

SUSTAVI ZAŠTITE KAO PREDUVJET ZA DOKAZIVANJE AUTENTIČNOSTI DIGITALNOGA GRADIVA

PROTECTIVE SYSTEMS AS A PRECONDITION FOR ESTABLISHING THE AUTHENTICITY OF DIGITAL DATA

Hrvoje Stancić

Odsjek za informacijske znanosti
Filozofski fakultet u Zagrebu
hrvoje.stancic@zg.tel.hr

Sažetak

U radu se konstatira da postoji trend digitalizacije gradiva, te da gradivo sve više nastaje u digitalnom obliku. Nadalje, uočava se da ustanove poput arhiva, knjižnica i muzeja sve više nude sadržaje svojih fondova putem weba. Iako su ti sadržaji uglavnom nedovoljno kvalitetni za reprodukciju koja bi bila bliska izvorniku, postoji i gradivo baš takve, visoke kvalitete. Uzimajući u obzir obje činjenice, autor naglašava da zaštita digitalnoga gradiva ima dvojaku ulogu: zaštitu od neovlaštenoga pristupa, kopiranja i daljnjeg distribuiranja, te dokazivanje autentičnosti gradiva. U radu se stoga objašnjavaju mehanizmi zaštite poput šifriranja simetričnim i javnim ključem, digitalnih potpisa, digitalnih certifikata, digitalnih vodenih žigova, te šifriranih omotnica. Autor posebice ističe potrebu za stvaranjem certifikacijske službe, koja djeluje neovisno o bilo kojoj ustanovi, kao okosnice za dokazivanje autentičnosti digitalnoga gradiva. Time se želi upozoriti na važnost razvoja infrastrukture za upravljanje digitalnim certifikatima, jer je ona nužna za provjeru identiteta (pravne) osobe koja je na određeno gradivo stavila digitalni potpis. Autor zaključuje da je razumijevanje problematike zaštite digitalnoga gradiva, kao i njezino dosljedno primjenjivanje preduvjet modernoga poslovanja AKM-ustanova, pri čemu korisnici mogu provjeriti autentičnost digitalnoga gradiva tj. njegovu vjernost izvorniku, a ustanove dokazati vlasništvo nad određenim digitalnim gradivom.

Ključne riječi: zaštita digitalnoga gradiva, autentičnost, šifriranje, digitalni potpis, digitalni certifikat, certifikacijska služba, digitalni vodeni žig, šifrirana omotnica

Summary

The paper acknowledges the trend towards the digitalisation of material and admits the fact that a great number of material is nowadays being directly created in digital form. Furthermore, it observes the fact that institutions such as archives, libraries and museums nowadays frequently tend to display their contents on the web. Although these materials are often of a lower standard and are not yielding to a ready reproduction which would remain close to its original, high-quality material can also be found. Taking both facts into consideration, the author emphasises the double role played by the protective systems of digital material: they protect against illegal access, copying and further distribution,

but also help establish the authenticity of a particular material. The paper explains the mechanisms of protection, such as encoding under the symmetric and under the public key, forming of digital signatures, digital certificates, digital watermarks and coded envelopes. The author particularly stresses the need of forming an independent certification service as the basis for establishing the authenticity of digital material. Thus he wants to stress the importance of developing an infrastructure which would have control over digital certificates, as it is necessary for investigating the true identity of an institution which puts its digital signature on a particular material. The author concludes his paper by stating that the understanding of the issue, as well as its consistent application are necessary preconditions for the modern functioning of the ALM institutions, offering their users the option of investigating into the authenticity of a particular digital material (i.e. its closeness to the original), while the institutions could thus prove and claim their ownership over a particular digital material.

Keywords: protection of digital material, authenticity, encoding, digital signature, digital certificate, certification service, digital watermark, coded envelope

Uvod

U svijetu se jasno uočavaju dva glavna načina nastajanja elektroničkih dokumenata. S jedne strane, elektronički dokumenti nastaju digitalizacijom postojećih dokumenata u klasičnom, papirnatom obliku, dok se s druge strane javljaju dokumenti koji izvorno nastaju u elektroničkom obliku. Postoje razni razlozi digitalizacije dokumenata – od želje za očuvanjem dokumenata koji neumitno propadaju, pa do želje za omogućavanjem brza pretraživanja gradiva i njegova prezentiranja na internetu. Uočljivo je da ustanove poput arhiva, knjižnica i muzeja sve više nude sadržaje svojih fondova putem web-stranica. Iako su ti sadržaji uglavnom nedovoljne kvalitete za reprodukciju koja bi bila bliska izvorniku, postoje i oni visoke kvalitete. U većini slučajeva pristup se takvom gradivu naplaćuje. No, u oba je slučaja važno da se gradivo u digitalnom obliku zaštiti od neovlaštena preuzimanja s interneta, te ugradi mehanizam za dokazivanje njegove autentičnosti, onosno vlasništva. Drugim riječima, ustanova koja je vlasnik određena digitalnog zapisa svojim kredibilitetom jamči da je digitalna inačica dokumenta identična izvorniku tj. da pri digitalizaciji nije došlo do modifikacije u sadržaju dokumenta, a mehanizmi za dokazivanje autentičnosti potvrđuju da je taj digitalni zapis zaista potekao iz dotične ustanove, te da on u procesu prijenosa nije promijenjen.

Zaštita

Uzimajući u obzir prethodno navedene činjenice, može se zaključiti da zaštita digitalizirana gradiva ima dvojaku ulogu: zaštitu od neovlaštena pristupa, umnažanja i daljnjeg raspačavanja, te dokazivanje autentičnosti gradiva. Mehanizmi zaštite mogu se podijeliti na mehanizme:

- zaštite i osiguranja,
- vezane uz prava i obveze prema vlasnicima i raspačavateljima,

- šifriranja (zakrivanja),
- postojanog šifriranja (*persistent encryption*),
- digitalnih potpisa i digitalnih vodenih žigova.¹

Šifriranje

Cilj je šifriranja zaštititi digitalno gradivo od neovlaštena korištenja. Ono se koristi za osiguranje privatnosti i tajnosti, osiguranje integriteta podataka, utvrđivanje autentičnosti ili identifikacije, autorizacije, izdavanja digitalnih potvrda, izdavanja računa, dodjelu vlasničkih prava, osiguranje anonimnosti itd. pri čemu nije bitno o kojoj je vrsti gradiva riječ, već je bitno da se radi o zapisu u digitalnom obliku.

Načelo šifriranja sastoji se u tome da se digitalni zapis uz pomoć ključa šifriranja preoblikuje tako da bude neprepoznatljiv, te da ga se bez poznavanja ključa ne može vratiti u izvorni oblik. Dva su glavna načina šifriranja digitalnoga gradiva: šifriranje simetričnim ključem (*symmetric-key encryption*) i šifriranje javnim ključem (*public-key encryption*).

Kod šifriranja simetričnim ključem isti se ključ koristi za šifriranje i dešifriranje poruke tj. nekog digitalnoga gradiva koje se želi poslati primatelju komunikacijskim kanalom. Tajnost je ključa vrlo bitna, jer svatko tko ga posjeduje može dešifrirati poruku. Stoga je glavni problem kako dostaviti ključ određenom korisniku, a da ga još netko pri prijenosu ne sazna. Jedan je od načina rješavanja ovog problema dostava pomoću zaštićena komunikacijskog kanala.

Kod šifriranja javnim ključem koriste se dvije vrste ključeva – javni ključ i privatni ključ. Ta dva ključa imaju jedinstveno svojstvo: poruka šifrirana javnim ključem može se dešifrirati jedino odgovarajućim privatnim ključem. Primatelj javno objavi (na internetu, u novinama i sl.) ili dostavi pošiljatelju svoj javni ključ, a privatni ključ strogo čuva. Pošiljatelj šifrira poruku koristeći javni ključ primatelja. Tako šifriranu poruku može dešifrirati jedino vlasnik privatnoga ključa koji odgovara javnom ključu kojim je poruka šifrirana. Pri tom se može zaključiti da je tajni ključ na neki način određen javnim ključem. No otkrivanje tajnog samo na osnovi poznavanja javnoga ključa grubom silom (*brute force*) tj. iskušavanjem svih mogućih kombinacija dok se ne pogodi prava, i uz današnji stupanj razvoja računala trajalo bi jedan cijeli ljudski vijek.

Digitalni potpisi

Digitalni potpis uspostavlja identitet sudionika u elektroničkoj razmjeni podataka i osigurava integritet podataka.² Sustav digitalnih potpisa zasniva se na

¹Stančić, Hrvoje. Upravljanje znanjem i globalna informacijska infrastruktura : magistarski rad. Zagreb : Filozofski fakultet, 2001., str. 45.

²Prema: Strategija razvitka Republike Hrvatske. "Hrvatska u 21. stoljeću", Informacijska i komunika-cijska tehnologija / Vlada Republike Hrvatske, studeni 2000. <http://www.hrvatska21.hr> (2001-02-08).

tehnologiji šifriranja javnim ključem. Digitalni je potpis binarni niz koji se dodaje dokumentu kako bi se potvrdila njegova točnost i ispravnost. Binarni niz izveden je iz tajnog ključa potpisnika dokumenta.

Digitalni potpisi funkcioniraju na isti način kao i klasični potpisi na papirnatom dokumentu. Razlika je jedino u tome da ista osoba svaki digitalni dokument potpisuje na različit način, što nije slučaj kod potpisivanja papirnatih dokumenata. To mora biti tako zato što se digitalni potpis, kao binarni niz, šalje uz poruku, pa kad bi se isti potpis koristio za više dokumenata, svatko tko je dobio dokument s dodanim binarnim nizom mogao bi ga nadodati nekom drugom dokumentu tj. potpisati nekog drugog, i takav dokument poslati dalje.

Digitalni certifikati

S obzirom da, kako je već napomenuto, digitalni potpis uspostavlja identitet sudionika u elektroničkoj razmjeni podataka, potrebno je izdavanje digitalnih certifikata tj. digitalnih potvrda kojima se dokazuje identitet (*identity certificate*) kako bi primatelj podataka mogao provjeriti identitet pošiljatelja. Digitalnu potvrdu identiteta dodjeljuje certifikacijska služba (*certifying authorities*). Ona mora biti ovlaštena za tu djelatnost kako bi digitalne potvrde imale potreban kredibilitet.

Problem digitalnih potvrda identiteta svodi se zapravo na razvoj infrastrukture za upravljanje javnim ključevima. Certifikacijska služba izdaje potvrdu identiteta, te je ovjerava svojim ključem za potpisivanje. Potvrda identiteta neke osobe, dakle, digitalno je potpisan binarni zapis koji sadrži javni ključ i ime vlasnika, a može sadržavati i još neke podatke poput "roka uporabe" tj. informacije o tome u kojem je razdoblju javni ključ pravovaljan. Stoga, kad primatelj posjeduje javni ključ certifikacijske službe, on može vjerovati u ispravnost potvrde identiteta koju je ona izdala, a poznavajući javni ključ osobe koja se navodi u toj potvrdi, vjerovati da mu je upravo ta osoba poslala podatke koje je primio.³

Postupak verificiranog upravljanja javnim ključevima tj. izdavanje potvrda koje jamče da iza određena javnog ključa i imena stvarno stoji određena osoba, vrlo je bitan za primatelja koji na taj način može provjeriti je li mu baš navedena ustanova dostavila određeni dokument, te povjerovati da je dokument stvarno identičan izvorniku tj. da nije neovlašteno promijenjen. Ovaj je postupak bitan i kod potpisivanja digitalnih ugovora, pri čemu se potpisnici mogu nalaziti na dva fizički udaljena mjesta.

Digitalni vodeni žigovi

Digitalni vodeni žig binarni je niz koji je dodan digitalnom gradivu s namjerom da prenese određenu, malu, količinu informacija. Detekcijom prisutnosti digitalnog vodenog žiga može se dokazati autentičnost digitalnoga gradiva. Postoje različite

³The digital dilemma. Intellectual property in the information age. National Academy of Sciences, SAD, National Academy Press, 2000., str. 278 digitalne verzije. http://books.nap.edu/html/digital_dilemma/ (2000-07-15).

primjene digitalnih vodenih žigova, a najčešće se odnose na dokazivanje vlasništva, umetanje podataka o primatelju, provjeru autentičnosti i integriteta, zaštitu itd.

Vrlo je interesantan upravo postupak umetanja podataka o primatelju (*fingerprinting*) u digitalni vodeni žig. Uz osnovni digitalni vodeni žig, dodaje se i šifra korisnika, kojom se na jedinstven način određuje primatelj tj. korisnik kojem je dopuštena uporaba određena digitalnog dokumenta.

Digitalni vodeni žigovi mogu korisnicima biti vidljivi ili nevidljivi, a po oblikovanju su krhki (*fragile*) ili robusni (*robust*). Vidljivi digitalni vodeni žigovi pojavljuju se u obliku logotipa ili neke poruke na vidljivom području digitalna gradiva, te korisnicima služe kao informacija o vlasništvu ili dopuštenom korištenju. Nevidljivi žigovi se, pak, mogu koristiti kao dokaz nelegalna korištenja digitalnih dokumenata. Krhki digitalni vodeni žigovi nisu postojani pri obradi digitalnih dokumenata, pa se koriste kako bi se detektirale eventualne izmjene dokumenata, dok se robusni žigovi provlače kroz cijeli digitalni zapis, te se njegovi dijelovi mogu detektirati i nakon što su obrađeni i uključeni u neki novi dokument. Postupak umetanja podataka o primatelju svojstven je za robusne digitalne vodene žigove.

Šifrirane omotnice

Šifrirane omotnice (*cryptographic envelopes*) nastale su kao sustav pojačane zaštite prijenosa i korištenja digitalnoga gradiva. Ovakvi sustavi koriste šifrirani digitalni spremnik koji sadrži izvornu poruku, izjavu o pravima pristupa i korištenja poruke, a također može sadržavati digitalni vodeni žig i digitalni vodeni žig s umetnutim podacima o primatelju. Korištenje digitalnoga gradiva odobrava softver za provjeru prava korištenja, a pri korištenju se primjenjuje načelo djelomičnog dešifriranja tj. dešifriranja samo onog dijela gradiva koje korisnik u određenom trenutku pregledava. Sustavom šifriranih omotnica omogućava se laka dostupnost gradiva bez ugrožavanja financijskih interesa ustanove koja je vlasnik gradiva zbog moguće izrade i raspačavanja nelegalnih kopija.

Zaključak

Sustavi zaštite digitalnoga gradiva dovoljno su uznapredovali da se mogu koristiti i za potrebe elektroničkog poslovanja tj. za siguran prijenos do korisnika koji je spreman platiti za pregledavanje ili korištenje gradiva. Naravno, uvijek postoje mjesta i kod već razvijenih tehnika gdje su potrebna daljnja istraživanja i razvoj.

Ipak, valja posebno istaknuti potrebu za stvaranjem certifikacijske službe, koja djeluje neovisno o bilo kojoj ustanovi, kao okosnice za dokazivanje autentičnosti digitalnoga gradiva. Ovime želim upozoriti na važnost razvoja infrastrukture za upravljanje digitalnim certifikatima, jer je ona nužna za provjeru identiteta (pravne) osobe koja je na određeno gradivo stavila digitalni potpis.

Stoga smatram da je razumijevanje problematike zaštite digitalnoga gradiva, kao i njezino dosljedno primjenjivanje, preduvjet modernog poslovanja arhiva, knjižnica i muzeja u kojem korisnici mogu provjeriti autentičnost digitalnoga

gradiva tj. njegovu vjernost izvorniku, a ustanove dokazati vlasništvo nad određenim digitalnim gradivom, te bez straha od daljnje neovlaštenog raspačavanja predstaviti gradivo, poštujući pritom dosljedno autorska prava. Zbog toga je ispravno primijenjen sustav zaštite preduvjet za dokazivanje autentičnosti digitalnoga gradiva, te značajan faktor kvalitetna promicanja hrvatske kulturne baštine u svijetu.

LITERATURA

The digital dilemma. Intellectual property in the information age. National Academy of Sciences, SAD. http://books.nap.edu/html/digital_dilemma/ (2000-07-15).

Stančić, Hrvoje. Upravljanje znanjem i globalna informacijska infrastruktura : magistarski rad. Zagreb : Filozofski fakultet, 2001.

Strategija razvitka Republike Hrvatske. "Hrvatska u 21. stoljeću", Informacijska i komunikacijska tehnologija / Vlada Republike Hrvatske, studeni 2000. <http://www.hrvatska21.hr> (2001-02-08).