Hrvoje Brzica
Boris Herceg
FINA
Vrtni put 3
Zagreb

Tihomir Katulić
Pravni fakultet Sveučilišta u Zagrebu
Trg maršala Tita 14
Zagreb

Hrvoje Stančić
Filozofski fakultet Sveučilišta u Zagrebu
Ivana Lučića 3
Zagreb

ANALIZA UTJECAJA HRVATSKOGA ZAKONODAVNOG OKVIRA NA ELEKTRONIČKO POSLOVANJE I DUGOROČNO OČUVANJE ELEKTRONIČKI POTPISANIH DOKUMENATA

UDK 340.134(497.5)]:658.01:004.73./78
UDK 004.738.5:347.74
Pregledni rad

U radu autori istražuju hrvatski zakonodavni okvir koji se odnosi na elektroničko poslovanje te ga stavljaju u kontekst sličnoga zakonodavnog okvira u zemljama Europske unije. Radi boljega razumijevanja problema koji se pojavljuju u rješenjima hrvatskoga zakonodavca, autori identificiraju ključne elemente infrastrukture javnoga ključa (PKI) koji su bitni za elektroničko poslovanje. Autori tumače pojmove infrastruktura javnoga ključa, digitalni certifikat, kvalificirani certifikat, certifikacijska služba, registracijski autoritet, neporecivost, pouzdana arhivska služba, vremenski žig, pouzdani vremenski žig, elektronički potpis, napredni elektronički potpis te PDF/A. Potom analiziraju postojeća zakonodavna ograničenja u Hrvatskoj, koja sprječavaju širu primjenu elektroničkoga poslovanja u praksi. Pritom provode komparativnu analizu s Direktivom 1999/93/EC, identificiraju problematične segmente postojećih

zakona te predlažu njihova konkretna poboljšanja. Konačno, autori se osvrću na ulogu arhivista u dugoročnom očuvanju elektronički potpisanih dokumenata.

Ključne riječi: *hrvatsko zakonodavstvo, elektroničko poslovanje, elektronički potpis, digitalni certifikat, dugoročno očuvanje elektroničkoga gradiva*

1. Uvod

Pitanje pravne regulacije elektroničkoga potpisa u vremenu kad se intenzivno prelazi na komunikaciju preko elektroničkih informacijskih sustava od presudne je važnosti. Elektronička je komunikacija brža, pouzdanija i bitno jeftinija. Direktna i indirektna elektronička trgovina[1] ključne su za globalne ekonomske procese. Razvoj trgovine internetom ubrzao je i razvoj drugih, danas široko prihvaćenih tehnologija, poput elektroničkoga transfera novca, internetskoga marketinga, tehnologija za razmjenu podataka (engl. *electronic data interchange – EDI)* te automatske pohrane i analize podataka.

Elektronički potpis bitan je element elektroničkoga poslovanja. Tehnički pouzdan i pravno prihvatljiv sustav elektroničkoga potpisa čini elektroničku komunikaciju, a time i elektroničko poslovanje, pravno sigurnima i pouzdanima, baš kao što je to moguće i uporabom nekih drugih, prije spomenutih, tehnologija. Tehnologije elektroničkoga potpisa kakve danas poznajemo možda ne pružaju apsolutnu sigurnost u identitet i sadržaj elektroničke komunikacije, ali mogu omogućiti prihvatljivu razinu sigurnosti. Upotreba elektroničkoga potpisa prožima sve aspekte upotrebe informacijske tehnologije u pravnom prometu. Elektroničkim potpisom mogu se autorizirati poruke elektroničke pošte, elektroničke isprave i druge dokumente (poput ugovora) u elektroničkom obliku,[2] zatim zaštititi uporabu sredstava neposredne elektroničke komunikacije u realnom vremenu, poput internetske telefonije, alata za trenutnu razmjenu poruka (engl. *instant messaging – IM*) i drugih komunikacijskih servisa.

Sve ove situacije imaju reperkusije na arhivistiku kao znanosti i kao struku. Vidljivo je povećanje broja međunarodnih znanstveno-istraživačkih projekata koji istražuju i donose preporuke i konkretna rješenja povezana s kratkoročnim i dugoročnim arhiviranjem (engl. *long-term preservation/archiving*) elektroničkih zapisa. Posve je jasno da digitalno potpisane elektroničke poruke, ugovore i sl. ne samo da nije moguće čuvati kao i klasična, analogna pisma ili ugovore u papirnatom obliku već ih nije moguće čuvati niti kao i »obične«, digitalno nepotpisane elektroničke dokumente. Oni, zbog činjenice da im je dodana još jedna razina složenosti (digitalni potpis i sl. o čem će više riječi biti u nastavku), imaju dodatne zahtjeve prilikom dugoročnoga čuvanja. Svemu tom potrebno je posvetiti pozornost te pri-

[1] Dragičević, D. *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb : Informatorov Biro Sustav, 2004., str. 40.

[2] Matić, T. Elektronički potpis. *Odvjetnik* (Zagreb). 11–12(2010), str. 8.

mijeniti rezultate znanstvenih istraživanja i specifična stručna znanja koja su sve više potrebna u suvremenoj, postkustodijalnoj arhivistici. Pritom je najbitnije istaknuti da dugoročno očuvanje elektroničkoga gradiva treba započeti u trenutku njegova nastanka. Stoga je u ovom tekstu fokus stavljen na zakonodavni okvir u Hrvatskoj koji uređuje pitanje elektroničkoga poslovanja koje bi u konačnici trebalo stvarati suvremeno arhivsko gradivo. Svrha je rada, dakle, istaknuti uočene realne prepreke u postojećem zakonodavnom okviru te sugerirati i argumentirati poboljšanja koja će za cilj imati pojednostavljenje i ubrzanje elektroničkoga poslovanja. U konačnici će to dovesti i do jednostavnijega rukovanja elektroničkim arhivskim gradivom, ali i do njegova stvaranja u skladu s relevantnim normama.

2. Zakonodavni okvir koji uređuje pitanje elektroničkoga načina poslovanja

Do donošenja hrvatskoga Zakona o elektroničkom potpisu (NN 10/02, 80/08, 30/14) u hrvatskom pravu nije bilo zakonâ koji bi definirali potpis, osobito u kontekstu pravno valjane isprave u elektroničkom obliku. Naravno, postoje mnogi zakoni koji određuju potpis kao uvjet sklapanja pravnoga posla, valjanosti podneska u postupku itd.[3] Zakon o obveznim odnosima sadržava odredbe koje koriste termin potpis podrazumijevajući pod njime čin stavljanja potpisa ili kakva drugoga neposrednog osobnog traga, ali istodobno ne definirajući u čem se potpis, odnosno potpisivanje sastoji[4]. Isto tako, Zakon o parničnom postupku[5] redovito navodi potpis stranke kao formalni uvjet bez kojega se nekoj ispravi ili podnesku ne mogu priznati ni autentičnost ni valjanost. Slične odredbe sadržavaju i Zakon o kaznenom postupku, Zakon o općem upravnom postupku, Zakon o upravnom sporu i mnogi drugi zakoni.

Elektronički potpis kao pravni ekvivalent vlastoručnom potpisu i pečatu sposoban je uvelike ubrzati poslovanje.[6] Elektronički potpis omogućuje veći broj paralelnih poslovnih transakcija, čuvajući istodobno sigurnost i povjerljivost poslovne komunikacije u digitalnom okruženju.

Unatoč tomu što u razvijenim zemljama Zapadne Europe i Sjedinjenim Američkim Državama uvođenje informacijskih tehnologija u poslovanje traje još od sedamdesetih godina 20. st.[7] te i unatoč činjenici da je prvi Zakon o informatičkoj

[3] *V.* Zakon o obveznim odnosima (NN 35/05, 41/08, 125/11) čl. 287., 292., 293. itd., Zakon o parničnom postupku (NN 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 123/08, 57/11, 148/11, 25/13) čl. 97., 106., 127. itd., Zakon o kaznenom postupku (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13), Zakon o općem upravnom postupku (47/09) itd.

[4] Matić, T. *Osnove prava elektroničke trgovine*. Zagreb : MEP Consult, 2008., str. 55.

[5] Npr. čl. 350. Sadržaj žalbe Zakona o parničnom postupku ili čl. 106. ZPP; Slične odredbe sadržavaju i Zakon o kaznenom postupku (čl. 79. Elektronička isprava), Zakon o općem upravnom postupku (čl. 75. Elektronička komunikacija), Zakon o upravnim sporovima (čl. 25. Predaja tužbe, čl. 49. Podnesci, čl. 53. Razgledavanje spisa itd.) itd.

[6] Vojković, G. Elektronički potpis. *Godišnjak 12 Hrvatskog društva za građanskopravne znanosti i praksu* (Zagreb). 2005., str 463.

[7] Dragičević, n. dj., str. 46.

djelatnosti u Republici Hrvatskoj donesen još davne 1977. kao republički zakon u sklopu bivše federativne države,[8] uvođenje informacijskih tehnologija u poslovanje u Republici Hrvatskoj, osobito u segmentu javne uprave, u proteklih dvadesetak godina nije bila sustavna, već sporadična pojava.

Reguliranje elektroničke trgovine i s njom povezanih tehnologija i postupaka ozbiljnije je ušlo u fokus hrvatskoga zakonodavca tek početkom novoga tisućljeća, tj. desetak godina kasnije nego na Zapadu. U vrijeme kad su doneseni zakoni poput Zakona o elektroničkoj trgovini (NN 173/03, 67/08, 36/09, 130/11, 30/14), Zakona o elektroničkom potpisu (NN 10/02, 80/08, 30/14), Zakona o elektroničkoj ispravi (NN 150/05), Zakona o elektroničkim medijima (NN 153/09, 84/11, 94/13, 136/13) i Zakona o elektroničkoj komunikaciji (NN 73/08, 90/11, 133/12, 80/13) dolazi do promjene u stavu zakonodavca prema utjecaju informacijske tehnologije na društvo i osvještavanja potrebe da se on odgovarajuće regulira, a sve pod utjecajem relevantne zakonodavne prakse u susjednim, teorijski i sustavno bliskim zakonodavstvima u postupku preuzimanja europske pravne stečevine.

Od svih pravnih pitanja i nedoumica koja prate pojavu elektroničke trgovine, osobito se ističe ono o regulaciji elektroničkoga potpisa. Bez elektroničkoga potpisa, već je istaknuto, nema zadovoljavajuće razine pravne sigurnosti prilikom sklapanja pravnih poslova u elektroničkom obliku[9].

Kad je riječ o elektroničkom potpisu, valja istaknuti kako on podrazumijeva i upotrebu elektroničkoga certifikata. Moglo bi se reći da elektronički potpis u širem smislu obuhvaća i elektronički potpis u užem smislu, kao metodu zaštite sadržaja elektroničkoga dokumenta ili elektroničke komunikacije, i elektronički certifikat, kojega je uloga pouzdano potvrditi identitet neke pravne ili fizičke osobe.[10]

Prije analize hrvatskoga i poredbenoga pravnog okvira regulacije instituta elektroničkoga potpisa treba istaknuti nekoliko zahtjeva koji se stavljaju pred zakonodavca i tijela državne uprave kako bi elektronički potpis zaživio.

Osnovni je zahtjev (1) pitanje potvrđivanja izvornosti, odnosno autentičnosti potpisnika i sadržaja potpisane komunikacije. Zatim (2) elektronički potpis treba biti jednostavan za upotrebu, kako za korisnike, tako i za tijela koja garantiraju njegovu autentičnost.

Radi promicanja upotrebe elektroničkoga potpisa u komunikaciji tijela državne uprave, ali i radi više razine pravne sigurnosti potrebno je, osim komercijalnih pružatelja usluge certificiranja (3), odrediti i tijelo državne uprave koje će voditi bazu podataka s registriranim elektroničkim potpisima tijela državne uprave.

---

[8] Zakon o informatičkoj djelatnosti. *NN* 49/1977.

[9] Nikšić, S. Elektronički potpis u skladu sa smjernicom 1999/93/EC. *Pravo u gospodarstvu* (Zagreb). 39, 5(2000), str. 258.

[10] Dragičević, n. dj., str. 87. i 88.

Posljednji je uvjet kvalitetnog usvajanja elektroničkoga potpisa u svakidašnji život (4) normativno izjednačavanje vrijednosti elektroničkoga i vlastoručnog potpisa. Bez toga koraka elektronički potpis i elektronička komunikacija neće adekvatno pridonijeti automatizaciji i ubrzavanju poslovnih procesa među tijelima državne uprave, gospodarstva i prema građanima Republike Hrvatske.

2.1. Zakon o elektroničkom potpisu

Hrvatski Zakon o elektroničkom potpisu (2002) nastao je kao implementacija europske Direktive o elektroničkom potpisu (1999/93/EC)[11], koja je nakon četverogodišnje zakonodavne procedure usvojena 1999. i predstavlja prekretnicu u razvoju pravnih standarda regulacije elektroničkoga potpisa. Zemlje članice EU-a u razdoblju nakon usvajanja Direktive relativno su brzo implementirale njezine odredbe u nacionalna zakonodavstva, a to je u postupku pristupa EU-u učinila i Republika Hrvatska.

Kronološki, među prvima je to učinila Njemačka.[12] Njemački se zakonodavac brzo priklonio sustavu dvaju kolosijeka, pa je već 2001. na snagu stupio *Gesetz über Rahmenbedingungen für elektronische Signaturen*, koji je u njemačko pravo unio definiciju elektroničkoga potpisa i naprednoga elektroničkog potpisa sukladno odredbama Direktive o elektroničkom potpisu. Slijedile su implementacije u Sloveniji *(Zakon o elektronskem poslovanju in elektronskem podpisu*, 2000), Češkoj *(Zákon o elektronickém podpisu)*, Slovačkoj *(Zakon o elektronickom podpise)*, Francuskoj *(Décr. No. 2002-535 18. Avr. 2002, relatif à l'évauation et à la certification de la sécurite offerte par les produits et les systémes des technologies de l'information)*, Poljskoj *(Ustawa o podpisie elektronicznym)* i drugim nacionalnim zakonodavstvima.

2.2. O Zakonu o elektroničkoj ispravi

Među zakonima koji uređuju područje elektroničke trgovine i elektroničkih komunikacija potrebno je posebno se osvrnuti na Zakon o elektroničkoj ispravi iz 2005.

Zakon uređuje upotrebu i promet elektroničkih isprava u Republici Hrvatskoj te pobliže uređuje postupke vezane za izradbu, promet, uporabu, pohranu i čuvanje informacijskih sadržaja ugrađenih u elektroničke isprave uz primjenu informacijske i komunikacijske opreme.

Kao razlog donošenja Zakona hrvatski je zakonodavac naveo *»proces stvaranja pravnog okruženja neophodnog za uspješno stvaranje, djelovanje i razvoj infor-*

[11] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML (07. 04. 2014).

[12] Njemačka je prvi zakon koji regulira elektronički potpis usvojila dvije godine prije europske Direktive (*Signaturgesetz*, 1997).

macijskog društva«.[13] Predlagatelj navodi da se Zakon predlaže unatoč tomu što je *»pri izradi teksta Konačnog prijedloga Zakona o elektroničkoj ispravi izvršen ... uvid u postojeća zakonodavstva u zemljama Europske unije, pri čemu je utvrđeno da nema pravne stečevine u ovom području«.*[14] U trenutku donošenja Zakona o elektroničkoj ispravi regulacija pojma »elektroničkoga dokumenta« nije, kao ni danas, široko raširen pravni standard[15]. Unatoč proklamiranoj nakani predlagača,[16] Zakon nije imao očekivan učinak. Uzrok tomu prepoznaje Blythe, koji za sve zakone koji se odnose na elektroničke dokumente sumarno navodi da pate od pretjeranoga broja iznimaka od primjene.[17]

3. Okviri korištenja infrastrukture javnoga ključa u elektroničkom poslovanju s obzirom na hrvatske zakone

3.1. Elementi infrastrukture javnoga ključa i njihova svojstva

Radi boljega razumijevanja analizirane zakonodavne problematike, ali i uvida u složenost problematike dugoročnoga očuvanja arhivskoga gradiva koje sadržava digitalne potpise, potrebno je pojasniti osnovne pojmove infrastrukture javnoga ključa (engl. *Public Key Infrastructure – PKI*) i njihova svojstva, formate realizacije, način djelovanja te pravne činjenice koje se iz njihove pravilne primjene mogu zaključiti ili dokazati. Stoga su u nastavku opisani pojmovi (1) infrastruktura javnoga ključa, (2) digitalni certifikat, (3) kvalificirani certifikat, (4) certifikacijska služba, (5) registracijski autoritet, (6) neporecivost, (7) pouzdana arhivska služba, (8) vremenski žig, (9) pouzdani vremenski žig, (10) elektronički potpis, (11) napredni elektronički potpis te (12) PDF/A.

3.1.1. Infrastruktura javnoga ključa

Infrastruktura javnoga ključa (PKI) predstavlja složenu informacijsku infrastrukturu koja služi za upravljanje elektroničkim identitetima. Temelj rada PKI

---

[13] V. Konačni prijedlog Zakona o elektroničkoj ispravi, studeni 2005. URL: http://hidra.srce.hr/arhiva/8/5508/www.sabor.hr/Download/2005/11/28/PZ_344.pdf (07. 04. 2014).

[14] Ibid., str. 11.

[15] U poredbenoj zakonodavnoj praksi zakona analognih Zakonu o elektroničkoj ispravi ima tek nekoliko. U Kanadi je 2000. usvojen *Personal Information Protection and Electronic Documents Act*. U Kazahstanu je 2003. usvojen Zakon o elektroničkoj ispravi i digitalnom potpisu (Law of the Republic of Kazakhstan on Electronic Document and Digital Signature).

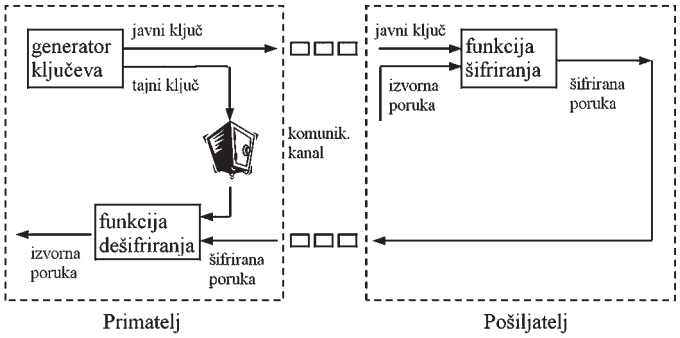
[16] »Predloženim se Zakonom želi stvoriti povjerenje najšire javnosti u uporabu i razmjenu elektroničkih isprava kroz otvorene telekomunikacijske sustave. Istodobno, ovim se Zakonom želi stvoriti prostor za intenzivnije djelovanje sustava elektroničkog poslovanja koji sve više postaju imperativ postizanja konkurentnosti na svjetskim tržištima. Predloženim Zakonom želi se također, promovirati i osigurati nesmetan i brz tehnološki razvoj elektroničkog poslovanja uporabom i razmjenom elektroničkih isprava koje se pravno izjednačavaju s klasičnim ispravama na papiru.«, Konačni prijedlog Zakona o elektroničkoj ispravi, n. dj.

[17] Bylthe, Stephen E. Croatia's computer laws: promotion of growth in E-commerce via greater cybersecurity. *European Journal of Law and Economics*. 26(2008), str. 99.

jest uporaba asimetrične kriptografije. Asimetrična kriptografija zapravo počiva na paru matematički povezanih ključeva, od kojih se jedan naziva javni ključ, a drugi privatni ključ, a generirani su kako bi se koristili zajedno.[18] Privatni je ključ tajan i koristi ga samo vlasnik, dok je javni ključ dostupan svima koji ga žele.[19] Svatko tko ima javni ključ može kriptirati poruku, ali samo osoba koja ima tajni ključ može je dekriptirati (Slika 1.[20]).

Suprotno tomu, osoba može digitalno potpisati poruku svojim tajnim ključem, a svatko potom može prije objavljenim javnim ključem provjeriti je li ta osoba potpisala dokument. Pritom se, dodatno, javlja problem provjere stoji li doista ta fizička osoba iza digitalnoga potpisa. Taj se problem rješava uspostavom kombinacije digitalnih certifikata i certifikacijske službe, o čemu će biti riječi nešto poslije.

Izračunavanje vrijednosti privatnoga na osnovi vrijednosti javnoga ključa preko faktorizacije, tj. upotrebom grube sile (engl. *brute force*) – načinom koji isprobava sve moguće kombinacije dok ne pogodi pravu – danas je gotovo nemoguće. Naravno, algoritmi su poznati, ali većina njih uz današnji stupanj razvoja računalne i procesorske snage nije dovoljno brza, pa su za faktorizaciju broja koji, primjerice, sadržava 200 znamenki potrebne dekade.[21] Iz navedenoga razloga PKI enkripcija drži se vrlo sigurnom, jer današnje duljine ključeva dosežu 2048 znakova. Zbog raširene uporabe PKI se sastoji od niza elemenata koji zapravo čine samu infrastrukturu. Međutim, za potrebe ovoga članka u nastavku se obrađuju pojmovi, odnosno elementi koji su nužni za dugotrajnu pohranu.



Slika 1. Postupak šifriranja i dešifriranja upotrebom javnoga i tajnoga ključa

[18] Jacobs, J., Clemmer, L., Dalton, M., Rogers, R., Posluns, J. *SSCP Study Guide*. Syngress Publishing, 2003., str. 330–331.
[19] Ibid.
[20] Stančić, H. *Upravljanje znanjem i globalna informacijska infrastruktura.* Magistarski rad, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb, 2001, str. 48.
[21] *PKI – Public and Private key pairs*. URL: http://queirozf.com/posts/pki-public-and-private-key-pairs (14. 04. 2014).

3.1.2. Digitalni certifikat

Digitalni certifikat (engl. *digital certificate*) predstavlja elektronički zapis koji služi za potvrdnu identifikaciju entiteta (npr. osobe, organizacije, uređaja) koji egzistiraju u elektroničkom, odnosno digitalno-računalnom svijetu. Općenito, certifikat javnoga ključa veže javni ključ entiteta sa setom informacija koje identificiraju entitet, odnosno povezuje odgovarajući privatni ključ entiteta.[22] Na ovaj način vidljiva je jasna povezanost između privatnoga i javnoga ključa. Najrašireniji format digitalnih certifikata jest x.509 v3, koji je vrlo složen, ali i standardiziran, pa je mogućnost pogreške implementacije smanjena uporabom standarda.[23] Svaki digitalni certifikat ima svoj sadržaj:[24]

1. informacije kojima se identificira korisnik ili organizacija, općenito entitet koji posjeduje certifikat,
2. javni ključ korisnika,
3. vremensko razdoblje valjanosti certifikata,
4. informacije o organizaciji koja izdaje certifikat,
5. digitalni potpis koji potvrđuje identitet organizacije koja je izdala certifikat,
6. digitalni zapis koji potvrđuje da je određeni entitet vlasnik određenoga javnog ključa,
7. javni zapis koji entitet distribuira zainteresiranim stranama kako bi se mogao provjeriti identitet entiteta.

3.1.3. Kvalificirani certifikat

Europska komisija rabi pojam kvalificiranoga certifikata (engl. *qualified certificate*) za opis određene vrste digitalnoga certifikata koji je relevantan za europsko zakonodavstvo.[25] Tako dokument Qualified Certificates Profile[26] pruža specifikaciju izdavanja kvalificiranoga certifikata koja jamči pouzdanu identifikaciju osobe kao entiteta pri uporabi javnih usluga unutar kojih se poštuje načelo neporecivosti.

---

[22] Chokhani, S. et al. *Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework*. Network Working Group, The Internet Society. 2003. URL: http://www.ietf.org/rfc/rfc3647.txt (14. 04. 2014).

[23] Ferguson, N., Schneier, B., Kohno, T. *Criptography Engineering: Deisign Principles and Practical Applicarion*, Wiley Publishing, 2010., str. 279.

[24] *E-potpis*. materijal predmeta Sigurnost elektroničkog poslovanja, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu. URL: http://www.fer.unizg.hr/_download/repository/7_sigurnost_potpis.pdf (14. 04. 2014).

[25] Santesson, S. et al. *Internet X.509 Public Key Infrastructure. Qualified Certificates Profile*. Network Working Group, The Internet Society. 2001. URL: http://www.ietf.org/rfc/rfc3039.txt (14. 04. 2014).

[26] Ibid.

Europska legislativa, konkretno Directive 1999/93/EC, propisuje da unutar kvalificiranoga certifikata moraju biti sadržane sljedeće informacije:[27]

(a) podatak da se certifikat izdaje kao kvalificirani certifikat,

(b) podatak o identifikaciji certifikacijske službe (izdavatelja) i državi u kojoj je uspostavljen,

(c) podatak o nazivu (imenu ili pseudonimu) potpisnika,

(d) podatak o specifičnom atributu potpisnika koji se po potrebi može dodati, ovisno o namjeni kvalificiranoga certifikata,

(e) podatci za provjeru potpisa koji odgovaraju podatcima o potpisivanju koji su pod nadzorom potpisnika,

(f) podatak o početku i kraju valjanosti certifikata,

(g) identifikacijski kôd certifikata,

(h) napredni elektronički potpis certifikacijske službe koja izdaje kvalificirani certifikat,

(i) ograničenja za uporabu certifikata, ako postoje,

(j) limit vrijednosti transakcija za koje se certifikat može rabiti, ako postoji.

Kvalificirani certifikat izdaje certifikacijska služba koja mora udovoljiti ovim specifičnim zahtjevima definiranima unutar EU Direktive. U Republici Hrvatskoj kvalificirani certifikat definiran je Zakonom o elektroničkom potpisu.

3.1.4. Certifikacijska služba

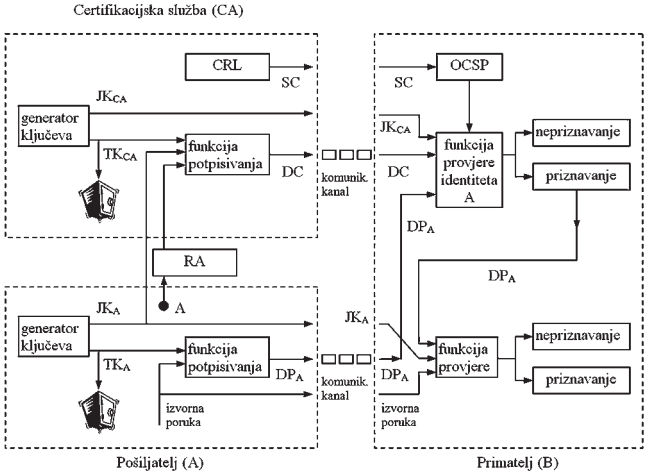
U PKI infrastrukturi digitalne certifikate izdaje i opoziva certifikacijska služba (engl. *certification authority – CA*) koja je mjerodavna za ovjeru identiteta. Certifikacijska služba organizirana je kao hijerarhija unutar koje se korijenski CA (engl. *Root CA*) rabi kao najviši entitet koji zapravo vjeruje sam sebi[28] te kojem se vjeruje, dok svi hijerarhijski niži entiteti vjeruju vršnomu CA. Ideja ovakve organizacije jest da svaki identificirani entitet dobije elektronički zapis, odnosno ovjeru svoga javnog ključa, čime se zapravo potvrđuje njegov identitet. To se provodi na način da CA svojim privatnim ključem potpisuje digitalni certifikat određenog entiteta i kojega se identitet može provjeriti javnim ključem CA. Bitno je napomenuti da CA provjerava s registracijskim autoritetom (RA) informacije o identitetu, što mu ih pruža entitet koji traži ovjeru, a ukoliko RA potvrdi vjerodostojnost informacija o entitetu, tad CA izdaje digitalni certifikat.[29] Uz izdavanje važećih cer-

[27] Directive 1999/93/EC, n. dj., str. 12.

[28] Iz sigurnosnih razloga pristup vršnomu CA imaju isključivo ovlaštene osobe, te se poslužitelju koji se koristi kao korijenski CA pristupa isključivo fizički, tj. ne preko mreže, a u najvećem broju slučajeva korijenski CA zapravo je ugašen.

[29] Certificate Authority (CA), *Search Security*. 2007. URL: http://searchsecurity.techtarget.com/definition/certificate-authority (14. 04. 2014).

tifikata, CA održava informacije o stanju digitalnih certifikata i objavi nevažećih certifikata preko tzv. liste opozvanih certifikata (engl. *Certificate Revocation List – CRL*).[30] Osim provjere valjanosti certifikata preko CRL-a, u PKI infrastrukturi koristi se i protokol za online provjeru certifikata (engl. *Online Certificate Status Protocol – OCSP*). OCSP omogućuje aplikacijama, odnosno klijentima određivanje statusa opoziva identificiranih, tj. korištenih certifikata.[31] OCSP klijent, dakle, izrađuje zahtjev za statusom certifikata za koji se traži provjera te ga upućuje OCSP poslužitelju. Ujedno OCSP klijent onemogućuje potvrđivanje certifikata sve dok ne dobije pozitivan odgovor od OCSP poslužitelja (Slika 2).[32]



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

Slika 2. Postupak rada certifikacijske službe prilikom provjere digitalno potpisane poruke i digitalnoga certifikata

U Republici Hrvatskoj FINA[33] je zasad jedini CA koji održava registar digitalnih certifikata i koji ima dozvolu Ministarstva gospodarstva. Prvi pravilnik o administriranju korisnika i certifikata FINA-PKI, kao i certifikacijska politika

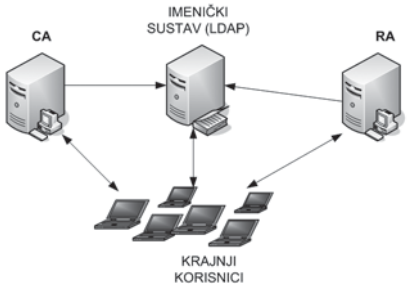
[30] Lista opozvanih certifikata jedan je od najvažnijih mehanizama PKI-a jer se preko njega provjerava valjanost certifikata. CRL je potpisan privatnim ključem CA, pa je samim time krivotvorenje CRL-a gotovo nemoguće. *What is a CRL?* PKI 101. URL: http://www.pki101.com/CRLWhat.html (14. 04. 2014).
[31] Myers, M. et al. *X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP*. Network Working Group, The Internet Society. 1999. URL: http://www.ietf.org/rfc/rfc2560.txt (14. 04. 2014).
[32] Prilagođeno prema: Stančić, H. *Upravljanje znanjem*, n. dj., str. 51.
[33] *FINA RDC (Registar Digitalnih Certifikata)*. URL: http://rdc.fina.hr/ (14. 04. 2014).

(engl. *certification policy*) FINA-PKI izrađeni su uz nadzor Ministarstva gospodarstva. Konačno, Europska je komisija 17. travnja 2014. objavila pouzdanu listu certifikacijskih službi koje izdaju kvalificirane certifikate[34] na kojoj se nalazi i certifikat FINA-e, pa se od toga datuma FINA može držati pouzdanim i priznatim izdavateljem.

3.1.5. Registracijski autoritet

Registracijski autoritet (engl. *Registration Authority – RA*) u PKI-u predstavlja autoritet koji provjerava zahtjeve entiteta za izdavanjem digitalnih certifikata i potvrđuje CA valjanost zahtjeva, odnosno pruža informaciju CA da bi CA mogao izdati digitalni certifikat.[35] Može se reći da RA provjerava sadržaj certifikata za CA, obavlja (fizičku) identifikaciju samih entiteta te autentifikaciju entiteta koji se prijavljuje za dobivanje digitalnih certifikata.[36] RA ujedno provodi određene administrativne i slične zadatke u korist CA, te mora provesti sve procedure pri ispitivanju zahtjeva za izdavanjem digitalnoga certifikata, kao i ime, podatke, javni ključ te proširenje certifikata.[37]

Imenički sustav (repozitorij) distribuira certifikate i liste opozvanih certifikata u realnom vremenu. Najčešće upotrebljavana usluga repozitorija je LDAP[38] (engl. *Lightweight Directory Access Protocol*) poslužitelj. CA objavljuje certifikate u repozitorij, a korisnici ih dohvaćaju uz pomoć LDAP-temeljene klijentske aplikacije (Slika 3).



Slika 3. Uloga imeničkoga sustava u provjeri digitalnih certifikata

[34] *List of Trusted List information as notified by Member States*. European Commission. 17. 04. 2014., str. 71–74, URL: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1788 (19. 04. 2014).
[35] Registration Authority (RA). *Search Security*. 2006. URL: http://searchsecurity.techtarget.com/definition/registration-authority (14. 04. 2014).
[36] Vojković, G. *Elektronički potpis*, n. dj.
[37] *Nedostaci PKI infrastrukture*. CARNet. Rev. 1. 03. 2009., str. 13. URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-02-255.pdf (14. 04. 2014).
[38] Zeilenga, K. (ur.). *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.* Network Working Group, The Internet Society. 2006. URL: https://tools.ietf.org/html/rfc4510 (14. 04. 2014).

3.1.6. Neporecivost

Neporecivost (engl. *non-repudiation*) svojstvo je elektroničkoga zapisa koje sprečava entitetu mogućnost poricanja njegova sadržaja, provedbe neke akcije ili preuzimanja nekih odgovornosti. Drugim riječima, svojstvo neporecivosti sprečava opovrgavanje neke poduzete radnje u elektroničkoj okolini. Neporecivost se uglavnom povezuje s činom potpisivanja digitalnim potpisom. Neporecivost se u hrvatskom zakonodavstvu vezuje uz potpisivanje naprednim elektroničkim potpisom koji je zasnovan na kvalificiranom certifikatu. S obzirom na izneseno te na temelju prije opisanih komponenti PKI-a, da bi neki zapis očuvao svojstvo neporecivosti, neophodno je osigurati:[39]

1. digitalni identitet potpisnikâ,
2. opoziv prava potpisa u realnom vremenu,
3. vremensku ovjeru elektroničkoga potpisa nakon provjere liste opozvanih certifikata, čime se osigurava valjanost elektroničkoga potpisa u trenutku potpisivanja,
4. dugoročno i sigurno očuvanje arhiviranoga zapisa koji je digitalno potpisan te osiguranje mogućnosti provjere elektroničkoga potpisa.

3.1.7. Pouzdana arhivska služba

Pouzdana arhivska služba (engl. *Trusted Archive Service – TAS*) mora osigurati mogućnost provjere arhiviranoga, elektronički potpisanoga zapisa godinama nakon njegove pohrane u digitalni arhiv, iako se u tomu budućemu trenutku aplikacijsko rješenje kojim je izvedena ovjera vremena nastanka elektroničkoga zapisa možda više ne koristi ili je zastarjelo.[40] Zapravo, pouzdana arhivska služba mora osigurati održavanje aplikativnoga rješenja za uvid u arhiv, kao i aplikacije za provjeru elektroničkoga potpisa zajedno s pripadajućom platformom (hardver i operacijski sustav) ili najmanje emulaciju takvoga okruženja. Na taj se način osigurava mogućnost provjere autentičnosti elektroničkih zapisa, uvid u arhivirane elektroničke zapise te provjera pripadajućih elektroničkih potpisa kroz duže razdoblje. Naravno, suvremeni arhivi čuvaju različite oblike elektroničkoga gradiva u digitalnim arhivima, pa je potpuno jasno da složenost postupaka dugoročnog očuvanja raste s brojem različitih formata koje je potrebno očuvati, kao i računalno-programskih okruženja.

---

[39] Brzica, H., Herceg, B., Stančić, H. Long-term Preservation of Validity of Electronically Signed Records, u: Gilliland, A. et al. (ur.), *INFuture2013: Information Governance* (Zagreb). 4(2013), str. 150, URL: http://infoz.ffzg.hr/infuture/papers/4-03%20Brzica,%20Herceg,%20Stancic,%20LTP%20of%20Validity%20of%20Electronically%20Signed%20Records.pdf (18. 04. 2014).

[40] Dumortier, J., Eynde, S. Van den. *Electronic Signatures and Trusted Archival Services*. DAVID Project (2000–2003), str. 7, URL: http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (14. 04. 2014).

3.1.8. Vremenski žig

Vremenski žig (engl. *time stamp*) potvrda je Službe za izradu vremenskoga žiga (engl. *Time Stamping Authority – TSA*) kojom se potvrđuje da su podatci postojali u određenom trenutku.[41] Vremenski žig koristi se kao dodatak elektroničkomu potpisu, čime se potvrđuje da je potpis izrađen u određenom trenutku. Time je omogućena provjera nastanka elektroničkoga potpisa.

3.1.9. Pouzdani vremenski žig

Pouzdani vremenski žig (engl. *trusted digital time stamp*) osigurava mogućnost sigurnog određivanja trenutka potpisivanja nekoga zapisa, ali i praćenja njegovih eventualnih promjena do kojih je dolazilo tijekom vremena.[42] Koncept pouzdanoga vremenskog žiga bitan je zbog dokazivanja integriteta zapisa tijekom njegova čuvanja.

3.1.10. Elektronički potpis

Elektronički potpis (engl. *electronic signature*) predstavlja ekvivalent vlastoručnomu potpisu u elektroničkom obliku. On sadržava podatke u elektroničkom obliku koji su vezani za elektroničke dokumente (računi, uplatnice, ugovori i sl.) ili transakcije te služi kao sredstvo za potvrdu i provjeru autentičnosti. Elektronički potpis nikako nije slika vlastoručnoga potpisa. Da jest, tad bi to bio *digitalizirani*, a ne digitalni ili elektronički potpis. Dok se za klasični, vlastoručni potpis očekuje da on prilikom svakoga potpisivanja bude jednak, digitalni potpis kod svakoga potpisivanja predstavlja drugačiji niz znakova kako se taj niz ne bi mogao neovlašteno kopirati na neki drugi elektronički dokument. Digitalni potpis stoga rabi kriptografske transformacije podataka, tako da se primatelju podataka omogući dokazivanje podrijetla i integriteta tih podataka. Za uporabu elektroničkih potpisa potrebna je infrastruktura javnoga ključa. Osim karakteristika potpisa, elektronički potpis ima i mogućnost autentifikacije korisnika preko digitalnih certifikata, pametnih kartica ili biometrijskih metoda.

Pitanje elektroničkoga potpisa bilo je iznimno bitno za pravni okvir elektroničke trgovine, te je nakon četverogodišnjega zakonodavnog postupka u Europskoj uniji potkraj 1999. donesena Direktiva o elektroničkom potpisu 1999/93/EC.[43] Osnovni zadatak te direktive bio je stvoriti jedinstveni zakonodavni okvir za primjenu elektroničkoga potpisa na području zemalja članica EU-a. Na taj se način elektronički potpis može upotrebljavati u poslovanju preko elektroničkih komu-

[41] Wallace, C., Pordesch, U. and Brandner R. *Long-Term Archive Service Requirements*. IETF Trust. 2007., str. 5. URL: http://tools.ietf.org/html/rfc4810 (14. 04. 2014).
[42] Ćosić, J., Bača, M. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. *MIPRO – Proceedings of the 33rd International Convention*. 2010, str. 1227–1228, URL: http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (14. 04. 2014).
[43] Directive 1999/93/EC, n. dj.

nikacija s istom pravnom snagom kao i vlastoručni potpis učinjen na papiru. Direktiva razlikuje dva tipa elektroničkih potpisa – elektronički potpis (osnovni) i napredni elektronički potpis.

3.1.11. Napredni elektronički potpis

Elektronički potpis, prema EU Direktivi 1999/93/EC, mora zadovoljiti sljedeće zahtjeve kako bi postao napredni elektronički potpis (engl. *advanced electronic signature*):

a) jedinstveno je povezan s potpisnikom,

b) njime je moguće jedinstveno identificirati potpisnika,

c) stvoren je načinima koje potpisnik kontrolira i koji nisu dostupni drugima,

d) povezan je s podatcima koje potpisuje tako da se svaka naknadna izmjena može detektirati.

Osim elektroničkoga potpisa i naprednoga elektroničkog potpisa Direktiva 1999/93/EC uvodi i pojam kvalificiranoga digitalnog certifikata. Zbog svega ovoga Direktivu se može držati tehnološkim propisom jer jasno upućuje na izradbu (naprednoga) elektroničkog potpisa primjenjujući tehnologiju infrastrukture javnoga ključa.

Bitno je spomenuti i formulaciju navedenu u članku 5. Direktive. U njemu je navedeno da zemlje članice EU-a neće uskratiti elektroničkomu potpisu (u smislu osnovnoga, a ne naprednoga) mogućnost ostvarivanja pravnih učinaka i upotrebe kao dokaza u pravnim postupcima samo zato što:

1. je potpis dan u elektroničkom obliku,
2. potpis nije baziran na kvalificiranom certifikatu,
3. potpis nije baziran na kvalificiranom certifikatu koje je izdalo ovlašteno certifikacijsko tijelo,
4. potpis nije učinjen preko posebnog uređaja za stvaranje elektroničkoga potpisa.

Navedenim točkama 2.–4. nadopunjen je okvir za izradbu naprednoga elektroničkog potpisa.

3.1.12. PDF/A

PDF/A-1[44] ISO norma je temeljena na PDF (engl. *Portable Document Format*) referentnoj verziji 1.4. Razvila ju je kompanije Adobe Systems Inc., koja je implementirala navedenu verziju u alatu Adobe Acrobat 5. PDF/A-1 definiran je s ISO 19005-1:2005, kao ISO norma za dugotrajnu pohranu elektroničkih dokume-

[44] *ISO 19005-1:2005 – Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)*. URL: http://www.iso.org/iso/catalogue_detail?csnumber=38920 (14. 04. 2014).

nata. Ova je norma primjenjiva na dokumente koji sadržavaju kombinacije znakova, rastera i vektorskih podataka.

PDF/A-2[45] – ISO 19005-2:2011 definira uporabu PDF 1.7 formata, formaliziranoga kao ISO 32000-1[46], te služi za očuvanje statičkoga vizualnog prikaza elektroničkoga dokumenta tijekom vremena. PDF/A-2 omogućuje JPEG2000 kompresiju, transparentne elemente i PDF slojeve[47]. PDF/A-2 omogućuje i ugradnju OpenType fontova te podržava PAdES (engl. *PDF Advanced Electronic Signatures*) format naprednoga elektroničkog potpisa. Jedna posebno važna inovacija jest tzv. kontejnerska funkcija – PDF/A datoteke mogu biti ugrađene unutar PDF/A-2 dokumenta.

PDF/A-3[48] – ISO 19005-3:2012 definira upotrebu PDF 1.7 formata (formaliziranoga u ISO 32000-1) za statički vizualni prikaz elektroničkoga dokumenta tijekom vremena, s dodatkom da dokumenti bilo kojega tipa mogu biti ugrađeni (engl. *embedded*) u dokument ili dodani kao privitak (engl. *attached*).

Razine sukladnosti (engl. *conformance levels*) za PDF/A standarde jesu:[49] A (engl. *Accessible*), B (engl. *Basic*) i U (engl. *Unicode*). Različite razine sukladnosti odražavaju kvalitetu arhiviranih dokumenata te ovise o uključenim materijalima i o svrsi dokumenta:

- *Razina A* – ispunauje sve zahtjeve norme, uključujući i logičku strukturu dokumenta i njegov redoslijed ispravnoga čitanja. Tekst mora biti moguće izvući iz dokumenta, a logička struktura mora odgovarati prirodnomu redoslijedu čitanja. Korišteni fontovi moraju zadovoljiti stroge uvjete.
- *Razina B* – jamči da se sadržaj dokumenta može jednoznačno reproducirati. Dokumenti razine B lakše se izrađuju nego dokumenti razine A, ali razina B ne jamči 100%-tno vađenje teksta ili pretraživost. Dakle, ne znači nužno da se sadržaj može ponovno koristiti bez ikakvih problema. Skenirani papirnati dokumenti obično se mogu pretvoriti u PDF/A razine B bez dodatnoga rada.
- *Razina U* – uvedena je zajedno s PDF/A-2. Ova razina proširuje razinu B na način da se sav tekst može preslikati na standardne Unicode znakove.

---

[45] *ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)*. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50655 (14. 04. 2014).

[46] *ISO 32000-1:2008 – Document management – Portable document format – Part 1: PDF 1.7.* URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502 (14. 04. 2014).

[47] Oettler, A. *PDF/A in a Nutshell 2.0. PDF for long-term archiving*. Berlin : Association for Digital Document Standards e. V., 2013, str. 8, URL:
http://www.pdfa.org/wp-content/uploads/2013/04/PDFA_in_a_Nutshell_21.pdf (14. 04. 2014).

[48] *ISO 19005-3:2012 – Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)*. URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=57229 (14. 04. 2014).

[49] Oettler, *PDF/A in a Nutshell*, n. dj., str. 8.

PDF/A-1 definira dvije razine sukladnosti: PDF/A-1a i PDF/A-1b. PDF/A-2 definira tri razine sukladnosti: PDF/A-2a, PDF/A-2b i novu razinu PDF/A-2u.

4. Problematika rješavanja zakonodavnih ograničenja za širu primjenu elektroničkoga poslovanja u praksi

U ovom poglavlju bit će navedena tri slučaja ograničivanja šire primjene elektroničkoga poslovanja u praksi uvjetovana hrvatskim zakonima i pravilnicima. Prvi je slučaj Pravilnik o porezu na dodanu vrijednost, koji je jednim svojim dijelom onemogućivao širu primjenu elektroničkoga računa. Drugi slučaj odnosi se na procedure i politike za definiranje ovlaštenićkih prava za elektroničko potpisivanje, koje su svojim odredbama značajno otežavale dostupnost elektroničkih certifikata i njihovo korištenje. Navedeni su slučajevi u međuvremenu, srećom, riješeni na zadovoljavajući način, pa su time otklonjene prepreke za širenje elektroničkoga poslovanja.

Treći, još uvijek neriješen, slučaj vezan je uz definiranje pojma pravne osobe u Zakonu o elektroničkom potpisu. Definicija potpisnika kao fizičke osobe u hrvatskom zakonodavstvu onemogućuje bilo kakvu automatizaciju izrade neporecivoga elektroničkog potpisa, jer ga može izvesti isključivo fizička osoba. Takvim se pristupom onemogućuje elektroničko poslovanje s primjenom elektroničkoga potpisa u smislu izdavanja pravno valjanih dokumenata koji stvaraju pravne učinke. U ovom poglavlju predlažu se konkretne izmjene odgovarajuće regulative kojima bi se navedeno ograničenje uklonilo.

4.1. Pravilnik o porezu na dodanu vrijednost i elektronički račun

Sukladno članku 15. stavku 1. Zakona o porezu na dodanu vrijednost[50] i članku 104. stavku 1. Pravilnika o porezu na dodanu vrijednost[51] porezni obveznik mora ispostaviti račun za isporučena dobra ili obavljene usluge te na računu posebno iskazati porez na dodanu vrijednost. Račun može biti ispostavljen na papiru ili u elektroničkom obliku. Poduzetnik kupcu dostavlja račun te osigurava primjerak koji služi kao isprava za knjiženje.

Člankom 15. stavkom 3. Zakona o porezu na dodanu vrijednost propisano je koje podatke moraju sadržavati računi poreznih obveznika, a članak 104. Pravilnika o porezu na dodanu vrijednost propisuje što se sve drži računom u elektroničkom obliku (e-računom).

Međutim, sve do 29. srpnja 2011. kad je u Narodnim novinama 89/11 objavljen Pravilnik o izmjenama i dopunama Pravilnika o porezu na dodanu vrijednost[52] postojale su prepreke koje su onemogućivale široku primjenu elektroničkoga računa.

---

[50] *Narodne novine,* od broja 47/95 do 22/12, više ne vrijedi.
[51] *Narodne novine,* od broja 149/09 do 64/12, više ne vrijedi.
[52] *Narodne novine,* URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_07_89_1896.html (14. 04. 2014).

Do toga je datuma širenje ovoga područja elektroničkoga poslovanja onemogućivalo hrvatsko zakonodavstvo, tj. Pravilnik o porezu na dodanu vrijednost. U Pravilniku se izričito navodilo da se »računi poslani telekomunikacijskim uređajima ne smatraju računima u smislu odredbe članka 15, Zakona i članka 75. ovog pravilnika« te se tražilo izdavanje računa u dvama primjercima ispisanima na papiru. Na račun dobiven od telekomunikacija (npr. elektroničkom poštom) nije se mogao odbiti PDV, što je odbijalo gospodarstvenike (tvrtke i obrte) od slanja i primanja računa elektroničkim putem. Time se u Republici Hrvatskoj usporavalo širenje elektroničkoga poslovanja.

Iz toga je razloga 2008. osnovano, uz sudjelovanje Ministarstva gospodarstva, akademskih institucija i privatnoga sektora, Povjerenstvo za e-račun, koje je imalo dva odbora – tehnički i poslovni. Povjerenstvo je, među ostalim, aktivno radilo i na otklanjanju najveće prepreke za uvođenje e-računa, a to su sporne odredbe iz Pravilnika o porezu na dodanu vrijednost. Ta je prepreka uklonjena spomenutom izmjenom Pravilnika iz 2011.

Pravilnikom o izmjenama i dopunama Pravilnika o porezu na dodanu vrijednost donesene su sljedeće bitne promjene.

Članak u kojem su definirani detalji načina slanja računa **novi** je **članak 104.a:**

(1) Računom u elektroničkom obliku smatra se račun ispostavljen kao elektronička isprava sukladno Zakonu o elektroničkoj ispravi pod uvjetom da postoji suglasnost primatelja za prihvat takvog računa, smislu ovoga Pravilnika računom u elektroničkom obliku, ispostavljenim kao elektronička isprava, smatra se i račun potpisan elektroničkim potpisom sukladno Zakonu o elektroničkom potpisu.

(2) Računom iz stavka 1. ovoga članka smatra se i račun ispostavljen primjenom jedne od sljedećih metoda:

1. putem elektroničke razmjene podataka, ako ugovor o razmjeni omogućuje korištenje postupaka kojima je zajamčena vjerodostojnost podrijetla računa i cjelovitost podataka odnosno sadržaja računa,

2. pomoću bilo koje metode poslovne kontrole koja omogućuje povezivanje računa s isporukama dobara i usluga i drugim poslovnim dokumentima te provjeru vjerodostojnosti podrijetla i cjelovitosti sadržaja računa prema utvrđenim procesima izdavanja odnosno primanja računa.

Ministarstvo gospodarstva, nadalje, navodi odgovor na pitanje trebaju li svi računi u elektroničkom obliku, neovisno o metodi ispostavljanja biti potpisani: »Iz odredbi Zakona i Pravilnika proizlazi da potpis treba sadržavati račun ispostavljen metodom naprednog elektroničkog potpisa sukladno Zakonu o elektroničkom potpisu. Računi u elektroničkom obliku ispostavljeni putem elektroničke razmjene podataka (EDI)[53] ili bilo koje druge metode poslovne kontrole prema propisima

[53] *Electronic Data Interchange – EDI*, URL: http://en.wikipedia.org/wiki/Electronic_data_interchange (15. 04. 2014).

o PDV-u ne trebaju sadržavati potpis obzirom da potpis nije naveden kao obvezan sadržaj računa.«[54]

Što se tiče arhiviranja elektroničkoga računa Ministarstvo gospodarstva navodi da Zakonom i Pravilnikom mjesto čuvanja nije propisano kao obvezan element računa. Međutim, »člankom 159. Pravilnika propisano je da računi u elektroničkom obliku moraju biti pohranjeni u izvornom obliku u kojem su i poslani u skladu s posebnim propisima, da vjerodostojnost podrijetla i cjelovitost sadržaja pohranjenih računa moraju biti zajamčeni od trenutka izdavanja do kraja razdoblja čuvanja, a podaci koje sadrže računi ne smiju se mijenjati. Nadalje je propisano da porezni obveznik na zahtjev Porezne uprave ili drugog tijela nadležnog za nadzor mora omogućiti uvid u ispostavljene i primljene račune. ... Način arhiviranja i potencijalni programi nisu propisani odredbama Zakona i Pravilnika, već je bitno da način arhiviranja ispunjuje uvjete iz članka 159. Pravilnika.«[55]

Nove stavke dodane u članku 159. jesu:

(5) Računi iz stavka 2. ovoga članka u elektroničkom obliku moraju biti pohranjeni u izvornom elektroničkom obliku u kojemu su i poslani u skladu s posebnim propisima.

(6) Vjerodostojnost podrijetla i cjelovitost sadržaja pohranjenih računa, kao i njihova čitljivost, moraju biti zajamčeni od trenutka izdavanja do kraja razdoblja čuvanja iz članka 24. Zakona, a podaci koje sadrže ti računi ne smiju se mijenjati.

(7) Porezni obveznik na zahtjev Porezne uprave ili drugog tijela nadležnog za nadzor mora omogućiti uvid u ispostavljene i primljene račune.

Ministarstvo gospodarstva navodi i da se »računi izrađeni u PDF/A formatu smatraju računima u elektroničkom obliku ako metoda kojom su izdani ispunjava uvjete iz članka 104.a stavka 3. Pravilnika«[56].

Zanimljiv je odgovor Ministarstva na pitanje povezano s donošenjem internih odluka u svezi s poslovnim procesima izdavanja računa u elektroničkom obliku, odnosno o metodi koja se primjenjuje te procesu arhiviranja i upravljanja arhivskim podtacima: »Odredbom članka 104.a stavka 4. Pravilnika propisano je da je porezni obveznik koji namjerava ispostavljati i primati račune u elektroničkom obliku obvezan utvrditi način na koji će osigurati odgovarajuće uvjete propisane Zakonom o elektroničkoj ispravi i uvjete iz stavka 3. toga članka, kao i uvjete za elektroničku obradu podataka u skladu s Općim poreznim zakonom. Prema tome Pravilnikom nije izričito propisana obveza donošenja internih odluka, međutim mišljenja smo da su takve interne odluke od izuzetnog značaja prilikom obavljanja poreznog nadzora.«[57]

Ovim provedenim izmjenama konačno je omogućena šira primjena elektroničkoga računa.

---

[54] *Često postavljena pitanja i odgovori*. e-Poslovanje, Ministarstvo gospodarstva. URL: http://www.mingo.hr/default.aspx?id=3309 (15. 04. 2014).
[55] Ibid.
[56] Ibid.
[57] Ibid.

4.2. Ovlaštenička prava za elektroničko potpisivanje

Proces izdavanja elektroničkih certifikata u Republici Hrvatskoj podliježe propisanim politikama koje uključuju izradbu zahtjeva za izdavanje certifikata. Povijesno gledano, politikama i pratećim pravilnicima propisane su odredbe koje su znatno otežale dostupnost elektroničkih certifikata, čime se elektroničko poslovanje svelo na minimalnu upotrebu. Tako je Pravilnikom o administriranju korisnika i certifikata od 31. ožujka 2003., koji je izdao FINA-PKI, unutar točke 6.1. bila propisana odredba kojom je nužno da osoba ovlaštena za zastupanje potpisuje zahtjev za izdavanje certifikata (slika 4). Ovakva odredba znatno otežava proces izdavanja elektroničkih certifikata, jer se očekuje da predsjednik, član uprave ili direktor društva potpisuje svaki zahtjev za izdavanje certifikata.

6.1. Zahtjev za izdavanje certifikata

Zahtjev je pisani zahtjev tražitelja (poslovnog subjekta) i podnosi se na propisanom obrascu (nalazi se na WEB stranicama FINE na adresi: **http://demo-pki.fina.hr/** ... **ili http://rdc.fina.hr/** ... OBRASCI) u dva primjerka. Tražitelju se vraća jedan primjerak Zahtjeva s potvrdom datuma primitka. Poslovni subjekti i njihovi dijelovi podnose Zahtjev u podružnici FINE na čijem je području sjedište poslovnog subjekta ili dijela poslovnog subjekta. Specifikacija traženog certifikata je sastavni dio Zahtjeva. Zahtjev uz pečat potpisuje osoba ovlaštena za zastupanje i time potvrđuje istinitost podataka u Zahtjevu.

Slika 4. Zahtjev za izdavanje certifikata[58]

Istim je pravilnikom osoba ovlaštena za zastupanje definirana kao osoba koja je upisana u ovlašteni registar, koji bi u ovom slučaju bio isključivo sudski registar (slika 5). Dakle, ovakva formulacija omogućuje potpisivanje Zahtjeva za izdavanje certifikata samo osobama koje su kao osobe ovlaštene za zastupanje upisane u sudski registar.

6.1.2. Osoba ovlaštena za zastupanje

Na Zahtjev i specifikaciju traženih certifikata uz pečat potpisuje se osoba ovlaštena za zastupanje i time potvrđuje istinitost podataka u obrascu. Ako je rješenjem o upisu poslovnog subjekta u nadležni registar više osoba određeno za samostalno i pojedinačno zastupanje, specifikaciju traženih certifikata potpisuje osoba ovlaštena za takvo zastupanje. Ako je više osoba određeno za zajedničko zastupanje, Zahtjev i specifikaciju traženih certifikata potpisuje jedna od njih uz pisanu suglasnost ostalih ovlaštenika. Ako je više osoba određeno za zastupanje od kojih neke samostalno i pojedinačno, a druge zajednički, Zahtjev i specifikaciju traženih certifikata može potpisati:

- osoba određena za samostalno i pojedinačno zastupanje ili
- jedna od osoba određenih za zajedničko zastupanje uz pisanu suglasnost ostalih ovlaštenika.

Tekst pečata mora biti istovjetan tekstu naziva tražitelja upisanog u registar u punom ili skraćenom nazivu.

Zaposlenik FINE iz rješenja o upisu u registar odnosno drugog akta ako upis u registar nije propisan utvrđuje da li je osoba koja je uz pečat potpisala Zahtjev i specifikaciju traženih certifikata osoba ovlaštena za zastupanje.

Slika 5. Osoba ovlaštena za zastupanje[59]

Nadalje, ovakva formulacija odredbe Pravilnika zapravo onemogućuje korištenje odredbi Zakona o trgovačkim društvima koji poznaje Zastupnike po

[58] *Pravilnik o administriranju korisnika i certifikata*. FINA-PKI. 2003.
[59] Ibid.

punomoći te Punomoćenike po zaposlenju. Zastupnici po punomoći i Punomoćenici po zaposlenju definirani su Zakonom o trgovačkim društvima na sljedeći način:

Zastupnici po punomoći

Članak 42.

(1) Zastupnik trgovačkoga društva iz članka 41. ovoga Zakona može dati punomoć drugoj osobi.

(2) Punomoć se može dati u granicama ovlasti zastupnika koje su upisane u sudskom registru.

(3) Ako ovim Zakonom nije drugačije određeno, punomoć iz stavka 1. ovoga članka daje se sukladno odredbama propisa kojima se uređuju obvezni odnosi.

(4) Ograničenje iz članka 49. ovoga Zakona odnosi se i na punomoćnike iz ovoga članka.

Punomoćnik po zaposlenju

Članak 43.

(1) Osoba čija je dužnost da kao radnik trgovačkoga društva obavlja poslove koji po redovitom tijeku stvari uključuju i sklapanje određenih ugovora, odnosno poduzimanje određenih pravnih radnji, ovlaštena je da kao punomoćnik društva sklapa i te ugovore i poduzima te pravne radnje u granicama poslova koje obavlja.

Odredbom članka 19. Zakona o izmjenama i dopunama Zakona o trgovačkim društvima, NN 118/03, stupio na snagu 1. kolovoza 2003., izmijenjen stavak 1.

(2) Ograničenje iz članka 49. ovoga Zakona odnosi se i na punomoćnike po zaposlenju.

Punomoć je definirana Zakonom o obveznim odnosima[60] (NN 35/05, 41/08, 125/11). Konkretna forma punomoći nije propisana – punomoć treba slijediti oblik propisan zakonom za pravni posao radi kojega se daje.[61] Ovakav pristup mogao bi se tumačiti kao davanje punomoći u određenoj formi s pečatom i potpisom društva, odnosno osobe ovlaštene za zastupanje. Ujedno bi se tako moglo opunomoćiti zaposlenika za potpisivanje Zahtjeva za izdavanje certifikata.

FINA-PKI je 31. listopada 2013. objavio dokument pod nazivom »Opća pravila davanja usluga certificiranja«, a pravila se primjenjuju od 7. studenoga 2013. Izdavanjem navedenog dokumenta dolazi do bitnije liberalizacije postupka predaje zahtjeva za izdavanje certifikata. Već u samoj definiciji osobe ovlaštene za zastupanje dolazi do zaokreta u pravnom tumačenju pojmova, čime se definicija na

[60] Čl. 313. st. 1 ZOO: »Punomoć je ovlaštenje za zastupanje što ga opunomoćitelj pravnim poslom daje opunomoćeniku.«
[61] Čl. 314. ZOO.

određeni način usklađuje s odredbama Zakona o trgovačkim društvima, koji poznaje ovlaštenika i punomoćenika (slika 6).

Osoba ovlaštena za zastupanje	Osoba koja vlastitim očitovanjem volje sklapa pravni posao ili poduzima neku drugu pravnu radnju za drugog (zastupnik). Ovlaštenje za zastupanje može se temeljiti na zakonu, statutu, društvenom ugovoru ili pravilima pravne osobe, aktu nadležnog državnog tijela ili na punomoći.

Slika 6. Definicija osobe ovlaštene za zastupanje unutar Općih pravila davanja usluga certificiranja[62]

Daljnje odredbe općih pravila davanja usluga certificiranja definiraju način provjere identiteta ovlaštenih osoba (slika 7).

3.2.5. Provjera identiteta ovlaštenih osoba

Službenik u RA mreži dužan je utvrditi je li osoba koja je uz pečat potpisala zahtjev ili ugovor osoba ovlaštena za zastupanje te utvrditi identitet osobe ovlaštene za zastupanje odnosno opunomoćenika poslovnog subjekta.

Utvrđivanje identiteta osobe ovlaštene za zastupanje provodi se provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta i identiteta navedene u točki 3.2.2. i usporedbom s podacima iz preslike prihvatljive i važeće identifikacijske isprave osobe ovlaštene za zastupanje. Vrste prihvatljivih identifikacijskih isprava navedene su u točki 3.2.3.1. ovih Općih pravila. Dodatno, vrši se upit na nacionalni OIB sustav i provjeravaju se svi podaci koje OIB sustav sadrži u odnosu na podatke iz preslike identifikacijske isprave.

Utvrđivanje identiteta opunomoćenika provodi se na jednak način kao i provjera identiteta osobe ovlaštene za zastupanje.

Slika 7. Provjera identiteta ovlaštenih osoba[63]

Kad se usporede odredbe Pravilnika o administriranju korisnika i certifikata s Općim pravilima davanja usluga certificiranja, može se zaključiti da je gotovo deset godina sazrijevala liberalizacija pristupačnosti elektroničkim certifikatima. Novim je odredbama izdavanje elektroničkih certifikata znatno olakšano, pa su navedenim pristupom stvoreni temelji za efikasnu svakidašnju primjenu elektroničkoga poslovanja.

4.3. Problematika definiranja pojma pravne osobe u Zakonu o elektroničkom potpisu

Direktive su jedan od najvažnijih instrumenata za harmonizaciju nacionalnih pravnih poredaka s pravom Europske unije.[64] Treba naglasiti da implementacija

[62] *Opća pravila davanja usluga certificiranja*. FINA-PKI. 2013.
[63] Ibid.
[64] Josipović, T. Izazovi harmonizacije građanskog prava putem direktiva. *Forum za građansko pravo za jugoistočnu Evropu*. Beograd : Jugoslovenski pregled, 2010., str. 291. URL: http://www.seelawschool.org/uploads/gtz2010-en-civil-law-forum-vol-1.pdf (19. 04. 2014).

direktivâ kao zakonodavnog instrumenta Europske unije u nacionalna zakonodavstva ne traži uvijek doslovnu implementaciju odredbi direktiva. Po svom djelovanju direktive mogu imati učinak maksimalne i minimalne harmonizacije.[65] Prema tomu kriteriju, a na temelju pojedinih uvodnih izjava Direktive[66], može se zaključiti da je Direktiva 1999/93/EC po svom učinku bliža tipu minimalne harmonizacije. Smisao je Direktive potaknuti usvajanje nacionalnoga pravnog okvira i priznanja elektroničkoga potpisa kao valjanoga načina autorizacije potpisnika i sadržaja pravnoga posla sklopljenoga elektroničkim putem.

Zakonom o elektroničkom potpisu (ZEP) definirana su pravila primjene neporecivoga elektroničkog potpisa, koji se u navedenom zakonu izvodi primjenom kvalificiranoga certifikata. Zakon se u svojim odredbama poziva na odredbe Direktive 1999/93/EC, unutar koje su raspisane opće smjernice te pojmovi povezani s kvalificiranim certifikat.

Međutim, komparativnom analizom utvrdili smo da postoji znatna razlika između Direktive 1999/93/EC i Zakona o elektroničkom potpisu Republike Hrvatske u dijelu s odredbama povezanima s kvalificiranim certifikatom. Osnovni pojam koji Direktiva poznaje jest »potpisnik« (engl. *signatory*). Hrvatsko zakonodavstvo taj pojam svodi na pojam fizičke osobe. Definicija potpisnika kao fizičke osobe u hrvatskom zakonodavstvu onemogućuje bilo kakvu automatizaciju izradbe neporecivoga elektroničkog potpisa, već s ga može izvesti isključivo fizička osoba[67].

Definicija potpisnika u ZEP-u se nalazi u čl. 2. točka 3: »Potpisnik – znači osobu koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koji djeluje u svoje ime ili u ime fizičke i pravne osobe koju predstavlja.« S druge strane definicija potpisnika u Direktivi koja se također nalazi u čl. 2. točka 3 kaže: *»Signatory« means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.*

Razmatrajući definiciju potpisnika s obzirom na odredbe koje se odnose na kvalificirani certifikat (Aneks I Direktive /v. poglavlje 3.1.3. ovoga rada/ i čl. 11 ZEP-a), osim nedosljednosti između točaka b, c i d Aneksa u odnosu na točke 2., 3. i 4. čl. 11., primjećuje se već spomenuta razlika gdje točka 3. čl. 11. kroz tražene podatke uvjetuje potpisnika kao fizičku osobu.

Zbog boljega razumijevanja i lakše usporedbe u nastavku su navedene definicije b, c i d kvalificiranoga certifikata iz Direktive EK 1999/93/EC u engleskom izvorniku, a kurzivom je naveden tekst točaka 2. i 3. iz čl. 11. Zakona o elektroničkom potpisu.

Qualified certificates must contain:

Kvalificirani certifikat ... mora sadržavati:

---

[65] Ibid., str. 294.

[66] Primjerice, uvodne izjave 4, 5, 6, 17 i 21 preambule Direktive.

[67] Čl. 11. točka 3 Zakona o elektroničkom potpisu.

(b) the identification of the certification-service-provider and the State in which it is established

–ne postoji u ZEP-u

(c) the name of the signatory or a pseudonym, which shall be identified as such

2. identifikacijski skup podataka o osobi koja izdaje certifikat (osobno ime; ime oca ili majke; nadimak, ako ga osoba ima; datum rođenja; prebivalište, odnosno boravište; naziv pravne osobe i sjedište, ako certifikat izdaje pravna osoba)

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended

3. identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako ga osoba ima, datum rođenja, prebivalište, odnosno boravište).

Postavlja se pitanje je li određenje potpisnika kao fizičke osobe stvarno bila intencija europskoga zakonodavca? Iz navedenoga se može sa sigurnošću zaključiti da nije. Stoga držimo da se ovakvim pristupom hrvatskoga zakonodavca praktički onemogućuje elektroničko poslovanje s primjenom elektroničkoga potpisa od pravnih osoba u smislu izdavanja pravno valjanih dokumenata koji stvaraju pravne učinke.

Prijedlozi poboljšanja zakonske regulative

Uzevši u obzir ograničenja u širenju elektroničkoga poslovanja spomenuta u svezi s pojmom pravne osobe, u nastavku predlažemo tekst zakonskih promjena. Promjene koje se predlažu odnose se na Zakon o elektroničkom potpisu, pročišćeni tekst Zakona NN 10/02, 80/08. U nastavku su navedeni ključni članci Zakona u obliku kako bi ih trebalo promijeniti.

Članak 11 ZEP-a u okviru odredbi koje se odnose na potpisnika kvalificiranoga certifikata (točka 3) treba izmijeniti tako da glasi (podcrtani dio treba dodati):

3. identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako ga osoba ima, datum rođenja, prebivalište, odnosno boravište ili naziv, sjedište i OIB pravne osobe ukoliko je riječ o pravnoj osobi kao potpisniku).

U postojeći članak 5. ZEP kao stavak 2. treba dodati:

Odredbe stavka 1. ovoga članka odnose se i na elektronički potpis zasnovan na kvalificiranom certifikatu kojem je potpisnik pravna osoba.

Iza članka 11. treba dodati članak 11.a, sadržaj kojega bi trebao glasiti:

Članak 11.a

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

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

1. izdavanje elektroničkih dokumenata iz područja opskrbnog lanca:

a. e-narudžbenica,

b. e-odgovor na narudžbu,

c. e-otpremnica,

d. e-primka,

e. e-povratnica,

f. e-račun,

g. e-odobrenje,

h. e-terećenje.

2. izdavanje potvrde fizičkim i pravnim osobama koje izdaju tijela državne uprave te lokalne i regionalne (područne) samouprave,

3. potvrde primitka upisa ili promjene podataka u registre tijela državne uprave te lokalne i regionalne (područne) samouprave,

4. ostale primjene definirane Pravilnikom o izradi elektroničkog potpisa.

5. Zaključak

Danas se s pravom može zaključiti da je upravo pitanje dugoročnoga očuvanja autentičnosti, pouzdanosti, integriteta i upotrebljivosti[68] arhiviranoga digitalnoga gradiva središnje pitanje suvremene arhivistike. Poznavanje problematike koja je istražena u ovom radu uvelike pomaže arhivistima koji su zaduženi za suvremeno, elektroničko gradivo da uspostave potrebne mehanizme u digitalnim arhivima. Kako vrijeme bude odmicalo, tako će se elektroničko gradivo u sve većem opsegu slijevati prema takvim arhivima. Elektroničko gradivo, zbog neprestanih promjena u računalno-programskoj okolini, vrlo brzo postaje nestabilno i već nakon pet do deset godina, ovisno o mediju na kojem se čuva te njegova dostupnost može biti ugrožena. Tada je potrebno takvo gradivo migrirati ili na medij nove generacije, ili u suvremeni format zapisa, ili oboje. Prilikom migracije, koja bi trebala biti planirana, može doći do situacija u kojima autentičnost, pouzdanost, integritet ili upotrebljivost može postati upitna, ili se, na primjer, autentičnost više ne može dokazati.

Ukoliko je pak riječ o elektroničkom gradivu koje je potpisano naprednim elektroničkim potpisom i uz koje se nalazi kvalificirani certifikat, tada dugoročno očuvanje autentičnosti takvoga gradiva ne ovisi više isključivo o arhivu u kojem je

[68] U skladu sa zahtjevima norme ISO 15489-1 – Information and documentation – Records management iz 2001. u točki 7.2. na stranici 7, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31908 (19. 04. 2014).

ono pohranjeno već i o ostaloj infrastrukturi koja služi kao potpora za dokazivanje autentičnosti takvih arhivskih zapisa. Drugim riječima, bi trebalo za primjerice pedeset godina biti moguće provjeriti autentičnost nekoga naprednog elektroničkog potpisa i kvalificiranoga certifikata jednako kao što je to moguće danas. Hoće li potrebna infrastruktura biti dostupna? Hoće li biti arhivirana lista opozvanih certifikata u trenutku kad je dokument bio potpisan kao oblik povijesne informacije kako bi se u kasnijem trenutku moglo utvrditi da se certifikat nije nalazio na njoj? Na ova, kao i na niz drugih sličnih tehnoloških pitanja suvremena postkustodijalna arhivistika mora pronaći odgovore.

Usklađivanje pravne regulative Republike Hrvatske s direktivama EU svakako pridonosi pojednostavljivanju svakidašnjih poslovnih aktivnosti. Stoga su u ovom radu predložene konkretne izmjene zakonske regulative koja uređuje elektroničko poslovanje radi operacionalizacije upotrebe elektroničkih potpisa i certifikata. Jednakopravna upotreba vlastoručnih i elektroničkih potpisa osnova je suvremenoga poslovanja. Zakonski okvir mora to omogućivati, jednako kao što dokumente i zapise s obje vrste potpisa sudska praksa ne smije pravno razlikovati u slučajevima sudskih sporova.

Sve ovdje navedeno, kako ono povezano s elektroničkim poslovanjem, pravnim okvirom i sudskom praksom tako i ono povezano s dugotrajnim očuvanjem elektroničkoga gradiva, podrazumijeva razumijevanje pojmova, svojstava i formata realizacije koji pripadaju području infrastrukture javnoga ključa. Drugim riječima, bez neprestanog osvježavanja osobnih znanja o struci i konceptima koji sve više utječu na nju, arhivisti neće moći adekvatno odgovoriti na izazove koje dugoročno očuvanje elektroničkoga gradiva pred njih postavlja. Jedino cjeloživotnim obrazovanjem, a ponekad i osobnim sudjelovanjem u znanstveno-istraživačkim projektima, moći će razvijati struku i graditi povjerenje korisnika da arhivske institucije znaju dugoročno očuvati elektroničko gradivo jednako kvalitetno kao i analogno te da to uspješno čine.

Buduća istraživanja

Autori planiraju buduća istraživanja usmjeriti k problematici povjerenja u elektronički potpisane digitalne zapise koji se dugoročno čuvaju u digitalnim arhivima. Težište tih istraživanja bit će stavljeno na zapise koji nastaju kao rezultat interakcije s e-servisima državne i javne uprave te koji bivaju pohranjeni u digitalnim arhivima i sličnim rješenjima pohrane u oblaku (engl. *cloud storage*). Pravna regulativa povezana sa zapisima koji nastaju korištenjem softvera u oblaku i koji se pohranjuju u oblaku još nije u potpunosti formulirana. S obzirom na to da su dva suautora ovoga rada, Hrvoje Brzica i Hrvoje Stančić, istraživači na međunarodnom znanstveno-istraživačkom projektu IntePARES Trust, kojega je cilj istraživanje slične problematike, buduća istraživanja bit će provedena u okviru šire međunarodne suradnje.

Informacija o projektu

Istraživanja u ovom članku rezultat su znanstveno-istraživačkoga rada na multinacionalnom znanstveno-istraživačkom projektu InterPARES Trust: Trust and Digital Records in an Increasingly Networked Society (http://www.interparestrust.org).

Literatura

Blažević, M. Nastavni materijali predmeta Sigurnost digitalnog identiteta i moguća rješenja autentifikacije, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, 2005., URL: http://web.zpr.fer.hr/ergonomija/2005/blazevic/ciljevi.htm (14. 04. 2014).

Bylthe, Stephen E. Croatia's computer laws: promotion of growth in E-commerce via greater cyber-security. *European Journal of Law and Economics*. 26(2008), str. 75–103.

Brzica, H., Herceg, B., Stančić, H. Long-term Preservation of Validity of Electronically Signed Records, u: Gilliland, A. et al. (ur.), *INFuture2013: Information Governance* (Zagreb). 4(2013), str. 147–158, URL: http://infoz.ffzg.hr/infuture/papers/4-03%20Brzica,%20Herceg,%20Stancic,%20LTP%20of%20Validity%20of%20Electronically%20Signed%20Records.pdf (18. 04. 2014).

Certificate Authority (CA), *Search Security*. 2007. URL: http://searchsecurity.techtarget.com/definition/certificate-authority (14. 04. 2014).

Chokhani, S. et al. *Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework*. Network Working Group, The Internet Society. 2003. URL: http://www.ietf.org/rfc/rfc3647.txt (14. 04. 2014).

Često postavljena pitanja i odgovori. e-Poslovanje, Ministarstvo gospodarstva. URL: http://www.mingo.hr/default.aspx?id=3309 (15. 04. 2014).

Ćosić, J., Bača, M. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. *MIPRO – Proceedings of the 33rd International Convention*. 2010, str. 1226–1230, URL: http://czb.foi.hr/upload/datoteke/10_400%281%29.pdf (14. 04. 2014).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML (07. 04. 2014).

Dragičević, D. *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb : Informatorov Biro Sustav, 2004.

Dumortier, J., Eynde, S. Van den. *Electronic Signatures and Trusted Archival Services*. DAVID Project (2000–2003). URL: http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (14. 04. 2014).

E-potpis. materijal predmeta Sigurnost elektroničkog poslovanja, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu. URL: http://www.fer.unizg.hr/_download/repository/7_sigurnost_potpis.pdf (14. 04. 2014).

Electronic Data Interchange – EDI, URL: http://en.wikipedia.org/wiki/Electronic_data_interchange (15. 04. 2014).

Ferguson, N., Schneier, B., Kohno, T. *Criptography Engineering: Deisign Principles and Practical Applicarion*, Wiley Publishing, 2010.

FINA RDC (Registar Digitalnih Certifikata). URL: http://rdc.fina.hr/

ISO 15489-1 – Information and documentation – Records management. 2001. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31908 (19. 04. 2014).

ISO 19005-1:2005 – Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1). URL: http://www.iso.org/iso/catalogue_detail?csnumber=38920 (14. 04. 2014).

ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2). URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50655 (14. 04. 2014).

ISO 19005-3:2012 – Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3). URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=57229 (14. 04. 2014).

ISO 32000-1:2008 – Document management – Portable document format – Part 1: PDF 1.7. URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502 (14. 04. 2014).

Jacobs, J., Clemmer, L., Dalton, M., Rogers, R., Posluns, J. *SSCP Study Guide*. Syngress Publishing, 2003.

Josipović, T. Izazovi harmonizacije građanskog prava putem direktiva. *Forum za građansko pravo za jugoistočnu Evropu*. Beograd : Jugoslovenski pregled, 2010., str. 291–306. URL: http://www.seelawschool.org/uploads/gtz2010-en-civil-law-forum-vol-1.pdf (19. 04. 2014).

List of Trusted List information as notified by Member States. European Commission. 17. 04. 2014., URL: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1788 (19. 04. 2014).

Matić, T. Elektronički potpis. *Odvjetnik* (Zagreb). 11–12(2010).

Matić, T. *Osnove prava elektroničke trgovine*. Zagreb : MEP Consult, 2008.

Myers, M. et al. *X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP*. Network Working Group, The Internet Society. 1999. URL: http://www.ietf.org/rfc/rfc2560.txt (14. 04. 2014).

Nedostaci PKI infrastrukture. CARNet. Rev. 1. 03. 2009. URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-02-255.pdf (14. 04. 2014).

Nikšić, S. Elektronički potpis u skladu sa smjernicom 1999/93/EC. *Pravo u gospodarstvu* (Zagreb). 39, 5(2000), str. 251–260.

Oettler, A. *PDF/A in a Nutshell 2.0. PDF for long-term archiving*. Berlin : Association for Digital Document Standards e. V., 2013. URL: http://www.pdfa.org/wp-content/uploads/2013/04/PDFA_in_a_Nutshell_21.pdf (14. 04. 2014).

Opća pravila davanja usluga certificiranja. FINA-PKI. 2013.

PKI – Public and Private key pairs. URL: http://queirozf.com/posts/pki-public-and-private-key-pairs (14. 04. 2014).

Pravilnik o administriranju korisnika i certifikata. FINA-PKI. 2003.

Registration Authority (RA). *Search Security*. 2006. URL: http://searchsecurity.techtarget.com/definition/registration-authority (14. 04. 2014).

Santesson, S. et al. *Internet X.509 Public Key Infrastructure. Qualified Certificates Profile*. Network Working Group, The Internet Society. 2001. URL: http://www.ietf.org/rfc/rfc3039.txt (14. 04. 2014).

Stančić, H. *Upravljanje znanjem i globalna informacijska infrastruktura.* Magistarski rad, Filozofski fakultet Sveučilišta u Zagrebu, Zagreb, 2001.

Vojković, G. Elektronički potpis. *Godišnjak 12 Hrvatskog društva za građanskopravne znanosti i praksu* (Zagreb). 2005, str. 463–469.

Wallace, C., Pordesch, U. and Brandner R. *Long-Term Archive Service Requirements*. IETF Trust. 2007. URL: http://tools.ietf.org/html/rfc4810 (14. 04. 2014).

What is a CRL? PKI 101. URL: http://www.pki101.com/CRLWhat.html (14. 04. 2014).

Zeilenga, K. (ur.). *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.* Network Working Group, The Internet Society. 2006. URL: https://tools.ietf.org/html/rfc4510 (14. 04. 2014).

Zakoni

Konačni prijedlog Zakona o elektroničkoj ispravi, studeni 2005. URL: http://hidra.srce.hr/arhiva/8/5508/www.sabor.hr/Download/2005/11/28/PZ_344.pdf (07. 04. 2014).

Zakon o elektroničkim medijima. NN 153/09, 84/11, 94/13, 136/13.

Zakon o elektroničkoj ispravi. NN 150/05.

Zakon o elektroničkoj komunikaciji. NN 73/08, 90/11, 133/12, 80/13.

Zakon o elektroničkoj trgovini. NN 173/03, 67/08, 36/09, 130/11, 30/14.

Zakon o elektroničkom potpisu. NN 10/02, 80/08, 30/14.

Zakon o informatičkoj djelatnosti. NN 49/1977.

Zakon o kaznenom postupku. NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13.

Zakon o obveznim odnosima. NN 35/05, 41/08, 125/11.

Zakon o općem upravnom postupku. NN 47/09.

Zakon o parničnom postupku. NN 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 123/08, 57/11, 148/11, 25/13.

Summary

ANALYSIS OF INFLUENCE OF CROATIAN LEGISLATION ON E-BUSINESS AND LONG-TERM PRESERVATION OF DIGITALLY SIGNED DOCUMENTS

The authors analyse Croatian legal framework covering e-business and compare it to the legal framework in the EU countries. Firstly, in order to better explain the problems that they detect in the Croatian legislation, the authors identify and explain the key elements in the public key infrastructure (PKI) concept which are relevant for e-Business. Therefore, the concepts of public key infrastructure, digital certificates, qualified certificates, certification authority, registration authority, non-repudiation, trusted archival service (TAS), time stamp, trusted digital time stamp, electronic signature, advanced electronic signature, and PDF/A are explained. Further, the authors analyse the existing constraints in Croatian legislation that make wider application and usage of e-Business rather complicate. By comparatively analysing the Croatian legislation and the "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" they identify the problematic segments of the existing legislation and suggest how they could be improved. Finally, considering the results of the research, the authors reflect on the role of archivists in the long-term preservation of digitally signed documents.

Keywords: *Croatian legislation, e-Business, electronic signature, digital certificate, long-term preservation of digital materials*