XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2013, Beograd, 3. i 4. decembar 2013.

TIME-STAMP KLIJENT APLIKACIJA I TESTNI TSA SERVER POŠTE SRBIJE

Dragan Spasić[1], Ivan Lazarević[2], Stevan Milinković[3], Branislav Milojković[3]
[1]Javno preduzeće PTT saobraćaja "Srbija"
[2]S&T Srbija
[3]Računarski fakultet Univerziteta Union

Sadržaj: *Vremensko žigosanje je servis koji pruža institucija koja se naziva izdavalac vremenskih žigova ili TSA telo. Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo informacioni sistem za izdavanje vremenskih žigova i postalo je TSA telo u Republici Srbiji. U ovom radu dat je pregled funkcionalnosti time-stamp klijent aplikacije i testnog TSA servera Pošte Srbije.*

Ključne reči: *Izdavalac vremenskih žigova, vremenski žig, time-stamp klijent aplikacija, TSA server.*

1. Uvod

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je akreditovani izdavalac vremenskih žigova (Time-Stamping Authority - TSA) u Republici Srbiji [1, 2, 3]. Pošta Srbije izdaje vremenske žigove u skladu sa Zakonom o elektronskom dokumentu [4], Pravilnikom o izdavanju vremenskog žiga [5] i Politikom izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" [6]. Vremenski žigovi Pošte namenjeni su svim učesnicima elektronskog poslovanja u Republici Srbiji, i fizičkim i pravnim licima (državna uprava, lokalna samouprava, javne službe, preduzeća, banke, osiguravajuća društva, organizacije, institucije,...).

Tokom izgradnje TSA sistema u Pošti Srbije pojavila se potreba za korišćenjem *time-stamp* klijentske aplikacije kojom bi se testirala ispravnost TSA servisa. U početku su kao *time-stamp* klijentske aplikacije korišćenje aplikacije Adobe Reader [7] i TimeStampClient [8]. Zbog različitih ograničenja obe pomenute aplikacije sa aspekta testiranja TSA funkcionalnosti, odlučeno je da se razvije u Pošti Srbije sopstvena aplikacija za testiranje TSA servisa.

Posle izgradnje TSA sistema u Pošti Srbije pojavila se potreba da se korisnicima za potrebe testiranja besplatno ponudi usluga izdavanja vremenskih žigova. Iz tog razloga, instalisan je i konfigurisan TSA server u Pošti Srbije za izdavanje vremenskih žigova koji se bazira na softveru otvorenog koda.

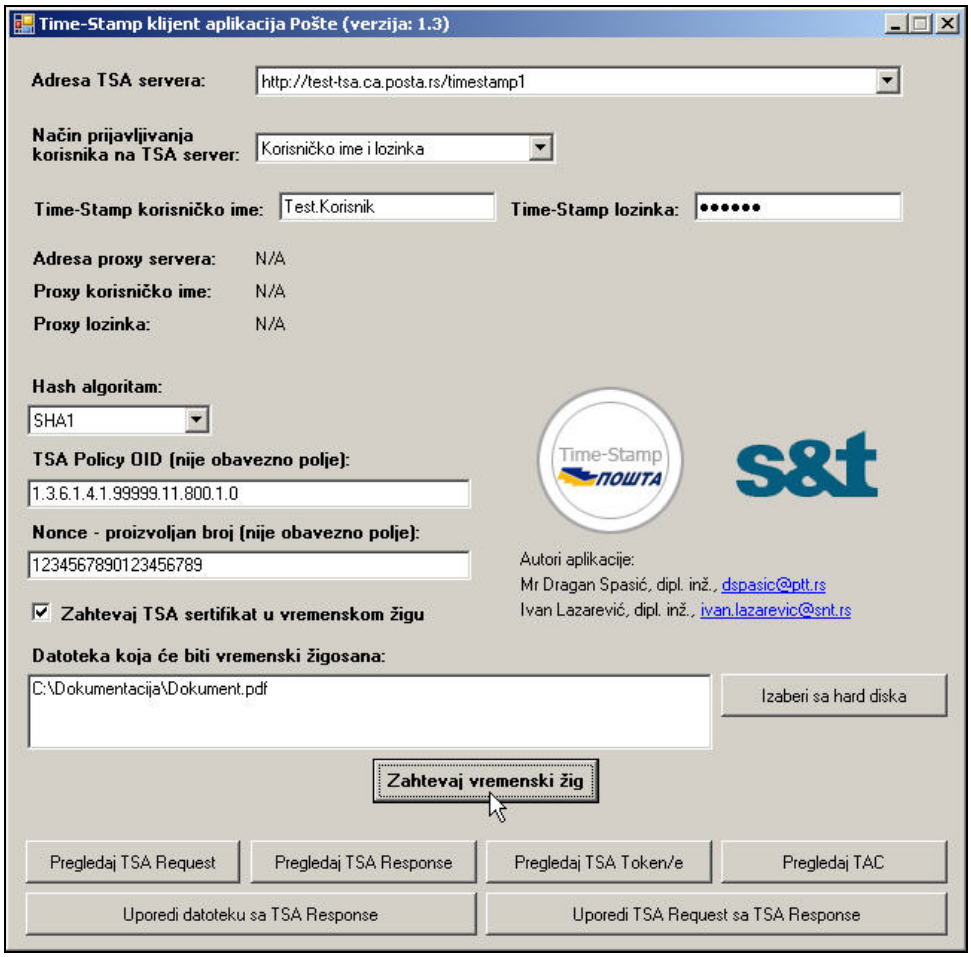
U nastavku rada dat je pregled funkcionalnosti *time-stamp* klijentske aplikacije Pošte Srbije, kao i testnog TSA servera za izdavanje vremenskih žigova.

2. Time-Stamp klijent aplikacija Pošte Srbije

Time-Stamp klijent aplikacija Pošte Srbije je razvijena u skladu sa zahtevima Pošte, sa ciljem da se njenim korišćenjem omogući testiranje različitih funkcionalnosti TSA servera. Funkcionalnosti Time-Stamp klijent aplikacije Pošte Srbije su:

- Aplikacija može da se koristi na Windows računarima na kojima je instalisan Microsoft .NET Framework 4. Od jednog Linux korisnika dobijeno je obaveštenje da aplikacija radi uz Mono 2.10 na GNU/Linux-u, samo je potrebno konfiguracionu datoteku "Time-Stamp konfiguracija.txt" preimenovati u "Time-Stamp klijent Poste v1.3.exe.config".
- U konfiguracionoj datoteci aplikacije moguće je podesiti sledeće parametre:
  - Adresa TSA servera. Adresa se unosi u URL formatu (sa http:// ili https://). Moguće je uneti proizvoljan broj adresa TSA servera koji se koriste za izdavanje vremenskih žigova. Sve adrese koje se unesu potrebno je razdvojiti znakom tačka zarez (;).
  - Adresa proksi servera, port, korisničko ime i lozinka za pristup proksi serveru. Adresa se unosi bez http://.
- Na glavnoj formi aplikacije moguće je izabrati ili uneti sledeće vrednosti (slika 1.):
  - Adresa TSA servera.
  - Način prijavljivanja korisnika na TSA server (korisničko ime i lozinka, elektronski sertifikat ili anonimno).
  - Time-Stamp korisničko ime i lozinka, ako je izabran takav način prijavljivanja korisnika na TSA server.
  - Hash algoritam kojim će se izračunati hash vrednost datoteke koju treba vremenski žigosati (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, RIPEMD-128, RIPEMD-160, RIPEMD-256 ili GOST R 34.11-94).
  - TSA Policy OID. Aplikacija proverava ispravnost formata OID-a i ako je on pogrešan prikazuje poruku o grešci: "Uneli ste neispravan TSA Policy OID.".
  - Nonce - proizvoljan broj. Aplikacija dozvoljava unos samo cifara, ali prva cifra ne može da bude nula. Najveći broj koji može da se unese je 9.223.372.036.854.775.807 (2^{64}/2-1; to polje je "long variable" bez mogućnosti unosa negativnih brojeva).
  - Zahtevaj TSA sertifikat u vremenskom žigu (da ili ne).
  - Datoteka koja će biti vremenski žigosana. Ako se pre žigosanja ne izabere datoteka, prilikom pokušaja žigosanja aplikacija će prikazati obaveštenje: "Izaberite sa hard diska računara datoteku koju želite da vremenski žigošete.".
- Posle uspešnog žigosanja izabrane datoteke, kreiraće se dve nove datoteke: TSA Request (to je zahtev za izdavanje vremeskog žiga) i TSA Response (to je vremenski žig u širem smislu, u okviru koga se nalazi TSA Token koji predstavlja vremenski žig u užem smislu i eventualno sertifikat vremenske sinhronizacije tj. TAC (Time Attribute Certificate) ako ga TSA server generiše). Ako dođe do greške prilikom žigosanja, aplikacija će obavestiti korisnika odgovarajućom porukom.
- Aplikacija omogućava prikaz TSA Request-a (ekstenzija .tsq), TSA Response-a (.tsr), TSA Tokena (.tst) i TAC-a (.tac) u *user friendly* formatu.

- Preko glavne forme aplikacije moguće je sprovesti sledeće upoređivanje (slika 1.):
  - Upoređivanje izabrane datoteke sa izabranim TSA Response.
  - Upoređivanje izabranog TSA Request-a sa izabranim TSA Response.



Slika 1. *Glavna forma Times-Stamp klijent aplikacije Pošte Srbije*

Time-Stamp klijent aplikacija Pošte Srbije je besplatna za korišćenje, a može da se preuzme sa Web strane "Preuzimanje softvera" Sertifikacionog tela Pošte (http://www.ca.posta.rs).

Time-Stamp klijent aplikacija Pošte Srbije sa koristi od strane sledećih korisnika:

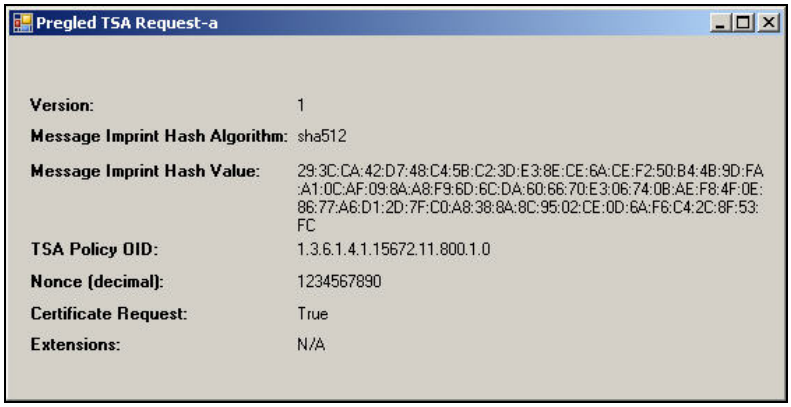
- TSA administratori: za testiranje TSA servera koji rade u skladu sa standardom RFC 3161 [9].
- Korisnici TSA servisa: za proveru komunikacije ka TSA serverima.
- Programeri: kao ideja za implementaciju *time-stamp* klijenta u okviru svojih aplikacija.

- Zainteresovani potencijalni korisnici TSA servisa i studenti: u cilju edukacije.

Sugestije za unapređenje postojeće verzije aplikacije (ver. 1.3) se evidentiraju i kada bude prikupljeno nekoliko korisnih sugestija biće razvijena nova verzija aplikacije (ver. 1.4). Do sada nisu primećene greške u postojećoj verziji aplikacije (ver. 1.3).

3. Prikaz zahteva za izdavanje vremenskog žiga

Aplikacija omogućava prikaz zahteva za izdavanje vremenskog žiga tj. TSA Request-a (ekstenzija .tsq) u *user friendly* formatu. Prikaz sadržaja TSA Request-a je u skladu sa terminologijom i redosledom navedenim u standardu RFC 3161 [9], a termini su zadržani na engleskom jeziku. Na slici 2. je prikazan primer zahteva za izdavanje vremenskog žiga. Struktura zahteva za izdavanje vremenskog žiga data je u tabeli 1.



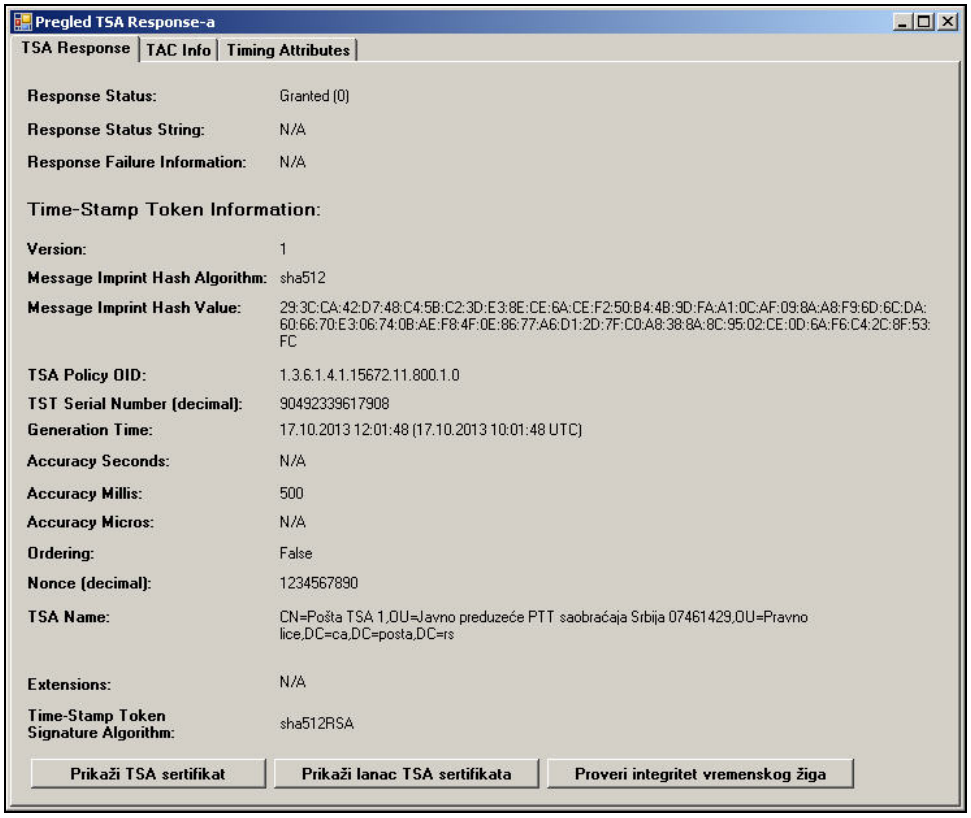
Slika 2. *Primer zahteva za izdavanje vremenskog žiga*

Tabela 1. *Zahtev za izdavanje vremenskog žiga*

RB	Naziv polja	Opisni naziv polja	Polje je obavezno?
1	version	Verzija zahteva	da, default 1
2	messageImprint hashAlgorithm	Identifikator hash algoritma (Object Identifier - OID)	da
3	messageImprint hashedMessage	Hash vrednost (sažetak ili otisak) datoteke koju treba žigosati	da
4	reqPolicy	Identifikacioni broj Politike izdavanja vremenskog žiga (TSA Policy OID)	ne
5	nonce	Proizvoljan broj (number used only once - nonce)	ne
6	certReq	Zahtevanje TSA sertifikata u vremenskom žigu (True ili False)	ne, default False
7	extensions	Ekstenzije ili proširenja zahteva	ne

4. Prikaz vremenskog žiga

Aplikacija omogućava prikaz vremenskog žiga u *user friendly* formatu.Vremenski žig u širem smislu predstavlja odgovor TSA tela na zahtev korisnika za izdavanje vremenskog žiga, a to je TSA Response (ekstenzija .tsr). Vremenski žig u užem smislu predstavlja token vremenskog žiga, a to je TSA Token (ekstenzija .tst). Prikaz sadržaja TSA Response-a i TSA Tokena je u skladu sa terminologijom i redosledom navedenim u standardu RFC 3161 [9], a termini su zadržani na engleskom jeziku. Aplikacija omogućava prikaz svih TSA Token-a koji se nalaze u jednoj .tst datoteci. Na slici 3. je prikazan primer vremenskog žiga. Struktura vremenskog žiga data je u tabeli 2., a tokena vremenskog žiga u tabeli 3.



Slika 3. *Primer vremenskog žiga*

Tabela 2. *Vremenski žig*

RB	Naziv polja	Opisni naziv polja	Polje je obavezno?
1	status	Status TSA odgovora (Response)	da
2	statusString	Poruka o statusu	ne
3	failInfo	Poruka o grešci	ne
4	timeStampToken	Token vremenskog žiga	ne

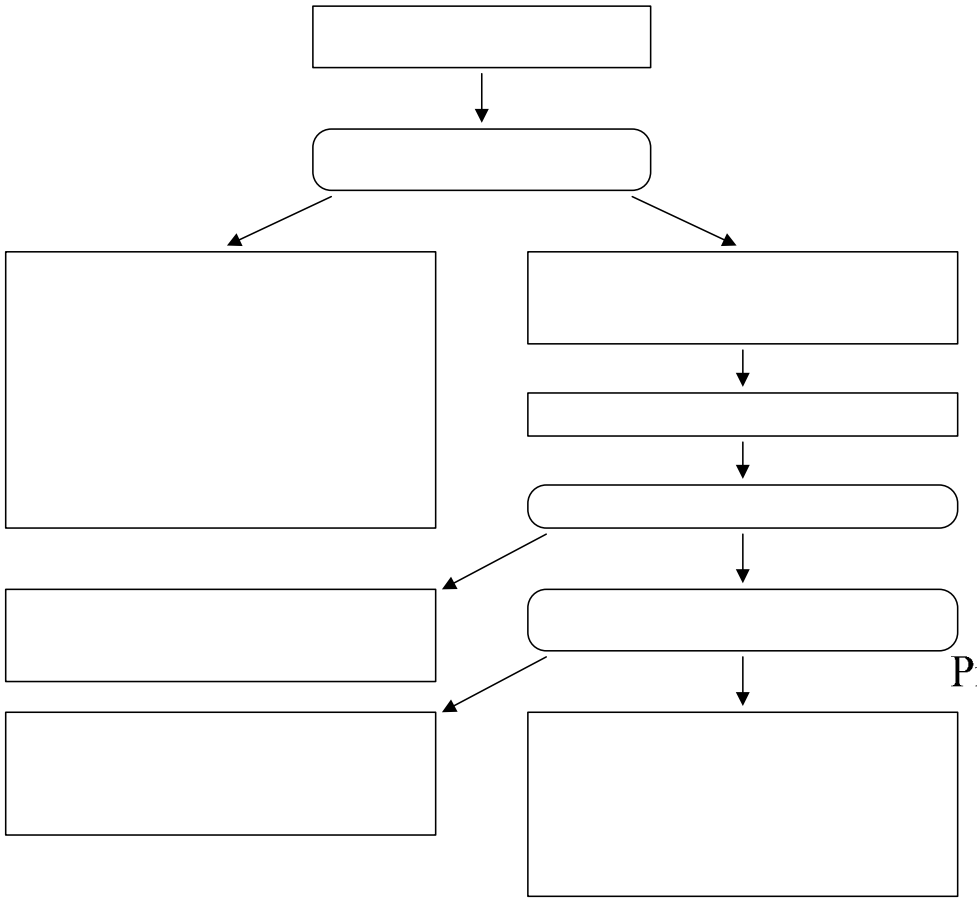
Tabela 3. *Token vremenskog žiga*

RB	Naziv polja	Opisni naziv polja	Polje je obavezno?
1	version	Verzija vremenskog žiga	da, default 1
2	policy	Identifikacioni broj Politike izdavanja vremenskog žiga (TSA Policy OID)	da
3	messageImprint hashAlgorithm	Identifikator hash algoritma (Object Identifier - OID)	da
4	messageImprint hashedMessage	Hash vrednost (sažetak ili otisak) žigosane datoteke	da
5	serialNumber	Jedinstveni serijski broj vremenskog žiga	da
6	genTime	Vreme generisanja vremenskog žiga	da
7	accuracy	Deklarisana tačnost vremena generisanja vremenskog žiga	ne
8	ordering	Redosled vremenskih žigova (True ili False)	ne, default False
9	nonce	Proizvoljan broj (number used only once - nonce)	ne
10	tsa	Ime TSA servera	ne
11	extensions	Ekstenzije ili proširenja vremenskog žiga	ne

Preko forme TSA Response (slika 3.) na kojoj su prikazani podaci o vremenskom žigu, moguće je:

- Prikazati TSA sertifikat, ako on postoji u vremenskom žigu. Pre prikazivanja TSA sertifikata aplikacija proverava da li je TSA sertifikat opozvan. Različiti rezultati provere opozvanosti TSA sertifikata su: "TSA sertifikat nije opozvan.", "TSA sertifikat je opozvan.", "Nemoguće je proveriti opozvanost TSA sertifikata, jer registar opozvanih sertifikata (CRL) nije dostupan. Proverite vašu Internet konekciju.", "Nemoguće je proveriti opozvanost TSA sertifikata, jer pripadajući CA sertifikati nisu instalisani u Windows skladištu sertifikata. Instališite CA sertifikate." i "Provera opozvanosti se ne radi za ROOT CA sertifikat, jer je to sertifikat kome se unapred veruje.".
- Prikazati lanac TSA sertifikat, ako on postoji u vremenskom žigu (slika 4.).
- Proveriti integritet vremenskog žiga. Algoritam provere integriteta vremenskog žiga dat je na slici 5.

Slika 4. *Primer lanca TSA sertifikata u vremenskom žigu*



Slika 5. *Provera integriteta vremenskog žiga u Times-Stamp klijent aplikaciji Pošte*

Preko forme TSA Response, kartice TAC Info i Timing Attributes (slika 3.), na kojima su prikazani podaci o sertifikatu vremenske sinhronizacije tj. o TAC-u (Time Attribute Certificate), moguće je pregledati sadržaj TAC-a i snimiti TAC na hard disk računara. Prikaz sadržaja TAC-a je u *user friendly* formatu i u skladu sa dokumentom Thales TSS SDK (Software Development Kit) [10], a termini su zadržani na engleskom jeziku. Struktura sertifikata vremenske sinhronizacije tj. TAC-a data je u tabeli 4.

Provera integriteta

TSA sertifikat

vremensk

Da

Četiri (4) moguća rezultata provere:

1. Integritet vremenskog žiga je očuvan.
2. Integritet vremenskog žiga je narušen.
3. Elektronski potpis vremenskog žiga je neispravan, tako da nije moguće proveriti integritet vremenskog žiga.
4. TSA sertifikatom koji je ugrađen u vremenski žig nije izvršeno elektronsko potpisivanje vremenskog žiga, tako da nije moguće proveriti integritet vremenskog žiga.

Tabela 4. *Sertifikat vremenske sinhronizacije (TAC) i primeri vrednosti*

RB	Naziv grupe polja	Naziv polja	Primer vrednosti
1	TAC Info	Version	2
2		Holder	CN=Pošta TSA 1,OU=Javno preduzeće PTT saobraćaja Srbija 07461429,OU=Pravno lice,DC=ca,DC=posta,DC=rs
3		Holder Thumbprint	F6:8F:AF:E8:4C:22:A8:A0:AB:02:7E:72:B3:1C:DB:37:44:34:78:77
4		Issuer	CN=LocalAudit.2FAF-719A-463C
5		Serial Number	00:D4:F1:85:C4
6		Valid From	18.03.2013 12:23:32 UTC
7		Valid To	19.03.2013 12:23:32 UTC
8		Signature Value	AB:BC:C7:24:E8:E6:E7:...
9		Signature Algorithm	sha1RSA
10	Clock Timing Metrics	TSA Certification Time	18.03.2013 12:23:32 UTC
11		TSA Certification Expiriation	19.03.2013 12:23:32 UTC
12		Offset (seconds)	0.007762
13		Delay (seconds)	0.004560
14		Leap Second Event Action	Disabled
15		Leap Second Event Time	Null
16	Clock Timing Policy	TAC Policy OID	1.3.6.1.4.1.601.10.3.2
17		Maximum Offset (seconds)	0.500000
18		Maximum Delay (seconds)	0.100000

5. Upoređivanje izabrane datoteke ili zahteva sa vremenskim žigom

Aplikacija omogućava da se proveri da li izdabranoj datoteci odgovara izabrani vremenski žig. Rezultati provere tj. upoređivanja mogu da budu: "Hash vrednost datoteke i hash vrednost iz TSA Response-a su identične vrednosti", "Hash vrednost datoteke i hash vrednost iz TSA Response-a su različite vrednosti", "Izabrali ste pogrešnu vrstu datoteke, tako da nije moguće sprovesti upoređivanje" ili "Hash algoritam iz TSA Response-a je nepoznat, tako da nije moguće sprovesti upoređivanje".

Takođe, aplikacija omogućava da se proveri da li izdabranom zahtevu za izdavanje vremenskog žiga odgovara izabrani vremenski žig. Rezultati provere tj. upoređivanja mogu da budu: "Hash vrednost iz TSA Request-a i hash vrednost iz TSA Response-a su identične vrednosti", "Hash vrednost iz TSA Request-a i hash vrednost iz TSA Response-a su različite vrednosti" ili "Izabrali ste pogrešnu vrstu datoteke, tako da nije moguće sprovesti upoređivanje". Aplikacija upoređuje samo hash vrednosti iz TSA Request-a i TSA Response-a, bez očitavanja hash algoritma iz polja "Message Imprint Hash Algorithm" i njihovog upoređivanja.

6. Testni TSA server Pošte Srbije

Namena testnog TSA servera Pošte Srbije je da omogući zainteresovanim korisnicima da besplatno testiraju izdavanje vremenskih žigova. Kompletan softver na testnom TSA serveru Pošte je softver otvorenog koda. Kao operativni sistem koristi se Debian verzija 6.0.5 (verzija kernela 2.6.32). Od ostalih neophodnih komponenti koriste se: OpenSSL verzija 0.9.8c, time-stamp patch za OpenSSL (ts-20060923-0_9_8c-patch), Web server Apache verzija 2.0.64 i time-stamp modul za Apache (mod_tsa-20060923), koji je razvijen u okviru projekta OpenTSA [11, 12].

S obzirom na činjenicu da OpenTSA server izdaje vremenske žigove sa vremenom koje je očitano sa operativnog sistema lokalnog servera, podešena je na testnom TSA serveru Pošte vremenska sinhronizacija sa određenim Stratum 1 serverima, korišćenjem NTP protokola [13, 14, 15].

Na testnom TSA serveru Pošte (http://test-tsa.ca.posta.rs) podešena su tri načina prijavljivanja korisnika na TSA server prilikom podnošenja zahteva za izdavanje vremenskih žigova, kao što je navedeno u tabeli 5.

Tabela 5. *Način prijavljivanja korisnika na testni TSA server Pošte i adrese servera*

RB	Način prijavljivanja	Adresa TSA servera
1	Anonimno	http://212.62.45.158/timestamp ili http://test-tsa.ca.posta.rs/timestamp
2	Korisničko ime i lozinka	http://212.62.45.158/timestamp1 ili http://test-tsa.ca.posta.rs/timestamp1
3	Elektronski sertifikat	https://212.62.45.158/timestamp2 ili https://test-tsa.ca.posta.rs/timestamp2

Korisnik koji želi da podnese zahtev za izdavanje vremenskog žiga ka testnom TSA serveru Pošte, neophodno je da kreira zahtev u skladu sa standardom RFC 3161 [9], tako da zahtev sadrži sledeće podatke:

- Verzija zahteva: 1.
- Hash algoritam kojim je izračunata hash vrednost datoteke koju treba vremenski žigosati: SHA-1 (drugi hash algoritmi ne mogu da se koriste).
- Hash vrednost datoteke koju treba vremenski žigosati.
- TSA Policy OID: 1.3.6.1.4.1.99999.11.800.1.0, ali ne mora da se navede u zahtevu.
- Nonce - proizvoljan broj: ne mora da se navede u zahtevu.
- Zahtev za TSA sertifikatom u vremenskom žigu: da (true) ili ne (false). Pravilnik o izdavanju vremenskog žiga [5] propisuje da mora da se zahteva TSA sertifikat u vremenskom žigu (certReq=True).
- Ekstenzije ili proširenja zahteva: ne koriste se.

Za godinu i 10 meseci rada testnog TSA servera Pošte (od 1.1.2012. godine), izdato je malo više od 2.500.000 vremenskih žigova.

Literatura

[1] D. Spasić, I. Lazarević, S. Milinković, B. Milojković, "Aplikacija za naplatu i evidentiranje izdatih vremenskih žigova Sertifikacionog tela Pošte", XXX simpozijum o

novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2012", Zbornik radova, str. 149-158, Saobraćajni fakultet, Beograd, decembar 2012.
[2] D. Spasić, S. Milinković, B. Milojković, Lj. Lazić, "Pošta Srbije kao izdavalac vremenskih žigova", XII međunarodni naučno-stručni simpozijum "Infoteh 2013", Zbornik radova, str. 685-688, Jahorina, Elektrotehnički fakultet, Univerzitet u Istočnom Sarajevu, mart 2013.
[3] D. Spasić, S. Milinković, B. Milojković, "Serbian Post Time-Stamping Authority", Metalurgia International, Vol. 18, No. 7, 2013, pp. 86-92, ISSN: 1582-2214.
[4] Zakon o elektronskom dokumentu ("Službeni glasnik Republike Srbije", br. 51/2009).
[5] Pravilnik o izdavanju vremenskog žiga ("Službeni glasnik Republike Srbije", br. 112/2009).
[6] Politika izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" kao izdavaoca vremenskog žiga ("Službeni PTT glasnik", br. 782/2012).
[7] Adobe Reader (http://www.adobe.com).
[8] TimeStampClient (http://timestampclient.sourceforge.net).
[9] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", August 2001.
[10] "Thales Time Stamp Server SDK Reference Guide", Thales e-Security, August 2009.
[11] OpenTSA (http://www.opentsa.org).
[12] R. Miškinis, D. Smirnov, E. Urba, A. Burokas, B. Malyško, P. Laud, F. Zuliani, "Digital Time Stamping System Based on Open Source Technologies", IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, Vol. 57, No. 3, March 2010, pp. 721-727, ISSN 0885-3010.
[13] D. L. Mills, "Computer network time synchronization: the Network Time Protocol on Earth and in Space", 2nd edition. CRC Press, Boca Raton, FL, USA, 2011.
[14] RFC 5905, "Network Time Protocol Version 4: Protocol and Algorithms Specification", June 2010.
[15] RFC 5906, "Network Time Protocol Version 4: Autokey Specification", June 2010.

Abstract: *Time-stamping is a service that is provided by an institution that is called a Time-Stamping Authority (TSA). The Public Enterprise of PTT Communications "Serbia" (Serbian Post) has built an information system for issuing time-stamps and has become a TSA in the Republic of Serbia. An overview of functionality of the time-stamp client application and test TSA server of the Serbian Post is given in this paper.*

Key words: *Time-Stamping Authority - TSA, time-stamp, time-stamp client application, TSA server.*

TIME-STAMP CLIENT APPLICATION AND TEST TSA SERVER OF THE SERBIAN POST

Dragan Spasić, Ivan Lazarević, Stevan Milinković, Branislav Milojković