

VREMENSKO OZNAČAVANJE DIGITALNO POTPISANIH SADRŽAJA

Bogdan Brkić

Ministarstvo finansija Republike Srpske

e-mail: bbogdan@teol.net

Miroslav Čajić

MikroByte doo

e-mail: miroslavcajic@gmail.com

Mladen Veinović

Univerzitet Singidunum

e-mail: mveinovic@singidunum.ac.rs

Sažetak

Najvažnije funkcionalnosti koje mora da posjeduje PKI sistem su: autentičnost pošiljaoca, integritet, tajnost i neporecivosti slanja podataka. Kao jedan od problema koji se postavlja pred PKI sistem jeste mogućnost provjere validnosti digitalnog potpisa i nakon opoziva sertifikata koji je korišten za potpisivanje. Postavlja se pitanje na koji način je moguće uspostaviti pouzdanu vezu između podataka i vremena odnosno garantovati da je dokument postojao i bio potpisan u nekom trenutku. U ovom preglednom radu biće opisane metode kreiranja i validacije vremenske oznake, kao i mjesto i uloga centra za vremensko označavanje u PKI sistemu.

Ključne riječi: Public key infrastructure, digitalni potpis, vremenska oznaka i označavanje

Abstract

The most important functionalities that PKI system must have are: sender authentication, data integrity, data confidentiality and non-repudiation of sending data. As one of the problems posed by the PKI system is the possibility to check the validity of digital signatures and certificates after revocation, which is used for signing. The question of how it is possible to establish a reliable connection between the data and time and guarantee that the document existed and was signed at some point. In this article we will describe methods of creating and validating timestamp and position and role of the time stamp authority in PKI.

Keywords: Public key infrastructure, digital signature, time stamp, time stamping

1. UVOD

Pri razmjeni elektronskih dokumenata od izuzetnog značaja su dvije informacije: prva je ko je kreirao dokument, a druga kada je dokument kreiran odnosno kada je poslednji put izmijenjen. Jedna od najčešće korištenih metoda za dokazivanje autorstva nad elektronskim dokumentom je digitalno potpisivanje. Kao rješenje za problem utvrđivanja tačnih vremenskih atributa elektronskog dokumenta najčešće se koristi vremensko označavanje (*time stamping*). Bilo koji sistem koji obezbjeđuje ove dvije funkcionalnosti uključuje dvije procedure: proceduru za digitalno potpisivanje elektronskog dokumenta kojom se potvrđuje

da je neko autor dokumenta i proceduru za vremensko označavanje kojom se potvrđuje da je dokument postojao u određenom vremenskom trenutku. U ovom radu nećemo detaljnije objašnjavati tehnologiju digitalnog potpisa.

2. VREMENSKO OZNAČAVANJE

Vremensko označavanje je tehnika kojom se dokazuje postojanje nekog podatka prije određenog trenutka vremena. To je postupak kojim se matematičkim metodama uspostavlja jednoznačna veza između elektronskog dokumenta i trenutka u kom je izvršeno vremensko označavanje. Vremenska oznaka je javno dostupna svima koji imaju pristup dokumentu. Za verifikaciju vremenske oznake neophodno je posjedovati: dokument, vremensku oznaku i javni sertifikat servisa za vremensko označavanje. Samo sa tim podacima moguće je utvrditi da li je dokument vremenski označen baš u nekom vremenskom trenutku. Jedna od dobrih osobina sistema za vremensko označavanje je da za kreiranje vremenske oznake nije potreban sam dokument već njegov sažetak – *hash* vrijednost. Ova osobina da je sadržaj dokumenta neophodan samo za verifikaciju vremenske oznake ali ne i za njeno kreiranje je jako značajna. Jedan od najočitijih primjera je proces zaštite patenata, gdje je važno da sadržaj dokumenta ostane tajan sve dok se patent ne prijavi. Ako prijavu patenta posmatramo kao dokazivanje vlasništva nad intelektualnom svojinom u određenom vremenskom trenutku, onda uviđamo potrebu za vremenskim označavanjem. Nakon prijavljivanja patenta vlasnik više nema problem sa autorizacijom istog, on postaje javan i pomoću izvornog dokumenta je moguće verifikovati vremensku oznaku.

U situacijama kada je korisnikov sertifikat opozvan i dalje treba obezbijediti verifikaciju digitalnog potpisa nad nekim sadržajem. Opoziv može da nastane iz raznih razloga: istek perioda važnosti sertifikata, narušavanje bezbjednost korisnikovih kredencijala usled krađe privatnog ključa, prestanak radnog odnosa vlasnika sertifikata u organizaciji koja je obezbijedila sertifikat za digitalno potpisivanje u poslovne svrhe i dr. Postavlja se pitanje kako izvršiti verifikaciju digitalnog potpisa dokumenata koji su potpisani opozvanim privatnim ključevima i kako utvrditi da je dokument potpisan u periodu kada je privatni ključ bio validan? Ove nedostatke infarstrukture javnih ključeva otklanja vremensko označavanje. Postoji još jedan zanimljiv slučaj gdje se kao rješenje nameće vremensko označavanje. Pretpostavimo da korisnik želi poreći da je digitalno potpisao neki važan dokument odnosno da lažno prijavljuje kompromitaciju privatnog ključa. Ako potpisani dokument nije vremenski označen ne može se utvrditi da li je do digitalnog potpisivanja došlo prije ili nakon navodne kompromitacije privatnog ključa. Međutim, ako postoji vremenska oznaka onda je moguće uporediti vrijeme kreiranja vremenske oznake i trenutak opoziva korisnikovog sertifikata. Možemo zaključiti da je integritet vremenski označenih i digitalno potpisanih dokumenata moguće zadržati i čak nakon opoziva digitalnog sertifikata i prestanka upotrebe privatnog ključa.

Entiteti koji se pojavljuju u procesu vremenskog označavanja su:

- podnosilac zahtjeva - entitet koji posjeduje podatke koje treba vremenski označiti,
- verifikator - entitet koji potvrđuje validnost vremenske oznake i
- centar za kreiranje vremenske oznake (Time Stamp Authority TSA) - treća strana od povjerenja koja dokazuje postojanje nekog podatka u datom vremenskom trenutku i koja garantuje za tačnost vremenskog parametra.

Kao što ćemo vidjeti kasnije u radu proces kreiranja vremenske oznake baziran je na matematičkim metodama odnosno na upotrebi jednosmjernih funkcija. Odabir *hash* funkcija i njihovo *update*-ovanje novim obezbjeđuje potreban nivo bezbjednosti ovakvog sistema. Postupak vremenskog označavanja dokumenata vrši *Timestamp* server. Da bi vremensko označavanje bilo precizno ovi serveri treba da su povezani sa nekim *Time* serverom tačnog vremena. Vremensko označavanje može se koristiti i za digitalno potpisane dokumente ali i za nepotpisane dokumente.

3. STANDARDI I ŠEME KOJE SE ODOSE NA VREMENSKO OZNAČAVANJE

Standardi koji se odnose na vremensko označavanje su: RFC 3161, ANSI ASC X9.95 i ISO/IEC 18014-1, 2 i 3. RFC 3161 je najstariji i datira iz 2001. godine. Ovaj standard opisuje format zahtjeva koji se dostavlja TSA centru kao i format odgovora koji TSA vraća. Također utvrđuje i nekoliko bezbjednosnih zahtjeva koji se odnose na procesiranje zahtjeva i generisanje odgovora TSA. Noviji standard ANSI ASC X9.95 iz 2005. godine proširuje standard RFC 3161 sa zahtjevima za bezbjednost na nivou podataka, obezbjeđujući integritet podataka pri čemu koristi pouzdan izvor vremena u koji povjerenje ima bilo koja treća strana tj. bilo koji TSA. Kao takav on specificira minimum zahtjeva za efektivnu upotrebu u finansijskim servisima. Primjenljiv je za vremensko označavanje i digitalno potpisanih i nepotpisanih podataka. Standard ISO/IEC 18014 sastoji se iz tri dijela:

- ISO/IEC 18014-1 opisuje i definiše opšti model servisa za vremensko označavanje, identifikuje ciljeve vremenskog označavanja i definiše osnovne protokole između ušesnika u procesu (2008. godina)
- ISO/IEC 18014-2 i ISO/IEC 18014-3 opisuju različite načine povezivanja sažetka i vremenskog parametra upotrebom različitih kriptografskih tehnika (2009. godina)

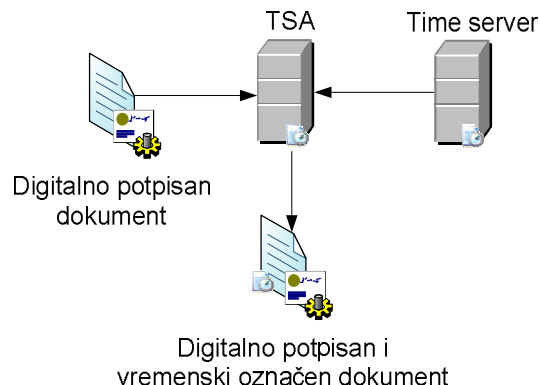
ISO/IEC 18014-2 definiše servise vremenskog označavanja koji proizvode nezavisne tokene koji se mogu zasebno verifikovati, dok ISO/IEC 18014-3 definiše servise koji generišu povezane tokene tj. tokene koji su kriptografski povezani sa drugim tokenima.

Postoji nekoliko različitih šema vremenskog označavanja koje se razlikuju prema nivoima bezbjednosti:

- PKI-bazirana šema (RFC3161, X9.95, ISO/IEC 18014) - dobijeni tokeni su zaštićeni upotrebom PKI digitalnog potpisa,
- šema povezanih tokena (X9.95, ISO/IEC 18014) - vremenske oznake su generisane na način da su povezane sa drugim vremenskim oznakama,
- distribuirana šema - vremenske oznake su generisane od strane više učesnika,
- šema tranzijentnih ključeva (X9.95) - varijanta PKI šeme sa ključevima kratkog životnog vijeka,
- MAC šema (X9.95) - šema zasnovana na jednostavnim ključevima,
- šema koja koristi bazu podataka (ISO/IEC 18014) - sažeci dokumenata se čuvaju u bazi podataka i postoji *online* servis za verifikaciju,
- hibridna šema (X9.95) - obično uključuju ili šemu potpisivanja ili šemu povezanih tokena.

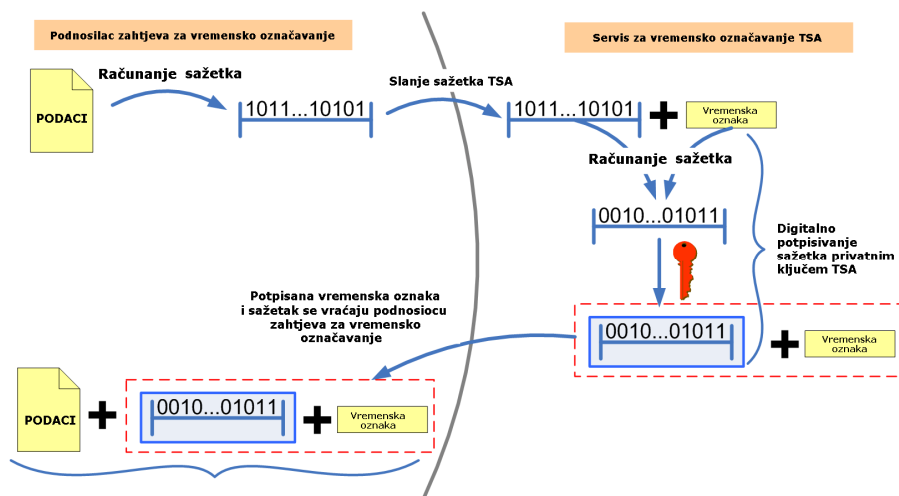
4. GENERALNI MODEL KREIRANJA I VERIFIKOVANJA VREMENSKIH OZNAKA U PKI BAZIRANOJ ŠEMI

U PKI sistemu vremensko označavanje se vrši nakon digitalnog potpisivanja. Čitav postupak predstavljen je na sledećoj slici.



Slika 1. Digitalno potpisivanje i vremensko označavanje

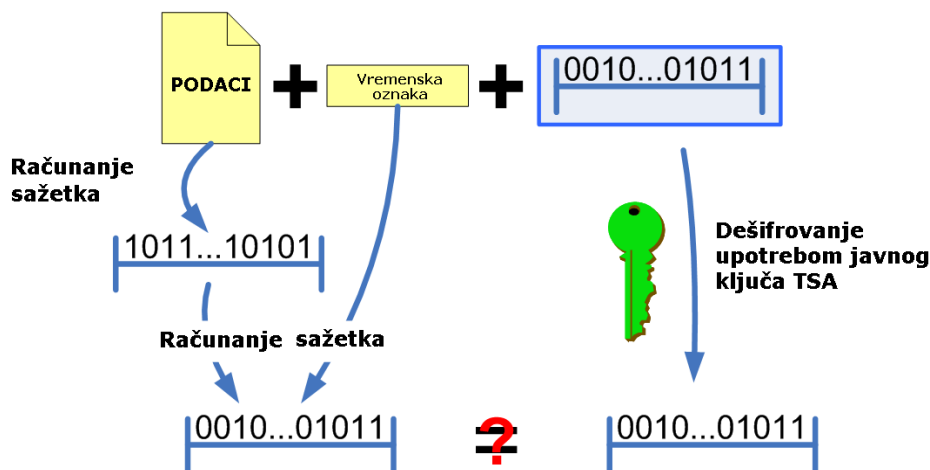
Postupak vremenskog označavanja se odvija na sledeći način. Vlasnik dokumenta kreira sažetak - *hash* vrijednost dokumenta i šalje je centru za kreiranje vremenske oznake (Time Stamp Authority - TSA). TSA na primljeni sažetak dodaje vremensku oznaku, kreira novi sažetak, koji zatim digitalno potpisuje svojim privatnim ključem. Potpisanom sažetku pridodaje vremensku oznaku i šalje je podnosiocu zahtjeva za vremensko označavanje. Podnosilac dobijenu informaciju koja se sastoji od potpisanog sažetka i vremenske oznake pridodaje originalnom dokumentu i nastaje vremenski označen dokument.



Slika 2. Kreiranje vremenske oznake

Postupak verifikacije je suprotan. Primalac vremenski označenog dokumenta želi da provjeri validnost vremenske oznake. On posjeduje: originalni dokument, digitalno potpisani sažetak i vremensku oznaku. Primalac pravi sažetak dokumenta i pridodaje mu vremensku oznaku i dobija niz bita. Zatim na primljeni digitalno potpisani sažetak primijeni dešifrovanje

javnim ključem TSA. Ukoliko su ove dvije vrijednosti jednake verifikacija je uspješna. Za postupak verifikacije vremenske oznake neophodno je provjeriti validnost digitalnog sertifikata tijela koje je izvršilo označavanje.



Slika 3. Verifikacija vremenske oznake

5. ZAKLJUČAK

U ovom radu su razmatrani razlozi za uvođenje vremenskog označavanja digitalnih dokumenata. Posebno su razmotreni nedostaci u infrastrukturi javnog ključa PKI koji se mogu otkloniti vremenskim označavanjem. Opisane su šeme i generalni model i navedeni su standardi koji su u vezi sa ovom metodom. Na kraju su objašnjeni procesi kreiranja i verifikacije vremenske oznake u PKI baziranoj šemi. Iako vremensko označavanje nije striktno povezano sa infrastrukturom javnih ključeva, poseban naglasak je dat otklanjanju nedostataka postupka digitalnog potpisa koji se odnose na vremenske odrednice.

LITERATURA

- [1.] Masahi Une: "The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies", IMES Discussion Papers Series 2001-E-18
- [2.] D. Bayer, S. Haber, W.S. Stornetta: "Improving the efficiency and reliability of digital timestamping", Proceedings Sequences II: Methods in Communication, Security, and Computer Science, Springer-Verlag (1993), 329-334
- [3.] A.Menzes, P.van Oorschot, S. Vanstone: "Handbook of Applied Cryptography", CRC Press, 1996
- [4.] B. Schneier: "Applied Cryptography", John Wiley & Sons, 1996
- [5.] IETF: "RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" (pristup 08.02.2011.) <http://tools.ietf.org/html/rfc3161>
- [6.] ANSI: "ANSI ASC X9.95 Standard for Trusted Time Stamps" (pristup 08.02.2011.) <http://www.ansi.org/>
- [7.] ISO: "ISO/IEC 18014-1" (pristup 08.02.2011.) <http://www.iso.org/>