APLIKACIJA ZA REGISTROVANJE KORISNIKA ELEKTRONSKIH SERTIFIKATA SERTIFIKACIONOG TELA POŠTE

Dragan Spasić, Dragana Graovac
Javno preduzeće "Pošta Srbije"

Sadržaj: *Sertifikaciono telo Pošte izdaje elektronske sertifikate korisnicima, koji mogu da budu fizička i pravna lica. Za registrovanje korisnika elektronskih sertifikata zaposleni u Sertifikacionom telu Pošte koriste aplikaciju koja se naziva RA (Registration Authority) aplikacija. U ovom radu dat je pregled funkcionalnosti RA aplikacije i navedeni su predlozi za njeno unapređenje.*

Ključne reči: *Zakon o elektronskom potpisu, sertifikaciono telo - CA, registraciono telo - RA, elektronski sertifikati.*

1. Uvod

Sertifikaciono telo Pošte je akreditovani izdavalac elektronskih sertifikata u Republici Srbiji [1]. Sertifikaciono telo Pošte izdaje elektronske sertifikate u skladu sa Zakonom o elektronskom potpisu [2], Pravilnikom o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata [3], Politikom [4] i Praktičnim pravilima pružanja usluge sertifikacije [5]. Profil izdatih elektronskih sertifikata je u skladu sa standardom RFC 5280 [6, 7]. Elektronski sertifikati Sertifikacionog tela 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,...).

Sertifikaciono telo Pošte izdaje sledeće vrste elektronskih sertifikata [8]:

1. Kvalifikovani sertifikat,
2. WEB sertifikat,
3. SER sertifikat za Web server,
4. SER sertifikat za elektronsko potpisivanje,
5. Unified Communications sertifikat,
6. TSA sertifikat za Timestamp server,
7. VPN sertifikat za VPN server,
8. Code Signing sertifikat.

Nad izdatim elektronskim sertifikatima mogu da se sprovedu različite operacije za promenu statusa sertifikata, od kojih su najvažnije sledeće [9]:

1. Produženje korišćenja sertifikata za željeni broj godina, maksimalno do roka važnosti sertifikata.
2. Opoziv sertifikata.
3. Suspenzija sertifikata.
4. Prekid suspenzije sertifikata.

Za registrovanje korisnika elektronskih sertifikata i za sprovođenje operacija za promenu statusa sertifikata, zaposleni u Sertifikacionom telu Pošte koriste aplikaciju koja se naziva RA (Registration Authority) aplikacija [10]. U nastavku rada dat je pregled funkcionalnosti postojeće RA aplikacije Sertifikacionog tela Pošte, i navedeni su predlozi za njeno unapređenje.

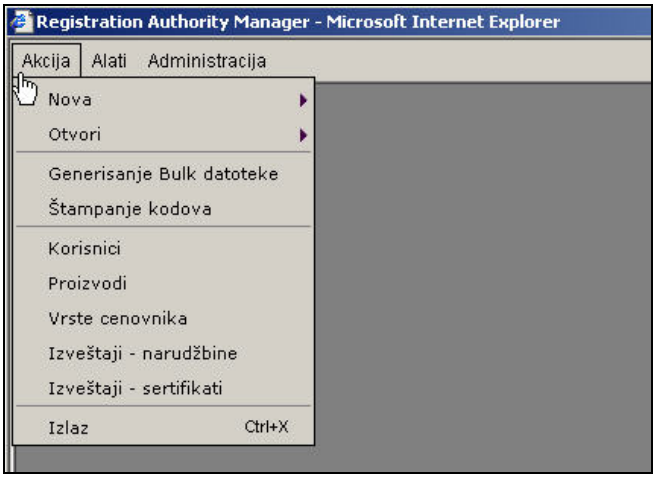
2. Funkcionalnosti postojeće RA aplikacije Sertifikacionog tela Pošte

Postojeća RA aplikacija je softverski sistem namenjem za realizaciju svih pripremnih aktivnosti koje su uslov za izdavanje elektronskih sertifikata Sertifikacionog tela Pošte. RA aplikacija je instalisana i integrisana sa sledećim važnim komponentama koje čine jedinstven sistem:

- PKI (Public Key Infrastructure) sistemom Sertifikacionog tela Pošte koji je izgrađen primenom rešenja kompanije Entrust,
- CMS (Card Management System) aplikacijom,
- SQL bazom podataka u kojoj su smešteni podaci RA aplikacije i
- Informix bazom podataka u kojoj su smešteni podaci neophodni za funkcionisanje Entrust PKI sistema.

Osnovne funkcionalnosti postojeće RA aplikacije (slika 1.) su:

- RA administratori i RA operateri se na RA aplikaciju prijavljuju isključivo elektronskim sertifikatima, a komunikacija se izvršava preko HTTPS protokola,
- unos podataka o korisnicima (naručiocima - pravnim i fizičkim licima),
- unos podataka o porudžbinama,
- ažuriranje podataka o korisnicima i porudžbinama,
- pretraga podataka o korisnicima i porudžbinama,
- unos, pretraga i ažuriranje šifarnika (vrste proizvoda, vrste naručilaca, vrste sertifikata, vrste plaćanja, vrste dokumenata, vrste zahteva, cenovnici, mesta, poštanski brojevi, vrste adresa, države, vrsta dostave, statusi narudžbina, jedinice mere, poreske stope, statusi sertifikata, statusi opoziva sertifikta),
- mogućnost sistemskih podešavanja (definisanje zakonitosti promene statusa, *default* vrednosti polja, preuzimanje unesenih vrednosti polja u aplikativnim formama),
- definisanje validacije unosa (kontrola obaveznog unosa i dozvoljenih vrednosti za unosna polja),
- generisanje *bulk* datoteke za potrebe izdavanja sertifikata,
- štampanje aktivacionih kodova za korisnike sertifikata,
- štampanje obaveštenja za korisnike sertifikata,
- štampanje evidencija i izveštaja,
- definisanje nivoa ovlašćenja i prava pristupa za korisnike aplikacije (RA administratore i RA operatere),
- ažuriranje ograničenja koja se odnose na organizacione jedinice (ograničenje u izboru proizvoda ili izboru naručilaca),
- ažuriranje grupa korisnika, ovlašćenja i poslovnih funkcija koje se dodeljuju grupama korisnika,
- elektronsko potpisivanje sprovedenih transakcija od strane RA administratora i RA operatera aplikacije (sa mogućnošću opcionog uključivanja/isključivanja ove funkcionalnosti).



Slika 1. *Glavna forma RA aplikacije*

3. Unapređenje postojeće RA aplikacije Sertifikacionog tela Pošte

Zbog povećanja obima usluga izdavanja elektronskih sertifikata koje je bilo najintenzivnije krajem 2013. i početkom 2014. godine zbog neophodnosti korišćenja elektronskih sertifikata prilikom podnošenja poreskih prijava preko Portala Poreske uprave "e-Porezi" [11-14], kao i zbog razvoja pojedinih usluga koje su povezane sa izdavanjem sertifikata, pojavila se potreba za proširenjem i unapređenjem postojećih funkcionalnosti RA aplikacije.

Unapređenje RA aplikacije obuhvata realizaciju sledećih zahteva:

- import podataka u RA aplikaciju,
- eksport podataka iz RA aplikacije,
- uvođenje novih statusa i dodatnih funkcionalnosti,
- funkcionalnosti vezane za statuse porudžbina i za formiranje pošiljaka sa sertifikatima na osnovu porudžbina,
- generisanje izveštaja po zadatim kriterijumima,
- integracija RA aplikacije sa postojećim sistemom za naplatu elektronskih usluga,
- Web pristup elektronskim formama za unos zahteva za izdavanje, produženje roka i promenu statusa sertifikata,
- Web pristup elektronskoj formi za unos zahteva za deblokadu smart kartice/USB tokena,
- Web pristup elektronskoj formi za proveru datuma isticanja sertifikata,
- Web pristup elektronskoj formi za proveru opozvanosti sertifikata,
- Web pristup elektronskoj formi za preuzimanje softverskog sertifikata kao PKCS#12 datoteke,
- Web pristup elektronskoj formi za deblokadu smart kartice/USB tokena,
- otklanjanje nedostataka uočenih u postojećoj RA aplikaciji.

Predviđeno je da RA administratori i RA operateri mogu da se prijave na RA aplikaciju sa elektronskim sertifikatima i sprovedu transakcije (uz opciono elektronsko potpisivanje transakcija), korišćenjem Web pretraživača Internet Explorer, Mozilla Firefox i Google Chrome na Windows, Linux i MAC računarima. Takođe, predviđeno je da korisnici mogu da pristupe Web elektronskim formama RA aplikacije i na tim formama da sprovedu transakcije, korišćenjem Web pretraživača Internet Explorer, Mozilla Firefox i Google Chrome na Windows, Linux i MAC računarima.

4. Web forma za unos zahtev za izdavanje sertifikata

Planirano je da postoji elektronski formular (zahtev za izdavanje sertifikata) koji bi za potrebe unosa podataka o korisnicima i porudžbinama bio dostupan na Web-u. Elektronski zahtev za izdavanje sertifikata treba da omogući:

- unos zahteva (porudžbina) kako za fizička tako i za pravna lica,
- *on-line* obračun naknade u skladu sa važećim cenovnikom usluga,
- izbor načina plaćanja (kod pravnih lica dostupno je plaćanje preko računa firme, a kod fizičkih lica plaćanje nalogom za uplatu ili PostFin uplatom),
- kreiranje instrukcije za plaćanje (kod pravnih lica instrukciju za plaćanje (predračun) dostavlja se naknadno na e-mail adresu, dok se za fizička lica na osnovu unesenih podataka iz porudžbenice generiše nalog za uplatu ili instrukcija za PostFin uplatu),
- umetanje priloga (*attachment*-a u PDF formatu) sa skeniranim dokumentima potrebnim za kompletiranje zahteva za izdavanje sertifikata.

5. Web forma za unos zahteva za promenu stausa sertifikata

Predviđeno je da se uvede elektronski formular koji bi za potrebe podnošenja zahteva za promenu statusa sertifikata bio dostupan na Web-u. Elektronski zahtev za promenu statusa sertifikata (opoziv, suspenziju, prekid suspenzije) treba da omogući:

- unos zahteva za fizičko lice (podnosioca zahteva),
- umetanje priloga (*attachment*-a u PDF formatu) sa skeniranim dokumentima potrebnim za kompletiranje zahteva za promenu statusa sertifikata.

6. Web forma za unos zahteva za deblokadu smart kartice/USB tokena

Zamišljeno je da se implementira elektronski formular koji bi za potrebe podnošenja zahteva za deblokadu smart kartice/USB tokena bio dostupan na Web-u. Elektronski zahtev za deblokadu smart kartice/USB tokena treba da omogući:

- unos zahteva (porudžbina) kako za fizička tako i za pravna lica,
- *on-line* obračun naknade u skladu sa važećim cenovnikom usluga,
- izbor načina plaćanja (kod pravnih lica dostupno je plaćanje preko računa firme, a kod fizičkih lica plaćanje nalogom za uplatu ili PostFin uplatom),
- kreiranje instrukcije za plaćanje (kod pravnih lica instrukciju za plaćanje (predračun) dostavlja se naknadno na e-mail adresu, dok se za fizička lica na osnovu unesenih podataka iz porudžbenice generiše nalog za uplatu ili instrukcija za PostFin uplatu),
- umetanje priloga (*attachment*-a u PDF formatu) sa skeniranim dokumentima potrebnim za kompletiranje zahteva za deblokadu smart kartice/USB tokena.

7. Web forma za proveru datuma isticanja sertifikata

Planirano je da postoji elektronska forma koja bi za potrebe provere datuma isticanja sertifkata bila dostupna na Web-u. Pristup ovom servisu bio bi omogućen uz prijavu korisnika sertifikatom za koji se zahteva informacija o datumu isticanja.

8. Web forma za proveru opozvanosti sertifikata

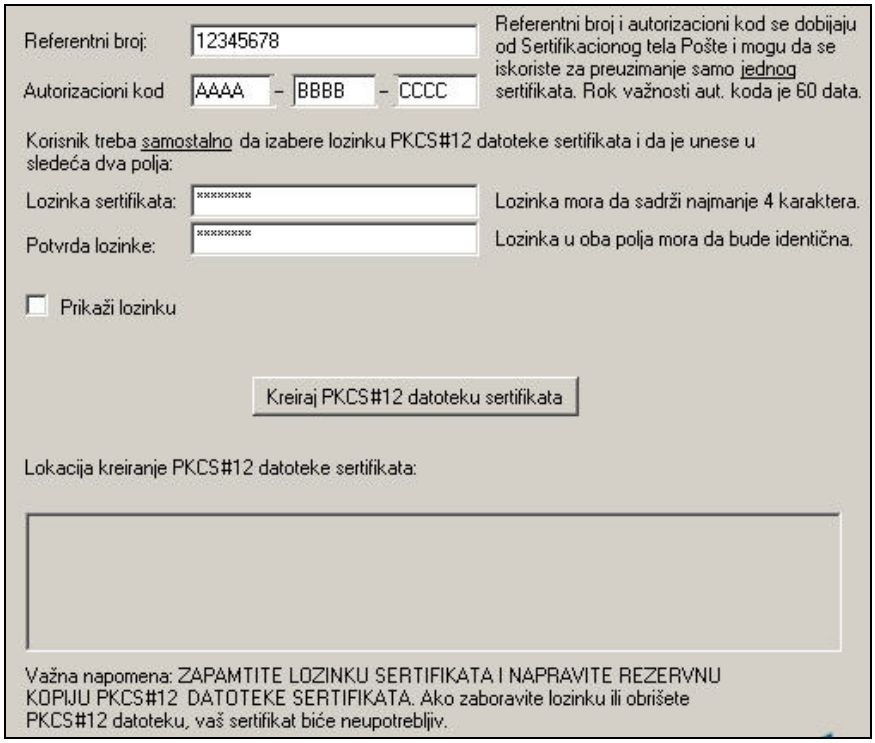
Predviđeno je da se uvede elektronska forma koja bi za potrebe provere opozvanosti sertifkata bila dostupna na Web-u. Provera opozvanosti bi se radila na osnovu unetog serijskog broja sertifikata, a korisnik bi trebao da izabere da li da se provera opozvanosti izvrši preko CRL, parcijalnog CRL ili OCSP (po default-u OCSP). Ako se provera opozvanosti radi preko parcijalnog CRL, korisnik treba da izabere sa padajuće liste redni broj parcijalnog CRL. Ako se provera opozvanosti radi preko OCSP, korisnik treba da izabere sa padajuće liste sertifikat izdavaoca. Rezultat provere treba da se prikaže korisniku, sa sledećim podacima:

- serijski broj sertifikata,
- status sertifikata (ispravan, opozvan, nepoznat),
- datum i vreme opoziva sertifikata.
- razlog opoziva sertifikata, a ako je razlog opoziva "Key Compromise", prikazati i "Invalidity Date".
- ime izdavaoca sertifikata čija se opozvanost proverava (redosled atributa treba da bude: CN, OU, DC),
- ime servera koji je pružio informaciju o opozvanosti sertifikata (redosled atributa treba da bude: CN, OU, DC),
- način provere opozvanosti sertifikata (CRL, parcijalni CRL ili OCSP),
- datum i vreme prikaza prethodno navedenih podataka.

Datum i vreme (uključujući i "InvalidityDate") biće prikazan na dva načina, kao srpsko i UTC, po formatu: dd.mm.gggg ss:mm:ss. Na primer: 04.07.2014 10:15:45 (04.07.2014 08:15:45 UTC).

9. Web forma za preuzimanje softverskog sertifikata kao PKCS#12 datoteke

Zamišljeno je da se implementira elektronska forma koja bi za potrebe preuzimanja softverskog sertifikata, kao PKCS#12 datoteke (.p12), bila dostupna na Web-u (slika 2.).



Slika 2. *Forma za preuzimanja softverskog sertifikata*

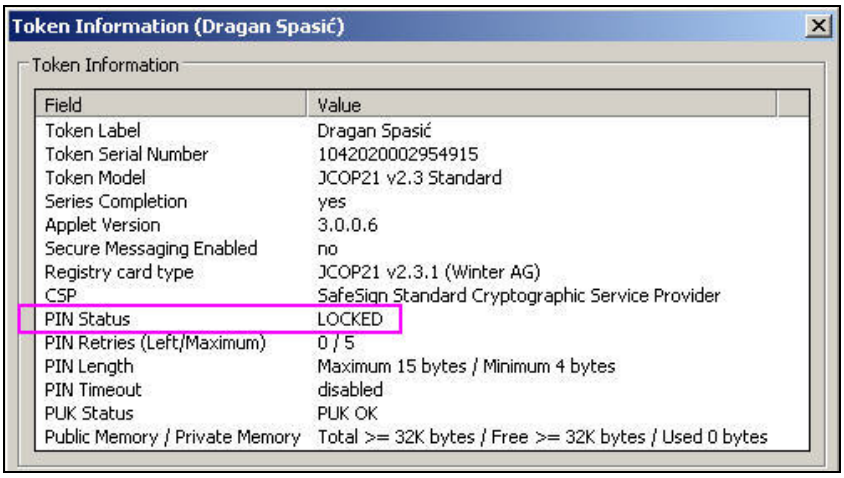
Korisnik bi preuzimao PKCS#12 datoteku sertifikata (.p12), na osnovu prethodno dobijenog referentnog broja i autorizacionog koda od Sertifikacionog tela Pošte. Korisnik bi samostalno izabrao lozinku PKCS#12 datoteke sertifikata (.p12), a istu lozinku bi morao da

unese u dva polja Web forme. Prilikom unosa lozinke, uneti karakteri lozinke biće prikazani crnim kružićima, a korisnik će imati mogućnost da podesi da se lozinka prikaže bez skrivanja. Polja za unos referentnog broja i autorizacionog koda imaće logičke kontrole, kako bi se mogućnost pogrešnog unosa smanjila. Na Web elektronskoj formi prikazivaće se poruke o uspešnosti preuzimanja softverskog sertifikata, kao i poruke o razlozima neuspešnog preuzimanja softverskog sertifikata. Korisnik će pristupati Web elektronskoj formi za preuzimanje softverskog sertifikata isključivo preko HTTPS protokola.

10. Web forma za deblokadu smart kartice/USB tokena

Planirano je da postoji elektronska forma preko koje bi korisnik radio deblokadu (otključavanje) smart kartice/USB tokena. Za izabranu smart karticu/USB token, korisnik bi sa padajuće liste birao da mu se nova lozinka (PIN) pošalje na SMS, e-poštu ili na adresu stanovanja, s tim što pomenute odredišne adrese moraju prethodno da postoje u RA bazi podataka.

Smart kartica/USB token se blokira posle pet (5) uzastopnih pogrešno unetih lozinki, u kom slučaju je nemoguće koristiti sertifikat i tajni kriptografski ključ na smart kartici/USB tokenu. Korišćenjem klijentskog softvera A.E.T. SafeSign može da se proveri da li je smart kartica/USB token blokiran. Ako je smart kartica/USB token blokiran, biće prikazana poruka "PIN Status = LOCKED", kao na slici 3.



Slika 3. *A.E.T. SafeSign forma sa podacima o smart kartici/USB tokenu*

11. Zaključak

Odluka Poreske uprave Republike Srbije da joj poreski obveznici od 1.3.2014. godine podnose poreske prijave isključivo u elektronskom obliku i elektronski potpisane, u skladu sa Pravilnikom o poreskoj prijavi za porez po odbitku [12] i Zakonom o elektronskom potpisu [2], značila je da svi poreski obveznici moraju da nabave kvalifikovane elektronske sertifikate. Sertifikaciono telo Pošte je vršilo masovno izdavanje kvalifikovanih elektronskih sertifikata poreskim obveznicima krajem 2013. i početkom 2014. godine. Tokom masovnog izdavanja elektronskih sertifikata, primećena su određena ograničenja i nedostaci u postojećoj verziji RA aplikacije, koja se koristi za registrovanje korisnika elektronskih sertifikata i

registrovanje zahteva za promenu statusa sertifikata. Zbog toga, Sertifikaciono telo Pošte je odlučilo da izvrši proširenje i unapređenje postojećih funkcionalnosti RA aplikacije.

Sertifikaciono telo Pošte osim elektronskih sertifikata, zainteresovanim korisnicima (fizičkim i pravnim licima) izdaje i vremenske žigove od marta 2012. godine [15], u skladu sa Zakonom o elektronskom dokumentu [16], Pravilnikom o izdavanju vremenskog žiga [17] i Politikom izdavanja vremenskog žiga [18]. Profil izdatih vremenskih žigova je u skladu sa standardom RFC 3161 [19-25]. U ovom trenutku, vremenski žigovi se još uvek ne koriste masovno u Republici Srbiji. Razlog tome može biti činjenica da u pravnim aktima u kojima se zahteva obavezna upotreba elektronskog potpisa, se ne pominje da se elektronskom potpisu mora pridružiti vremenski žig. Jedini pravni akt u kome se zahteva primena vremenskog žiga prilikom elektronskog potpisivanja je Uputstvo o elektronskom kancelarijskom poslovanju [26].

Evropski parlament i savet su 23.7.2014. usvojili eIDAS Uredbu [27] koja treba da reguliše primenu pouzdanih elektronskih servisa u državama Evropske unije. Očekuje se da pravni akti Republike Srbije budu usklađeni sa pomenutom uredbom.

Literatura

[1] Elektronski registar i evidencija sertifikacionih tela u Republici Srbiji: http://epotpis.mtt.gov.rs/elektronski-potpis.

[2] Zakon o elektronskom potpisu ("Službeni glasnik Republike Srbije", br. 135/2004).

[3] Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata ("Službeni glasnik Republike Srbije", br. 26/2008).

[4] Politika sertifikacije Sertifikacionog tela Javnog preduzeća "Pošta Srbije" za kvalifikovane elektronske sertifikate ("Službeni PTT glasnik", br. 908, 31.3.2014.).

[5] Praktična pravila pružanja usluge sertifikacije Sertifikacionog tela Javnog preduzeća "Pošta Srbije"za kvalifikovane elektronske sertifikate ("Službeni PTT glasnik", br. 908, 31.3.2014.).

[6] RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[7] D. Spasić, "Profil kvalifikovanog elektronskog sertifikata", XVI telekomunikacioni forum "Telfor 2008", Zbornik radova (medijum je CD-ROM), Društvo za telekomunikacije, Beograd, novembar 2008.

[8] Web strana Sertifikacionog tela Pošte: http://www.ca.posta.rs.

[9] D. Spasić, M. Kujačić, "Operacije za promenu statusa elektronskih sertifikata Sertifikacionog tela Pošte", XXVI simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2008", Zbornik radova, str. 197-206, Saobraćajni fakultet, Beograd, decembar 2008.

[10] Korisničko uputstvo za rad na aplikaciji za registrovanje korisnika elektronskih sertifikata ("RA aplikacija") na šalterima Postnet pošta, Sertifikaciono telo Pošte, verzija 1.0, oktobar 2006.

[11] Portala Poreske uprave "e-Porezi": https://eporezi.poreskauprava.gov.rs.

[12] Pravilnik o poreskoj prijavi za porez po odbitku ("Službeni glasnik Republike Srbije", br. 74/2013, 118/2013).

[13] Pristup Portalu Poreske uprave korišćenjem kvalifikovanog elektronskog sertifikata, Sertifikaciono telo Pošte, verzija 1.3, februar 2014. (http://www.ca.posta.rs/dokumentacija).

[14] Kvalifikovani sertifikat Pošte, Linux i portal e-porezi Poreske uprave: http://www.elitesecurity.org/t474616.

[15] Elektronski registar izdavalaca vremenskog žiga u Republici Srbiji: http://epotpis.mtt.gov.rs/vremenski-zig.
[16] Zakon o elektronskom dokumentu ("Službeni glasnik Republike Srbije", br. 51/2009).
[17] Pravilnik o izdavanju vremenskog žiga ("Službeni glasnik Republike Srbije", br. 112/2009).
[18] Politika izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" kao izdavaoca vremenskog žiga ("Službeni PTT glasnik", br. 782/2012).
[19] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", August 2001.
[20] 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.
[21] 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.
[22] 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.
[23] D. Spasić, S. Milinković, B. Milojković, "Serbian Post Time-Stamping Authority", Metalurgia International, Vol. 18, No. 7, 2013, pp. 86-92, ISSN: 1582-2214.
[24] D. Spasić, I. Lazarević, S. Milinković, B. Milojković, "Time-Stamp klijent aplikacija i testni TSA server Pošte Srbije", XXXI simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2013", Zbornik radova, str. 99-108, Saobraćajni fakultet, Beograd, decembar 2013.
[25] D. Spasić, "Prilog istraživanju sistema za vremensko žigosanje", doktorska disertacija, Računarski fakultet Univerziteta Union, Beograd, jun 2014.
[26] Uputstvo o elektronskom kancelarijskom poslovanju ("Službeni glasnik Republike Srbije", br. 102/2010).
[27] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Abstract: *Serbian Post Certification Authority is issuing electronic certificates to users who are both legal and natural persons. For the purpose of registration of certificate users, employees at the Serbian Post Certification Authority are using an application called RA (Registration Authority) application. This paper provides an overview of the functionality of RA application and lists suggestions for its improvement.*

Key words: *Electronic Signature Act, Certification Authority - CA, Registration Authority - RA, electronic certificates.*

APPLICATION FOR REGISTRATION OF SERBIAN POST CERTIFICATION AUTHORITY ELECTRONIC CERTIFICATE USERS

Dragan Spasić, Dragana Graovac