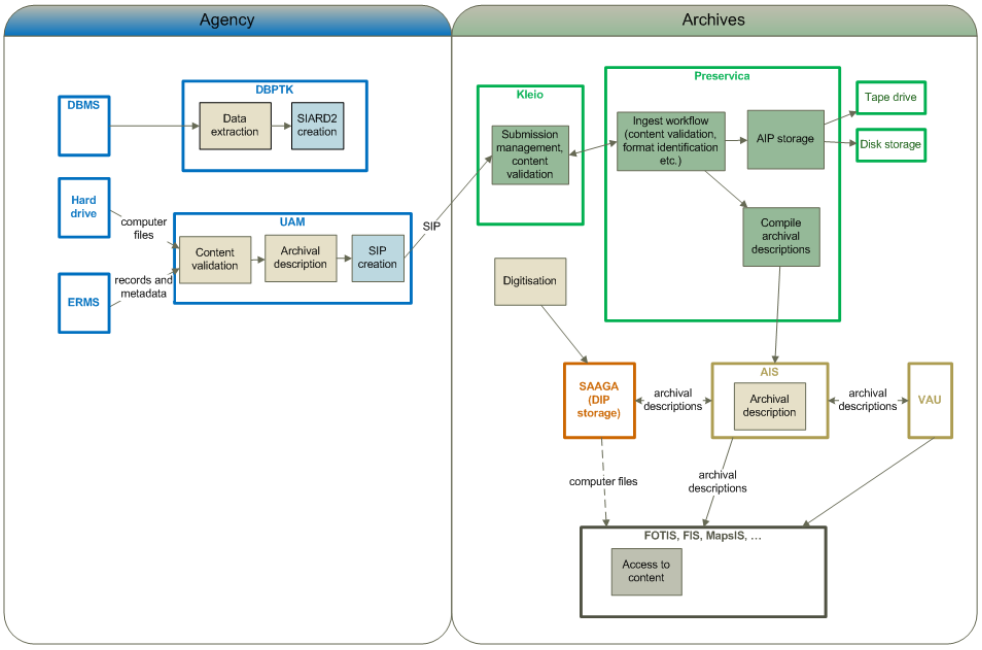
9.7 ESTONIJA – ELEKTRONIČKI ARHIVI NACIONALNOG ARHIVA

Elektronički arhiv Nacionalnog arhiva Estonije[588] (engl. Digital Archives of the National Archives of Estonia) sam kontaktirao preko upitnika koji je naveden u Prilogu 2. U nastavku teksta će biti analizirani vraćeni odgovori iz Elektroničkog arhiva Nacionalnog arhiva Estonije (u nastavku teksta Elektronički arhiv) na poslani upitnik[589].

Pripremne aktivnosti započele su 2006. godine pripremanjem konceptualnih i funkcionalnih načela i definicija tijeka rada (engl. workflows). Navedene aktivnosti su trajale do 2008. godine. U naredne četiri godine (2009.-2012.) izgrađeni su moduli Predprihvata (engl. pre-ingest), Prihvata (engl. ingest), Arhivska pohrana (engl. Storage), Aktivnog očuvanja (engl. Active preservation) i Upravljanja podacima (engl. Data management). Istodobno su razvijeni brojni pristupni sustavi: prva verzija digitalnog kataloga bila je dostupna 1999. godine, 2004. godine objavljeno je web sučelje za katalog,

[587] E-ARK arhitektura, http://www.eark-project.com/resources/architecture (06.03.2018.)
[588] Digital archives, Rahvusarhiiv, http://www.ra.ee/en/information-management/digital-archives/ (16.03.2018.)
[589] Odgovori iz Digitalnog arhiva Nacionalnog arhiva Estonije su pristigli 13. ožujka 2018. Na pitanja je odgovorio gospodin Kuldar Aas.

od 2005. godine razvijeno je oko 20 specifičnih komponenti pristupa (engl. Access) te se razvijaju i nove. Ukupno, cijeli aktualni "elektronički arhivski ekosustav" sastoji se od dva glavna alata za module Predprihvata i Prihvata: Sustav očuvanja (Preservica), središnji katalog i već spomenutih 20 dodatnih pristupnih komponenti. Na slici 50 je dan prikaz generičkog modela arhitekture estonskog Elektroničkog arhiva iz 2017.



Slika 50. Arhitektura estonskog nacionalnog Elektroničkog arhiva[590]

Elektronički arhiv za transferiranje digitalnih zapisa i metapodata u druge arhive koristi estonsku nacionalnu interoperabilnu infrastrukturu X-Road[591], a udomljen je u estonskom Nacionalnom arhivu[592] (est. Rahvusarhiiv). Implementirane su dvije serverske sobe (u Tallinu i Tartuu). Primarna lokacija za digitalnu pohranu (Preservica) je u Tallinu te se u njemu drži online kopija (disk) i jedan kopija na traci. Sekundarna lokacija je Tartu gdje se također drže jedna online kopija i jedna kopija na traci. Sveukupno estonski elektronički arhivi imaju četiri kopije na dvije lokacije.

Sljedeće su korisničke uloge u sustavu:

[590] Arhitektura estonskog Digitalnog arhiva, slika je dobivena putem Upitnika za digitalne arhive iz Priloga 2 (16.03.2018.)
[591] X-Road, https://e-estonia.com/solutions/interoperability-services/x-road/ (16.03.2018.)
[592] Rahvusarhiiv, http://www.ra.ee/en (16.03.2018.)

- arhivisti i tehničko osoblje agencija - zaduženi su za pripremu isporuka. Oni preuzimaju i koriste komponente Elektroničkog arhiva,
- arhivisti Elektroničkog arhiva - zaduženi su za provođenje provjere kvalitete prenesenih zapisa. Koriste komponentu Prihvata – Kleio,
- krajnji korisnici - nema potrebe za korištenjem online alata, a većina korisnika (više od 90%) koristi virtualnu čitaonicu (VAU). Pomoću nje mogu pronaći relevantne arhivske zapisa (uglavnom iz AIS, FIS, FOTIS). Nadalje, mogu naručiti kopije arhivskih zapisa. Osim toga krajnji korisnici mogu naručiti te zapise unaprijed u čitaonici gledati online digitalne zapise (Saaga, FIS, FOTIS, baza podataka geografskih karata itd.).

Kleio komponentu koriste dvije role korisnika: arhivist i administratori. Preservica komponentu koriste standardne korisničke uloge (krajnji korisnik, administrator, anonimni korisnik, upravljanje podacima, prihvat, manager, administrator registra, podnositelj sadržaja, transformacija). Arhivisti se prijavljuju u interne sustave Elektroničkog arhiva koristeći kombinaciju korisničkog imena i lozinke. Pristupni sustavi (VAU) nude razne mogućnosti za: korisničko ime i lozinku, LinkedIn, Twitter, Facebook, Google račune, nacionalnu e-osobnu iskaznicu[593] ili nacionalni mobilni ID.

Elektronički arhiv prihvaća elektronički potpisane zapise. Jedna kopiju zapisa ostaje "kakva jest" (engl. „as is“), tj. u potpisanom formatu, a druga kopija je tretirana kao otvorena datoteka (podaci potpisa premješteni u zapis metapodataka, a sam zapis je preseljen u arhivski format - uglavnom PDF). Od formata naprednog elektroničkog potpisa koristi se XAdES. Politika koja propisuje korištenje takvog potpisa[594] se odnosi, što je vrlo zanimljivo, na Latviju i Estoniju. Svi zapisi koji su u pohrani (bez obzira jesu li elektronički potpisani ili ne) pokriveni su sigurnosnim mehanizmima na cijelom sustavu. Trenutačno postoje jednostavne provjere integriteta sustava te dva različita hasheva za svaku datoteku (uključujući datoteke metapodataka). U tijeku je provedba rješenja GuardTime KSI za tu svrhu. Zasada se ne koristi ovjeravanje vremenskim žigom za očuvanje elektronički potpisanih zapisa. Sve operacije u sustavu jednostavno se bilježe s datumom i vremenom sustava. Nakon što se implementira GuardTime KSI rješenje

[593] Estonska e-ID kartica, https://www.id.ee/?lang=en (16.03.2018.)
[594] Sertifitseerimiskeskus AS (2016.), ASiC-E/XAdES Signature Policy in Latvia and Estonia–Draft, https://www.ria.ee/public/PKI/LV-EE-Signature-Policy_Draft_EE_TC.pdf (16.03.2018.)

implementirat će se korištenje vremenskog žiga za navedenu svrhu. Trenutačni oblik elektroničkog potpisa u Estoniji naziva se BDOC[595]. To nije puna XAdES LTV implementacija kao što je opisano u službenim standardima, ali bitno je da su svi relevantni podaci potrebni za izvanmrežnu (engl. offline) i validaciju potpisa i validaciju u dugom roku uključeni u potpis.

Elektronički arhiv je i propisao popis formata[596] (TXT, PDF, XML, TIFF, PNG, WAV, MPEG-2,..).

Elektronički arhiv, tj. komponenta Preservica je sukladna s OAIS (ISO 14721:2003) standardom.

Elektronički arhiv je implementirao E-ARK SIP specifikaciju u alatima za predprihvat i prihva te u radnim procesima. Koristi se alat RODA-in u odgovarajućim scenarijima za izradu SIP paketa. Koristi se SIARD2 format za arhiviranje baze podataka te odgovarajuće alate (DBPTK, DBVTK). E-ARK projekt je u ovom radu opisan u poglavlju 9.6 E-ARK projekt.

UAM (engl. Universal Archiving Module) alati za predprihvat (za agencije za pripremu transfera): omogućuje stvaranje metapodataka i stvaranje SIP paketa za zapise i metapodatke iz ERMS-a, sustava za upravljanje elektroničkim zapisima (engl. Electronic Record Management System). Alat je razvijen od strane djelatnika Elektroničkog arhiva, ali je slobodno dostupan na internetu[597]. Lukičić i Sruk napominju da postoji ISO standard koji je postao najvažnije uporište kada se razmatra definicija ERM sustava[598], a to je ISO 15489-1: 2001[599] standard. Osim toga isti autori navode[600] da je MoReq2 specifikacija

[595] BDOC, https://www.id.ee/public/bdoc-spec212-eng.pdf (16.03.2018.)
[596] Arhiivivormingud, https://www.riigiteataja.ee/aktilisa/1291/2201/1229/VV181_lisa1.pdf (16.03.2018.)
[597] UAM, Universal Archiving Module, http://www.ra.ee/en/information-management/universal-archiving-module/ (16.03.2018.)
[598] Lukičić, M., Sruk, V. (2009.), Electronic Records Management System Requirements, INFuture2009: "Digital Resources and Knowledge Sharing", Zagreb, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjHl8GW4fHZAhWPKCwKHd2CAPwQFgg0MAI&url=https%3A%2F%2Finfoz.ffzg.hr%2Finfuture%2F2009%2Fpapers%2F2-02%2520Lukicic%2C%2520Sruk%2C%2520ERMS%2520requirements.pdf&usg=AOvVaw1HDduFU1CF7-Z_GGgyF9Ck , str. 67 (16.03.2018.)
[599] ISO (2011., 2.), ISO 15489: Information and documentation – Records management, International Organization for Standardization, https://www.iso.org/standard/31908.html
[600] Isto, str. 72

zbirka obaveznih i neobveznih funkcionalnih i nefunkcionalnih zahtjeve za ERM sustave. MoReq2 specifikacija je opisana u poglavlju 8.4 Norme za dugoročno očuvanje elektroničkih dokumenata.

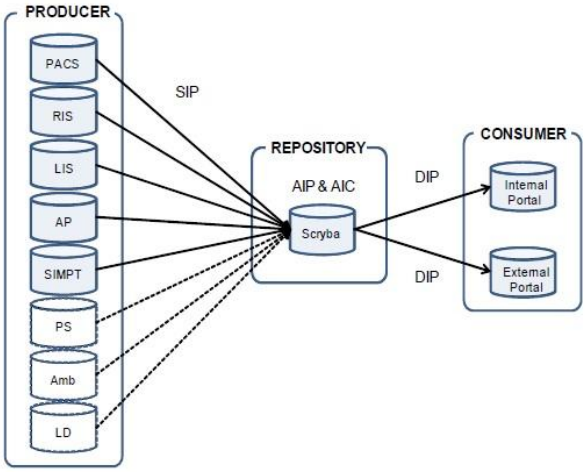
9.8 ITALIJA – VICENZA ZDRAVSTVENI SUSTAV

Salsa i Guerizio pišu[601] o sustavu za dugotrajnu pohranu elektronički potpisanih medicinskih podataka izrađenom za zdravstveni sustav okruga Vicenze (Italija). Zdravstveni sustav se temelji na repozitorij za očuvanju podataka, a njegova posebnost je što je i geografski distribuiran po okrugu. Ovaj sustav usvaja međunarodne standarde, ali i vrlo složeno talijansko zakonodavstvo za područje izrade, spremanja i dugotrajnog čuvanja elektroničkih zapisa. Postoje i dodatna specifična pravila za čuvanje medicinskih zapisa koja se temelje na upotrebi elektroničkog potpisa i certificiranih vremenskih žigova. Implementacija je obavljena uz strogo pridržavanje standardiziranih rješenja temeljenih na XML shemama i definiranom rječniku koji je temeljen na PREMIS-u.

Infrastruktura za dugotrajno očuvanje medicinskih elektroničkih zapisa u okrugu Vicenza je temeljena na sustavu Scryba[602] koji je izradila kompanija MEDAS Srl. Sustav Scryba je temeljen na OAIS referentnom modelu te su implementirane dodatne specijalne funkcionalnosti koje su imale za cilj podrške talijanskom zakonodavstvu za područje dugotrajnog očuvanja elektroničkih zapisa. Scryba je modularni sustav koji se temelji na skupu funkcionalnosti te se može konfigurirati za udovoljavanjem specifičnim zahtjevima koji nastaju u različitim okruženjima. Sustav je implementiran na način da su osnovni elementi nekoliko spremišta za digitalno očuvanje u talijanskim bolnicama.

[601] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=182 , str. 172-179 (06.03.2018.)

[602] Scryba, http://www.medas-solutions.it/products/product-scryba.html (06.03.2018.)



Slika 51. Sustav za dugotrajno očuvanje medicinskih digitalnih zapisa okruga Vicenze, preuzeto iz Salza, S., Guercio, M. (2012)[603]

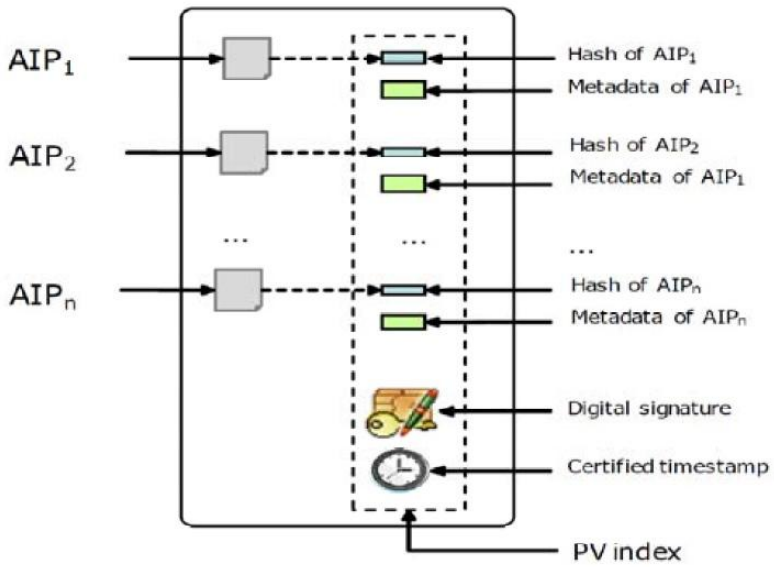
Prema talijanskim propisima svi medicinski zapisi dostavljaju se na dugotrajno očuvanje odmah po njihovoj izradi i potpisivanju. Iz tog razloga se ubrzo nakon izrade i potpisivanja svaki digitalni resurs čuva u dvije različite kopije. Jedna ide u sustav odjela za konzultacije u kratkom razdoblju, a druga u repozitorij za dugotrajno očuvanje, LDTP (engl. Long Term digital Preservation). Korisnici LTDP sustavu mogu pristupiti preko dva sučelja:

- Internog portala – koriste ga liječnici i medicinsko osoblje. Preko ovog sučelja ovlaštene osobe mogu preko interneta dobiti pristup cjelovitim digitalnim sadržajima koji se čuvaju na dugi rok,
- Vanjski portal – preko ovog portala na internetu građani i njihovi ovlaštenici mogu pristupiti vlastitoj medicinskoj dokumentaciji.

Sustav Scryba ima modularnu strukturu čiji su temelj komponente za upravljanje AIP paketima. Bitne su funkcije ovog sustava i agregacija podataka i migracije iz formata. Uz sustav su vezani adapteri koji služe za upravljanje komunikacijom s vanjskim svijetom, tj. s proizvođačima (engl. producers) s jedne strane i potrošačima (engl. consumers) s druge strane. Proces očuvanja temelji se na prikupljanju digitalnih resursa koji će biti sačuvani u velikim serijama pod nazivom Volumen očuvanja, PV (engl. Preservation Volume). PV

[603] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=18 , str. 173 (172-179), slika 2 (06.03.2018.)

sadrži stvarne objekte očuvanja i mora proći dobro definiran formalni postupak koji uključuje elektroničko potpisivanje ovjereno certificiranim vremenskim žigom te periodične kontrole i eventualno stvaranje novih kopija na različitim medijima za pohranu. Talijanski propisi također zahtijevaju izradu određenog broja rezervnih kopija, BC (engl. Backup Copies) za svaki PV te da se pohranjuju u različite lokacijama prema unaprijed definiranoj i formalno navedenoj shemi.



Slika 52. Struktura Volumena očuvanja (PV), preuzeto iz Salza, S., Guercio, M. (2012)[604]

Struktura Volumena očuvanje prikazana na slici 52 sadrži sve agregirane digitalne resurse te dodatnu datoteku koja se naziva Indeks volumena očuvanja (PV indeks). PV indeks je sukladan UNI SInCRO[605] standardu. To je talijanski nacionalni standard za metapodataka. PV indeks je XML datoteka koja sadrži sljedeće podatke:

- hash datoteku za svaki AIP u Volumenu očuvanja,
- skup metapodataka za svaki AIP u Volumenu očuvanja,

[604] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=18 , str. 174 (172-179), slika 3 (06.03.2018.)

[605] UNI - Ente Italioano de normazione, UNI 11386:2010 (2010.), Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO), http://store.uni.com/catalogo/index.php/uni-11386-2010.html?josso_back_to=http://store.uni.com/josso-security-check.php&josso_cmd=login_optional&josso_partnerapp_host=store.uni.com (06.03.2018.)

- elektronički potpis,
- certificirani vremenski žig.

Sukladno OAIS modelu i talijanskom zakonodavstvu, SIP se učitava u sustav odmah po izradi digitalnog sadržaja u medicinskom sustavu, a AIP se generira za svaki SIP. Dakle, svaka medicinska dijagnoza ili izvještaj odmah podliježe procesu očuvanja. S druge strane, skup AIP-ova se od svakog proizvođača digitalnih zapisa periodički prikuplja u AIC (engl. Archival Information Collections). AIC je sukladan Volumenu očuvanja po talijanskim propisima. U Scryba sustavu svaki Volumen očuvanja mora sadržavati digitalni sadržaj samo određenog tipa, a Volumeni očuvanja podliježu sljedećim kriterijima:

- Volumen očuvanja (PV) mora biti zatvoren maksimalno u roku od 24 sata nakon njegovog otvaranja,
- Veličina Volumena očuvanja[606] ne smije premašiti maksimalnu veličinu (trenutno je 1GB).

9.9 NJEMAČKA – BSI REFERENTNI MODEL

Model dugotrajne pohrane elektronički potpisanih dokumenata njemačkog ureda za informacijsku sigurnost, BSI[607] (njem. Bundesamt für Sicherheit in der Informationstechnik) temelji se na međunarodnim standardima. Osim međunarodnih standarda, temelj ovog modela je i njemački zakon o arhiviranju, BarchG[608] (njem. Bundesarchivgesetz). Ovaj zakon pokriva područje arhiviranja dokumenata vladinih tijela. BSI je objavio Tehnički priručnik 03125[609] (njem. BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente; engl. BSI Technical Guideline 03125, Preservation

[606] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=18 , str. 174 (172-179) (06.03.2018.)

[607] BSI, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Home/home_node.html (05.03.2018.)

[608] Bundesarchivgesetz, BarchG, (2017.), https://www.bundesarchiv.de/DE/Content/Downloads/Rechtliches/bundesarchivgesetz.pdf?__blob=publicationFile (05.03.2018.)

[609] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile (05.03.2018)

of Evidence of Cryptographically Signed Documents), u daljem tekstu Tehnički priručnik 03125. Tehnički priručnik 03125 detaljno opisuje referentnu arhitekturu sustava za dugotrajnu pohranu elektronički potpisanih dokumenata te se navode zahtjevi po svakoj komponenti arhitekture.

Kao ciljevi i izazovi referentne arhitekture za dugotrajnu pohranu elektronički potpisanih dokumenata je navedeno[610] da treba osigurati sljedeće zahtjeve za dugotrajnu pohranu digitalnih sadržaja i meta podataka:

- Dostupnost i čitljivost (eng. availability and readability),
- Cjelovitost (eng. integrity),
- Autentičnost (eng. authenticity),
- Zaštita podataka, sigurnost podataka i povjerljivost (eng. data protection, data security, and confidentiality).

Referentna arhitektura navedena u ovom priručniku pokriva sljedeće funkcionalnosti: kreiranje, pohranu, indeksiranje, pretraživanje, administraciju, čitanje elektronički potpisanih dokumenata.

BSI referentna arhitektura se sastoji od dva glavna dijela:

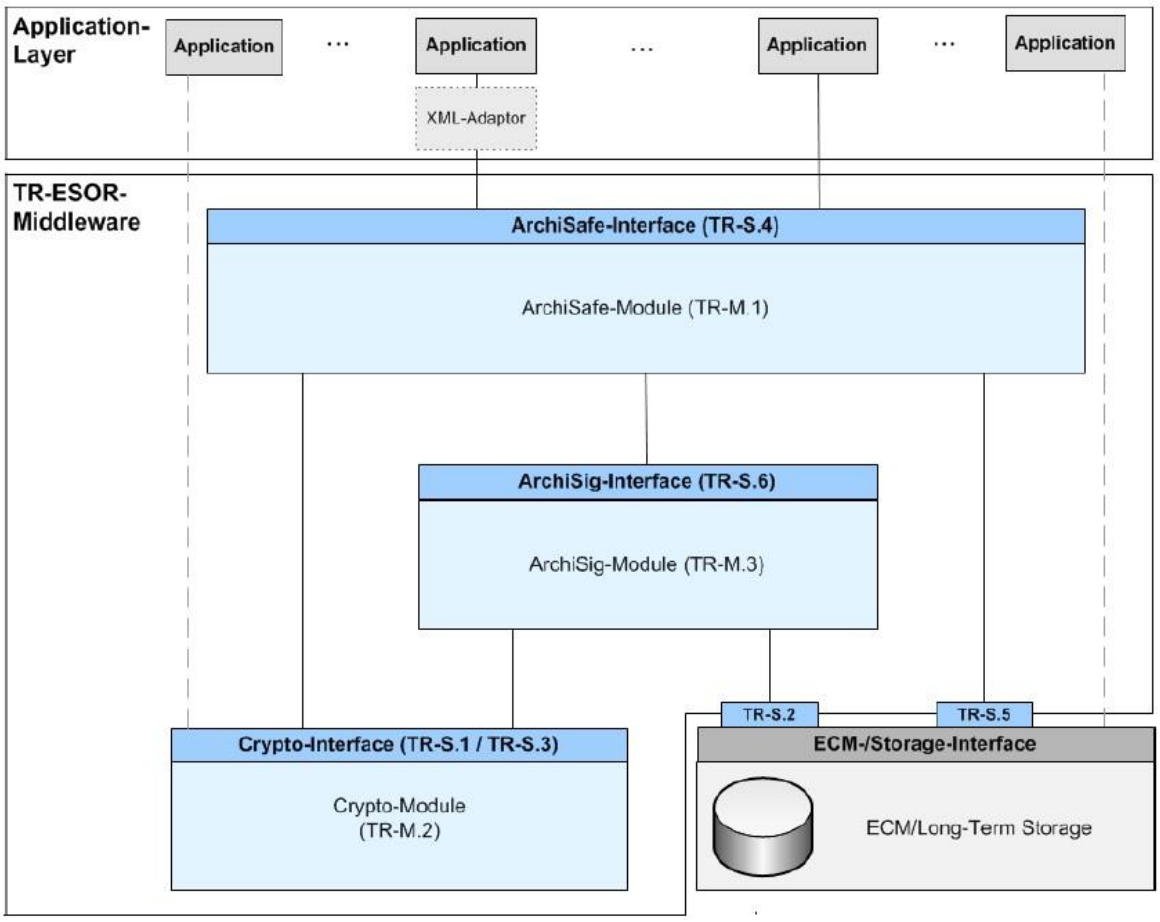
- IT infrastrukture namijenjene za arhiviranje, tj. dugotrajnu pohranu (eng. long term storage),
- IT aplikacija koje arhiviraju podatke i dokumente ili rade s arhiviranim podacima i dokumentima (engl. Application-Layer).

IT infrastruktura namijenjena za pohranu se sastoji od[611]:

- ECM (engl. Enterprise Content Management) sustava za dugotrajnu koji uključuje i upravlja različitim medijima za pohranu te jamči pouzdan i siguran pristup mediju za pohranu prilikom spremanja, dohvata i brisanja arhiviranih dokumenata i podataka,
- Međusloja (engl. Middleware) - uključuje kriptografske komponente koje podržavaju očuvanje dokumenata sukladno propisanim zakonskim aktima. Ovaj međusloj se navodi kao TR-ESOR Međusloj ili jednostavno kao Međusloj.

[610] Isto, str. 14
[611] Isto, str. 15

U nastavku je dana slika 53 koja prikazuje referentnu arhitekturu iz Tehničkog priručnika 03125:



Slika 53. BSI referentna arhitektura za dugotrajnu pohranu elektronički potpisanih dokumenata, preuzeto iz BSI (2014.)[612]

U nastavku slijedi kratak opis komponenti BSI referentne arhitekture.

Aplikacijski sloj[613] (engl. Application Layer)

Aplikacije i servisi iz ovog sloja trebaju zadovoljiti sljedeće zahtjeve:

- Stvaranje dokumenata koji su namijenjeni arhiviranju na način sukladan standardiziranim podatkovnim formatima koji su preporučeni za dugotrajnu pohranu (npr. PDF ili XML),
- U ovom sloju je potrebno osigurati XML adaptere i konvertere za formate podataka koji su specifični za aplikaciju koja je stvorila standardizirani XML format

[612] Isto, str. 26, slika 3
[613] Isto, str. 37-40

podataka za pohranu. To također može uključivati pretvorbu vlasničkih formata podataka u otvorene formate podataka (npr. PDF/A). Pohranjivanje otvorenih formata podataka za razliku od vlasničkih (engl. propriaty) proizvoda dugoročno ima prednost jer će ih biti moguće čitati i kasnije. Za vlasničke formate podataka postoji rizik da ih je moguće čitati u svakom slučaju. Inače, za vlasničke formate podataka postoji rizik da se neće moći pročitati u budućnosti ili se neće moći obaviti konverzija podataka.

- Osiguravanje funkcionalnosti verifikacije elektroničkog potpisa,
- Za prikazivanje dokumenata i podataka potpisanih naprednim elektroničkim potpisom, aplikacija treba imati vjerodostojnu komponentu za prikaz naprednog elektroničkog potpisa (engl. Trusted viewer),
- Osiguravanje sučelja i funkcionalnosti za arhiviranje dokumenata,
- Osiguravanje sučelja i funkcionalnosti za pronalaženje i brisanje dokumenata koji su arhivirani te za pronalaženje zapisa o dokazima.

TR-ESOR-Međusloj[614] (engl. TR-ESOR-Middleware)

Moduli i sučelja iz sloja TR-ESOR-Međusloj (međusloja) su:

- ArchiSafe modul,
- Kriptografski modul,
- ArchiSig modul,

Sučelja između tih modula uključuju:

- Sučelja između aplikacija iz aplikacijskog sloja i ArchiSafe modula. XML adapteri specifični za aplikacije mapiraju aplikaciju na sučelja arhiva.
- Sučelja između internih i eksternih komponenti međusloja

ArchiSafe modul[615]

ArchiSafe modul je standardiziran i siguran gateway koji kontrolira pristup poslovnih aplikacija prema ECM/dugotrajnom arhivu. Namjena ovog modula je izričito logičko razdvajanje aplikacija iz aplikacijskog sloja od ECM/dugotrajnog arhiva. Svaka (pisanje/promjena/brisanje) akcija sa strane specijaliziranih aplikacija prema ECM/dugotrajnoj arhivi treba biti obavljena kroz ovaj modul.

[614] Isto, str. 37
[615] Isto, str. 38

Tijekom spremanja elektronički potpisanih dokumenata i podataka ArchiSafe modul osigurava dokaznu kvalitetu informacija koje trebaju biti arhivirane na način da:

1. Elektronički potpisi budu validirani, a rezultat verifikacije se ugrađuje u XML dokument u standardiziranoj formi. Verifikacija potpisa se obavlja pomoću Kriptografskog modula,
2. ArchiSig modul koji je odgovoran za obnavljanje elektroničkih potpisa vraća identifikator arhivskog informacijskog paketa (AOID) poslije izračunavanja hash vrijednosti. Naknadni pristup do arhivskog informacijskog paketa je moguć samo iz navođenje AOID podatka.

Kriptografski modul[616] (engl. Cryptographic-Module)

Kriptografski modul osigurava različite kriptografske funkcije koje su potrebne za čuvanje dokaza. Ovaj modul može biti izveden kao hardverski modul kojem se pristupa preko hardverskih sučelja, kao mješavina hardvera i softvera kojem se pristupa preko softverskog sučelja ili kao isključivi softverski modul koji sadrži programske biblioteke ili poziv servisa. Kriptografski modul obavlja sljedeće funkcije:

- Kreiranje elektroničkih potpisa (opcionalno),
- Verificiranje potpisa; posebno potpisanih arhivskih informacijskih paketa,
- Validacija certifikata,
- Izračunavanje hash vrijednosti,
- Zahtijevanje i verifikacija kvalificiranih vremenskih žigova.

ArchiSig modul[617] (eng. ArchiSig-Module)

ArchiSig modul primarno obavlja funkcije zaprimanja i obnove dokazne vrijednosti elektroničkog potpisa u smislu zaštite integriteta arhiviranih informacijskih paketa. Za sve kriptografske funkcije ArchiSig modul pristupa Kriptografskom modulu iz razloga jer nema implementiranu niti jednu kriptografsku funkciju.

Ovaj modul implementira kriptografska rješenja koja osiguravaju da se prema potrebi može pristupiti ponovnom potpisivanju elektroničkog potpisa na pouzdan i ekonomičan način. Posebno je to bitno kod velike količine podataka. Ponovno potpisani elektronički potpisi moraju uključivati podatke i ranije potpise i moraju biti kreirani s kriptografskim

[616] Isto, str. 38
[617] Isto, str. 39

algoritmima i parametrima koji su prilagođeni zadanim mjerama sigurnosti. Kvalificirani vremenski žig koji ovjerava kvalificirani elektronički potpis je nužna mjera kod ponovnog potpisivanja elektroničkih potpisa. Procedura ponovnog potpisivanje može biti automatizirana i podešena tako da se mnogi dokumenti zajedno ponovo potpisuju. Za slučaj elektroničkog potpisa koji je temeljen na kvalificiranom certifikatu izdanom od certificiranog izdavatelja, mora biti korišten i kvalificirani vremenski žig od certificiranog izdavatelja. Temelj ArchiSig modula je IT implementacija ERS (eng. Evidence Record Syntax) standarda. Aneks TR-ESOR-F[618] koji dolazi uz Tehnički priručnik 03125 preporuča korištenje ERS ili XMLERS standarda, te opisuje njihovu sintaksu, tj. sintaksu zapisa o dokazu. ERS (engl. Evidence Record Syntax) standard je definiran kao RFC4998[619], a XMLERS (engl. Extensible Markup Language Evidence Record Syntax) standard je definiran kao RFC6283[620]. ERS i XMLERS standardi su tehnički temeljeni na pristupu da je hash vrijednost arhivskog informacijskog paketa (XAIP dokumenta) organizirana kao hash stablo. U navedenom hash stablu korijeni (engl. roots) su osigurani (ili zapečaćeni) s kvalificiranim vremenskim žigovima koji sadrže kvalificirane elektroničke potpise radi osiguravanja integriteta.

Stančić, Herceg i Rajh navode da za postizanje cjelovitosti i autentičnosti unutar BSI referentne arhitekture postoje sljedeći preduvjeti[621]:

- Elektronički potpis i vremenski žig trebaju biti na siguran i pouzdan način kreirani, verificirani, obnavljani i pohranjeni te pohranjeni sukladno zakonskim odredbama.
- Verifikacijski podaci koji će biti potrebni kasnije za verifikaciju elektroničkog potpisa trebaju biti dobiveni odmah poslije stvaranja i/ili verifikacije potpisa. Nakon toga se navedeni verifikacijski podaci deponiraju skupa s dokumentima i podacima koji se trebaju arhivirati. Dokumente, podatke i verifikacijske podatke je prije arhiviranja potrebno formirati u formu prikladnu za dugotrajno očuvanje.

[618] BSI (2015.), Annex TR-ESOR-F - Formats, BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/PrevVersion/TG-03125AnnexTR-ESOR-F.pdf?__blob=publicationFile (06.03.2018.)
[619] RFC 4998, Evidence Record Syntax (ERS), http://tools.ietf.org/html/rfc4998 (06.03.2018.)
[620] RFC 6283, Extensible Markup Language Evidence Record Syntax (XMLERS), https://tools.ietf.org/html/rfc6283 (06.03.2018.)
[621] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 11 (24.02.2018.)

- Svi verifikacijski koraci i verifikacijski rezultati trebaju biti logirani te biti u formi iz koje se jasno mogu ustanoviti bitne činjenice.
- Za vremenske žigove mora biti osigurana kompatibilnost sa standardima i preporukama BSI agencije i federalne mrežne agencije (njem. Bundesnetzagentur[622], engl. Federal Network Agency).
- Elektronički potpisi trebaju biti produženi (engl. augmentated) prije isteka zaštitnih mjera korištenih u kriptografskim algoritmima. Produženje (engl. augmentation) potpisa mora biti obavljeno u skladu sa zakonskim propisima i na način koji je u većoj mjeri automatiziran i ekonomičan.
- Prema važećem pravnom mišljenju, dokument može biti ponovo potpisan ako je originalno bio elektronički potpisan s kvalificiranim vremenskim žigom koji uključuje barem jedan kvalificirani elektronički potpis.
- Komponente sustava za prikaz podataka trebaju biti u mogućnosti vizualizirati potpisane podatke, certifikate i verifikacijske rezultate.
- Integritet nepotpisanih podataka prilikom prijenosa u ECM/dugotrajno skladištenje treba biti osiguran kriptografskim sigurnosnim mjerama kao što su hash vrijednosti ili elektronički potpis i kvalificirani vremenski žig.

Nadalje, Stančić, Herceg i Rajh navode preporuke za formate dokumenata i preporučene kriptografske formate iz Tehničkog priručnika 03125 koje su prepoznali kao bitne[623]. Preporuke navode da meta podaci i verifikacijski podaci trebaju biti spremljeni uz dokumente namijenjene dugotrajnoj pohrani na način da kreiraju arhivski informacijski paket unutar XML sintakse. Takav paket se naziva XAIP (eng. XML formatted Archival Information Package).

Preporučeni formati podataka su: XML, XSD, PDF/A, ODF, TIFF, JPG, PNG.
Preporučeni kriptografski formati su: PKCS#7, CMS, CAdES, XMLdSig, XAdES.
Format certifikata: X.509.
Formati validacije certifikata: OCSP i SCVP.

[622] Bundesnetzagentur, http://www.bundesnetzagentur.de/EN/Home/home_node.html (05.03.2018.)
[623] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf, str. 11-12 (24.02.2018.)

Navedene preporuke su usvojene od njemačkih (SAGA[624], XÖV[625], ArchiSafe[626]) i internacionalnih standardizacijskih inicijativa (MoReq2, OASIS).

Schwalm piše[627] o BSI referentnom modelu u kontekstu izgradnje arhitekture za dugotrajno očuvanje elektronički potpisanih dokumenta temeljene na SOA (engl. Service Oriented Architecture) konceptu i OAIS funkcionalnom modelu. Schwalm eksplicitno upućuje[628] na TR-03125 model (definiran Tehničkim priručnikom 03125) kao model za dugotrajno očuvanje i na korištenje AIP paketa za čuvanje dokaza postojanja. Navodi i da se referentna arhitektura definirana Tehničkim priručnikom 03125 koristi širom industrije (npr. avioindustrija, javna uprava, zdravstvo, bankarstvo) te da je temeljena na međunarodnim standardima.

Postoje i konkretni primjeri BSI TR-03125 sukladnih komercijalnih proizvoda za dugotrajno arhiviranje dokumenata u Njemačkoj:

- Ceyoniq Technology GmbH[629] (A Kyocera group company),
- FUJITSU[630], Security Solution Compliant Archiving SecDocs,
- FTK[631] – Research Institute for Telecommunication and Cooperation – Njemačka,
- Secrypt GmbH[632],
- …

ETSI je 2017. godine objavio studiju „Elektronički potpisi i infrastrukture (ESI); Proučavanje i okvir za standardizaciju usluga dugotrajnog očuvanja podataka, uključujući

---

[624] SAGA, http://www.kbst.bund.de/saga (05.03.2018.)
[625] XÖV, https://www.xoev.de (05.03.2018.)
[626] ArchiSafe, http://www.archisafe.de (05.03.2018.)
[627] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business
Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 131-144 (05.03.2018.)
[628] Isto, str. 138
[629] Ceyoniq technology, Saving electronic documents and preserving their evidentiary value in accordance with TR-ESOR, https://www.ceyoniq.com/en/en/bsi-compliant-long-term-archiving (06.03.2018.)
[630] Fujitsu (2015.), Security Solution Compliant Archiving SecDocs V2.3, https://sp.ts.fujitsu.com/dmsp/Publications/public/ds-secdocs-eu-en.pdf (06.03.2018.)
[631] FTK, Long-Term Archiving & Digital Preservation, http://www.ftk.de/en/competences/long-term-archiving-and-digital-preservation (06.03.2018.)
[632] Secrypt, Long-term management of signed data with official time stamps, https://www.secrypt.de/en/solutions/preserving-probative-value (06.03.2018.)

očuvanje s elektroničkim potpisima“[633] (engl. Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures). Navedena studija proučava različite koncepte servisa dugotrajno očuvanje podataka te predlaže ETSI AIP strukturu paketa. Ova studija prepoznaje njemački (BSI TR-03125) referentni model i talijanski model (Scryba) kao podlogu za izradu svog prijedloga. Naime, i njemački i talijanski referentni modeli se temelje na OAIS modelu te koriste različite XML sheme za AOP pakete. Ova studija je svoj prijedlog koji podržava njemačko i talijansko rješenje na način da definira granice između standardizacije nacionalnih rješenja i ETSI domene[634].

9.10 ZAKLJUČAK

Komparativna analiza implementiranih elektroničkih javnih servisa je kao istraživačka obavljena unutar projekta InterPARES Trust 2014. godine. Obrađene su informacije o uslugama kako bi provjerili jesu li usluge izgrađene kao: odgovorne, pouzdane, točne, sigurne, transparentne i vjerodostojne te razmatraju li problematiku pitanja vezana uz privatnost, obaveze čuvanja i pravo na zaborav. Nađeno je malo informacija o dugotrajnoj pohrani podataka. Informacija o preferiranim dugoročnim formatima očuvanja zapisa je bila dostupna samo za litvanske e-usluge za socijalne doprinose zaposlenicima (PDF/A i XAdES-A). Razdoblje čuvanja podataka u sustavima istraživanih usluga razlikuju se u ovisnosti o vrsti podataka koji se čuvaju te vrsti institucije odgovorne za podatke. U Njemačkoj i Ujedinjenom Kraljevstvu visokoškolske institucije i sveučilišta su dužni čuvati podatke tijekom studiranja te još dodatne tri. U Hrvatskoj i Švedskoj, evidencije o podacima zdravstvene i socijalne skrbi stvorene e-uslugama trebaju se čuvati najmanje 30 godina. Istraživački tim je objavio preporuku da bi servisi trebali imati obavezu objave načina skladištenja i dugoročnog očuvanja podataka.

[633] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (06.03.2018.)

[634] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 34 (06.03.2018.)

Analiziran je i HALMED[635] DAIS sustav u Hrvatskoj. DAIS je u većoj mjeri kompatibilan s ISO standardom za otvorene arhivske informacijske sustave (OAIS) te s PDF/A standardom. DAIS podupire i procedure konverzije u arhivski PDF format i prijenos metapodataka putem XML formata za razmjenu podataka. DAIS koristi svoj interni elektronički potpis. Bitno je spomenuti podatak o dimenzijama spremljenih podataka u DAIS sustav. Na dan 26. veljače 2018. u DAIS sustavu je bilo 24,8 milijuna skenova[636]. Važnost HALMED DAIS sustava za ovaj rad je ta što je to jedini (koliko je meni poznato) takav sustav u Hrvatskoj. Njegova vrijednost je što se i dalje nadograđuje sukladno otvorenim standardima.

Njemačka klinike Braunschweig[637] je korištenjem PDF/A standarda unaprijedila radne procese te smanjila troškove arhiviranja medicinske dokumentacije. Bitno je spomenuti da su razdoblja čuvanja medicinskih dokumenata po 30 ili više godina (npr. rendegenske snimke ili slike sa CT pretrage). U ovom informacijskom sustavu se potpisivanjem kvalificiranim elektroničkim potpisom te korištenjem vremenskog žiga osigurava nepobitan dokaz o vremenu izrade.

Litvanski EAIS[638] arhivski sustav pohranjuje i elektronički potpisane dokumente (koristi se i kvalificirani elektronički potpis). Struktura takvih dokumenata je temeljena na XML jeziku, a potpis se izvodi pomoću XAdES potpisnog formata (koristi se XAdES-A format iz razloga što zapisi potpisani takvim potpisom mogu biti dugoročno sačuvani). Svi elektronički zapisi koji uđu u EAIS konvertiraju se u format namijenjen dugotrajnoj pohrani podataka - PDF/A.

Komparativna analiza unutarnje strukture i funkcija elektroničkih arhiva za složene elektroničke zapise koju su napravili Stančić, Herceg i Rajh[639] 2014. godine je donijela usporedbu: arhivskog sustava austrijskih zemljišnih knjiga (BAIK), HALMED-DAIS

[635] HALMED, Agencija za lijekove i medicinske proizvode, http://www.halmed.hr/ (24.02.2018.)
[636] Informacija priopćena iz HALMED ustanove (26.02.2018.)
[637] Wild, B. (2012.), PDF/A in Healthcare, white paper, PDF Association – PDF/A Competence Center, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiCnczNv77ZAhXD26QKHU7KCZIQFggsMAA&url=https%3A%2F%2Fwww.pdfa.org%2Fwp-content%2Funtil2016_uploads%2F2012%2F05%2FWP-PDFA-in-Healthcare.pdf&usg=AOvVaw0PYq9l9u_u5UJwI9zwCdCW (24.02.2018.)
[638] Electronic Archive Information System, http://eais-pub.archyvai.lt/eais (23.02.2018.)
[639] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)

sustav, arhivski sustav klinika Braunschweig, litvanski EAIS sustav te referentni njemački model za dugoročno očuvanje elektronički potpisanih zapisa (BSI). Autentičnost i uvid u arhivske zapise BAIK sustava je omogućena korištenjem elektroničkog potpisa i dokumentacije u formatu PDF/A1-b, a kao format elektroničkog potpisa koristi se isključivo XMLDSig. Stančić, Herceg i Rajh su na kraju komparativne analize zaključili[640] da proces dugoročnog očuvanja složenih elektroničkih zapisa ostaje tehnički i organizacijski izazov. Predlažu korištenje otvorenih standarda te izbjegavanje vlasničkih radi osiguravanja stabilnosti u procesu arhiviranja.

Proučen je i E-ARK projekt[641] čiji je cilj bio pilotirati postojeće arhivske servise koji zadržavaju autentičnost i čitljivost na postojećim najboljim praksama. Projekt su obavljali akteri unutar Europske Unije. E-ARK Specifikacija polazi od OAIS referentnog modela i OAIS informacijskih paketa: SIP, AIP i DIP. E-ARK Specifikacija se može provesti kroz dva osnovna elementa: fiksne fizičke strukture informacijskog paketa i uporabe metapodataka u METS i PREMIS formatima.

Podaci o Elektroničkom arhivu Nacionalnog arhiva Estonije[642] sam dobio preko upitnika navedenog u Prilogu 2. Radi se o u Estoniji vrlo uspješnog i široko prihvaćenom e-arhivu. Ovaj arhiv (sukladan OIAS referentnom modelu) prihvaća elektronički potpisane zapise te jedna kopija zapisa ostaje u potpisanom formatu, ali druga kopija je tretirana kao otvorena datoteka. Kod nje se podaci potpisa premještaju u zapis metapodataka, a sam zapis se seli u arhivski format, uglavnom PDF. Od formata naprednog elektroničkog potpisa koristi se XAdES.

Salsa i Guerizio pišu[643] o e-arhivu elektronički potpisanih medicinskih podataka zdravstvenog sustava okruga Vicenze u Italiji. Središnji dio tog e-arhiva je sustav

[640] Isto, str. 15
[641] E-ARK, European Archival Records and Knowledge Preservation, http://www.eark-project.com (06.03.2018.)
[642] Digital archives, Rahvusarhiiv, http://www.ra.ee/en/information-management/digital-archives/ (16.03.2018.)
[643] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=182 , str. 172-179 (06.03.2018.)

Scryba[644] koji je temeljen na OAIS referentnom modelu. Prema talijanskim propisima svi medicinski zapisi dostavljaju se na dugotrajno očuvanje odmah po njihovoj izradi i potpisivanju. Proces očuvanja u ovom arhivskom sustavu se temelji na prikupljanju digitalnih resursa koji će biti sačuvani u velikim serijama pod nazivom Volumen očuvanja, PV. PV sadrži stvarne objekte očuvanja i prolazi kroz proces elektroničkog potpisivanja ovjerenog certificiranim vremenskim žigom te periodične kontrole.

Vrlo bitan za ovaj rad je i referentni model dugotrajne pohrane elektronički potpisanih dokumenata njemačkog ureda za informacijsku sigurnost, BSI[645]. On se temelji na međunarodnim standardima (XML, XAdES, CAdES, općenito Uredba eIDAS, standardizirani formati podataka). Osim međunarodnih standarda, temelj ovog modela je i njemački zakon o arhiviranju, BarchG[646] BSI je objavio Tehnički priručnik 03125[647] (Priručnik) koji sadrži velik broj kvalitetnih i korisnih preporuka koje sam i sam. Priručnik detaljno opisuje referentnu arhitekturu sustava za dugotrajnu pohranu elektronički potpisanih dokumenata te se navode zahtjevi po svakoj komponenti arhitekture. Za ovaj rad je od iznimne vrijednosti prijedlog tehničke implementacije zapisa dokaza postojanja pomoću standarda ERS (RFC4998[648]) ili XMLERS (RFC6283[649]). ERS i XMLERS standardi su tehnički temeljeni na pristupu da je hash vrijednost arhivskog XML informacijskog paketa (XAIP dokumenta) organizirana kao hash stablo. U navedenom hash stablu korijeni su osigurani (ili zapečaćeni) s kvalificiranim vremenskim žigovima koji sadrže kvalificirane elektroničke potpise radi osiguravanja integriteta. Ovakav način implementacije zapisa dokaza postojanja će se detaljnije razraditi u ovoj doktorskoj disertaciji za potrebe izrade koncepta uspostave elektroničkog arhiva u javnoj upravi. Schwalm eksplicitno upućuje[650] na TR-03125 model kao model za dugotrajno očuvanje i

[644] Scryba, http://www.medas-solutions.it/products/product-scryba.html (06.03.2018.)
[645] BSI, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Home/home_node.html (05.03.2018.)
[646] Bundesarchivgesetz, BarchG, (2017.), https://www.bundesarchiv.de/DE/Content/Downloads/Rechtliches/bundesarchivgesetz.pdf?__blob=publicationFile (05.03.2018.)
[647] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile (05.03.2018)
[648] RFC 4998, Evidence Record Syntax (ERS), http://tools.ietf.org/html/rfc4998 (06.03.2018.)
[649] RFC 6283, Extensible Markup Language Evidence Record Syntax (XMLERS), https://tools.ietf.org/html/rfc6283 (06.03.2018.)
[650] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business

na korištenje AIP paketa za čuvanje dokaza postojanja te navodi i da se ova referentna arhitektura koristi širom industrije. ETSI je je kroz studiju „Elektronički potpisi i infrastrukture (ESI); Proučavanje i okvir za standardizaciju usluga dugotrajnog očuvanja podataka, uključujući očuvanje s elektroničkim potpisima“[651] prepoznala njemački (BSI TR-03125) referentni model i talijanski model (Scryba) kao podlogu za izradu svog prijedloga usluge dugotrajnog očuvanja podataka.

Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 131-144 (05.03.2018.)

[651] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (06.03.2018.)

10. MODEL INFORMACIJSKOG SUSTAVA ZA DUGOTRAJNU POHRANU POTPISANIH ELEKTRONIČKIH DOKUMENATA

U ovom poglavlju će biti dani konačni elementi modela informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata na temelju obrađenih uspješnih implementacija i referentnih modela u ovom radu. Detaljno će biti obrađena tematika očuvanja dokaza postojanja, tj. PoE (engl. Proof of Existence). Što se tiče samog modela, bit će detaljno razrađene korisničke uloge, načini pristupa sustavu, standardi i formati koji će se koristiti. Bit će dana i arhitektura i opis funkcionalnosti za predloženi model. Pod ostalim zahtjevima će biti navedeni zahtjevi iz područja: sigurnosti pohrane podataka, migracije i topologije informacijskog sustava. Na kraju poglavlja će biti dan prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave. Predložena infrastruktura će se u radu nazivati: sustav e-Arhiv.hr.

10.1 OČUVANJE DOKAZA POSTOJANJA

Lipp je u svojem članku „Signature Validation – a Dark Art“ [652] dao osvrt na sam proces validacije naprednog elektroničkog potpisa. O tome je u ovom radu već pisano u poglavlju 4.5 Validacija naprednog elektroničkog potpisa. Navedeni autor pojašnjava da ETSI norma ETSI EN 319 102-1 utvrđuje mogućnost da validacijski algoritmi odrađuju validaciju potpisa u dugom roku kada postoji vremenski žig koji jamči da je potpis postojao u vrijeme vremenskog žiga. U ovom slučaju se radi se o dokazu postojanja. Lipp, nadalje, predlaže validiranje potpisa neposredno nakon njegove izrade te njihovo sigurno arhiviranje zajedno s validacijskim rezultatom, validacijskim izvješćem i materijalom korištenim za validiranje.

Očuvanje dokaza postojanja (PoE) smatram bitnim u modelu informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata, tj. za sustav e-Arhiv.hr. Kao bitan izvor podataka o načinu očuvanja dokaza postojanja prepoznajem BSI tehnički

[652] Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

priručnik 03125[653] koji daje opis generalnih zahtjeva za arhiviranje s očuvanjem dokaza (engl. preservation of evidence). Za dugoročni dokaz autentičnosti potpisanih podataka je bitno da se postojanje certifikata i njegove valjanosti u vrijeme kada je potpis nastao može provjeriti i kasnije.

Odgovornost je primatelja potpisanih podataka (sustav e-Arhiv.hr) da osigura predočenje certifikata i povezanih podataka o certifikatu ako su potrebne za zahtjev za dokazom. Iz tog razloga sustav e-Arhiv.hr će odmah po zaprimanju SIP paketa s potpisanim podacima trebati pohraniti i potrebne certifikate i dodatne podatke o tim certifikatima zajedno s potpisanim podacima, a možda već i po samom stvaranju potpisanih podataka. Za elektroničke potpise temeljene na kvalificiranom certifikatu potrebno je predočiti i tehnički provjeriti sljedeće podatke kako bi se potvrdilo postojanje i valjanost certifikata u vrijeme kada je potpis stvoren[654]:

- Korisnički certifikat i, ako je potrebno, cijeli lanac certifikata do korijenskog certifikata,
- Izvješće o statusu (OCSP) od pružatelja usluga certificiranja o postojanju i valjanosti certifikata, kao i lanca certifikata do korijenskog certifikata,
- Kvalificirani vremenski žig koji se odnosi na potpis, također s lancem certifikata do korijenskog certifikata.

Svi prethodno navedeni podaci mogu se spremati uz same potpisane podatke, ali mogu biti spremljeni i u zasebnoj bazi podataka da bi se osigurala njezina dostupnost putem jedinstvene reference. Za kasniju provjeru valjanosti elektroničkog potpisa u trenutku njegovog stvaranja potrebno će biti razlučiti vrijeme potpisivanja s kvalificiranog vremenskog žiga s kojim je potpis ovjeren. Ako će prilikom kasnije provjere takav kvalificirani vremenski žig biti nedostupan što uzrokuje da se valjanost potpisa u ranijoj vremenskoj točki ne može dokazati, onda se provjera valjanosti treba provesti u odnosu na sadašnje vrijeme.

[653] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile (08.03.2018)
[654] Isto, str. 18

Obnavljanje elektroničkog potpisa je potrebno radi osiguravanja integriteta potpisanih zapisa u dugom roku. Podaci s kvalificiranim elektroničkim potpisom trebaju biti ponovno potpisani ako se u potpisanom obliku trebaju čuvati u razdoblju dužem od razdoblja za koje se potpisni algoritam smatra da je prikladan. Sustav e-Arhiv.hr treba kontinuirano pratiti prikladnost primijenjenih kriptografskim algoritama. Ako je ugrožena prikladnost korištenih algoritama potpisivanja i pripadajućih parametara za zaštitu, tada se podaci i svi postojeći potpisi trebaju ponovno potpisati. Gore navedeni postupak opisan u BSI tehničkom priručniku 03125[655] je osnova očuvanja dokaza postojanja za elektroničke dokumente. S druge strane, kvalificirani vremenski žig može sadržavati kvalificirani elektronički potpis te se za produženje (engl. augmentation) potpisa može koristiti i ovako potpisani vremenski žig. U tom slučaju dodatni potpis nije niti potreban za očuvanje dokaza postojanja.

Produženje elektroničkog potpisa se u sustavu e-Arhiv.hr treba provoditi pravovremeno, tj. prije isteka prikladnosti korištenih algoritama. Produženje potpisa treba obuhvatiti sve dostupne elektroničke potpise jer se na taj način zadržava cjelokupna struktura dokumenata i pridruženih potpisa i informacija. Osnovna namjera produženja potpisa jest osigurati provjerljivost cjelovitosti i autentičnosti već potpisanih dokumenata.

Što se tiče vremenskih žigova, oni isto mogu s vremenom izgubiti svoju prikladnost. Prije nego što se navedeno dogodi, vremenski žigovi trebaju biti sačuvani na način da se dohvati novi vremenski žig. Kvalificirani vremenski žig se mora odnositi i na potpisane podatke i na potpis (kako je navedeno u BSI tehničkom priručniku 03125)[656] ako korištenom hash algoritmu prijeti da postane nesiguran. Ako je hash algoritam još uvijek prikladan, tada se vremenski žig koji se treba izraditi mora odnositi samo na potpis. To je dovoljno jer podaci i dalje odgovaraju starom potpisu. Iz perspektive sigurnosne tehnologije nije potrebno izračunati novu hash vrijednost za podatke kako bi se izvršilo produženje potpisa. Isto tako, nije potrebno dohvaćati zasebne vremenske žigove za svaki elektronički dokument koji treba biti ponovno potpisan. Dohvaćanje vremenskog žiga za svaki elektronički dokument nije ekonomično pa je za sustav e-Arhiv.hr prijedlog dohvatiti jedan vremenski žig na veći broj potpisanih dokumenata. Učinak vremenskog žiga za osiguravanje

[655] Isto, str. 19
[656] Isto, str. 20

integriteta zapisa ne ovisi o broju potpisa koji su istovremeno sačuvani, a osim toga jedan (sveobuhvatan) novi potpis može biti stavljen na bilo koji broj potpisanih podataka[657].

U sustavu e-Arhiv.hr će se ponovno potpisivanje većeg broja elektronički potpisanih zapisa obavljati periodički, putem automatiziranog programa o čijem se pokretanju i obavljanju aktivnosti treba brinuti sam e-Arhiv.hr informacijski sustav. Preduvjet za navedene aktivnosti ponovnog potpisivanja pomoću automatiziranog programa je da djelatnik sustava e-Arhiv.hr konfigurira parametre za periodičko potpisivanje sukladno definiranim procedurama sustava e-Arhiv.hr. Dakle, navedeni djelatnik svjesno pokreće taj proces, tj. namješta parametre za pokretanje izvođenja aplikacije kroz neko vrijeme, ali ne potvrđuje podatke koji se trebaju potpisati u pojedinačnim slučajevima prije potpisivanja (npr. unos PIN-a).

Potpisani zapisi, potpisi i verifikacijski podaci u sustav e-Arhiv.hr se trebaju pohranjivati u arhivski ECM sustav. Pohrana navedenih podataka se treba provesti u obliku koji osigurava potpunost, dostupnost, čitljivost i cjelovitost podataka pohranjenih za cijelo vrijeme zadržavanja zapisa (engl. retention time). Za provedbu navedenog potrebno je (kako je navedeno u BSI tehničkom priručniku 03125)[658] koristiti otvorene, standardizirane formate podataka. Otvorene i standardizirane formate podataka je potrebno koristiti zbog izbjegavanja konverzija formata tijekom čuvanja spremljenih podataka na dugi rok. Naime, konverzijom formata elektronički potpisanih podataka, postojeći potpisi mogu postati bezvrijedni. Detaljnije o formatima podataka koji se predlažu za sustav e-Arhiv.hr će biti navedeno u poglavlju 10.3 Standardi i formati.

Sa stanovišta sustava e-Arhiv.hr, aplikacije u aplikacijskom sloju sustava (ili potpisni moduli izvan samog sustava) trebaju osigurati da se dokumenti potpišu od strane autoriziranih osoba s propisanim potpisnim procedurama i certificiranim potpisnim komponentama.

U svrhu održavanja prikladnosti dokaza postojanja (PoE) o elektroničkim potpisanim podacima i dokumentima za vrijeme trajanja njihovog očuvanja u sustavu e-Arhiv.hr podaci potrebni za provjeru potpisa u budućnosti bi se trebali dohvatiti neposredno nakon

[657] Isto, str. 20
[658] Isto, str. 21

izrade i/ili provjere potpisa te trebaju biti arhivirani skupa s dokumentima i ostalim podacima u obliku koji će biti čitljiv i upotrebljiv na dugi rok. Sustav e-Arhiv.hr treba moći logirati sve korake provjere potpisa te rezultat provjere. Logiranje navedenih podataka dobivenih provjerom potpisa podrazumijeva zapisivanje u aplikativni log i/ili u bazu podataka. Dokaze postojanja i logirane podatke je potrebno moći prikazivati tijekom razdoblja čuvanja kroz specijaliziranu aplikaciju u ljudski čitljivom obliku. Naime, sam elektronički potpis je prikazan kao niz znakova, originalno ljudima nečitljiv pa je potrebno osigurati prikaz informacije o valjanosti potpisa te ostale informacije o dokazu postojanja. Kako bi se mogla jamčiti provjerljivost elektroničkog potpisa s elektronički potpisanim vremenom potrebno je koristiti standardizirane formate za elektroničke potpise. Detaljnije o njima će biti navedeno u poglavlju 10.3 Standardi i formati.

Osim potpisanih podataka potrebno je u sustavu e-Arhiv.hr osigurati integritet nepotpisanih podataka u trenutku prijenosa u ECM sustav na način da se izračuna ulazna hash vrijednosti tih podataka ili da se takvi podaci ovjere kvalificiranim vremenskim žigom.

Schwalm i Korte opisuju i funkcionalne zahtjeve potrebne za očuvanje dokaza postojanja[659] za koje smatram da ih i sustav e-Arhiv.hr treba implementirati:

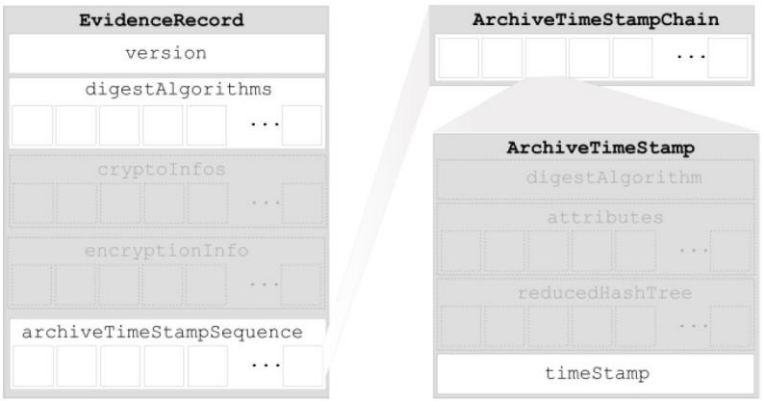
- Hashing AIP-a
    - Izrada kriptografskih hash-eva,
    - Osiguravanje potpisanih podataka,
    - Rano hashiranje AIP paketa kako bi se sačuvala njihova autentičnost i integritet,
    - Sortiranje, spajanje i kanonizacija podataka,
- Čuvanje dokaza postojanja tijekom dugog roka,
- Neovisnost od specifičnih (vlasničkih) tehničkih proizvoda i okruženja,
- Osiguravanje interoperabilnosti u razmjeni podataka između sustava i ostalih aktera dionika pružajući samostalni, standardizirani AIP format,
    - AIP treba osim opisnih i tehničkih metapodataka sadržavati i dopunske podataka o dokazima postojanja.

[659] Schwalm, S., Korte, U. (2014.), Standards for the Preservation of Evidence and Trust for Electronic Records, IS&T Archiving 2014 Conference, Berlin, https://www.researchgate.net/publication/263474467_Standards_for_the_Preservation_of_Evidence_and_Trust_for_Electronic_Records , str. 3 (10.03.2018.)

Kako bi se osigurali navedeni zahtjevi nužno je da su sljedeće funkcije implicitni dijelovi sustava za očuvanje dokaza o elektroničkim zapisima:

- Prikupljanje i provjera dopunskih podataka o dokazima,
- Izrada zapisa o dokazima koji su usklađeni s RFC 4998 (ERS, Evidence Record Syntax) ili RFC 6283 (XMLERS, XML temeljen ERS),
- Pristup evidencijama zapisa i dopunskim podacima o dokazima u skladu s pravilima pristupa elektroničkom arhivu,
- Provjeru evidencije dokaza radi dokazivanja autentičnosti i integriteta AIP paketa,
- Očuvanje ponovnim potpisivanjem arhivskim vremenskim žigom ili ponovnim uspostavljanjem hash stabla s novim i sigurnim hash kriptografskim algoritmom.

Schwalm i Korte tvrde da ERS/XMLERS omogućuje obradu više arhivskih objekata unutar jedne obrade koristeći tehniku hash stabla, tj. Merkleovo stablo[660] i to na način da se samo jednim arhivskim vremenskim žigom osigura zaštita svih arhivskih objekata. Da bi se dokazalo postojanje jednog podatkovnog objekta, hash stablo se može svesti na nekoliko skupova hash vrijednosti, nazvanih reduciranim hash stablom. Tih nekoliko skupova hash vrijednosti su dovoljni za dokazivanje postojanja jednog podatkovnog objekta. Slika 54 prikazuje strukture zapisa o dokazu postojanja sukladno RFC 4998.

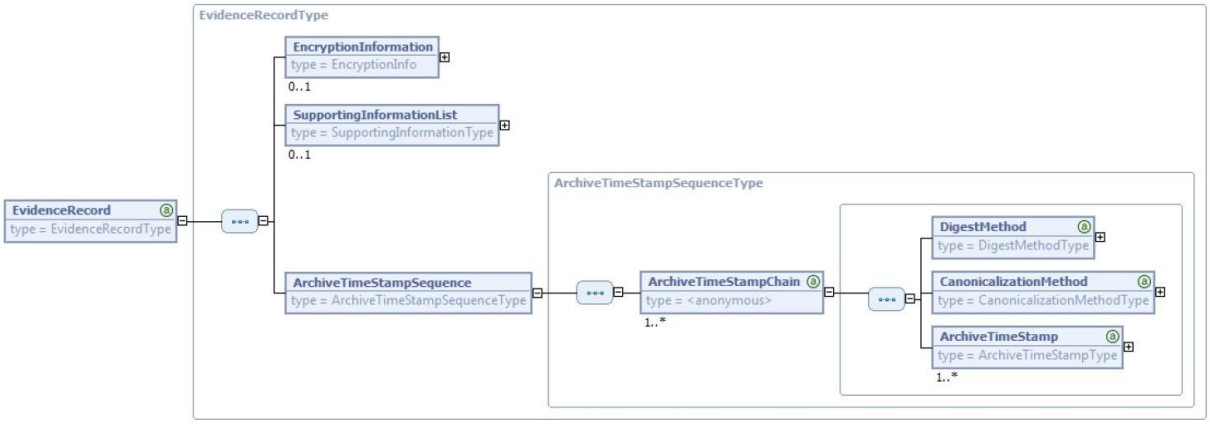


Slika 54. Struktura zapisa o dokazu postojanja sukladno RFC 4998, preuzeto iz Schwalm, S., Korte, U. (2014.)[661]

[660] Merkle, R., C. (1980.), Protocols for public key cryptosystems, Simpozij sigurnosti i privatnosti, Oakland, https://www.computer.org/csdl/proceedings/sp/1980/0335/00/06233691-abs.html , str. 122–134. (10.03.2018.)

[661] Schwalm, S., Korte, U. (2014.), Standards for the Preservation of Evidence and Trust for Electronic Records, IS&T Archiving 2014 Conference, Berlin,

Osim navedenih autora i ETSI organizacija se bavila istraživanjem tematike očuvanja dokaza postojanja te je 2017. objavila istraživačku studiju servisa za dugotrajnu pohranu podataka[662] (u nastavku teksta ETSI studija). ETSI studija također navodi ERS i XMLERS sintakse kao podlogu za izradu zapisa dokaza postojanja. U nastavku slijedi prikaz XML strukture zapisa o dokazu postojanja sukladno RFC 6283 (XMLERS).



Slika 55. XML struktura zapisa o dokazu postojanja (EvidenceRecord), sukladno RFC 6283, preuzeto iz ETSI (2017.)[663]

Ako postoji rizik da će kriptografski algoritm koji je korišten za izradu arhivskog vremenskog žiga izgubiti svoju prikladnost, tada je potrebno arhivski vremenski žig zaštititi još jednim arhivskom vremenskim žigom s novim prikladnim algoritmom[664]. U ovom koraku očuvanja treba procijeniti hoće li algoritam potpisa ili uključeni hash postati slabi. U slučaju kada je algoritam potpisa slab, potrebno je izraditi novi arhivski vremenski žig koji jednostavno pokriva prethodni. Ovaj proces Schwalm i Korte nazivaju obnovom vremenskog žiga (engl. Timestamp Renewal). U slučaju kada slabi hash algoritam korišten za izgradnju hash stabla potrebno je obaviti obnovu hash stabla (engl. Hash-Tree Renewal). Tada se arhivski vremenski žig i arhivirani podatkovni objekti koji su

---

https://www.researchgate.net/publication/263474467_Standards_for_the_Preservation_of_Evidence_and_Trust_for_Electronic_Records , str. 4, slika 4 (10.03.2018.)

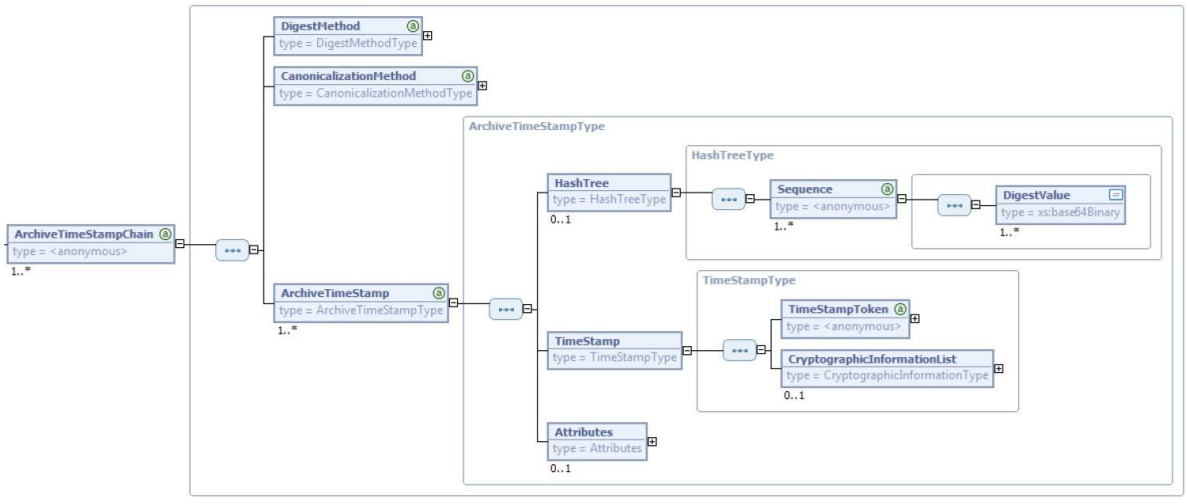
[662] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (06.03.2018.)

[663] Isto, str. 53

[664] Schwalm, S., Korte, U. (2014.), Standards for the Preservation of Evidence and Trust for Electronic Records, IS&T Archiving 2014 Conference, Berlin, https://www.researchgate.net/publication/263474467_Standards_for_the_Preservation_of_Evidence_and_Trust_for_Electronic_Records , str. 4 (10.03.2018.)

obuhvaćeni arhivskim vremenskim žigom arhiva moraju ponovo hashirati preko novog prikladnog hash algoritma te ponovo obuhvatiti vremenskim žigom.

Niz arhivskih vremenskih žigova stvorenih tijekom procesa obnavljanja vremenskih žigova stvara lanac arhivskih vremenskih žigova (ArchiveTimeStampChain), a niz lanaca arhivskih vremenskih žigova koji je stvoren tijekom procesa obnove hash stabla stvara slijed arhivskih vremenskih žigova (ArchiveTimeStampSequence) koji zajedno s administrativnim podacima (EncryptionInformations, SupportingInformationList…) tvori zapis dokaza postojanja (EvidenceRecord)[665]. Svaki novi arhivski vremenski žig u slijedu vremenskih žigova i lancu arhivskih vremenskih žigova uključuje prethodne vremenske žigove, tako da postoji zabilježen vremenski poredak kojim se čuva autentičnost i integritet uključenih vremenskih žigova. Da bi se autentičnost i integritet sačuvala u dugom roku, svaki se novi arhivski vremenski žig treba izraditi još za vremena prikladnosti kriptografskog algoritma prethodno dodanog arhivskog vremenskog žiga. Na slici 56 je prikazana i XML struktura lanca arhivskih vremenskih žigova iz ETSI studije.



Slika 56. XML struktura lanca arhivskih vremenskih žigova (ArchiveTimeStampChain) sukladno RFC 6283, preuzeto iz ETSI (2017.)[666]

[665] Isto, str. 4
„The sequence of Archive Timestamps created during Timestamp Renewal forms an Archive Timestamp Chain and the sequence of Archive Timestamp Chains, which is created during corresponding Hash-Tree Renewals, form the Archive Timestamp Sequence, which together with some administrative data forms the Evidence Record, which is used to prove the authenticity and integrity of the data which is to be protected."
[666] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 53, slika C-3 (06.03.2018.)

Za dokazivanje autentičnosti i integriteta podataka koji se čuvaju u sustavu e-Arhiv.hr predlažem izrađivanje i korištenje zapisa dokaza postojanja.

Standardi RFC 4998 i RFC 6283 detaljno propisuju kako se mora izvesti izrađivanje i provjera dokaza postojanja te procesi obnove vremenskih žigova i obnove hash stabala. Osim toga, u ovim standardima se detaljno propisuju formati zapisa dokaza postojanja na način osiguravanja interoperabilnosti tako da se dokazi postojanja mogu razmijenjivati između različitih arhivskih sustava.

Za potrebe implementacije sustava e-Arhiv.hr predlažem korištenje RFC 6283 standarda, tj. zapis dokaza postojanja u XML formatu (XMLERS).

Schwalm[667] stavlja u isti kontekst korištenje arhivskog vremenskog žiga i Uredbe eIDAS. Spominje kvalificirani vremenski žig kao pravnu podlogu na razini Europske Unije za dugotrajno očuvanje elektroničkih zapisa. U poglavlju 3.5.4 Elektronički vremenski žig sam naveo saznanja iz Uredbe eIDAS u kojoj se vodi dosta računa o tome da bi se elektronički vremenski žig mogao koristiti kao dokaz u sudskim postupcima i to u različitim državama članicama Europske unije. Elektroničkim vremenskim žigom se omogućuje povjerenje u elektronički potpis i poslije isteka certifikata potpisnika (zbog isteka valjanosti ili zbog opoziva). Na taj način se omogućuju pretpostavke za dugotrajno arhiviranje elektronički potpisanih dokumenata. Uredba eIDAS podrazumijevaju da kvalificirani vremenski žig izdaje kvalificirani pružatelja usluga povjerenja. U ovom slučaju se radi o Službi za izradu kvalificiranog vremenskog žiga, QTSA (engl. Qualified Time-Stamping Authority).

Dakle, za potrebe sustava e-Arhiv.hr predlažem korištenje usluga Službe za izradu kvalificiranog vremenskog žiga (QTSA) radi dohvaćanja kvalificiranog vremenskog žiga u svrhu izrade zapisa o dokazu postojanja.

[667] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business
Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al.,
https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 132. (131-144) (05.03.2018.)

U poglavlju 4.2 Elektronički pečat iz Uredbe eIDAS za elektronički pečat navedene su sljedeće odredbe[668]:

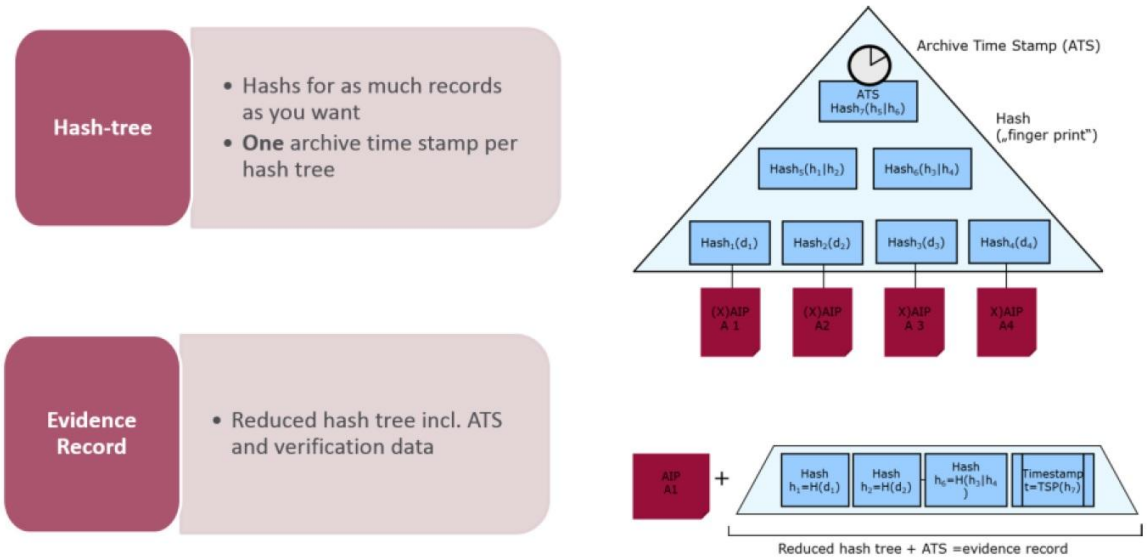
„(58) Kada je za transakciju potreban kvalificirani elektronički pečat pravne osobe, kvalificirani elektronički potpis ovlaštenog predstavnika pravne osobe trebao bi biti jednako prihvatljiv.

(59) Elektronički pečati trebali bi služiti kao dokaz da je elektronički dokument izdala pravna osoba, jamčeći na taj način izvornost i cjelovitost dokumenta.“

Schwalm[669] s obzirom na novu pravnu regulativu u Europskoj Uniji vezanu uz Uredbu eIDAS, spominje i pojam elektroničkog pečata vezano uz očuvanje dokaza postojanja te navodi sljedeće: „Trenutno se očuvanje dokaza postojanja ostvaruje ponovnim potpisivanjem i ponovnim postupkom izrade hash vrijednosti postojećih potpisa/pečata iste razine i kvalificiranim elektroničkim vremenskim žigom prije isteka njihove razine sigurnosti. Korištenjem Merkleovih hash stabala osigurava se učinkovit postupak ponovnog potpisivanja velikog broja elektroničkih potpisa ili elektroničkih pečata. Ponovno potpisivanje sadrži sve "stare" potpise i vremenske žigove. Navedeno Schwalm ilustrira slikom 57.

[668] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/80, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

[669] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business
Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 133. (131-144) (05.03.2018.)



Slika 57. Očuvanje dokaza postojanja temeljeno na Merkleovom hash stablu, preuzeto iz Schwalm, S. (2017.)[670]

Dakle, s primjenom Uredbe eIDAS se kvalificirani vremenski žig i pravno može upotrijebiti u svrhu dugotrajne pohrane elektroničkih zapisa i može se smatrati arhivskim vremenskim žigom.

BSI tehnički priručnik 03125[671], također spominje ERS standard kao podlogu za implementaciju dokaza postojanja u svom referentnom modelu e-arhiva. Navodi se da se ERS standard temelji na pristupu da su hash vrijednosti arhivskih podatkovnih objekata (XAIP paketi - engl. XML formatted Archival Information Package) organizirani u hash stablo (Merkleovo hash stablo). Navedeni priručnik koristi kvalificirani vremenski žig koji sadrži kvalificirani elektronički potpis za dokazivanje integriteta. BSI tehnički priručnik 03125 navodi i da se prvi stavljeni vremenski žig naziva inicijalni arhivski vremenski žig (engl. initial archive time stamp) te da je temelj povjerenja u arhivsko vrijeme kvalificirani vremenski žig koji sadrži kvalificirani elektronički potpis.

[670] Isto, , str. 134. , slika 1
[671] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 37 (06.03.2018.)

Bitno je imati u vidu i nedostatak na koji upozorava ETSI istraživačka studiju servisa za dugotrajnu pohranu podataka[672]. Naime, ETSI studija ističe da reducirano hash stablo omogućuje izdvajanje dokumenta s odgovarajućim zapisom dokaza postojanja (ERS/XMLERS). Jednom izdvojen, ERS se također može povećati samostalno, s vlastitim nizom vremenskih žigova. U slučaju korištenja reduciranog hash stabla, nedostatak je da se jednom izdvojen i odvojen od izvornog ERS-a, taj izdvojeni ERS povećava pojedinačno. Time se gubi prednost jedinstvenog vremenskog žiga koji bi zaštitio više dokumenata u isto vrijeme. Do sličnog zaključka u svom članku dolazi Lipp u svojem članku „Signature Validation – a Dark Art“[673] što je već detaljno obrađeno u ovom radu u poglavlju 4.5 Validacija naprednog elektroničkog potpisa. Naime, Lipp napominje da se proces validacije LTV potpisa iz AdES obitelji potpisa odvija rekurzivno. Isto načelo rekurzije vrijedi za certifikate CRL lista i OCSP servisa jer oni isto mogu isteći i biti opozvani. Lipp nadalje daje preporuke izbjegavanja potrebe za dugoročnom validacijom za ovakve potpise, a u slučaju kada je dugoročna validacija potpisa nužna, predlaže validiranje potpisa neposredno nakon izrade te njihovo sigurno arhiviranje zajedno s validacijskim rezultatom, validacijskim izvješćem i materijalom korištenim za validiranje što ide prema konceptu zapisa dokaza postojanja (ERS/XMLERS).

Dakle, može se zaključiti da prilikom izgradnje sustava e-Arhiv.hr treba dobro procijeniti hoće li se koristiti zapisi dokaza postojanja (ERS/XMLERS) za dugotrajno očuvanje elektroničkih dokumenata koji imaju pravni karakter elektroničke isprave (po još važećem hrvatskom Zakonu o elektroničkoj ispravi) ili će se pribjeći samostalnom periodičkom ovjeravanju vremenskim žigom. Elektronički dokumenti potpisani elektroničkim potpisima iz AdES obitelji potpisa s LTV svojstvom su samostalni, a ako se po potrebi obnavljaju tada sadrže sve podatke koji omogućavaju provjeru potpisa nakon duže vremena. Sve ovo navedeno isključuje zajedničko potpisivanje kvalificiranim vremenskim žigom, a time periodičko ovjeravanje nije ekonomično kao kod dokumenata koji se ovjeravaju po konceptu Merkleovog stabla. O elektroničkoj ispravi sam detaljno pisao u poglavlju 8.2 Pravna uređenost elektroničkih dokumenata. Može se pokazati potreba da se pohranjeni elektronički dokumenti koji imaju pravni karakter elektroničke isprave pohranjuju i periodički ovjeravaju kao samostalni te da se validacijski rezultati njihovih potpisa ne

[672] Isto, str. 23
[673] Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

spremaju u ERS/XMLERS. Primjeri ovakvih elektroničkih dokumenata, tj. elektroničkih isprava mogu biti elektronički rodni listovi ili izvodi iz matičnih knjiga koji po svojoj prirodi zahtjevaju ljudima prilagođenu čitljivost i mogućnost strojne i ljudske provjere podataka s dokumenta radi ostvarivanja socijalnih prava. Osim toga, elektroničke isprave trebaju imati unutarnji i vanjski obrazac tijekom cijelog svog dokumentacijskog ciklusa. Očuvanjem ovakvih potpisanih dokumenata modelom ERS/XMLERS-a izgubio bi se njihov pravni integritet (tehnički bi ostao i dalje očuvan). Primjeri dokumenata koji su potpisani, a mogli bi se čuvati u dugom roku po konceptu ERS/XMLERS-a mogu biti primjerice razne potpisane potvrde o uplatama u mirovinske fondove te mnogi drugi dokumenti koji se izrađuju komunikacijom tijela javne uprave i građana i poslovnih subjekata, a ne bi imali pravni karakter elektroničke isprave.

Stoga predlažem da se u sustavu e-Arhiv.hr omogući očuvanje potpisanih elektroničkih dokumenata na dvojak način:

- po modelu očuvanja dokaza postojanja (ERS/XMLERS) za potpisane elektroničke dokumente koji nemaju pravni karakter elektroničke isprave te za koje se može upotrijebiti ekonomično periodično ovjeravanje kvalificiranim vremenskim žigom automatskom obradom (više dokumenata bi se ovjeravalo jednim vremenskim žigom). Moja procjena je da bi se po ovom modelu u dugom roku čuvala velika većina pohranjenih potpisanih elektroničkih dokumenata,
- po modelu samostalne produženja (engl. augmentation) potpisa (AdES obitelj LTV potpisa) za elektroničke dokumente koji imaju pravni karakter elektroničke isprave te koji trebaju zadržati svojstvo unutarnjeg i vanjskog obrasca tijekom cijelog svog dokumentacijskog ciklusa. To bi bio relativno mali postotak elektronički potpisanih dokumenata u sustavu e-Arhiv.hr.

10.2 ULOGE KORISNIKA I PRISTUP SUSTAVU

Informacijski sustav e-Arhiv.hr treba imati mogućnost prijave korisnika s različitim ulogama koji će koristiti ovaj sustav. Kroz izradu ovog rada prepoznao sam sljedeće vrste korisnika koji trebaju imati pravo pristupa na e-Arhiv.hr:

- Djelatnici sustava e-Arhiv.hr,
- Autorizirani djelatnici tijela javne uprave (npr. ministarstva, agencije i dr.),

- Informacijski sustavi tijela javne uprave,
- Građani i poslovni subjekti.

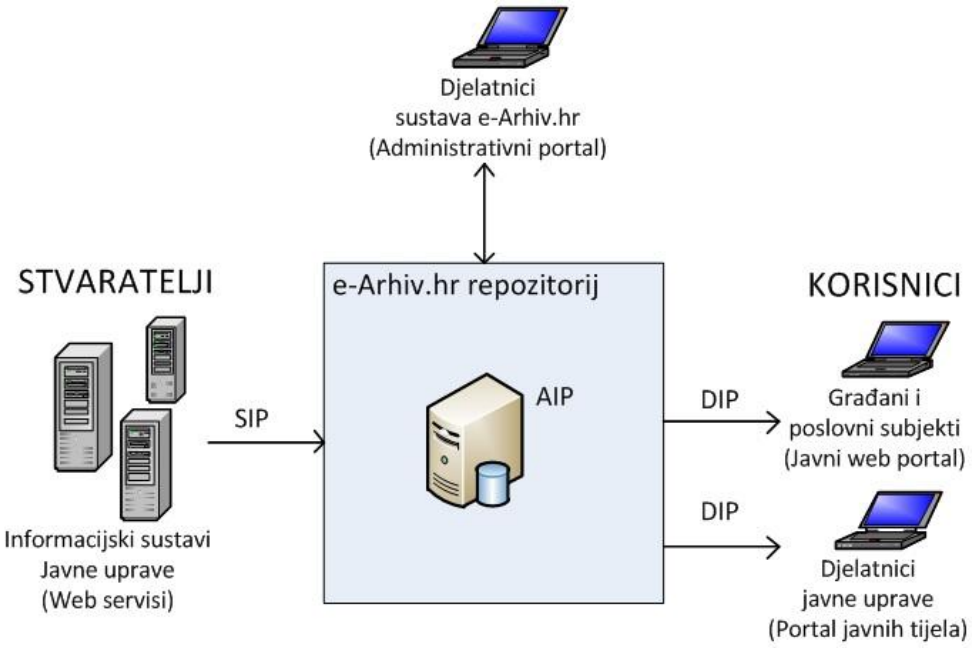
Djelatnici sustava e-Arhiv.hr trebaju imati pristup sustavu kroz web portal za administraciju sustava e-Arhiv.hr (u nastavku Administrativni portal). Administrativni portal treba biti vidljiv samo unutar institucije koja održava sustav e-Arhiv.hr, a navedeno će se postići podešavanjem na mrežnom segmentu. Djelatnici institucije koja održava sustav će kroz Administrativni portal obavljati administraciju sustava, upravljati podacima i po potrebi obavljati različite pretrage.

Autorizirani djelatnici tijela javne uprave mogu biti iz ministarstava, agencija i drugih tijela čije institucije povjeravaju svoje digitalne zapise na dugotrajno očuvanje u sustav e-Arhiv.hr. Pristup na sustav e-Arhiv.hr treba dati samo djelatnicima institucija koji će biti administratori podataka za svoje institucije te djelatnicima koja za potrebe obavljanja svojih radnih zadataka trebaju imati uvid u arhivirane digitalne zapise preko preuzetih DIP paketa. Navedeni djelatnici trebaju imati pristup preko web portal za tijela javne uprave (u nastavku Portal javnih tijela).

Informacijski sustavi javne uprave se trebaju moći spajati na informacijski sustav e-Arhiv.hr preko web servisa. Preko web servisa bi tijela javne uprave dostavljala svoje SIP pakete u sustav e-Arhiv.hr.

Građani i poslovni subjekti bi preko javnog web portala mogli pristupati arhiviranim digitalnim zapisima preko preuzetih DIP paketa na koje imaju pravo. Sličan koncept pristupa na e-Arhiv preko internog (za korisnike iz državnih arhiva) i vanjskog portala (za sve ostale korisnike) ima i litvanski EAIS arhivski sustav koji je obrađen u poglavlju 9.4 Litva – EAIS. Slično je implementirano i u e-arhivu zdravstvenog sustava Vicenze u Italiji koji je obrađen u poglavlju 9.8 Italija – Vicenza zdravstveni sustav. U tom slučaju interni portal koriste liječnici i medicinsko osoblje, a vanjski portal koriste preko interneta građani i njihovi ovlaštenici radi pristupanja vlastitoj medicinskoj dokumentaciji.

U nastavku slijedi slika koja prikazuje vezu različitih korisničkih uloga i sustava e-Arhiv.hr (napomena: slika ne prikazuje arhitekturu sustava e-Arhiv.hr već je pojednostavljena skica radi uvida u različite načine pristupa sustavu).



Slika 58. Pristup različitih vrsta korisnika na sustav e-Arhiv.hr

Za pristup sustavu e-Arhiv.hr bi se trebao koristiti sustav e-Građanin i Nacionalni identifikacijski i autentifikacijski sustav (NIAS) kao jedinstveno mjesto verifikacije elektroničkog identiteta za pristup elektroničkim javnim uslugama. Slično je napravljeno u estonskom modelu nacionalnog elektroničkog arhiva gdje se koristi estonska e-ID kartica ili mobilni eID (navedeno je opisano u poglavlju 9.7 Estonija – Elektronički arhivi Nacionalnog arhiva). Sustav e-Građanin i NIAS su već detaljnije opisani u poglavlju 6.3. Elektronička javna uprava u Republici Hrvatskoj pa se ovdje neće zasebno opisivati.

U nastavku je dan tablični prikaz odnosa korisničkih uloga (rola) koje koriste sustav e-Arhiv.hr, razine vjerodajnice koje trebaju imati za pristup sustavu, te OAIS paketa koju koriste.

Tablica 15. Tablica odnosa korisničkih uloga sustava e-Arhiv.hr, vjerodajnica koje je potrebno koristiti te odnos s OAIS paketima

Rola korisnika	**Razina NIAS vjerodajnice potrebne za pristup**	**SIP**	**AIP**	**DIP**
Djelatnici sustava e-Arhiv.hr	Najviša razine (4 - kvalificirani hard certifikat)	+	+	+
Autorizirani djelatnici tijela javne uprave	Najviša razine (4 - kvalificirani hard certifikat)			+
Informacijski sustavi tijela javne uprave	Aplikacijski i SSL certifikati	+		
Građani i poslovni subjekti	Srednja razina (3 - soft certifikat ili uređaj za OTP, soft certifikat ili uređaj za OTP, hard certifikat)			+

Razine sigurnosti mogu biti od najniže razine (2 – zaporka ili PIN), srednje razine (3 - soft certifikat ili uređaj za OTP, soft certifikat ili uređaj za OTP, hard certifikat) do najviše razine (4 - kvalificirani hard certifikat).

10.3 STANDARDI I FORMATI

U ovom poglavlju će biti dani prijedlozi standarda i formata za sustav e-Arhiv.hr s obzirom na obrađene studije slučajeva, referentne modele i relevantne studije modela za dugotrajno očuvanje elektronički potpisanih dokumenata.

Formati podataka

Predlažem sljedeće formate:

- XML AIP – podaci, metapodaci i verifikacijski podaci koji trebaju biti očuvani na dugi rok trebaju biti spremljeni i upravljani kao samostalni AIP paket koji je temeljen na XML sintaksi. AIP paketi koju su temeljeni na XML sintaksi

omogućavaju neutralnost od platforme i alata te omogućavaju migraciju arhiviranih podataka uz očuvane dokaze postojanja. Na razini sintakse, XML kao tekstualni metajezik podržava automatsku obradu logički strukturiranih podataka te visok stupanj fleksibilnosti. S druge strane, na semantičkoj razini definicija pravila i strukture u XML sintaksi koje se odrađuje pomoću XML sheme podržava mapiranje strukturiranih modela sadržaja. XML sheme su te koje omogućavaju strojno čitljivi opis XML rječnika koji je dopušten za razmjenu podataka, a osim toga pomoću njih se mogu razviti i složene strukture podataka te formulirati uputa za obradu. Za XML AIP je bitno postojanje identifikatora preko kojeg se u sustavu e-Arhiv.hr može svaki AIP jedinstveno voditi i po potrebi pretražiti. Za sustav e-Arhiv.hr predlažem imenovanje identifikatora kao ID_XML_AIP,

- ASCII (engl. American Standard Code for Information Interchange) - BSI tehnički priručnik 03125[674] za TR-ESOR referentni sustav e-Arhiva propisuje da se svaki sadržaj zaprimljen na očuvanje koji je u ASCII formatu može kao takav umetati u XAIP paket. Godine 1972. standard ISO-646[675] je definirao način prilagođavanja nacionalnim abecedama pa je tako inačica za hrvatsku abecedu danas poznata pod nazivom CROSCII,
- XML kao jedan od predloženih formata ulaznih podataka,
- PDF/A – Schwalm[676] za PDF/A prepoznaje da se za potrebe izgradnje servisa za očuvanje dokaza postojanja i podataka treba izraditi i modul za validaciju i konverziju izvornih podataka u PDF/A formatu (izvorni podaci mogu se pohraniti u AIP sukladno poslovnim zahtjevima). Ovaj format opisan je u poglavlju 8.4 Norme za dugoročno očuvanje elektroničkih dokumenata.
- Base64 kodiranje podataka – učitavanje dokumenata u binarnom formatu u e-Arhiv.hr sustav bi omogućilo veliku fleksibilnost prema proizvođačima koji šalju svoje SIP pakete na dugotrajno očuvanje. Dokumenti u binarnom formatu bi se na taj način mogli zapisati u XML AIP. Međutim, unos binarnih podataka u XML AIP

[674] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile, str. 26 (05.03.2018)
[675] ASCII, https://hr.wikipedia.org/wiki/ASCII (11.03.2018.)
[676] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 138. (131-144) (05.03.2018.)

bez izmjene takvih binarnih datoteka može uzrokovati probleme i dovesti do neovisnosti o softveru i/ili platformi. Zbog toga se binarni podaci prvo moraju kodirati u oblik neovisan o platformi. Danas je najšire prihvaćena metoda za kodiranje – Base64 kodiranje podataka sukladno RFC 4648[677]. BSI tehnički priručnik 03125[678] za TR-ESOR referentni sustav e-arhiva propisuje da će se sav sadržaj zaprimljen na očuvanje koji nije u ASCII formatu prvo kodirati u Base64 pa onda umetati u XAIP paket. Stoga smatram kako je to vrlo dobro rješenje pa predlažem usvajanje ove prakse. Dakle, u sustavu e-Arhiv.hr bi se svaki sadržaj koji nije u ASCII formatu prije umetanja u XML AIP paket prvo kodirao u Base64,

- Ostali formati koji bi bili podržani su: TIFF, PNG, WAV, MPEG-2. Prepoznao sam potrebu da se podrže i navedeni formati u sustavu e-Arhiv.hr. Razlog je navođenje istih od strane estonskog Elektroničkog arhiva[679] i njemačkog BSI tehničkog priručnika 03125[680] koje sam prepoznao kao dobre modele i prakse za implementaciju elektroničkog arhiva za područje javne uprave.

Formati elektroničkog potpisa

Schwalm i Korte predlažu sljedeće ETSI formate elektroničkog potpisa: CAdES i XAdES[681] za koje osobno smatram da ih i sustav e-Arhiv.hr treba prihvaćati. Već spomenuta ETSI istraživačka studija servisa za dugotrajnu pohranu podataka navodi pogodnost AdES obitelji naprednih elektroničkih potpisa za dugotrajnu pohranu (i to CAdES i XAdES)[682], a posebno potpisa koji osiguravaju dugotrajnu dostupnost i integritet

[677] RFC 4648 - The Base16, Base32, and Base64 Data Encodings; https://tools.ietf.org/html/rfc4648 (11.03.2018.)
[678] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile, str. 32 (05.03.2018)
[679] Arhiivivormingud, https://www.riigiteataja.ee/aktilisa/1291/2201/1229/VV181_lisa1.pdf (16.03.2018.)
[680] BSI (2015.), Annex TR-ESOR-F - Formats, BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/PrevVersion/TG-03125AnnexTR-ESOR-F.pdf?__blob=publicationFile , str. 24 (06.03.2018.)
[681] Schwalm, S., Korte, U. (2014.), Standards for the Preservation of Evidence and Trust for Electronic Records, IS&T Archiving 2014 Conference, Berlin, https://www.researchgate.net/publication/263474467_Standards_for_the_Preservation_of_Evidence_and_Trust_for_Electronic_Records , str. 4 (10.03.2018.)
[682] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 23 (06.03.2018.)

validacijskog materijala. Oni, naime, imaju prednost da su samostalni, a ako se po potrebi obnavljaju, tada sadrže sve podatke koji omogućavaju provjeru potpisa nakon duže vremena. Budući da se AdES obitelj potpisa temelji na standardiziranim formatima, takvi potpisi imaju visok stupanj interoperabilnost te se lako mogu migrirati iz jednog servisa za dugotrajno očuvanje u drugi servis. ETSI istraživačka studija navodi nedostatak, a to je da je općenito jedan vremenski žig potreban za zaštitu jednog paralelnog potpisa. Estonski model nacionalnog Elektroničkog arhiva opisan u poglavlju 9.7 Estonija – Elektronički arhivi Nacionalnog arhiva navodi XAdES kao prikladan forrmat potpisa. U poglavlju 10.1 Očuvanje dokaza postojanja sam naveo prijedlog za suživot dva modela očuvanja elektronički potpisanih dokumenata (model očuvanja dokaza postojanja (ERS/XMLERS) te modelu samostalnog produženja potpisa) tako da bi ovaj nedostatak rezultirao samo periodičnim pojedinačnim potpisivanjima manjeg broja potpisanih dokumenata u sustavu e-Arhiv.hr što ne bi pretjerano utjecalo na povećanje troškova samog sustava. Naime, za ovaj drugi model bi se trebao koristiti zaseban vremenski žig za svaki dokument što za koncept Merkleovog reduciranog hash stabla nije slučaj (temelj ERS/XMLERS modela).

Dakle, što se tiče formata elektroničkog potpisa, predlažem sljedeće formate koji su obrađeni u poglavlju 4. Napredni elektronički potpis kao podloga za dugoročno očuvanje elektroničkih zapisa:

- CAdES,
- XAdES,
- PAdES.

Predlažem uzeti u obzir i PAdES format naprednog elektroničkog potpisa koji Schwalm i Korte te ETSI istraživačka studija nisu predložili. Razlog je pravni koncept elektroničke isprave. Naime, unutrašnji obrazac elektroničke isprave omogućava da se različite informacije u ispravi mogu strukturirati. Informacije se unutar unutrašnjeg obrasca mogu lakše strukturirati, procesirati te lakše spremati i kasnije pretraživati. Naime, u poglavlju 8. Aspekti elektronički potpisanih dokumenata je spomenut OCD, tj. raznovrsni spremnik za eDokumente iz SPOCS projekta koji može biti temeljen na PDF formatu. PDF koristi mehanizam PDF-a s privicima te naprednog elektroničkog potpisa (PAdES) za

osiguravanje autentičnosti[683]. Kod OCD-a temeljenog na PDF-u glavna datoteka služi za vizualni prikaz OCD metapodataka (time je pokriven vanjski obrazac). Sve ostale datoteke se kao privici dodaju u glavnu OCD PDF datoteku (time se pokriva unutrašnji obrazac). Prednost PDF datoteke (koja može biti tehnologija za implementaciju elektroničke isprave) je što je to samostalna aplikacija (preduvjet za njezino korištenje je odgovarajuća verzija preglednika za PDF format). Svojstva elektroničke isprave kao samostalne aplikacije su velika prednost za aktere u elektroničkoj javnoj upravi (široka prihvaćenost PDF formata, jednostavnost korištenja te velik broj instaliranih PDF preglednika). Kako bi se sačuvala interoperabilnost u dugom roku, PDF dokumenti potpisani PAdES potpisom bi prilikom prihvata u sustav u XML AIP ušli kao Base64 kodirani podaci.

Definicija tehničkih metapodataka

Za definiciju tehničkih metapodataka, predlažem PREMIS. Naime, kroz istraživanja u ovom radu, proučene studije slučajeva i referentne modele, PREMIS se pokazao kao najčešće korišten standard za metapodatke. PREMIS je obrađen u poglavlju 5.2 Bilježenje traga o elektroničkim potpisima u metapodacima. Provedba E-ARK specifikacije se sastoji od dva osnovna elementa: fiksne fizičke strukture informacijskog paketa i točne uporabe metapodataka u METS i PREMIS formatima[684]. Schwalm[685] predlaže PREMIS za definiciju tehničkih metapodataka za potrebe izgradnje servisa za očuvanje dokaza postojanja i očuvanje podataka. BSI tehnički priručnik 03125 za formate[686] navodi da se za specifikaciju metapodataka određenih klasa mogu koristiti događaji definirani u PREMIS standardu metapodataka.

[683] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (21.08.2017.)
[684] DLM Archival Standards Board (2017.), Common Specification for Information Packages v1.0, http://www.dasboard.eu/images/Specifications/CS/Common_Specifications_for_IPs_v10.pdf (06.03.2018.)
[684] E-ARK SIP, http://www.dasboard.eu/images/Specifications/SIP/General_SIP-Specification_v1.4.pdf, str. 24. (06.03.2018.)
[685] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business
Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 138. (131-144) (05.03.2018.)
[686] BSI (2015.), Annex TR-ESOR-F - Formats, BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/PrevVersion/TG-03125AnnexTR-ESOR-F.pdf?__blob=publicationFile , str. 16 (06.03.2018.)

10.4 ARHITEKTURA I FUNKCIONALNOSTI INFORMACIJSKOG SUSTAVA

Ovdje predložena arhitektura informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata za sustav e-Arhiv.hr temelji se na istraženim informacijskim sustavima u ovom radu.

Definitivno se OAIS (ISO 14721:2012[687]) kao referentni model za izgradnju sustava za dugotrajnu pohranu gradiva nametnuo kroz cijeli ovaj istraživački rad. Gotovo svi istraženi sustavi i modeli su ga prepoznali i implementirali. Magenta knjiga kojom se definira **O**tvoreni **A**rhivski **I**nformacijski **S**ustav[688] navodi da OAIS model (kasnije poznat i kao ISO 14721:2003) pruža referentni model ili okvir na visokoj razini koji identificira sudionike digitalnog očuvanja, njihove uloge i odgovornosti te vrste informacija koje će biti razmijenjene tijekom prihvata i pohrane te diseminacije iz digitalnog repozitorija. OAIS model je u ovom radu detaljno obrađen u poglavlju 2. OAIS – referentni model za elektronički arhiv.

ETSI studija predlaže dva osnovna modela servisa za dugotrajno očuvanje digitalnog sadržaja:

- Očuvanje s pohranom[689] (engl. Preservation with storage),
- Očuvanje bez pohrane[690] (engl. Preservation without storage).

Ova dva modela se razlikuju s obzirom na dostupnost podataka. Dostupnost podataka osigurava se na način da se digitalni objekti negdje pohrane. Digitalni objekti se mogu pohraniti na strani servisa (e-arhiva) ili na strani klijenta. U prvom slučaju je riječ o modelu očuvanja s pohranom, a u drugom slučaju o modelu očuvanja bez pohrane. U drugom slučaju je obveza sigurnog pohranjivanja podataka prebačena na stranu klijenta.

---

[687] ISO (2012.), ISO 14721:2012, http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683 (07.08.2016.)

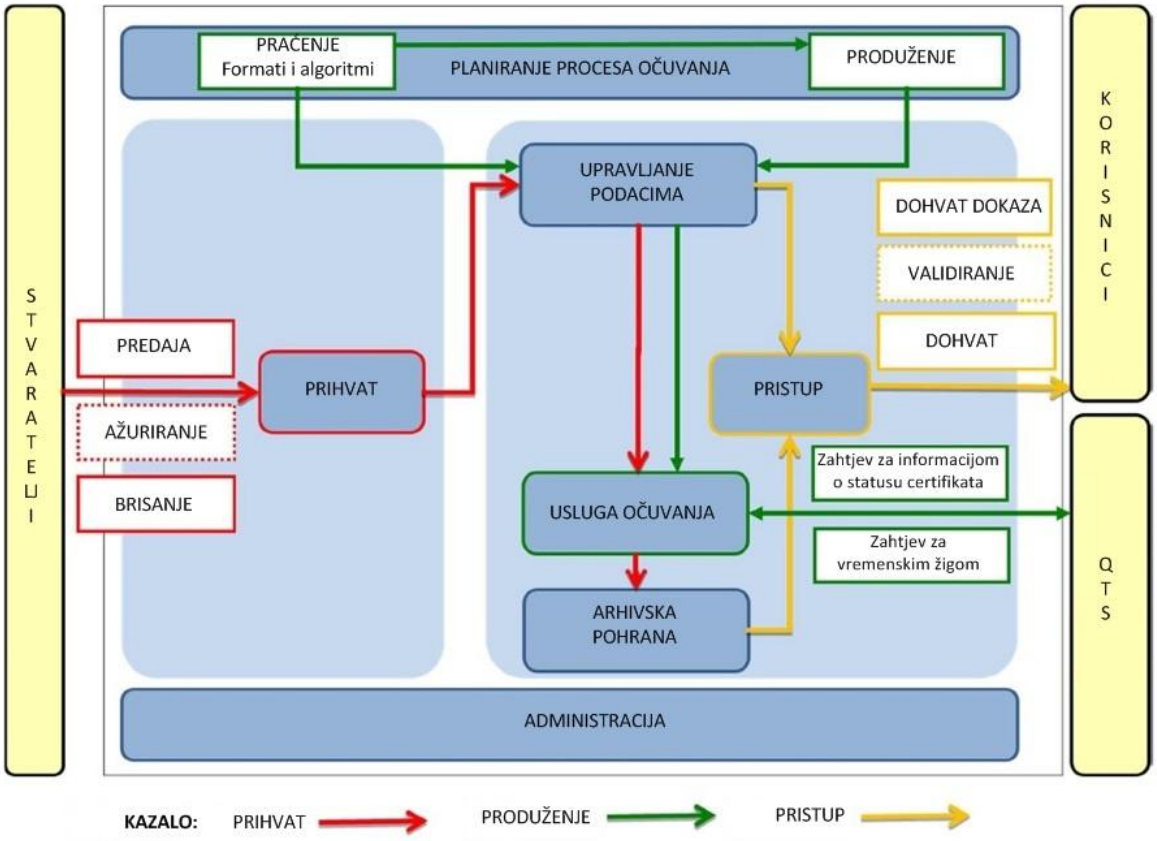
[688] Consultative Committee for Space Data Systems (2012.), Reference model for an open archival information system (OAIS) - 062012 - Magneta book, str. 2-2, http://public.ccsds.org/publications/archive/650x0m2.pdf (07.08.2016.)

[689] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 17 (11.03.2018.)

[690] Isto, str. 18

Predlažem za sustav e-Arhiv.hr model očuvanja s pohranom.

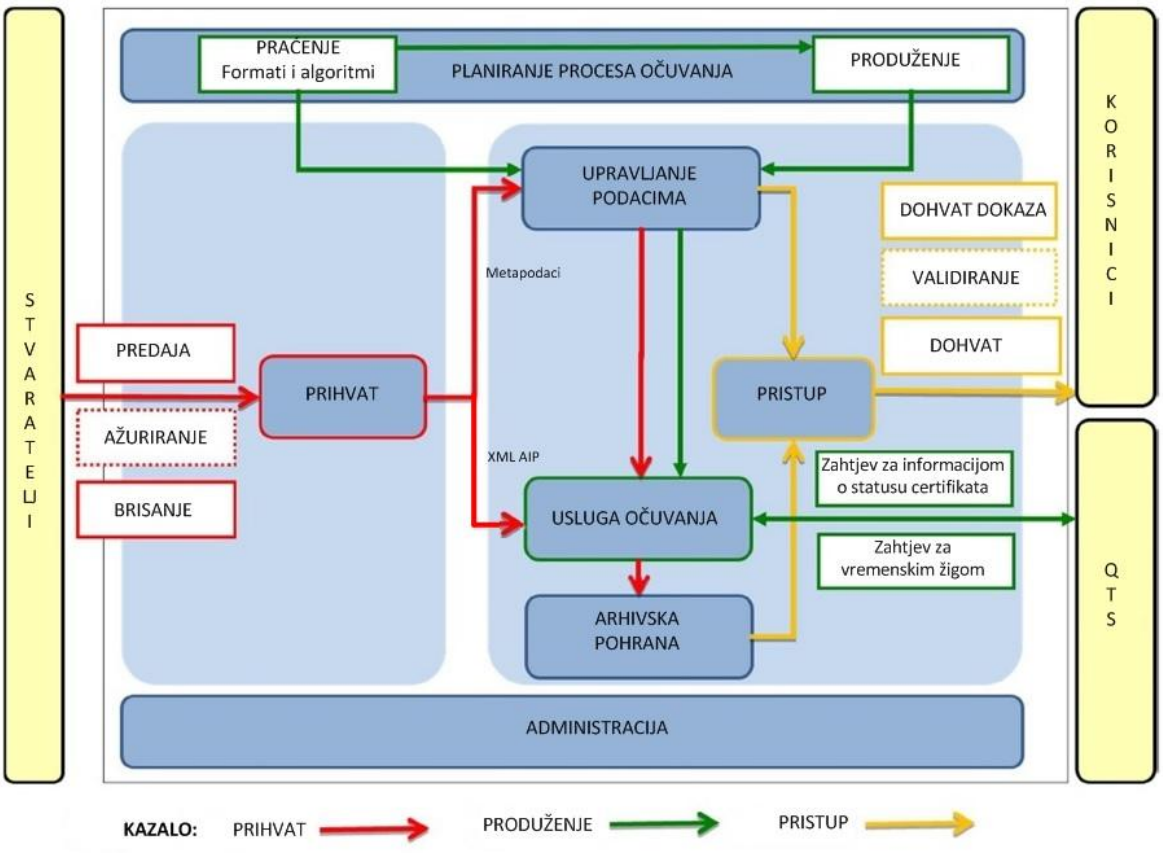
Na slici 59 je dan prikaz OAIS sukladnih proces prihvata (engl. Ingest) i pristupa (engl. Access) za odabrani model očuvanja s pohranom kako ga predlaže ETSI studija.



Slika 59. ETSI - OAIS sukladni procesi prihvata (engl. Ingest) i pristupa (engl. Access), preuzeto iz ETSI (2017.)[691]

Na slici 60 se nalazi prijedlog modifikacije na slici 59 prikazanog ETSI-OAIS modela sukladnih procesa prihvata i pristupa. Predlaže se direktna veza entiteta Prihvata i Usluge očuvanja kako je prikazano na donjoj slici. Direktna veza entiteta Prihvata i Upravljanja podacima treba ostati (zbog prijenosa metapodataka), ali se uvodi i direktna veza između entiteta Prihvata i Usluge očuvanja (zbog postupka izrade dokaza postojanja).

[691] Isto, str. 33, slika A-3



Slika 60. Modifikacija ETSI - OAIS modela za potrebe izrade koncepta sustava e-Arhiv.hr

U nastavku teksta slijedi opis operacija (engl. operations) iz ETSI modela očuvanja s pohranom[692]. Operacije iz ETSI modela ostaju iste bez obzira na napravljenu modifikaciju.

Predaja (engl. Deposit): proizvođač šalje digitalni objekt (SIP paket) u sustav e-Arhiv.hr. Sustav e-Arhiv.hr izvršava interne procese za očuvanje digitalnog objekta. Nakon toga sustav e-Arhiv.hr vraća stvaratelju identifikator AIP paketa (u nastavku teksta ID_XML_AIP) te može na zahtjev stvaratelja vratiti zapis dokaza postojanja. Ova operacija je dio OAIS procesa prihvata (engl. ingest).

Dohvat (engl. Retrieve): ovlašteni subjekt koji može biti različit od stvaratelja (npr. može postupati po ovlaštenju) šalje ID_XML_AIP sustavu e-Arhiv.hr. Osim toga, može zatražiti odgovarajuće očuvane dokaze. Servis očuvanja može vratiti DIP paket tražitelju sa zapisom dokaza postojanja. Ova operacija je dio OAIS procesa pristupa (engl. Access).

[692] Isto, str. 17

Dohvat dokaza (engl. Retrieve proof): ovlašteni subjekt koji može biti različit od stvaratelja šalje ID_XML_AIP i može zatražiti zapise dokaza postojanja ili neke njegove dijelove. Ova operacija se može implementirati kao dio operacije dohvata.

Brisanje (engl. Delete): ovlašteni subjekt koji može biti različit od stvaratelja šalje ID_XML_AIP i dodatne informacije (npr. informacije o autentifikaciji i autorizaciji, informacije koje navode razlog brisanja) te time traži brisanje određenog XML AIP paketa, zapisa dokaza postojanja i pridruženih metapodataka. Brisanje može biti pokrenuto i automatiziranim postupkom (npr. periodičkim pokretanjem aplikacije za brisanje XML AIP paketa sukladno propisanim politikama očuvanja gradiva). Operacija brisanja je dio OAIS procesa prihvata (engl. ingest).

Ažuriranje pohranjenih zapisa (engl. Update stored elements), nije obavezna operacija: ovlašteni subjekt koji može biti različit od stvaratelja šalje e-Arhiv sustavu ID_XML_AIP i paket s opisom željenih promjena na spremljenom XML AIP paketom (engl. Delta AIP). Originalno spremljeni XML AIP se potom ažurira u skladištu podataka te nastaje nova verzija XML AIP paketa. Korisniku se vraća identifikator ažuriranog XML AIP paketa (engl. VersionID) s ažuriranim dokazom postojanja. Originalni XML AIP te ID_XML_AIP su također očuvani.

Praćenje (engl. Monitor): ova operacija nije izložena na sučelju, već ga sustav e-Arhiv.hr treba interno aktivirati (ručno ili automatski) prema definiranim procedurama očuvanja digitalnih objekata. Ova operacija prati različite događaje koji bi mogli ugroziti mogućnost provjere dokaza postojanja. Ova metoda po potrebi (npr. rizik nesukladnosti kriptografskog algoritma) može pokrenuti operaciju produženja (engl. augmentation). Ova operacija je dio procesa produženja u ovom modelu.

Produženje (engl. augmentation): ova se operacija aktivira interno kako bi se osiguralo očuvanje XML AIP paketa na dugi rok. Produženjem se osigurava valjanost XML AIP paketa u skladu s ciljevima očuvanja te da bi se produžilo razdoblje tijekom kojeg se dokazi postojanja mogu provjeriti. U slučaju kada se koriste zapisi dokaza postojanja (ERS/XMLERS) produženje se može obaviti obnavljanjem vremenskog žiga ili obnavljanjem hash stabla. U slučaju kada se koristi elektronički potpis, produženje se može

obaviti dodavanjem novog arhivskog atributa ili svojstva (npr. po modelu samostalnog uvećanja potpisa kao za AdES obitelj LTV potpisa).

Na gore navedenoj slici je uz šest funkcionalnih OAIS entiteta (Prihvat, Arhivska pohrana, Upravljanje podacima, Administracija, Planiranje procesa očuvanja i Pristup) dodan za potrebe ovog OAIS sukladnog modela i entitet Usluga očuvanja (engl. Preservation service). Na slici je prikazano i izvođenje zahtjeva za informacijom o statusu certifikata (engl. Request Certificate Status Info) i zahtjeva za vremenskim žigom (engl. Request Timestamp) od strane sustava e-Arhiv.hr (i u njemu Usluge očuvanja) prema vanjskim kvalificiranim servisima od povjerenja (QTS, Qualified Trust Services). Zahtjevi za servise od povjerenja su definirani Uredbom eIDAS[693]. Navedeni zahtjevi se s pomoću entiteta Usluge očuvanja izvode u svrhu procesa produženja zapisa dokaza postojanja ili obnavljanja elektroničkog potpisa. Funkcionalnosti entiteta Usluge očuvanja su detaljno opisane za:

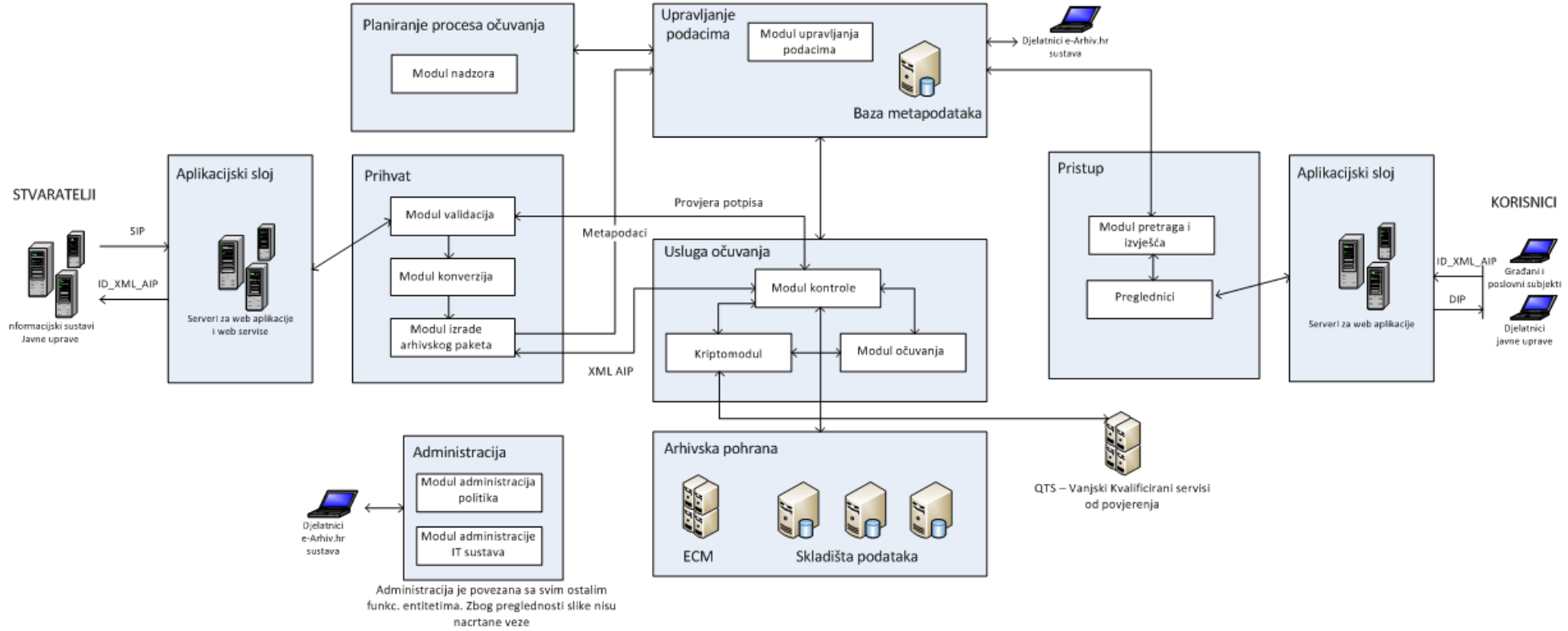
- očuvanje dokaza postojanja u poglavlju 10.1 Očuvanje dokaza postojanja,
- obnavljanje elektroničkih potpisa (AdES obitelj naprednog elektroničkog potpisa) u poglavlju 4.4 Izrađivanje naprednog elektroničkog potpisa.

ETSI studija za ovaj model očuvanja s pohranom navodi[694] i mogućnost da pohrana ne bude pod kontrolom e-arhiva. Ako se za taj slučaj žele postići ciljevi dostupnosti, povjerljivosti i integriteta, možda će trebati kriptirati pohranjene podataka, primijeniti dodatne mehanizme zaštite integriteta i koristiti redundantnu pohranu tako da podaci ostanu dostupni čak i ako dio pohrane nije pouzdan. Stoga predlažem za sustav e-Arhiv.hr model očuvanja s pohranom kod kojeg je pohrana pod kontrolom sustava e-Arhiv.hr.

Na slici 61 je prikazana arhitektura sustava e-Arhiv.hr.

[693] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, članak 3. Definicije, L 257/96, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (12.03.2018.)

[694] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 17 (06.03.2018.)



Slika 61. Arhitektura sustava e-Arhiv.hr

Što se tiče prikazane arhitekture bitno je napomenuti da je Aplikacijski sloj koji je vezan za entitete Pristupa i Prihvata u stvari jedna te ista fizička implementacija. Na slici je to, na logičkoj razini, prikazano odvojeno. Predlažem za aplikacijski sloj koji je vezan i na entitet Prihvata i na entitet Pristupa, smještaj web i aplikacijskih servera na kojima će biti sljedeće aplikacije:

- modul za komunikaciju sa sustavom e-Građanin (preko NIAS vjerodajnica),
- web portal javnih tijela,
- javni web portal (za građane i poslovne subjekte),
- web servisi za spajanje tijela javne uprave.

U nastavku slijedi opis funkcionalnosti sustava e-Arhiv.hr po šest osnovnih OAIS funkcionalnih entiteta i naknadno dodanog entiteta Usluge očuvanja (engl. Preservation service).

Prihvat (engl. Ingest) – u ovom entitetu se prihvaćaju podaci poslani od stvaratelja i pripremaju se za arhiviranje. U ovom etnitetu bi se obavljale sljedeće operacije objašnjene u prethodnom tekstu: predaja, ažuriranje arhiviranih zapisa, brisanje. Od funkcionalnosti za ovaj entitet je bitno implementirati: validaciju SIP paketa, validaciju sadržaja, validaciju potpisa (pozivom na Kriptomodul u entitetu Usluge očuvanja), konverzije iz formata u format (npr. konverziju u PDF/A format), izradu metapodataka (predlažem PREMIS standard), izradu XML AIP paketa (zapis dokaza postojanja bi se izradio pozivom Modula očuvanja iz entiteta Usluge očuvanja). U ovom entitetu bi se implementirali sljedeći moduli: Modul validacije, Modul konverzije i Modul izrade arhivskog paketa. Između stvaratelja i entiteta Prihvata bi bio smješten Aplikacijski sloj. Sljedeći koncept kreiranja zapisa dokaza postojanja i razmjene među OAIS entitetima preuzet je iz BSI tehničkog priručnika 03125[695]. Modul izrade arhivskog paketa predaje privremenu verziju XML AIP paketa entitetu Usluge očuvanja. U modulu očuvanja se provjerava očekivani XML AIP format te se privremeni XML AIP predaje Kriptomodulu da bi se dobio dokaz postojanja. Kriptomodul vraća dokaz postojanja Modulu očuvanja koji na osnovu toga arhivski paket dodaje u hash stablo da bi se izradio zapis dokaza postojanja (XMLERS). Ovaj zapis dokaza postojanja uz njegov jedinstveni identifikator (ID_XML_AIP) se vraća kao

[695] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile, str. 41 (05.03.2018)

odgovor u entitet Prihvata u Modul izrade arhivskog paketa gdje se konačno pakira u arhivsku verziju XML AIP paketa. Nakon pakiranja arhivske verziju XML AIP paketa ona se preko entiteta Usluge očuvanja (te Modula kotrole) arhivira u entitet Arhivske pohrane. ID_XML_AIP će kasnije biti potreban za dohvaćanje izrađenog arhivskog paketa (XML AIP) od strane svih rola u sustavu e-Arhiv.hr. U slučaju da se u XML AIP sprema potpisani dokument s naprednim LTV potpisom iz AdES obitelji potpisa koji je po pravnoj prirodi elektronička isprava, tada nije potrebno obaviti dohvaćanje zapisa dokaza postojanja jer je takav potpis samostojeći (engl. self-contained) o čemu je već pisano u poglavlju 10.1 Očuvanje dokaza postojanja. U tom slučaju se prije arhiviranja XML AIP paketa u entitet Arhivske pohrane samo provjerava potpis pomoću funkcionalnosti Kriptomodula.

Arhivska pohrana (engl. Archival Storage) – upravlja se dugotrajnim očuvanjem digitalnih sadržaja. U ovom entitetu je bitno implementirati ECM sustav te odgovarajuća skladišta podataka. O sigurnosnim zahtjevima nad skladištima podataka će biti više navedeno u poglavlju 10.5 Ostali zahtjevi.

Upravljanje podacima (engl. Data Management) – u ovom se entitetu održava baza podataka opisnih metapodataka koji identificiraju i opisuju arhivirane podatke u entitetu arhivske pohrane. Funkcije ovog OAIS entiteta su i: izrada izvješća kroz postavljanje upita nad bazom podataka, pohranjivanje i izmjene informacija o pristiglim paketima, brisanje informacija iz sustava te za održavanje administrativnih podataka OAIS arhiva. U ovom entitetu navedene funkcije obavlja Modul upravljanja podacima. Za bazu metapodataka važno je kvalitetno održavanje indeksa.

Pristup (engl. Access) – obavlja se zahtijevanje i pronalaženje arhiviranih podataka iz entiteta arhivske pohrane. U ovom etnitetu bi se obavljale sljedeće operacije objašnjene u prethodnom tekstu: dohvat, dohvat dokaza. U ovom entitetu bi se trebale osigurati sljedeće funkcionalnosti: provjera prava korisnika na sadržaj (autorizacija), razna pretraživanja (po zadanim kriterijima od korisnika), dohvaćanje izvješća, pretvaranje dohvaćenog XML AIP paketa u DIP. Navedene funkcije bi obavljao Modul pretraga i izvješća. Osim tog modula, za ovaj entitet je potrebno implementirati preglednike za elektroničke dokumente te vizualizaciju elektroničkih potpisa i dokaza postojanja. Između korisnika i entiteta Pristupa bi bio smješten Aplikacijski sloj.

Planiranje procesa očuvanja (engl. Preservation Planning) – ovaj entitet je zadužen za praćenje promjena i rizika na relevantnim tehnologijama, formatima, kriptografskim algoritmima i dr. U ovom etnitetu bi se obavljala operacija Praćenje (objašnjena u prethodnom tekstu). Modul koji bi navedeno obavljao je Modul nadzora. U modulu nadzora je potrebno omogućiti promjene u formatima arhiviranih dokumenata. Naime, promjenom formata koji nisu temeljeni na otvorenim standardima (npr. XML) potrebno je uzeti u obzir i konverziju u tom formatu arhiviranih dokumenata. Naime, potrebno je omogućiti i upotrebljivost dokumenata i nakon dužeg roka pohrane u sustavu e-Arhiv.hr. Vodeći se potrebom za konverzijom formata arhiviranih dokumenata, Haber i Kamat[696] predlažu tehniku za izmjenu sadržaja dokumenta ne brisanjem ili mijenjanjem originalnog dokumenta već pohranjivanjem opisa obavljenih izmjena te izmijenjenog dokumenta zajedno s originalnim dokumentom. Autori navedenu tehniku spominju u kontekstu problematike zastarijevanja formata dokumenata i softvera koji s njima rukuje. Time se rješava problematika čitljivosti dokumenata u dugom roku. Ova tehnika podrazumijeva konverziju na novije verzije formata dokumenta, a uvjetuje i pohranjivanje algoritma kojim je obavljena transformacija da bi se stvorila povijest zapisa promjena između izvornog i konačno preoblikovanog dokumenta. Time se za pohranjeni dokument osigurava i povijest promjena (engl. version history). Tako pohranjeni zapis transformacija osigurava utvrđivanje da izvorni i konačno preoblikovani dokument sadrže isti sadržaj.

Administracija (engl. Administration) – to je etnitet koji je zadužen za upravljanje svakodnevnim aktivnostima unutar sustava e-Arhiv.hr. Planirani moduli u ovom entitetu su Modul administracije politika očuvanja koji upravlja politikama očuvanja (engl. preservation policies) te Modul administracije IT sustava koji se odnosi na administriranje računalnim komponentama unutar sustava e-Arhiv.hr (od aplikacija do skladišta podataka). Ova dva modula bi trebali koristiti isključivo djelatnici sustava e-Arhiv.hr. OAIS etnitet Administracije je povezan sa svim drugim funkcionalnim etnitetima, ali zbog preglednosti slike nisu nacrtane relacije s drugim etnitetima.

Usluga očuvanja (engl. Preservation service) – ovaj entitet je za potrebe sustava e-Arhiv.hr dodan na osnovni OAIS referentni model. Tehnički bi se implementirao pomoću

[696] Haber, S., Kamat, P. (2006.), A content integrity service for long-term digital archives, IS&T Archiving 2006 Conference, http://www.hpl.hp.com/techreports/2006/HPL-2006-54.pdf , str. 3 (14.03.2018.)

Kriptomodula koji služi isključivo za obavljanje sljedećih kriptografskih funkcija potrebnih u sustavu e-Arhiv.hr: verifikaciju potpisa, provjeru certifikata, provjeru vremenskih žigova, potpisivanje potpisom, ovjeravanje vremenskim žigom, izračunavanje hash vrijednosti. Osim njega u ovom entitetu bi se implementirali Modul očuvanja i Modul kontrole. Modul kontrole treba zaprimiti sve zahtjeve prema Modulu očuvanja i Kriptomodulu. Preko Modula kontrole se obavlja i spremanje i dohvat XML AIP paketa u entitet Arhivske pohrane gdje se prema potrebi obavljaju dodatne validacije prije isporuke arhivskog paketa korisnicima. Modul očuvanja bi upravljao složenim postupkom izrade i obnavljanja zapisa dokaza postojanja (ERS/XMLERS) te postupkom produženja potpisa. Dakle, u ovom entitetu bi se obavljao najveći dio operacije Produženja (objašnjena u prethodnom tekstu). Za potrebe dohvata informacija o statusu certifikata i vremenskih žigova ovaj entitet bi trebao moći komunicirati s kvalificiranim servisima od povjerenja (QTS).

10.5 OSTALI ZAHTJEVI

U nastavku slijede ostali zahtjevi za izradu sustava e-Arhiv.hr iz područja: sigurnosti pohrane podataka, migracije i topologije informacijskog sustava.

Sigurnost pohrane podataka

Schwalm[697] predlaže koristiti standardnu pohranu neovisnu o specijalnim platformama ili proizvođačima. Predlaže korištenje sigurnosnog koncepta koji uvažava standard ISO 27001[698] da bi se izbjegla neželjena promjena AIP paketa. Schwalm, nadalje, navodi da taj sigurnosni koncept kao i sam elektronički arhiv trebaju biti integrirani u holistički i održivi sustav upravljanja informacijskom sigurnošću. Ovakvim pristupom se izbjegava korištenje skupe WORM[699] (engl. Write Once Read Many) tehnologije kod koje postoji visoka ovisnost o vlasničkoj platformi. Vrijeme zadržavanja digitalnih zapisa u e-arhivima može

[697] Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 140. (131-144) (05.03.2018.)
[698] ISO 27001, the international information security standard, https://www.itgovernance.co.uk/iso27001 (14.03.2018.)
[699] WORM (write once, read many), http://searchstorage.techtarget.com/definition/WORM-write-once-read-many (14.03.2018.)

biti i više desetaka godina pa je zbog toga WORM tehnologija velik rizik za dostupnost takvih zapisa u budućnosti. Vodim se ovom preporukom te predlažem i za sustav e-Arhiv.hr korištenje standardne pohranu neovisne o specijalnim platformama ili proizvođačima.

Migracija zapisa

Što se tiče migracije arhiviranih zapisa iz sustava e-Arhiv.hr u ciljni OAIS kompatibilni arhiv, migracija u drugi e-arhiv će biti moguća u slučaju da je i ciljni arhivski sustav temeljen na otvorenim standardima kao što je XML te korištenju elektroničkih potpisa iz AdES obitelji potpisa. Naime XML AIP paketi (podaci, metapodaci i dokazi postojanja) koji bi bili arhivirani u sustavu e-Arhiv.hr radi očuvanja na dugi rok trebaju biti spremljeni i upravljani kao samostalni AIP paket koji su temeljeni na XML sintaksi. AIP paketi koji su temeljeni na XML sintaksi omogućavaju neutralnost od platforme i alata te omogućavaju migraciju arhiviranih podataka uz očuvane dokaze postojanja.

Što se tiče migracije formata, Haber i Kamat[700] predlažu tehniku za izmjenu sadržaja dokumenta ne brisanjem ili mijenjanjem originalnog dokumenta već pohranjivanjem opisa obavljenih izmjena te izmijenjenog dokumenta zajedno s originalnim dokumentom. Haber i Kamat tvrde da se ova metoda može primijeniti na problematiku zastarijevanja formata dokumenata i softvera koji s njima rukuje, tj. općenito na problematiku čitljivosti. Njihova metoda podrazumijeva migraciju na novije verzije formata dokumenta da bi se osigurala čitljivost dokumenta u budućnosti. Nadalje se pohranjuje algoritam kojim je obavljena transformacija da bi se stvorila povijest zapisa promjena između izvornog i konačno preoblikovanog dokumenta. S tako pohranjenim zapisom transformacija je moguće sa sigurnošću utvrditi da izvorni i konačno preoblikovani dokument sadrže isti sadržaj. Ova metoda ima nedostatak jer primjena algoritma na izvorni dokument možda više neće biti moguća zbog zastarjelosti softvera za pretvorbu arhiviranog sadržaja.
BSI tehnički priručnik 03125[701] navodi da postupci i tehnička rješenja koja se koriste za očuvanje dokaza potpisanih elektroničkih dokumenata ne smiju umanjiti mogućnost

[700] Haber, S., Kamat, P. (2006.), A content integrity service for long-term digital archives, IS&T Archiving 2006 Conference, http://www.hpl.hp.com/techreports/2006/HPL-2006-54.pdf , str. 3 (14.03.2018.)
[701] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2,

nastavka korištenja elektroničkih dokumenata za različite svrhe primjene i u različitim aplikacijskim sustavima. Posebno, ne smije doći do oštećenja zbog postupaka i tehničkih rješenja koja se koriste za obnavljanje potpisa u odnosu na:

- razmjenu dokumenata između aplikacijskih sustava,
- promjenu formata podataka u aplikacijskim sustavima,
- zamjenu aplikacijskih sustava ili komponenti.

Priručnik, nadalje (u svezi promjena formata podataka u aplikacijskim sustavima), navodi da može doći do promjene formata podataka u aplikacijskim sustavima te da mehanizmi za očuvanje dokaza također mogu funkcionirati s novim formatom podataka. Priručnik navodi da se funkcije korištene za produženje potpisa ne smiju ograničavati na posebne formate podataka. Nadalje, navedeni priručnik pretpostavlja[702] da na jednom arhivirane podatke promjene formata ne utječu te da transformacija (potpisanih) podataka nije potrebna. U slučaju da se to ipak dogodi, Priručnik upućuje na rezultate TransiDoc projekta[703].

Predlažem, nastavno na preporuke BSI tehničkog priručnika 03125, da se transformacija potpisanih podataka u sustavu e-Arhiv.hr ne obavlja već da se koriste isključivo otvoreni, općeprihvaćeni standardi (npr. XML) iz razloga izbjegavanja kasnije konverzije formata. Otvorene standarde je potrebno upotrebljavati i zbog interoperabilnosti (migracija arhiviranih potpisanih zapisa iz jednog e-Arhiva u drugi).

Topologija informacijskog sustava

Za topologiju informacijskog sustava su izdvojena tri primjera implementacije: litvanski, estonski (čije su informacije dobivene upitnikom) i slovenski.
Litvanski EAIS sustav je fizički smješten na dvije geografski udaljene lokacije[704] (jedna je u Vilniusu, a druga u Šiauliai). Obavlja se replikacija arhivskih podataka između glavnog i rezervnog podatkovnog centra. U slučaju grešaka ili nesreće moguće je prebaciti aktivnosti s jednog na drugi.

---

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile, str. 31 (05.03.2018)

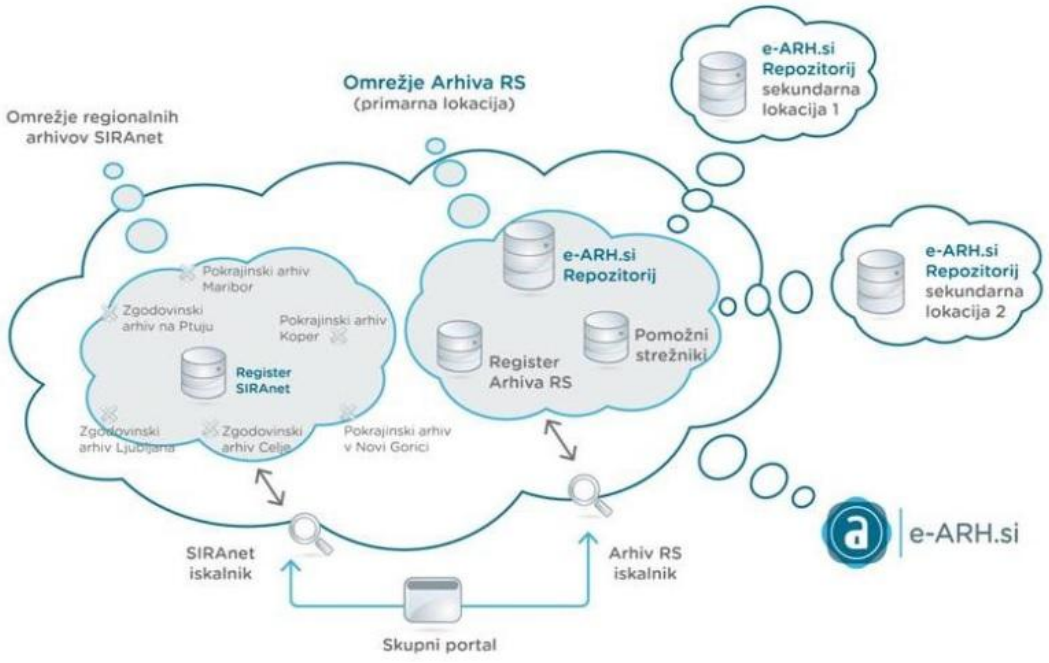
[702] Isto, str. 31 „It is assumed in this Technical Guideline that data that has been archived once is not affected by a format change and that a transformation of (signed) data is thus not necessary.“

[703] TransiDoc projekt, https://wiki.dnb.de/display/NESTOR/TransiDoc (15.03.2018.)

[704] Electronic Archive Information System, Office of the Chief Archivist of Lithuania, http://www.archyvai.lt/en/new/system.html (23.02.2018.)

Elektronički arhivi Nacionalnih arhiva Estonije (engl. Digital Archives of the National Archives of Estonia) su implementirali[705] dvije serverske sobe (u Tallinu i Tartuu). Primarna lokacija za digitalnu pohranu (Preservica) je u Tallinu te se u njemu drži online kopija (disk) i jedan kopija na traci. Sekundarna lokacija je Tartu gdje se također drže jedna online kopija i jedna kopija na traci. Sveukupno estonski elektronički arhivi imaju četiri kopije na dvije lokacije.

Slovenski elektronički arhiv (e-ARH.si) u dokumentu Strategije i izvedbenog nacrta slovenskog elektroničkog arhiva za razdoblje 2016-2020 navodi[706], međuostalim, i topologiju primarne i sekundarnih lokacija u arhitekturi sustava. Kao što je prikazano na slici 62, e-Arh.si repozitorij ima jednu primarnu i dvije sekundarne lokacije.



Slika 62. Arhitektura e-Arh.si sustava s prikazanom topologijom primarne i sekundarnih lokacija, preuzeto iz Arhiv Republike Slovenije (2016.)[707]

[705] Podaci dobiveni upitnikom, a navedeni su u prilogu Prilog 2. Upitnik za digitalne arhive

[706] Arhiv Republike Slovenije (2016.), Strategija in izvedbeni načrt razvoja slovenskega elektronskega arhiva 2016-2020, http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/Strategija_e-ARH.si/Strategija_e-ARH_si_2016-2020_1.0.pdf , str. 19 (14.03.2018.)

[707] Arhiv Republike Slovenije (2016.), Strategija in izvedbeni načrt razvoja slovenskega elektronskega arhiva 2016-2020, http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/Strategija_e-ARH.si/Strategija_e-ARH_si_2016-2020_1.0.pdf , str. 19 (14.03.2018.)

Za implementaciju sustava e-Arhiv.hr predlažem dvije sekundarne lokacije (slovenski model). Jedna od tih dviju sekundarnih lokacija bi imala i funkciju zamjenske lokacije za slučaj katastrofe (engl. disaster location). Primjerice, za slučaj potresa takva zamjenska lokacija bi trebala biti smještena na drugoj tektonskoj ploči.

10.6 PRIJEDLOG ZA USPOSTAVU INFRASTRUKTURE ZA POTPISIVANJE I DUGOTRAJNU POHRANU ELEKTRONIČKI POTPISANIH DOKUMENATA

U ovom poglavlju će biti dan prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata. Sam prijedlog se nastavlja na istraženo i izneseno u prethodnim poglavljima za model informacijskog sustava e-Arhiv.hr. Sam prijedlog ne nudi potpune implementacijske detalje već polazišne postavke, definirane standarde i formate, arhitekturu na logičkoj razini, opise logičkih podsustava te opise ostalih zahtjeva nad sustavom.

Osiguravanje očuvanja dokaza postojanja

Dokaz postojanja, PoE (engl. Proof of Existence) je vrlo bitan pojam za izradu sustava e-Arhiv.hr. U smislu sustava e-Arhiv.hr bit će potrebno izrađivati zapise dokaza postojanja za elektronički potpisane dokumente. Integritet potpisanih zapisa u dugom roku će se izvoditi produženjem potpisa. Sustav e-Arhiv.hr treba kontinuirano pratiti prikladnost primijenjenih kriptografskim algoritama. U slučaju kada bude ugrožena prikladnost korištenih algoritama potpisivanja i pripadajućih parametara za zaštitu, podaci i svi postojeći potpisi trebaju se ponovno potpisati. Navedeni postupak će poslužiti kao osnova očuvanja dokaza postojanja za elektroničke dokumente.

Slijedi popis bitnih postavki sustava e-Arhiv.hr za osiguravanje očuvanja dokaza postojanja:

- aplikacije u aplikacijskom sloju samog sustava (ili potpisni moduli izvan samog sustava) trebaju osigurati da se dokumenti potpišu od strane autoriziranih osoba s propisanim potpisnim procedurama i certificiranim potpisnim komponentama,

- za kasniju provjeru valjanosti elektroničkog potpisa u trenutku njegovog stvaranja potrebno će biti razlučiti vrijeme potpisivanja s kvalificiranog vremenskog žiga s kojim je potpis ovjeren,
- podaci potrebni za provjeru potpisa u budućnosti trebali bi se dohvatiti neposredno nakon izrade i/ili provjere potpisa te trebaju biti arhivirani skupa s dokumentima i ostalim podacima u obliku koji će biti čitljiv i upotrebljiv na dugi rok,
- osim potpisanih podataka potrebno je osigurati integritet nepotpisanih podataka u trenutku prijenosa u ECM sustav na način da se izračuna ulazna hash vrijednost tih podataka ili da se takvi podaci ovjere kvalificiranim vremenskim žigom,
- dohvaćanje vremenskog žiga za svaki elektronički dokument nije ekonomično pa će se dohvaćati jedan vremenski žig na veći broj potpisanih dokumenata,
- ponovno potpisivanje većeg broja elektronički potpisanih zapisa obavljat će se periodički, putem automatiziranog programa o čijem će se pokretanju i obavljanju brinuti sam sustav,
- logirat će se svi koraci provjere potpisa te rezultat provjere. Logiranje navedenih podataka dobivenih provjerom potpisa će se zapisivati u aplikativni log i/ili u bazu podataka,
- za dokazivanje autentičnosti i integriteta podataka koji se čuvaju u sustavu e-Arhiv.hr će se izrađivati i koristiti zapis dokaza postojanja (engl. Evidence record). Koristit će se RFC 6283 standard, XMLERS (zapis dokaza postojanja u XML formatu). Postupak izrade dokaza postojanja je opisan u poglavlju 10.1 Očuvanje dokaza postojanja,
- Koristit će se usluga Službe za izradu kvalificiranog vremenskog žiga (QTSA) radi dohvaćanja kvalificiranog vremenskog žiga u svrhu izrade zapisa o dokazu postojanja te za dohvaćanja informacije o statusu certifikata,
- Omogućit će se očuvanje potpisanih elektroničkih dokumenata na dvojak način:
    - Korištenje XMLERS standarda (RFC 6283) za potpisane elektroničke dokumente koji nemaju pravni karakter elektroničke isprave. tj. za one dokumente koji se mogu u skupu od više dokumenata periodično ovjeravati jednim kvalificiranim vremenskim žigom,
    - po modelu samostalnog produženja potpisa (AdES obitelj LTV potpisa) za elektroničke dokumente koji imaju pravni karakter elektroničke isprave te

koji trebaju zadržati svojstvo unutarnjeg i vanjskog obrasca tijekom cijelog svog dokumentacijskog ciklusa.

Detaljnije o izradi zapisa dokaza postojanja je navedeno u poglavlju 10.1 Očuvanje dokaza postojanja.

Korisničke uloge

Korisničke uloge (role) sustava e-Arhiv.hr bi bile sljedeće:

- Djelatnici sustava e-Arhiv.hr,
- Autorizirani djelatnici tijela javne uprave (npr. ministarstva, agencije i dr.),
- Informacijski sustavi tijela javne uprave,
- Građani i poslovni subjekti.

Detaljnije o korisničkim ulogama je navedeno u poglavlju 10.2 Uloge korisnika i pristup sustavu.

Pristup sustav e-Arhiv.hr

Za pristup sustavu e-Arhiv.hr bi se trebao koristiti sustav e-Građanin i Nacionalni identifikacijski i autentifikacijski sustav (NIAS) kao jedinstveno mjesto verifikacije elektroničkog identiteta za pristup elektroničkim javnim uslugama. Djelatnici sustava e-Arhiv.hr trebaju imati pristup sustavu kroz web portal za administraciju sustava e-Arhiv.hr, autorizirani djelatnici javne uprave kroz web portal za tijela javne uprave, a građani i poslovni subjekti trebaju imati pristup preko javnog web portala. Detaljnije o pristupu sustavu e-Arhiv.hr je navedeno u poglavlju 10.2 Uloge korisnika i pristup sustavu.

Standardi i formati podataka

XML kao otvoreni standard podataka bi bio i temelj za sustav e-Arhiv.hr. Arhivski informacijski paket bi, također bio u XML formatu (XML AIP).

PDF/A je prepoznat kao arhivski format u svim proučenim sustavima u ovom radu te bi on bio preporučeni format i za sustav e-Arhiv.hr.

Svi zapisi koji su u ASCII formatu mogli bi se kao takvi umetati u XML AIP paket.

U sustavu e-Arhiv.hr bi se svaki sadržaj koji nije u ASCII formatu prije umetanja u XML AIP paket prvo kodirao u Base64.

Od ostalih formata podataka bi bili preporučeni još: TIFF, PNG, WAV, MPEG-2

Detaljnije o standardima i formatima podataka je navedeno u poglavlju 10.3 Standardi i formati.

Formati elektroničkog potpisa

Formati naprednog elektroničkog potpisa preporučeni za sustav e-Arhiv.hr su:

- CAdES,
- XAdES,
- PAdES.

O formatima elektroničkog potpisa koji bi bili preporučeni za sustav e-Arhiv.hr je detaljnije napisano u poglavlju 10.3 Standardi i formati.

Metapodaci

Kao standard za metapodatke u sustavu e-Arhiv.hr je predložen PREMIS. Više o predloženom standardu je navedeno u poglavlju 5.2 Bilježenje traga o elektroničkim potpisima u metapodacima te u poglavlju 10.3 Standardi i formati.

Arhitektura sustava

Za arhitekturu sustava e-Arhiv.hr predložen je model očuvanja s pohranom (ETSI model sukladan OAIS referentnom modelu) uz modifikaciju ETSI-OAIS sukladnih procesa

prihvata i pristupa u smislu relacije s uslugom očuvanja. Tu se predlaže direktna veza entiteta Prihvata i Usluge očuvanja.

U arhitekturi sustava e-Arhiv.hr je uz šest funkcionalnih OAIS entiteta (Prihvat, Arhivska pohrana, Upravljanje podacima, Administracija, Planiranje procesa očuvanja i Pristup) dodan za potrebe ovog OAIS sukladnog modela i entitet Usluge očuvanja (engl. Preservation service).

Slika arhitekture i detaljnija razrada arhitekture je navedena u poglavlju 10.4 Arhitektura i funkcionalnosti informacijskog sustava.

Sigurnost pohrane podataka

Potrebno je uvažiti standard ISO 27001 da bi se izbjegla neželjena promjena AIP paketa. Osim toga, potrebno je izbjeći korištenje skupe WORM tehnologije kod koje postoji visoka ovisnost o vlasničkoj platformi. Za sustav e-Arhiv.hr se preporučuje korištenje standardne pohranu neovisne o specijalnim platformama ili proizvođačima. Više o sigurnosti pohrane podataka je napisano u poglavlju 10.5 Ostali zahtjevi.

Migracija zapisa

Predlaže se da se transformacija potpisanih podataka u sustavu e-Arhiv.hr ne obavlja već da se koriste isključivo otvoreni, općeprihvaćeni standardi (npr. XML) iz razloga izbjegavanja kasnije konverzije formata. Otvorene standarde je potrebno upotrebljavati i zbog interoperabilnosti (migracija arhiviranih potpisanih zapisa iz jednog e-Arhiva u drugi). Za slučaj promjene u formatima arhiviranih dokumenata predlaže se korištenje tehnike za izmjenu sadržaja dokumenta ne brisanjem ili mijenjanjem originalnog dokumenta već pohranjivanjem opisa obavljenih izmjena te izmijenjenog dokumenta zajedno s originalnim dokumentom Više o tematici migracije zapisa je navedeno u poglavlju 10.5 Ostali zahtjevi.

Topologija informacijskog sustava

Za implementaciju sustava e-Arhiv.hr predlažu se dvije sekundarne lokacije. Jedna od tih dviju sekundarnih lokacija bi imala i funkciju zamjenske lokacije za slučaj katastrofe (engl. disaster location). Više je navedeno u poglavlju 10.5 Ostali zahtjevi.

Financiranje

Kao primjer uspješnog financiranja uspostave sličnih infrastruktura predlaže se preuzeti model projektnog financiranja HALMED-DAIS sustava koji je realiziran kroz europski IPA 2009 TAIB projekt. Više o navedenoj tematici je navedeno u poglavlju 9.2 HRVATSKA – HALMED – DAIS.

11. ZAKLJUČAK

Osnovni cilj ovog doktorskog rada je bio razviti koncept uspostave elektroničkog arhiva u javnoj upravi te na osnovu toga izraditi prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave. Na temelju analiziranog OAIS referentnog modela, infrastrukture javnog ključa, tematike naprednog elektroničkog potpisa, tematike elektroničke javne uprave i elektroničke isprave te analiziranih uspješnih implementacija i referentnih modela za e-arhive izrađen je model informacijskog sustava e-Arhiv.hr te je dan prijedlog njegove uspostave.

Obradom elemenata infrastrukture javnog ključa u 3. poglavlju dokazana je H-1 ovog doktorskog rada. Naime, u Republici Hrvatskoj postoji odgovarajući zakonodavni okvir za implementaciju elektroničke isprave zasnovan na infrastrukturi javnog ključa. Uredba eIDAS (Uredba (EU) br. 910/2014) je 2014. godine dodatno uredila navedeno područje u Europskoj Uniji (navedenu uredbu je implementiralo i hrvatsko zakonodavstvo) te je definirala pojam kvalificiranih pružatelja usluga od povjerenja, QTS (engl. Qualified Trust Service) koji se odnosi na pružanje usluga izdavanja kvalificiranih certifikata za elektronički potpis te na usluge izdavanja kvalificiranih vremenskih žigova. Navedeno je bitno za potrebe implementacije elektroničke isprave. Osim toga, infrastruktura javnog ključa predstavlja nužan temelj za izgradnju i implementaciju informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata što je i detaljno opisano u poglavlju 10. Model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata. Time je dokazana i hipoteza H-2 ovog doktorskog rada. Hipoteza H-3 je dokazana kroz pregled dostupnih servisa i komponenata temeljenih na infrastrukturi javnog ključa u Republici Hrvatskoj, a koji se mogu učinkovito iskoristiti za izgradnju infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata za područje hrvatske javne uprave. Naime, osim u poglavlju 3. Infrastruktura javnog ključa, i u poglavlju 6. Elektronička javna uprava je dan pregled dostupnih servisa i komponenata temeljenih na PKI infrastrukturi u RH. Hipoteza H-4 je predstavljala najveći izazov za ovaj doktorski rad. Naime, trebalo je dokazati da uspostava informacijskog sustava za dugotrajnu pohranu elektronički potpisanih dokumenata osigurava pohranu i dugotrajno čuvanje e-gradiva uz zadovoljavanje zahtjeva autentičnosti, neporecivosti, zaštite integriteta i upotrebljivosti. Hipoteza H-4 nije opovrgnuta jer postoje uspješne

implementacije e-arhiva koji funkcionalno osiguravaju sve navedene zahtjeve, ali nije ni dokazana jer nema primjera iz prakse koji su dovoljno dugo u funkciji da bi se to moglo dokazati. Kao tvrdnju koja ide u prilog da se ova hipoteza za sada ne može dokazati već eventualno za par desetljeća, slijedi izjava iz popunjenog upitnika za elektroničke arhive (Prilog 2) od strane estonskog Nacionalnog arhiva: „Nema smisla govoriti o 100-godišnjoj dugotrajnosti elektroničkih potpisa, već 10-20 godina“[708].

Kod klasičnih dokumenata autentičnost se provjerava na originalnom dokumentu, a provjera autentičnosti elektroničkih informacijskih objekata je daleko kompliciranija. Poznat je Thibodeauov inherentni paradoks[709] koji govori da je očuvanjem elektroničkih informacijskih objekata s jedne strane potrebno dostaviti povijest u budućnost u autentičnom stanju, ali s druge strane dohvaćanje takvog sadržaja iz prošlosti zahtijeva određene izmjene. Kako bi se navedeno riješilo izrađen je referentni model za otvoreni arhivski informacijski sustav (OAIS). Ovaj model je pokriven i međunarodnim ISO standardom (ISO 14721:2003, Space data and information transfer systems - Open archival information system - Reference model). Postoji šest funkcionalnih entiteta OAIS modela: prihvat, arhivska pohrana, upravljanje podacima, administracija, planiranje procesa očuvanja i pristup. OAIS je kroz vrijeme postao standardni model za izradu sustava za dugotrajno očuvanje za mnoge institucije i organizacije, primjerice za knjižnice (postoje mnogi primjeri nacionalnih knjižnica Nizozemske, Britanije, Francuske, SAD i dr. koji su izgradili e-arhive na temelju OAIS modela).

Infrastrukturu javnog ključa (PKI) sam prepoznao kao ključnu u izradi modela uspostave elektroničkog arhiva u javnoj upravi. Na stranicama Ministarstva gospodarstva Republike Hrvatske su na dan 28. prosinca 2017. kao davatelji usluga certificiranja u Republici Hrvatskoj navedeni: FINA, AKD i Zagrebačka banka. Uredba eIDAS je u velikoj mjeri utjecala na pravnu pokrivenost korištenja elektroničkog potpisa u Europskoj Uniji. Važnost Uredbe eIDAS je što je za područje Europske Unije stavljena van snage do tada važeća EU Direktiva 1999/93/EC o okviru Zajednice za elektroničke potpise i

[708] Kuldar Aas, podaci dobiveni upitnikom, „There is no point in talking about 100-year longetivity of digital signatures, but rather for 10-20 years.“ (26.02.2018.)
[709] Thibodeau, K. (2002.), Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, u: The State of Digital Preservation: An International Perspective, Council on Library and Information Resources (CLIR), Washington, D.C., SAD, str. 28., https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10 (07.08.2016.)

propisana su nova pravila, posebno u svrhu prekogranične suradnje i razmjene podataka u Europskoj Uniji. Navedena uredba je propisala i QTS (engl. Qualified Trust Service), tj. koncept QTS kvalificiranih pružatelja usluga povjerenja (za izdavanje certifikata, vremenskih žigova i dr.). Vodi se dosta računa o tome da bi se elektronički vremenski žig mogao koristiti kao dokaz u sudskim postupcima i to u različitim državama članicama Europske unije. Vremenski žig je bitan i za ovaj rad iz razloga što omogućuje povjerenje u elektronički potpis i poslije isteka certifikata potpisnika te time omogućuje pretpostavke za dugoročno arhiviranje elektronički potpisanih dokumenata. Uredba eIDAS uvodi strogo razdvajanje namjene elektroničkog potpisa i elektroničkog pečata. Naime, potpisnik se u Uredbi eIDAS definira kao fizička osoba koja izrađuje elektronički potpis, a autor elektroničkog pečata može biti samo pravna osoba. Bitno je napomenuti da je svaki kvalificirani elektronički potpis ujedno i napredan elektronički potpis. Međutim, svaki napredni elektronički potpis ne mora biti i kvalificirani elektronički potpis. Važnost kvalificiranog elektroničkog potpisa je u tome što za Uredbu eIDAS on ima jednak pravni učinak kao vlastoručni potpis. Različiti su formati elektroničkog potpisa. Za izradu modela u radu preferiram otvorene standarde pa su obrađeni sljedeći formati elektroničkog potpisa: CMS (PKCS#7), XMLDSig, CAdES, XAdES i PAdES. Elektronički potpisi iz AdES obitelji potpisa (XAdES, CAdES i PAdES) su napredni elektronički potpisi koji su sukladni s Uredbom eIDAS, a bitni su za ovaj rad zbog mogućnost dugotrajnog očuvanja potpisanih zapisa. Lipp[710] pojašnjava da ETSI EN 319 102-1 norma utvrđuje mogućnost da validacijski algoritmi odrađuju validaciju potpisa u dugom roku kada postoji vremenski žig koji jamči da je potpis postojao u vrijeme vremenskog žiga. U tom slučaju se radi o dokazu postojanja, tj. PoE (engl. Proof of Existence). Stoga sam prepoznao navedeni pojam kao dobru polazišnu osnovu za daljnju razrada u pogledu dugotrajnog očuvanja elektronički potpisanih zapisa. Lipp preporučuje izbjegavanja potrebe za dugoročnom validacijom potpisa zbog rekurzivne potrebe validacije potpisa, a za slučaj kada je ona nužna predlaže validiranje potpisa neposredno nakon izrade te njihovo sigurno arhiviranje zajedno s validacijskim rezultatom, validacijskim izvješćem i materijalom korištenim za validiranje.

[710] Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

Blanchette navodi tri moguće strategije za očuvanje elektroničkih zapisa s elektroničkim potpisima:[711]: očuvanje elektroničkih potpisa, uklanjanje elektroničkih potpisa i bilježenje traga o elektroničkim potpisima u metapodacima. Kao najprihvatljiviju strategiju navodi bilježenje traga o elektroničkim potpisima u metapodacima jer je u najvećoj mjeri komforno s arhivskom praksom i teorijom. Stančić[712] predlaže i četvrtu strategiju, a radi se o bilježenju podataka o valjanosti elektroničkih potpisa u ulančanim blokovima (engl. blokchain). Strategija očuvanja elektroničkih potpisa detaljno je obrađena u poglavlju 4. Napredni elektronički potpis. Strategija uklanjanja elektroničkih potpisa je bila aktualna početkom ovog stoljeća i to posebno u Sjevernoj Americi (SAD i Kanada) te se ona kombinirala s bilježenjem podataka o valjanosti potpisa u metapodatke ili neki drugi oblik elektroničkog zapisa i ispisa. Takvu strategiju navodi i finalni izvještaj InterPARES projekta[713] iz 2002. godine. Što se strategije bilježenja traga o elektroničkim potpisima u metapodacima tiče navodim Boudrezovu[714] tezu da zapisi o valjanosti elektroničkog potpisa u metapodacima mogu zamijeniti elektronički potpis za one elektronički potpisane zapise čije je razdoblje očuvanja trajno. U razradi navedene strategije obrađeni su standardi i inicijative za metapodatke: Dublin Core, METS, VRA Core, DIF, PREMIS, FEDORA, XFDU, LOTAR, E-ARK. Płoszajski navodi[715] da su standardi metapodataka koji zaslužuju više pozornosti u kontekstu dugoročnog arhiviranja METS i PREMIS. METS u pogledu stvaranja SIP paketa (namijenjen je sadržavanju metapodataka o pravima) dok PREMIS definira obilježja prava koja se odnose na očuvanje aktivnosti i skuplja informacije tijekom pohrane digitalnih objekata u arhivu. Strategija bilježenja valjanosti o elektroničkim potpisima u blokchainu je nova strategija kao i sama blokchain tehnologija. Bralić, Kuleš i Stančić prezentirali su model za očuvanje valjanosti elektroničkog potpisa u blokchainu[716], TrustChain te predlažu

[711] Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf , str. 1. (06.02.2018.)
[712] Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague, https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf, slide 19. (06.02.2108.)
[713] InterPARES (2002.), The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, http://www.interpares.org/book/index.htm (10.02.2018.)
[714] Boudrez, F. (2007.), Digital signatures and electronic records, Archival Science, ISSN: 1389-0166, str. 190 (179-193)
[715] Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., http://www.springer.com/978-3-319-51800-8, str. 45 (15.-61) (19.02.2018.)
[716] Bralić, V., Kuleš, M., Stančić, H. (2017.), A model for long-term preservation of digital signature validity: TrustChain, Konferencija INFuture 2017: Integrating ICT in Society, https://bib.irb.hr/datoteka/906471.TrustChainV11-final.pdf (18.02.2018.)

model gdje bi se pohranjivali kontrolni hashevi (ili elektronički potpisi) u nepromjenjiv i javno čitljiv blokchain. Na ovaj način, svaka zainteresirana strana može potvrditi da je elektronički potpisan i arhiviran dokument ostao nepromijenjen te da je u trenutku stvaranja zapisa u blokchainu elektronički potpis bio valjan. Strategija očuvanja elektroničkih potpisa mi je ključna za ovaj rad pa sam ju detaljnije i obradio u poglavlju 4. Napredni elektronički potpis kao podloga za dugoročno očuvanje elektroničkih zapisa te u poglavlju 10. Model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata.

Područje elektroničke javne uprave (engl. e-Government) je području koje se propulzivno mijenja i prilagođava novim potrebama i okolnostima. Stoga sam prepoznao važnost ovog područja za ovaj rad (u pogledu izvedbe e-arhiva za to područje te istraživanja dostupnih servisa i komponenata temeljenih na infrastrukturi javnog ključa u RH što je i bilo potrebno za dokazivanje H-3). Motivacija za detaljniju obradu ovog područja je i sudjelovanje na InterPARES Trust projektu za istraživanje e-servisa javne uprave. Izvješće UN-a za 2005. o globalnom stanju elektroničke javne uprave[717] daje ambiciozne ciljeve u modelu razvoja elektroničke javne uprave. Poushter[718] dokazuje da postoji vrlo jaka korelacija između bogatstva zemlje (mjereno BDP-om) i pristupa internetu što je opet jedan od temeljnih uvjeta za razvoj elektroničke javne uprave. Europska unija strategijom Europa 2020 postavlja prioritete: pametnog, održivog i uključivog rasta, a inicijativa Digitalna agenda za Europu[719] je strateški kontekst koji je u velikoj mjeri odredio smjer razvoja elektroničke javne uprave za zemlje EU i zemlje kandidate. Stoga sam istražio i dao pregled zakonskih osnova i strategija za razvoj hrvatske e-Uprave od 2004. do 2017. Strategijom e-Hrvatska 2020[720] su zacrtani ciljeve daljnjeg razvoja. Osnovni cilj navedene Strategije je omogućiti povezivanje informacijskih sustava tijela javne uprave iz svih sektora radi pružanja što većeg broja

[717] United Nations, Department of Economic and Social Affairs (2005.), Global e-government readiness report 2005, New York, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf (11.01.2018.)
[718] Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ (01.01.2018.)
[719] Europska komisija (2010., 2.), Digital agenda for Europe, Rebooting Europe's economy, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (12.01.2018.)
[720] Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 , str. 27 (10.01.2018.)

kompleksnih e-usluga i olakšavanja interakcije građana s javnom upravom. Nadalje su detaljno obrađena izvješća i metodologije mjerenja UN-a i Europske unije. UN razvoj elektroničke javne uprave prati preko EGDI kompozitnog indeksa. Svjetski lideri po UN istraživanju za 2016. godinu su: Ujedinjeno Kraljevstvo, Australija, Južna Koreja, Singapur, Finska, Švedska, Nizozemska, Novi Zeland, Danska, Francuska, Japan, SAD, Estonija, Kanada i Njemačka. Hrvatska je u smještena na 37. mjestu. Europska unija ima svoje metodologije kojima prati napredak u e-upravi za zemlje članice i zemlje kandidate za članstvo. Jedan od indikatora uspješnosti je indeks DESI (Indeks digitalnog gospodarstva i društva). Osim DESI indeksa, postoji Digitalni semafor (engl. Digital Scoreboard) koji objavljuje podatke u sklopu Europskog izvješća o digitalnom napretku (EDPR). DESI 2017 (podaci za 2016.) navodi da Danska, Finska, Švedska i Nizozemska imaju najnaprednije digitalne ekonomije u EU. Hrvatska je na 24. mjestu (od 28 zemalja). Kao jedan od razloga stagnacije razvoja e-Uprave u Izvješću za Hrvatsku se navode održani izbori u 2015. i politička nestabilnost. Hrvatska je na dnu ljestvice Europske Unije po rezultatima u području iskorištenosti širokopojasnih mreža. Razlozi su ograničena potražnja za širokopojasnim mrežama velike brzine te financijska nepristupačnost (Hrvatska ima najskuplju pretplatu za samostalni fiksni širokopojasni pristup u cijeloj Europskoj uniji).

U okviru proučavanja aspekata elektronički potpisanih dokumenata obrađena je interoperabilnosti i pravna uređenost. Europski okvir za interoperabilnost (EIF) daje specifične smjernice o uspostavljanju interoperabilnih elektroničkih javnih usluga, a jedan od projekata interoperabilnosti je SPOCS čiji su gradivni blokovi eDokumenti i elektronički potpisi. SPOCS specifikacija definira višeslojni format kontejnera elektroničkih dokumenata (OCD). OCD temeljen na PDF formatu koristi mehanizam PDF dokumenta s privicima[721] što može biti podloga za realizaciju elektroničke isprave. Hrvatski zakon o elektroničkoj ispravi (ZEI) donesen je 2005. Iako je Zakon o elektroničkom potpisu opozvan Uredbom eIDAS[722], ZEI je ostao na snazi, tj. mjerodavno

[721] ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (21.08.2017.)

[722] Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

tijelo za njega (Ministarstvo gospodarstvo[723]) nije propisalo nikakve zakonske akte nastavno na Uredbu eIDAS ili bar donijelo smjernice za postupanje. Smatram da postoji prostor za donošenje zasebnih zakonskih akata ili barem smjernica za ZEI u kontekstu Uredbe eIDAS jer je ZEI usko vezan za elektronički potpis. Nakon analize pravne uređenosti elektroničke isprave u Hrvatskoj, analizira se pravni aspekt korištenja elektroničkog dokumenta po odabranim svjetskim zemljama: SAD, Rusija, Škotska, Litva, Urugvaj, Filipini i dr. Manji dio zemalja je elektroničkom dokumentu posvetio zaseban zakon, a većina zemalja je istim zakonom pokrila i područje elektroničkog potpisa i elektroničkog dokumenta. U Hrvatskoj su za manji dio dokumentacije propisane Pravilnikom o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva navedeni definirani rokovi čuvanja (rokovi su: 50, 10, 5, 3, 2, 1 godinu te trajno). Međutim, javna uprave svake godine stvara veliku količinu elektroničkih dokumenata (međuostalim i elektronički potpisanih) pa dugotrajna pohrana takve dokumentacije postaje ozbiljan izazov. Obrađene su i norme za dugoročno očuvanje elektroničkih dokumenata (MoReq2, PDF/A-1, PDF/A-2, PDF/A-3 i dr.). Došao sam do saznanja da se konverzijom elektronički potpisanih dokumenata u PDF/A format (koji je najčešće upotrebljavan za arhiviranje) gube elektronički potpisi te se navedeni format ne preporuča za dugotrajnu pohranu elektronički potpisanih dokumenata. Kada se elektronički potpis izrađuje u skladu s ETSI standardima za napredni elektronički potpis (AdES obitelj naprednog elektroničkog potpisa) i profilima za dugoročno arhiviranje, tada se takvim potpisima valjanost može provjeriti i naknadno validirati što je i preduvjet za izgradnju arhiva za elektronički potpisane dokumente.

Navedeni su i rezultati Komparativne analize implementiranih elektroničkih javnih servisa koja je u formi Završnog izvješća[724] obavljena unutar projekta InterPARES Trust 2014. godine. Ipak, nađeno je malo informacija o dugotrajnoj pohrani podataka. Informacije o preferiranim dugotrajnim formatima za očuvanja zapisa je bila dostupna samo za litvanske e-usluge (koriste se formati PDF/A i XAdES-A). Zanimljiva je informacija da se u Hrvatskoj i Švedskoj evidencije o podacima zdravstvene i socijalne skrbi stvorene e-uslugama trebaju čuvati najmanje 30 godina. Istraživački tim je objavio preporuku da bi

[723] Ministarstvo gospodarstva, https://www.mingo.hr/
[724] Stančić, H., Brzica, H., Adžaga, I., Garić, A., Poljičak-Sušec, M., Presečki, K., Stanković, A. (2015.), Comparative Analysis of Implemented Governmental
e-Services (EU09), Final report, InterPARES Trust Project,
https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisImplementedGovernmentaleServices_FinalReport.pdf (20.02.2018.)

servisi trebali imati obavezu objave načina skladištenja i dugotrajnog očuvanja podataka jer je nađeno vrlo malo takvih javno objavljenih informacija. U nastavku su analizirane uspješne implementacije e-arhiva: HALMED[725] DAIS sustav u Hrvatskoj, elektronički arhivski sustav njemačke klinike Braunschweig[726], litvanski EAIS[727] arhivski sustav, Elektronički Arhiv Nacionalnog arhiva Estonije[728] te e-arhiv zdravstvenog sustava okruga Vicenze u Italiji[729]. Osim toga su analizirani referentni model dugotrajne pohrane elektronički potpisanih dokumenata njemačkog ureda za informacijsku sigurnost, BSI[730], te rezultati europskog E-ARK projekta[731] čiji je cilj bio istražiti postojeće arhivske servise koji zadržavaju autentičnost i čitljivost na postojećim najboljim praksama. Obrađena je i Komparativna analiza unutarnje strukture i funkcija elektroničkih arhiva za složene elektroničke zapise koju su napravili Stančić, Herceg i Rajh[732] 2014. godine. Spoznaje dobivene analizom prethodno navedenih uspješnih implementacija e-arhiva, referentnog modela, E-ARK istraživačkog projekta i komparativnih analiza poslužile su mi za sintezu modela informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata.

Na kraju rada sam izradio model informacijskog sustava za dugotrajnu pohranu potpisanih elektroničkih dokumenata te dao prijedlog za uspostavu infrastrukture za potpisivanje i dugotrajnu pohranu elektronički potpisanih dokumenata. Imenovao sam informacijski sustav kao sustav e-Arhiv.hr. Model počiva na dvojakom konceptu: očuvanju dokaza postojanja elektroničkog potpisa te produženju potpisa. Podaci za očuvanje postojanja se

[725] HALMED, Agencija za lijekove i medicinske proizvode, http://www.halmed.hr/ (24.02.2018.)
[726] Wild, B. (2012.), PDF/A in Healthcare, white paper, PDF Association – PDF/A Competence Center, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiCnczNv77ZAhXD26QKHU7KCZIQFggsMAA&url=https%3A%2F%2Fwww.pdfa.org%2Fwp-content%2Funtil2016_uploads%2F2012%2F05%2FWP-PDFA-in-Healthcare.pdf&usg=AOvVaw0PYq9l9u_u5UJwI9zwCdCW (24.02.2018.)
[727] Electronic Archive Information System, http://eais-pub.archyvai.lt/eais (23.02.2018.)
[728] Digital archives, Rahvusarhiiv, http://www.ra.ee/en/information-management/digital-archives/ (16.03.2018.)
[729] Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=182, str. 172-179 (06.03.2018.)
[730] BSI, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Home/home_node.html (05.03.2018.)
[731] E-ARK, European Archival Records and Knowledge Preservation, http://www.eark-project.com/ (06.03.2018.)
[732] Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)

zapisuje u zapis očuvanja postojanja po standardu RFC 6283 (XMLERS, ERS temeljen na XML jeziku). Podaci potrebni za provjeru potpisa u budućnosti se trebaju dohvatiti neposredno nakon izrade i/ili provjere potpisa te trebaju biti arhivirani skupa s dokumentima i ostalim podacima. Osim potpisanih zapisa osiguravat će se i integritet nepotpisanih podataka njihovim ulaskom u sustav e-Arhiv.hr na način da se izračuna ulazna hash vrijednost tih podataka ili da se takvi podaci ovjere kvalificiranim vremenskim žigom. Koristit će se usluga Službe za izradu kvalificiranog vremenskog žiga (QTSA) radi dohvaćanja kvalificiranog vremenskog žiga u svrhu izrade zapisa o dokazu postojanja te za dohvaćanje informacija o statusu certifikata. Očuvanje potpisanih elektroničkih dokumenata će se omogućiti na dvojak način: već spomenuto korištenje XMLERS standarda za potpisane elektroničke dokumente koji nemaju pravni karakter elektroničke isprave te po modelu samostalnog produženja potpisa (za potpise iz AdES obitelji LTV potpisa) za elektroničke dokumente koji imaju pravni karakter elektroničke isprave te koji trebaju zadržati svojstvo unutarnjeg i vanjskog obrasca tijekom cijelog svog dokumentacijskog ciklusa. Dohvaćanje vremenskog žiga za svaki elektronički dokument nije ekonomično pa je za sustav e-Arhiv.hr prijedlog dohvatiti jedan vremenski žig za veći broj potpisanih dokumenata (vrijedi za strategiju korištenja zapisa očuvanja dokaza postojanja). S druge strane elektronički dokumenti potpisani potpisima iz AdES obitelji potpisa s LTV svojstvom su samostalni i time pogodni za elektroničku ispravu, a ako se po potrebi produžuju tada sadrže sve podatke koji omogućavaju provjeru potpisa nakon duže vremena. Na taj način je kod takvih dokumenata isključeno zajedničko potpisivanje kvalificiranim vremenskim žigom jer se time gubi pravni karakter elektroničke isprave.

Sustav e-Arhiv.hr će imati sljedeće korisničke uloge: djelatnike sustava e-Arhiv.hr, autorizirane djelatnike tijela javne uprave, informacijske sustave tijela javne uprave te građane i poslovne subjekte. Svaka od tih korisničkih uloga će imati svoj način i kanal pristupa na sustav. Pristup sustavu e-Arhiv.hr bit će moguć preko sustava e-Građanin te NIAS (Nacionalni identifikacijski i autentifikacijski sustav) vjerodajnica. XML kao otvoreni standard podataka je i temelj za sustav e-Arhiv.hr. Preporučeni su i sljedeći formati podataka: PDF/A, ASCII, Base64 kodirani podaci, TIFF, PNG, WAV, MPEG-2. Formati naprednog elektroničkog potpisa preporučeni za sustav e-Arhiv.hr su: CAdES, XAdES i PAdES. Kao standard za metapodatke u sustav e-Arhiv.hr je predložen PREMIS.

Za arhitekturu sustava e-Arhiv.hr je predložen ETSI model očuvanja s pohranom[733] (sukladan OAIS referentnom modelu) uz modifikaciju ETSI-OAIS sukladnih procesa prihvata i pristupa u smislu relacije s uslugom očuvanja (predlažem direktnu vezu entiteta Prihvata i Usluge očuvanja.). Dakle, osim šest osnovnih OAIS entiteta, predlažem i proširuženi entitet Uslugu očuvanja (engl. Preservation service). Potrebno je uvažiti standard ISO 27001[734] da bi se izbjegla neželjena promjena AIP paketa. Predlažem (nastavno na preporuke BSI tehničkog priručnika 03125[735]) da se transformacija potpisanih podataka u druge formate u sustavu e-Arhiv.hr ne obavlja već da se koriste isključivo otvoreni, općeprihvaćeni standardi (npr. XML) iz razloga izbjegavanja kasnije konverzije formata. Predložena je sljedeća topologija sustava e-Arhiv.hr: primarna i dvije sekundarne lokacije (jedna od tih dviju sekundarnih lokacija bi imala i funkciju zamjenske lokacije za slučaj katastrofe). Predlažem uspostavu sustava e-Arhiv.hr financiranjem iz EU fondova (po modelu projektnog financiranja HALMED-DAIS sustava koji je realiziran kroz europski IPA 2009 TAIB projekt).

Još sam u magistarskom radu pisao o elektroničkoj javnoj upravi, a dodatnim istraživanjem u ovom doktorskom radu sam pokazao relativnu nisku razvijenost e-Uprave u Hrvatskoj u usporedbi s drugim zemljama EU. U ovom su radu analizirani uspješni primjeri e-arhiva i modela iz Njemačke i Estonije, a UN studija iz 2016. je pokazala da su te dvije zemlje među liderima u e-upravi. Stoga vjerujem da se, uz postojeće strateške planove razvoja, implementacijom predloženog sustava elektroničkog arhiva za elektronički potpisane dokumente (uključivo elektroničke isprave) može dodatno unaprijediti stanje e-Uprave u Hrvatskoj.

[733] ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05), http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf, str. 17 (06.03.2018.)

[734] ISO 27001, the international information security standard, https://www.itgovernance.co.uk/iso27001 (14.03.2018.)

[735] BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile (05.03.2018)

12. PRILOZI

12.1 PRILOG 1 – UPITNIK ZA ELEKTRONIČKE JAVNE USLUGE

1. Osnovne informacije o servisu	
1.	URL servisa
2.	Kategorija servisa (Prilog A)
3.	Kategorija/vrsta ustanove nadležne za e-servis
4.	Početak rada
5.	Razina informatiziranosti
6.	Je li servis povezan s drugim servisima javne uprave i, ako da, s kojima?
7.	Usporedba teorije i stvarne razvijenosti pojedinog e-servisa
8.	Postoji li ograničenje u terminu korištenja servisa? Ako da, u kojim terminima?
9.	Kratak opis servisa
10.	Slika karakterističnog ekrana iz servisa
11.	Obavlja li servis ono što piše da obavlja?
2. Korisnici	
12.	Je li korištenje elektroničkog servisa obavezno za određenu kategoriju korisnika? Ako da, za koga je obavezno?
13.	Postoji li više tipova korisnika?
14.	Koliko korisnika po pojedinoj vrsti ima?
15.	Postotak korisnika koji javni servis koriste elektroničkim putem
16.	Koje su najčešće dobne skupine koje koriste ovu uslugu?
17.	Je li servis prilagođen osobama s posebnim potrebama?
18.	Kakvo je zadovoljstvo korisnika servisom?
3. Optimizacija poslovanja	

19.	Postoje li pozitivni financijski pokazatelji e-servisa (za ustanovu čiji je servis, te za korisnike)?
20.	Smanjenje vremena za obradu zahtjeva (ubrzanje procesa)
21.	Na koji način je rad servisa imao utjecaj na organizaciju radnih procesa u smislu potrebnog broja radnika?
22.	Koji su planovi za nadogradnju i širenje servisa u budućnosti?
4. Tehnološka rješenja	
23.	Način autentifikacije
24.	Kriptira li se kanal komunikacije između servera i klijentske stanice (SSL, neki drugi protokol)?
25.	Koristi li se eID u servisu? Ako da, koji (ili koje ako se mogu koristiti više njih)?
26.	Koriste li se digitalni certifikati za elektronički potpis?
27.	Ako da, koji format elektroničkog potpisa se koristi?
28.	Na koji način korisnik popunjava i šalje podatke
29.	Šalje li korisnik privitke uz popunjene podatke? Ako da, na koji način?
30.	Imaju li korisnici prilikom popunjavanja i slanja podataka propisane formate dokumenata? Ako da koje?
31.	Je li servis implementiran open-source ili komercijalnim tehnologijama? Koje su to tehnologije?
32.	Koji je tip aplikacije na klijentskoj strani?
33.	Kroz koje kanale je servis dostupan?
34.	Je li servis udomljen u ustanovi nadležnoj za e-servis?
35.	Ako ustanova nadležna za e-servis udomljava servis, posjeduje li odgovarajuće certifikate?
36.	Ako je servis ili dio servisa udomljen van ustanove nadležne za servis koristi li se Cloud? Je li Cloud/Data centar unutar iste zemlje?
5. Pohrana i trajna dostupnost sadržaja	
37.	U kojem roku se zaprimljeni podaci čuvaju u sustavu?
38.	Je li rok čuvanja podataka zadan zakonom/pravilnikom ili nekim drugim aktom? Ako da, kojim?
39.	Brišu li se podaci zaprimljeni kroz servis nakon roka predviđenog za čuvanje?
40.	U kojim formatima se dugoročno čuvaju podaci?

41.	Koristi li se metoda materijalizacije kroz e-servis zaprimljenih podataka, pa mikrofilmiranje?
42.	Jesu li zadovoljeni neki od standarda za dugotrajnu pohranu podataka? Ako da, koji?
43.	Postoji li uz e-servis korisnicima ponuđena i usluga korištenja elektroničkog arhiva (možda kao usluga za više servisa istovremeno)? Postoje li electronic document safe usluge?
44.	Spremaju li se kroz servis zaprimljeni podaci unutar informacijskog sustava ustanove nadležne za servis?
45.	Posjeduje li ustanova nadležna za servis odgovarajuće certifikate koje jamče sigurnost pohranjenih podataka?
46.	Ako se podaci barem djelomično spremaju izvan ustanove nadležne za servis, koristi li se Data Cloud? Je li Cloud/Data centar unutar iste zemlje kao i ustanova davatelj usluge?
6. Transparentnost rada sustava	
47.	Postoji li definirana politika korištenja servisa?
48.	Postoje li proklamirane tehnološke mjere kojim se korisnicima jamči da se njihovi podaci zaprimljeni kroz servis koriste isključivo za definiranu namjenu?
49.	Postoje li definirane interne radne procedure, potpisivanje izjava i edukacije za zaposlenike kojim se zaposlenici obavezuju da neće koristiti i iznositi podatke o korisnicima trećoj strani mimo definiranih procedura?
50.	Ima li korisnik pravo kroz elektronički servis pregledavati svoje podatke?
51.	Ima li korisnik pravo na ispravku netočnih podataka koji su zaprimljeni u servis? Ako da, može li zahtjev za ispravkom podataka poslati elektroničkim putem?
52.	Može li korisnik pratiti stanje obrađenosti/status svoga zahtjeva?

12.2 PRILOG 2 – UPITNIK ZA ELEKTRONIČKE ARHIVE

1. Osnovne informacije o elektroničkom arhivu	
1.	Kratak opis elektroničkog arhiva.
2.	Je li elektronički arhiv povezan s drugim servisima javne uprave i, ako da, s kojima?
3.	Je li elektronički arhiv udomljen u matičnoj instituciji?
4.	Kakva je topologija elektroničkog arhiva (primarna i sekundarna lokacija)?
5.	Slike korisničkog sučelja aplikacija elektroničkog arhiva/početne stranice.
2. Korisnici	
6.	Je li korištenje elektroničkog arhiva obavezno za određenu kategoriju korisnika? Ako da, za koga je obavezno?
7.	Postoji li više tipova korisnika/rola (sustav prava temeljen na ulogama)?
8.	Koje su korisničke role koje koriste elektronički arhiv?
3. Optimizacija poslovanja	
9.	Postoji li smanjenje vremena za obradu zahtjeva (ubrzanje procesa) s obzirom na prethodna rješenja
10.	Na koji način je rad elektroničkog arhiva imao utjecaj na organizaciju radnih procesa u smislu potrebnog broja radnika?
4. Tehnološka rješenja	
11.	Na koji način se korisnici autentificiraju kada pristupaju elektroničkom arhivu?
12.	Koristi li se eID za pristup elektroničkom arhivu? Ako da, koji (ili koje ako se mogu koristiti više njih)?
13.	Koristi li elektronički arhiv elektroničke potpise interno? Ako da, u kojim slučajevima?
14.	Koriste li se digitalni certifikati za elektronički potpis (omogućavaju li takvi certifikati izradu naprednog elektroničkog potpisa)?
15.	Ako da, koji format elektroničkog potpisa se koristi?
16.	Traži li se od korisnika da popunjavaju forme prilikom slanja podataka u elektronički arhiv. Ako da, o kakvim vrstama formi se radi i za koju je to svrhu potrebno?
17.	Imaju li korisnici prilikom popunjavanja i slanja podataka propisane formate dokumenata? Ako da koje?
18.	Prihvaćaju li se potpisani podaci u elektronički arhiv (prihvat, engl. ingest)?
19.	Na koji način se osigurava integritet i autentičnost elektronički potpisanih podataka u elektroničkom arhivu (očuvanjem elektroničkog potpisa, čuvanjem zapisa o valjanosti

	elektroničkog potpisa u metapodacima, nekim trećim načinom)? Možete li opisati detaljnije procedure koje se primjenjuju za tu svrhu?
20.	Koristite li se ovjeravanjem vremenskim žigom za očuvanje elektronički potpisanih zapisa?
21.	Koristite li sljedeći tip elektroničkog potpisa unutar elektroničkog arhiva: elektronički potpis koji osigurava dugoročnu dostupnost i integritet potvrdnog materijala (engl. Signature providing Long Term Availability and Integrity of Validation Material)? Ako ga ne koristite, planirate li korištenje navedenog u budućnosti?
5. Pohrana i trajna dostupnost sadržaja	
22.	Je li rok čuvanja podataka zadan zakonom/pravilnikom ili nekim drugim aktom? Ako da, kojim?
23.	Brišu li se podaci zaprimljeni kroz servis nakon roka predviđenog za čuvanje?
24.	Koji su formati preferirani za dugoročno čuvanje podataka?
25.	Jesu li zadovoljeni neki od standarda za dugotrajnu pohranu podataka? Ako da, koji?
26.	Je li elektronički arhiv sukladan s OAIS referentnim modelom (ISO 14721:2003)?
27.	Je li elektronički arhiv implementirao koji aspekt E-ARK procesa e-arhiviranja? Ako da, je li implementirana E-ARK specifikacija informacijskih paketa? Jeste li implementirali neki drugi aspekt E-ARK pristupa? Ako da, molim Vas, objasnite?
28.	Koristite li besplatne alate za transfer elektroničkih zapisa između poslovnih sustava i elektroničkih arhiva? Ako da, možete li specificirati koje alate koristite?
29.	Koji su vaši budući planovi za nadogradnje i širenje elektroničkog arhiva?
30.	Postoji li neki drugi koncept izgradnje očuvanja elektronički potpisanih podataka u elektroničkom arhivu koji bi koristili sada da gradite elektronički arhiv ispočetka (što ste identificirali kao područje koje bi se moglo dizajnirati drukčije unutar sustava)? Možete li navedeno opisati detaljnije?
31.	Imate li kakvih dodatnih napomena?

POPIS LITERATURE

Adobe (2009.), The AdES family of standards: CAdES, XAdES, and PAdES: Implementation guidance for using electronic signatures in the European Union, Adobe Systems Incoporated, https://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf (21.08.2017.)

Adobe (2016.), Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability, https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf (02.02.2018.)

Archivematica, https://wiki.archivematica.org (03.09.2018.)

Arhiv Republike Slovenije (2016.), Strategija in izvedbeni načrt razvoja slovenskega elektronskega arhiva 2016-2020, http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/Strategija_e-ARH.si/Strategija_e-ARH_si_2016-2020_1.0.pdf (14.03.2018.)

Armenski parlament (2004.), The law of the Republic of Armenia "on electronic document and electronic signature", http://www.parliament.am/law_docs/150105HO40eng.pdf (03.02.2018.)

Banco central de Costa Rica, The Law of Digital Signatures, Certificates and Electronic Documents, http://www.bccr.fi.cr/bccr_home_page/digital_signature/ (03.02.2018.)

Bangemann, M. et al. (1994.), Europe and the global information society, Bangemann report recommendations to the European Council, High-Level Group on the Information Society, http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (10.01.2018.)

Bekaert, J., Liu, X., Van de Sompel, H. (2005.), aDORe - A Modular and Standards-Based Digital Object Repository at the Los Alamos National Laboratory, Los Alamos National Laboratory,https://pdfs.semanticscholar.org/09f9/ad95b839780705725b6afb2f56e91436c0d9.pdf (28.11.2016.)

Blanchette, J.F. (2004.), Defining Electronic Authenticity: An Interdisciplinary Journey, International Conference on Dependable Systems and Networks, IEEE Computer Society Press, str. 228-232, http://kavehh.com/my%20Document/Essex/Digital%20signature/blanchettejf_authenticity.pdf (10.02.2018.)

Blanchette, J.F. (2006.), The digital signature dilemma, Pour publication dans Annales des Télécommunications, https://pages.gseis.ucla.edu/faculty/blanchette/papers/annals.pdf (06.02.2018.)

Boudrez, F. (2007.), Digital signatures and electronic records, Archival Science, ISSN: 1389-0166, str. 179-193

Bralić, V., Kuleš, M., Stančić, H. (2017.), A model for long-term preservation of digital signature validity: TrustChain, Konferencija INFuture 2017: Integrating ICT in Society, https://bib.irb.hr/datoteka/906471.TrustChainV11-final.pdf (18.02.2018.)

Brzica, H. (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, magistarski rad, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf (17.03.2018.)

Brzica, H., Herceg, B., Stančić, H. (2013), Long-term Preservation of Validity of Electronically Signed Records, u: Gilliland, A. et al. (ur.), INFuture2013: Information Governance, Zagreb : Odsjek za informacijske i komunikacijske znanosti Filozofskoga fakulteta Sveučilišta u Zagrebu, https://bib.irb.hr/datoteka/662133.403_Brzica_Herceg_Stancic_LTP_of_Validity_of_Electronically_Signed_Records.pdf (21.03.2018.)

Brzica, H., Herceg, B., Katulić, T., Stančić, H. (2014.), Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata, Arh. vjesn. 57, str. 129-157, https://scholar.google.com/citations?view_op=view_citation&hl=ja&user=OCjAcywAAAAJ&citation_for_view=OCjAcywAAAAJ:2osOgNQ5qMEC (24.07.2017.)

BSI (2014.), BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents v1.2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR_V1_2_EN_Main.pdf?__blob=publicationFile (05.03.2018)

BSI (2015.), Annex TR-ESOR-F - Formats, BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/PrevVersion/TG-03125AnnexTR-ESOR-F.pdf?__blob=publicationFile (06.03.2018.)

Bugarski parlament (2001.), Law for the electronic document and electronic signature, http://www.crc.bg/files/_en/ZED_ENG_15.01.2008.htm (03.02.2018.)

Bundesarchivgesetz, BarchG, (2017.), https://www.bundesarchiv.de/DE/Content/Downloads/Rechtliches/bundesarchivgesetz.pdf?__blob=publicationFile (05.03.2018.)

Capgemini et al. (2010.), Digitizing Public Services in Europe: Putting ambition into action, 9 th. Benchmark Measurement, pripremili Capgemini, IDC, Rand Europe, Sogeti i DTi za Europsku komisiju, ec.europa.eu/newsroom/document.cfm?action=display&doc_id=747 (20.02.2018.)

Capgemini et al. (2016.), eGovernment Benchmark 2016 Background Report, Final background report – volume 2, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17856 (21.03.2018.)

Capgemini et al. (2016., 2.), eGovernment Benchmark 2016, Final insight report – volume 1, https://www.capgemini.com/wp-content/uploads/2017/07/egovernment_benchmark_2016.pdf (15.01.2018.)

Consultative Committee for Space Data Systems (2012.), Reference model for an open archival information system (OAIS) - 062012 - Magneta book, http://public.ccsds.org/publications/archive/650x0m2.pdf (07.08.2016.)

Corrado, M. C., Moulaison, H. L. (2014.), Digital preservation for libraries, archives, & museums, izdavač: Rowman & Littlefield, Plymouth

Ćosić, J., Bača, M. (2010.), (Im)Proving Chain of Custody and Digital Evidence Integ¬rity with Time Stamp, MIPRO – Proceedings of the 33rd International Convention, str. 1227-1228, URL: http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (14.04.2014.)

Di Maio, B. (2000.), Gartner's Four Phases of E-Government Model, Gartner Group, November 2000

Diffie, W., E., Hellman, M. (1976.), New Directions in Cryptography,IEEE Transactions on information theory, vol. IT22, no. 6, http://www-ee.stanford.edu/~hellman/publications/24.pdf (28.11.2016.)

Digital Library Federation (2010.), METS Reference Manual, https://web.archive.org/web/20130516023805/http://www.loc.gov/standards/mets/METSPrimerRevised.pdf (18.02.2018.)

DLM Archival Standards Board (2017.), Common Specification for Information Packages v1.0, http://www.dasboard.eu/images/Specifications/CS/Common_Specifications_for_IPs_v10.pdf (06.03.2018.)

Dumortier, J., Van Den Eynde, S., Electronic Signatures and Trusted Archival Services, http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (07.02.2018.)

DLM Archival Standards Board, E-ARK arhitektura, http://www.eark-project.com/resources/architecture (06.03.2018.)

DLM Archival Standards Board (2017.), E-ARK AIP, http://www.dasboard.eu/images/Specifications/AIP/DASBOARD_E-ARK_AIP_1_0.pdf (06.03.2018.)

DLM Archival Standards Board (2017., 2.), E_ARK DIP, http://www.dasboard.eu/images/Specifications/DIP/DIP_10_v2.pdf (06.03.2018.)

DLM Archival Standards Board (2017., 3.), E-ARK SIP, http://www.dasboard.eu/images/Specifications/SIP/General_SIP-Specification_v1.4.pdf (06.03.2018.)

eKapija, Usvojen Zakon o elektronskom dokumentu - Elektronski pečat za pravna lica imaće punopravnu snagu, https://www.ekapija.com/news/1910885/usvojen-zakon-o-elektronskom-dokumentu-elektronski-pecat-za-pravna-lica-imace-punopravnu (17.10.2017.)

ETSI (2009.), ETSI TS 102 778-1 V1.1.1 (2009-07); Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES; http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf (21.08.2017.)

ETSI (2009., 2.), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles; TS 102 778-3, http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.01.02_60/ts_10277803v010102p.pdf (30.01.2018.)

ETSI (2010), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), ETSI TS 101 903 V1.4.2 (2010-12), Technical Specification, http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf (21.08.2017.)

ETSI (2010, 2.), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures ETSI TS 102 778-6 V1.1.1 (2010-07) - Technical Specification http://www.etsi.org/deliver/etsi_ts/102700_102799/10277806/01.01.01_60/ts_10277806v010101p.pdf (21.08.2017.)

ETSI (2012.), ETSI TS 103 171 V2.1.1 (2012-03), http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf (21.08.2017.)

ETSI (2013.), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES); ETSI TS 101 733 V2.2.1 (2013-04); http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf (21.08.2017.)

ETSI (2013., 2.), Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile; ETSI TS 103 172 V2.2.2 (2013-04); http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf (22.08.2017.)

ETSI (2016.), Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation ; ETSI EN 319 102-1 V1.1.1 (2016-05); http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf (22.08.2017.)

ETSI (2016., 2.), ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES); http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf (21.08.2017.)

ETSI (2017.), Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI SR 019 510 V1.1.1 (2017-05),

http://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (06.03.2018.)

eurocloud.org, First Cloud Certification in Europe for E-Government-Platform of the BMNT (01.08.2018.)

Europska komisija (2006.), i2010 eGovernment Action Plan, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24226j (10.01.2018.)

Europska komisija (2008.), MoReq2, Model Requirements for the Management of Electronic Records, second version, European Commision, http://moreq2.eu/attachments/article/189/MoReq2_typeset_version.pdf (04.02.2018.)

Europska komisija (2010.), Europa 2020, Europska strategija za pametan, održiv i uključiv rast, https://mzo.hr/sites/default/files/migrated/europa-2020.pdf (12.01.2018.)

Europska komisija (2010., 2.), Digital agenda for Europe, Rebooting Europe's economy, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (12.01.2018.)

Europska komisija (2010., 3.), The European eGovernment Action Plan 2011-2015, Harnessing ICT to promote smart, sustainable & innovative Government, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF (13.01.2018.)

Europska komisija (2013.), A vision for public services, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3179 (13.01.2018.)

Europska komisija (2014.), Directive on the reuse of Public Sector Information, http://europa.eu/rapid/press-release_IP-14-840_en.htm (16.01.2018.)

Europska komisija (2014., 2.), Study on measuring the economic impact of cloud computing in Europe — SMART 2014/0031,

http://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:173873-2014:TEXT:EN:HTML (18.01.2018.)

Europska komisija (2016.), EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268 (13.01.2018.)

Europska komisija (2016., 2.), European Cloud initiative, http://europa.eu/rapid/press-release_IP-16-1408_en.htm (16.01.2018.)

Europska komisija (2017.),European Interoperability Framework – Implementation Strategy, http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF (16.01.2018.)

Europska komisija (2017., 2.), Akcijski plan za interoperabilnost 2016.-2020., http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN (16.01.2018.)

Europska komisija (2017., 3.), Izvješće o digitalnom razvoju Europe (EDPR) 2017. – profil države: Hrvatska, ec.europa.eu/newsroom/document.cfm?doc_id=44293(15.01.2018.)

Europska komisija, Measuring the economic impact of cloud computing in Europe, Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe (10.01.2017.)

Europska komisija, List of Trusted List information as notified by Member States, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1788 (07.04.2014.)

Europski parlament i Vijeće (1995.), Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, azop.hr/images/dokumenti/168/direktiva_9546ez.doc (20.01.2018.)

Europski parlament i Vijeće (1999.), Uredba 1999/93/EC, https://portal.etsi.org/esi/documents/e-sign-directive.pdf (23.07.2017.)

Europski parlament i Vijeće (2003.), Direktiva 2003/98/EZ Europskog parlamenta i Vijeća iz studenog 2003. o ponovnoj uporabi informacija javnog sektora, https://data.gov.hr/sites/default/files/library/CELEX-32003L0098-HR-TXT.pdf (20.01.2018.)

Europski parlament i Vijeće (2006.), Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123 (30.01.2018.)

Europski parlament i Vijeće (2011.), Uredba br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32011R0182&from=HR (07.08.2017.)

Europski parlament i Vijeće (2012.), Prijedlog uredbe o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kretanja takvih podataka (opća uredba o zaštiti podataka) (COM(2012) 11)

Europski parlament i Vijeće (2013.), Direktiva 2013/37/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o izmjeni Direktive 2003/98/EZ o ponovnoj uporabi informacija javnog sektora, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32013L0037&from=FR (29.01.2018.)

Europski parlament i Vijeće (2014.), Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://publications.europa.eu/hr/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-hr (23.07.2017.)

Europski parlament i Vijeće (2016.), 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 te o stavljanju izvan snage direktive 95/46/EZ (Opća uredba o zaštiti podataka) (23.07.2017.)

Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, e-potpis, materijal predmeta Sigurnost elektroničkog poslovanja, http://www.fer.unizg.hr/_download/repository/7_sigurnost_potpis.pdf (08.04.2015.)

Ferguson, N., Schneier, B., Kohno, T. (2010.), Criptography Engineering: Deisign Principles and Practical Applicarion, Wiley Publishing

FINA (2.), Pravilnik o administriranju korisnika i certifikata v1.0, http://demo-pki.fina.hr/dokumentacija/pak.pdf (31.03.2003).

Filipinski Senat (2000.), Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, http://www.fda.gov.ph/attachments/article/29048/RA%208792%20E%20Commerce%20Law.pdf (02.02.2018.)

Friedman, W. F. (1987.), The Index of Coincidence and Its Applications in Cryptography, A Cryptographic series, Riverbank Publication No. 22, Riverbank Labs, 1920. Reprinted by Aegean Park Press

Giacomello, G. (2005.), National Governments and Control of the Internet: A Digital Challenge, New York

Gladney, H. (2011.), US Patent, US Patent 13/219,630 Method And System For Preparing Digital Information For
Long-Term Preservation, https://patents.google.com/patent/US20130054607 (06.03.2018.)

Grbac, M. (2016.), Tranzicija javnobilježničke službe - od tradicije do elektronifikacije, Javni bilježnik, broj 43, str. 107-112,

http://www.hjk.hr/Portals/0/CasopisJB/Javni%20bilje%C5%BEnik%2043.pdf (01.02.2018.)

Gruzijski parlament (2008.), Law of Georgia on electronic signatures and electronic documents, https://matsne.gov.ge/ru/document/download/20866/4/en/pdf (03.02.2018.)

Haber, S., Kamat, P. (2006.), A content integrity service for long-term digital archives, IS&T Archiving 2006 Conference, http://www.hpl.hp.com/techreports/2006/HPL-2006-54.pdf (14.03.2018.)

Halachmi, A., E-Government Theory and Practice: The Evidence from Tennessee (USA), National Center for Public Productivity, Rutgers University

Halderman, B., Moore, H., Wustrow, N. (2014.), Elliptic Curve Cryptography in Practice; Financial Cryptography and Data Security, Springer; https://eprint.iacr.org/2013/734.pdf (18.03.2015.)

Heđbeli, Ž., Missoni, E. et al. (2016.), Arhiviranje, evidencije i rokovi čuvanja dokumentacije, TEB Poslovno savjetovanje d.o.o., Zagreb

Housley, R., Polk, W., Ford, W., Solo, D. (2002.), Internet X.509 Public Key Infrastructure, IETF, https://www.ietf.org/rfc/rfc3280.txt (21.03.2018.)

Hrvatski sabor (1997.), Zakon o arhivskom gradivu i arhivima, https://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_105_1617.html (03.02.2018.)

Hrvatski sabor (2002.), Zakon o elektroničkom potpisu, NN 10/02, http://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html (21.03.2018.)

Hrvatski sabor (2005.), Zakon o elektroničkoj ispravi, NN 150/2005, http://www.nn.hr/clanci/sluzbeno/2005/2898.htm (01.02.2018.)

Hrvatski sabor (2014.), Zakon o državnoj informacijskoj infrastrukturi, https://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1840.html (21.01.2018.)

Hrvatski sabor (2017.), Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, NN 62/17 , http://narodne-novine.nn.hr/clanci/sluzbeni/2017_06_62_1430.html (23.07.2017.)

Hrvatski sabor (2017., 2.), Zakon o izmjenama i dopunama zakona o arhivskom gradivu i arhivima, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2017_05_46_1070.html (03.02.2018.)

Hrvatsko arhivsko vijeće (2012), Opći popis arhivskog i registraturnog gradiva s rokovima čuvanja, http://arhinet.arhiv.hr/_Download/PDF/Opci_popis_gradiva_s_rokovima_cuvanja.pdf (28.08.2018.)

Internet World Stats (2006.), Usage and Population Statistics, http://www.internetworldstats.com/stats.htm , (18.09.2006.)

Internet World Stats (2018.), Usage and Population Statistics, http://www.internetworldstats.com/stats.htm , (03.01.2018.)

InterPARES (2002.), The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, http://www.interpares.org/book/index.htm (10.02.2018.)

ISO (2003.), ISO 14721:2003 - Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model; http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284 (07.08.2016.)

ISO (2005.), ISO/IEC 18033-3, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=37972 (04.03.2015.)

ISO (2005., 2.), ISO 19005-1:2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1), https://www.iso.org/standard/38920.html (04.02.2018.)

ISO (2008), ISO 32000-1:2008 - Document management - Portable document format - Part 1: PDF 1.7; https://www.iso.org/standard/51502.html (21.08.2017.)

ISO (2008., 2.), XFDU, XML Formatted Data Unit, Structure and Construction Rules, CCSDS 661.0-B-1. Blue Book, ISO 13527:2010, https://public.ccsds.org/Pubs/661x0b1.pdf (19.02.2018.)

ISO (2011.), ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2), https://www.iso.org/standard/50655.html (04.02.2018.)

ISO (2011., 2.), ISO 15489: Information and documentation – Records management, International Organization for Standardization, https://www.iso.org/standard/31908.html

ISO (2012.), ISO 14721:2012, http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683 (07.08.2016.)

ISO (2012., 2.), ISO 19005-3:2012 - Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3) (04.02.2018.)

Jacobs, J., Clemmer, L., Dalton, M., Rogers, R., Posluns, J. (2003.), SSCP Study Guide, Syngress Publishing, str. 330-331.

Jeroen, B., Van de Sompel, H. (2005.), Access Interfaces for Open Archival Information Systems based on the OAI-PMH and the OpenURL Framework for Context-Sensitive Services, Digital Library Research & Prototyping Team, Los Alamos National Laboratory, Dept. of Architecture and Urbanism, Faculty of Engineering, Ghent University, http://www.ukoln.ac.uk/events/pv-2005/pv-2005-final-papers/032.pdf (28.11.2016.)

Kahn, D. (1996.), The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised edition, New York,

Scribner, http://math.boisestate.edu/~liljanab/MATH509Spring2012/IndexCoincidence.pdf (04.03.2015.)

Kanadski parlament (2000.), Personal Information Protection and Electronic Documents Act, https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html (02.02.2018.)

Katulić, T. (2011.), Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u hrvatskom i poredbenom pravu, Zbornik PFZ, 61, (4) 1339-1378 (2011), http://hrcak.srce.hr/70481 (31.01.2018.)

Katulić. T. (2016.), Stiže Opća uredba o zaštiti podataka, https://www.bug.hr/molex/general-data-protection-regulation/97346.aspx (29.05.2016.)

Kazahstanski parlament (2003.). Law of the Republic of Kazakhstan No. 370-?? of January 7, 2003, on Electronic Documents and Electronic Digital Signatures, http://www.wipo.int/wipolex/en/details.jsp?id=16138 (03.02.2018.)

Konheim, A. G. (2007.), Computer security and cryptography, Wiley

Krier, L., Strasser, C. (2014.), Data Management for Libraries: A LITA Guide StrasserData Management for Libraries: A LITA Guide, Chicago(18.02.2014.)

Kushchu, I., Kuscu, H. (2003.), From E-government to M-government: Facing the Inevitable, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan045367.pdf (21.03.2018.)

Kushchu, I., Kuscu, H., Mobile Government, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040049.pdf (31.12.2017.)

Kutičić, D., Infrastruktura javnog ključa - PKI, Otvoreni sustavi i sigurnost, http://security.foi.hr/wiki/index.php/Infrastruktura_javnog_klju%C4%8Da_-_PKI (04.03.2015.)

Kuvajtska centralna agencija za informacijsku tehnologiju (2014.), Law No. 20 of 2014. Concerning Electronic Transactions, https://www.csb.gov.kw/images/Magazine_E.pdf (03.02.2018.)

Lavoie, B. (2014.), The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition), DPC Technology Watch Series Report 14-02, https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file (28.11.2016.)

Lee, C. A. (2005.), Defining digital preservation work: a case study of the development of the reference model for an open archival information system, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/39372/dissertation_callee.pdf?sequence=2&isAllowed=y (20.11.2016.)

Lemieux, V. L. (2015.), Blockchain Technology for Recordkeeping, The University of British Columbia, Vancouver, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjo45yquaHZAhWH_ywKHarXDBwQFgg9MAI&url=https%3A%2F%2Fwww.researchgate.net%2Fprofile%2FVictoria_Lemieux%2Fpublication%2F309414363_Blockchain_for_Recordkeeping_Help_or_Hype%2Flinks%2F580f539408ae009606bb62f6%2FBlockchain-for-Recordkeeping-Help-or-Hype.pdf&usg=AOvVaw3BACiNT3YaeubXd3zG54iJ (12.02.2018.)

Lenstra, A.K., Verheul, E.R. (2001.), Selecting cryptographic key sizes, Journal of Cryptology 14, str. 255-293.

Linn, J. (1993.), Privacy Enhancement for Internet Electronic Mail, IETF, http://www.ietf.org/rfc/rfc1421.txt (21.03.2018.)

Lipp, P. (2015.), Signature Validation – a Dark Art?, Information Security Solutions Europe 2015 Conference, Berlin, str. 196-205 (11.03.2018.)

Lipp, P. (2015., 2.), Signature Validation - a black art? TU Graz, prezentacija s konferencije Information Security Solutions Europe konferencije, Berlin, https://www.eema.org/wp-content/uploads/lipp.pdf , str. 12.-13, (25.12.2017.)

Lisičar, H. (2010.), Mogućnosti uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku, Zbornik PFZ, 60, (3) 1391-1422 (2010), str.1395, https://hrcak.srce.hr/file/94423 (31.01.2018.)

Litvanski parlament, Seima (1995.), Law on Documents and Archives, Seimas of the Republic of Lithuania, (zadnji amadmani su iz 2008.), http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=404607 (23.02.2018.)

Litvanski parlament, Seima (2004.), Electronic Documents Law, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&cad=rja&uact=8&ved=0ahUKEwjl9sWM-PjYAhUSKuwKHcIZAts4ChAWCDMwAQ&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FCiti%2FElectronic_Documents_Law.doc&usg=AOvVaw0QRJjM2mPtfH3lGZSiH0Xl (03.02.2018.)

Lukičić, M., Sruk, V. (2009.), Electronic Records Management System Requirements, INFuture2009: "Digital Resources and Knowledge Sharing", Zagreb, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjHl8GW4fHZAhWPKCwKHd2CAPwQFgg0MAI&url=https%3A%2F%2Finfoz.ffzg.hr%2Finfuture%2F2009%2Fpapers%2F2-02%2520Lukicic%2C%2520Sruk%2C%2520ERMS%2520requirements.pdf&usg=AOvVaw1HDduFU1CF7-Z_GGgyF9Ck (16.03.2018.)

Lukšaite, D. (2012.), The life cycle of e-documents: methodological and legal approach in Lithuania, Nordic Baltic Seminar "Practical Aspects of E-Signature and E-Documents Use in the Framework of Digital Single Market", http://www.rrt.lt/download/16522/5%20nb8%20archives%20lt-1.pdf (23.02.2018.)

Maganić, A. (2013.), Javni bilježnik u elektroničkom pravnom prometu, Zbornik PFZ, 63, (2) 383-431 (2013), https://hrcak.srce.hr/file/161630 (01.02.2018.)

Malmö Declaration on eGovernment (2009.), 5th Ministerial eGovernment Conference, Malmö, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf (13.01.2018.)

Markovinović, N. (2017.), Kako učinkovito provesti Data Protection Impact Assessment (DPIA)?, https://gdpr2018.eu/kako-ucinkovito-provesti-data-protection-impact-assessment-dpia/ (09.10.2017.)

McDonough, J., METS: Standardized Encoding for Digital Library Objects, University of Illinois, https://www.ideals.illinois.edu/bitstream/handle/2142/177/METS.pdf?sequence=2 (18.02.2018.)

Mell, P., Grance, T. (2011.), The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (17.01.2018.)

Menezes, A., van Oorschot, P., Vanstone, S. (1997.), Handbook of Applied Cryptography, CRC Press

Merkle, R., C. (1980.), Protocols for public key cryptosystems, Simpozij sigurnosti i privatnosti, Oakland, https://www.computer.org/csdl/proceedings/sp/1980/0335/00/06233691-abs.html , str. 122–134 (10.03.2018.)

Ministarstvo gospodarstva RH, Evidencija davatelja usluga certificiranja u Republici Hrvatskoj, http://mingo.fina.hr/index.html (07.04.2015.)

Ministarstvo gospodarstva (2013.), Popis normizacijskih dokumenata u području primjene zakona o elektroničkom potpisu i pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj, (NN 89/13), https://narodne-novine.nn.hr/clanci/sluzbeni/2013_07_89_1957.html (04.02.2018.)

Ministarstvo kulture (2002.), Pravilnik o vrednovanju te postupku odabiranja i izlučivanja arhivskoga gradiva, Ministarstvo kulture, https://narodne-novine.nn.hr/clanci/sluzbeni/2002_07_90_1476.html (03.02.2018.)

Ministarstvo kulture (2004.), Pravilnik o zaštiti i čuvanju arhivskog i registraturnog gradiva izvan arhiva, https://narodne-novine.nn.hr/clanci/sluzbeni/2004_05_63_1383.html (03.02.2018.)

Ministarstvo uprave (2017.), Strategija e-Hrvatska 2020, https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 (10.01.2018.)

Ministarstvo uprave (2017., 2.), Akcijski plan za provedbu Strategije e-Hrvatska 2020, https://uprava.gov.hr/UserDocsImages//e-Hrvatska//Akcijski%20plan%20za%20provedbu%20Strategije%20e-Hrvatska%202020.pdf (21.01.2018.)

Moriarty, K., Nystrom, M., Parkinson, S., Rusch, A., Scott, M. (2004.), PKCS #12: Personal Information Exchange Syntax v1.1, http://tools.ietf.org/html/rfc7292 (21.03.2018.)

Myers, M. et al. (1999), X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP, Network Working Group, The Internet Society, URL: http://www.ietf.org/rfc/rfc2560.txt (14.04.2014.)

Nacional Archives and Record Administration (2000.), Records Management Guidance for Agencies Implementing Electronic Signature Technologies, https://www.archives.gov/files/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf (08.02.2018.)

Narodna skupština Republike Srbije (2017.), Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, https://www.ekapija.com/dokumenti/ZAKON_o_elektronskom_dokumentu_elektronskoj_identifikaciji_i_uslugama_od_poverenja_u_elektronskom_poslovanju_231017.pdf (03.02.2018.)

National Archives of Canada (2001.), Guidelines For Records Created Under a Public KeyInfrastructure Using Encryption And Digital Signatures (10.02.2018.)

Nakomoto, S.(2008.), Bitcoin: A Peer-to-Peer Electronic Cash System, http://nakamotoinstitute.org/bitcoin/#selection-7.4-9.38 (12.02.2018.)

New Zealand e-Government Interoperability Framework (2005.), https://www.oasis-open.org/committees/download.php/13081/e-GIF%20v3.0%20draft%2023-05-2005.pdf (16.01.2108.)

Paradigm.ac.uk, Metadata for authenticity: hash functions and digital signatures, http://www.paradigm.ac.uk/workbook/metadata/authenticity-xml.html (19.02.2018.)

Pinkas, D. et al. (2003.), RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs), https://tools.ietf.org/html/rfc3628 (25.07.2017.)

Płoszajski, G. (2017.), Metadata in Long-Term Digital Preservation; Digital Preservation: Putting It to Work; Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T., str. 15-61, http://www.springer.com/978-3-319-51800-8 (19.02.2018.)

Poushter, J. (2016.), Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use, PewResearchCenter, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-

internet-usage-continues-to-climb-in-emerging-economies/technology-report-01-03/ (01.01.2018.)

Publiciations Quebec (2012.), Act to establish a legal framework for information technology, https://www.canlii.org/en/qc/laws/stat/rsq-c-c-1.1/latest/rsq-c-c-1.1.html?searchUrlHash=AAAAAQBBQW4gQWN0IHRvIGVzdGFibGlzaCBhIGxlZ2FsIGZyYW1ld29yayBmb3IgaW5mb3JtYXRpb24gdGVjaG5vbG9neSAAAAAAAQ (02.02.2018.)

Ragaisis, S., Birstunas, A., Mitasiunas, A., Stockus, A. (2012.), Electronic Archive Information System, Vilnius University, Lithuania; http://ceur-ws.org/Vol-924/paper11.pdf , str. 107-114 (23.02.2018.)

Rajh, A. (2010.), Teorijski model digitalnog arhivskog sustava u domeni regulacije tržišta lijekova, doktorska disertacija, Zagreb, Filozofski fakultet, 303 str. Voditelj: Stančić, H., https://www.researchgate.net/publication/310450300_Teorijski_model_digitalnog_arhivskog_sustava_u_domeni_regulacije_trzista_lijekova_Theoretical_Model_of_Digital_Archival_System_in_the_National_Competent_Body_for_Marketing_Authorization_of_Medicines (26.02.2018.)

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, 48. savjetovanje hrvatskih arhivista Zaštita arhivskog gradiva u nastajanju, Topusko, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjA1or9sL_ZAhUBDuwKHRiMDJcQFgguMAE&url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F310453035_Digitalizacija_prihvat_i_migracija_gradiva_u_sustav_upravljanja_zapisima_sa_ciljevima_ostvarivanja_temeljnih_funkcija_HALMED-a_i_ocuvanja_gradiva_Digitisation_ingest_and_migration_of_archival_records_&usg=AOvVaw178pndAHhSZ8dNVMffRT91 (24.02.2018.)

Rajh, A., Šimundža-Perojević, Z. (2016.), Projekti digitalizacije dokumentacije o lijekovima u Agenciji za lijekove i medicinske proizvode, Šesti festival hrvatskih

digitalizacijskih projekata, Nacionalna i sveučilišna knjižnica u Zagrebu, http://dfest.nsk.hr/2016/wp-content/uploads/2016/04/Rajh_Simundza.pdf (24.02.2018.)

Rajh, A. (2017.), Digital Archives: Towards the Next Step, INFuture 2017: The Future of Information Sciences: Integrating ICT in Society; Atanassova, Iana; Zaghouani, Wajdi; Kragić, Bruno; Kuldar, Aas; Stančić, Hrvoje; Seljan, Sanja (ur.)., Zagreb, Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, 116. (115-120.) , https://www.researchgate.net/publication/320934421_Digital_Archives_Towards_the_Next_Step_INFuture_2017_The_Future_of_Information_Sciences_Integrating_ICT_in_Society_Atanassova_Iana_Zaghouani_Wajdi_Kragic_Bruno_Kuldar_Aas_Stancic_Hrvoje_Seljan_Sanja_u (26.02.2018.)

Rajh, A., Šimundža-Perojević, Z. (2018.), Lessons learned from internal and external digitisation processes implemented at the Croatian Agency for Medicinal Products and Medical Devices, izlaganje na konferenciji Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja (Radenci, 11. – 13.4.2018.), https://www.researchgate.net/publication/326836150_Lessons_learned_from_internal_and_external_digitisation_processes_implemented_at_the_Croatian_Agency_for_Medicinal_Products_and_Medical_Devices (03.09.2018.)

Ramadoss, B., Palanisamy, R. (2004.), Issues and challenges in electronic governance planning, https://www.researchgate.net/publication/220082762_Issues_and_challenges_in_e-governance_planning (31.12.2017.)

Registri Škotske u ime škotske vlade (2014.), The electronic documents (Scotland) regulations, SSI 2014/83, http://www.legislation.gov.uk/ssi/2014/83/pdfs/ssipn_20140083_en.pdf (03.02.2018.)

Rivest, R.L., Shamir A., Aldeman, L.M. (1977.), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, str. 120.-126.

Roessler, T. et al. (2010.), D2.1 Inventory of standard documents and relations to open specifications, projekt SPOCS, http://www.eu-spocs-starterkit.eu/images/files/D2.1_List_of_standard_documents_and_relations_to_open_specifications.pdf (30.01.2018.)

Rueppel, R.A. (1992.), Stream Ciphers, Contemporary Cryptology - The Science of Information Integrity, edited by G.J.Simmons, New York, IEEE Press, str. 65.-134.

Sabor Republike Hrvatske (2014.), Zakon o državnoj informacijskoj infrastrukturi, https://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1840.html (21.01.2018.)

Sabor Republike Hrvatske (2016.), Zakon o mjerama za smanjenje troškova postavljanja elektroničkih komunikacijskih mreža velikih brzina, https://narodne-novine.nn.hr/clanci/sluzbeni/2016_12_121_2623.html (21.01.2018.)

Salza, S., Guercio, M. (2012), Authenticity Management in Long Term Digital Preservation of Medical Records, iPRES2012, Proceedings of the 9th International

Conference on Preservation of Digital Objects, Toronto, https://www.researchgate.net/profile/Joy_Davidson/publication/263850207_Addressing_data_management_training_needs_a_practice_based_approach_from_the_UK/links/0046353c14234d93c7000000.pdf#page=182 , str. 172-179 (06.03.2018.)

Schwalm, S., Korte, U. (2014.), Standards for the Preservation of Evidence and Trust for Electronic Records, IS&T Archiving 2014 Conference, Berlin, https://www.researchgate.net/publication/263474467_Standards_for_the_Preservation_of_Evidence_and_Trust_for_Electronic_Records (10.03.2018.)

Schwalm, S. (2017.), A service for the preservation of evidence and data-a key for a trustworthy & sustainable electronic business
Conference: Open Identity Summit 2017 der Gesellschaft für Informatik, Karlstad/Sweden, Volume: GI Editions, Lecturer Notes in Informatics, Lothar Fritsch et. al., https://www.researchgate.net/publication/320286971_A_service_for_the_preservation_of_

evidence_and_data-a_key_for_a_trustworthy_sustainable_electronic_business , str. 131-144 (05.03.2018.)

Seifert, J. W. (2003.), A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance, https://fas.org/sgp/crs/RL31057.pdf

Sertifitseerimiskeskus AS (2016.), ASiC-E/XAdES Signature Policy in Latvia and Estonia–Draft, https://www.ria.ee/public/PKI/LV-EE-Signature-Policy_Draft_EE_TC.pdf (16.03.2018.)

Shannon, C.E. (1949.), Communication Theory of Secrecy Systems, Bell System Tehnical Journal, v. 28, n.4, str. 656-715, http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf (04.03.2015.)

Smith, J.L. (1971.), The Design of Lucifer, a Cryptographic Device for Data Communications, IBM Research Report RC3326, Yorktown Heights, New York, 1971.

Spremić, M, Brzica, H. (2008.), Comparative Analysis of e-Government Implementation Models and Progressive Services, WSEAS transactions on business and economics, http://www.wseas.us/e-library/transactions/economics/2008/27-124.pdf , str. 254-263 (20.01.2018.)

Središnji državni ured za e-Hrvatsku (2004.), Operativni plan provedbe programa e-Hrvatska 2007. za 2004. godinu, http://digured.srce.hr/arhiva/10/10/www.vlada.hr/Download/2004/07/12/Operativni_plan_eHR2004_V1_5.pdf (21.01.2018.)

Središnji državni ured za e-Hrvatsku (2006.), Operativni plan provedbe programa e-Hrvatska 2007. za 2006. godinu, http://digured.srce.hr/arhiva/434/8002/www.e-hrvatska.hr/ehrvatska/modules/Downloads/upload/Operativni_plan_provedbe_Programa_e-Hrvatska_2007_za_2006.pdf (21.01.2018.)

Središnji državni ured za e-Hrvatsku (2009.), Strategija razvoja elektroničke uprave za razdoblje 2009.-2012., http://digured.srce.hr/arhiva/10/31637/strategija_e_Uprave_HRV_final.pdf (21.01.2018.)

Središnji državni ured za e-Hrvatsku (2009., 2.), Operativni plan provedbe programa e-Hrvatska 2009., http://digured.srce.hr/arhiva/434/42111/e-hrvatska.hr/sdu/hr/e-hrv/contentParagraph/011111111111111/document2/Plan_provedbe_e-Hrvatska_2009.pdf (21.01.2018.)

Središnji državni ured za e-Hrvatsku (2011.), Odluka o utvrđivanju ciljeva razvoja elektroničke uprave u tijelima državne uprave za razdoblje od 2011. do 2015. godine, https://uprava.gov.hr/UserDocsImages/eHrvatska/5-Odluka%20Vlade%20RH%20o%20ciljevima%20e-Uprave%202011-2015.pdf (21.01.2018.)

Stallings, W. (2006.), Cryptography and Network Security, Principles and Practices, 5th Edition, Pearson Education

Stančić, H. (2001.), Upravljanje znanjem i globalna informacijska infrastruktura, Magistarski rad, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb

Stančić, H. (2004.), Očuvanje elektroničkih informacijskih objekata: arhivi, knjižnice, muzeji –zajednička koncepcija, u: Katić, Tinka (ur.), Zbornik 7. seminara Arhivi, knjižnice, muzeji, Hrvatsko knjižničarsko društvo, Zagreb, str. 26-35.

Stančić, H. (2005.), Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata, Doktorska disertacija, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb

Stančić, H., Herceg, B., Rajh, A. (2014.), Comparative analysis of internal structure and functions of digital archives preserving complex electronic records, Girona 2014 : Arxius i Indústries Culturals, https://www.girona.cat/web/ica2014/ponents/textos/id185.pdf (24.02.2018.)

Stančić, H., Brzica, H., Adžaga, I., Garić, A., Poljičak-Sušec, M., Presečki, K., Stanković, A. (2015.), Comparative Analysis of Implemented Governmental e-Services (EU09), Final report, InterPARES Trust Project, https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisImplementedGovernmentaleServices_FinalReport.pdf (20.02.2018.)

Stančić, H. (2016.), Preservation of Records Entrusted to the Cloud, Presentation of the InterPARES Trust project, Hague, https://interparestrust.org/assets/public/dissemination/IPT_20161101_eApostilleProgram_TheHague_Stancic_Presentation.pdf (06.02.2108.)

Strahonja, V., Šimić, D. (2010.), Kako EU strategiju za interoperabilnost (EIS) i EU okvir za interoperabilnost (EIF) propagirati u Hrvatskoj i SEE regiji?, 8. Europska konferencija o poslovnim procesima, https://bib.irb.hr/datoteka/579053.2010-04-15_BPC2010_Strahonja_Simic.pdf (16.01.2018.)

Stranacher, K. (2012.), Final Report Work Package 2: eDocuments, http://www.eu-spocs-starterkit.eu/documents#d31 (29.01.2018.)

Tallinn Declaration on eGovernment (2017.), Ministerial eGovernment Conference, Tallin, https://ec.europa.eu/newsroom/document.cfm?doc_id=47559 (13.01.2018.)

Tannam, E. (2017.), Confusion remains around GDPR compliance, https://www.siliconrepublic.com/enterprise/gdpr-compliance-watchguard-survey (14.07.2017.)

Teiwes, S., Hartmann, P., Kuenzi, D. (2001.), RFC 3058 - Use of the IDEA Encryption Algorithm in CMS, http://www.faqs.org/rfcs/rfc3058.html (21.03.2018.)

Thibodeau, K. (2002.), Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, u: The State of Digital Preservation: An International Perspective, Council on Library and Information Resources (CLIR), Washington, D.C., SAD, str. 4-31., https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10 (07.08.2016.)

Thompson, T. (2017.), The preservation of digital signatures on the blockchain, The University of British Columbia iSchool Student Journal Vol. 3 (Spring 2017), http://ojs.library.ubc.ca/index.php/seealso/article/view/188841/186525 (10.02.2018.)

Turner, D. M. (2016.), Advanced Electronic Signatures for eIDAS, Cryptomathic, https://www.cryptomathic.com/news-events/blog/advanced-electronic-signatures (09.08.2017.)

Turner, D. M. (2017.), PAdES and Long Term archival (LTA); https://www.cryptomathic.com/news-events/blog/pades-and-long-term-archival-lta (17.03.2017.)

Ukrajinski parlament (2003.), LAW OF UKRAINE About electronic documents and electronic document management No. 851-IV, http://cis-legislation.com/document.fwx?rgn=11196 (03.02.2018.)

UNI - Ente Italioano de normazione, UNI 11386:2010 (2010.), Supporto all'Interoperabilita nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO), http://store.uni.com/catalogo/index.php/uni-11386-2010.html?josso_back_to=http://store.uni.com/josso-security-check.php&josso_cmd=login_optional&josso_partnerapp_host=store.uni.com (06.03.2018.)

United Nations, Department of Economic and Social Affairs (2003.), World Public sector Report 2003, E-Government at the Crossroads, https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/World%20Public%20Sector%20Report%20series/World%20Public%20Sector%20Report.2003.pdf (03.01.2018.)

United Nations, Department of Economic and Social Affairs (2005.), Global e-government readiness report 2005, New York, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf (11.01.2018.)

United Nations, Department of Economic and Social Affairs (2015.), Transforming our world: the 2030 Agenda for Sustainable Development, Paragraf 15., https://sustainabledevelopment.un.org/post2015/transformingourworld (31.12.2017.)

United Nations, Department of Economic and Social Affairs (2016.), UN E-Government Survey 2016, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016 (31.12.2017.)

Urugvajski Senat (2009.), Ley No 18.600 DOCUMENTO ELECTRÓNICO Y FIRMA ELECTRÓNICA, http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/D09A96E064A5815705257D1C0078B0B3/$FILE/Ley_N%C2%BA_18.600_Documento_Electr%C3%B3nico_y_Firma_Electr%C3%B3nica.pdf (02.02.2018.)

U.S. Congress (2000.), ESIGN - Electronic Signatures in global and national commerce act, https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm (03.02.2018.)

Vacca, J.R. (2004.), Public Key Infrastructure, Building Trusted Applications and Webservices, Taylor & Francis Group

Vlada Republike Hrvatske (2016.), Strategija razvoja širokopojasnog pristupa u Republici Hrvatskoj za razdoblje 2016. – 2020, http://www.mppi.hr/UserDocsImages/Strategija-sirokopojasni-pristup2016-2020-usvojeno%20na%20VRH.pdf (21.01.2018.)

Volarević, I., Stančić, H. (2016.), Norme za elektroničke vremenske žigove i mogućnosti njihove primjene u arhivskoj struci, Arhivi i domovinski rat, Zagreb, str. 425-435, http://www.bib.irb.hr/850052 (08.02.2018.)

Wild, B. (2012.), PDF/A in Healthcare, white paper, PDF Association – PDF/A Competence Center, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiCnczNv77ZAhXD26QKHU7KCZIQFggsMAA&url=https%3A%2F%2

Fwww.pdfa.org%2Fwp-content%2Funtil2016_uploads%2F2012%2F05%2FWP-PDFA-in-Healthcare.pdf&usg=AOvVaw0PYq9l9u_u5UJwI9zwCdCW (24.02.2018.)

World bank (2002.), The E-Government Handbook for Developing Countries, infoDev and The Center for Democracy & Technology, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN007462.pdf (10.01.2018.)

POPIS SLIKA

POPIS TABLICA

ŽIVOTOPIS AUTORA

Hrvoje Brzica je rođen 13.07.1975. u Ivankovu. Nakon završene Gimnazije Matija Antun Reljković u Vinkovcima 1994. upisuje Fakultet elektrotehnike i računarstva, studij računarstva. Navedeni fakultet završava 2000. Pohađa pedagoško-psihološko obrazovanje na Učiteljskom fakultetu u Zagrebu od 2002. do 2003. te ga uspješno završava. Upisuje poslijediplomski znanstveni studij Informatički menadžment na Ekonomskom fakultetu u Zagrebu 2003. te ga završava 2007. godine. obranivši magistarski rad „Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge“ kod mentora dr. sc. Maria Spremića.

Zapošljava se 2000. godine u tvrtki Ericsson NT d.d. u Zagrebu na radnom mjestu softver dizajnera. U Ericssonu radi na projektima VIPNet mShopping te e-Zdravstva. U razdoblju 2003.-2005. radi u tvrtki Combis d.o.o. na radnom mjestu softver dizajnera te sudjeluje na projektima e-ZABA BiH te Carinski IT sustav RH. U razdoblju 2005.-2014. godine radi u Financijskoj agenciji (FINA) na radnom mjestu IT arhitekta te sudjeluje na projektima: e-Mirovinsko, HITRO.HR, e-Račun, HUB3, Sustav ovrha, Predstečajne nagodbe i dr. Od 2014. radi kao voditelj Centra aplikativnog razvoja u Fini. Cijelo vrijeme od prvog zaposlenja pohađa stručne tečajeve i konferencije te je položio certifikacijski program za programiranje u java programskom jeziku.

Doktorski studij Informacijskih i komunikacijskih znanosti upisuje u studenom 2012. godine, a od 2014. godine je uključen u međunarodni znanstveno-istraživački projekt InterPARES Trust, pod vodstvom prof. dr. sc. Hrvoje Stančića. Na navedenom projektu sudjeluje na stručnim sastancima. Zajedno je s istraživačkim timom razvijao metodologije istraživanja te je provodio pojedine faze istraživanja. Tijekom rada na InterPARES Trust projektu te izrade doktorske radnje je intenzivno razmjenjivao iskustava s drugim stručnjacima te je sudjelovao na stručnim radionicama u sklopu kojih se odvijala međunarodna suradnja i razmjena. Objavio je više znanstvenih i preglednih radova s međunarodnom recenzijom. Dva puta je izlagao na međunarodnom znanstvenom skupu INFuture (The Future of Information Sciences).

POPIS OBJAVLJENIH RADOVA

1. Brzica, H (2007.), Razvojne mogućnosti elektroničke javne uprave u Hrvatskoj i primjena pametne kartice za elektroničke javne usluge, Zagreb: Ekonomski fakultet, 189 str. Voditelj: Spremić, Mario, https://bib.irb.hr/datoteka/625998.Poslijediplomski_rad_-_Hrvoje_Brzica.pdf (magistarski rad)
2. Spremić, M, Brzica, H. (2008.), Comparative Analysis of e-Government Implementation Models and Progressive Services, WSEAS transactions on business and economics, str. 254-263, http://www.wseas.us/e-library/transactions/economics/2008/27-124.pdf (objavljeni rad, znanstveni)
3. Brzica, H., Herceg, B., Stančić, H. (2013.), Long-term Preservation of Validity of Electronically Signed Records, Information Governance; Gilliland, A., McKemmish, S., Stančić, H., Seljan, S., Lasić-Lazić, J. (ur.); Zagreb: Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, 4 (2013), str. 147-158, https://bib.irb.hr/datoteka/662133.403_Brzica_Herceg_Stancic_LTP_of_Validity_of_Electronically_Signed_Records.pdf (predavanje, međunarodna recenzija, objavljeni rad, znanstveni)
4. Stančić, H., Rajh, A., Brzica, H. (2015.), Archival Cloud Services : Portability, Continuity, and Sustainability Aspects of Long-term Preservation of Electronically Signed Records = Les services d'archivage dans un nuage informatique : Portabilité, continuité et durabilité: Aspects de la conservation à long terme des documents signés électroniquement, Canadian journal of information and library science, 39 (2015) , str. 210-227, http://muse.jhu.edu/article/590941 (objavljeni rad, znanstveni)
5. Herceg, B., Brzica, H., Stančić, H. (2015.), Digitally Signed Records – Friend or Foe?, e-Institutions - Openness, Accessibility, and Preservation; Anderson, K., Duranti, L., Jaworski, R., Stančić, H., Seljan, S., Mateljan, V. (ur.); Zagreb : Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, Croatia, str. 147-150, https://bib.irb.hr/datoteka/786910.3-07_Herceg_Brzica_Stancic_Digitally_Signed_Records_-_Friend_or_Foe.pdf (predavanje, međunarodna recenzija, objavljeni rad, znanstveni)