Digitalni potpis

Mario Zovkić, Tedo Vrbanec
Učiteljski fakultet Sveučilišta u Zagrebu, Odsjek u Čakovcu
Ulica dr. Ante Starčevića 55, Čakovec, Hrvatska
Telefon: (040) 37 00 00 Fax: (040) 37 00 25 E-mail: {mario.zovkic, tedo.vrbanec}@gmail.com

Sažetak - Rad daje kratki pregled digitalnog potpisa. Govori o PKI infrastrukturi i o zakonskom okviru koji omogućuje postojanje i pravovaljanost digitalnog potpisa. Ukratko se opisuju najvažniji algoritmi simetričnog i asimetričnog šifriranja te funkcije za izračunavanje sažetka poruke. Daje se kratki povijesni razvoj šifriranja i razvijanja kriptografskih algoritama.

I. UVOD

U poslovnom i ICT svijetu često susrećemo pojam digitalni potpis, elektronički potpis, ili engleski naziv *e-signature* koji bitno ubrzava i pojednostavnjuje poslovanje uz ogromnu uštedu vremena.

Da bismo ga mogli definirati uzet ćemo definiciju iz Hrvatskog enciklopedijskog rječnika koji nudi slijedeće: Digitalni potpis je [1] „šifriranje kojim se dokazuje autorstvo, tj. izvor elektroničkog dokumenta.“ Jednostavnije rečeno, digitalni potpis je digitalna verzija vlastoručnog potpisa, (a ne skenirana odnosno digitalizirana verzija analognog slikovnog predloška), koja uz odgovarajuće zakone vrijedi jednako kao i rukom (ili vlastoručno) potpisan dokument.

Svrha digitalnog potpisa je zaštita korisnika od mogućnosti da se netko u njegovo ime nezakonito koristi njegovim identitetom. Prednost digitalnog potpisa je u tome što kod transakcija koje iziskuju vlastoručne potpise dokumenta štedimo vrijeme i novac jer sve možemo napraviti putem Interneta.

Funkcija potpisa je dokazivanje autentičnosti neke osobe i dokumenta što se obavlja elektroničkim putem koristeći dva kriptografska ključa koji se nazivaju: javni ključ (engl. *public key*) i tajni ključ (engl. *private key*).

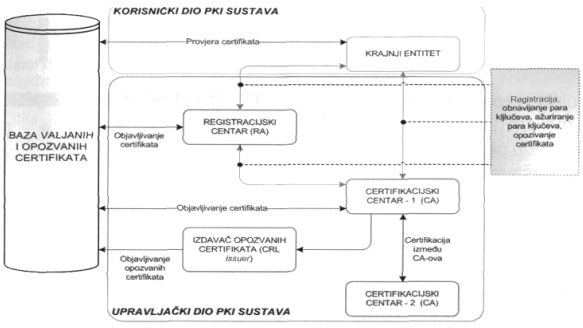
II. ŠIFRIRANJE

Pokušat ćemo jednostavnim jezikom objasniti šifriranje na ovom primjeru; uzmimo proizvoljne alfanumeričke podatke koje možemo pročitati i razumjeti bez posebnih metoda i načina, dakle one koje nazivamo običnim ili otvorenim tekstom (engl. *plain text*) ili (engl. *clear text*). Metoda skrivanja otvorenog teksta na način da se sakriju njegove sastavnice jest šifriranje. Šifrirajući običan tekst, dobivamo nečitljiv materijal kojeg zovemo šifrat. Proces pretvaranja šifrata natrag u originalni tekst naziva se dešifriranje. Znanost koja izučava metode šifriranja jest kriptografija koja se definira kao [2] „znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.“

III. NAČINI ŠIFRIRANJA

Općenito govoreći, danas su raširene tri vrste metoda šifriranja: metoda simetričnog šifriranja, metoda asimetričnog šifriranja i metoda potpisivanja jednosmjernom funkcijom. Prva je najstarija i koristi isti tajni ključ za šifriranje i dešifriranje. Algoritmi koji se pri tome koriste su simetrični, imaju prednost u brzini izvođenja i korisni su pri šifriranju podataka koji se ne prenose javnim medijem, već se koriste za, primjerice, sigurnu pohranu [3]. Kod simetrične kriptografije postoji problem razmjene tajnog ključa između učesnika u konverzaciji, jer postoji potencijalna opasnost od njegove krađe ako se koristi neki nesiguran mehanizam prijenosa poput e-pošte ili telefona. Svatko tko presretne ključ koji prolazi nesigurnim komunikacijskim kanalom može čitati, modificirati i krivotvoriti njime šifrirane informacije.

Asimetrični sustav uvodi javni ključ koji se koristi za šifriranje. Pošiljatelj poruke mora poznavati javni ključ primatelja koji se generira na temelju tajnog ključa tako da je nemoguće iz javnog ključa dobiti njegov tajni komplement. Provjera stvarne pripadnosti javnog ključa određenoj osobi omogućena je pomoću elektroničkih certifikata koje izdaje treća strana tako da ne bi došlo do lažnog predstavljanja. Infrastuktura sustava javnih ključeva je shematski i pojednostavljeno predstavljena slikom 1. Primatelj poruke posjeduje tajni ključ koji ne treba distribuirati ostalim korisnicima, odnosno pošiljateljima poruka, a pomoću kojeg samo on može dešifrirati poruku. [4]



Sl. 1. Shematski prikaz PKI sustava [5]

Asimetrični algoritmi imaju prednost zbog veće sigurnosti i tajnosti šifriranja, ali nedostaci su im potrebna količina vremena utrošena za svaki postupak dešifriranja te znatno povećanje šifrirane poruke u odnosu na njezin izvornik. Zbog tog povećanja veličine poruke, u praksi se tajnim ključem šifrira samo sažetak poruke.

Jednosmjerno šifriranje je metoda čije je glavno obilježje ireverzibilnost-iz jednom šifriranog podatka natrag se ne može dobiti originalni sadržaj. Pri tome se koriste jednosmjerne funkcije koje često nazivamo i (engl.) *hash* funkcije. Najčešće služe za potpisivanje sadržaja, tj. za provjeru vjerodostojnosti sadržaja i poruka, jer je vjerojatnost da se od dva različita (a primatelju smislena) sadržaja korištenjem kvalitetne funkcije dobije jednaki sažetak toliko mala da primatelj može biti gotovo potpuno siguran, (ali bez neke formalne garancije), da je primljena poruka istovjetna izvornoj. Pronalaženje takve smislene poruke jednakog sažetka iz gotovo beskonačnog skupa svih mogućih poruka ujedno je i izuzetno zahtjevna zadaća u računalnom smislu.

IV. KRIPTOGRAFSKI ALGORITMI I FUNKCIJE

Najviše korišteni simetrični algoritmi se dijele na algoritme koji šifriraju tokove podataka (poput STREAM CIPHER i RC4) i na algoritme koji šifriraju blokove podataka poput: AES, TRIPLE DES (3DES), RC2, IDEA i BLOWFISH. Asimetrični kriptografski algoritmi koriste dva odvojena ključa: javni i tajni. Najčešće korišteni su RSA i Diffie-Hellman, a u nastavku ćemo pobliže objasniti RSA algoritam. RSA je algoritam koji se može koristiti i za šifriranje informacijskog sadržaja i za autentifikaciju nastao 1977. godine. Zasniva se na primjeni dvaju ključeva - tajnog i javnog, čija dužina može biti između 40 i 2048 bita. Primjenjuje se u svim važnijim načinima ostvarivanja sigurne komunikacije putem Interneta kao što su SSL, S-HTTP, SET, S/MIME... Njegova sigurnost je zasnovana na teškoći faktorizacije velikih brojeva i postao je „de facto“ standard u asimetričnoj kriptografiji [5]. Svoj uspjeh RSA algoritam može uvelike zahvaliti Philipu Zimmermanu koji je 1991. godine razvio program *Pretty Good Privacy* u kome se algoritam koristi.

Hash funkciju matematički možemo definirati kao funkciju koja transformira proizvoljan broj elemenata ulazne domene u jedan element kodomene. Gledano s programerske strane, ona za poruku varijabilne duljine daje sažetak konstantne duljine, pa je prema tome, iz sažetka, nemoguće rekonstruirati polaznu informaciju ili bilo koji njezin dio. Algoritmi iz obitelji SHA grupe namijenjeni su za korištenje u aplikacijama za digitalno potpisivanje gdje postoji potreba potpisivanja velike datoteke na siguran način prije šifriranja privatnim ključem kriptosustava.

V. DIGITALNI POTPIS I ELEKTRONIČKO POTPISIVANJE DOKUMENATA

Bitno je razlučiti dva različita pojma. Elektronički i napredni elektronički potpis izrazi su neovisni od tehnologije i načina izvedbe te obuhvaćaju sve metode kojima se elektronička informacija može potpisati (od preslika vlastoručnog potpisa do digitalnog potpisa koji se temelji na asimetričnoj kriptografiji i funkcijama sažimanja). Digitalni potpis je ostvarenje elektroničkog potpisa temeljenog na asimetričnoj kriptografiji i funkcijama za izračunavanje sažetaka poruke koji pruža sigurnost u smislu nemogućnost krivotvorenja i ponovnog korištenja potpisa.

Ideju o korištenju parova javnih/privatnih ključeva za izradu elektroničkih potpisa predstavili su Whitfried Diffie i Martin Hellman 1976. godine, [6] iako je poznato kako je asimetričnu kriptografiju otkrio Clifford Cocks u sklopu Britanske tajne službe par godina ranije. [3]

Postoji više algoritama primjene javnog ključa za elektroničko potpisivanje. Korištenjem RSA (Rivest–Shamir-Adleman) algoritma moguće je istim algoritmom dokumente šifrirati i elektronički potpisivati dok DSA (engl. *Digital Signature Algorithm*) algoritam ima zasebne algoritme za šifriranje i elektroničko potpisivanje. Bez obzira koji algoritam utemeljen na kriptografiji javnog ključa odabrali, osnovni protokol razmjene elektronički potpisanih poruka između osobe A i osobe B teče otprilike ovako:

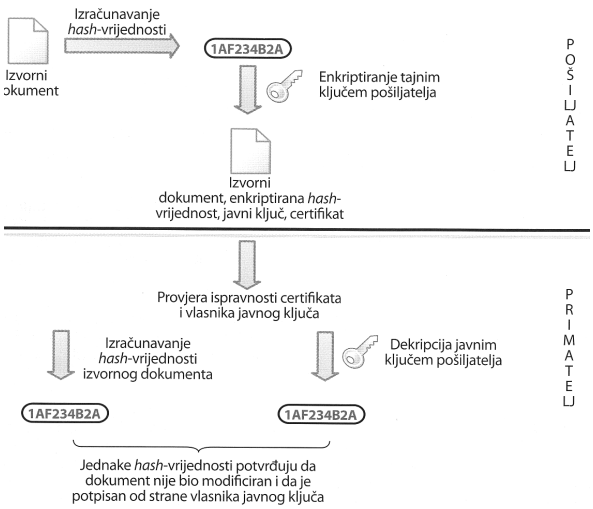
1. Osoba A šifrira poruku svojim privatnim ključem i tim činom potpisuje dokument.
2. Osoba A šalje potpisanu poruku osobi B.
3. Osoba B dešifrira primljenu poruku pomoću javnog ključa osobe A, čime provjerava vjerodostojnost potpisa osobe A.

Važno je naglasiti da ovaj protokol ne zahtijeva posrednika koji će provjeravati ispravnost potpisa i dodjeljivati tajne ključeve kao kod elektroničkog potpisivanja korištenjem simetrične kriptografije. Ispravnost potpisa osoba B provjerava prilikom dešifriranja poruke. Ukoliko dešifriranje pomoću javnog ključa osobe A nije moguće tada je poruka falsifikat. Posrednik, međutim, ne može biti u potpunosti izbjegnut; potreban je posvjedočiti kako je javni ključ osobe A uistinu javni ključ osobe A, tj. potreban je radi certifikacije javnog ključa pošiljatelja poruke.

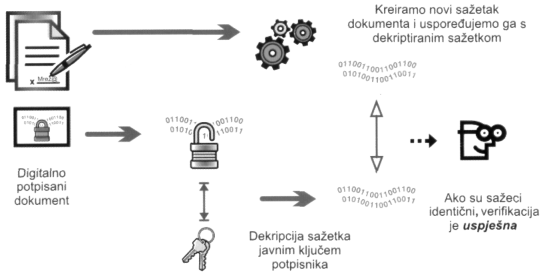
Temelji elektroničkog potpisivanja korištenjem kriptografije javnog ključa su: apsolutna tajnost privatnog ključa pošiljatelja (poznat je samo pošiljatelju) i povjerenje u vjerodostojnost javnog ključa pošiljatelja poruke.

Usprkos pozitivnim obilježjima kriptografije javnog ključa, praktične implementacije nisu dovoljno efikasne za potpisivanje dugačkih dokumenata, pa se protokoli za elektroničko potpisivanje, radi uštede vremena, implementiraju korištenjem jednosmjernih *hash* funkcija. Algoritam razmjene elektronički potpisanih poruka se modificira, pa osoba A potpisuje samo sažetak dokumenta. Modificirani algoritam [6] glasi:

1. Osoba A stvara sažetak polaznog dokumenta.
2. Osoba A šifrira sažetak svojim privatnim ključem i tim činom potpisuje dokument.
3. Osoba A šalje dokument i potpisani sažetak osobi B.
4. Osoba B stvara sažetak dokumenta kojeg je primila od osobe A. Zatim osoba B dešifrira primljeni sažetak pomoću javnog ključa osobe A. Ako se primljeni sažetak i sažetak kojeg je stvorila osoba B podudaraju, potpis je vjerodostojan (sl. 2).



Sl 2. Postupak dig. potpisivanja dokumenta i provjere potpisa [7]



Sl 3. Verifikacija digitalnog potpisa [3]

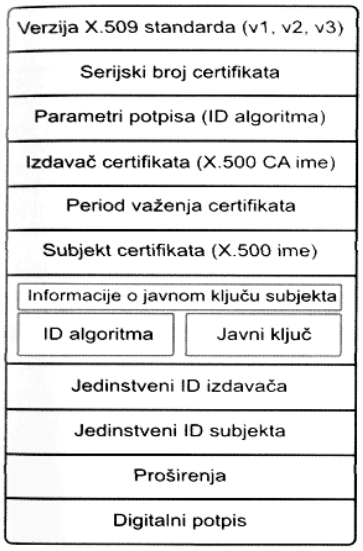
Verifikacija digitalnog potpisa se odvija u dva koraka (sl. 3). Najprije se digitalni dokument odvoji od njegovog potpisa, a potpis dešifrira javnim ključem potpisnika. Drugi korak je ponovno računanje sažetka dokumenta i uspoređivanje s dešifriranim. Ukoliko su sažeci jednaki verifikacija je uspješna i digitalni potpis je valjan.

Provjera javnog ključa se vrši pomoću elektroničkih certifikata javnih ključeva koji povezuju podatke o identitetu osobe s njenim javnim ključem. Certifikat je skup bitnih informacija koje nedvojbeno povezuju korisnika i njegov javni ključ [5], a izdaju ih davatelji usluga certificiranja čiji rad je propisan zakonima.

Elektronički certifikat se sastoji od pet elemenata: [5]

1. informacije o CA-u
2. informacije o vlasniku tj. pošiljatelju
3. javnog ključa vlasnika
4. nadnevka izdavanja i isteka certifikata
5. digitalnog potpisa s CA-a

Verzija (standard) certifikata koji se danas najčešće koristi jest verzija X.509, a na slici 4 mogu se vidjeti njegove sastavnice.



Sl. 4. Sastavnice X.509 formata certifikata [5]

Davatelji usluga certificiranja elektronički potpisuju certifikate. Primatelj prilikom provjere elektroničkog potpisa pošiljatelja provjerava da li postoji valjani certifikat za pošiljateljev javni ključ. Ukoliko postoji, primatelj smatra da je javni ključ (elektronički potpis) pošiljatelja vjerodostojan. Pronalaženje valjanog certifikata jedan je od ključnih koraka u korištenju infrastrukture javnog ključa. Zbog lakšeg pronalaženja certifikata infrastruktura javnog ključa nudi uslugu repozitorija certifikata koji su zapravo robusni *on-line* sustavi koji pomažu primatelju pronaći pošiljateljev certifikat.

Prema namjeni certifikate možemo podijeliti na: [8]

1. osobne (za građane-fizičke osobe)
2. poslovne (za poslovne subjekte)
3. TDU-za tijela državne uprave

U svrhu povezivanja para ključeva s potencijalnim potpisnikom uvodi se treća strana; CA (engl. *Certification Authority*) koja identitet potpisnika povezuje s javnim ključem. Javni ključ i njegov certifikat trebaju biti dostupni korisnicima, pa se pohranjuju u *on-line* repozitoriju (engl. *Repository*) podataka, koji sadržava javne ključeve, certifikate korisnika i listu opozvanih certifikata (engl. *Certificate Revocation List*) koje su potrebne prigodom verifikacije digitalnih potpisa.

Proces registracije predstavlja prvu i najvažniju kariku u realizaciji neporecivosti jer, ako se certifikat izda pogrešnoj osobi, čitav sustav ostvarivanja neporecivosti postaje kompromitiran. To je razlog zašto se na razinama jedne države pokušavaju izgraditi autoritativne i ovlaštene institucije TRA (engl. *Trusted Registration Authority*) i TCA (engl. *Trusted Certificate Authority*) kao institucije najvišeg povjerenja. RA (engl. *Registration authority*) osigurava proces registracije korisnika, prihvaća i obrađuje zahtjeve za izdavanjem certifikata te ih prosljeđuje CA radi izdavanja certifikata.

VI. PROCEDURA DIGITALNOG POTPISIVANJA U PRAKSI

Za primjenu digitalnog potpisa u novčanom poslovanju potrebne su sljedeće komponente:

- šifrirajući program za potpisnika,
- pametna kartica (engl. *Smart Card*) na koju se pohranjuje tajni ključ i certifikat potpisnika,
- čitač kartice koji se instalira na računalo,
- verifikacijski program na strani primatelja.

Potpisivanje se obavlja na sljedeći način:

1. Pametna kartica se umetne u čitač i na taj se način otvara pristup korisničkom kodu.
2. Označe se podaci koji se žele digitalno potpisati.
3. S pomoću *hash* algoritma stvara se sažetak poruke.
4. Sažetak poruke se kombinira s tajnim ključem kako bi se stvorio jedinstven niz podataka-digitalni potpis.
5. Digitalni potpis se pridodaje dokumentu.
6. Verifikacijski program primatelja provjerava potpis na certifikatu pošiljatelja uz korištenje javnog ključa ustanove koja je potpisala certifikat.
7. Uspješno dešifriranje digitalnog potpisa na certifikatu pošiljatelja potvrđuje da je ta ustanova uistinu kreirala potpis i povezuje javni ključ s identitetom pošiljatelja.
8. Primatelj dokumenta na njemu (ne uključujući digitalni potpis) primjenjuje isti *hash* algoritam i kreira sažetak poruke.
9. Primjenom javnog ključa digitalni potpis se dešifrira kako bi se dobio sažetak poslanog dokumenta.
10. Verifikacijski program utvrđuje jesu li vrijednosti sažetka poslanog i primljenog dokumenta identične i odgovara li primijenjeni javni ključ tajnom ključu potpisnika.
11. Ako su sve provjere uspješno izvršene, program potvrđuje pravnu ispravnost obavljenog procesa, transakcije ili dokumenta.

U Hrvatskoj primjenu digitalnog potpisa možemo vidjeti na uslugama PBZ-a (usluga PBZCOM@NET), na primjeru hrvatskih ministara koji koriste pametne kartice prilikom „vođenja“ sjednica Vlade i primjeru vladinog internetskog servisa naziva HITRO.HR koji pruža usluge: e-Katastar, e-Regos, e-Porezna, e-Mirovinsko, e-Zdravstveno i FINA e-kartice. Ministarstvo gospodarstva je vršni CA u Hrvatskoj, a FINA je CA certificirana od ministarstva.

Digitalni certifikat u Hrvatskoj za sad nudi jedino FINA zbog složenosti i kompleksnosti tehničkih mjera, informacijske sigurnosti i dr. uvjeta.

VII. ZAKONSKA REGULATIVA

Hrvatski Sabor je 17. siječnja 2002. godine izglasao Zakon o elektroničkom potpisu koji predstavlja temeljni zakonski akt o elektroničkom potpisu u Republici Hrvatskoj i koji je dopunjen u srpnju 2008. godine kako bi se uskladio s Direktivom 199/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o sustavu za elektroničke potpise [9].

Stupanjem na snagu Zakona o elektroničkoj ispravi krajem 2005. godine zakonodavac je omogućio postojanje pravno-valjanih isprava (dokumenata, ugovora, izjava, potvrda i drugo) koje egzistiraju isključivo u elektroničkom obliku i mogu se slati putem računalnih mreža čime je zaokružen pravni okvir koji omogućuje potpuno elektroničko poslovanje. [10]

Uz Zakon o elektroničkom potpisu donesena su i tri pravilnika o:

1. Registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate. [11]
2. Mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata. [12]
3. Tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa. [13]

Spomenimo ovdje i ostale zakone koji omogućuju primjenu e-poslovanja poput: Zakona o institucijama za elektronički novac [14], Zakona o tajnosti podataka (NN 79/2007), Zakona o informacijskoj sigurnosti (NN 79/2007), Zakona o zaštiti osobnih podataka (NN 103/2003; 118/2006), Zakona o pravu na pristup informacijama (NN 172/03), Zakona o zaštiti potrošača (NN 79/2007, 125/2007), Zakona o telekomunikacijama (NN 122/2003, 158/2003, 60/2004, 70/2005) s pravilnicima i Zakona o javnoj nabavi (110/2007) u dijelu kojim se regulira elektroničko poslovanje u sustavu javne nabave.

Da bismo u praksi koristili digitalni potpis imamo tri mogućnosti njegove izrade:

1. Programom koji omogućuje izradu digitalnog potpisa (poput GnuPG).
2. Preko neke organizacije koja nudi certifikate. (poput *VeriSign*, *GlobalSign* ili *Thawte* na komercijalnoj (uglavnom) ili besplatnoj osnovi (rjeđe).
3. Od države ovlaštene organizacije, poduzeća, institucija ili agencije. U hrvatskom slučaju FINA-e.

VIII. ZAKLJUČAK

Elektronički potpis je ključ sigurnosti i povjerenja u suvremenom poslovanju. Omogućio je kvalitativni skok u razvoju mnogih aplikacija jer omogućava brže i jednostavnije poslovanje, lakše sklapanje ugovora, uštedu poštanskih troškova, elektroničko slanje poreznih prijava, zahtjeva za izdavanje dozvola i slično. Koncepcija *on-line* potpisivanja ugovora zasigurno će otvoriti vrata novim uslugama i oblicima poslovanja. Međutim, praktično uvođenje tehnologije digitalnog potpisa je u Hrvatskoj kasno počelo i slabo se uvodi i koristi. Informatička pismenost u mnogim tvrtkama nije na zadovoljavajućoj razini, a to je osnova za uspješnu implementaciju nove i skupe tehnologije. Mnogi poduzetnici još uvijek preferiraju osobnu komunikaciju, nedovoljno se educiraju i nemaju povjerenje u prednosti takvog poslovanja. Ovdje

valja spomenuti i troškove vezane uz implementaciju digitalnog potpisa. To su prije svega troškovi uspostave i korištenja ustanove za certifikate, baza podataka i drugih servisa te troškovi korisnika (potpisniku treba osigurati programsku podršku, a ustanovi za certifikate platiti izdavanje dokumenta). Potrebno je i sklopovlje za pohranjivanje i obradu potpisnikovog privatnog ključa. Osobe koje primaju digitalno potpisane dokumente trebaju programsku podršku za verifikaciju koja za sobom povlači troškove oko plaćanja pristupa bazama podataka s certifikatima.

Najširа primjena digitalnog potpisa vidi se kod Internet bankarstva (u kojem se koriste pametne kartice za sigurno pristupanje *web* aplikaciji) i u korištenju (skeniranjem) digitaliziranog ručnog potpisa kojim se potpisuju klijenti u bankama prilikom bankarskih transakcija (radi uštede papira, ali je jasno je da ovakav potpis nema pravnu snagu).

Budućnost digitalnog potpisa leži u njegovoj sigurnosti, a njegova sigurnost u algoritmima koji se koriste za šifriranje podataka. Digitalni potpis će zasigurno postati prevladavajući način utvrđivanja autentičnosti dokumenata.

LITERATURA

[1] Anić, V. i dr. , *Hrvatski enciklopedijski rječnik*, Zagreb, EPH d.o.o. i Novi Liber d.o.o., 2004.

[2] Dujella, A., Kriptografija, *osobna web stranica*, <http://web.math.hr/~duje/kript/osnovni.html>, (veljača, 2010.)

[3] Siladi, D., Pogled u digitalizaciju tinte, *Mreža*, broj 5., str. 62 - 64., godina XI. (in Croatian)

[4] Vrbanec, T.; Hutinski, Ž. (2002.) *Data protection; identifications and autentification in applications and protocols, 21st Scientific Conference on Development of Organizational Sciences*, Portorož, str. 1011-1025.

[5] Siladi, D., *Penkala odlazi u mirovinu*, *Mreža*, broj 5., str. 65 - 67., godina XI.

[6] Scheiner, B., *Applied Cryptography*, 2nd Edn., John Wiley & Sons, New York, 1996.

[7] Ždrnja, B., *Potpis bez papira*, *Mreža*, broj 10., str. 62., godina XIII.

[8] FINA, *Digitalni certifikati*, <http://www.fina.hr/Default.aspx?sec=963>, (veljača, 2010.)

[9] Vojković, G., *Šest godina poslije*, *Mreža*, broj 10., str. 53., godina XIII.

[10] Vojković, G., *Digitalna ispravnost*, *Mreža*, broj 10., str. 57., godina XIII.

[11] *Pravilnik o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate,* NN 54/02, <http://narodne-novine.nn.hr/clanci/sluzbeni/308781.html>, (veljača, 2010.)

[12] *Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata*, NN 54/02, <http://narodne-novine.nn.hr/clanci/sluzbeni/308782.html>, (veljača, 2010.)

[13] *Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa*, NN 89/02, <http://narodne-novine.nn.hr/clanci/sluzbeni/309231.html>, (veljača, 2010.)

[14] *Zakon o institucijama za elektronički novac*, NN 117/08, <http://narodne-novine.nn.hr/clanci/sluzbeni/341917.html>, (veljača, 2010.)