*XXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2008**, Beograd, 16. i 17. decembar 2008.*

OPERACIJE ZA PROMENU STATUSA ELEKTRONSKIH SERTIFIKATA SERTIFIKACIONOG TELA POŠTE

Dragan Spasić[1], Momčilo Kujačić[2]
[1]Javno preduzeće PTT saobraćaja "Srbija"
[2]Fakultet tehničkih nauka u Novom Sadu

Sadržaj: *U radu su objašnjene operacije za promenu statusa elektronskih sertifikata koje može da izvršava Sertifikaciono telo Pošte: opoziv sertifikata, suspenzija i prekid suspenzije sertifikata, obnova korisničkog profila, promena imena, prezimena i E-mail adrese korisnika sertifikata.*

Ključne reči: *Zakon o elektronskom potpisu, Sertifikaciono telo - CA, elektronski (digitalni) sertifikati.*

1. Uvod

Javno preduzeće PTT saobraćaja "Srbija" je izgradilo javno sertifikaciono telo za izdavanje elektronskih i kvalifikovanih elektronskih sertifikata, koje se zove Sertifikaciono telo Pošte (http://www.cepp.co.yu/ca). Sertifikaciono telo Pošte je izgrađeno u skladu sa Evropskom Direktivom o elektronskom potpisu 1999/93/EC, srpskim Zakonom o elektronskom potpisu ("Sl. glasnik RS", br. 135/2004) i podzakonskim aktima tj. Pravilnicima o elektronskom potpisu. Ministarstvo za telekomunikacije i informatičko društvo upisalo je Javno preduzeće PTT saobraćaja "Srbija" - Sertifikaciono telo Pošte u Evidenciju sertifikacionih tela, pod rednim brojem 1, Rešenjem broj 345-01-00273/2008-01 od 26.5.2008. godine. Sledeći cilj Pošte kao sertifikacionog tela je da se registruje za izdavanje kvalifikovanih elektronskih sertifikata i počne da izdaje kvalifikovane elektronske sertifikate za potrebe javnih elektronskih Internet servisa u Republici Srbiji (tu se pre svega misli na servise e-Uprave tj. e-Government-a i servise e-Trgovine tj. e-Commerce-a). Prvi korak ka tom cilju Pošta je uradila dana 25.9.2008. godine podnošenjem Zahteva za upis u Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata, pomenutom Ministarstvu.

Sertifikaciono telo Pošte izdaje sledeće četiri (4) kategorije elektronskih sertifikata zainteresovanim korisnicima (pravnim i fizičkim licima) [1, 2]:

1. **WEB sertifikate**,
2. **SID Enterprise sertifikate** (Single application ID),
3. **MID Enterprise sertifikate** (Multiple application ID),
4. **SER sertifikate za Web servere**.

Kada Sertifikaciono telo Pošte bude bilo upisano u Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji, počeće da izdaje i **kvalifikovane sertifikate** (slika 1.).

Slika 1. Kvalifikovani sertifikat

Nad izdatim sertifikatima mogu da se sprovedu sledeće operacije za promenu statusa sertifikata [1, 2, 3, 4]:

1. Produženje korišćenja sertifikata za željeni broj godina, maksimalno do roka važnosti sertifikata.
2. Opoziv sertifikata.
3. Opoziv sertifikata i obnova Entrust profila (samo za SID i MID Enterprise sertifikate, u slučaju kompromitovanja ili sumnje na kompromitovanje tajnog kriptografskog ključa).*
4. Suspenzija sertifikata.
5. Prekid suspenzije sertifikata.
6. Obnova Entrust profila (samo za SID i MID Enterprise sertifikate).
7. Promena imena ili prezimena korisnika (samo za SID i MID Enterprise sertifikate).*
8. Promena E-mail adrese korisnika (samo za SID i MID Enterprise sertifikate).*

Neophodno je pre sprovođenja navedenih operacija označenih zvezdicom (*) izvršiti dešifrovanje prethodno šifrovanih datoteka, elektronskih pisama i transakcija, ako šifrovanje nije izvršeno sa Entrust aplikacijama (na primer: ako je šifrovanje elektronskih pisama izvršeno sa Microsoft Outlook ili Microsoft Outlook Express), jer je posle sprovođenja navedenih operacija dešifrovanje **ne**moguće.

Korisnik, odnosno ovlašćeno lice može da podnese popunjen Zahtev za promenu statusa elektronskog sertifikata fizičkog lica / pravnog lica [3, 4], na jedan od sledeća dva (2) načina:

1. Slanjem elektronski potpisanog Zahteva na adresu: ca@cepp.co.yu. Pri tome, priznaju se samo elektronski potpisani Zahtevi sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
2. Dolaskom u bilo koju poštu (lokalno registraciono telo) koja je ovlašćena za prihvatanje Zahteva.

Korisnik, odnosno ovlašćeno lice može da zahteva suspenziju sertifikata i telefonskim putem, pozivanjem korisničkog servisa Sertifikacionog tela Pošte: 011/3607-888 ili 011/3607-889. Korisnik, odnosno ovlašćeno lice se identifikuje saopštavanjem tajne reči iz Ugovora o izdavanju i korišćenju elektronskog sertifikata za fizičko lice / pravno lice [5, 6].

2. Produženje korišćenja sertifikata za željeni broj godina

Korisnik, odnosno ovlašćeno lice može da naruči sertifikat/e za korišćenje u periodu od jedne (1) do pet (5) godina (**rok korišćenja sertifikata**), pri čemu je **rok važnosti** svakog izdatog sertifikata Sertifikacionog tela Pošte pet (5) godina. Posle isteka roka korišćenja sertifikata, korisnik može da podnese Zahtev i uplati novčani iznos za produženje korišćenja sertifikata [1, 3, 4].

Produženje korišćenja sertifikata, vrši se na sledeći način:

1. Korisnik se identifikuje lično, predaje Zahtev lokalnom registracionom telu Sertifikacionog tela Pošte i plaća novčani iznos za produženje korišćenja sertifikata.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog tela i produžava rok korišćenja sertifikata.

Ukoliko istekne rok korišćenja sertifikata, a korisnik **ne** podnese Zahtev i **ne** uplati novčani iznos za produženje korišćenja sertifikata, Sertifikaciono telo Pošte će sprovesti opoziv sertifikata i podatke o opozvanom sertifikatu će objaviti u registru opozvanih sertifikata (Certificate Revocation List - CRL). Osim toga, Sertifikaciono telo Pošte će deaktivirati nalog korisnika na sistemu i obrisaće sertifikat korisnika iz javnog imenika (direktorijuma), ukoliko je sertifikat bio objavljen u javnom imeniku.

3. Opoziv sertifikata

Opoziv sertifikata, kao i objavljivanje registra opozvanih sertifikata (Certificate Revocation List - CRL) u javnom imeniku (direktorijumu), je posle izdavanja sertifikata, najvažniji posao svakog sertifikacionog tela [7, 8, 9, 10]. Opoziv sertifikata je namenjen trajnom deaktiviranju izdatog sertifikata. Posle opoziva, nije moguće aktivirati sertifikat.

Prema Praktičnim pravilima pružanja usluge sertifikacije Sertifikacionog tela Javnog preduzeća PTT saobraćaja "Srbija" [1], opoziv sertifikata može da zahteva:

- korisnik sertifikata,
- Sertifikaciono telo Pošte,
- nadležni državni organ na osnovu zakona.

Sertifikaciono telo Pošte može da opozove sertifikat iz sledećih razloga:

- gubitka, oštećenja ili zloupotrebe tehničkih sredstava (hardvera ili softvera) ili tajnog kriptografskog ključa korisnika, odnosno kompromitovanja ili sumnje u kompromitovanje tajnog kriptografskog ključa,
- promene podataka u sertifikatu, koje zahtevaju izdavanje novog sertifikata,
- prestanka obavljanja delatnosti korisnika kojem je izdat sertifikat,
- neispunjavanja obaveza korisnika sertifikata određenih Praktičnim pravilima [1] i Ugovorom o izdavanju i korišćenju elektronskog sertifikata za fizičko lice / pravno lice [5, 6],
- naknadnog utvrđivanja da podaci koje je dostavio korisnik pri identifikaciji, nisu tačni,
- iz drugih razloga, na zahtev korisnika.

Opoziv sertifikata usled kompromitovanja ili sumnje u kompromitovanje tajnog kriptografskog ključa, kao i usled promene podataka u sertifikatu, vrši se na sledeći način:

1. Korisnik zahteva opoziv sertifikata po jednoj od sledećih procedura:
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog tela i opoziva postojeći sertifikat (slika 2.).
4. Centralno registraciono telo obaveštava korisnika o opozivu sertifikata elektronskom poštom. U slučaju da korisnik ne poseduje adresu elektronske pošte, obaveštenje o opozivu biće mu poslato poštom na adresu naznačenu u Ugovoru [5, 6].

Sertifikaciono telo Pošte može da se odluči za opoziv sertifikata i bez zahteva korisnika, ukoliko utvrdi da je došlo do kompromitovanja tajnog kriptografskog ključa ili ukoliko proceni da je došlo do promene podataka u sertifikatu, koje zahtevaju izdavanje novog sertifikata.

U slučaju da korisnik ne ispunjava svoje obaveze, Sertifikaciono telo Pošte sprovodi proceduru opoziva sertifikata korisnika posredstvom centralnog registracionog tela:

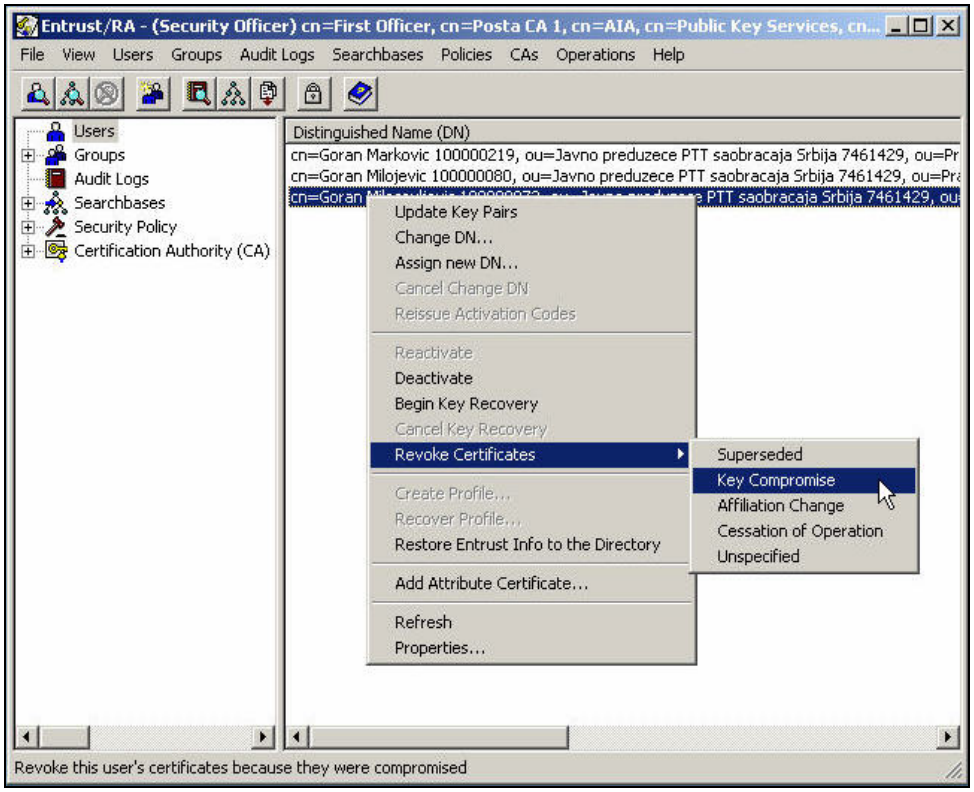
1. Centralno registraciono telo opoziva sertifikat korisnika (slika 2.).
2. Centralno registraciono telo deaktivira korisnika i briše njegove podatke iz javnog imenika.
3. Centralno registraciono telo obaveštava korisnika o opozivu sertifikata elektronskom poštom. U slučaju da korisnik ne poseduje adresu elektronske pošte, obaveštenje o opozivu biće mu poslato poštom na adresu naznačenu u Ugovoru [5, 6].

Posle opoziva sertifikata, korisnik može da zahteva izdavanje **novog** sertifikata, u kom slučaju je dužan da ponovo popuni i potpiše Ugovor o izdavanju i korišćenju elektronskog sertifikata za fizičko lice / pravno lice [5, 6], ispuni zahteve za identifikaciju i ispuni finansijske obaveze prema cenovniku Sertifikacionog tela Pošte.

4. Opoziv sertifikata i obnova Entrust profila

Korisnik SID ili MID Enterprise sertifikata u slučaju kompromitovanja ili sumnje u kompromitovanje tajnog kriptografskog ključa, može da zahteva opoziv sertifikata i obnovu Entrust profila. Opoziv sertifikata i obnova Entrust profila sprovodi se korišćenjem PKIX-CMP protokola [11], na sledeći način:

1. Korisnik podnosi Zahtev za opoziv sertifikata i obnovu Entrust profila po jednoj od sledećih procedura:
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog tela, opoziva postojeći sertifikat (slika 2.) i vrši obnovu Entrust profila.
4. Centralno registraciono telo šalje korisniku novi referentni broj elektronskom poštom, a autorizacioni kod dostavlja korisniku redovnom poštom na adresu naznačenu u Zahtevu. Ukoliko korisnik ne poseduje adresu elektronske pošte, i referentni broj i autorizacioni kod će mu biti dostavljeni odvojenim pošiljkama na adresu naznačenu u Zahtevu.
5. Korisnik preuzima sertifikat tj. sprovodi obnovu Entrust profila (slika 3.).



Slika 2. Centralno registraciono telo opoziva sertifikat

Slika 3. Startovanje *Wizard*-a za obnovu Entrust profila korisnika iz *System tray*-a

5. Suspenzija sertifikata i prekid suspenzije sertifikata

Suspenzija je namenjena deaktiviranju izdatog sertifikata na određeno vreme [1, 9]. Sertifikaciono telo Pošte može da suspenduje sertifikat u toku proveravanja okolnosti u vezi sa mogućim opozivom sertifikata. Prekidom (ukidanjem) suspenzije, sertifikat postaje aktivan, tako da ima sve funkcionalnosti koje je imao i pre suspenzije.

Prema Praktičnim pravilima [1], suspenziju sertifikata može da zahteva:

- korisnik sertifikata,
- Sertifikaciono telo Pošte,
- nadležni državni organ na osnovu zakona.

Prekid suspenzije može da zahteva [1]:

- korisnik sertifikata, kada ustanovi da su razlozi za suspenziju prestali,
- Sertifikaciono telo Pošte, kada ustanovi da su razlozi za suspenziju prestali,
- nadležni državni organ, na osnovu zakona.

Suspenzija ili prekid suspenzije sertifikata, vrši se na sledeći način:

1. Korisnik podnosi Zahtev za suspenziju ili prekid suspenzije sertifikata po jednoj od sledećih procedura:
   - Korisnik telefonom poziva centralno registraciono telo i identifikuje se saopštavanjem tajne reči upisanoj na Ugovoru (važi samo za suspenziju sertifikata).
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog tela i izvršava suspenziju ili prekid suspenzije sertifikata.

6. Obnova entrust profila

Obnova Entrust profila, moguća je samo za SID i MID Enterprise sertifikate korišćenjem PKIX-CMP protokola [11], a sprovodi se po zahtevu korisnika sertifikata u slučaju kada je:

- Korisnik zaboravio lozinku za pristup Entrust profilu.
- Entrust profil korisnika izgubljen, greškom obrisan ili oštećen. Ukoliko je Entrust profil izgubljen pri čemu postoji sumnja da bi neko mogao da dođe u posed Entrust profila, korisnik je dužan da zahteva opoziv sertifikata ili opoziv sertifikata i obnovu Entrust profila. Ako je Entrust profil izgubljen tako što je nepovratno uništen, nije potrebno zahtevati opoziv sertifikata.

Obnova Entrust profila, vrši se na sledeći način:

1. Korisnik predaje Zahtev za obnovu Entrust profila po jednoj od sledećih procedura:
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.

2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog tela i vrši obnovu Entrust profila.
4. Centralno registraciono telo šalje korisniku novi referentni broj elektronskom poštom, a autorizacioni kod dostavlja korisniku redovnom poštom na adresu naznačenu u Zahtevu. Ukoliko korisnik ne poseduje adresu elektronske pošte, i referentni broj i autorizacioni kod će mu biti dostavljeni odvojenim pošiljkama na adresu naznačenu u Zahtevu.
5. Korisnik preuzima sertifikat tj. sprovodi obnovu Entrust profila (slika 3.).

7. Promena imena ili prezimena korisnika

Korisnik SID ili MID Enterprise sertifikata, u slučaju promene imena ili prezimena, može da zahteva promenu imena ili prezimena korisnika u sertifikatu. Promena imena ili prezimena korisnika u sertifikatu, sprovodi se korišćenjem PKIX-CMP protokola [11], na sledeći način:

1. Korisnik podnosi Zahtev za promenu imena ili prezimena korisnika po jednoj od sledećih procedura:
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog i vrši promenu imena ili prezimena korisnika u sertifikatu.
4. Pri prvoj sledećoj prijavi (logovanju) korisnika na korisničku aplikaciju Entrust Entelligence (slika 4.), korisnik automatski preuzima novi sertifikat sa promenjenim imenom ili prezimenom.

Korisnik u Zahtevu [3, 4] **ne** može, umesto imena ili prezimena korisnika iz Ugovora [5, 6], da navede ime ili prezime drugog lica.

Slika 4. Prijavljivanje korisnika na aplikaciju Entrust Entelligence iz *System tray*-a

8. Promena E-mail adrese korisnika

Korisnik SID ili MID Enterprise sertifikata, u slučaju promene adrese elektronske pošte, može da zahteva promenu adrese elektronske pošte korisnika u sertifikatu. Promena adrese elektronske pošte korisnika u sertifikatu, sprovodi se korišćenjem PKIX-CMP protokola [11], na sledeći način:

1. Korisnik podnosi Zahtev za promenu adrese elektronske pošte po jednoj od sledećih procedura:
   - Korisnik šalje elektronski potpisan Zahtev elektronskom poštom centralnom registracionom telu. Centralno registraciono telo priznaje samo elektronski potpisane Zahteve sa važećim sertifikatom izdatim od strane Sertifikacionog tela Pošte.
   - Korisnik se identifikuje lično i predaje Zahtev lokalnom registracionom telu.
2. Posle uspešne identifikacije korisnika, lokalno registraciono telo šalje Zahtev centralnom registracionom telu.
3. Centralno registraciono telo proverava Zahtev dobijen od lokalnog registracionog i vrši promenu adrese elektronske pošte korisnika u sertifikatu.
4. Pri prvoj sledećoj prijavi (logovanju) korisnika na korisničku aplikaciju Entrust Entelligence (slika 4.), korisnik automatski preuzima novi sertifikat sa promenjenom adresom elektronske pošte.

Korisnik u Zahtevu [3, 4] **ne** može, umesto adrese elektronske pošte korisnika iz Ugovora [5, 6], da navede adresu elektronske pošte drugog lica.

Literatura

[1] "Praktična pravila pružanja usluge sertifikacije Sertifikacionog tela Javnog preduzeća PTT saobraćaja "Srbija"", oktobar 2008. godine. Napomena: Stupanjem na snagu Praktičnih pravila prestaje da važi "Pravilnik o elektronskim sertifikatima Javnog preduzeća PTT saobraćaja "Srbija"", "Službeni PTT glasnik", broj 341, 8.10.2004. godine (http://www.cepp.co.yu/ca).

[2] Web strana Sertifikacionog tela Pošte: http://www.cepp.co.yu/ca.

[3] "Zahtev za promenu statusa elektronskog sertifikata fizičkog lica", Sertifikaciono telo Pošte (http://www.cepp.co.yu/ca/dokumentacija).

[4] "Zahtev za promenu statusa elektronskog sertifikata pravnog lica", Sertifikaciono telo Pošte (http://www.cepp.co.yu/ca/dokumentacija).

[5] "Ugovor o izdavanju i korišćenju elektronskog sertifikata za fizičko lice", Sertifikaciono telo Pošte (http://www.cepp.co.yu/ca/dokumentacija).

[6] "Ugovor o izdavanju i korišćenju elektronskog sertifikata za pravno lice", Sertifikaciono telo Pošte (http://www.cepp.co.yu/ca/dokumentacija).

[7] "Zakon o elektronskom potpisu" ("Sl. glasnik RS", br. 135/2004).

[8] "Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata" ("Sl. glasnik RS", br. 26/2008).

[9] D. Spasić, "Registri opozvanih sertifikata Sertifikacionog tela Pošte", XII festival informatičkih dostignuća "Infofest 2005", Zbornik radova, str. 57-64, Republički

sekretarijat za razvoj Republike Crne Gore i kompanija Biznis Link, Budva, septembar-oktobar 2005.
[10] D. Spasić, "Provera opozvanosti sertifikata u okviru različitih aplikacija", VI međunarodni simpozijum o elektronskoj trgovini i elektronskom poslovanju "E-trgovina 2006", Zbornik radova (medijum je CD-ROM), Agencija "E-trgovina", Palić, april 2006.
[11] C. Adams, S. Farrell, T. Kause, T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210 (Obsoletes RFC 2510), September 2005.

Abstract: *This paper describes operations for the changing status of digital certificates that can perform Post Serbia Certification Authority: revoking a certificate, suspending and cancel suspending a certificate, recovering a user's profile, changing a user's name, surname and E-mail address within a certificate.*

Key words: *Electronic Signature Act, Certification Authority - CA, electronic (digital) certificates.*

POST SERBIA CERTIFICATION AUTHORITY OPERATIONS FOR THE CHANGING ELECTRONIC CERTIFICATES STATUS

Dragan Spasić, Momčilo Kujačić