# PRAVNI I TEHNIČKI ASPEKTI KVALIFIKOVANOSTI ELEKTRONSKOG POTPISA PREMA ZAKONU O ELEKTRONSKOM POTPISU RS I AKTUELNIM PRAVILNICIMA
# LEGAL AND TEHNICAL ASPECTS THAT DESCRIBE QUALIFIED ELECTRONIC SIGNATURE ACCORDING TO ELECTRONIC SIGNATURE LAW OF REPUBLIC OF SRPSKA AND CURRENT REGULATIONS

*Milan Latinović, Srđan Rajčević, Saša Vojnović, Agencija za informaciono društvo Republike Srpske*

**Sadržaj** – *U ovom radu opisani su pravni i tehnički aspekti kvalifikovanosti elektronskog potpisa prema Zakonu o elektronskom potpisu i aktuelnim pravilnicima. Zakon o elektronskom potpisu Republike Srpske definiše elektronski potpis i kvalifikovani elektronski potpis kao dva stepena ispunjenosti pomenutih pravnih i tehničkih aspekata. Ovaj rad razmatra zahtjeve za kvalifikovanost kroz analizu postojećeg zakonodavstva i načine provjere te kvalifikovanosti. Cilj ovog rada jeste jasno definisanje pojmova elektronskog potpisa i kvalifikovanog elektronskog potpisa, definisanje ključnih zahtjeva za kvalifikovanost koji se odnose na certifikaciona tijela i analiza mehanizama za provjeru kvalifikovanosti sa stanovišta krajnjeg korisnika.*

**Abstract** – *This paper describes the legal and technical aspects of the qualification of electronic signatures under the Electronic Signature Law and the current regulations. Electronic Signature Law of the Republic of Srpska defines an electronic signature and the qualified electronic signature as two different degrees of fulfillment of these legal and technical aspects. This paper discusses the requirements for qualification through the analysis of existing legislation and methods of assessment and qualifications. The aim of this paper is to clearly define the concepts of electronic signature and qualified electronic signature, defining the key requirements for qualifications relating to certification bodies and analysis of mechanisms for verification of eligibility from the standpoint of the end user.*

## 1. UVOD

Informaciono društvo bazira se na kreiranju, arhiviranju, distribuciji i manipulaciji informacijama u svrhu generisanja i eksploatacije znanja. Svaki vid kreiranja ili upotrebe informacija povlači za sobom neophodnost provjere autentičnosti, neporecivosti i integriteta informacija i učesnika u komunikaciji ili poslovanju.

Tradicionalno poslovanje oslanja se na pisanu formu potvrde identiteta učesnika, odnosno lični potpis i otisak pečata. Stalni razvoj informacionih i komunikacionih tehnologija (IKT) omogućio je novi vid poslovanja upotrebom pomenutih tehnologija, odnosno elektronsko poslovanje (*eng. E-business*) gdje se potvrda identiteta učesnika vrši putem elektronskog potpisa (*eng. electronic signature*).

Na osnovu člana 2, stav 1, tačka a) Zakona o elektronskom potpisu Republike Srpske, elektronski potpis predstavlja *„skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i autentičnost potpisanog elektronskog dokumenta“*. [1] Isto tako, prema gore navedenom stavu, tačka b) kvalifikovani elektronski potpis predstavlja *„elektronski potpis kojim se pouzdano garantuje identitet potpisnika i koji ispunjava uslove iz člana 4. ovog zakona“*.

Takođe, prema članu 5. stav 1 Zakona o elektronskom potpisu Republike Srpske *„kvalifikovani elektronski potpis ima istu pravnu snagu i ravnopravan je sa pisanom formom, odnosno ličnim potpisom i otiskom pečata ako je izrađen u skladu sa odredbama ovog zakona, te ako su ispunjeni ostali uslovi propisani ovim zakonom i propisima koji su doneseni na osnovu ovog zakona“*. [1]

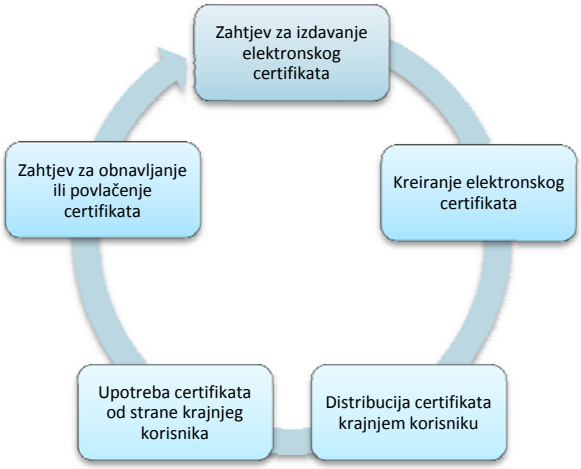
Dakle, Zakon o elektronskom potpisu Republike Srpske razlikuje elektronski potpis i kvalifikovani elektronski potpis, pri čemu jedino kvalifikovani elektronski potpis ima istu pravnu snagu kao lični potpis i otisak pečata.

Shodno navedenom, ovaj rad razlikuje certifikaciona tijela i certifikaciona tijela za izdavanje kvalifikovanih elektronskih certifikata. Cilj ovog rada jeste analiza pravnih i tehničkih aspekata koje certifikaciono tijelo i korisnik certifikata trebaju ispuniti da bi se osigurala kvalifikovanost, tj. pravna snaga elektronskog potpisa.

Pored [1] postoje i sljedeći podzakonski akti: [2], [3], [4], [5] i [6], od kojih su [2] i [3] ključni za analizu kojom se bavi ovaj rad.

## 2. ŽIVOTNI CIKLUS ELEKTRONSKOG CERTIFIKATA

Kompletan životni ciklus elektronskog certifikata odvija se unutar infrastrukture javnog ključa *(eng. Public Key Infrastructure – PKI*), unutar koje razlikujemo osnovne komponente: politika sertifikacije (*eng. Certificate Policy - CP*), praktična pravila rada (*eng. Certificate Practice Statement – CPS*), certifikaciono tijelo (*eng. Certificate Authority – CA*), registraciono tijelo (*eng. Registration Authority – RA*), sistemi za distribuciju sertifikata (*eng. Certificate Distribution Systems – CDS*) i PKI aplikacije.

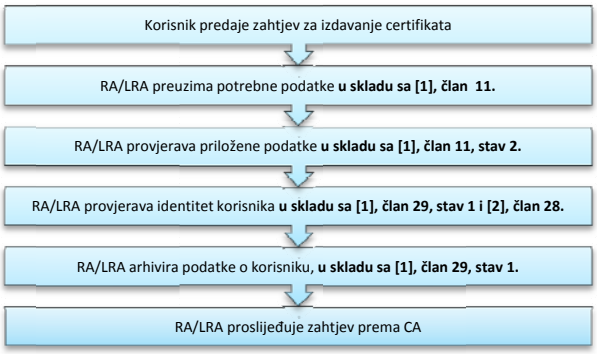



**Slika 2.1.** – Životni ciklus elektronskog certifikata

Na slici 2.1. prikazan je životni ciklus elektronskog certifikata, koji počinje sa zahtjevom za izdavanje certifikata, a završava zahtjevom za obnavljanje ili povlačenje certifikata, zavisno od pravilnika certifikacionog tijela (*eng. Certificate Authority – CA*) i samog zahtjeva korisnika. Svaka od faza navedenog ciklusa zahtjeva postojanje adekvatnih procedura propraćenih hardverskom i softverskom osnovom koja je usklađena sa zakonom i pravilnicima.

Početna faza životnog ciklusa elektronskog certifikata, tj. zahtjev za izdavanje certifikata razložen je na sljedeće komponente i prikazan na slici 2.2. Nakon što korisnik (budući potpisnik) preda zahtjev za izdavanje certifikata, RA ili lokalno registraciono tijelo (eng. *Local Registration Authority – LRA*) treba da izvrši provjeru priloženih podataka, tj. zahtjeva za izdavanje certifikata i ovjerene kopije lične karte.

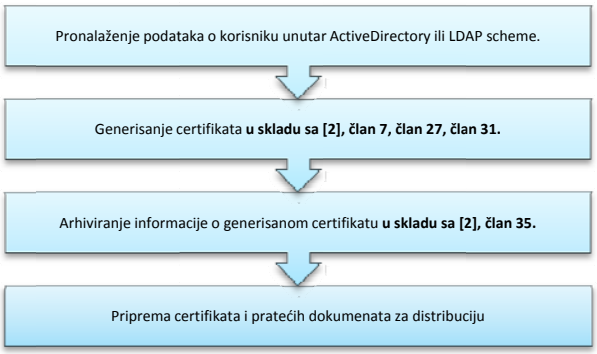
Na osnovu [1], član 11, stav 2. tačka c) identifikacioni skup podataka o potpisniku čine: lično ime; ime oca ili majke; prezime; nadimak, ako ga lice ima; datum rođenja; prebivalište, odnosno boravište.




**Slika 2.2.** – Zahtjev za izdavanje certifikata

Podaci o javnom matičnom broju građanina (JMBG), broj lične karte, datum izdavanja lične karte, datum isteka lične karte, nadležni organ za izdavanje lične karte preuzimaju se sa ovjerene kopije lične karte koja se prilaže u sklopu zahtjeva za izdavanje certifikata.

Arhiviranje podataka o korisniku pominje se u [1], član 29, stav 1. tačka z), na osnovu čega se svi podaci i dokumentacija o izdatim certifikatima arhiviraju najmanje deset godina, pri čemu podaci i prateća dokumentacija mogu biti i u elektronskom obliku.




**Slika 2.3.** – Kreiranje elektronskog certifikata

Na slici 2.3. prikazana je faza kreiranja elektronskog certifikata koja zajedno sa fazom distribucije certifikata krajnjem korisniku predstavlja najveći izazov za ispunjavanje pravnih i tehničkih aspekata kvalifikovanosti elektronskih certifikata opisanih zakonom i pravilnicima.

Prilikom generisanja elektronskog certifikata neophodno je obratiti pažnju na sljedeće aspekte:

- dužina kriptografskih ključeva i upotreba odgovarajućih kriptografskih modula;
- struktura elektronskog certifikata u skladu sa X.509 v3; i
- fizički medij na kom se skladišti elektronski certifikat i generiše privatni ključ.

Na osnovu [2], član 7, stav 1. da bi kreirani elektronski potpis bio kvalifikovan dužina ključa za izradu kvalifikovanog elektronskog potpisa (privatnog ključa) mora biti dužine najmanje 1024 bita, uz primjenu kriptografskih algoritama iz klase RSA (*eng. Rivest, Shamir and Adleman*) / DSA (eng. *Digital Signature Algorithm*).

Isto tako, prema [2], član 31, stav 2. definiše osnovne elemente koje certifikat obavezno sadrži. Pregledom ovih elemenata može se zaključiti da je ovaj član pravilnika ustvari zahtjev za upotrebom X.509 strukture.

Neophodno je napomenuti da prilikom kreiranja i upotrebe elektronskog certifikata, ne smije postojati tehnička mogućnost umnožavanja sredstva za izradu elektronskog potpisa, odnosno privatnog ključa. Ovdje se postavlja pitanje medija za skladištenje elektronskog certifikata.

Dakle, elektronski certifikat moguće je skladištiti na nekoliko načina:

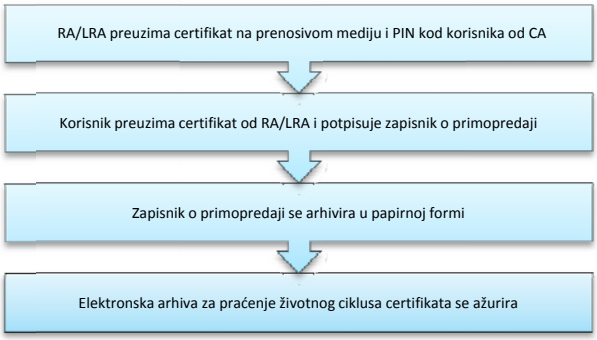
- elektronski certifikati na hard disku (nalaze se unutar repozitorija certifikata koji posjeduje operativni sistem računara);
- elektronski certifikati na prenosivim medijima (smart kartice, tokeni).

U slučaju generisanja elektronskog certifikata na hard disku korisnika kompletna sigurnost i mobilnost elektronskog certifikata vezana je za radnu stanicu korisnika. Dakle, ako radna stanica korisnika **nije adekvatno zaštićena** (lozinka za pristup operativnom sistemu, biometrijska kontrola i sl.) svako lice koje pristupi operativnom sistemu može zloupotrebiti elektronski certifikat. Ovaj problem može se riješiti postavljanjem dodatne lozinke čija se provjera inicira prilikom svake upotrebe elektronskog certifikata.

Generisanje certifikata na hard disku stvara i problem mobilnosti, pošto je korisnički certifikat fizički vezan za repozitorij jedne radne stanice i korisnik ga ne može koristiti za ostalim radnim stanicama (npr. korisnici koji za obavljanje posla koriste dvije ili više radnih stanica, korisnici koji imaju potrebu da koriste elektronski certifikat van prostorija unutar kojih rade, upotreba elektronskih certifikata na terenu ili od kuće). Ako se korisniku (ili u tu svrhu lokalnom administratoru) omogući kopiranje certifikata i njegovo prenošenje na druge radne stanice tada elektronski certifikat postaje nekvalifikovan čim se prvi put napravi kopija. Shodno navedenom, generisanje kvalifikovanog certifikata na hard disk (lokalnu radnu stanicu) nije u skladu sa pravnim i tehničkim normama.

Generisanjem certifikata na prenosive medije postiže se mobilnost koja je izgubljena prilikom kreiranja certifikata na hard disku. U ovom slučaju elektronski certifikat je trajno vezan za prenosivi medij (npr. smart karticu) koja postaje svojevrsni identifikacioni dokument korisnika, pri čemu ispunjava kriterije jedinstvenosti i mobilnosti.

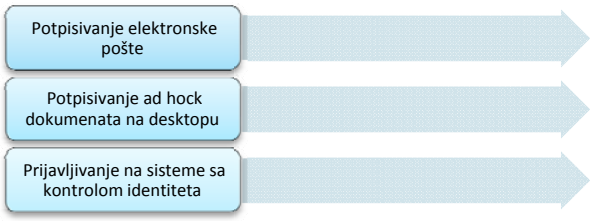
Prilikom kreiranja certifikata na prenosive medije **neophodno je generisati privatni ključ direktno na smart karticu ili token bez mogućnosti preuzimanja privatnog ključa sa upotrebnog medija**. U slučaju da CA kreira elektronski certifikat na smart karticu ili token tako što ga prvo kreira unutar nekog lokalnog repozitorija u koji arhivira i privatni ključ, a tek nakon toga vrši njegovo kopiranje na smart karticu ili token, elektronski potpis kreiran upotrebom ovog elektronskog certifikata neće biti kvalifikovan.




**Slika 2.4.** – Distribucija certifikata krajnjem korisniku

Proces preuzimanja certifikata od strane krajnjeg korisnika prikazan je na slici 2.4., pri čemu se pretpostavlja da je struktura certifikacionog tijela takva da je za distribuciju certifikata zaduženo RA/LRA. Ključni aspekti preuzimanja certifikata jesu uspostavljanje procedure koja onemogućava upotrebu certifikata u toku njegovog dostavljanja do krajnjeg korisnika i obavezno postojanje zapisnika o primopredaji koji korisnik potpisuje prilikom preuzimanja certifikata.

Najčešći slučajevi upotrebe certifikata od strane korisnika prikazani su na slici 2.5. što podrazumijeva: potpisivanje elektronske pošte; potpisivanje ad hock dokumenata na desktopu i prijavljivanje korisnika na sisteme sa kontrolom identiteta. Samo certifikaciono tijelo dužno je da obezbjedi korisniku adekvatan hardver i softver koji omogućava ispunjavanje ovih osnovnih slučajeva upotrebe. Potrebno je napomenuti da od momenta preuzimanja certifikata, prema [1], korisnik preuzima potpunu odgovornost za upotrebu i eventualnu zloupotrebu istog.




**Slika 2.5.** – Upotreba certifikata od strane krajnjeg korisnika

Kada se razmatra finalna faza životnog ciklusa certifikata, tj. njegovo obnavljanje ili opoziv (povlačenje certifikata), prema [2], član 10, stav 2., iskazuje potrebu za postojanjem procedure opoziva certifikata koja se opisuje unutar Internog pravilnika certifikacionog tijela.

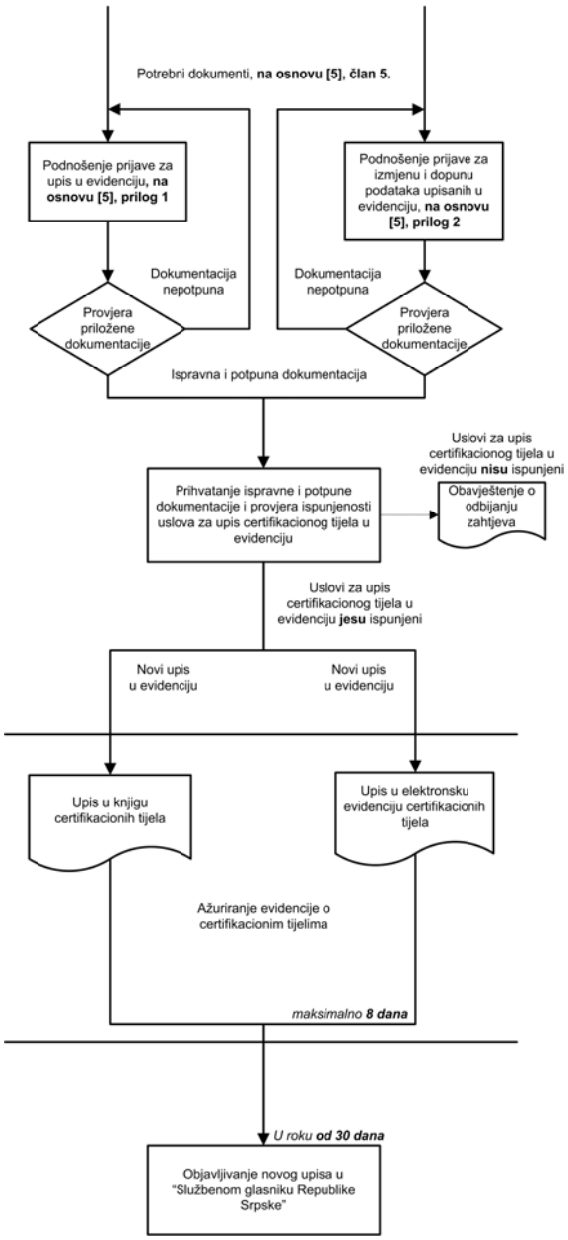
Isto tako, u sklopu [2], član 32., govori se o politici opoziva certifikata, kao sastavnom dijelu pravilnika o postupcima certifikacije (eng. *Certificate Policy – CP*).

Unutar [2] ne defineše se konkretna procedura opoziva certifikata i tehnička sredstva za sprovođenje ove procedure. Ipak, evidentno je da se pomenuta procedura mora sastojati iz sljedećih koraka: identifikovanje razloga opoziva certifikata, provjera identiteta korisnika čiji se certifikat opoziva, vođenje evidencije opozvanih certifikata i periodično kreiranje liste povučenih certifikata (eng. *Certificate Revoked List – CRL*), koja je javno dostupna.

## 3. PROCES EVIDENCIJE I REGISTRACIJE CERTIFIKACIONIH TIJELA

Na osnovu [1], [5], član 2, stav 1., certifikaciono tijelo prije početka obavljanja usluga certifikacije podnosi prijavu za upis u evidenciju, čiji je sadržaj javno dostupan. Slika 3.1. ima za cilj da ilustruje proces evidencije certifikacionog tijela u skladu sa kompletnim [5].

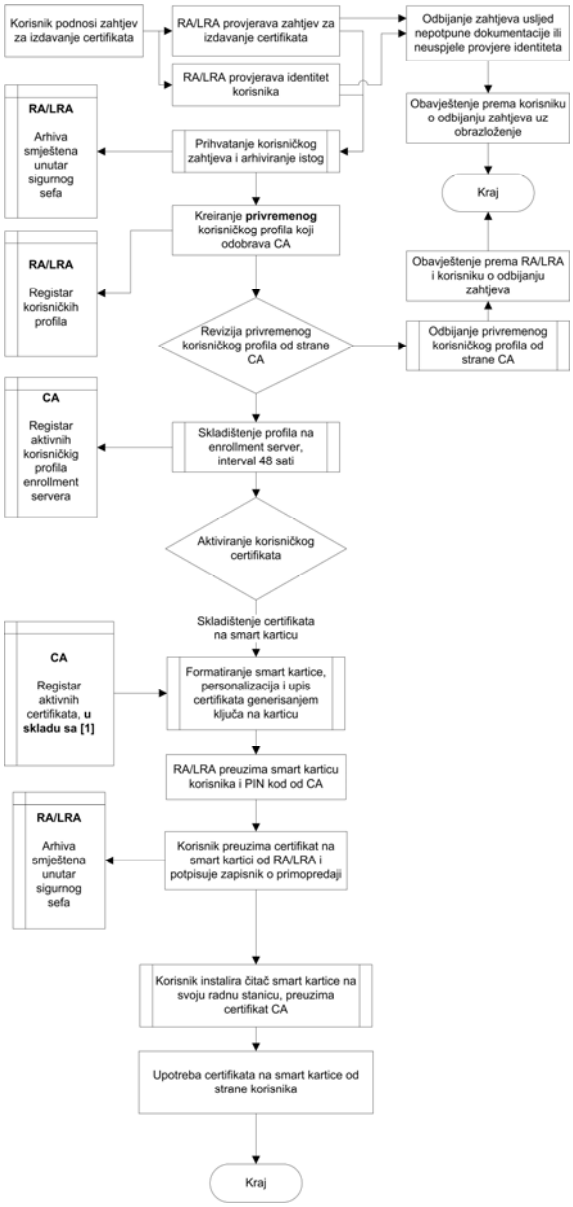
Isto tako, na osnovu [4] certifikaciona tijela za izdavanje kvalifikovanih elektronskih certifikata dužna su podnijeti zahtjev za upis u registar, prije početka izdavanja kvalifikovanih certifikata.




**Slika 3.1.** – Proces evidencije certifikacionog tijela, **u skladu sa [5]**

## 4. PROCES KREIRANJA KVALIFIKOVANIH CERTIFIKATA GENERISANJEM PRIVATNOG KLJUČA DIREKTNO NA SMART KARTICI

Uzevši u obzir već opisani životni ciklus elektronskog certifikata jasno se vidi da se kao jedan od ključnih izazova postavlja kreiranje kvalifikovanih certifikata, tj. formiranje procedure koja omogućava kreiranje kvalifikovanih certifikata generisanjem privatnog ključa direktno na smart kartici. Takođe, može se primjetiti da je, u cilju ispunjavanja pravnih i tehničkih aspekta zakona i podzakonskih akata, potrebno posjedovati repozitorije podataka (arhive, registre i sl.) koji predstavljaju ključne tačke u procesu kreiranja jednog kvalifikovanoh certifikata.




**Slika 4.1.** – Teorijski prikaz procedure kreiranja kvalifikovanog certifikata

Na slici 4.1. teorijski je prikazan dijagram jedne od mogućih procedura kreiranja kvalifikovanih elektronskih certifikata, generisanjem privatnog ključa direktno na smart kartici.

Važno je napomenuti da prikazana procedura obuhvata sve pravne i tehničke aspekte koji su razmatrani u ovom radu. Isto tako, u slučaju praktične realizacije, zavisno od softverskog rješenja za uspostavljanje CA, hardverske platforme, operativnog sistema koji se koristi, kao i vrste smart kartica prikazana procedura može se detaljnije obrazložiti.

## 5. ZAKLJUČAK

Zakonodavstvo Republike Srpske detaljno opisuje pravne i tehničke aspekte koje je potrebno ispuniti prije evidentiranja ili registracije certifikacionog tijela, tj. prije samog početka rada.

Shodno ovome, detaljno poznavanje i tumačenje zakonodavstva u timovima inženjera i pravnika neophodan je preduslov za uspješno realizovanje kompleksnog zadatka uspostavljanja certifikacionog tijela ili certifikacionog tijela za izdavanje kvalifikovanih elektronskih certifikata.

## 6. LITERATURA


[1] Zakon o elektronskom potpisu Republike Srpske („Službeni glasnik Republike Srpske“, br. 59/08)

[2] Pravilnik o mjerama zaštite elektronskog potpisa i kvalifikovanog elektronskog potpisa, najnižem iznosu obaveznog osiguranja i primjeni organizacionih i tehničkih mjera zaštite certifikata („Službeni glasnik Republike Srpske“, br. 88/08)

[3] Pravilnik o tehničkim pravilima za osiguranje povezanosti evidencija izdatih i opozvanih certifikacionih tijela u Republici Srpskoj („Službeni glasnik Republike Srpske“, br. 88/08)

[4] Pravilnik o sadržaju i načinu vođenja registra certifikacionih tijela za izdavanje kvalifikovanih elektronskih certifikata („Službeni glasnik Republike Srpske“, br. 88/08)

[5] Pravilnik o evidenciji certifikacionog tijela („Službeni glasnik Republike Srpske“, br. 88/08)

[6] Uredba o nosiocima poslova elektronske certifikacije („Službeni glasnik Republike Srpske“, br. 114/08)