*XXVIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2010**, Beograd, 14. i 15. decembar 2010.*

VREMENSKI ŽIGOVI SERTIFIKACIONOG TELA POŠTE

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"

Sadržaj: *U radu je opisana namena i postupak vremenskog žigosanja dokumenta. Objašnjene su tehničke karakteristike Timestamp severa, kao i akrediracija izdavaoca vremenskih žigova (TSA tela). Dat je sadržaj zahteva za izdavanje vremenskog žiga i sadržaj vremenskog žiga. Na kraju, objašnjen je redundantan TSA sistem.*

Ključne reči: *Zakon o elektronskom dokumentu, izdavalac vremenskih žigova ili TSA telo, vremenski žig.*

1. Uvod

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) se opredelilo da izgradi sistem za izdavanje vremenskih žigova i tako postane izdavalac vremenskih žigova (Time-Stamping Authority - TSA) u Republici Srbji, u skladu sa Zakonom o elektronskom dokumentu [1] i Pravilnikom o izdavanju vremenskog žiga [2]. Posle izgradnje TSA sistema, PTT će podneti zahtev Ministarstvu za telekomunikacije i informaciono društvo za upis u Registar izdavalaca vremenskih žigova u Republici Srbiji. Tek kada bude upisan u Registar, PTT će početi da izdaje vremenske žigove zainteresovanim korisnicima, i fizičkim i pravnim licima (državna uprava, lokalna samouprava, javne službe, preduzeća, banke, osiguravajuća društva, organizacije, institucije,...).

2. Vremensko žigosanje kao dodatna vrednost elektronskog potpisa

Vremensko žigosanje je tesno povezano sa elektronskim potpisivanjem dokumenata i transakcija, i predstavlja dodatnu vrednost elektronskom potpisu. Razlozi korišćenja vremenskog žigosanja su:

- Vremenskim žigosanjem se onemogućava lažiranje trenutka elektronskog potpisivanja, jer se vremenskim žigosanjem koje sprovodi TSA telo dobija tačno vreme žigosanja, koje nekoliko trenutaka kasni u odnosu na trenutak elektronskog potpisivanja. Znači, nemoguć je događaj da trenutak elektronskog potpisivanja bude posle trenutka vremenskog žigosanja.

- Vremenskim žigosanjem je omogućena uspešna verifikacija elektronskog potpisa i posle isteka roka važnosti elektronskog sertifikata kojim je elektronski potpis kreiran.
- Vremenskim žigosanjem je omogućena uspešna verifikacija elektronskog potpisa i posle opoziva elektronskog sertifikata kojim je elektronski potpis kreiran.

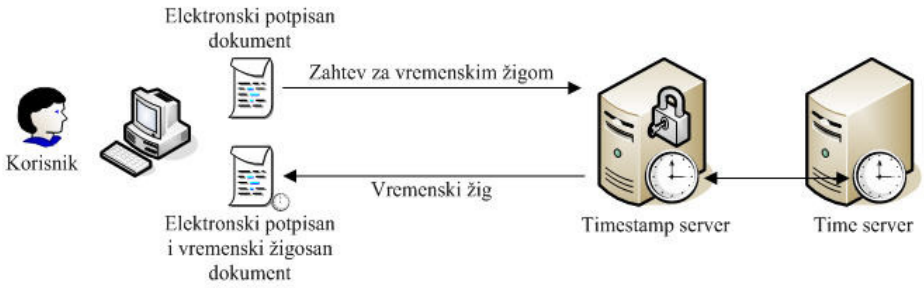
Bez obzira što se vremensko žigosanje najčešće primenjuje uz elektronsko potpisivanje, vremensko žigosanje je moguće primeniti nad elektronskim dokumentom i bez elektronskog potpisivanja. Time se dokazuje da je elektronski dokument postojao pre trenutka vremenskog žigosanja.

3. Postupak vremenskog žigosanja elektronski potpisanog dokumenta

Postupak vremenskog žigosanja se sprovodi na sledeći način (slika 1.):

- Korisnik najpre izvrši elektronsko potpisivanje dokumenta korišćenjem odgovarajuće aplikacije, koja prema Timestamp serveru pošalje zahtev za vremenskim žigom.
- Timestamp server generiše vremenski žig koji pošalje ka korisničkoj aplikaciji, koja vremenski žig pridruži elektronskom potpisu dokumenta.

Da bi Timestamp server mogao precizno da vrši vremensko žigosanje, potrebno je da bude vremenski sinhronizovan sa nekim Time serverom, tj. serverom tačnog vremena.



Slika 1. *Postupak vremenskog žigosanja elektronski potpisanog dokumenta [3]*

4. Najvažnije tehničke karakteristike Timestamp servera

Najvažnije karakteristike aplikacije Timestamp servera su:

- Mogućnost korišćenja hardverskog kriptografskog uređaja - HSM (Hardware Security Module) za generisanje i čuvanje TSA tajnog (privatnog) ključa za potpisivanje vremenskih žigova, što omogućava znatno viši nivo sigurnosti u odnosu na softversko generisanje i čuvanje tajnog ključa.
- Mogućnost izbora kriptografskog algoritma i dužine TSA tajnog ključa za potpisivanje vremenskih žigova (RSA - 2048, RSA - 4096, DSA - 1024,...).

- Mogućnost generisanja PKCS#10 zahteva u postupku instalisanja TSA sertifikata, koji je po standardu X.509.
- Mogućnost instalisanja TSA sertifikata dobijenog od sertifikacionog tela.
- Mogućnost zamene TSA tajnog ključa i sertifikata pre i posle isteka roka važnosti, kao i pre i posle eventualnog opoziva TSA sertifikata.
- Mogućnost instalisanja CA sertifikata (ROOT i Subordinate) dužine RSA ključa od 2048, 4096 bita,...
- Podržava barem jedan od četiri transportna protokola za komunikaciju sa korisnikom koja su definisana standardom RFC 3161 [4], a poželjno je da to bude "Time-Stamp Protocol via HTTP", prema ETSI TS 101 861 [5].
- Mogućnost prijema zahteva od korisnika za žigosanjem sa *hash* vrednostima po sledećim algoritmima: SHA-1, SHA-256, SHA-384, SHA-512,...
- Mogućnost prijema zahteva i korišćenja istovremeno različitih TSA sertifikata za žigosanje, za različite korisnike na osnovu različitih TSA Policy OID tj. mogućnost kreiranja različitih TSA profila.
- Mogućnost autentifikacije korisnika prilikom prijema zahteva za žigosanjem: anonimno - bez autentifikacije, korisničko ime/lozinka (username/password) i/ili elektronski sertifikat.
- Mogućnost izdavanja vremenskih žigova čiji je profi u skladu sa standardom RFC 3161 [4] i ETSI TS 101 861 [5].
- Mogućnost izbora kriptografskog algoritma za potpisivanje vremenskih žigova (RSA/SHA-1, RSA/SHA-256, RSA/SHA-384, RSA/SHA-512, DSA/SHA-1,...).
- Mogućnost evidentiranja u elektronskom dnevniku (Transactions Log) svih aktivnosti prijema zahteva i izdavanja vremenskih žigova, kao i eventualnih grešaka.
- Mogućnost prikazivanja zahteva i vremenskih žigova u *user friendly* formatu.
- Mogućnost izlistavanja zahteva i vremenskih žigova u rastućem i opadajućem redosledu, filtriranje, eksportovanje i importovanje.
- Mogućnost sinhronizacije sa izvorom tačnog vremena po UTC (Coordinated Universal Time) [6] sa razlikom manjom od jedne sekunde.
- Prestanak izdavanja vremenskih žigova ukoliko je nastupio poremećaj u vremenskoj sinhronizaciji.
- Podela administrativnih ovlašćenja ovlašćenog TSA osoblja prema dodeljenim TSA ulogama.
- Mogućnost višestruke autorizacije ovlašćenog TSA osoblja prilikom obavljanja kritičnih i sigurnosno osetljivih operacija.
- Kompatibilnost sa različitim operativnim sistemima, PKI sistemima i aplikacijama drugih proizvođača.
- Mogućnost izdavanja velikog broja vremenskih žigova u sekundi (napomena: broj izdatih žigova u sekundi pre svega zavisi od karakteristika HSM uređaja).
- Velika raspoloživost sistema i servisa. Da bi se povećala raspoloživost kompletnog TSA sistema i servisa uvodi se dodatni Timestamp server, i formira se *load balancer* ili klaster konfiguracija od dva Timestamp servera.

5. Najpoznatija komercijalna rešenja za Timestamp servere

Najpoznatija komercijalna rešenja za Timestamp servere su:

- Thales (bivši nCipher) Time Stamp Server, http://iss.thalesgroup.com
- Ascertia TrustFinderTSA Server, http://www.ascertia.com
- Entrust Verification Server, http://www.entrust.com
- PrimeKey SignServer TSA, http://www.primekey.se, http://www.signserver.org
- Keynectis K.Stamp, http://www.keynectis.com
- OpenTrust TSA, http://www.opentrust.com
- Cryptomathic TSA, http://www.cryptomathic.com

6. Procedura akreditacije TSA tela

Proceduru akreditacije TSA tela u Republici Srbiji izvršava Ministarstvo za telekomunikacije i informaciono društvo, i ona obuhvata [2]:

- proveru Politike izdavanja vremenskih žigova (Time-Stamp Policy i TSA Practice Statement) i internih pravila rada TSA tela i njihove usklađenosti sa Zakonom i podzakonskim aktima,
- proveru operativnog rada TSA tela,
- proveru ispunjenosti tehničkih i bezbednosnih uslova za komponente koje koristi TSA telo za izdavanje vremenskih žigova.

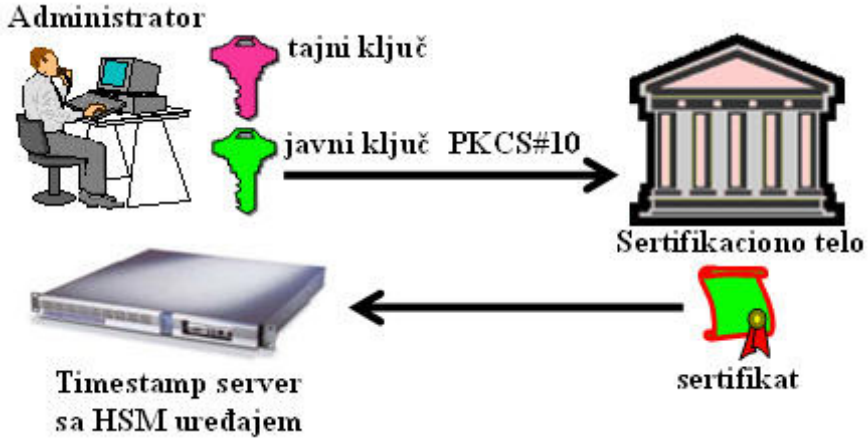
Provera operativnog rada TSA tela obuhvata:

- proceduru dostavljanja zahteva korisnika za izdavanje vremenskog žiga do TSA tela,
- proceduru generisanja vremenskog žiga,
- korišćenje bezbednih hardverskih sredstava (HSM uređaj) za formiranje vremenskog žiga,
- proceduru dostavljanja vremenskog žiga korisniku,
- sisteme fizičke kontrole pristupa u prostorije TSA tela,
- sisteme logičke kontrole pristupa računarskim resursima TSA tela,
- sistem za javno objavljivanje osnovnih informacija o pružanju usluga izdavanja vremenskih žigova, kao i Politike izdavanja vremenskih žigova.

7. Procedura generisanja TSA kriptografskih ključeva i importovanja TSA sertifikata

Proceduru generisanja TSA kriptografskih ključeva i importovanja TSA sertifikata izvršava administrator Timestamp servera u tri (3) koraka (slika 2.):

- Administrator na Timestamp serveru generiše PKCS#10 zahtev za TSA sertifikat, pri čemu se prethodno generišu TSA kriptografski ključevi (javni i tajni). Prema Pravilniku o izdavanju vremenskog žiga [2] generisanje TSA ključeva mora da se izvrši u HSM uređaju, koji ima sertifikat FIPS 140-2 nivo 3 ili viši ili Common Criteria EAL 4+.
- Administrator na osnovu PKCS#10 zahteva, a posredstvom sajta sertifikacionog tela, preuzme TSA sertifikat.
- Administrator izvrši importovanja TSA sertifikata na Timestamp serveru.



Slika 2. *Generisanje TSA kriptografskih ključeva i importovanje TSA sertifikata*

8. Rok važnosti TSA sertifikata i period korišćenja tajnog (privatnog) TSA ključa

U ETSI i RFC standardima koji se odnose na TSA tela **ne** postoje odredbe koje propisuju rok važnosti TSA sertifikata i period korišćenja tajnog (privatnog) TSA ključa. Preporuka kompanije Entrust koja ima jedno od najpoznatijih svetskih rešenja za Timestamp server, je da rok važnosti TSA sertifikata bude pet (5) godina, a da period korišćenja tajnog TSA ključa bude jedna (1) godina, tako da se zamena sertifikata i ključeva vrši jednom godišnje.

Prema Pravilniku o izdavanju vremenskog žiga [2], u Republici Srbiji rok važnosti TSA sertifikata mora da bude najmanje pet (5) godina, a period korišćenja tajnog TSA ključa mora da bude najviše tri (3) meseca, što znači da zamena sertifikata i ključeva mora da se vrši najmanje četiri (4) puta godišnje. To znači da TSA tela u Srbiji moraju znatno češće da vrše zamenu TSA sertifikata i ključeva, od TSA tela u drugim državama (tabela 1.).

Tabela 1. *Primeri roka važnosti tajnog TSA ključa i sertifikata*

RB	TSA telo	Rok važnosti tajnog (privatnog) TSA ključa	Rok važnost TSA sertifikta
1	Ministarstvo za javnu upravu Slovenije	3 godine	5 godina
2	Pošte Slovenije	1 godina	5 godina
3	FINA Demo TSA	5 godina	5 godina
4	VeriSign	* Između 2,3 i 5 godina	5 godina
5	Microsoft	* Između 3 i 5 godina	5 godina
6	Adobe	* Između 4,7 i 10 godina	10 godina
7	SwissSign	* Između 2,8 i 5 godina	5 godina

* Napomena: U TSA sertifikatu ne postoji polje "Private Key Usage Period" tako da rok važnosti tajnog (privatnog) TSA ključa ne može da se očita iz TSA sertifikata. Donja granica roka važnosti tajnog TSA ključa koja je data u tabeli, izračunata je kao razlika između datuma žigosanja jednog dokumenta (datoteke) i datuma početka važnosti TSA sertifikata i tajnog ključa (polje "Valid from" iz TSA sertifikata). Gornja granica roka važnosti tajnog TSA ključa je rok važnosti TSA sertifikata.

9. Politika izdavanja vremenskih žigova

Javni dokument TSA tela je Politika izdavanja vremenskih žigova (Time-Stamp Policy i TSA Practice Statement), i ona mora da bude objavljena na Web strani TSA tela.

Politika mora da bude u skladu sa tehničkom specifikacijom ETSI TS 102 023 "Policy requirements for time-stamping authorities" [6] i drugim standardima za TSA.

Politika definiše zahteve poslovanja TSA tela, kao i procese i resurse TSA tela koji postoje u cilju ispunjenja tih zahteva.

U Politici mora da bude naveden identifikacioni broj Politike (Object Identifier - OID).

TSA telo mora da ima definisan proces periodične analize i održavanja Politike.

10. Sadržaj zahteva za izdavanje vremenskog žiga

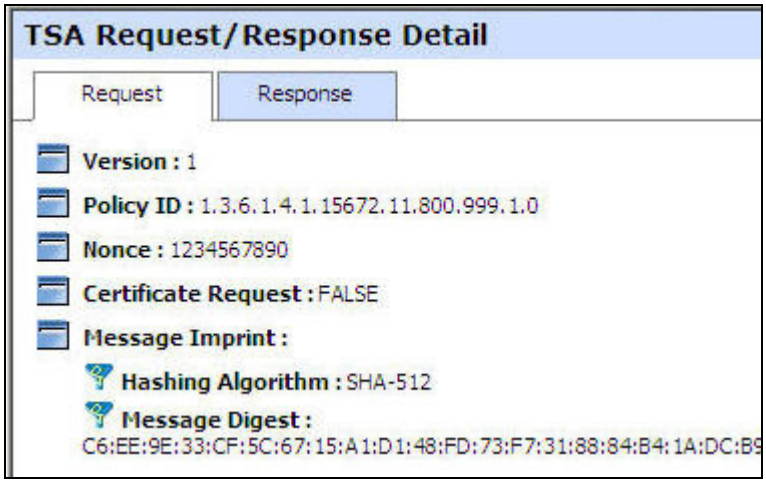
Zahtev za izdavanje vremeskog žiga definisan je standardom RFC 3161 [4] i Pravilnikom [2], i on treba da sadrži sledeća polja:

- Verzija (Version),
- Kriptografski otisak: *hash* algoritam i *hash* vrednost (Message Imprint: Hash Algorithm i Hash Value),
- Identifikacioni broj TSA Politike (TSA Policy OID),
- Veliki slučajan broj (Nonce),
- Zahtev za sertifikatom (Certificate Request),

- Proširenja (Extensions).

Prema standardu RFC 3161 [4] polje "Rertificate Request" je opciono, i može da ima vrednost "True" ili "False" (default False), a Pravilnikom [2] je propisano da polje "Rertificate Request" mora da sadrži vrednost "True".

Primer prikaza TSA zahteva (Request) u *user friendly* formatu dat je na slici 3.



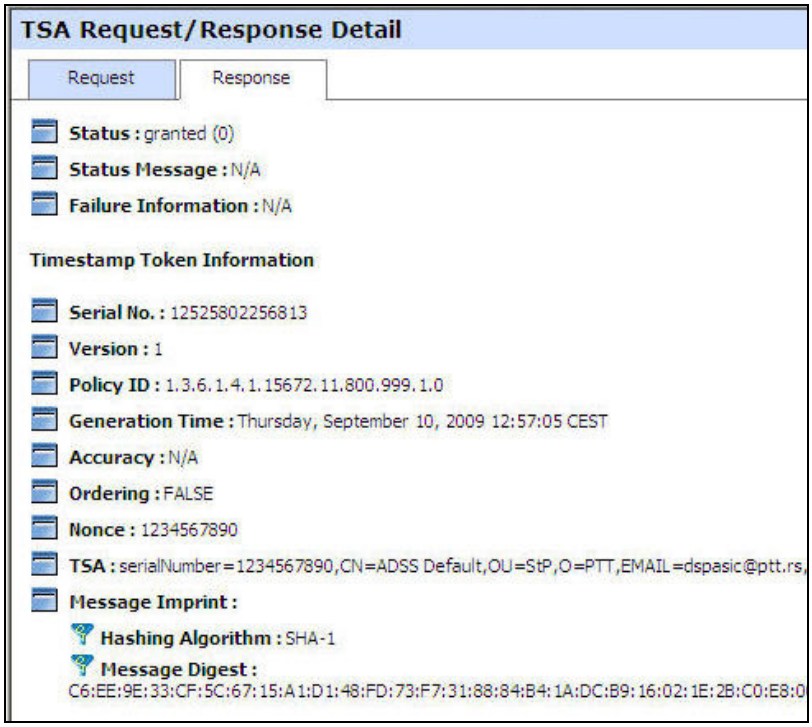
Slika 3. *Primer TSA zahteva*

11. Sadržaj vremenskog žiga

Sadržaj vremenskog žiga definisan je standardom RFC 3161 [4] i Pravilnikom [2], i on treba da sadrži sledeća polja:

- Verzija (Version),
- Identifikacioni broj TSA Politike (TSA Policy OID),
- Kriptografski otisak: *hash* algoritam i *hash* vrednost (Message Imprint: Hash Algorithm i Hash Value),
- Serijski broj (Serial Number),
- Datum i vreme kreiranja vremenskog žiga (Generation Time),
- Tačnost (Accuracy),
- Redosled (Ordering),
- Veliki slučajan broj, koji mora da bude isti kao u TSA zahtevu (Nonce),
- TSA ime ili sadržaj polja "Subject" iz TSA sertifikata (TSA Name),
- Proširenja (Extensions).

Primer prikaza TSA odgovora (Response) i vremenskog žiga (TimeStamp Token - TST) u *user friendly* formatu dat je na slici 4.



Slika 4. *Primer TSA zahteva i vremenskog žiga*

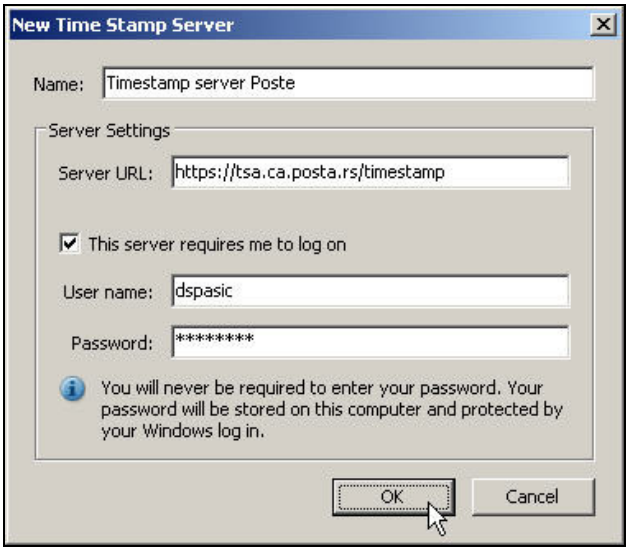
12. Načini autentifikacije Timestamp klijenata na Timestamp server

Postoje tri (3) vrste autentifikacije Timestamp klijenata na Timestamp server:

- Anonimno - bez autentifikacije (poželjno je da se onemogući anoniman pristup Timestamp server zbog izloženosti Timestamp servera Denial-of-Service tj. DoS napadu).
- Korisničko ime i lozinka (username/password).
- Elektronski sertifikat.

Ako se želi naplata izdatih vremenskih žigova, anoniman pristup Timestamp server treba onemogućiti.

Primer podešavanja autentifikacije korisničkim imenom i lozinkom u aplikaciji Adobe Acrobat i Reader, prikazan je na slici 5.



Slika 5. *Podaci o Timestamp serveru i korisničkom nalogu za pristup*

13. Evidentiranje u elektronskom dnevniku svih aktivnosti prijema zahteva i izdavanja vremenskih žigova

Prema Zakonu o elektronskom dokumentu [1], TSA tela su dužna da podatke o izdatim vremenskim žigovima čuvaju na bezbedan način najmanje pet (5) godina od dana izdavanja.

Timestamp serveri koje koriste TSA tela moraju da imaju mogućnost evidentiranja u elektronskom dnevniku (Transactions Log) svih aktivnosti prijema zahteva i izdavanja vremenskih žigova, kao i eventualnih grešaka.

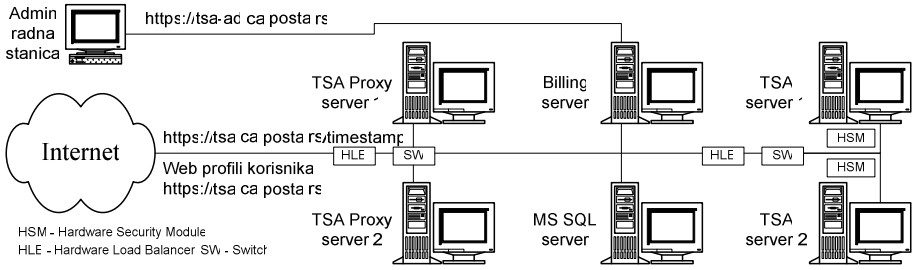
14. Redundantnost TSA sistema

Od TSA sistema se zahteva velika raspoloživost servisa za izdavanje vremenskih žigova. Ako je servis za izdavanje vremenskih žigova u prekidu, i zbog njegovog prekida ne mogu da se izvrše transakcije e-Uprave, e-Trgovine i/ili e-Bankarstva, mogu da nastanu veliki finansijski gubici. Iz tog razloga, veoma je važno obezbediti redundantnost TSA sistema.

Redundantnost TSA sistema Pošte se zasniva na sledeća dva (2) principa (slika 6.):

- Zahtevi za izdavanje vremenskih žigova se od Timestamp klijenata ravnomerno raspoređuju na dva (2) TSA Proxy servera. Ako je jedan od TSA Proxy servera nedostupan (hardverski ili softverski kvar, isključenje, restar,...), svi zahtevi Timestamp klijenata se automatski usmeravaju na drugi TSA Proxy server. TSA Proxy serveri su u *load balancer* konfiguraciji. TSA Proxy serveri ne prihvataju zahteve Timestamp klijenata koji nisu u skladu sa standardom RFC 3161.
- Zahtevi Timestamp klijenata za izdavanje vremenskih žigova se od TSA Proxy servera ravnomerno raspoređuju na dva (2) TSA servera. Ako je jedan od TSA

servera nedostupan (zamena TSA tajnog ključa i sertifikata, hardverski ili softverski kvar, isključenje, restar,...), svi zahtevi Timestamp klijenata se automatski usmeravaju na drugi TSA server. TSA serveri su u *load balancer* konfiguraciji.



Slika 6. *Arhitektura i redundantnost TSA sistema Pošte*

Literatura

[1] Zakon o elektronskom dokumentu ("Službeni glasnik Republike Srbije", br. 51/2009).

[2] Pravilnik o izdavanju vremenskog žiga ("Službeni glasnik Republike Srbije ", br. 112/2009).

[3] D. Spasić, "Status implementacije Zakona o elektronskom potpisu u Republici Srbiji", XXV simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2007", Zbornik radova, str. 181-190, Saobraćajni fakultet, Beograd, decembar 2007.

[4] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[5] ETSI TS 101 861, V1.3.1 (2006-01), "Time stamping profile".

[6] ETSI TS 102 023, V1.2.2 (2008-10), "Policy requirements for time-stamping authorities".

[7] "Potpisivanje i sertifikovanje PDF dokumenata korišćenjem aplikacije Adobe Acrobat", Sertifikaciono telo Pošte (http://www.ca.posta.rs/dokumentacija).

[8] "Konfigurisanje aplikacije Adobe Acrobat i Reader za kvalifikovano elektronsko potpisivanje prema tehničkoj specifikaciji ETSI TS 102 778 (PAdES) Part 2", Sertifikaciono telo Pošte.

Abstract: *This paper describes a purpose and procedure for secure document timestamping. Technical characteristics of Timestamp servers are explained, as well as accreditation of Time-Stamping Authority (TSA). Content of a timestamp request and timestamp token is provided. Finally, a redundant TSA system is explained.*

Key words: *Electronic Document Act, Time-Stamping Authority - TSA, time stamp.*

TIME STAMPS OF THE SERBIAN POST CERTIFICATION AUTHORITY

Dragan Spasić