Arian Rajh
Agencija za lijekove i medicinske proizvode
Zagreb, Hrvatska
arian.rajh@halmed.hr

Bojan Romčević
Agencija za lijekove i medicinske proizvode
Zagreb, Hrvatska
bromcevic@halmed.hr

Hrvoje Stančić
Filozofski fakultet Sveučilišta u Zagrebu
Zagreb, Hrvatska
hstancic@ffzg.hr

Marin Vitaljić
Agencija za lijekove i medicinske proizvode
Zagreb, Hrvatska
mvitaljic@halmed.hr

KONCEPT RJEŠENJA ZA OSIGURANJE I OČUVANJE VJERODOSTOJNOSTI ZAPISA U UPRAVNIM ORGANIZACIJAMA PRILIKOM RAZVOJA DRŽAVNOG RAČUNALNOG OBLAKA I DRŽAVNOG DIGITALNOG ARHIVA

UDK 005.922.3:004.63]:3.07
Pregledni rad

Autori predlažu rješenje za pohranu tekućeg digitalnoga gradiva upravnih ustanova, uz osiguranje njegove autentičnosti, koje se temelji na komponenti državnog oblaka i komponenti ulančanih blokova (engl. blockchain). Takvo rješenje mogle bi koristiti upravne ustanove koje nemaju svoje sustave za upravljanje gradivom, a ono bi se moglo, na temelju dijeljenja iste platforme i funkcija, nadograditi državnim digitalnim arhivom, koji bi tada trebao imati funkciju očuvanja digitalnoga gradiva i njegove autentičnosti. Razvojem komponente ulančanih blokova koja je distribuirana na učesnike sustava (ustanove) i, konačno, razvojem predloženog sustava od povjerenja kao cjeline, ojačavaju se kapaciteti i vjerodostojnost svih upravnih ustanova koje koriste predloženi koncept sustava. Sustav se može nadograditi državnim digitalnim arhivom za arhivski dio digitalnoga gradiva upravnih (i drugih) ustanova.

Ključne riječi: *autentično gradivo; državni oblak; povjerenje javnosti; ulančani blokovi; vjerodostojne ustanove; nacionalni digitalni arhiv*

1. Povjerenje u ustanove i autentično gradivo

Vjerodostojne ustanove (lat. loca credibilia), odnosno konvencije povjerenja u ustanove nisu nove pojave, upravo suprotno. One se danas ne mogu temeljiti na »povjerenju javnosti u instituciju po sebi, zbog institucije same i zbog porijekla utemeljitelja te institucije«, nego na kvalitetnom funkcioniranju ustanove i njezina (digitalnog) arhiva[1] ili digitalnog arhiva koji ona koristi. Ni pouzdanost ustanove ni kvaliteta njezinih procesa nisu apsolutna svojstva. Treba imati na umu da je riječ o društvenim konvencijama koje se mogu u određenoj većoj ili manjoj mjeri odnositi na ustanove. Upravo zato je potrebno konstantno raditi na poboljšavanju procesa ustanova, struktura i sustava koje ih podupiru te proizvoda tih procesa. Kvalitetno dizajnirani procesi s gradivom i sustavi koji gradivom upravljaju i čuvaju ga u velikoj mjeri doprinose povećanju pouzdanosti ustanova-stvaratelja gradiva. Kad javnost ima visok stupanj povjerenja u ustanove, tada ona vjeruje da je funkcioniranje takvih pouzdanih ustanova kvalitetno (jednoobrazno, uhodano, s predvidljivim rezultatima), a neposredni rezultati njihova funkcioniranja i poslovanja svrsishodni i pouzdani (rješenja koja izlaze, službeni zapisi, njihovo gradivo). Tako se ostvaruje povjerenje u službeno gradivo koje u tim ustanovama nastaje.

Prema modelu iz projekta InterPARES 2, zapisi vrijedni povjerenja (engl. trustworthy) imaju visok stupanj pouzdanosti (engl. reliability), autentičnosti (engl. authenticity) i točnosti (engl. accuracy).[2] Stupanj pouzdanosti utvrđuje se prema cjelovitosti zapisa i pouzdanosti procesa kreiranja zapisa, što je svojstvo procesa ili sustava. Stupanj autentičnosti ovisi o mogućnostima identifikacije zapisa i provjere njegova integriteta. Stupanj točnosti ovisi o preciznosti sadržaja, ispravnosti zapisa, istinitosti zapisa i njegovoj primjerenosti. Neke sastavnice tog određenja nejasno su određene u arhivistici, posebice autentičnost, koja je tautološki određena u ISO 15489 normi: za autentičan zapis može se 1) dokazati da jest ono što tvrdi da jest, 2) da ga je stvorila ili poslala osoba za koju tvrdi da ga je stvorila ili poslala i 3) da je bio stvoren ili poslan kada tvrdi da jest.[3] Autentičnost u arhivistici nije određena bez pribjegavanja kružnim definicijama ili bez izvođenja iz drugih već konstruiranih pojmova. Vrijednost povjerenja (engl. trustworthiness), auten-

---

[1] Arian Rajh, "Teorijski model digitalnog arhivskog sustava," (doktorski rad, Sveučilište u Zagrebu, 2010).

[2] Joseph T. Tennis i Randy Preston, "Part Eight – Terminological Instruments: Terminology Cross-domain Task Force Report," u *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, ur. Luciana Duranti and Randy Preston (Padova: Associazione Nazionale Archivistica Italiana, 2008), str. 7, pristupljeno 5. travnja 2018., http://www.interpares.org/display_file.cfm?doc=ip2_book_part_8_terminology_task_force.pdf.

[3] International Organization for Standardization. *Information and documentation – Records management – Part 1: Concepts and principles*, ISO 15489-1:2016 (Geneva: International Organization for Standardization, 2016), dio 5.2.2.

tičnost i pouzdanost dakle pojmovi su koji se u literaturi objašnjavaju međusobno.[4] Svaki od njih funkcionira gotovo poput fraktala. Autentičnost je, tako, fluidno svojstvo koje se neprestano izvodi iz drugih svojstava (primjerice iz izvornosti ili pravosti, ne-lažnosti).[5] Ona je uz to i konstruirano svojstvo.[6] Sam pojam autentičnosti ima u povijesti višestruko značenje,[7] a on je višestruk po značenju i danas. Duranti autentičnost zapisa dijeli na povijesnu, pravnu i diplomatičku.[8] Povijesna autentičnost pruža dokaz minulih događaja, pravna pruža dopuštenost korištenja zapisa na sudovima i temelji se na autoritetu stvaratelja koji stoji iza gradiva, a diplomatička autentičnost ovisi o provenijenciji koja je vidljiva iz unutarnjih i vanjskih elemenata zapisa. Diplomatička i pravna autentičnost bile su podvrgnute kritici drugih autora uslijed propitivanja prikladnosti sudskih procesa za provjeravanje pouzdanosti zapisa i činjenice da mnogi zapisi iz istog vremena i iste provenijencije dijele veći broj sličnih obilježja.[9] Autentičnost je složeno i naslijeđeno svojstvo.[10] Ono se oblikovalo i kroz različite uporabe – sjevernoamerički, europski i kineski pogled na autentičnost nisu isti: prvi je vezuje, prije svega, uz integritet i identitet zapisa, drugi ponajviše uz provenijenciju, administrativne procese i oblik zapisa, a treći ju sagledava kroz kombinaciju pojmova autentičnosti i izvornosti (engl. originality), s naglaskom na cjelovitost.[11] Europljani su skloni elektronički potpis smatrati instrumentom osiguranja autentičnosti, što ne odgovara modelu autentičnosti koji je razvio projekt InterPARES ni poimanju autentičnosti u njegovim izvješćima.[12] Ipak, korištenjem koncepta ulančanih blokova (engl. blockchain) moguće je osigurati autentičnost digitalno potpisanih zapisa, unatoč činjenici da potpisni certifikati prestaju vrijediti već nakon 2-5 godina.[13]

---

[4] Corinne Rogers, "A literature review of authenticity of records in digital systems from 'machine-readable' to records in the cloud," *Acervo* 29, br. 2 (2016): str. 25-26.

[5] Richard Pearce-Moses, *A Glossary of Archival and Records Terminology* (Chicago: The Society of American Archivists, 2005), s. v. authenticity.

[6] Heather MacNeil, "Trusting records in a postmodern world," *Archivaria* br. 51 (2001): str. 40-41.

[7] Rogers, "A literature review of authenticity," str. 18.

[8] Luciana Duranti, "Diplomatics: New Uses for an Old Science," *Archivaria* br. 28 (1989): str. 17.

[9] Heather MacNeil i Bonnie Mak, "Constructions of Authenticity," *Library Trends* 56, br. 1 (2007): str. 26-52.

[10] Rajh, "Teorijski model digitalnog arhivskog sustava," str. 98.

[11] Luciana Duranti, "Policy Cross-domain: Authenticity and Authentication in the Law," u *International Research on Permanent Authentic Records in Electronic Systems: InterPARES 2 Project* (Associazione Nazionale Archivistica Italiana, 2005), pristupljeno 4. travnja 2018., http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf.

[12] Duranti, "Policy Cross-domain," str. 5.

[13] Vladimir Bralić, Magdalena Kuleš i Hrvoje Stančić, "A model for long-term preservation of digital signature validity: TrustChain," u *INFuture2017 Proceedings: The Future of Information Sciences*, ur. Ana Atanassova, Wajdi Zaghouani, Bruno Kragić, Kuldar Aas, Hrvoje Stančić i Sanja Seljan (Zagreb: University of Zagreb, 2017), str. 89-103.

Zbog svega nabrojanoga, autentičnost se operativno može shvatiti kao složeno svojstvo zapisa koje podupire i osigurava sustav od povjerenja u kojem se gradivo čuva, svojstvo koje obuhvaća kvalitetu sadržaja zapisa (njegovih podataka i metapodataka), konteksta i oblika gradiva, kao i svojstvo upravljivosti procesa koji gradivo oblikuju i čuvaju. Svrha osiguranja i dokazivanja autentičnosti ogleda se u osiguranju iskoristivosti zapisa i osiguranju povjerenja u arhive ustanova[14] ili arhive koje ustanove zajednički koriste. To složeno svojstvo podupiru identifikacijski metapodatci i metapodatci za dokazivanje integriteta, kontekstualni metapodatci i metapodatci za dokazivanje provenijencije,[15] poznat oblik i format gradiva te poznati procesi stvaranja, upravljanja i očuvanja gradiva. Stoga se vrijednost povjerenja može tumačiti kao svojstvo sustava, s povjerenjem u ustanovu kao logičkom posljedicom, a autentičnost kao svojstvo gradiva, s integritetom i identitetom gradiva kao dijelovima tog svojstva. Tek se na toj, najnižoj, razini barata pojmovima koji mogu biti precizno određeni – uvidom u evidenciju, provjerom metapodataka ili forenzičkim metodama. Zbog toga je važno posvetiti dovoljno pažnje toj najnižoj razini prilikom oblikovanja sustava. Autentični zapisi su, stoga, dio sustava od povjerenja, a sustav od povjerenja je rješenje u kojem se nalazi autentično gradivo. Upravo zbog toga što sustav podupire i osigurava autentičnost zapisa, i zbog toga što se s pohranjenoga gradiva povjerenje u autentičnost može prenijeti na arhiv ustanove (ili arhiv koji ustanova koristi) pa i na samu ustanovu,[16] smatramo da je od iznimne važnosti pomoći stvarateljima u oblikovanju sustava vrijednih povjerenja. Pouzdanost arhiva ustanove smatramo važnim uvjetom osiguranja autentičnosti gradiva, a povjerenje u ustanovu vidimo kao krajnji rezultat kvalitetno oblikovanih sustava i procesa s gradivom.

Drugi dio ovog članka bavi se arhivističkim konceptom pohrane i problemom vremenski ograničenih potpisnih certifikata. Treći dio obrađuje tehnologije koje su raspoložive i koje stvaratelji danas mogu koristiti. U četvrtom i petom dijelu iznesen je prijedlog sustava za upravljanje gradivom i arhivima te se raspravlja o svrsi takovog rješenja. U šestom se dijelu predlažu moguća daljnja istraživanja i daje zaključak obrađene teme.

---

[14] Arian Rajh, "The problem of maintaining and proving authenticity in the transition from Producer to Archive," predavanje s prezentacijom održano na Veleučilištu u Oslu i Akershusu, 24. listopada 2016., doi:10.13140/RG.2.2.29500.64640.

[15] Postoje mnoge podjele metapodataka. Tako primjerice Gartner dijeli metapodatke na tri osnovne vrste: opisne, administrativne i strukturne. Richard Gartner, *Metadata: Shaping Knowledge from Antiquity to the Semantic Web* (Cham: Springer, 2016). Ne ulazeći u tu temu, ovdje smo samo naveli vrste (odnosno upotrebe) metapodaka koje smatramo ključnim za pitanje autentičnosti.

[16] International Organization for Standardization, *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*, ISO 16363:2012 (Geneva: International Organization for Standardization, 2012); The Center for Research Libraries i Online Computer Library Center, *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (Chicago: The Center for Research Libraries, 2007).

2. Čuvanje autentičnoga gradiva koje nastaje u ustanovama

Arhivistički koncept očuvanja podrazumijeva usmjeravanje na očuvanje gradiva sa što manje dodatnih komplikacija u vezi s očuvanjem pomoćnih mehanizama koje je potrebno uspostaviti da bi to gradivo bilo dohvatljivo, interpretabilno i iskoristivo u najrazličitijim situacijama. Zbog toga je, primjerice, koncept potpisnih certifikata, koji se koriste u elektroničkim potpisima kao potvrda identiteta potpisnika i koji se najčešće izdaju na rok od dvije do pet godina, bez obzira na to što podupiru integritet zapisa, odnosno najmanjih jedinica gradiva ustanove, u očima arhivista unaprijed problematičan. Naime, posve je realno odmah se zapitati kako očuvati zapis, primjerice, na rok od 20 godina – kad se već nakon desetine tog razdoblja ne može, gledajući sam zapis, utvrditi je li on u potpunosti autentičan. To bi moglo postati ostvarivo tek ako sam sustav-arhiv preuzme ulogu jamca autentičnosti zapisa koji su sadržani u njemu. Dovoljno je to što se arhivisti moraju (pro)aktivno i intenzivno brinuti o medijima, formatima zapisa, fontovima, identifikatorima i drugim intrinzičnim i ekstrinzičnim elementima zapisa, pa pristup s potpisivanjem digitalnoga gradiva baš i nije naišao na plodno tlo u krugovima arhivista.[17] Aktivna uloga sustava-arhiva u očuvanju autentičnoga gradiva ujedno je i promišljanje koje se može iščitati iz raznih izvješća InterPARES projekata. Budući da je riječ o gradivu koje će djelomično postati arhivskim gradivom, smatramo da je potrebno planirati rješenje za digitalno (i potpisano i nepotpisano) gradivo koje će uzeti u obzir i arhivistički koncept očuvanja gradiva.

3. E-potpis, računalni oblak i ulančani blokovi

Elektroničkim potpisom (engl. *electronic/digital signature*) utvrđuje se autentičnost pojedinog zapisa. Zapis, elektronička pošta ili bilo koji drugi digitalni dokument ili transakcija mogu biti potpisani elektroničkim potpisom. Postoji više vrsta elektroničkih potpisa, kao što su to, primjerice, XMLDSig, XAdES, CAdES i PAdES.[18] Autentičnost je vjerodostojna dokle god je poznat i provjerljiv identitet potpisnika i dokle god se može dokazati da zapis nije promijenjen od trenutka potpisivanja. Vjerodostojnost se ostvaruje kodiranjem zapisa (potpisivanjem elektroničkim potpisom) prije slanja zapisa i njegovim dekodiranjem na strani primatelja (provjerom valjanosti elektroničkog potpisa). Time se osigurava ne samo autentičnost zapisa (informacija o identitetu potpisnika nalazi se u dijelu poruke, tj. u potpisnom certifikatu koji je ograničenog vremenskog trajanja), nego se osigurava i integritet zapisa (provjera je li došlo do neovlaštene ili neželjene promjene za-

---

[17] Hrvoje Stančić i Tomislav Ivanjko, "Povjerenje u arhivske e-zapise," *BugOnline*, 6. lipnja 2016., pristupljeno 5. travnja 2018., https://www.bug.hr/molex/elektronicki-potpisi-pecati-okviru-uredbe-eida/97352.aspx.

[18] Hrvoje Brzica, Boris Herceg i Hrvoje Stančić, "Long-term Preservation of Validity of Electronically Signed Records," u *The Future of Information Sciences: INFuture2013: Information Governance*, ur. Anne Gilliland, Sue McKemmish, Hrvoje Stančić, Sanja Seljan i Jadranka Lasić-Lazić (Zagreb: Sveučilište u Zagrebu, 2013), str. 147-158.

pisa). Isto tako treba kazati da se time dodatno ostvaruje karakteristika neporecivosti zapisa, tj. potpisnik (ili više njih u slučaju da ga je više osoba supotpisalo) ne može poreći činjenicu da je potpisao dokument. Naime, (napredni) elektronički potpis oslanja se na infrastrukturu javnog ključa (engl. *Public Key Infrastructure* – PKI) koja generira dva međusobno ovisna ključa – privatni i javni – koji se koriste za potpisivanje dokumenta (privatni) i za provjeru elektroničkog potpisa (javni).[19] Potpisani se zapis pritom sažima algoritmom za izračunavanje sažetka (engl. *hash*) koji uz privatni ključ stvara elektronički potpis. Upotrebom javnoga ključa bilo tko može provjeriti vjerodostojnost potpisa, a time i zapisa.[20]

Digitalni potpisi bili su do stupanja na snagu eIDAS uredbe regulirani Uredbom 1999/93/EZ. Uredba EU br. 910/2014, odnosno eIDAS (engl. *electronic Identification, Authentication and trust Services*) uredba je iz rujna 2014. koja je stupila na snagu u srpnju 2016. i kojom se reguliraju digitalni potpisi, transakcije i kvalificirane usluge povjerenja.[21] Uredba uspostavlja mehanizme utvrđivanja sredstva elektroničke identifikacije koji su važeći u cijeloj Europskoj uniji, olakšava interoperabilnost sustava elektroničke identifikacije, daje okvir za usluge povjerenja, olakšava izgradnju povjerenja među tržišnim pružateljima usluge povjerenja te daje okvir za napredne elektroničke potpise, pečate i elektroničke vremenske žigove. Da bi e-potpisi i e-pečati bili priznati, moraju biti izdani od kvalificiranog pružatelja usluge povjerenja koji se nalazi na popisu kvalificiranih pružatelja. Tada je potpis važeći na razini Europske unije.[22]

Računalstvo u oblaku (engl. *Cloud Computing*) sveprisutan je model sustava koji omogućava dostupne računalne resurse na zahtjev putem lokalne mreže, intraneta ili Interneta. Računalni oblak može se sastojati od poslužitelja, spremišta podataka, mrežnih aplikacija i servisa. Resursi se mogu dinamički dodjeljivati korisnicima u skladu s njihovim potrebama i u nekoliko minuta su dostupni za korištenje. Riječ je o karakteristici koja se naziva elastičnošću usluge. Druge karakteristike računalstva u oblaku su i stalna dostupnost te usluga na zahtjev, prema želji i potrebama pojedinoga korisnika s više uređaja (pametni telefoni, stolna računala, prijenosna računala) i s bilo kojeg mjesta. Sustav automatski kontrolira i optimizira resurse koji su zauzeti ili slobodni te bilježi njihovo korištenje. Više je modela implementacije oblaka u organizacijama i tvrtkama. Privatni oblak (engl. *Private Cloud*) računalni je oblak koji je u vlasništvu, kojim upravlja i koji koristi jedna

[19] Brzica, Herceg i Stančić, "Long-term Preservation," str. 148.

[20] Hrvoje Stančić, "Long-term Preservation of Digital Signatures," u *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: Zbornik mednarodne konference, Radenci, 13.-15. april 2016: Popisovanje arhivskega gradiva*, ur. Nina Gostenčnik (Maribor: Pokrajinski arhiv Maribor, 2016), str. 481-491.

[21] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, *Službeni list Europske unije*, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[22] Stančić i Ivanjko, "Povjerenje u arhivske e-zapise."

organizacija ili tvrtka s više korisnika na jednoj ili više lokacija. Oblak zajednice (engl. *Community Cloud*) računalni je oblak u kojem više institucija dijeli i zajednički upravlja infrastrukturom. Javni oblak (engl. *Public Cloud*) dostupan je za javno korištenje te njime mogu upravljati javne ustanove, akademske zajednice, državne ustanove i tvrtke ili neka kombinacija svih navedenih. On se nalazi na lokaciji pružatelja usluge u računalnom oblaku. Hibridni oblak (engl. *Hybrid Cloud*) kombinacija je javnog i privatnog računalnog oblaka. Nadalje, postoji nekoliko modela usluga u oblaku. To su Softver kao usluga (engl. *Software-as-a-Service* – SaaS), Platforma kao usluga (engl. *Platform-as-a-Service* – PaaS) i Infrastruktura kao usluga (engl. *Infrastructure-as-a-Service* – IaaS). Prema modelu SaaS korisnik koristi računalne aplikacije putem oblaka bez doticaja s računalnom infrastrukturom, a prema modelu PaaS na infrastrukturu oblaka instalira se računalna aplikacija sa svim popratim servisima i ponovo bez doticaja s infrastrukturom, osim ovlasti vezanih za postavke kod instalacije i podešavanja aplikacije. Prema modelu IaaS korisnik samostalno raspolaže potrebnim računalnim resursima na kojima će instalirati i koristiti svoje aplikacije te ima potpuni pristup infrastrukturi koju koristi.[23]

Infrastrukturu javnog ključa, digitalne potpise i potpisne certifikate koji potvrđuju identitet potpisnika potrebno je razumjeti baš kao i modele implementacije te modele usluga u računalnom oblaku jer dokumenti i zapisi danas sve više nastaju upravo tako opremljeni i u takvim okruženjima. Stoga je važno ostvariti mogućnost njihova dugoročnog očuvanja kao autentičnih, pouzdanih, cjelovitih i upotrebljivih zapisa. Jedna od novijih tehnologija kojom se može postići dugoročno očuvanje valjanosti digitalno potpisanih zapisa bez periodičnog ponovnog potpisivanja, odnosno bez periodičnog dodavanja arhivskog vremenskog žiga, upravo je tehnologija ulančanih blokova.

Ulančani blokovi (engl. *blockchain*) i tehnologija distribuirane glavne knjige (engl. *distributed ledger technology* – DLT) predstavljaju tehnologiju koja je najpoznatija po uporabi u području kriptovaluta, no ona ujedno stoji u pozadini mnogih drugih rješenja, kao što su to rješenja za praćenje provenijencije proizvoda, sustavi za vođenje zemljišnih knjiga i mnoga druga. Osnovni koncepti koji omogućavaju tu tehnologiju su računalni sažetak (engl. *hash*), distribuirana mreža koja nema centralnu točku kontrole ili nadzora (engl. *peer-to-peer network*), distribuirani konsenzus te Merkleovo stablo. Računalni sažetak je jednosmjerna matematička funkcija kojom se stvara niz znakova koji je jedinstven za svaku računalnu datoteku i na temelju kojega se nikako ne može rekonstruirati izvorni sadržaj koji on jedinstveno predstavlja. Računalni sažetak može se nazivati i "digitalnim otiskom

[23] Hrvoje Stančić, Arian Rajh i Ivor Milošević, "Archiving-as-a-Service: Influence of Cloud Computing on the Archival Theory and Practice," u *The Memory of the World in the Digital Age: Digitization and Preservation: An international conference on permanent access to digital documentary heritage*, ur. Luciana Duranti i Elizabeth Shaffer (UNESCO, 2013), str. 108-125.

prsta" neke datoteke ili nekog sadržaja.[24] Nadalje, distribuirana mreža jest mreža koja nema centralnu točku, pa tako njome ne upravlja pojedina osoba ili organizacija, nego su svi njezini korisnici (povezana računala) jednakih prava – svatko od njih upravlja svojim računalom ili poslužiteljem i u dogovoru s ostalim korisnicima koristi isti protokol za povezivanje. Upravo zbog toga je računalni sažetak moguće poslati distribuiranoj mreži na provjeru. Svi članovi mreže koji ga provjere i potvrde o tome obavijeste ostale pa tako dolazi do distribuiranog konsenzusa oko toga da neki računalni sažetak predstavlja određenu datoteku ili sadržaj. Ako ga kvalificirana većina (50% + 1 korisnik) potvrdi, onda se taj sažetak, zajedno s ostalim potvrđenim sažetcima drugih datoteka ili sadržaja, objedinjuje u jedan blok sadržaja i od svih njih stvara se jedan zajednički sažetak koristeći se načelom Merkleova stabla. Tako izračunati vršni sažetak (engl. *top hash*) ili sažetak bloka (engl. *block hash*) objedinjuje se s drugim sadržajem u prvom sljedećem bloku te se tako blokovi međusobno povezuju, čime nastaju ulančani blokovi. Svaki blok na svojem računalu ili poslužitelju zapisuju svi umreženi korisnici te tako nastaje distribuirana glavna knjiga. Ulančani blokovi međusobno ovise jedan o drugom, pa promjena jednog sažetka koji je zapisan u nekom bloku poništava valjanost svih narednih blokova te se vrlo jednostavno može detektirati. Kriptovalute, primjerice, koriste takav pristup za bilježenje novčanih transakcija i sprječavanje da se isti virtualni novac potroši dva puta. No, u području arhivistike, koncept ulančanih blokova Bralić, Kuleš i Stančić koriste za trajnu pohranu informacije o valjanosti potpisnog certifikata u digitalnim potpisima nazivajući takvo rješenje *TrustChain*.[25]

4. Prijedlog rješenja i studija slučaja

4.1. Ulančani blokovi i pametni ugovori

Rješenje koje se u ovom radu predlaže uspostava je okoline koju bi mogle koristiti upravne ustanove koje nemaju svoje sustave za upravljanje tekućom dokumentacijom, a ista okolina mogla bi se nadograditi s dodatnim rješenjem državnog digitalnog arhiva. On se ne razrađuje u ovom članku, nego ga se samo spominje zbog mogućnosti korištenja iste infrastrukture i funkcija. Osnovne komponente predloženog rješenja za čuvanje gradiva u nastanku u upravnim ustanovama jesu državni oblak i ulančani blokovi. Ako se komponenta za državni oblak razvija od početka, potrebno je osigurati pohranu dovoljnoga kapaciteta (u fazi definiranja zahtjeva potrebno ju je parametrizirati), a uz nju potrebno je razviti i aplikaciju za upravljanje pohranom. Pored toga, potrebno je nabaviti aplikaciju za stvaranje i upravljanje virtualnim strojevima (engl. *virtual machine*) te odrediti mrežno rješenje sustava. Primjer toga može biti komponenta nastala na Microsoft Azure platformi u računalnom oblaku, koja je obrađena niže u obliku kraće studije slu-

[24] Rafał Kuchta, "The hash – a computer file's digital fingerprint," *Newtech.law*, 9. rujna 2017., pristupljeno 4. travnja 2018., https://newtech.law/en/the-hash-a-computer-files-digital-fingerprint/.

[25] Bralić, Kuleš i Stančić, "A model for long-term preservation," str. 89-113.

čaja. Druga je komponenta ulančanih blokova. Za njih su dostupna rješenja koja su već povezana na servise koji rade s kriptovalutama, primjerice gotovo rješenje *time:beat* švedske tvrtke Enigio Time, na koje se povezuje putem API-a.[26] Ako se koristi, primjerice, komponenta Azure, ona se može nadograditi s nadolazećim radnim okvirom Coco kao gotovom podlogom za postizanje konsenzusa (detaljnije opisan u nastavku u okviru studije slučaja). Državni oblak trebao bi poslužiti za pohranu koju koriste već postojeće aplikacije uredskog poslovanja (primjerice elektronički urudžbeni zapisnici), a ulančani blokovi služili bi za, najopćenitije rečeno, potvrdu među stranama u komunikaciji. One bi u tom slučaju bile građani i predstavnici drugih ustanova, to jest stranke koje šalju podneske i dopune, primaju rješenja i drugo. Rješenje utemeljeno na ulančanim blokovima podrazumijeva komunikaciju nekoliko strana, odnosno sudionika u nekom poslovnom ili administrativnom procesu. Korištenjem ulančanih blokova moguće je stvoriti rješenje u koje se može imati povjerenje i koje dijelom može automatizirati komunikaciju.

Važno je napomenuti da je rješenje utemeljeno na ulančanim blokovima moguće ostvariti kao otvoreno rješenje u koje se bilo tko može uključiti i potvrđivati transakcije (engl. *public* ili *premissionless blockchain*) te kao zatvoreno rješenje (engl. *private* ili *permissioned blockchain*) u koje su uključeni samo oni korisnici kojima je to dopušteno. U drugom slučaju to, primjerice, mogu biti isključivo (određeni) zaposlenici grupacije organizacija koje upravljaju vlastitim rješenjem ulančanih blokova koje nije javno dostupno, odnosno isključivo određeni mrežni čvorovi u koje postoji povjerenje. Dakle, upravne ustanove trebale bi zadržati komponentu sustava koja služi za potvrđivanje dokumenata i pohranu distribuirane glavne knjige, jer se tako može ostvariti koncept distribuiranoga konsenzusa, a samo gradivo trebalo bi pohranjivati u državnom oblaku. Na taj se način kvalitetnije osigurava distribuirana potvrda autentičnosti uz ekonomičniju centraliziranu pohranu.

Jedno od rješenja arhitekture ulančanih blokova na kojoj se mogu ostvariti automatski ugovorni odnosi između dviju ili više strana korištenjem pametnih ugovora (engl. *smart contract*) predstavlja, primjerice, Azure platforma za računalni oblak koja je utemeljena na usluzi Ulančanih blokova kao usluge (engl. *Blockchain-as-a-Service*). Iz iskustva ranih implementacija tog rješenja i prijašnjih rješenja takve vrste uz pomoć drugih tehnologija može se zaključiti da su dijeljeni poslovni procesi zanimljivi za implementaciju u okviru paradigme ulančanih blokova. Riječ je, naime, o poslovnim procesima koji prelaze granice organizacije i stvaraju povjerenje između ustanova. Upravljanje interakcijama s djelomično pouzdanim stranama, primjerice s građanima, podrazumijeva jasno definiranje obveza, pravila pojedine strane, pravila kako ih ispuniti, u što su uključene i kazne ako se ona ne ispune. Ukratko, može se smatrati da je u tim slučajevima riječ o jednom obliku ugovora.

[26] Enigio Time, "Protect your files," početna stranica za *time:beat*, pristupljeno 4. travnja 2018., https://timebeat.com/.

Kod klasičnih, pisanih, ugovora ugovorna strana mora samostalno izvršiti definirane stavke ugovora, primjerice provesti uplatu nakon što je druga strana izvršila uslugu, a kod pametnih ugovora uvjeti se definiraju u obliku programa koji se automatski provede kad su uvjeti za njegovo provođenje ispunjeni. Dakle, čim jedna strana završi uslugu, automatski će se, bez zadrške, pokrenuti program koji će provesti prijenos potrebnih financijskih sredstava ili na drugačiji način ispuniti uvjete ugovora. U pametne se ugovore tako mogu definirati (programirati) različiti uvjeti, takav pametni ugovor nakon toga sve ugovorne strane potpisuju svojim elektroničkim potpisom i on se bilježi u ulančane blokove. Komponente koje su potrebne za uspostavu sustava pametnih ugovora su shema (elementi podataka za provedbu), logika (poslovna pravila definirana u shemama), ugovorne strane (privatne osobe, organizacije, poslovne organizacije), vanjski izvori (podatci za pokretanje provedbe ugovora i njegovo dovršenje), instanca glavne knjige (nepromjenjiva instanca svih potvrđenih i ulančanih blokova) i obvezujući ugovor. Obvezujući ugovor nastaje tako da se najprije pokrene razmjena shema između ugovornih strana, potom se verzionira te se, kada ga sve strane potvrde, ubilježi u ulančane blokove i distribuiranu glavnu knjigu. To je važno razumjeti i zato što arhivisti u budućnosti realno mogu očekivati da će pametne ugovore biti potrebno očuvati, baš kao i klasične ugovore. Drugim riječima, znanja i kompetencije koje će arhivisti trebati usvojiti nalaze se i u području ulančanih blokova.

4.2. Studija slučaja – radni okvir Coco

Kao jedan od primjera tehnologije koja se može iskoristiti za razvoj rješenja koja koriste ulančane blokove radni je okvir Coco (engl. Coco – *Confidential Consortium – Framework*), koji radi na Azure usluzi u oblaku i koji će biti predstavljen tijekom 2018. godine. Prema najavama, Coco je sustav otvorenoga koda koji omogućava formiranje cjelovitih rješenja utemeljenih na ulančanim blokovima i koji se koristi pouzdanim okruženjima (engl. *Trusted Execution Environment* – TEE), čime omogućava formiranje pouzdanih mreža fizičkih čvorova na kojima će se nalaziti distribuirana glavna knjiga. Riječ je, dakle, o osnovi u koju se može imati povjerenja prilikom nadogradnje, tj. integracije drugih, već postojećih, rješenja za ulančane blokove. Radni okvir dizajniran je tako da pruža sigurnu i pouzdanu bazu komponenti koje mogu koristiti bilo koji protokol ulančanih blokova, pri čemu radni okvir osigurava algoritme za uspostavu konsenzusa.[27]

Sasvim konkretno, tijekom transakcijskog procesa radni okvir provodi dvije vrste transakcija – aplikacijske i administrativne. Aplikacijske transakcije predstavljaju skup glavnih poslovnih transakcija koje prolaze kroz mrežu i koje sudionici potvrđuju. S druge strane, administrativna transakcija je primjerice dodavanje novih članova u mrežu. Pritom se koriste slični postupci za primanje i obradu obje vrste transakcija, uključujući i način na koji se postiže konsenzus. S logičke strane,

[27] Microsoft, *The Coco Framework: Technical Overview* (Microsoft, 2017).

kako se te dvije vrste transakcija ne bi miješale, na svakom povezanom čvoru postoje dvije distribuirane glavne knjige – jedna za aplikacijske, a druga za administrativne transakcije. Bez obzira na vrstu transakcije, taj radni okvir koristi sigurne komunikacijske kanale za komunikaciju aplikacije s čvorom i za komunikaciju čvora s čvorom kako bi zaštitio povjerljive zapise. Autentikacija korisnika i enkripcija komunikacije podržani su u aplikacijskom umjesto u transportnom sloju, kako je to standardno uobičajeno, što doprinosi sigurnosti. Dakle, aplikacija uspostavlja vezu te je prema mreži kriptira. Nakon toga radni okvir prima transakciju, dekriptira ju i šalje prema protokolu za ulančavanje blokova. On izvršava transakciju i potom je replicira. Dakle, takav pristup daje mogućnost organizacije komponenti sustava u slojeve, što ga čini jednostavnijim za implementaciju i sigurnijim.

Ta kratka studija slučaja može se iskoristi za testiranje koncepata. Implementacija konkretnog sustava svakako treba biti izvedena tehnologijama koje omogućavaju smještaj svih resursa i podataka u Republici Hrvatskoj. Tehnologije kojima je izveden sustav treba ionako biti moguće mijenjati, što je zahtjev norme za otvorene arhivske informacijske sustave[28] u pogledu neovisnosti sadržaja arhiva, odnosno gradiva u arhivu od trenutačne tehnologije u kojoj je taj digitalni arhiv izveden.

4.3. Osiguranje i očuvanje autentičnosti

Nakon razjašnjenja kako funkcioniraju koncepti ulančanih blokova, distribuirane glavne knjige i pametnih ugovora te nakon razjašnjenja kako funkcionira jedan od mogućih implementacijskih radnih okvira, u nastavku je potrebno pojasniti kako bi u operativnom smislu u jednom takvom sustavu funkcioniralo osiguranje i očuvanje autentičnosti. U osiguranje autentičnosti gradiva trebaju biti uključeni procesi sustava koji izračunavaju sažetak zapisa, identifikacijski metapodatci i metapodatci o obliku, tehničkim karakteristikama, poslovnom i stvarateljevom kontekstu gradiva koji su zabilježeni u sustav te, dodatno, poveznica s dokumentiranim procedurama u internim aktima ili s operativnim procedurama sustava kvalitete. Očuvanje autentičnosti gradiva tada preuzima sustav od povjerenja, koji je formiran kao distribuirani sustav čiji se čvorovi nalaze u upravnim organizacijama i koji u ulančane blokove dodaje nove sažetke sadržaja svakog novog zapisa, posve novog ili postojećeg koji se konvertira u novi format zapisa ili migrira na novi medij, odnosno nad kojim se provela neka aktivnost u vezi s njegovim očuvanjem. Jedinice gradiva moraju biti vidljive i iz sustava za upravljanje arhivskim gradivom (engl. *Archives Management System*, AMS) ili elektroničkih knjiga pismohrane, iako one nisu u opsegu ovog predloženog rješenja. Tako se zadovoljava zahtjev za pridruženim opisom jedinice digitalnog arhiva norme za otvorene

[28] International Organization for Standardization, *Space data and information transfer systems – Producer-Archive Interface Specification (PAIS)*, ISO 20104:2015 (Geneva: International Organization for Standardization, 2015).

arhivske informacijske sustave,[29] a kada se u AMS-u uz jedinice gradiva vidi i informacija o aktivnom postupku očuvanja arhivista, tada se zadovoljava i B3 zahtjev za ocjenu i očuvanje autentičnosti digitalnih zapisa projekta InterPARES.[30]

Sustav – sloj koji osigurava distribuirani konsenzus čiji se čvorovi nalaze u upravnim organizacijama i koji je povezan s državnim oblakom za centraliziranu pohranu – treba omogućavati izvoz gradiva u digitalni arhiv nadležnog arhiva (u slučaju da su digitalni repozitoriji nadležnih arhiva zasebni sustavi), prikazati odabrano gradivo u pogledu na ukupno gradivo stvaratelja u jedinstvenom državnom digitalnom arhivu (u slučaju da je taj sustav već izrađen na istoj infrastrukturi), odnosno napraviti transfer u bilo koju drugu digitalnu okolinu. Transfer u neku drugu okolinu treba se provoditi prema prilagođenim specifikacijama za dostavljene informacijske pakete,[31] prema normi ISO 20104:2015 odnosno CCSDS 651.1-B-1, a bliski primjeri su specifikacije E-ARK projekta. Također treba napomenuti da se u sloj sustava koji koristi ulančane blokove pohranjuju isključivo izračunati sažetci i manja količina pripadajućih metapodataka, a sami zapisi i dalje zahtijevaju posve funkcionalan digitalni arhiv, usklađen s normom za otvorene arhivske informacijske sustave i povezanim normama. Drugim riječima, potrebno je nadograditi koncept digitalnog arhiva infrastrukturom za ulančane blokove i distribuiranu glavnu knjigu radi osiguranja i očuvanja autentičnosti, napose elektronički potpisanoga gradiva.

---

[29] International Organization for Standardization, *Space data and information transfer systems – Open archival information system (OAIS) – Reference model*, ISO 14721:2012 (Geneva: International Organization for Standardization, 2012); Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices: Reference Model for an Open Archival Information System (OAIS): Recommended practice: CCSDS 650.0-M-2* (Washington, DC: Consultative Committee for Space Data Systems, 2012).

[30] Authenticity Task Force, *Requirements for Assessing and Maintaining the Authenticity of Electronic Records: Appendix 2* (InterPARES, 2002), str. 8, pristupljeno 4. travnja 2018., http://www.interpares.org/display_file.cfm?doc=interpares_book_k_app02.pdf.

[31] Hrvoje Stančić, *Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata* (doktorski rad, Sveučilište u Zagrebu, 2005), str. 31-32.

4.4. Razvojne faze projekta

Uzevši sve do sada rečeno, u nastavku se ukratko razrađene moguće projektne faze projekta razvoja državnog oblaka nadograđenog slojem za ulančavanje zapisa i distribuirani konsenzus. Predviđene su faze kako je to prikazano na Slici 1, odnosno predviđene su određene grupe aktivnosti za koje smatramo da su ključne za uspješno pokretanje i vođenje takvog projekta. Neke faze mogle bi se odvijati paralelno, a druge bi se mogle odvijati slijedno, odnosno dovršetak prethodne faze trebao bi biti uvjet za početak sljedeće. Za svaku fazu treba definirati aktere koji su za nju odgovorni. Vrijeme izraženo u mjesecima (M1-M18) ilustrativnog je karaktera i ne odražava stavove autora o stvarno potrebnom vremenu za odvijanje pojedine faze, jer ono ovisi o mnogo čimbenika, no međusobne odnose dužine trajanja pojedinih faza smatramo realnima (Slika 1).

Gantogram na Slici 1 predstavlja, dakle, ogledni primjer planiranja aktivnosti za projekt te vrste. Prema vrsti aktivnosti (određivanje nositelja, resursa, tehnologija itd.), dijagram predstavlja jednu metarazinu bavljenja tematikom. Smatramo da je od velike društvene važnosti osmisliti, predložiti i provesti konkretan projekt na tu temu i nadamo se da će taj ogledni primjerak navođenja i raspoređivanja nužnih aktivnosti pomoći potencijalnim autorima projekta.

Br.	Naziv faze	Odgovornost za fazu	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
1	Određivanje nositelja projekta	Uprava																		
2	Određivanje početnih resursa	Voditelj projekta																		
3	Određivanje jezgre resursa	Voditelj projekta																		
4	Popisivanje zahtjeva	Razvojni tim																		
5	Određivanje tehnologije i rješenja	Razvojni tim																		
6	Izrada specifikacije	Analitičar																		
7	Nabava tehnologija	Razvojni tim																		
8	Razvoj sustava	Razvojni tim																		
9	Testiranje sustava	Tim za testiranje																		
10	Obuka korisnika	Tim za obuku																		
11	Testno uvođenje u rad u odabranim institucijama	Razvojni tim; Voditelj projekta																		
12	Uvođenje u rad	Razvojni tim; Voditelj projekta																		
13	Upravljanje projektom	Voditelj projekta																		

Slika 1. Ganttov dijagram razvojnih faza projekta

5. Rasprava

Sagledavajući cjelokupnu sliku stanja u Republici Hrvatskoj prije svega je potrebno konstatirati da državni oblak nije razvijen. Budući da nemaju sve upravne ustanove mogućnost adekvatne pohrane gradiva u digitalnom obliku, potrebno ga je razviti kako bi dokumentarno i arhivsko digitalno gradivo moglo ostati očuvano i autentično te se kao vjerodostojno moglo koristiti u svim potrebnim procesima. Razvoj takvog cjelovitog rješenja nije ni jednostavan ni jeftin, a IT stručnjaci ne mogu ga razviti bez suradnje s arhivistima. Od financijskih resursa koje je potrebno osigurati za predloženi sustav treba prije svega spomenuti da su potrebna ulaganja u infrastrukturu državnog oblaka. To zahtijeva ulaganja u komponente namijenjene pohrani cjelokupnoga gradiva i arhiviranju arhivskoga gradiva, uz

postupke proaktivnog očuvanja, te pripadajuće upravljačke aplikacije, potom ulaganje u mrežno rješenje, u podatkovne centre za drugu i treću sigurnosnu kopiju gradiva te ulaganje u razvoj okoline za primjenu koncepta ulančanih blokova i tehnologije distribuirane glavne knjige. Također su potrebna ulaganja u razvoj usluga i sučelja cjelokupnog rješenja. Potom je potrebno razviti funkcije na tom rješenju koje se odnose na prihvat, pohranu, provjeru autentičnosti, očuvanje i diseminaciju gradiva za različite kategorije korisnika. Dodatna ulaganja potrebna su u licence za gotova rješenja koja se mogu uklopiti u sustav (primjerice za aktivnosti u vezi s dugoročnim očuvanjem – konverzija, migracija i sl.). Naposljetku, sustav i sve njegove komponente potrebno je održavati dulji niz godina, dokle god se tehnologije primijenjene u razvoju sustava koriste.

Uz vrlo realnu pretpostavku da dio ustanova nema dovoljan broj kvalitetnog informatičkog osoblja, sučelje sustava treba biti razvijeno tako da zahtijeva gotovo intuitivno korištenje. Obvezna nacionalna kampanja osposobljavanja osoblja ustanova treba biti izvedena temeljito i učinkovito, za što se mogu iskoristiti i sustavi za e-učenje kako bi se dodatno smanjili troškovi i ubrzao proces edukacije. Korist koju upravne ustanove u Hrvatskoj mogu ostvariti implementacijom i korištenjem takvog rješenja višestruka je. Prvo, budući da predložena infrastruktura stvara uslugu u oblaku na državnoj razini, ulaganja pojedinih ustanova u infrastrukturu prestaju ili su minimalna. Naravno, upravne organizacije trebaju zadržati dovoljno infrastrukture za uspostavljanje distribuiranog konsenzusa koji je potreban za očuvanje autentičnosti konceptom ulančanih blokova, ali to je zanemariv dio u odnosu na sustave koji bi bili potrebni za pohranu kad se ona ne bi centralizirala u državni oblak. Drugo, pravovremeno uključivanje svih ili većeg broja upravnih ustanova ne samo da smanjuje pojedinačne troškove, nego dugoročno osigurava jednoobraznu zaštitu i očuvanje digitalnog ili digitaliziranoga gradiva na standardiziranoj razini kvalitete. Treće, s obzirom na to da je riječ o usluzi u oblaku, održavanje sustava je jednostavnije, a održivost sustava veća. Četvrto, predloženo rješenje kvalitetnije i efikasnije priprema gradivo za transfer u budući državni digitalni arhiv. Ne treba zaboraviti da će ustanove, prema novom Zakonu o arhivskom gradivu i arhivima, najkasnije u roku od deset godina od nastanka digitalnoga gradiva to gradivo morati predati u (nadležnost) arhiva. Najzad, predloženo rješenje može biti osnova državnog digitalnog arhiva.

Trenutačno ne postoji državni digitalni arhiv, a trebalo bi ga uspostaviti koristeći infrastrukturu državnog oblaka kao što je predloženo u ovom članku. Prilikom razvoja valjalo bi koristiti ISO norme za implementaciju digitalnih arhiva (arhiv – ISO 14721:2012, transfer – ISO 20104:2015, certifikacija – ISO 16363:2012) te iskustva nekomercijalnih projekata (primjerice projekt E-ARK) i komercijalnih organizacija koji su imali za cilj razvoj (Preservica i dr.) ili vrednovanje digitalnih arhiva. U 2010-ima su se znanstvene zajednice i državne ustanove raznih zemalja EU intenzivno bavile temama implementacije digitalnih arhiva, pa je moguće graditi jedan takav projekt na temeljima dosadašnjih dostignuća. Državv-

ni digitalni arhiv predstavlja logičnu nadogradnju predloženog rješenja koje pritom koristi istu strukturu kao rješenje i koji, slikovito rečeno, predstavlja "sigurni trezor" za onaj dio gradiva koji je prema posebnim popisima gradiva unaprijed proglašen arhivskim. Uz proširenje infrastrukturnih kapaciteta prema potrebama u budućnosti, dodatni troškovi državnog digitalnog arhiva, u odnosu na opisan ishodišni sustav za upravu koja stvara gradivo, nisu veliki jer se koristi ista infrastruktura, a potrebni su za razvoj i uspostavu rješenja za opis gradiva, formatiranje opisa, semantičko obogaćivanje gradiva, stvaranje obavijesnih pomagala te povećanje vidljivosti gradiva za građane.

6. Daljnje istraživanje i zaključak

Proces upravljanja digitalnim gradivom upravnih ustanova i proces očuvanja toga gradiva u istoj okolini koja se tijekom vremena neprestano mijenja ili u okolini nadležnog arhiva, provođen na način da to gradivo bude očuvano kao autentično, proaktivni je i ciklični proces. U njemu svojstvo autentičnosti zapisa (povjerenje u zapis) prelazi u svojstvo pouzdanosti sustava, repozitorija ili arhiva (povjerenje u sustav), a potom se prilikom transfera opet transponira na zapise koji ulaze u neku drugotnu okolinu ili istu, ali izmijenjenu okolinu u budućnosti. Autentičnost zapisa tada se opet prenosi na sustav. Zbog toga je iznimno važno izgraditi pouzdane sustave upravljanja gradivom za sve stvaratelje koji svojim gradivom moraju pouzdano upravljati radi očuvanja prava članova društva i ostvarenja viših društvenih ciljeva. Isto tako je važno uspostaviti pouzdane arhivske sustave radi izgradnje memorije društva i društvenih skupina, izgraditi digitalne arhive koji će osigurati dugoročnu ili trajnu pohranu najvrjednijeg dijela toga gradiva. Sustav tog tipa mora biti utemeljen na suvremenim spoznajama i dostignućima u arhivistici te mora funkcionirati prema suvremenim stručnim normama kako bi se gradivom upravljalo na rutinski, kvalitetan i pouzdan način, odnosno kako bi se izgradilo povjerenje internih korisnika ustanova i javnosti koja je u interakciji s njima. Izostanak takvog sustava jednak je izostanku prakse upravljanja papirnatim gradivom i potpunom nepostojanju arhiva od opeka i betona. Dobar dio ustanova u Hrvatskoj nema adekvatne sustave koji mogu upravljati tekućim digitalnim (dokumentarnim) gradivom na način da ono bude pohranjeno kao autentično te da ostane autentično. Hrvatska nema vlastiti digitalni arhiv koji može sustavno, planski i u skladu s propisima preuzimati digitalno arhivsko gradivo i očuvati njegovu autentičnost.

Baš kao što država treba imati uređene procese s konvencionalnim gradivom, tako ona treba urediti i procese s digitalnim gradivom koje nastaje te osigurati uvjete za učinkovito upravljanje i pohranu toga gradiva. Sustav za upravljanje digitalnim gradivom koji može osigurati i očuvati autentičnost toga gradiva potencijalni je projekt od interesa za veliki broj ustanova iz upravne domene. Ustanove koje već imaju razvijene svoje sustave za upravljanje digitalnim i digitaliziranim gradivom mogu integrirati potrebne i u ovom članku opisane funkcionalnosti u te

postojeće sustave i kasnije prenositi digitalno arhivsko gradivo u budući državni digitalni arhiv.

Mogu li građani imati povjerenje u institucije države koje nemaju osigurane mehanizme i načine upravljanja vlastitim informacijama, gradivom i memorijom? Izgradnja sustava za upravljanje gradivom prema predloženom modelu uspostave mreže institucija koje ravnopravno sudjeluju u potvrđivanju i očuvanju autentičnosti digitalnoga gradiva, razvoja državnog računalnog oblaka i njegove nadogradnje u obliku državnog digitalnog arhiva pridonijet će, između ostaloga, izgradnji suvremenih institucija uređenog društva te izgradnji šireg povjerenja u njih.

Službena glasila

Službeni list Europske unije (Bruxelles), 2014.

Literatura

Authenticity Task Force. *Requirements for Assessing and Maintaining the Authenticity of Electronic Records: Appendix 2*. InterPARES, 2002. Pristupljeno 4. travnja 2018., http://www.interpares.org/display_file.cfm?doc=interpares_book_k_app02.pdf.

Bralić, Vladimir, Magdalena Kuleš, Hrvoje Stančić. "A model for long-term preservation of digital signature validity: TrustChain." U *INFuture2017 Proceedings: The Future of Information Sciences*, ur. Iana Atanassova, Wajdi Zaghouani, Bruno Kragić, Kuldar Aas, Hrvoje Stančić i Sanja Seljan, str. 89-103. Zagreb: University of Zagreb, 2017.

Brzica, Hrvoje, Boris Herceg, Hrvoje Stančić. "Long-term Preservation of Validity of Electronically Signed Records." U *The Future of Information Sciences: INFuture2013: Information Governance*, ur. Anne Gilliland, Sue McKemmish, Hrvoje Stančić, Sanja Seljan i Jadranka Lasić-Lazić, str. 147-158. Zagreb: Sveučilište u Zagrebu, 2013.

Consultative Committee for Space Data Systems. *Recommendation for Space Data System Practices: Reference Model for an Open Archival Information System (OAIS): Recommended practice: CCSDS 650.0-M-2*. Washington, DC: Consultative Committee for Space Data Systems, 2012.

Duranti, Luciana. "Diplomatics: New Uses for an Old Science." *Archivaria* br. 28 (1989): str. 7-27.

Duranti, Luciana. "Policy Cross-domain: Authenticity and Authentication in the Law." U *International Research on Permanent Authentic Records in Electronic Systems: InterPARES 2 Project*. Associazione Nazionale Archivistica

Italiana, 2005. Pristupljeno 4. travnja 2018., http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf.

Enigio Time. "Protect your files." Početna stranica Internet stranice *time:beat*. Pristupljeno 4. travnja 2018., https://timebeat.com/.

Gartner, Richard. *Metadata: Shaping Knowledge from Antiquity to the Semantic Web*. Cham: Springer, 2016.

International Organization for Standardization. *Information and documentation – Records management – Part 1: Concepts and principles*. ISO 15489-1:2016. Geneva: International Organization for Standardization, 2016.

International Organization for Standardization. *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*. ISO 16363:2012. Geneva: International Organization for Standardization, 2012.

International Organization for Standardization. *Space data and information transfer systems – Producer-Archive Interface Specification (PAIS)*. ISO 20104:2015. Geneva: International Organization for Standardization, 2015.

International Organization for Standardization. *Space data and information transfer systems – Open archival information system (OAIS) – Reference model*. ISO 14721:2012. Geneva: International Organization for Standardization, 2012.

Kuchta, Rafał. "The hash – a computer file's digital fingerprint." *Newtech. law*, 9. rujna 2017. Pristupljeno 4. travnja 2018., https://newtech.law/en/the-hash-a-computer-files-digital-fingerprint/.

MacNeil, Heather, Bonnie Mak. "Constructions of Authenticity." *Library Trends* 56, br. 1 (2007): str. 26-52.

MacNeil, Heather. "Trusting records in a postmodern world." *Archivaria* br. 51 (2001): str. 36-47.

Microsoft. *The Coco Framework: Technical Overview*. Microsoft, 2017.

Pearce-Moses, Richard. *A Glossary of Archival and Records Terminology*. Chicago: The Society of American Archivists, 2005.

Rajh, Arian. "Teorijski model digitalnog arhivskog sustava." Doktorski rad, Sveučilište u Zagrebu, 2010.

Rajh, Arian. "The problem of maintaining and proving authenticity in the transition from Producer to Archive." Predavanje s prezentacijom održano na Veleučilištu u Oslu i Akershusu, 24. listopada 2016. doi:10.13140/RG.2.2.29500.64640.

Rogers, Corinne. "A literature review of authenticity of records in digital systems from 'machine-readable' to records in the cloud." *Acervo* 29, br. 2 (2016): str. 16-44.

Stančić, Hrvoje, Arian Rajh, Ivor Milošević. "Archiving-as-a-Service: Influence of Cloud Computing on the Archival Theory and Practice." U *The Memory of the World in the Digital Age: Digitization and Preservation: An international conference on permanent access to digital documentary heritage*, ur. Luciana Duranti i Elizabeth Shaffer, str. 108-125. UNESCO, 2013.

Stančić, Hrvoje, Tomislav Ivanjko. "Povjerenje u arhivske e-zapise." *BugOnline*, 6. lipnja 2016. Pristupljeno 5. travnja 2018., https://www.bug.hr/molex/elektronicki-potpisi-pecati-okviru-uredbe-eida/97352.aspx.

Stančić, Hrvoje. "Long-term Preservation of Digital Signatures." U *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: Zbornik mednarodne konference, Radenci, 13.-15. april 2016: Popisovanje arhivskega gradiva*, ur. Nina Gostenčnik, str. 481-491. Maribor: Pokrajinski arhiv Maribor, 2016.

Stančić, Hrvoje. *Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata*. Doktorski rad, Sveučilište u Zagrebu, 2005.

Tennis, Joseph T., Randy Preston. "Part Eight – Terminological Instruments: Terminology Cross-domain Task Force Report." U *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, ur. Luciana Duranti and Randy Preston. Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008. Pristupljeno 5. travnja 2018., http://www.interpares.org/display_file.cfm?doc=ip2_book_part_8_terminology_task_force.pdf.

The Center for Research Libraries, Online Computer Library Center. *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. Chicago: The Center for Research Libraries, 2007.

Summary

THE CONCEPT FOR SUPPORTING AND PRESERVING THE TRUSTWORTHINESS OF GOVERNMENTAL INSTITUTIONS' RECORDS IN CROATIA BY THE DEVELOPMENT OF A STATE CLOUD AND THE NATIONAL DIGITAL ARCHIVES

This article proposes a conceptual solution for the cloud-based electronic recordkeeping system for Croatian governmental institutions. The solution could provide maintenance of authentic records for a large group of Croatian governmental institutions and the preservation of their archived materials. The proposed solution can also be the foundation for the national digital archives, which Croatia certainly needs. The absence of the national digital archives today resembles the nonexistence of the national archives made of brick and concrete. In their proposal,

the authors rely on a cloud solution, governed by the state for the reasons of storing large amounts of material more economically, and a blockchain solution controlled by the institutions-participants which can support the important archival aspects of the preserved digital records over time.

What does it mean to store and archive authentic current and archival materials? What would be the consequences of this practice for the institutions themselves? Trust in institutions through the trust in their founders cannot be the foundation for the "places of authentication" (loca credibilia, trustworthy institutions) or the similar convention in the contemporary world. The quality of functions, processes and their digital recordkeeping systems and archives should be the cornerstone of this convention of confidence in institutions nowadays. In the first part of the article, the authors decompose the complex, tautological and fractally created notions of trustworthiness, reliability, and authenticity of the institutions, their systems and archives, and their records. The results of this deconstruction are operational concepts of the authenticity of records and trustworthiness of systems, archives, and institutions. These deconstructed concepts are now suitable for the construction of electronic records management systems and digital archives. The preservation of the digital records, especially those which are digitally signed, and maintenance of their authenticity, represent the challenge for contemporary administrative and archival practice. The second part of the article deals with the archival concept of preservation and the problem of certificates issued only for a limited duration. In the third part of the article, the authors focus on the available technologies, and in the fourth part of the article, the authors deal with the possible case study suggestion and the reference project management framework for one of the possible solutions. The fifth part of the article brings the discussion and reasoning for this endeavour. Comparing this cloud-based solution with a variety of in-house developed projects, it would take less investment per institution, the entire network would have a standardised level of protection of digital materials, the sustainability would be higher, and the transfers of materials to the national archives would be better prepared. The authors offer the conclusion and the further research directions in the last part of the article.

The government and its institutions should have their administrative (business) processes streamlined and maintained, as well as their processes with current and archival records. There are many governmental institutions in Croatia which do not have this kind of controls in place and a system based on the proposed concept would help them catch up with the developed world. Finally, the development of the system and the digital archives according to the proposed conceptual solution should significantly contribute to the proper recordkeeping practice and public's trust in the governmental institutions.

Keywords*: authentic archival materials; state cloud; public trust; blockchain; trusted institutions; national digital archives*