APLIKACIJA ZA NAPLATU I EVIDENTIRANJE IZDATIH VREMENSKIH ŽIGOVA SERTIFIKACIONOG TELA POŠTE

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: *Institucije koje žele da postanu izdavalac vremenskih žigova (Time-Stamping Authority - TSA) u Republici Srbiji, u skladu sa Zakonom o elektronskom dokumentu [1] i Pravilnikom o izdavanju vremenskog žiga [2], a izdavanje vremenskih žigova planiraju da ponude korisnicima pod komercijalnim uslovima, potrebno je da poseduju aplikaciju za naplatu i evidentiranje izdatih vremenskih žigova, s obzirom na to TSA softveri za izdavanje vremenskih žigova [3, 4, 5] nemaju funkcionalnost registrovanja korisnika i primene različitih modela naplate vremenskih žigova. Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je registrovano za izdavanje vremenskih žigova u Republici Srbiji od marta 2012. godine. Pošta za izdavanje vremenskih žigova koristi TSA softver kompanije Thales e-Security [6], a za naplatu i evidentiranje izdatih vremenskih žigova koristi se aplikacija koja je razvijena u skladu sa zahtevima Pošte. U ovom radu dat je pregled funkcionalnosti aplikacije koja se koristi u Pošti za naplatu i evidentiranje izdatih vremenskih žigova.*

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

1. Uvod

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo sistem za izdavanje vremenskih žigova i postalo je 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]. 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,...).

Ministarstvo kulture, informisanja i informacionog društva upisalo je Javno preduzeće PTT saobraćaja "Srbija" u Registar izdavalaca vremenskog žiga, Rešenjem broj 345-01-00283/2011-07 od 9.3.2012. godine.

Pošta izdaje vremenske žigove u skladu sa Politikom izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" [7].

Cene vremenskih žigova Pošte svrstane su u tri tarifna modela:

- PREPAID model naplate,
- POSTPAID model naplate i
- FLAT RATE model naplate.

Za naplatu vremenskih žigova koje izdaje Pošta koristi se Aplikacija za naplatu i evidentiranje izdatih vremenskih žigova Sertifikacionog tela Pošte (u daljem tekstu Billing aplikacija). Billing aplikacija omogućava:

- unos, promenu, pretragu, brisanje, aktiviranje, deaktiviranje, eksport i import podataka administratora Billing aplikacije, registrovanje i deregistrovanje sertifikata administratora,
- unos, promenu, pretragu, brisanje, eksport i import pravnih lica sa kojima se sklapa ugovor o izdavanju vremenskih žigova,
- unos, promenu, pretragu, brisanje, aktiviranje, deaktiviranje, eksport i import pripadnika pravnih lica, koji mogu da koriste uslugu izdavanja vremenskih žigova,
- unos, promenu, pretragu, brisanje, aktiviranje, deaktiviranje, eksport i import fizičkih lica sa kojima se sklapa ugovor o izdavanju vremenskih žigova,
- unos, promenu, pretragu, brisanje i eksport modela pretplata koji mogu da se koriste za izdavanje vremenskih žigova,
- dodeljivanje, promenu, aktiviranje i deaktiviranje pretpata fizičkim i pravnim licima,
- pregled, pretragu i eksport dodeljenih pretplata fizičkim i pravnim licima,
- pregled, pretragu i eksport izdatih vremenskih žigova fizičkim i pravnim licima,
- pragled potraživanja prema fizičkim i pravnim licima, kao i prikaz podataka kroz PDF izveštaje,
- grupisane preglede izdatih vremenskih žigova po pretplatama, korisnicima, pravnim licima, danima i svih izdatih vremenskih žigova, kao i prikaz podataka kroz PDF izveštaje,
- podešavanje parametara TSA sistema i aplikacije (kontrola obaveznih polja za unos, provere matičnih podataka, aktivacionog e-pisma, dozvoljenih sertifikata za izdavanje vremenskih žigova, dozvoljenih sertifikata administratora za prijavu na Billing aplikaciju, kreiranje različitih administratorski uloga i podešavanje ovlašćenja, podešavanje dozvoljenih TSA Policy OID-a i Hash algoritama za izdavanje vremenskih žigova i drugo.

2. Modeli naplate vremenskih žigova

Modeli naplate vremenskih žigova Billing aplikacije su:

- Model prethodne naplate (PREPAID model). Prema tom modelu, korisnik kupuje odgovarajući broj vremenskih žigova i može da vrši vremensko žigosanje onoliko puta koliko je kupio vremenskih žigova.
- Model fakturisanja (POSTPAID model). Prema tom modelu, korisniku se na kraju meseca dostavlja faktura na osnovu broja sprovedenih transakcija vremenskog žigosanja.

- Model paušalne naplate (FLAT RATE). Prema tom modelu, korisnik plaća fiksni iznos usluge na mesečnom nivou, bez obzira na broj sprovedenih transakcija vremenskog žigosanja.

Billing aplikacija omogućava definisanje neograničenog broja PREPAID paketa, pri čemu su atributi paketa sledeći:

- Oznaka PREPAID paketa,
- Broj vremenskih žigova u paketu,
- Cena paketa i
- Rok trajanja paketa.

Za POSTPAID korisnike omogućen je unos u Billing aplikaciji neograničenog broja platnih razreda pri čemu su atributi platnog razreda sledeći:

- Oznaka POSTPAID platnog razreda,
- Donja granica opsega,
- Gornja granica opsega,
- Pojedinačna cena vremenskog žiga u opsegu i
- Minimalni mesečni iznos za naplatu.

Za FLAT RATE korisnike omogućen je unos u Billing aplikaciji neograničenog broja paketa čiji su atributi sledeći:

- Oznaka FLAT RATE paketa,
- Mesečni iznos za naplatu i
- Rok trajanja paketa.

Billing aplikacija identifikuje korisnika na osnovu korisničkog imena i lozinke ili na osnovu elektronskog sertifikata u skladu sa tarifnim modelom koji je vezan za korisnika (ugovorom definisan tarifni model) i vrši tarifiranje. Kod modela paušalne naplate (FLAT RATE) onemogućeno je prijavljivanje korisnika na TSA sistem korisničkim imenom i lozinkom tj. dozvoljeno je samo prijavljivanje elektronskim sertifikatom. Jednom korisniku može da bude pridružen samo jedan tarifni model. Ukoliko se pojavi potreba za promenom tarifnog modela sklapa se novi ugovor sa korisnikom i definiše početak važenja novog ugovora, a samim tim i momenat od kad se primenjuje novi tarifni model. U momentu kad počne da važi novi ugovor i tarifni model, stari prestaje da važi.

U ceni vremenskih žigova za pravno lice uračunato je otvaranje jednog administratorskog naloga koji ima mogućnost da kreira korisničke naloge za zaposlene iz svog pravnog lica ili jednog korisničkog naloga. Otvaranje dodatnih administratorskih ili korisničkih naloga, dodatno se naplaćuje po svakom nalogu.

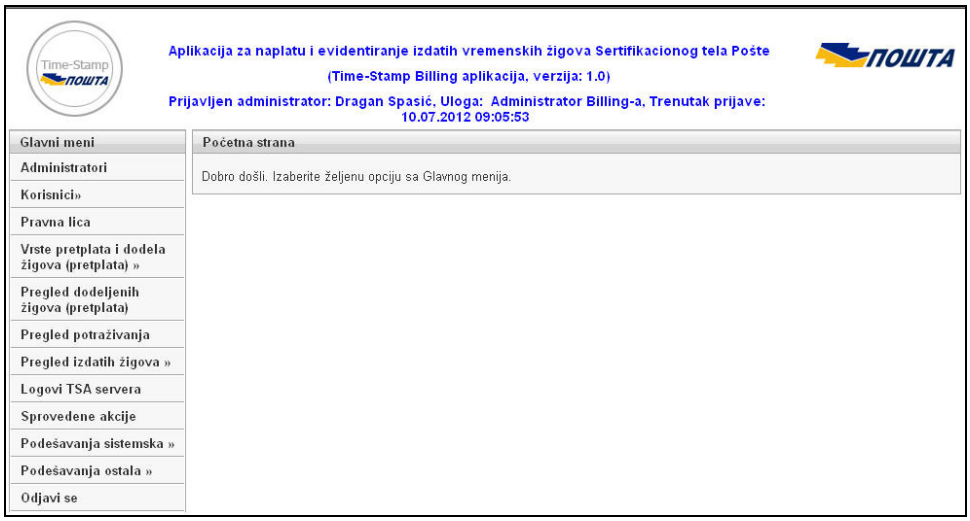
Prilikom obračunavanja utrošenih vremenskih žigova računaju se samo uspešno izdati vremenski žigovi. Ako na zahtev korisnika odgovor TSA sistema ne sadrži vremenski žig iz bilo kog razloga, takav neuspešan odgovor TSA sistema se ne evidentira kao izdat vremenski žig.

3. Prijava na Billing aplikaciju i opcije

Na Billing aplikaciju može da se prijavi isključivo administrator aplikacije kome je prethodno kreiran nalog i pridružen elektronski sertifikat. Administrator se prijavljuje

na Billing aplikaciju svojim elektronskim sertifikatom. Billing aplikacija proverava ispravnost elektronskog sertifikata koji se koristi za prijavu.

Posle uspešne prijave administratora na Billing aplikaciju pojaviće se forma u čijem zaglavlju se nalaze osnovni podaci o administratoru i trenutak prijave administratora, sa leve strane se nalazi glavni meni sa svim opcijama koje administrator ima na raspolaganju, a u centralnom delu forme se nalazi tekst dobrodošlice, kao što je prikazano na slici 1.



Slika 1. *Početna strana Billing aplikacije*

Opcije koje su na raspolaganju administratoru Billing aplikacije su:

- Administratori.
- Korisnici: svi korisnici, fizička lica i pripadnici pravnih lica.
- Pravna lica.
- Vrste pretplata i dodela žigova (pretplata).
- Pregled dodeljenih žigova (pretplata).
- Pregled potraživanja.
- Pregled izdatih žigova: grupisano po pretplatama, korisnicima, pravnim licima, danima i svih žigova pojedinačno.
- Logovi TSA servera.
- Sprovedene akcije.
- Podešavanja sistemska: izbor obaveznih polja na formi za unos administratora, korisnika, pravnog lica, izbor provere matičnih podataka, podešavanje broja prikazanih zapisa u tabelama, podešavanje proveravanja sertifikata u zahtevima za žigovima, podešavanje politike generisanja lozinke, podešavanje notifikacija, podešavanje aktivacionog e-pisma, podešavanje početne strane korisničkog profila i podešavanje redosleda zapisa u tabelama.
- Podešavanja ostala: podešavanje ovlašćenja različitih administratorskih uloga, dozvoljenih TSA Policy OID-a, dozvoljenih Hash algoritama u zahtevima za

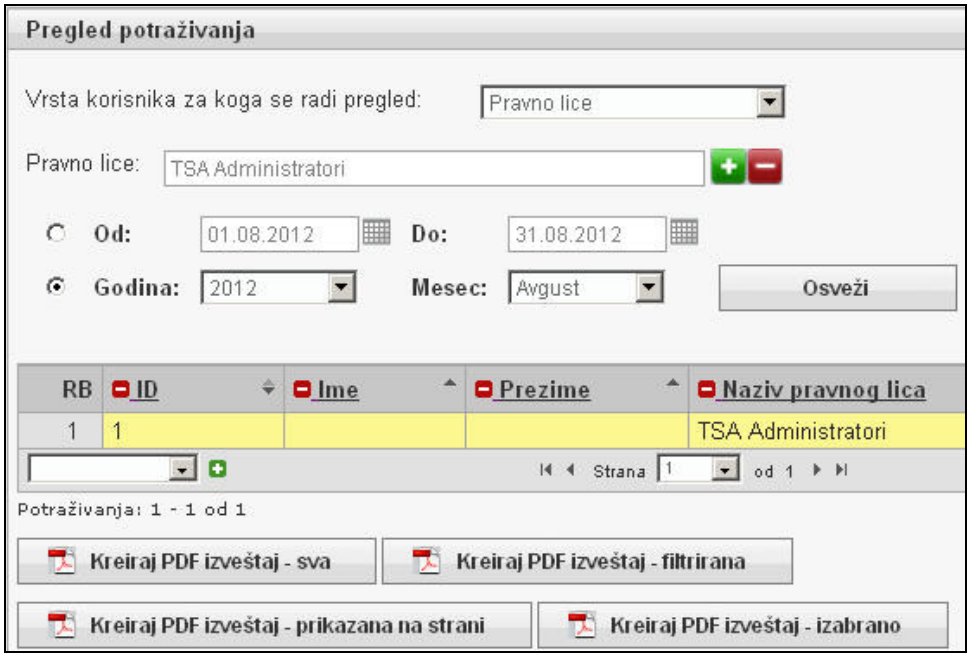
žigovima, dozvoljenih sertifikata za zahtevanje žigova, dozvoljenih sertifikata administratora za prijavu na Billing aplikaciju, vrsta ID dokumenata i država.

- Odjavi se.

U nastavku rada dato je objašnjenje najvažnijih opcija Billing aplikacije.

4. Pregled potraživanja

Administrator Billing aplikacije na osnovu podataka sa forme Pregled potraživanja (slika 2.) kreira fakture za POSTPAID i FLAT RATE korisnike. Izborom opcije Pregled potraživanja iz glavnog menija administrator može da pregleda potraživanja za sve korisnike, izabrano prano lice ili fizičko lice. Prilikom pregleda potraživanja administrator ima mogućnost izbora određenog meseca i godine ili vremenskog perioda za koji se radi pregled. Prikaz podataka je u formi tabele sa sledećim kolonama: ID potraživanja, ime, prezime, naziv pravnog lica, PIB, matični broj, vrsta pretplate, paket pretplate, status paketa za naplatu, broj izdatih žigova, broj preostalih žigova, broj žigova u paketu, pojedinačna cena i ukupno za naplatu.



Slika 2. *Pregled potraživanja*

Podatke iz tabele Pregled potraživanja moguće je prikazati preko izveštaja koji su u formi PDF datoteke, i to:

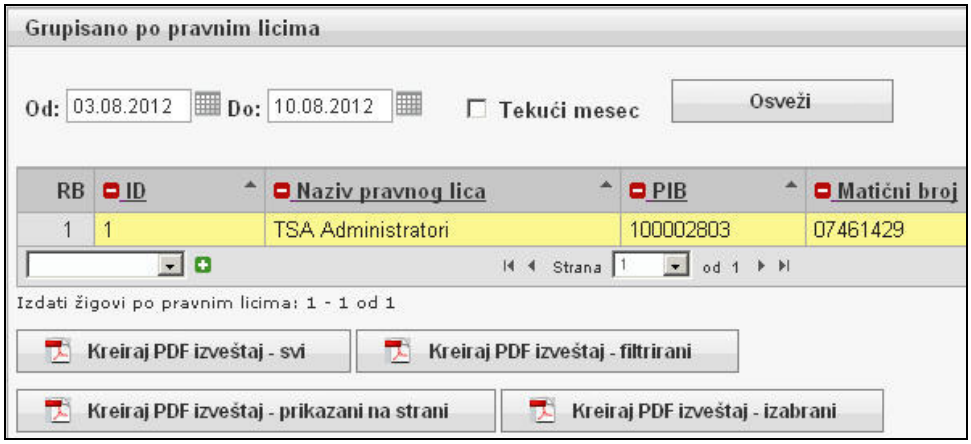
- Prikaz PDF izveštaja svih potraživanja koji se nalaze u tabeli pritiskom na dugme "Kreiraj PDF izveštaj - sva".

- Prikaz PDF izveštaja filtriranih potraživanja pritiskom na dugme "Kreiraj PDF izveštaj - filtrirana".
- Prikaz PDF izveštaja prikazanih potraživanja na strani pritiskom na dugme "Kreiraj PDF izveštaj - prikazana na strani".
- Prikaz PDF izveštaja izabranog potraživanja pritiskom na dugme "Kreiraj PDF izveštaj - izabrano".

5. Pregled izdatih žigova

Izborom opcije Pregled izdatih žigova iz glavnog menija administrator Billing aplikacije može da pregleda izdate vremenske žigove preko pet različitih tabela u kojima su izdati vremenski žigovi grupisani po pretplatama, korisnicima, pravnim licima (slika 3.), danima i svih žigova pojedinačno.

Podatke iz tabela Pregled izdatih žigova moguće je prikazati preko izveštaja koji su u formi PDF datoteke. Te izveštaje administrator može da snimi na svoj računar.



Slika 3. *Pregled izdatih žigova po pravnim licima*

6. Logovi TSA servera

Prema Zakonu o elektronskom dokumentu [1], izdavaoci vremenskih žigova su dužni da podatke o izdatim vremenskim žigovima čuvaju na bezbedan način najmanje pet (5) godina od dana izdavanja [8].

Billing aplikacija omogućava evidentiranje u elektronskom dnevniku svih primljenih zahteva koje su poslali korisnici i izdatih vremenskih žigova, kao i eventualnih grešaka. Podaci o zahtevima korisnika i izdatim vremenskim žigovima dati su na formi Logovi TSA servera (slika 4.).

Izborom opcije Logovi TSA servera iz glavnog menija administrator Billing aplikacije može da pregleda logove TSA servera izdatih vremenskih žigova za izabrani vremenski period. Prikaz podataka je u formi tabele sa sledećim kolonama:

- ID loga, koji je jedinstven identifikator loga.

- Response Status, koji u skladu sa standardom RFC 3161 [9] može da ima sledeće vrednosti: granted (0), grantedWithMods (1), rejection (2), waiting (3), revocationWarning (4) i revocationNotification (5).
- Failure Info, koji u skladu sa standardom RFC 3161 [9] može da ima sledeće vrednosti: badAlg (0), badRequest (2), badDataFormat (5), timeNotAvailable (14), unacceptedPolicy (15), unacceptedExtension (16), addInfoNotAvailable (17) i systemFailure (25).
- Request time, to je trenutak prijema zahteva od korisnika.
- Response time, to je trenutak izdavanja vremenskog žiga.
- TSA Request Policy OID, to je identifikacioni broj TSA Politike iz zahteva korisnika.
- TSA Response Policy OID, to je identifikacioni broj TSA Politike iz izdatog vremenskog žiga.
- TSA sertifikat, kojim je potpisan vremenski žig. Sadržaj ovog polja je link prema TSA sertifikatu.
- TSA Request, to je zahtev za izdavanje vremeskog žiga definisan standardom RFC 3161 [9] i Pravilnikom [2]. Sadržaj ovog polja je link prema detaljnim podacima iz zahteva. Prilikom pregleda zahteva administrator može da ga snimi na svoj računar u formi datoteke.
- TSA Response, to je sadržaj vremenskog žiga definisan standardom RFC 3161 [4] i Pravilnikom [2]. Sadržaj ovog polja je link prema detaljnim podacima iz vremenskog žiga. Prilikom pregleda vremenskog žiga administrator može da ga snimi na svoj računar u formi datoteke.
- Korisničko ime, kojim se korisnik identifikovao prilikom podnošenja zahteva za izdavanje vremenskog žiga.
- Korisnički CN, je podatak o imenu i prezimenu korisnika ako se korisnik identifikovao elektronskim sertifikatom prilikom podnošenja zahteva za izdavanje vremenskog žiga.
- Korisnički sertifikat, kojim se korisnik identifikovao prilikom podnošenja zahteva za izdavanje vremenskog žiga. Sadržaj ovog polja je link prema sertifikatu korisnika.
- Korisnička IP adresa, je IP adresa računara korisnika sa koga je korisnik podneo zahteva za izdavanje vremenskog žiga.
- TSA Request prosleđen ka, je URL adresa servera kome je prosleđen zahtev korisnika za izdavanje vremenskog žiga.

Logove iz tabele Logovi TSA servera moguće je ekportovati u .CSV datoteku, i to:

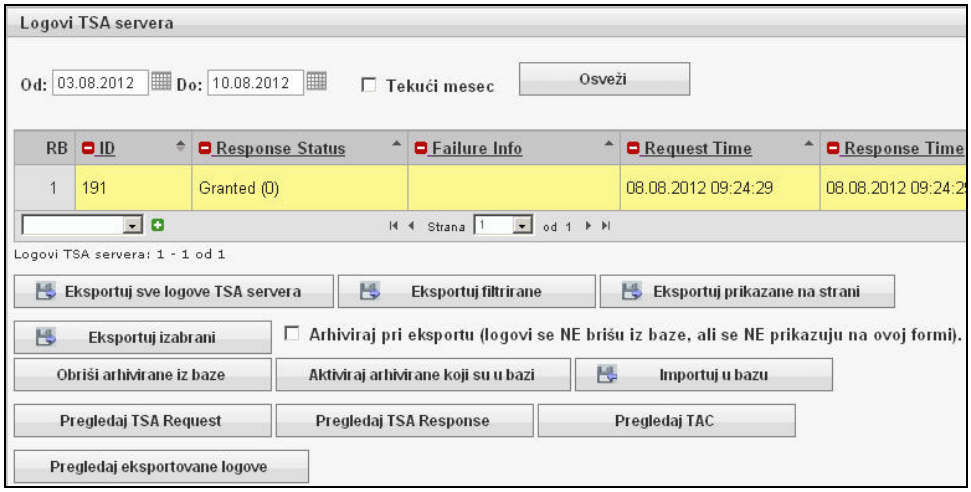
- Eksport svih logova pritiskom na dugme "Eksportuj sve logove TSA servera".
- Eksport filtriranih logova pritiskom na dugme "Eksportuj filtrirane".
- Eksport prikazanih logova na strani pritiskom na dugme "Eksportuj prikazane na strani".
- Eksport izabranog loga pritiskom na dugme "Eksportuj izabranog".

Ako administrator pre eksportovanja logova čekira opciju Arhiviraj pri eksportu, logovi koji se eksportuju više se neće prikazivati u tabeli Logovi TSA servera, ali će u

bazi podataka i dalje postojati, ali sa statusom da su arhivirani. Administratoru su na raspolaganju četiri opcije za rad sa arhiviranim logovima:

- Brisanje arhiviranih logova iz baze podataka, pritiskom na dugme "Obriši arhivirane iz baze".
- Aktiviranje arhiviranih logova posle čega će se prikazivati u tabeli Logovi TSA servera, pritiskom na dugme "Aktiviraj arhivirane koji su u bazi". Preduslov za sprovođenje ove akcije je da arhivirani logovi nisu obrisani iz baze podataka.
- Importovanje prethodno eksportovanih logova u bazu podataka, pritiskom na dugme "Importuj u bazu".
- Pregledanje prethodno eksportovanih logova bez importovanja u bazu podataka, pritiskom na dugme "Pregledaj eksportovane logove".

Administrator može da pregleda i prethodno eksportovane zahteve za izdavanje vremeskog žiga (TSA Request), izdate vremenske žigove (TSA Response) i TAC-ove (Time Attribute Certificate) pritiskom na odgovarajuće dugme koje se nalazi ispod tabele.



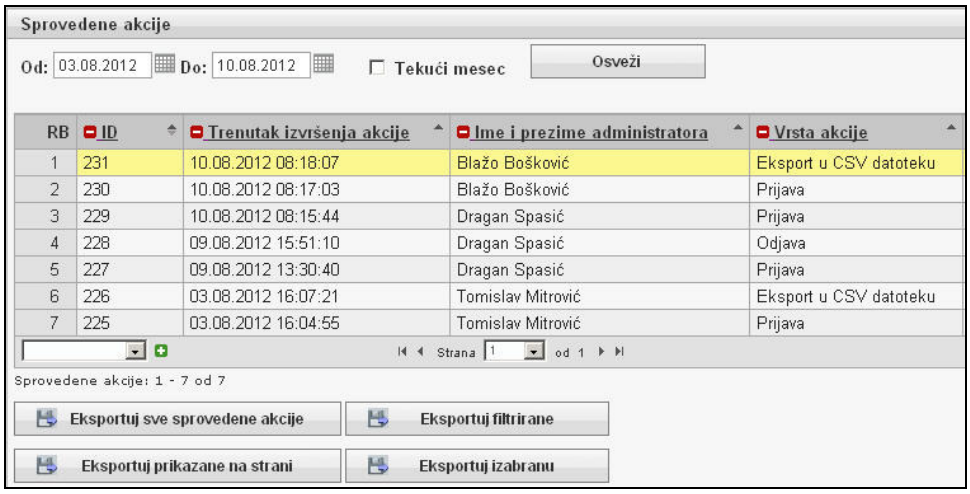
Slika 4. *Logovi TSA servera*

7. Sprovedene akcije

Sve akcije (dodavanje, promene, deaktiviranje, aktiviranje, brisanje administratora, korisnika, pravnog lica, dodela žigova i drugo) koje administrator sprovede u Billing aplikaciji evidentiraju se i elektronski potpisuju i moguće ih je naknadno pregledati uz proveru elektronskog potpisa.

Administrator Billing aplikacije može da pregleda sve sprovedene akcije na formi Sprovedene akcije (slika 5.). Prikaz sprovedenih akcija je u formi tabele sa sledećim kolonama: ID akcije, trenutak izvršenja akcije, ime i prezime administratora, vrsta akcije, vrsta objekta nad kojim je akcija sprovedena, ID objekta, naziv kolone u kojoj je dodata ili promenjena vrednost, prethodna vrednost u koloni i nova vrednost u koloni.

Akcije iz tabele Sprovedene akcije moguće je ekportovati u .CSV datoteku, pritiskom na odgovarajuće dugme za eksport koje se nalazi ispod tabele.



Slika 5. *Sprovedene akcije*

Svaka akcija je elektronski potpisana, a na pregledu detalja sprovedene akcije moguće je proveriti:

- Status sertifikata administratora koji je sproveo i potpisao akciju, u trenutku potpisivanja i u realnom vremenu. Mogući statusi sertifikata su: ispravan, opozvan, istekao, opozvan i istekao, opozvanost je nemoguće proveriti i neispravan.
- Integritet sprovedene akcije, sa dva moguća statusa: očuvan i narušen. Različite varijante narušavanja integriteta navedene su u tabeli 1.

Tabela 1. *Različite varijante narušavanja integriteta sprovedene akcije*

RB	Način narušavanje integriteta	Integritet akcije proveren na osnovu e-potpisa	Integritet podataka proveren na osnovu izvršene akcije
1	Promenjena je akcija u bazi ili elektronski potpis	Narušen	Narušen
2	Promenjeni su podaci u bazi (bilo koja tabela sa podacima: administratori, korisnici,...).	Očuvan	Narušen
3	Promenjena je akcija u bazi i promenjeni su podaci u bazi, ali tako da je urađena identična izmena podataka.	Narušen	Očuvan

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] S. Milinković, B. Milojković, D. Spasić, "Some Results of Research in Temporal Authentication", 2nd International Conference on Internet Society Technology and Management "ICIST 2012", Conference Proceedings, pp. 147-152, Kopaonik, Serbia, March 2012.
[4] S. Milinković, B. Milojković, D. Spasić, "Neka iskustva u implementaciji sistema za izdavanje vremenskih žigova", XI međunarodni naučno-stručni simpozijum "Infoteh 2012", Zbornik radova, str. 746-750, Jahorina, Elektrotehnički fakultet, Univerzitet u Istočnom Sarajevu, mart 2012.
[5] S. Milinković, B. Milojković, D. Spasić, Lj. Lazić, "Evaluation of Some Time-Stamping Authority Software", 6th International Conference on Methodologies, Technologies and Tools enabling e-Government "MeTTeG 2012", Conference Proceedings, pp. 89-99, Belgrade, Serbia, July 2012.
[6] Thales Time Stamp Server Administrator Guide, Thales e-Security, March 2012.
[7] Politika izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" kao izdavaoca vremenskog žiga ("Službeni PTT glasnik", br. 782/2012).
[8] D. Spasić, "Vremenski žigovi Sertifikacionog tela Pošte", XXVIII simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2010", Zbornik radova, str. 175-184, Saobraćajni fakultet, Beograd, decembar 2010.
[9] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

Abstract: *Considering the fact that Time-Stamping Authority (TSA) software has limited functionality in terms of user registration and application of different billing models for issuance of time-stamps, all institutions who wish to become TSA in the Republic of Serbia in accordance with the Electronic Document Act and Time-Stamp Issuance Regulation and are planning to issue time-stamps on a commercial basis need to have software for billing and recording of issued time-stamps. For issuing of time-stamps Serbian Post is using commercial solution developed by Thales, and for the billing and recording of issued time-stamps software developed according to specifications given by Serbian Post. An overview of software functionality is provided in this paper.*

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

SERBIAN POST CERTIFICATION AUTHORITY SOFTWARE FOR BILLING AND RECORDING OF ISSUED TIME-STAMPS*

Dragan Spasić, Ivan Lazarević, Stevan Milinković, Branislav Milojković

* Rad je deo istraživanja koje finansira Ministarstvo prosvete i nauke Republike Srbije, projekti: III-45003 i TR-35026.