Filozofski fakultet
Sveučilišta u Zagrebu
Odsjek za informacijske i komunikacijske znanosti
Katedra za arhivistiku i dokumentalistiku
Ak. god. 2017./2018.

Ira Volarević

Digitalne vremenske oznake i mogućnosti njihovog korištenja u kontekstu dugotrajnog očuvanja digitalnih zapisa

Diplomski rad

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

Zagreb, rujan 2018.

SADRŽAJ

1. UVOD

Jedna od najuočljivijih karakteristika suvremenog svijeta upravo je tehnologija koja se sve brže razvija te preuzima sve veću važnost u našim svakodnevnim životima, kako privatnim tako i poslovnim. Poslovni svijet gotovo je nezamisliv bez interneta i digitalnog okruženja, a to se najviše očituje u sve manjoj uporabi papira, te prelasku na elektroničke dokumente. Posljedično, standardni vlastoručni potpisi sve se češće zamjenjuju elektroničkima, što s jedne strane olakšava poslovanje, ali otvara vrata novim vrstama problema. Između ostalog, postavlja se pitanje kako se pismohrane i arhivi trebaju nositi s takvim dokumentima te kako njihovo postojanje utječe na tradicionalne metode dugoročnog očuvanja. Premda postoje međunarodne norme te zakonski okviri na državnim razinama koji propisuju uporabu elektroničkih potpisa, njihova primjena i provođenje u praksi još uvijek su u ranoj fazi, osobito u Republici Hrvatskoj. Stupanjem na snagu Uredbe Europske Unije br. 910/2014 (eIDAS), stvorili su se zajednički temelji za sigurnu elektroničku interakciju između građana, tvrtki i tijela javne vlasti na području EU-a, pa tako i Hrvatske. Tom se uredbom, između ostalog, uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate i elektroničke vremenske žigove, a upravo su ti posljednji tema ovog diplomskog rada. Naime, elektronički vremenski žigovi važni su jer služe kao dokaz da je neki podatak postojao u točno određenom trenutku, pa se zato najčešće vežu uz elektroničke potpise jer doprinose njihovoj vjerodostojnosti i povjerljivosti. Međutim, može li se njihova uloga proširiti i na područje arhivske djelatnosti, odnosno dugoročnog očuvanja elektroničkih dokumenata? Također, na koji način njihova primjena u arhivskoj praksi, bilo u kontekstu dugoročnog upravljanja zapisima ili dugoročnog arhiviranja, može biti korisna, odnosno problematična? Na ta i druga povezana pitanja pokušat će se odgovoriti u ovom diplomskom radu. Najprije će se objasniti pojam elektroničkog vremenskog žiga i to putem analize odgovarajućih međunarodnih normi. Potom će se analizirati standardi posvećeni vremenskim žigovima u kontekstu dugoročnog očuvanja te oni standardi koji se bave tijelima i uslugama povezanim s izdavanjem i verifikacijom elektroničkih vremenskih žigova. U tom će se kontekstu analizirati i modaliteti primjene prodiskutiranih normi, prvenstveno u zakonodavnom okviru Republike Hrvatske. Na kraju će se raspraviti o značenju elektroničkih vremenskih žigova u kontekstu arhivske djelatnosti i dugoročnog očuvanja elektroničkih zapisa, s posebnim naglaskom na potencijalnim poteškoćama i ograničenjima.

2. VREMENSKI ŽIGOVI

Vremenska oznaka, odnosno vremenski žig, po svojoj najširoj definiciji može se opisati kao niz znakova kojima se utvrđuje vrijeme nekog događaja. Primjerice, vremenskim žigom možemo smatrati datum izdanja na naslovnici novina, godinu proizvodnje otisnutu na boci vina, ili pak datum slanja pisma koji je žigom otisnut na omotnici. Dapače, engleski izraz *timestamp* izvorno se odnosio upravo na poštanske žigove. Drugim riječima, vremenski žig daje informaciju o vremenu kada je nešto nastalo ili kada se nešto dogodilo, u obliku i širini koja je u danom kontekstu potrebna. Tako je na spomenutoj boci vina otisnuta samo godina jer je to dovoljna informacija u kontekstu enologije, dok je na novinama otisnut puni datum jer one izlaze svakodnevno i takva je informacija ključna radi razlikovanja aktualnih od starih vijesti. Upravo je ta distinkcija jedan od osnovnih razloga zašto postoji te zašto se upotrebljava digitalni vremenski žig. U digitalnom su svijetu vremenski žigovi sveprisutni – kada pišemo dokumente na računalu, uvijek im se automatski dodaje i informacija o trenutku kada ih pohranjujemo kako bismo znali kada su posljednji put izmijenjeni; kada objavljujemo statuse na društvenim mrežama, uvijek im je dodana informacija o vremenu; kada fotografiramo mobitelom ili digitalnim fotoaparatom, svaka fotografija ima vrlo detaljnu vremensku oznaku. Ukratko, većina naših poteza na internetu ili u digitalnom svijetu općenito može se poredati u vrlo jasan i razrađen vremenski slijed. Zašto je to potrebno? Mnogo je razloga zašto su vremenski žigovi važni, od potrebe da se – kao u slučaju novina – lako identificiraju aktualnosti, do želje da se jednostavno prati kada je neka informacija nastala ili kada je izbrisana. U većini slučajeva, informacija o vremenu nije nam osobito važna, te ni ne upravljamo njezinim stvaranjem. Međutim, u određenim situacijama vremenska oznaka može biti ključna za rješavanje nekog problema ili utvrđivanja istinitosti neke informacije. Takva vrsta vremenskih oznaka tema je ovog diplomskog rada.

Elektronički vremenski žig, prema definiciji danoj u standardu ETSI EN 319 422, čine „podaci u elektroničkom obliku koji vežu druge elektroničke podatke s određenim trenutkom u vremenu i tako uspostavljaju dokaz da je taj podatak postojao u to vrijeme.“[1] Oni dakle nikada ne postoje samostalno, nego se najčešće vežu uz elektroničke potpise, potvrđujući tako njihovo

[1] ETSI, 2016. ETSI EN 319 422 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf (10.9.2018.), str. 6

postojanje u određenom vremenskom razdoblju. Kao takvi imaju važnu ulogu za potvrdu valjanosti i ispravnosti elektronički potpisanih dokumenata, pa ih se najčešće upotrebljava za svakodnevne poslovne aktivnosti u okviru raznih područja rada. Kako se radi o računalno generiranim podacima čija je uporaba svestrana i važna u našem vrlo digitaliziranom svijetu, vrlo se rano javila potreba na standardizacijom postupka stvaranja te samih funkcija elektroničkih vremenskih žigova. Time se osigurava da je njihova uporaba sigurna te ujednačena na globalnoj razini. U nastavku će se detaljnije proći tri takva standarda: RFC 3161, izdan 2001. godine, te kao takav najraniji, potom ISO 18014, podijeljen u tri poglavlja izdana 2008. i 2009. godine, te europska norma ETSI EN 319 422 iz 2016. godine, kojom se standardizira uporaba vremenskih žigova na europskom tržištu, a u okviru regulative Europske unije poznatije kao eIDAS. Kroz te će se standarde opisati što su elektronički vremenski žigovi, kako se stvaraju i koja je njihova uloga, te koja se sve tijela i institucije mogu povezati s njima.

2.1. RFC 3161

Standard RFC 3161, punog naziva *Internet X.509 Public Key Infrastructure Time-Stamp Protocol*, objavljen je 2001. godine, a opisuje postupak kojim nadležna služba izdaje vremenske žigove, te se njime također utvrđuje nekoliko sigurnosnih preduvjeta za rad tog tijela, u kontekstu obrade zahtjeva za izdavanjem vremenskog žiga. Naglasak je stavljen na precizno definiranje formata poruka koje naručitelj i nadležna služba razmjenjuju. Također, u standardu se definira što je točno služba za izdavanje vremenskih žigova (engl. *Time Stamping Authority*, TSA), koja je njezina uloga te koje sve zahtjeve treba zadovoljiti kako bi se vremenske žigovi koje izdaje smatrali točnima i vjerodostojnima. S obzirom na to da se radi o jednoj od najranijih normi koji se odnose na elektroničke vremenske žigove, RFC 3161 poslužio je i kao osnova za tehničku specifikaciju Europske unije, ETSI TS 119 422 (*Electronic Signatures and Infrastructures; Time-stamping protocol and time-stamp profiles*). Naime, u okviru Europske organizacije za standarde (European Standards Organization) te Europske unije funkcionira i ETSI (European Telecommunications Standards Institute), neprofitna organizacija koja se bavi izradom normi na području telekomunikacija. Među standardima koje je ta organizacija objavila ima nekoliko koji su relevantni za temu ovog diplomskog rada, poput spomenute specifikacije ETSI TS 119 422. Ona uvelike preuzima tekst norme RFC 3161, samo što dodaje određena ograničenja, kojima se ta norma prilagođava propisima koji vrijede unutar EU-a.[2]

[2] ETSI EN 319 422, str. 4

Također, tom se tehničkom specifikacijom obrađuju samo protokoli vezani uz izdavanje vremenskih žigova, dok je postupak njihove verifikacije obuhvaćen drugim standardom, kojemu je posvećeno kasnije poglavlje (ETSI 319 102-1).

Prema RFC-u 3161, „uloga službe za izdavanje vremenskih žigova jest vezati vremenski žig na određene podatke i tako stvoriti dokaz da su ti podaci postojali prije određenog datuma, odnosno trenutka.“[3] Takvim se vremenskim žigom može, primjerice, označiti da je dokument predan unutar zadanog roka, ili svjedočiti o točnom trenutku provođenja neke transakcije. Ipak, vremenski se žigovi najčešće vežu uz elektroničke potpise i dokazuju da je potpis postojao u određenom trenutku, odnosno prije isteka njegovog certifikata. Na taj se način elektronički potpisi mogu validirati i nakon isteka valjanosti njihovog certifikata.

Ovom normom opisan je postupak izdavanja vremenskih žigova, a on uključuje nekoliko koraka. Prvi je korak poruka koju podnositelj zahtjeva za izdavanjem vremenskog žiga šalje nadležnom tijelu. Ta bi poruka trebala uključivati *hash* vrijednost podataka kojima se želi pridodati vremenski žig (ta bi vrijednost trebala biti jednosmjerna i otporna na koliziju; engl. *one-way, collision-resistant*), a koju nadležno tijelo treba provjeriti te utvrditi je li zadovoljavajuća, odnosno dovoljna. Ako nadležno tijelo ne prepoznaje *hash* vrijednost ili smatra da ona nije dovoljno snažna, dužna je odbiti izdati vremenski žig te poslati povratnu informaciju s objašnjenjem da zahtjev sadrži neispravan algoritam. Osim tog ključnog podatka, poruka podnositelja zahtjeva može sadržavati i točan protokol, odnosno pravila kojih se nadležno tijelo treba držati, *nonce* vrijednost (veliki nasumičan broj za koji je vrlo vjerojatno da ga je klijent generirao samo jednom) kojom se potvrđuje pravovremenost odgovora, te ekstenzije kojima se otvara mogućnost dodavanja naknadnih informacija zahtjevu. Također je moguće da podnositelj zahtjeva traži da nadležno tijelo pošalje certifikat svog tajnog ključa. Prema specifikaciji ETSI TS 119 422, svi navedeni elementi poruke moraju biti prisutni.

Drugi je korak odgovor koji nadležno tijelo šalje podnositelju zahtjeva, a u kojemu mu šalje odgovarajući vremenski žig. Međutim, ako neki od elemenata poruke koju je poslao podnositelj zahtjeva ne prođu provjeru, nadležno tijelo mora obavijestiti podnositelja zahtjeva o prisutnosti greške te mu ne smije izdati vremenski žig. Također, svaka poruka s izdanim vremenskim žigom mora sadržavati i identifikator certifikata nadležnog tijela u obliku atributa, te mora sadržavati pravila u okviru kojih je vremenski žig izdan. Naravno, ako poruka sadrži

[3] Adams, C., Cain, P., Pinkas, D., Zuccherato, R., Integris, 2001. RFC 3161: Internet x.509 Public key infrastructure time-stamp protocol, https://tools.ietf.org/pdf/rfc3161.pdf (10.9.2018.), str. 2

izdani vremenski žig, dodana je i informacija o trenutku njegovog izdavanja, u obliku UTC vremena (engl. *Coordinated Universal Time*). Ako je zahtjev klijenta sadržavao *nonce* vrijednost, mora je sadržavati i poruka odgovora. Također je moguće da podnositelj zahtjeva traži da nadležno tijelo pošalje certifikat svog privatnog ključa. I specifikacija ETSI TS 119 422 zahtijeva da svi navedeni elementi poruke budu prisutni.

Po primitku odgovora, podnositelj zahtjeva treba potvrditi sve elemente, uključujući pravovremenost primljenog odgovora. U slučaju primitka poruke koja izvještava o postojanju greške, podnositelj zahtjeva treba je ispraviti te ponoviti čitav postupak. Jako je važno da podnositelj zahtjeva provjeri valjanost certifikata nadležnoga tijela, jer u slučaju njegovoga isteka ili opoziva dobiveni vremenski žig nije valjan. Na istu stvar upozorava i specifikacija ETSI TS 119 422.

Nakon teoretskog opisa ovog postupka, u standardu RFC 3161 na prilično se opširan i detaljan način opisuje tehnička strana postupka izdavanja vremenskih žigova (daje se potpuna sintaksa poruka te precizan format i poredak svih elemenata zahtjeva i odgovora), koji nije nužno objašnjavati za potrebe ovoga rada. Jednako tako, gotovo jednak opis daje se i u specifikaciji ETSI TS 119 422.

2.2. ISO/IEC 18014

Međunarodni standard ISO/IEC 18014 prvi je put izdan 2002. godine, ali drugo izdanje, iz 2008. godine, koje je tehnički revidirano, zamijenilo je tu prvu verziju, a čitav je standard ponovno pregledan i potvrđen 2014. godine, tako da i dalje vrijedi u postojećem obliku. Sastavio ga je zajednički tehnički odbor (Joint Technical Committee), a smješten je u kategoriju informacijskih tehnologija, potkategorija tehnike sigurnosti. U cijelosti je posvećen vremenskim žigovima, a podijeljen je na tri dijela:

- Prvi dio: Okvir *(Framework)*
- Drugi dio: Mehanizmi stvaranja neovisnih tokena *(Mechanisms producing independent tokens)*
- Treći dio: Mehanizmi stvaranja vezanih tokena *(Mechanisms producing linked tokens)*

U nastavku će se analizirati svaki od ta tri dijela, s naglaskom na prvom, koji daje osnovne informacije o stvaranju i uporabi vremenskih žigova, te se također može povezati s ranije opisanim standardom RFC 3161.

2.2.1. ISO 18014-1

U prvom dijelu ove norme objašnjava se uloga službe za izdavanje vremenskih žigova, daje se opis temeljnog modela na kojem te službe rade, definiraju se usluge izdavanja vremenskih žigova te temeljni protokoli između sudionika u tom procesu. U tu svrhu, daju se i definicije najvažnijih pojmova. Tako je vremenski žig (engl. *Time-stamp*) definiran kao parametar vremena kojim se određuje jedan trenutak u kontekstu dogovorene vremenske reference.[4] Srodan i jednako važan termin jest token vremenskog žiga (engl. *Time-stamp Token*), odnosno podatkovna struktura kojom se uspostavlja provjerljiva veza između prikaza podataka i parametra vremena.[5] Kako bi služba za izdavanje vremenskih žigova (engl. *Time-stamping Authority*), odnosno treća strana od povjerenja, mogla izdati valjani vremenski žig, nužno je postojanje *hash* funkcije koja je otporna na koliziju. *Hash* funkcija definira se kao funkcija koja mapira niz bitova u nizove fiksne duljine, tako da je računalno nemoguće za zadani izlaz pronaći ulaz koji vodi do njega, ili za zadani ulaz pronaći još jedan ulaz koji vodi do istog izlaza.[6] Također, ta vrijednost mora biti otporna na koliziju, što znači da ne postoje dva različita ulaza koja vode do istog izlaza. Naravno, definira se i elektronički potpis (engl. *Digital Signature*), i to kao skup podataka dodan jedinici podataka koji omogućuju primatelju jedinice podataka da dokaže porijeklo i integritet tih podataka te štite pošiljatelja i primatelja jedinice podataka od krivotvorenja.[7] Od ostalih temeljnih termina može se izdvojiti i protokol prema kojem se izdaju vremenski žigovi (engl. *Time-stamping Policy*), a što je zapravo sustav pravila kojima se opisuje uporaba tokena vremenskog žiga za određenu skupinu ili vrstu primjene zajedničkih sigurnosnih zahtjeva.[8]

S obzirom na to da digitalni zapisi u današnje vrijeme uvelike dominiraju u odnosu na one papirnate, rastuća je potreba za pronalaskom načina kojim bi se potvrdilo točno vrijeme kada je neki dokument nastao ili je promijenjen. U tu svrhu upotrebljavaju se vremenski žigovi, a kako bi ispunjavali svoju svrhu valjano, nužno je da vremenska varijabla bude vezana uz podatke na način koji se ne može krivotvoriti, a kako bi se mogao pružiti dokaz da je određeni podatak postojao prije određenog trenutka. Stoga se ovim međunarodnim standardom rješava taj problem tako da se vremenski žig veže na *hash* vrijednost podatka, čime se lakše upravlja

[4] ISO/IEC, 2008. ISO/IEC 18014-1: Information technology – security techniques – time-stamping services – part 1: Framework, str. 3
[5] ISO/IEC 18014-1, str. 3
[6] ISO/IEC 18014-1, str. 2
[7] ISO/IEC 18014-1, str. 2
[8] ISO/IEC 18014-1, str. 4

njihovim integritetom te sprječava njihovo otkrivanje. Ukratko, *hash* vrijednost podataka veže se uz parametar vremena koji pruži TSA, čime se garantira integritet i autentičnost vremenskog žiga.

Uz vremenske žigove vežu se dvije osnovne radnje: postupak izrade vremenskog žiga te postupak njegove verifikacije. Za izdavanje je odgovorno nadležno tijelo (TSA), dok žig može potvrditi i neko drugo tijelo od povjerenja. S obzirom na to da je postupak izdavanja žiga detaljno opisan u standardu RFC 3161, te objašnjen u prethodnom poglavlju, sada se neće ponovno ulaziti u te detalje.

Uporaba vremenskog žiga

Vremenski žig ne predstavlja točan trenutak kada je neki podatak nastao ili se mijenjao, pa čak ni kada je potpisan. Služba za izdavanje vremenskog žiga može vremenski označiti neki podatak, a da ga njegov vlasnik odluči tek naknadno upotpuniti elektroničkim potpisom. Jedina informacija koju vremenski žig daje jest da je određeni podatak postojao prije određenog trenutka. Ipak, s obzirom na to da se vremenski žigovi najčešće vežu s elektroničkim potpisima, standard opisuje tri moguća scenarija kada se uz podatke mogu vezati žig i potpis: vremenski žig može se izdati prije potpisivanja dokumenta, nakon potpisivanja dokumenta te i prije i poslije potpisivanja dokumenta. U tablici 1. prikazane su te mogućnosti.[9]

Tablica 1. Tri moguća redoslijeda vezanja vremenskog žiga i elektroničkog potpisa

1. slučaj	t_1	TSA stvara vremenski žig
	S	Izdavatelj zahtjeva elektronički potpisuje podatke označene žigom
2. slučaj	S	Izdavatelj zahtjeva potpisuje podatke
	t_2	TSA stvara vremenski žig za potpisane podatke
3. slučaj	t_1	TSA stvara vremenski žig
	S	Izdavatelj zahtjeva elektronički potpisuje podatke označene žigom
	t_2	TSA stvara vremenski žig za potpisane podatke

[9] ISO/IEC 18014-1, str. 6

Drugim riječima, u prvom slučaju ne zna se kada je točno dokument potpisan, samo da se to dogodilo nakon određenog trenutka (onog označenog vremenskim žigom); u drugom slučaju zna se da je dokument potpisan prije određenog trenutka (onog označenog vremenskim žigom); a u trećem slučaju zna se točno u kojem je razdoblju dokument potpisan (nakon i prije kojeg trenutka).

Osim postupka izdavanja i verificiranja vremenskog žiga, postoji i postupak njegovog obnavljanja, odnosno produživanja. To može biti potrebno zbog različitih stvari, primjerice ako je mehanizam koji veže vremenski žig i podatke na svom isteku; ako je kriptografska funkcija koja veže žig s podacima i dalje povjerljiva, ali postoje snažne indicije da će u bliskoj budućnosti biti u opasnosti; ili ako TSA koji je izdao vremenski žig prestaje vršiti tu uslugu. Postupak obnavljanja vremenskog žiga vrlo je sličan postupku njegovog izdavanja – razlika je u tome što prethodni žig i podaci uz koje je vezan postaju eksplicitno iskazani atributi na koje se veže novi vremenski žig s novim parametrom vremena. Na temelju pretpostavke da su zadovoljeni svi sigurnosni preduvjeti, vezanjem novog vremenskog žiga na stariji produžuje se valjanost podataka i oni ostaju valjani tijekom razdoblja trajanja novog vremenskog žiga.[10] Uzmimo da je podatak P dobio vremenski žig VŽ u vrijeme T_0:

VŽ (P (ostale informacije), T_0)

Dodavanjem vremenskog žiga u vrijeme T_1 produžuje se valjanost podatka P, odnosno potvrđuje se da je taj podatak bio valjan u vrijeme T_0, pod uvjetom da je prvi vremenski žig vrijedio u vrijeme dodavanja drugog vremenskog žiga:

VŽ (P(P (ostale informacije), T_0), ostale informacije), T_1)

Naravno, vremenski se žig mora produžiti prije no što se ostvari ijedna od opisanih situacija te prije no što prvi vremenski žig prestane vrijediti. Također, ovom se metodom vremenski žigovi mogu nizati jedan na drugi te se tako valjanost označenog podatka može

[10] ISO/IEC 18014-1, str. 7

dugotrajno očuvati. U tom slučaju govorimo o arhivskom vremenskom žigu, ali o tom će se pojmu više govoriti u sljedećem poglavlju.

Kao što je već spomenuto, ovaj ISO standard detaljno opisuje komunikaciju između strane koja traži izdavanje ili verifikaciju vremenskog žiga te TSA-a ili nekog drugog tijela od povjerenja, baš poput već obrađenog standarda RFC 3161.

Ukratko, u slučaju zahtjeva za izdavanjem vremenskog žiga, tražitelj mora prvo generirati *hash* vrijednost podataka koje želi označiti, a potom TSA-u šalje poruku koja sadrži tu *hash* vrijednost, upotrijebljeni *hash* algoritam, te *nonce* vrijednost (opcionalno). Po primitku zahtjeva, TSA provjerava jesu li dane sve nužne informacije. Ako jesu, generira se vremenski žig, koji je zapravo podatkovna struktura u kojoj su sadržani vremenski parametar iz pouzdanog izvora, podaci koje je dao tražitelj, te podaci koje je generirao TSA, a kojima se povezuju *hash* vrijednost, vremenski žig te *nonce* (ako je uključen). Potom se poruka s tim tokenom vremenskog žiga šalje tražitelju, koji može po primitku provjeriti je li primljeni token potpun i ispravan.

U slučaju zahtjeva za obnavljanjem vremenskog žiga, provjeravaju se informacije sadržane u izvornom (ili posljednje izrađenom) tokenu vremenskog žiga. Moguće je da će tijelo od povjerenja zaduženo za potvrđivanje trebati dodatne informacije, ovisno o mehanizmu provjere. Isto vrijedi i u slučaju verifikacije nizanih tokena vremenskih žigova. Više o ovoj temi govori se u drugom i trećem dijelu standarda ISO/IEC 18014. Također, u ovom se dijelu daje detaljan opis formata poruka koje razmjenjuju tražitelj izdavanja/obnavljanja vremenskog žiga i TSA. Međutim, i ovom će se prilikom preskočiti ulazak u takve tehničke detalje.

2.2.2. ISO 18014-2

Drugi dio standarda ISO/IEC 18014, naslovljen *Mechanisms producing independent tokens*, bavi se mehanizmima stvaranja neovisnih tokena vremenskih žigova, odnosno tokena vremenskih žigova za čiju verifikaciju nije potreban pristup ni jednom drugom vremenskom žigu, kao što je slučaj za nizane vremenske žigove, a o čemu će biti riječ u trećem dijelu ovog standarda.

Za potrebe ovog dijela standarda daje se niz definicija ključnih pojmova. Neki se ponavljaju iz prvog dijela standarda, ali ima i nekih novih. Tako integritet podataka (engl. *Data*

Integrity) znači da podaci nisu mijenjani ili uništeni bez autorizacije.[11] Nadalje, autentikacija (engl. *Authentication*) jest postupak potvrde identiteta nekog entiteta, a u tom kontekstu postoji i autentikacija podrijetla podataka (engl. *Data Origin Authentication*), odnosno postupak kojim se potvrđuje da je naveden izvor podataka točan.[12] Prvi se put spominje i termin jedinica vremenskog žiga (engl. *Time-stamping Unit*), koja je definirana kao set hardvera i softvera kojim se upravlja kao jednom cjelinom, a koja služi za generiranje vremenskih žigova.[13]

Kao što je već rečeno u prvom dijelu standarda, tijela koja pružaju usluge vezane uz vremenske žigove mogu izdavati, obnavljati i verificirati tokene vremenskih žigova. Također, sudionici tih postupaka su tražitelj izdavanja, obnavljanja ili verificiranja vremenskog žiga, tijelo koje izdaje i obnavlja vremenske žigove (TSU) te treća strana od povjerenja koja verificira vremenske žigove. Tijela koja pružaju navedene usluge mogu vršiti dva protokola: protokol za izdavanje/obnavljanje vremenskog žiga i protokol za njegovu verifikaciju. Temelj oba ta protokola jest token vremenskog žiga, koji se definira kao podatkovna struktura koja sadrži provjerljivu vezu između *hash* vrijednosti koja predstavlja podatak i parametra vremena. Svaki token vremenskog žiga sadrži jednu ili više *hash* vrijednosti podataka koje treba označiti vremenskim žigom, parametar vremena, te referencu na protokol u okviru kojeg je generiran token vremenskog žiga. Uz te nužne vrijednosti, token može identificirati pružatelja usluge izdavanja vremenskog žiga, sadržavati informaciju o maksimalnom prostoru za pogrešku u pogledu parametra vremena, naznaku poretka, identifikaciju verzije formata, serijski broj, te referencu na zahtjev korisnika (*nonce*).

Kada korisnik zatraži verifikaciju tokena vremenskog žiga, tijelo od povjerenja zaduženo za taj zadatak obavlja taj postupak u nekoliko koraka:[14]

- provjerom je li token vremenskog žiga sintaktički ispravan,
- provjerom je li vrijeme izdavanja tokena starije od vremena njegove verifikacije ($t<t_v$),
- provjerom odgovara li svaka komponenta tokena vremenskog žiga *hash* vrijednosti podataka u trenutku verifikacije,
- provjerom je li barem jedna od *hash* vrijednosti i dalje ispravna,

[11] ISO/IEC, 2009b. ISO/IEC 18014-2: Information technology – security techniques – time-stamping services – part 2: Mechanisms producing independent tokens., str. 2
[12] ISO/IEC 18014-2, str. 2
[13] ISO/IEC 18014-2, str. 4
[14] ISO/IEC 18014-2, str. 7

- provjerom je li zaštita tokena vremenskog žiga i dalje tehnički ispravna u trenutku verifikacije i
- provjerom je li protokol u okviru kojeg je token izdan prihvatljiv za potrebe verifikacije.

Ako sve te provjere daju pozitivne rezultate, token vremenskog žiga može se smatrati verificiranim. Također, tijelo koje provodi verifikaciju može zatražiti dodatne provjere, ali one nisu obuhvaćene ovim standardom.

Prilikom obnavljanja tokena vremenskog žiga, postupak je malo drugačiji. U teoriji, vremenski žig izdan u vremenu t_0 vrijedi zauvijek, ali u praksi je nužno postaviti vremensko ograničenje, zato što, primjerice, sigurnost izdanog tokena može biti u opasnosti zbog napretka kriptografskih napada, zato što ključ potpisa TSA-a uskoro istječe, zato što TSA prestaje nuditi usluge izdavanja vremenskih žigova i sl. U takvim je situacijama potrebno produljiti trajanje izvornog tokena vremenskog žiga dodavanjem novoga. Kako bi se to uspješno ostvarilo, novi vremenski žig mora se izdati dok prethodni još uvijek vrijedi, taj novi token vremenskog žiga mora sadržavati izvorni token kao jedan od zaštićenih atributa, u zahtjevu za izdavanjem vremenskog žiga mora se eksplicitno navesti prethodni token kako bi bio uključen u odgovor, a verifikacija se mora provesti provjerom cijelog niza vremenskih žigova. Točnije, postupak verifikacije obuhvaća provjeru svakog tokena vremenskog žiga i to obrnutim redoslijedom od redoslijeda njihovog izdavanja. Kada se ustvrdi da je svaki novi token vremenskog žiga izdan dok je prethodni još uvijek vrijedio, može se verificirati ispravnost vezanih podataka.

Mehanizmi zaštite

Token vremenskog žiga može se zaštititi raznim mehanizmima, bilo po izboru zahtjevatelja, bilo po naredbi tijela za izdavanje vremenskih žigova. Sve službe za izdavanje vremenskih žigova koje se pridržavaju ovog dijela standarda ISO/IEC 18014 dužne su zaštiti izdane tokene vremenskog žiga jednom od sljedeće tri metode:

1. Pružatelj usluge izdavanja tokena vremenskog žiga mora elektronički potpisati izdani token, kako bi taj potpis služio kao dokaz.
2. Drugi mehanizam podrazumijeva uporabu MAC verifikacije (engl. *Message Authentication Code*) za zaštitu tokena. Za generiranje i verifikaciju MAC-a potreban

je tajni ključ, a njega čuva TSA. Drugim riječima, TSA je nezaobilazan u postupku verifikacije tokena.

3. Treći mehanizam zahtijeva da TSA arhivira token, a objavi samo referencu na taj arhiv. Dakle, TSA je potreban i za arhiviranje i za verifikaciju.

U nastavku drugog dijela standarda ulazi se u tehničke detalje raznih sigurnosnih mjera za zaštitu tokena vremenskih žigova. Ta tema nije relevantna za ovaj diplomski rad jer je suviše tehničkog karaktera, pa stoga nema pretjerane važnosti u kontekstu pitanja dugoročnog očuvanja vremenskih žigova u arhivima.

2.2.3. ISO 18014-3

Treći dio međunarodnog standarda ISO/IEC 18014 naslovljen je *Mechanism producing linked tokens*, a bavi se načinom i postupcima stvaranja vezanih tokena vremenskog žiga, odnosno tokena koji su međusobno srodni, te svim elementima vezanima uz njih. Za početak, vezani tokeni (engl. *Linked Tokens*) nisu definirani kao termin, ali daje se definicija veze (engl. *Link*) kao podatka koji svjedoči o postojanju barem dva druga podatka putem *hash* vrijednosti otporne na koliziju.[15] Drugim riječima, te veze pridonose boljoj zaštićenosti integriteta tokena vremenskih žigova jer se sam integritet repozitorija veza TSA-a te metoda njihovog stvaranja mogu provjeriti kriptografski, te ne ovise o pouzdanosti infrastrukture javnih ključeva (engl. *Public Key Infrastructure,* PKI), odnosno sigurnosti javnih i privatnih ključeva.

Općenito gledano, TSA koji stvara vezane tokene upotrebljava kriptografske karakteristike *hash* vrijednosti kako bi se novi token vremenskog žiga povezao s onim koji je TSA prethodno stvorio. To se postiže tako da se podatkovni prikaz stvaranja ranijih tokena pridoda novoj *hash* vrijednosti koja se dodaje sljedećem tokenu. Tako se stvara logičan niz među stvorenim tokenima, a *hash* vrijednosti otporne na koliziju, čija se upotreba preporučuje, onemogućuju da se taj niz na bilo koji način komprimira ili promijeni.

Norma navodi tri metode izrade povezanih tokena vremenskih žigova, ali njihovo detaljnije objašnjenje odvelo bi ovaj rad u suviše tehničkome smjeru. Norma također predviđa mogućnost povezivanja čitave grupe tokena u jednu cjelinu kojoj se tada dodjeljuje jedna

[15] ISO/IEC, 2009a. ISO/IEC 18014-3: Information technology – security techniques – time-stamping services – Part 3: mechanisms producing linked tokens, str. 2

vremenska vrijednost, a zatim se takve grupe povezuju kao što bi se inače povezivali pojedinačni tokeni vremenskih žigova. Takav je pristup odličan ako se velik broj vremenskih žigova generira u isto vrijeme. U ovome slučaju primjenjuje se koncept tzv. ulančanih blokova (engl. *Blockchain*). Ipak, i ta je tema manje relevantna jer povezane tokene vremenskog žiga može stvarati samo jedan TSA, dok je tema ovog rada problematika kako razni nepovezani vremenski žigovi, odnosno njihovi tokeni, mogu funkcionirati u arhivima.

3. VREMENSKI ŽIGOVI U KONTEKSTU DUGOROČNOG OČUVANJA

U prethodnom poglavlju detaljno su objašnjeni elektronički vremenski žigovi, od njihove osnovne definicije, preko definicija pojmova vezanih uz same žigove, do opisa postupaka kojima se oni stvaraju, provjeravaju i potvrđuju, te obnavljanju. U ovom će se, pak, poglavlju elektronički vremenski žigovi promatrati u širem kontekstu dugoročnog očuvanja. Preciznije, promotrit će se njihova potencijalna uloga za dugoročno očuvanje elektroničkih dokumenata, kako u uredskom poslovanju, tako i u arhivima. Ta će se analiza ponovno temeljiti na postojećim europskim standardima, koji se već primjenjuju u okviru Uredbe eIDAS, te koji definiraju temeljne pojmove, ali i daju prijedloge za sustav dugoročnog očuvanja elektroničkih podataka u poslovnom okruženju, koji bi mogao poslužiti i kao model dugoročnog očuvanja takvih podataka u arhivima.

3.1. ETSI EN 319 102-1

ETSI standard 319 102-1, naziva *Procedures for Creation and Validation of AdES Digital Signatures (Part one: Creation and Validation)*, bavi se pitanjima stvaranja i validacije naprednih elektroničkih potpisa, i to u okviru Uredbe Europske unije br. 910/2014 (eIDAS).

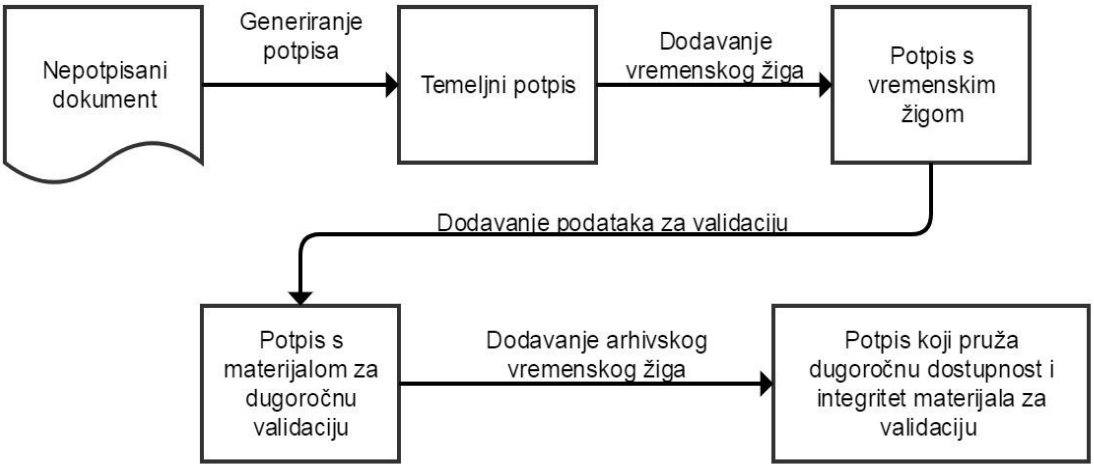
Za početak, elektronički potpis definira se kao podaci povezani s drugim podacima, odnosno kriptografska transformacija podataka kojom se omogućuje da primatelj tih podataka dokaže njihovo podrijetlo i integritet, i na taj se način zaštiti od krivotvorenja i zlouporabe.[16] Drugi važan termin jest augmentacija potpisa (engl. *Signature Augmentation*), odnosno postupak kojim se elektroničkom potpisu dodaju atributi radi dugoročnog očuvanja dostupnosti i integriteta materijala za validaciju.[17] Među njima je i (arhivski) vremenski žig, ali tome će se više riječi posvetiti u nastavku.

S obzirom na to da je ovaj standard posvećen elektroničkim potpisima, ulazi u detalje oko postupaka njihovog stvaranja, a kasnije i validacije. Ipak, za potrebe ovog diplomskog rada potrebno je samo izdvojiti one elemente koji se tiču vremenskih žigova te dugoročnog očuvanja elektroničkih potpisa. Drugim riječima, početni dio standarda posvećen općenitom postupku stvaranja elektroničkih potpisa može se zaobići, ali je zato odjeljak posvećen podjeli potpisa na

[16] ETSI, 2016b. ETSI EN 319 102-1 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf (10.9.2018.), str. 9

[17] ETS 319 102-1, str. 10

razrede vrlo važan te će se detaljnije obraditi. Naime, poglavlje 4.3., naslovljeno *Signature Classes and Creation Processes*, bavi se životnim ciklusom elektroničkog potpisa, od kojih se svaki korak definira kao jedna razina pa se tako mogu razlikovati četiri razine potpisa.



Slika 1. Životni ciklus elektroničkog potpisa

Izvor: ETSI EN 319 102-1 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Na prvoj je razini temeljni potpis (engl. *Basic Signature*; B-B razina), čija se valjanost može provjeriti samo dok odgovarajući certifikat nije povučen ili nije istekao.[18]

Temeljni potpis upotrebljava se kako bi se spriječila jednostavna zamjena valjanog potpisa krivotvorenim te kako bi se naveli certifikati na temelju kojih se valjanost potpisa može provjeriti. Dodatni atributi nisu nužni, ali može ih se dodati koliko god je potrebno u danoj situaciji.

Na drugoj je razini potpis s vremenskim žigom (engl. *Signature with Time*, B-T razina), koji sadrži dokaz da je potpis nastao prije određenog trenutka.[19]

Ova razina potpisa ima najosnovniju referencu na vrijeme – vremenski žig. On dokazuje da je potpis postojao u točno određenom trenutku. Kao što je objašnjeno u standardu RFC 3161,

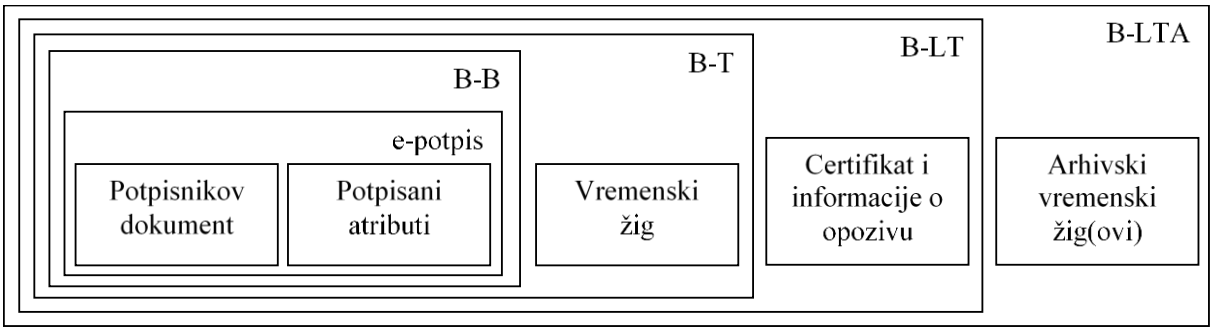
[18] ETS 319 102-1, str. 19
[19] ETS 319 102-1, str. 19

vremenski žig može se dodati nakon stvaranja elektroničkog potpisa, prije stvaranja elektroničkog potpisa ili i prije i nakon stvaranja elektroničkog potpisa. Idealno bi bilo da razdoblje između stvaranja jednog i drugog bude što kraće, ali konačnu odluku o tome donosi sam korisnik. U svakom slučaju, dodavanje vremenskog žiga prvi je korak u osiguravanju dugoročne validnosti elektroničkog potpisa.

Na trećoj je razini potpis s materijalom za dugoročnu validaciju (engl. *Signature with Long-Term Validation Material*, B-LT razina), kojemu se dodaju podaci za dugoročnu provjeru valjanosti u razdoblju kad je potpisni certifikat istekao na B-T razinu.[20]

U ovom slučaju, elektroničkom potpisu s vremenskim žigom dodaju se podaci nužni za verifikaciju potpisa i nakon što istekne valjanost njegovog certifikata. Preciznije, dodaju se certifikati te informacije o opozivu svih certifikata sadržanih u potpisu. Tako se dugoročna provjerljivost elektroničkog potpisa dodatno produžuje i osigurava.

Na kraju, dolazi se do potpisa koji pruža dugoročnu dostupnost i integritet materijala za validaciju (engl. *Signature Providing Long Term Availability and Integrity of Validation Material*, B-LTA razina), a kojim se omogućuju periodička dodavanja arhivskih vremenskih žigova (engl. *Archive Time-stamps*) na B-LT razinu.[21]



Slika 2. Uporaba arhivskog vremenskog žiga

Izvor: ETSI EN 319 102-1 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Ovom najvišom razinom elektroničkog potpisa osigurava se njegova dugoročna valjanost tako da se na prethodnu, B-LT razinu, pravovremeno doda tzv. arhivski vremenski žig. Pravovremeno znači prije no što kriptografski elementi potpisa, poput ključeva i

[20] ETS 319 102-1, str. 19
[21] ETS 319 102-1, str. 19

algoritama, postanu slabi ili podložni napadima, te prije no što certifikati prethodnih vremenskih žigova isteknu ili se opozovu. Arhivski žigovi nisu ništa drugo nego obični vremenski žigovi koji se dodaju elektroničkom potpisu i svim njegovim elementima kao nepotpisani atributi te jamče dugoročnu dostupnost i integritet materijala za validaciju. Drugim riječima, oni se ne razlikuju od standardnih vremenskih žigova po principu djelovanja, nego po svom obuhvatu. Prije no što posljednji dodani arhivski žig istekne, valja dodati novi koji će obuhvatiti sve prethodne te tako nastaviti garantirati dugoročnu valjanost elektroničkog potpisa, čak i kada svi vezani certifikati isteknu ili se opozovu. Upravo se zato ti žigovi nazivaju arhivskima. Nema ograničenja broja dodanih arhivskih vremenskih žigova, pa je njihova periodična obnova vjerojatno najjednostavnija metoda očuvanja električnog potpisa te garancije njegove valjanosti.

Prilikom izrade svake sljedeće razine potpisa, novi materijali dodaju se na prethodnu razinu potpisa, koja je obuhvaćena u cijelosti, kao što je prikazano na slici 2. Taj se postupak naziva augmentacija potpisa, a njegova je definicija dana u uvodnom dijelu ovog poglavlja.

U slučaju postupka validacije elektroničkog potpisa, uvijek se kreće od osnovne razine prema gore. Primjerice, u slučaju četvrte, B-LTA, razine potpisa, prvo se provjerava temeljni potpis, odnosno njegova valjanost. Ako se ona može ustvrditi, postupak validacije se završava; međutim, ako se ne može ustvrditi, prelazi se na provjeru valjanosti sljedeće razine. Postupak se nastavlja po tom principu, sve dok se ne ustvrdi valjanost jedne od razina, odnosno dok se ne obradi i posljednja razina, bez obzira na pozitivan ili negativan ishod.[22]

U ostatku dokumenta daje se pregledan i detaljan opis postupka validacije svake razine potpisa, s primjerima i objašnjenjima. Međutim, ulazak u takve detalje, osobito zato što su tehničke prirode, nije potreban.

3.2. ETSI SR 019 510

Europski standard ETSI SR 019 510, naslovljen *Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures*, zapravo se smješta u kategoriju posebnog izvještaja. Kao što se ističe u njegovom uvodu, elektronički potpisi i elektronički vremenski žigovi sve se češće upotrebljavaju u svakodnevnom životu, pa je nužno primjenjivati odgovarajuće mehanizme zaštite kako bi se

[22] ETSI EN 319 102-1, str. 27

oni mogli što dugotrajnije očuvati. Ta potreba za dugoročnim očuvanjem istaknuta je i u odredbi EU br. 910/2014, koja je stupila na snagu i u Hrvatskoj, u srpnju 2017. godine. Stoga je cilj ovog izvještaja dati pregled mehanizama očuvanja kojima se može zaštititi valjanost elektroničkih potpisa.

U dokumentu se obrađuju dva osnovna slučaja: zaštita validnosti elektroničkog potpisa i atributa vezanih uz njega, te zaštita integriteta bitova digitalnih objekata upotrebom tehnika elektroničkih potpisa.

Kada je cilj dugoročno očuvati neki digitalni zapis, to podrazumijeva različita rješenja, primjerice očuvanje integriteta i dokaza postojanja, ili pak i dostupnost samih podataka. U okviru ovog dokumenta, cilj je zadovoljiti minimalne sigurnosne preduvjete dugoročnim očuvanjem integriteta i dokaza postojanja samih podataka (dokaz postojanja upravo su vremenski žigovi – oni dokazuju da su podaci postojali u određenom trenutku). Što se tiče dostupnosti samih podataka, to se može riješiti tako da se digitalni podaci pohrane ili kod klijenta ili kod pružatelja usluga, a u tom slučaju razlikujemo uslugu očuvanja s pohranom (engl. *with storage*), odnosno bez pohrane (engl. *without storage*). Ako je cilj očuvanje valjanosti elektroničkog potpisa, nužno je sačuvati sve atribute koji svjedoče o tome, a koji vjerojatno neće biti dostupni u budućnosti (certifikate, informacije o opozivu i sl.). Također, dodatni cilj može biti očuvanje metode identifikacije tijela koje pruža uslugu očuvanja (engl. *Data Preservation Service Provider*, DPSP), što je korisno ako dođe do premještanja podataka ili ako treba jasno iskazati koja se praksa očuvanja upotrebljavala.

Svi ovi ciljevi mogu se realizirati putem nekoliko metoda. Ukratko, podatkovni objekt za očuvanje (engl. *Preservation Data Object*, PDO) naziv je podataka kojima upravlja pružatelj usluge očuvanja. Moguće je sačuvati više PDO-a unutar jednog spremnika (engl. *Preservation Object Container*, POC). Također, unutar jednog POC-a mogu se nalaziti i dodatni atributi, primjerice metapodaci koji objašnjavaju semantiku PDO-a. Uz to, PDO-i se mogu periodično dodavati istom POC-u. Uz ova dva termina, prepoznajemo i jedinicu podataka za očuvanje (engl. *Preservation Data Unit*, PDU), koja može obuhvaćati PDO u cjelini ili djelomično, a koja označava dio podataka za koje se primjenjuje jedan cilj očuvanja.

Kada vlasnik ili neka treća strana daju podatke na dugoročno očuvanje, a ta usluga uključuje i pohranu samih podataka, pružatelj usluge dat će davatelju podataka i jedinstveni identifikator POCID.

Također, uz svaki PDO veže se protokol očuvanja, odnosno sustav pravila kojim se određuju tehničke i proceduralne obveze u kontekstu očuvanja dotičnih podataka. Ta pravila nisu generička, nego se prilagođavaju potrebama pojedinih korisnika usluge očuvanja.

U slučaju očuvanja s pohranom (engl. *Preservation with Storage*), predviđeno je nekoliko mogućih postupaka.[23] Uobičajeni su predaja (engl. *Deposit*) i preuzimanje podataka za očuvanje (engl. *Retrieve*), gdje prvi postupak podrazumijeva predaju podataka za očuvanje nadležnoj usluzi, koja potom nad njima provodi odgovarajuće postupke radi očuvanja, a davatelju podataka vraća POCID, dok drugi postupak može inicirati izvorni davatelj podataka ili neko drugo autorizirano tijelo na temelju izdanog POCID-a. Također, postoje i drugi postupci: preuzimanje dokaza očuvanja (engl. *Retrieve proof*) ili opisa radnji provođenih na podacima (engl. *Retrieve trace of operations*), kojima autorizirano tijelo na temelju POCID-a traži izdavanje dokaza da su podaci za očuvanje uistinu očuvani, odnosno traži dokumentaciju o svim postupcima koji su se provodili nad podacima za očuvanje; ažuriranje postojećih elemenata (engl. *Update stored elements*); brisanje podataka (engl. *Delete*); nadzor podataka (engl. *Monitor*), što je interni postupak praćenja jesu li podaci za očuvanje u opasnosti od gubitka preduvjeta za buduću validaciju; te augmentacija (engl. *Augmentation*), odnosno proširenje temeljnih podataka dodavanjem atributa radi dugoročnog očuvanja. U slučaju očuvanja bez pohrane, predviđeni su samo postupci augmentacije i nadzora, odnosno klijent tada mora periodički slati POC pružatelju usluga očuvanja kako bi to tijelo produžilo validnost potpisa metodom augmentacije.

Prilikom očuvanja podataka, nužno je nadzirati sljedeće elemente:

- *Hash* funkcije, koje mogu biti dio postupka očuvanja, dio elektroničkog potpisa ili vremenskog žiga uključenog u dokument, ili dio elektroničkog potpisa ili vremenskog žiga povezanog s dokumentom. Ovisno o metodi očuvanja, važno je nadzirati različite *hash* vrijednosti. Primjerice, ako metoda očuvanja uključuje augmentaciju (dakle, dodavanje vremenskih žigova i/ili elektroničkog potpisa na izvorne dokumente), nužno

[23] ETSI, 2017. ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, https://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (10.9.2018.), str. 17

je nadzirati *hash* funkcije posljednjeg generiranog vremenskog žiga, odnosno elektroničkog potpisa.

- Status opoziva certifikata. Certifikati se mogu upotrebljavati za glavni elektronički potpis ili pak za elektronički potpis koji se naknadno dodaje radi potreba očuvanja podataka. Stoga je nužno da se sve informacije o opozivu svih upotrijebljenih certifikata prikupe na vrijeme, te očuvaju. To se može učiniti tako da ih se, primjerice, obuhvati vremenskim žigom. Iako to nije nužno, u slučaju opoziva certifikata bilo bi idealno kada bi se podacima dodao razlog za provođenje te odluke u obliku odgovarajućeg koda (razlozi uključuju podložnost kibernetičkim napadima, prestanak djelatnosti tijela za izdavanje certifikata i sl.).

Temeljne tehnike očuvanja

Temeljne tehnike očuvanja uključuju sljedeće opcije:

- Vremenske žigove. Njihova je prednost jednostavnost, ali nedostatak je što nema preduvjeta za dugoročno očuvanje jer se njima ne predviđa kako prikupljati informacije o certifikatima ili kako se nositi sa zaštitom *hash* vrijednosti.
- Napredne elektroničke potpise (B, B-T, B-LT, B-LTV). Prednost im je što je sve sadržano unutar njih, čime se osigurava temelj dugoročnog očuvanja, pogotovo u slučaju najviše razine potpisa. Međutim, nedostatak je što je za svaki potpis potreban jedan vremenski žig.
- ERS (engl. *Evidence Record Syntax*), kodiran u ASN.1 ili XML formatu, omogućuje očuvanje jednog ili više dokumenata, odnosno jedne ili više skupine dokumenata paralelno. Za te se potrebe oblikuje Merkleovo stablo, u kojem svaki list predstavlja *hash* vrijednost jedne grupe dokumenata. Zaštita dokumenata može se obnavljati ili obnovom vremenskog žiga ili obnovom *hash* stabla. Prednost ove opcije jest to što se jednim vremenskim žigom može obuhvatiti više potpisa.
- Ostalo. Postoje i druge metode, međutim nemoguće je sve ih uključiti u ovaj standard.

Svaki pružatelj usluge dugoročnog očuvanja podataka može podržavati jedan ili više protokola dugoročnog očuvanja (engl. *Long-term Preservation Policy,* LTPP). Cilj takvih protokola jest jasno objasniti koji je cilj očuvanja, koja se metoda očuvanja primjenjuje, koji se

protokol validacije primjenjuje i sl. Također je važno odrediti format u kojem se predočuju dokazi očuvanja kako bi se omogućila interoperabilnost te prenošenje očuvanih podataka iz jedne usluge u drugu. S obzirom na to da je cilj dugoročno očuvati podatke, nužno je i da sam protokol bude dugoročno dostupan i primjenjiv.

U nastavku ovog standarda daju se primjeri očuvanja s ili bez pohrane u različitim okolnostima, primjerice dugoročno očuvanje AdES elektroničkog potpisa uporabom postupka augmentacije bez pohrane. Ti primjeri dani su kako bi se ranije opisane teoretske smjernice objasnile u praksi. Također, autori ovog izvješća daju prijedloge daljnjih koraka koji bi se trebali poduzeti u pogledu standardizacije metode dugoročnog očuvanja digitalnih podataka, među kojima su definiranje uvjeta koje pružatelji usluga dugoročnog očuvanja moraju ispunjavati te sigurnosnih pravila kojih se moraju pridržavati, definiranje protokola koje moraju odraditi, s ciljem omogućavanja interoperabilnosti, te zaštita uređaja koji podržavaju postupke dugoročnog očuvanja. S obzirom na to da se još uvijek radi o prijedlozima, a ne o definiranim standardima, neće se dublje ulaziti u analizu ovog aspekta posebnog izvješća ETSI SR 019 510. Zanimljivija tema u kontekstu ovog diplomskog rada jest aneks izvješća, u kojem se analizira odnos usluga očuvanja kako ih zamišlja ETSI te OAIS referentnog modela.

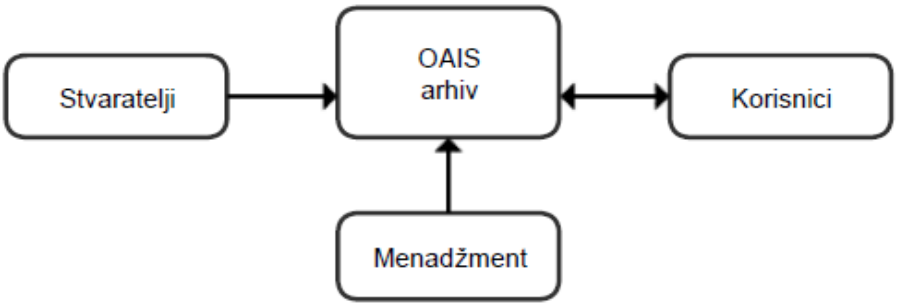
3.3. OAIS

Referentni model za otvoreni arhivski informacijski sustav (engl. *Open Archival Information System*, OAIS), razvilo je NASA-ino tijelo Consultative Committee for Space Data Systems 1999. godine, a taj je model postao i ISO standardom 2002. godine. Ukratko, radi se o konceptualnom okviru arhivskog sustava posvećenom dugoročnom očuvanju i osiguranju pristupa digitalnim informacijama.[24] Naime, dugoročno očuvanje digitalnih zapisa za sobom povlači niz problema koji se ne susreću kada se radi o očuvanju papirnatih zapisa. Za početak, dugoročno očuvanje podrazumijeva i dugoročan pristup čuvanim podacima, što otežava činjenica da se tehnologija razvija nevjerojatnom brzinom te da razni formati, operativni sustavi, programi i uređaji za pohranu lako postaju zastarjeli, pa podaci vezani uz njih postaju nečitljivi. Stoga postoji potreba za sustavom koji bi pomogao da se taj problem nadiđe, odnosno da se digitalni zapisi pohranjuju u obliku koji će što duže ostati strojno čitljiv, te da se tako omogući dugoročno očuvanje. Upravo je zato osmišljen OAIS sustav, i to kao referentni model,

[24] Lavoie, B. Meeting the challenges of digital preservation: The OAIS reference model, https://www.oclc.org/research/publications/library/2000/lavoie-oais.html (10.9.2018.)

što znači da se radi samo o osnovnoj, polazišnoj točki od koje institucije koje se bave dugoročnim očuvanjem digitalnih zapisa mogu krenuti razvijati vlastite sustave. Također, cilj ovog modela jest postaviti temeljne smjernice za dugoročno očuvanje podataka u što univerzalnijem obliku, tako da se postigne određena razina konsenzusa u pogledu procesa i elemenata ključnih za dugoročno očuvanje.

Za početak, OAIS nije izolirano tijelo, nego arhiv smješten u okolini na koju utječe, te koja utječe na njega. U modelu se ta okolina opisuje jednostavno, sastavljena od samo četiri elementa: OAIS arhiva, stvaratelja, korisnika i menadžmenta, kao što je prikazano na slici 3.



Slika 3. Okolina OAIS arhiva

Izvor: Consultative Committee for Space Data Systems (CCSDS), 2012. Reference model for an open archival information system

Ulogu stvaratelja čine klijenti koji predaju digitalne podatke za očuvanje. OAIS arhiv te podatke obrađuje kako bi mu mogli pristupiti korisnici, a uloga menadžmenta jest oblikovati politiku rada arhiva na višim razinama, što znači da nema utjecaj na svakodnevne aktivnosti unutar arhiva.[25]

OAIS model podijeljen je na tri osnovne razine: informacijski model, model transformacija informacijskih paketa te funkcionalni model, koji će se ukratko opisati u nastavku.

[25] Consultative Committee for Space Data Systems (CCSDS), 2012. Reference model for an open archival information system, https://public.ccsds.org/pubs/650x0m2.pdf (10.9.2018.), str. 2-2

Informacijski model

Informacijski model osnovni je model kojim se opisuju temeljna načela funkcioniranja OAIS arhiva, a sadrži logički model arhivskih informacija te logički model informacija.

Za početak, ključno je definirati termin „informacija“ jer je ona temelj čitavog modela, odnosno cilj samog arhiva jest očuvati informacije. Stoga se informacija definira kao bilo kakav oblik znanja koje se može razmijeniti, a pritom se uvijek iskazuje u nekakvom podatkovnom obliku.[26] Tu temeljnu informaciju, odnosno informacijski objekt (engl. *Information Object*), čine podatkovni objekt (engl. *Data Object*) i informacije za prikaz (engl. *Representation Information*), kao što je prikazano na slici 4.

Slika 4. Pretvaranje podataka u informacije

Izvor: Consultative Committee for Space Data Systems (CCSDS), 2012. Reference model for an open archival information system

Podatkovni objekt može biti u fizičkom ili digitalnom obliku; kada se govori o digitalnom obliku, govori se o sirovim elektroničkim podacima, odnosno nizovima bitova. Kako bi se takav podatkovni objekt mogao razumjeti, potrebno ga je prikazati u razumljivijem obliku, a to je uloga informacija za prikaz. Također, ispravno razumijevanje podataka podrazumijeva i postojanje temeljnog znanja koje dijele korisnici kojima su podaci namijenjeni (engl. *Knowledge Base*).

Dok se logičkim modelom arhivskih informacija opisuje struktura informacijskog objekta, logičkim modelom informacija definira se informacijski paket te se opisuju njegova struktura i vrste. Informacijski paket (engl. *Information Package*) (slika 5.) konceptualni je paket koji sadrži dvije vrste informacija – informacije o sadržaju (engl. *Content Information*)

[26] Reference model for an open archival information system, str. 2-3

te o opisu zaštite (engl. *Preservation Description Information*), objedinjene informacijama o pakiranju (engl. *Packaging Information*) te dodatno objašnjene opisnim informacijama (engl. *Descriptive Information*).[27]

Informacija o sadržaju osnovna je informacija koju valja očuvati, a čine ju podatkovni objekt i odgovarajuće informacije za prikaz potrebne kako bi korisnici kojima su informacije namijenjene mogli razumjeti očuvane informacije.

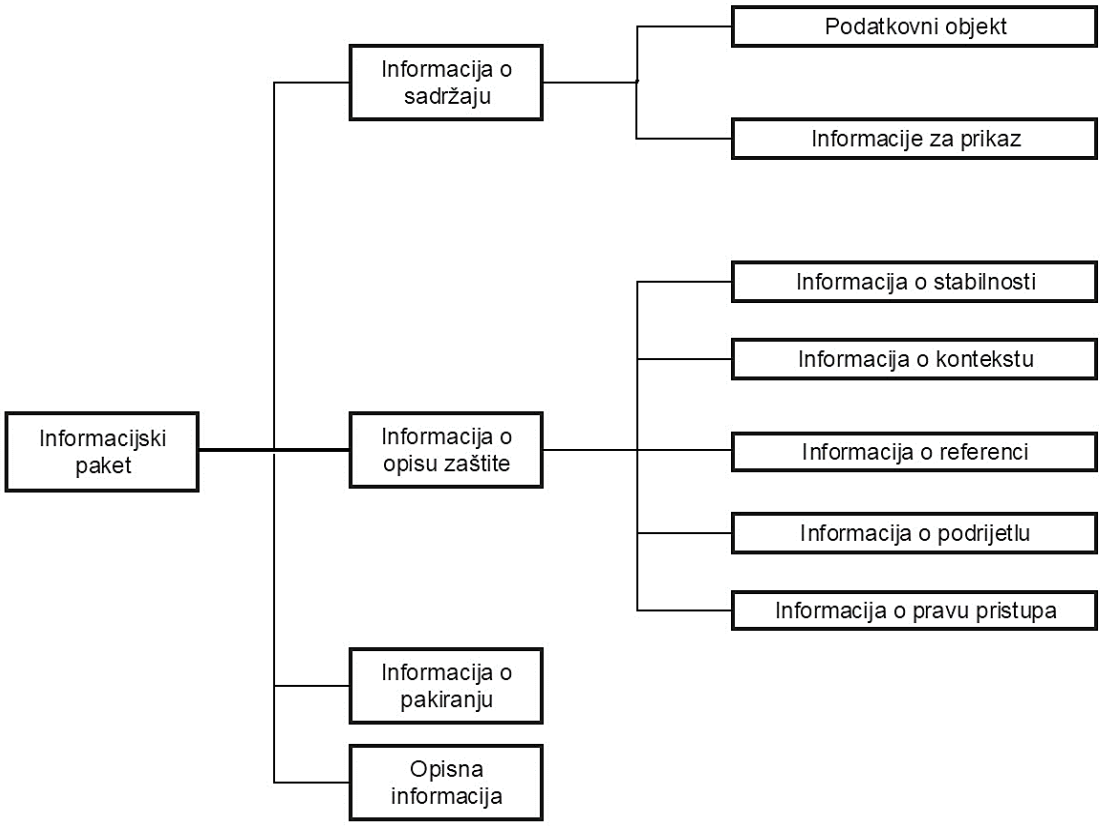
Podaci o opisu zaštite nužni su kako bi se informacija o sadržaju mogla očuvati, jasno identificirati te kako bi se razumjelo okruženje u kojem je nastala. Ta razina dalje se dijeli u pet podvrsta:[28]

- Informacija o podrijetlu (engl. *Provenance Information*), kojom se navodi izvor informacija o sadržaju te opisuje njegova povijest;
- Informacija o kontekstu (engl. *Context Information*), kojom se opisuje kako je informacija o sadržaju povezana s ostalim informacijama izvan ovog informacijskog paketa (zašto je informacija o sadržaju nastala, te kako se odnosi prema drugim informacijama o sadržaju);
- Informacija o referenci (engl. *Reference Information*), kojom se daje jedan ili više identifikatora pomoću kojih se informacija o sadržaju može jedinstveno identificirati;
- Informacija o stabilnosti (engl. *Fixity Information*), kojom se informacija o sadržaju štiti od nedokumentiranih izmjena, i
- Informacija o pravu pristupa (engl. *Access Rights Information*), kojom se opisuju uvjeti zaštite, distribucije i uporabe informacije o sadržaju (primjerice, izjava o davanju dopuštenja OAIS-u za aktivnosti očuvanja).

Informacijom o pakiranju svi se elementi informacijskog paketa fizički ili logički povezuju u cjelinu.

[27] Reference model for an open archival information system, str. 2-5
[28] Reference model for an open archival information system, str. 2-6

Opisna informacija upotrebljava se kako bi se pronašao informacijski paket koji sadrži traženu informaciju o sadržaju. To može biti običan opisni naslov ili pak cjelovit set atributa koje korisnici mogu pretraživati u katalogu.



Slika 5. Struktura informacijskog paketa

Izvor: Stančić, H. Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata: doktorska disertacija, Zagreb, 2005.

Vrste informacijskih paketa

Premda OAIS referentni model definira temeljnu strukturu informacijskih paketa, ona može varirati pod utjecajem okoline samog OAIS arhiva. Naime, informacijski paket koji klijent dostavlja arhivu može sadržavati nedovoljno informacija ili one mogu biti strukturirane na način koji ne zadovoljava pravila tog OAIS arhiva. S druge strane, informacijski paket koji OAIS arhiv dijeli daljnjim korisnicima ne mora nužno sadržavati sve informacije koje čine

cjelokupan paket (primjerice, zbog sigurnosnog ili nekog drugog razloga). Zato se razlikuju tri vrste informacijskih paketa:

- dostavljeni informacijski paket (engl. *Submission Information Package*, SIP),
- arhivski informacijski paket (engl. *Archival Information package*, AIP) i
- diseminacijski informacijski paket (engl. *Dissemination Archival Package*, DIP).

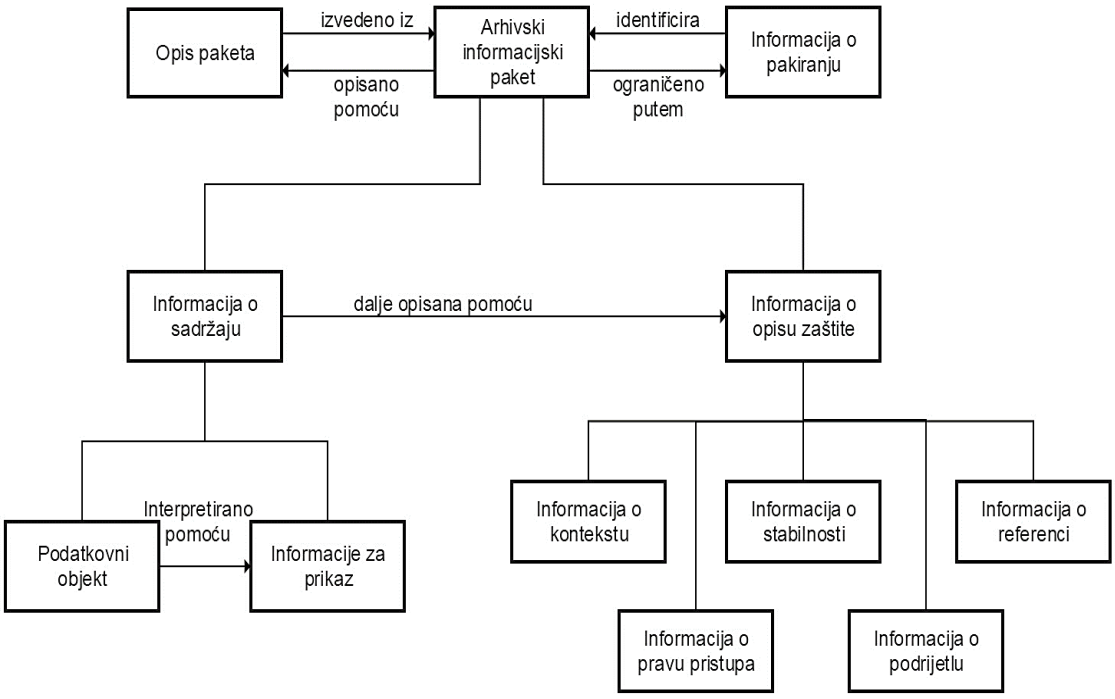
Slika 6. Pretvorba informacijskih paketa u OAIS arhivu

Izvor: Stančić, H. Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata: doktorska disertacija, Zagreb, 2005.

Kao što se vidi na slici 6, stvaratelji dostavljaju OAIS arhivu informacijski paket (SIP) s informacijama strukturiranima na prethodno dogovoren način, kako bi se olakšao unos podataka u sustav arhiva, te kako bi se dostavile sve nužne informacije. Naravno, nerealno je očekivati da će svaki dostavljeni informacijski paket u potpunosti zadovoljiti kriterije OAIS arhiva, što znači da će se SIP morati transformirati u jedan ili više arhivskih informacijskih paketa.

Arhivski informacijski paket (AIP) strukturiran je na prethodno opisan način, odnosno sadrži sve nužne informacije, čime se osigurava njegovo dugoročno očuvanje. Također, važno je istaknuti da izraz „sve nužne informacije“ podrazumijeva one informacije koje pojedini OAIS arhiv smatra nužnima, a što je istaknuto u samom pravilniku rada pojedine institucije. Nadalje, odnos SIP-a i AIP-a može biti jednostavan (za jedan SIP stvara se jedan AIP), ali i vrlo složen (od jednog SIP-a može se stvoriti više AIP-a ili se više SIP-ova može objediniti jednim AIP-om).

Na kraju, diseminacijski informacijski paket (DIP) onaj je paket informacija koji OAIS arhiv na zahtjev isporučuje krajnjim korisnicima. DIP može sadržavati više arhivskih informacijskih paketa, ili pak dio samo jednog AIP-a (npr., bez svih opisa o zaštiti).



Slika 7. OAIS informacijski model

Izvor: ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures

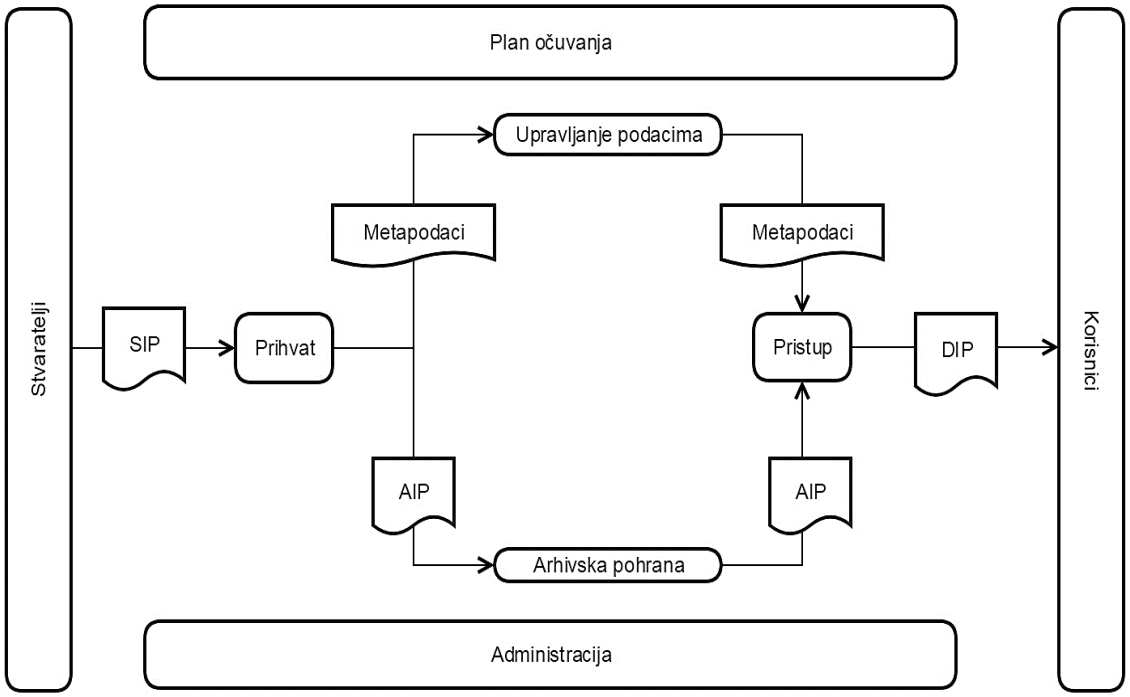
Funkcionalni model OAIS arhiva

Nakon opisa temeljnih pojmova i elemenata OAIS arhiva, mogu se opisati i funkcionalni entiteti OAIS arhiva, njihova uloga te njihova međusobna povezanost. Drugim riječima, radi se o šest osnovnih funkcija, kojima arhiv realizira dugoročno očuvanje podataka, te kojima se omogućuje pristup tip podacima. Radi se o sljedećih šest funkcionalnih entiteta:[29]

- prihvatu (engl. *Ingest*): „prihvat informacija koje predaje stvaratelj te njihova priprema za arhiviranje“;
- arhivskoj pohrani (engl. *Archival Storage*): „upravljanje dugoročnim prostorom za pohranu te njegovo održavanje“;

[29] ETSI SR 019 510, str. 31

- upravljanju podacima (engl. *Data Management*): „održavanje baze podataka s opisnim metapodacima kojima se identificiraju i opisuju informacije arhivirane u arhivskom prostoru za pohranu“;
- pristupu (engl. *Access*): „zahtjev za informacijama pohranjenima u arhivskom prostoru za pohranu, te njihovo dohvaćanje“;
- planiranju procesa očuvanja (engl. *Preservation Planning*): „nadzor promjena i rizika, primjerice, u kontekstu inovacija na području tehnologija pohrane, pristupa ili očuvanja“ i
- administraciji (engl. *Administration*): „briga o svakodnevnim zadacima unutar OAIS arhiva“.



Slika 8. Shematski prikaz OAIS sustava

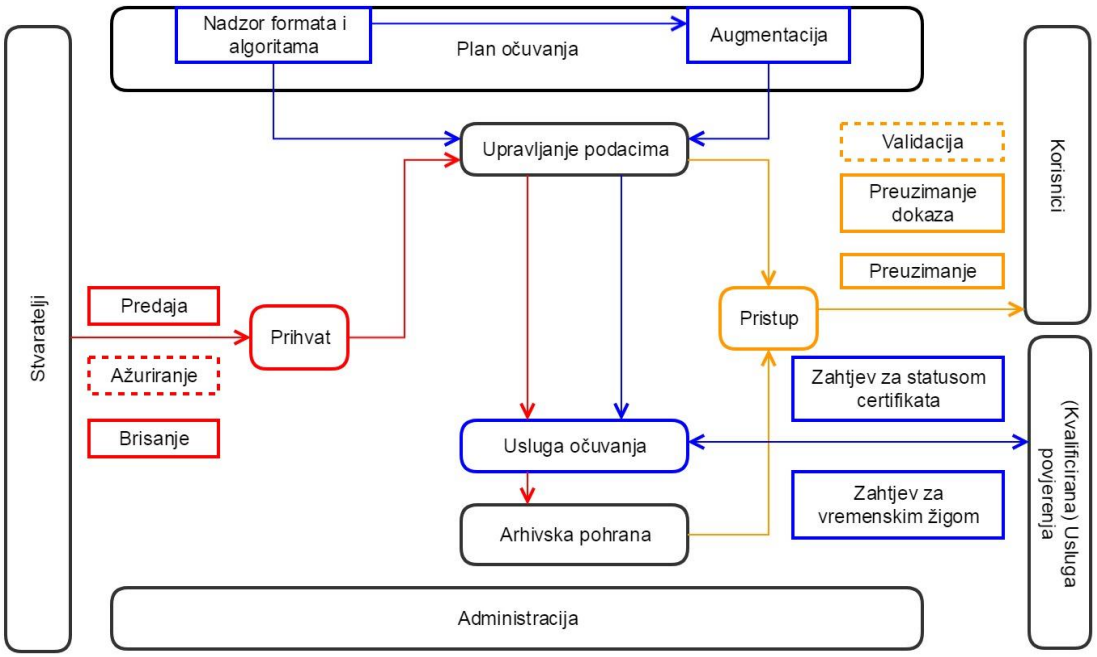
Izvor: ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures

Model transformacija informacijskih paketa

Kao što je već objašnjeno prilikom opisivanja različitih vrsta informacijskih paketa, OAIS arhiv prima dostavljeni informacijski paket, koji potom pretvara, odnosno transformira u arhivski informacijski paket. To znači da se informacijskom paketu koji stvaratelj predaje arhivu dodaju potrebne informacije radi njegovog očuvanja, kao što je prikazano na slici 6. Također, u kontekstu politike pojedine institucije, moguće je da se više AIP-a poveže u jednu cjelinu, odnosno arhivsku informacijsku zbirku, ali i da se jedan dostavljeni informacijski paket podijeli na više različitih arhivskih informacijskih paketa. Jednako tako, prilikom davanja diseminacijskog informacijskog paketa vanjskim korisnicima, moguće je da se radi o jednom cijelom AIP-u, dijelu jednog AIP-a, ili pak zbirci AIP-a. Svaki taj postupak preoblikovanja dobivenog SIP-a naziva se transformacijom informacijskog paketa.

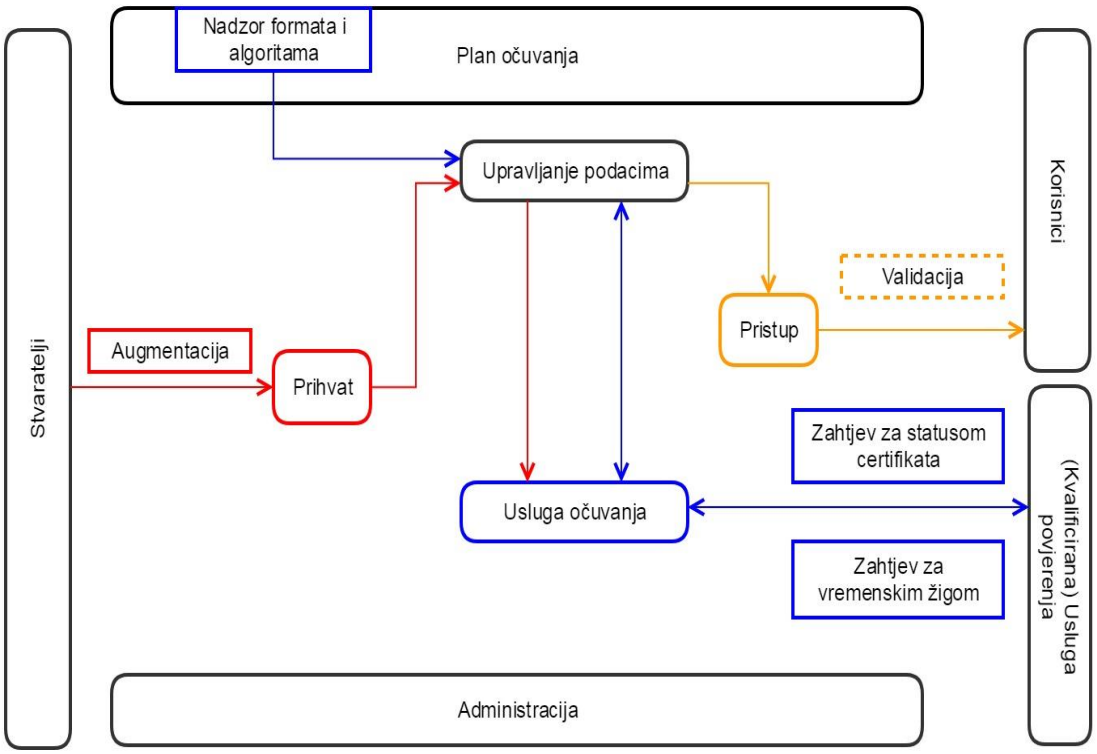
3.4. Odnos funkcija ETSI-jeve sheme za očuvanje i OAIS funkcionalnog modela

Na slikama 9 i 10 prikazan je odnos procesa dugoročnog očuvanja podataka kako je opisano ovim europskim standardnom, te funkcionalnog modela OAIS arhiva. Na tim su slikama u pravokutnim poljima prikazani procesi dugoročnog očuvanja kako ih predviđa ETSI, s time da je crvenom bojom označen postupak prihvata, plavom bojom postupak augmentacije, a narančastom postupak pristupa. Također, na slici 9 prikazan postupak dugoročnog očuvanja s pohranom, a na slici 10 bez pohrane.



Slika 9. Proces prihvata podataka (s pohranom)

Izvor: ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures



Slika 10. Proces prihvata podataka (bez pohrane)

Izvor: ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures

Ova dva shematska prikaza jasno pokazuju sličnosti između OAIS referentnog modela i ETSI-jevog prijedloga sustava za dugoročno očuvanje digitalnih podataka. Naime, funkcionalni entiteti koje predviđa OAIS model savršeno se uklapaju u shemu koja je zamišljena ETSI-jevim standardom, s time da je primjenjiva i za arhive i za uredsko poslovanje. Jedina je razlika što se podaci dostavljaju i korisnicima i trećim stranama od povjerenja, samo u različitim okolnostima.

Međutim, zanimljivi je odnos između OAIS-ovog informacijskog paketa i ETSI-jevog podatkovnog objekta za očuvanje. Naime, ako uzmemo arhivski informacijski paket kao najvažniji među informacijskim paketima OAIS referentnog modela (zato što je taj paket oblikovan kako bi se mogao dugoročno čuvati), te ga pokušamo prilagoditi zahtjevima ETSI-jevog modela dugoročnog očuvanja, vidimo da je to prilično lak zadatak. Arhivski informacijski paket sastoji se od informacije o sadržaju, informacije o opisu zaštite, informacije o pakiranju

i opisne informacije. Tablica 2 prikazuje kako bi izgledalo pridruživanje elemenata predstavljenih u ETSI-jevoj shemi elementima OAIS-a.

Tablica 2. Prihvat OAIS arhivskog informacijskog paketa u kombinaciji s elementima postupka prihvata prema ETSI SR 019 510

1.	Informacija o sadržaju	**a) Podatkovni objekt za očuvanje (PDO)**	
		b) Informacije za prikaz	
2.	Informacija o opisu zaštite	a) Informacija o referenci	
		b) Informacija o kontekstu	
		c) Informacija o podrijetlu	
		d) Informacija o pravu pristupa	
		e) Informacija o stabilnosti	**e.1) Elektronički potpis**
			e.2) Vremenski žig
			e.3) Dokazni zapis
			e.4) Podaci za verifikaciju
			e.5) Izvješće o verifikaciji
3.	Informacija o pakiranju	**a) Identifikator paketa (POCID)**	
		b) ASiC manifest	
4.	Opisna informacija		

Elementi otisnuti masnim slovima preuzeti su iz ETSI-jeve sheme očuvanja te dodani temeljnim elementima OAIS-ovog informacijskog paketa. S obzirom na to da se radi o sustavu dugoročnog očuvanja, informacijama o opisu zaštite dodani su elektronički potpis, vremenski

žig, elementi ERS sustava, te informacije potrebne za verifikaciju. Dakle, očigledno je da se sustav dugoročnog očuvanja kako ga zamišlja ETSI lako uklapa u međunarodno priznat referentni model OAIS arhiva. Štoviše, neke države, poput Njemačke i Italije, upotrebljavaju vlastita rješenja za dugoročno očuvanje, koja se temelje na OAIS modelu te imaju posebnu XML shemu arhivskog informacijskog paketa. Upravo je zato cilj ovog posebnog izvješća dati temeljne smjernice za ovaj postupak, kako bi se omogućila međunarodna interoperabilnost, ali bez davanja obavezne sheme koju moraju upotrebljavati sve zemlje članice EU-a.

Glavni prijedlog iznesen u aneksu ovog izvješća jest stvaranje AIP adaptera, kojim bi se različite sheme arhivskog informacijskog paketa transformirale u jednostavne ETSI-jeve podatkovne objekte za očuvanje, odnosno spremnike takvih objekata (POC-e). Taj adapter mogao bi biti dio aplikacije, primjerice sučelje usluge dugoročnog očuvanja, ili pak samostalna aplikacija kojom se različito strukturirani podaci transformiraju u standardizirane formate usluga za dugoročno očuvanje.[30]

Također, kako bi se usluge za očuvanje koje se temelje na OAIS referentnom modelu mogle nositi s podatkovnim objektima za očuvanje (PDO), trebaju poštivati sljedeća pravila:

- Pružatelj usluge očuvanja mora verificirati PDO-e, što znači da mora obraditi te podatkovne objekte u skladu s vlastitim pravilima očuvanja. To može uključivati provjeru validnosti postojećih elektroničkih potpisa, dodavanje kriptografske razine zaštite radi dugoročnog očuvanja autentičnosti podataka, obnavljanje podataka kojima se dokazuje da se podaci nisu mijenjali i sl.
- Svaki pohranjeni spremnik objekta za očuvanje (POC) mora imati vlastiti identifikator POCID, kojim se jednoznačno označava.
- Moguća je uporaba i dodatnih ulaznih elemenata. Ovim se standardom ne navode svi mogući takvi elementi, ali se preporučuje nacrt mogućih predložaka kojim bi se omogućila standardizacija takvih elemenata u skladu s temeljnim pravilima funkcioniranja usluga za dugoročno očuvanje.
- Svaki pružatelj usluge očuvanja odabire pravila očuvanja prema vlastitom nahođenju, a potom je dužan pridržavati ih se točno kako je propisano.

[30] ETSI 019 510, str. 35

Ukratko, vjerojatno je najjednostavnija metoda za dugoročno očuvanje elektroničkih zapisa pomoću elektroničkih potpisa i vremenskih žigova uporaba postojećeg OAIS referentnog modela kao temelja na koji će se nadograditi procesi očuvanja kako ih predviđa ETSI. S obzirom na to da je OAIS model međunarodno priznat te se upotrebljava već dulje vrijeme, izbjeglo bi se nepotrebno uvođenje novih modela, odnosno postojeći bi se sustavi mogli samo proširiti. To bi ujedno podrazumijevalo uštedu sredstava, vremena i obuke stručnjaka, a interoperabilnost na međunarodnoj razini bila bi gotovo zajamčena.

4. PRUŽATELJI USLUGE POVJERENJA

Elektronički vremenski žigovi, kao što je do sada ustvrđeno, imaju važnu ulogu u elektroničkom poslovanju jer funkcioniraju kao jedni od entiteta koji jamče valjanost elektroničkih zapisa i elektroničkih potpisa, te mogu pridonijeti potvrdi njihove autentičnosti i pouzdanosti. Naravno, kako bi mogli ispunjavati tu svoju ulogu, tijela koja ih izdaju moraju također biti pouzdana, pa ih se zato i naziva pružateljima usluge povjerenja (engl. *Trust Service Providers*, TSP). Ta tijela, njihova uloga i zadaće, standardizirani su europskim i međunarodnim normama, baš kao i vremenski žigovi. Time se jamči da se uistinu radi o službama kojima korisnici i institucije mogu vjerovati, što je ključno kako bi svi elektronički oblici poslovanja uistinu bili pouzdani.

Tako se europski standard ETSI EN 319 421, naslovljen *Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*, bavi proceduralnim i sigurnosnim zahtjevima koje trebaju ispuniti pružatelji usluga koji izdaju elektroničke vremenske žigove (engl. *Time-Stamping Authority*, TSA). Također, cilj je ovog standarda dati smjernice tijelima koje izdaju vremenske žigove i kvalificirane vremenske žigove kako bi svi postupci bili u skladu s Uredbom EU br. 910/2014 (eIDAS).

Za početak, ovim se standardom propisuje organizacijska struktura pružatelja usluga izdavanja vremenskih žigova, odnosno ističe se da oni moraju biti utemeljeni prema zakonima države u kojoj se nalaze, a njihovi zaposlenici moraju biti kvalificirani za obavljanje poslova vezanih uz izdavanje vremenskih žigova. Također, definiraju se dvije osnovne zadaće takvih tijela: generiranje, odnosno izdavanje vremenskih žigova i upravljanje svim djelatnostima samog pružatelja usluga, u smislu da pružatelj usluga mora voditi brigu o tome provodi li se njegova politika kako je propisano, ispunjava li sve svoje obveze te je li sama usluga izdavanja vremenskih žigova potpuna.[31] Drugim riječima, svaka institucija koja je ujedno i pružatelj usluge izdavanja vremenskih žigova mora imati jasno definiran i javno dostupan program (odnosno svoju politiku) u kojoj se objašnjava kakve sve usluge pruža, kome su one namijenjene, koja su eventualna ograničenja, trebaju li korisnici tih usluga zadovoljavati ikakve uvjete, koji su postupci provjere vremenskih žigova, postoje li neka ograničenja njihove

[31] ETSI, 2016c. ETSI EN 319 421 (v1.1.1): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf (10.9.2018.), str. 10

valjanosti i sl. Ključno je da se u toj politici jasno navedu sve informacije vezane uz same vremenske žigove i načine njihovog izdavanja te da se informacije o toj politici uvijek pridodaju tokenu vremenskoga žiga u obliku atributa.

Standardom se propisuju i sve potrebne razine zaštite, od zaštite fizičkog vlasništva do zaštite svih elektroničkih podataka koji su dani na povjerenje instituciji. Detaljno se propisuje i način generiranja tajnih ključeva kojima tijelo za izdavanje vremenskih žigova potpisuje izdane žigove. Sam postupak izdavanja mora se odvijati u fizički sigurnom okruženju, moraju ga izvoditi zaposlenici koji su kvalificirani za provođenja tog posla, a sam tajni ključ mora biti kriptografski snažno zaštićen kako bi odolio napadima što je dulje moguće. Kada se takav privatni ključ generira, on mora ostati tajan te biti zaštićen po najvišim sigurnosnim standardima kako njegov integritet ne bi bio narušen. Što se pak javnoga ključa tiče, njegov certifikat mora biti javno dostupan, a njegov status uvijek ažuran. Svi ti ključevi moraju imati definirani životni vijek te postupke koji se poduzimaju po isteku tog razdoblja. Također, nužno je napraviti sve moguće korake kako bi se osiguralo da se istek valjanosti ključeva odmah detektira te kako se takvi ključevi ne bi upotrebljavali za izdavanje novih vremenskih žigova.

Što se samog postupka izdavanja vremenskih žigova tiče, ključno je upravo vrijeme. Već se u politici institucije mora navesti s kojim je međunarodno priznatim i koordiniranim satom (engl. *Coordinated Universal Time*) usklađeno mjerenje vremena. Kako bi se osigurala stalna preciznost vremena, potrebno je često kalibrirati sat, a ako se primijeti da pružatelj usluge mjeri vrijeme prema satu koji je neprecizan ili čija mjera odstupanja nije u skladu s onom propisanom u samoj politici institucije, tada će se izdani vremenski žigovi smatrati nevažećima.[32]

Pružatelj usluge izdavanja vremenskih žigova mora propisati i sve postupke koji će se poduzeti nakon što prestane s djelovanjem. Nužno je da se svi korisnici te usluge povjerenja pravovremeno o tome obavijeste kako bi imali vremena obaviti potrebne radnje prije no što davatelj usluga opozove sve certifikate, što je dužan učiniti.

Standard sadrži i dodatak koji se tiče dugoročne provjere vremenskih žigova. Naime, po isteku certifikata, vremenski je žig nemoguće provjeriti kako bi se potvrdio njegov status. Međutim, ako u trenutku postupka provjere vremenskoga žiga korišteni privatni ključ nije kompromitiran, ako je korištena *hash* vrijednost i dalje jedinstvena te ako su algoritmi na

[32] ETSI EN 319 421, str. 17

kojima se temelje potpis i ključ i dalje otporni na napade, moguće je provesti postupak provjere bez obzira na istek certifikata. Ipak, savjetuje se da se postojeći vremenski žig te podaci na koje je vezan sačuvaju generiranjem novog vremenskog žiga.

Premda je ovim standardom jasno preciziran svaki aspekt djelovanja institucije koja se bavi izdavanjem elektroničkih vremenskih žigova, postoje kako državna tako i međunarodna tijela koja se bave provjerom rada takvih institucija te odlučuju o tome zaslužuju li se one smatrati pružateljem usluge povjerenja. Provjere koje ta tijela provode iznimno su detaljne, a svaka uočena pogreška može rezultirati negativnom ocjenom te sprječavanjem daljnjega rada institucije. Logično je da takva tijela postoje te da su njihove provjere rigorozne jer pružatelji usluge povjerenja zaista moraju opravdati svoju titulu. Naglasak je upravo na riječi „povjerenje“ te na činjenici da postaje sve teže dokazati vjerodostojnost podataka u elektroničkom okruženju. Zato vremenski žigovi i jesu važni – oni dokazuju da je neki podatak postojao u točno određeno vrijeme i u točno određenom obliku. Kako bi oni i nastavili biti uvjerljiv i prihvatljiv dokaz, institucije koje ih izdaju moraju proći svaku, pa i najdetaljniju analizu. Upravo zahvaljujući detaljnim propisima te tijelima koja nadgledaju njihovo provođenje, nema mnogo pružatelja usluga povjerenja, a one institucije koje su prošle provjeru nalaze se na javno dostupnom popisu kojim se dodatno jamči njihova sukladnost. Europski standard koji se bavi tijelima koja provode provjere te daju ocjene sukladnosti (njihovom organizacijom te načinom rada) jest ETSI EN 319 403, *Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers*, a gotovo se u potpunosti zasniva na međunarodnoj normi ISO/IEC 17065. Za potrebe ovog rada taj se standard neće detaljnije analizirati. Važno je samo istaknuti kako se i u Uredbi eIDAS ističe važnost uloge tijela za ocjenu sukladnosti jer ona jamči da pružatelji usluge povjerenja i usluge koje obavljaju jesu usklađeni s odredbama same Uredbe.[33] U Republici Hrvatskoj, prema Zakonu 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, „nadležno tijelo za provedbu Uredbe [eIDAS] u pogledu odredbi kojima se uređuju usluge povjerenja […] je središnje tijelo državne uprave nadležno za poslove gospodarstva“, a „tijelo

[33] The European Parliament and the Council of the European Union, 2014. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (10.9.2018.) eIDAS, uvodni st. 43.

nadležno za akreditaciju Tijela za ocjenjivanje sukladnosti kvalificiranih pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža […] je nacionalno akreditacijsko tijelo.“[34] Doduše, nije određeno o kojim se to tijelima konkretno radi, ali jasno je da ta tijela postoje, što znači da nema zakonskih i pravnih prepreka legitimnoj uporabi elektroničkih potpisa i elektroničkih vremenskih žigova u svakodnevnom poslovanju i za dugoročno očuvanje elektroničkih dokumenata. Štoviše, upravo će se u sljedećem poglavlju analizirati zakoni koji se odnose na elektroničke transakcije, odnosno na elektroničke potpise i njihovu uporabu, te na očuvanje elektroničkih podataka.

[34] 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 br. 62/17), https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-(EU)-br.-910/2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999/93/EZ (10.9.2018.), čl. 4., st. 1., i čl. 5.

5. ZAKONSKI OKVIR

U okviru hrvatskog zakonodavstva, vremenski se žigovi spominju u kontekstu elektroničkog poslovanja, odnosno u zakonima koji se dotiču elektroničkih potpisa. Konkretno, radi se o Zakonu o elektroničkom potpisu (NN 10/02, 80/08, 30/14), koji je prestao vrijediti 7. kolovoza 2017. godine, kada je na snagu stupio 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). U oba ta zakona daje se definicija vremenskog žiga i naprednog vremenskog žiga, s time da se definicija dana u Zakonu o elektroničkom potpisu može smatrati prvom definicijom tog pojma u hrvatskom zakonodavstvu: „Vremenski žig – je elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu, a napredan vremenski žig je elektronički potpisana potvrda ovjerovitelja koja ispunjava uvjete za napredan elektronički potpis.“[35] Ipak, s obzirom na to da se radi o zakonu koji se bavi elektroničkim potpisima, vremenskom je žigu posvećeno samo ovih par citiranih redaka. S druge strane, u Uredbi (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 (poznatijoj kao Uredba eIDAS), vremenskim je žigovima posvećeno malo više teksta. Za početak, u članku 1. jasno se ističe da se ovom Uredbom – između ostaloga – „uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.“[36] Dakle, vremenski žigovi spominju se u samom uvodu, čime se njihova važnost u kontekstu elektroničkog poslovanja, a posljedično i u kontekstu očuvanja elektroničkih dokumenata, dodatno naglašava. Prema ovoj Uredbi, 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“.[37] Ova definicija svojom je formulacijom bliskija definicijama citiranima iz normi u prethodnim poglavljima ovog rada (primjerice iz standarda RFC 3161 ili ISO/IEC 18014-1), nego definicija iz hrvatskog

---

[35] Zakon o elektroničkom potpisu, NN 10/02, 80/08, 30/14, http://www.digured.hr/cadial/searchdoc.php?action=search&lang=hr&query=Zakon+o+elektroni%C4%8Dkom+potpisu&searchText=on&searchTitle=on&resultdetails=basic&bid=WuKTobTXWydclF5QZSRzTQ%3d%3d&annotate=on (10.9.2018.), čl. 2

[36] Uredba eIDAS, čl. 1.

[37] Uredba eIDAS, čl. 3., st. 33.

zakona. Štoviše, u Uredbi eIDAS vremenskim žigovima posvećen je čitav članak 41., u kojem se navodi da se „elektroničkom vremenskom žigu 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“, te da se „kvalificirani elektronički vremenski žig izdan u jednoj državi članici priznaje […] kao kvalificirani elektronički vremenski žig u svim državama članicama.“[38] Ovaj drugi dio važan je jer potvrđuje aspiraciju EU-a da se temeljni pojmovi elektroničkog poslovanja unificiraju na razini čitave Unije te da se tako omogući interoperabilnost. To ne podrazumijeva samo interoperabilnost na razini aktivnog poslovanja, nego i na razini dugoročnog očuvanja (premda se to izrijekom ne spominje u samoj Uredbi). Zapravo, jedini put kada se u Uredbi spominje izraz „dugoročno očuvanje“ jest na samom početku, prije članka 1., kada se iznosi da bi se ovom „Uredbom trebalo osigurati dugoročno čuvanje informacija kako bi se osigurala pravna valjanost elektroničkih potpisa i elektroničkih pečata tijekom duljih razdoblja, čime bi se zajamčila mogućnost njihove validacije neovisno o budućim tehnološkim promjenama.“[39] Upravo se na tu točku referira standard ETSI SR 019 510, o kojem je bilo riječi ranije.

Na temelju citiranog, jasno je kako se o elektroničkim potpisima, elektroničkim pečatima, elektroničkim vremenskim žigovima i drugim srodnim pojmovima u hrvatskom zakonodavstvu govori samo u kontekstu aktivnog poslovanja. Drugim riječima, zakoni vezani uz arhive i pismohrane, odnosno uz postupke dugoročnog očuvanja ne dotiču se tih pojmova. Tako se u Uredbi o uredskom poslovanju (NN br. 7/09) elektronički potpis spominje samo jednom i to kada se navodi da se „pismena dostavljena u elektroničkom obliku s elektroničkim potpisom smatraju […] vlastoručno potpisanim sukladno posebnim propisima o elektroničkoj ispravi.“[40] Premda se jasno definira kako je uloga pismohrane između ostaloga i predati arhivirane dokumente nadležnom arhivu, ne spominje se, niti definira točan postupak kojim se to radi, a osobito ne kada je riječ o elektronički potpisanim dokumentima. Kao što je već raspravljeno u prethodnim poglavljima, očuvanje elektroničkih potpisa (bilo da se radi o kratkoročnom, a osobito dugoročnom očuvanju) podrazumijeva niz postupaka predostrožnosti, ali očigledno je da se o njima pretežito raspravlja u akademskim krugovima, te da je njihov put do ulaska u državno zakonodavstvo, pa tako i u zakonsku praksu, vrlo spor. Ipak, činjenica da

[38] Uredba eIDAS, čl. 41., st. 1., st. 3.
[39] Uredba eIDAS, uvodni st. 61.
[40] Uredba o uredskom poslovanju, NN 7/09, https://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html (10.9.2018.), čl. 13., st. 2.

je u kolovozu 2017. na snagu i u Hrvatskoj stupila Uredba eIDAS pozitivan je znak da hrvatsko zakonodavstvo usklađuje pravnu regulativu s onom na razini Europske unije.

Jednako tako, u srpnju 2018. godine izmijenjen je i Zakon o arhivskom gradivu i arhivima (NN br. 105/9., 64/00, 65/09, 125/11, 46/17, 61/18), pa je sada jedna od svrha ovog zakona i „osigurati stvaranje, čuvanje i pretvorbu dokumentarnog i arhivskoga gradiva u digitalni oblik.“[41] Naime, u prethodnoj verziji zakona nije se predviđala digitalizacija kao dio dugoročnog očuvanja gradiva, odnosno taj se postupak nije spominjao ni u jednom kontekstu. Međutim, napokon je prepoznato da je od donošenja ovog Zakona došlo do „osjetnih promjena u okruženju u kojem djeluju arhivi“, odnosno da su „stvaratelji dokumentarnog i arhivskog gradiva u znatnoj mjeri digitalizirali svoje poslovanje […] te stvaraju izvorno elektroničko gradivo u raznovrsnim informacijskim sustavima i oblicima.“[42] Stoga se novom verzijom zakona predviđa da arhivi zaprimaju gradivo i u elektroničkom obliku, odnosno da gradivo primljeno u analognom obliku digitaliziraju radi očuvanja prostora jer je jedan od problema što arhivi u Hrvatskoj nisu preuzeli prevelike količine gradiva kojima je rok za predaju u arhiv već istekao upravo zbog manjka prostora.[43] Zato se ovim Zakonom propisuje da je tijelo javne vlasti „dužno utvrditi pravila i postupke nastajanja izvornog javnog dokumentarnoga gradiva u digitalnom obliku“ te „osigurati pretvorbu arhivskoga gradiva koje je u fizičkom ili analognom obliku u digitalni oblik.“[44] Također, u članku 6., stavku 2. propisuje se da će se – između ostalog – načini i uvjeti pretvorbe gradiva u digitalni oblik utvrditi pravilnikom o upravljanju dokumentarnim gradivom izvan arhiva, a koji će donijeti nadležni ministar.[45] Drugim riječima, ovim se Zakonom ne utvrđuju postupci digitalizacije kako bi se ona ujednačila na državnoj razini, ali se predviđa donošenje odgovarajućeg pravilnika. Točnije, tim bi se pravilnikom trebao urediti „način pretvorbe gradiva u drugi oblik, karakteristike tehnologije i postupaka koji pružaju razumno jamstvo da nije bilo neovlaštenog i nedokumentiranoga dodavanja, mijenjanja ili uklanjanja svojstava gradiva odnosno pojedinih podataka i drugi zahtjevi za očuvanje uporabivosti dokumentarnoga gradiva“.[46] Na žalost, ne predviđa se kada bi se ovaj pravilnik mogao objaviti, ali se očekuje da bi to moglo biti unutar godine dana od donošenja Zakona.

---

[41] Zakon o arhivskom gradivu i arhivima, NN 105/97, 64/00, 65/09, 125/11, 46/17, 61/18, https://www.zakon.hr/z/373/Zakon-o-arhivskom-gradivu-i-arhivima (10.9.2018.), čl. 2.
[42] Vijesti o Zakonu o arhivskom gradivu i arhivima, Novosti u zakonu iz NN 61/18, 2018. https://www.zakon.hr/cms.htm?id=31075 (10.9.2018.)
[43] Ibid.
[44] Zakon o arhivskom gradivu i arhivima, čl. 6., st. 1.
[45] Zakon o arhivskom gradivu i arhivima, čl. 6., st. 2.
[46] Zakon o arhivskom gradivu i arhivima, čl. 8., st. 4.

Međutim, ni u novom Zakonu o arhivskom gradivu i arhivima ne spominje se izraz „dugoročno očuvanje“, ni u kontekstu analognih, ni u kontekstu digitalnih zapisa. Pretpostavka je da će se te stvari urediti u spomenutom pravilniku koji se tek mora sastaviti te stupiti na snagu. Doduše, Zakonom se utvrđuje da digitalno gradivo namijenjeno pohrani u arhivu mora biti cjelovito te da je i nakon pretvorbe očuvana njegova vjerodostojnost.[47] Također, stvaratelji su prije postupka pretvorbe dužni ishoditi potvrdu Hrvatskog državnog arhiva o sukladnosti pravila, tehnologije i postupaka pretvorbe (premda ona još nisu definirana).[48]

U principu, Zakon o arhivskom gradivu i arhivima sa svojim je izmjenama koje se tiču digitalizacije i podataka u elektroničkom obliku otvorio put prema modernizaciji sustava dugoročnog očuvanja elektroničkog gradiva u Republici Hrvatskoj, te odgovarajućoj brizi o elektroničkim dokumentima. Naravno, to je tek prvi korak, ali uzevši u obzir da je na snazi i Uredba eIDAS, moglo bi se zaključiti kako su temelji za spomenutu modernizaciju solidni. S druge strane, postoji mnoštvo problema koje tek treba riješiti, a njima je posvećeno sljedeće poglavlje.

[47] Zakon o arhivskom gradivu i arhivima, čl. 8., st. 2.
[48] Zakon o arhivskom gradivu i arhivima, čl. 9. st. 3.

6. DUGOROČNO OČUVANJE ELEKTRONIČKIH ZAPISA U ARHIVIMA

U dosadašnjoj analizi elektroničkih vremenskih žigova, elektroničkih potpisa te njihove uporabe u kontekstu dugoročnog očuvanja, citirani standardi mahom su se bavili tim temama u okviru uredskog poslovanja, odnosno dugoročnog upravljanja zapisima (engl. *long term records management*). Taj se termin uvelike razlikuje od dugoročnog arhiviranja (engl. *long term archiving*) u tome da se u prvom slučaju radi o arhivskim zapisima koji se koriste svakodnevno ili često kao temelj za poslovanje. To znači da se takvi elektronički potpisi i vremenski žigovi vezani uz te zapise moraju biti strojno provjerljivi, te moraju biti valjani. Dakle, svi atributi sadržani unutar takvog elektroničkog potpisa moraju biti ažurni i moraju vrijediti. S druge strane, kada je riječ o arhivskoj pohrani elektroničkih zapisa s elektroničkim potpisima i vremenskim žigovima, dovoljno je da u trenutku zaprimanja takvog zapisa u arhiv potpis, vremenski žig i drugi relevantni atributi vrijede te da se ta informacija zabilježi. Naime, za dugoročno arhiviranje dovoljan je dokaz da je elektronički potpis postojao u jednom trenutku i da je tada bio valjan, te nema potrebe da se taj potpis naknadno provjerava. Za takve je slučajeve potrebno jedino periodički obnavljati arhivski vremenski žig, kako je predviđeno standardom ETSI EN 319 102-1. Drugim riječima, dugoročno očuvanje u arhivima trebalo bi biti jednostavnije od dugoročnog upravljanja zapisima, barem u pogledu tehničke zahtjevnosti. Naravno, sve dok ne dođe trenutak u kojem će zbog zastarjelosti biti potrebno napraviti konverziju starog u novi format.

Ipak, to nipošto ne znači da u praksi sve teče bez problema. Kao što je naglašeno u prethodnom poglavlju, arhivi u Republici Hrvatskoj vrlo sporo ulaze u elektronički svijet. Ako je u zakon tek 2018. godine uveden pojam digitalizacije, jasno je da se do tada masovno baratalo isključivo papirnatim dokumentima. To znači da još uvijek nema adekvatnog sustava koji bi se nosio s elektroničkim zapisima, njihovom obradom, pohranom i diseminacijom, a jednako tako manjka i stručnog kadra u arhivima koji bi takve sustave implementirao, a potom i upotrebljavao. Možda je upravo problem implementiranja elektroničkog sustava najveći, ponajviše baš u arhivima. Uredsko poslovanje već je davno prošlo digitalnu transformaciju, pa bi u takvim uvjetima bilo jednostavnije implementirati sustav za prihvat, pohranu i diseminaciju elektroničkih podataka po uzoru na OAIS referentni model, kao što je opisan u ranijem poglavlju. Razlog je taj što tehnički preduvjeti već postoje, dakle računala, skeneri, serveri, sva oprema, ili barem većina. S druge strane, takvih uvjeta nema u postojećim arhivima. To znači

da je potrebno uložiti mnogo sredstava kako bi se arhivi adekvatno opremili, s time da za razliku od pismohrana, arhivi pohranjuju ogromne količine materijala – dakle, problem nedostatka fizičkog prostora zamjenjuje problem stvaranja adekvatno velikog digitalnog prostora za pohranu. To, dakako, za sobom povlači i druge početne poteškoće – zapošljavanje dodatnih zaposlenika koji će brinuti o toj opremi, ulaganje u adekvatan sustav zaštite na fizičkoj i digitalnoj razini, dodatno obrazovanje arhivista za skrb o elektroničkom gradivu i sl. Na žalost, najčešće je upravo nedostatak novčanih sredstava potrebnih za rješavanje svih ovih poteškoća glavni razlog zašto se sve odvija tako sporo.

Ipak, bez obzira na sve opisane probleme (kojih je vjerojatno i više, ali oni će se manifestirati tek kada se u prkasi doista krene provoditi digitalizacija arhiva), promjene su neminovne. Činjenica je da će se elektronički potpisi, elektronički pečati i elektronički vremenski žigovi sve češće koristiti u suvremenom poslovanju, a spisovoditelji i arhivisti morat će procjenjivati njihovu točnost, vjerodostojnost, autentičnost, cjelovitost i pouzdanost. Upravo je zato nužno dobro razumjeti iznesenu problematiku kako bi se mogle donositi pravovremene i ispravne odluke.

7. ZAKLJUČAK

Arhivska djelatnost ima tisućljetnu tradiciju, a kroz svoju bogatu povijest prošla je kroz mnogo promjena, držeći tako korak sa suvremenim tendencijama. Jedna takva promjena upravo traje – prelazak u digitalni svijet – pa je upravo pitanje dugoročnog očuvanja autentičnosti, pouzdanosti i cjelovitosti elektroničkoga gradiva najaktualnija problematika arhivske struke. Da bi se takvo gradivo dugoročno očuvalo, potrebno je prije svega brinuti o medijima na kojima je pohranjeno, jer tehnologija napreduje tolikom brzinom da tehnička oprema vrlo brzo zastarijeva. Ako, pak, takvo gradivo sadrži i elektronički potpisane dokumente, otvara se sasvim novi niz pravila kojih se valja pridržavati kako bi takvi dokumenti i za pedeset ili više godina sačuvali sve propisane karakteristike. Kako to postići? Jedna od mogućih metoda jest uporaba arhivskog vremenskog žiga, kojim bi se elektronički potpisani dokument označio po primitku u arhiv, te koji bi služio kao dokaz da je potpis u tom trenutku bio valjan. Potom bi bilo nužno samo periodički obnavljati samo taj arhivski vremenski žig. Implementacija te metode podrazumijevala bi učenje sasvim novih vještina te razvoj i uvođenje novih procesa u arhivima. Ne radi se o lakom pothvatu, ali postoji mnogo primjera dobre prakse iz pismohrana i arhiva diljem Europe i šire, a tu je i čitav niz normi i prijedloga za što jednostavnije dugoročno očuvanje elektroničkih podataka, od kojih je dobar dio analiziran u ovom radu. Postoje, dakle, svi preduvjeti za modernizaciju arhivskog sustava, pa tako i u Republici Hrvatskoj, gdje je i zakonska regulativa napokon usklađena s tom potrebom. U konačnici, pitanje dugoročnog očuvanja elektroničkih zapisa samo je još jedan u nizu izazova s kojim se arhivisti moraju suočiti, a jedini način da u tome uspiju jest da održavaju korak s promjenama i inovacijama u vlastitoj struci te u okolini koja na nju utječe, te da na njih odgovaraju pravovremeno i proaktivno.

8. LITERATURA

1. Adams, C., Cain, P., Pinkas, D., Zuccherato, R., Integris, 2001. RFC 3161: Internet x.509 Public key infrastructure time-stamp protocol, https://tools.ietf.org/pdf/rfc3161.pdf (10.9.2018.)
2. Consultative Committee for Space Data Systems (CCSDS), 2012. Reference model for an open archival information system, https://public.ccsds.org/pubs/650x0m2.pdf (10.9.2018.)
3. ETSI, 2015a. ETSI TR 119 000 (v1.1.1): Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview, http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.01.01_60/tr_119000v010101p.pdf (10.9.2018.)
4. ETSI, 2015b. ETSI EN 319 403 (v.2.2.2): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers, https://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_319403v020202p.pdf (10.9.2018.)
5. ETSI, 2016a. ETSI TR 119 100: Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation, http://www.etsi.org/deliver/etsi_tr/119100_119199/119100/01.01.01_60/tr_119100v010101p.pdf (10.9.2018.)
6. ETSI, 2016b. ETSI EN 319 102-1 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_319102011v010101p.pdf (10.9.2018.)
7. ETSI, 2016c. ETSI EN 319 421 (v1.1.1): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf (10.9.2018.)
8. ETSI, 2016d. ETSI EN 319 422 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf (10.9.2018.)

9. ETSI, 2017. ETSI SR 019 510 (v1.1.1): Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, https://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf (10.9.2018.)
10. ISO/IEC, 2008. ISO/IEC 18014-1: Information technology – security techniques – time-stamping services – part 1: Framework.
11. ISO/IEC, 2009b. ISO/IEC 18014-2: Information technology – security techniques – time-stamping services – part 2: Mechanisms producing independent tokens.
12. ISO/IEC, 2009a. ISO/IEC 18014-3: Information technology – security techniques – time-stamping services – Part 3: mechanisms producing linked tokens.
13. ISO/IEC, 2012. ISO/IEC 17065: Conformity assessment – Requirements for bodies certifying products, processes and services.
14. Lavoie, B. Meeting the challenges of digital preservation: The OAIS reference model, https://www.oclc.org/research/publications/library/2000/lavoie-oais.html (10.9.2018.)
15. Stančić, H. Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata: doktorska disertacija, Zagreb, 2005.
16. Uredba o uredskom poslovanju, NN 7/09, https://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html (10.9.2018.)
17. Vijesti o Zakonu o arhivskom gradivu i arhivima, Novosti u zakonu iz NN 61/18, 2018. https://www.zakon.hr/cms.htm?id=31075 (10.9.2018.)
18. The European Parliament and the Council of the European Union, 2014. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (10.9.2018.)
19. Zakon o arhivskom gradivu i arhivima, NN 105/97, 64/00, 65/09, 125/11, 46/17, 61/18, https://www.zakon.hr/z/373/Zakon-o-arhivskom-gradivu-i-arhivima (10.9.2018.)
20. Zakon o elektroničkom potpisu, NN 10/02, 80/08, 30/14, http://www.digured.hr/cadial/searchdoc.php?action=search&lang=hr&query=Zakon+o+elektroni%C4%8Dkom+potpisu&searchText=on&searchTitle=on&resultdetails=basic&bid=WuKTobTXWydclF5QZSRzTQ%3d%3d&annotate=on (10.9.2018.)
21. 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, https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-(EU)-br.-910/2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999/93/EZ (10.9.2018.)

POPIS SLIKA

POPIS TABLICA

SAŽETAK

Digitalne vremenske oznake i mogućnosti njihovoga korištenja u kontekstu dugotrajnog očuvanja digitalnih zapisa

U današnje digitalno doba javlja se sve veći broj dokumenata digitalnog porijekla koji su elektronički potpisani te pohranjeni u arhiv. I premda postoje brojne norme kojima se propisuje i standardizira uporaba elektroničkih potpisa, vremenskih oznaka, elektroničkih pečata i sličnih oznaka kojima se potvrđuje da je dokument autentičan, vjerodostojan, cjelovit i provjerljiv, u njima se ne propisuje kako se te oznake mogu učiniti dugoročno valjanima. U ovom se diplomskom radu opisuje osnovni model na kojem se temelje vremenske oznake, objašnjava proces stvaranja vremenskih oznaka i analiziraju postojeće norme. Potom se analiziraju modaliteti primjena pojašnjenih normi, identificiraju procesi u kojima se elektroničke vremenske oznake pojavljuju te raspravlja o njihovom značaju i ograničenjima u kontekstu dugotrajnog očuvanja elektroničkih zapisa.

Ključne riječi: elektronički vremenski žigovi, elektronički potpisi, dugoročno očuvanje, digitalni zapisi, arhiv

SUMMARY

Electronic time-stamps and the possibilities of their use in the context of long-term preservation of electronic records

In today's digital age there is a growing production of digital documents, which are digitally signed and archived. Although there are numerous standards regulating the use of electronic signatures, time-stamps, electronic seals and similar methods for confirming records' authenticity, trustworthiness, integrity and completeness, they do not regulate the long-term preservation of those entities. In this thesis, the basic model on which time-stamps are based is described, followed by explanation of the process of their creation and analysis of the existing standards. The modalities of implementing described standards are analysed, followed by the identification of the processes in which electronic time-stamps appear and discussion of their importance and limitations in the context of long-term preservation of digital records.

Key words: electronic time-stamps, digital signature, long-term preservation, digital records, archives