

ZAKON O ELEKTRONSKOM POTPISU REPUBLIKE SRPSKE

Službeni glasnik Republike Srpske 106/15 od 10.12.2015

GLAVA I OSNOVNE ODREDBE

Član 1.

Ovim zakonom uređuje se pravo fizičkih i pravnih lica na upotrebu elektronskog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obaveze i odgovornosti fizičkih i pravnih lica koja pružaju usluge izrade, verifikacije i validacije elektronskog potpisa, vremenskog žiga, elektronskog pečata i certifikata za autentifikaciju mrežnih stranica na teritoriji Republike Srpske (u daljem tekstu: Republika), ako posebnim zakonom nije drugačije određeno.

Član 2.

Pojedini izrazi koji se koriste u ovom zakonu imaju sljedeće značenje:

- 1) elektronski dokument – jednoobrazno povezan cjelovit skup podataka koji su elektronski oblikovani (izrađeni pomoću računara i drugih elektronskih uređaja), poslani, primljeni ili sačuvani na elektronskom, magnetnom, optičkom ili drugom mediju, i koji sadrži osobine kojima se utvrđuje autor, utvrđuje vjerodostojnost sadržaja, te dokazuje vrijeme kada je dokument sačinjen,
- 2) korisnik – pravno lice, odnosno samostalni preduzetnik ili fizičko lice koje koristi usluge certifikacionog tijela,
- 3) potpisnik – lice koje posjeduje sredstvo za izradu elektronskog potpisa, a koje potpisuje u svoje ime ili u ime pravnog lica, odnosno samostalnog preduzetnika,
- 4) podaci za izradu elektronskog potpisa – jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi koje potpisnik koristi za izradu elektronskog potpisa,
- 5) sredstvo za izradu elektronskog potpisa – odgovarajuća računarska oprema i računarski program koje potpisnik koristi pri izradi elektronskog potpisa,
- 6) sredstvo za izradu kvalifikovanog elektronskog potpisa – odgovarajuća računarska oprema i računarski program koje potpisnik koristi pri izradi elektronskog potpisa i koji ispunjavaju uslove utvrđene ovim zakonom,
- 7) podaci za verifikaciju elektronskog potpisa – podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste radi provjere validnosti elektronskog potpisa,
- 8) sredstvo za verifikaciju elektronskog potpisa – odgovarajuća računarska oprema i računarski program koji se koriste za provjeru podataka za verifikaciju potpisa,
- 9) certifikaciono tijelo – pravno lice, odnosno samostalni preduzetnik koji je registrovan i koji obavlja poslove u skladu sa Zakonom o zanatsko-preduzetničkoj djelatnosti, koje izdaje elektronske certifikate ili pruža druge usluge koje su u vezi sa elektronskim potpisima,
- 10) vremenski žig – zvanično vrijeme pridruženo elektronskom dokumentu ili grupi elektronskih dokumenata kojim se potvrđuje sadržaj elektronskog dokumenta u to vrijeme, odnosno sadržaj svakog dokumenta u grupi,
- 11) elektronski pečat – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku radi osiguranja izvornosti i cjelovitosti tih podataka,
- 12) kvalifikovani elektronski pečat – elektronski pečat koji je kreiran pomoću sredstva za izradu kvalifikovanog elektronskog pečata i koji se zasniva na kvalifikovanom certifikatu za elektronski pečat,

13) autor elektronskog pečata – pravno lice, odnosno samostalni preduzetnik koji kreira elektronski pečat,

14) certifikat za autentifikaciju mrežnih stranica – potvrda pomoću koje je moguće izvršiti autentifikaciju mrežnih stranica, te kojom se mrežne stranice povezuju sa fizičkim ili pravnim licem kojem je izdat certifikat i

15) kvalifikovani certifikat za autentifikaciju mrežnih stranica – potvrda koju je izdalo certifikaciono tijelo i koja ispunjava uslove iz člana 18. ovog zakona.

GLAVA II

ELEKTRONSKI POTPIS I KVALIFIKOVANI ELEKTRONSKI POTPIS

Član 3.

Elektronski potpis je 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.

Član 4.

Kvalifikovani elektronski potpis je elektronski potpis koji:

- 1) je povezan isključivo sa potpisnikom,
- 2) pouzdano identifikuje potpisnika,
- 3) nastaje korištenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika i
- 4) je direktno povezan sa podacima na koje se odnosi i to na način koji nedvosmisleno omogućava uvid u bilo koju izmjenu izvornih podataka.

Član 5.

Kvalifikovani elektronski potpis u odnosu na podatke u elektronskom obliku ima istu pravnu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

Član 6.

(1) Elektronski potpis smatra se pravno valjanim i dopušteno ga je koristiti u sudskim i drugim postupcima ako ispunjava uslove propisane ovim zakonom.

(2) Elektronski potpis se ne može osporavati u sudskim i drugim postupcima isključivo na osnovu toga što je u elektronskom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalifikovani elektronski potpis.

Član 7.

(1) Elektronski potpis izrađuje se sredstvima za izradu elektronskog potpisa.

(2) Kvalifikovan elektronski potpis izrađuje se sredstvima za izradu kvalifikovanog elektronskog potpisa koja moraju da ispunjavaju uslove iz člana 8. ovog zakona.

Član 8.

(1) Sredstvo za izradu kvalifikovanog elektronskog potpisa mora ispunjavati sljedeće uslove:

1) da osigura da se podaci za izradu kvalifikovanog elektronskog potpisa mogu pojaviti samo jednom, te da je obezbijedena njihova tajnost u razumnoj mjeri,

2) da osigura da se podaci za izradu kvalifikovanog elektronskog potpisa ne mogu, uz razumne sigurnosne mjere, ponoviti, te da je potpis zaštićen od falsifikovanja korištenjem postojeće raspoložive tehnologije i

3) da osigura da podaci za izradu kvalifikovanog elektronskog potpisa budu pouzdano zaštićeni od neovlaštenog korištenja od strane trećih lica.

(2) Sredstvo za izradu kvalifikovanog elektronskog potpisa ne može prilikom izrade kvalifikovanog elektronskog potpisa promijeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke prije procesa potpisivanja.

(3) Izuzetno od odredbe stava 1. ovog člana, certifikaciono tijelo koje izdaje kvalifikovane elektronske certifikate i koje upravlja podacima za izradu elektronskog potpisa u ime potpisnika može kopirati podatke za izradu elektronskog potpisa isključivo u svrhu izrade rezervnih kopija, pod uslovom da su ispunjeni sljedeći uslovi:

1) sigurnost kopiranih skupova podataka mora biti na jednakom nivou sigurnosti izvornih skupova podataka i

2) broj kopiranih skupova podataka ne prelazi broj neophodan za osiguravanje kontinuiteta usluge.

(4) Ministar nauke i tehnologije (u daljem tekstu: ministar) pravilnikom propisuje koje se mjere zaštite elektronskog potpisa i kvalifikovanog elektronskog potpisa moraju preduzeti, tehničko-tehnološke postupke za izradu kvalifikovanog elektronskog potpisa i uslove koje treba da ispune sredstva za izradu elektronskog potpisa i kvalifikovanog elektronskog potpisa.

Član 9.

Sredstvo za verifikaciju kvalifikovanog elektronskog potpisa mora ispunjavati sljedeće uslove:

1) mora se osigurati da podaci koji se koriste za verifikaciju elektronskog potpisa odgovaraju podacima prikazanim licu koje obavlja verifikaciju,

2) potpis mora biti pouzdano verifikovan, a rezultat te verifikacije na ispravan način prikazan,

3) lice koje obavlja verifikaciju mora imati mogućnost uvida u sadržaj potpisanih podataka,

4) mora se osigurati pouzdana provjera autentičnosti i valjanosti certifikata koji se zahtijeva u vrijeme provjere potpisa,

5) identitet potpisnika mora biti prikazan na ispravan način,

6) upotreba pseudonima, ako je pseudonim bio korišten u trenutku potpisivanja, mora biti jasno naznačena i

7) mora se osigurati da se pouzdano otkriju bilo kakve promjene u potpisanim podacima.

GLAVA III VREMENSKI ŽIG

Član 10.

Vremenski žig je skup podataka u elektronskom obliku koji povezuje druge podatke u elektronskom obliku sa određenim vremenom i na taj način dokazuje da su ti podaci postojali u to vrijeme.

Član 11.

Kvalifikovani vremenski žig mora ispunjavati sljedeće uslove:

1) mora povezivati datum i vrijeme sa podacima na takav način da se može, u razumnoj mjeri, isključiti mogućnost neovlaštene promjene podataka,

2) mora se zasnivati na izvoru tačnog vremena koji je povezan sa koordinisanim univerzalnim vremenom (UTC engl. Coordinated Universal Time) i

3) mora biti potpisan pomoću kvalifikovanog elektronskog potpisa ili pečaćen pomoću kvalifikovanog elektronskog pečata ili na neki drugi odgovorajući način koji obezbjeđuje jednak nivo sigurnosti.

Član 12.

(1) Certifikaciono tijelo koje izdaje vremenski žig dužno je da, na osnovu zahtjeva za formiranje vremenskog žiga, obezbijedi formiranje propisane strukture podataka vremenskog žiga, kao i pouzdano utvrđivanje vremena njegovog nastanka i elektronsko potpisivanje strukture podataka vremenskog žiga.

(2) Certifikaciono tijelo koje izdaje vremenski žig dužno je da obezbijedi pouzdan sistem skladištenja relevantnih informacija koje se odnose na vremenski žig u propisanom periodu, posebno u svrhu dokazivanja za potrebe određenih postupaka.

(3) Na vremenski žig i s njim povezane usluge primjenjuju se odredbe ovog zakona koje se odnose na certifikat.

(4) Ministar pravilnikom propisuje uslove koje mora da ispunjava sistem za formiranje vremenskog žiga, sadržaj zahtjeva za formiranje vremenskog žiga, sadržaj strukture podataka vremenskog žiga i postupak označavanja vremena koje je sadržano u vremenskom žigu.

GLAVA IV ELEKTRONSKI PEČAT

Član 13.

(1) Elektronski pečat je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji obezbjeđuju autentičnost i cjelovitost tih podataka.

(2) Kvalifikovani elektronski pečat mora ispunjavati sljedeće uslove:

1) mora biti povezan isključivo sa autorom pečata,

2) mora pouzdano identifikovati autora pečata,

3) nastaje korištenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika i

4) mora biti direktno povezan sa podacima na koje se odnosi i to na način koji nedvosmisleno omogućava uvid u bilo koju izmjenu izvornih podataka.

Član 14.

(1) Elektronski pečat smatra se pravno valjanim i dopušteno ga je koristiti u sudskim i drugim postupcima ako ispunjava uslove propisane ovim zakonom.

(2) U pogledu sredstva za izradu kvalifikovanog elektronskog pečata i sredstva za verifikaciju kvalifikovanog elektronskog pečata primjenjuju se odredbe čl. 8. i 9. ovog zakona koje se odnose na kvalifikovani elektronski potpis.

GLAVA V ELEKTRONSKI CERTIFIKATI I CERTIFIKACIONA TIJELA

Član 15.

(1) Elektronski certifikat za elektronski potpis je potvrda u elektronskom obliku koja povezuje podatke za verifikaciju elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.

(2) Elektronski certifikat za elektronski pečat je potvrda u elektronskom obliku koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem, odnosno samostalnim preduzetnikom i potvrđuje naziv tog pravnog lica, odnosno samostalnog preduzetnika.

(3) Elektronski certifikat za autentifikaciju mrežnih stranica je elektronska potvrda pomoću koje je moguće izvršiti autentifikaciju mrežnih stranica i kojom se te mrežne stranice povezuju sa fičkim ili pravnim licem, odnosno samostalnim preduzetnikom kojima je izdat certifikat.

Član 16.

(1) Kvalifikovani elektronski certifikat za elektronski potpis je potvrda u elektronskom obliku kojom certifikaciono tijelo potvrđuje kvalifikovani elektronski potpis.

(2) Kvalifikovani elektronski certifikat iz stava 1. ovog člana mora sadržavati:

- 1) oznaku o tome da je riječ o kvalifikovanom elektronskom certifikatu,
- 2) identifikacioni skup podataka o certifikacionom tijelu koje izdaje kvalifikovani elektronski certifikat, uključujući i naziv države u kojoj ima sjedište, i:
 1. naziv pravnog lica i broj sudskog registra, kada je to primjenljivo, ako elektronski certifikat izdaje pravno lice,
 2. naziv samostalnog preduzetnika ako elektronski certifikat izdaje preduzetnik,
- 3) ime potpisnika ili pseudonim, ako se potpisnik koristi pseudonimom,
- 4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa,
- 5) podatke o početku i kraju važenja elektronskog certifikata,
- 6) identifikacionu oznaku izdatog elektronskog certifikata,
- 7) kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat certifikacionog tijela,
- 8) lokaciju na kojoj je besplatno dostupan certifikat koji podržava kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat iz tačke 7) ovog člana,
- 9) lokaciju usluga koje se mogu koristiti za provjeru statusa kvalifikovanog certifikata,
- 10) informaciju o tome ako su podaci za izradu elektronskog potpisa koji su povezani sa podacima za verifikaciju elektronskog potpisa smješteni u sredstvu za izradu kvalifikovanog elektronskog potpisa.

Član 17.

Kvalifikovani elektronski certifikat za elektronski pečat mora sadržavati:

- 1) oznaku o tome da je certifikat izdat kao kvalifikovani elektronski certifikat za elektronske pečate,
- 2) identifikacioni skup podataka o certifikacionom tijelu koje izdaje kvalifikovani elektronski certifikat, uključujući i naziv države u kojoj ima sjedište, i:
 1. naziv pravnog lica i broj sudskog registra, kada je to primjenljivo, ako elektronski certifikat izdaje pravno lice,
 2. naziv samostalnog preduzetnika, ako elektronski certifikat izdaje preduzetnik,
- 3) naziv autora pečata i, kada je to primjenljivo, registarski broj,
- 4) podatke za verifikaciju elektronskog pečata koji odgovaraju podacima za izradu elektronskog pečata,
- 5) podatke o početku i kraju roka važenja certifikata,
- 6) identifikacionu oznaku izdatog elektronskog certifikata,
- 7) kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat certifikacionog tijela,
- 8) lokaciju na kojoj je besplatno dostupan certifikat koji podržava kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat iz tačke 7) ovog člana,
- 9) lokaciju usluga koje se mogu koristiti za provjeru statusa kvalifikovanog certifikata,

10) informaciju o tome ako su podaci za izradu elektronskog pečata koji su povezani sa podacima za verifikaciju elektronskog pečata smješteni u sredstvu za izradu kvalifikovanog elektronskog pečata.

Član 18.

Kvalifikovani elektronski certifikat za autentifikaciju mrežnih stranica mora sadržavati:

- 1) oznaku o tome da je certifikat izdat kao kvalifikovani elektronski certifikat za autentifikaciju mrežnih stranica,
- 2) identifikacioni skup podataka o certifikacionom tijelu koje izdaje kvalifikovane elektronske certifikate za autentifikaciju mrežnih stranica, uključujući i naziv države u kojoj certifikaciono tijelo ima sjedište, i:
 1. naziv pravnog lica i broj sudskog registra, kada je to primjenljivo, ako elektronski certifikat izdaje pravno lice,
 2. naziv samostalnog preduzetnika, ako elektronski certifikat izdaje samostalni preduzetnik,
- 3) identifikacioni skup podataka o korisniku certifikata:
 1. najmanje ime lica kojem je izdat certifikat ili pseudonim, ako ga koristi, ukoliko je riječ o samostalnom preduzetniku ili fizičkom licu,
 2. naziv pravnog lica i broj sudskog registra, kada je to primjenljivo, ukoliko se radi o pravnom licu,
- 4) adresu, uključujući najmanje oznaku grada i države, korisnika kome je izdat certifikat,
- 5) naziv(-e) domene(-a) kojom(-ima) upravlja korisnik certifikata,
- 6) podatke o početku i kraju roka važenja certifikata,
- 7) identifikacionu oznaku izdatog elektronskog certifikata,
- 8) kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat certifikacionog tijela,
- 9) lokaciju na kojoj je besplatno dostupan certifikat koji podržava kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat iz tačke 8) ovog člana i
- 10) lokaciju usluga koje se mogu koristiti za provjeru statusa kvalifikovanog certifikata.

Član 19.

- (1) Certifikaciono tijelo koje izdaje nekvalifikovane elektronske certifikate ne treba posebnu dozvolu za obavljanje usluga.
- (2) Certifikaciono tijelo može obavljati usluge elektronske certifikacije ako ima:
 - 1) organizaciju rada koja obezbjeđuje kvalitet izdavanja elektronskih certifikata,
 - 2) finansijska i materijalna sredstva koja su dovoljna za trajnije izdavanje elektronskih certifikata i pokrivanje moguće štete, naknade na ime osiguranja i slično,
 - 3) zaposleno lice koje je kvalifikovano za izvršavanje odgovarajućih stručno-tehničkih poslova usluga izdavanja elektronskih certifikata, vođenje registra certifikata i zaštite ličnih podataka,
 - 4) tehničku i programsku osnovu koja osigurava međunarodne standarde za sprovođenje usluge elektronske certifikacije,
 - 5) sistem fizičke zaštite uređaja, opreme i podataka i
 - 6) rješenja za zaštitu od neovlaštenog pristupa, kao i sigurnosna rješenja za čuvanje informacija.

Član 20.

- (1) Ministarstvo nauke i tehnologije (u daljem tekstu: Ministarstvo) vodi evidenciju o certifikacionim tijelima u Republici (u daljem tekstu: evidencija) koja je javno dostupna.
- (2) Certifikaciona tijela koja izdaju certifikate na komercijalnoj osnovi dužna su da prijave Ministarstvu početak obavljanja usluga elektronske certifikacije najmanje 14 dana prije početka rada.
- (3) Ministarstvo upisuje certifikaciono tijelo u evidenciju, odmah nakon što certifikaciono tijelo podnese prijavu kojom obavještava Ministarstvo o početku obavljanja usluga.

(4) Ministar pravilnikom propisuje sadržaj evidencije, način vođenja evidencije, obrasce prijave za upis u evidenciju, obrasce prijave za upis promjena, kao i vrstu, sadržaj i način dostavljanja dokumentacije neophodne za upis u evidenciju.

Član 21.

(1) Pored uslova iz člana 19. ovog zakona, certifikaciono tijelo koje izdaje kvalifikovane elektronske certifikate mora da ispunjava i sljedeće uslove:

- 1) prikazuje pouzdanost neophodnu za pružanje usluga elektronske certifikacije,
- 2) obezbjeđuje sigurno i ažurno vođenje registra certifikata, te sprovođenje bezbjednog i trenutnog prekida, odnosno opoziva usluge elektronske certifikacije na zahtjev korisnika,
- 3) omogućava tačno utvrđivanje datuma i vremena (sat i minuta) izdavanja ili opoziva elektronskog certifikata,
- 4) provjerava na odgovarajući način i u skladu sa propisima identitet i, ako je potrebno, druga obilježja korisnika kojima se izdaje elektronski certifikat,
- 5) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za vršenje usluge izdavanja elektronskih certifikata, a naročito u odnosu na: upravljačke sposobnosti, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih bezbjednosnih procedura i bezbjednu primjenu odgovarajućih administrativnih i upravljačkih postupaka koji su usaglašeni sa priznatim standardima,
- 6) ima pouzdane sisteme i proizvode koji su zaštićeni od promjena i osiguravaju tehničku i kriptografsku sigurnost procesa,
- 7) preduzima mjere protiv falsifikovanja i krađe podataka,
- 8) ima obezbijedena potrebna finansijska sredstva za rad, posebno za snošenje rizika od odgovornosti za štetu,
- 9) ima obezbijeden pouzdan sistem skladištenja relevantnih informacija koje se odnose na kvalifikovane elektronske certifikate u propisanom periodu/roku, posebno u svrhu dokazivanja za potrebe određenih postupaka,
- 10) ne čuva i ne kopira podatke iz certifikata za korisnike kojima se pruža usluga elektronske certifikacije,
- 11) informiše korisnike koji traže uslugu elektronske certifikacije o tačnim uslovima korištenja usluga, uključujući bilo koja ograničenja u korištenju, kao i postupke za rješavanje pritužbi i žalbi, s tim da te informacije moraju:
 1. biti napisane i pripremljene na jednom od jezika konstitutivnih naroda u Republici Srpskoj, na ćirilici ili latinici i mogu se dostaviti elektronskim putem,
 2. relevantni dijelovi tih informacija biti na raspolaganju na zahtjev trećih lica koja koriste elektronski certifikat,
- 12) ima obezbijeden pouzdan sistem čuvanja elektronskih certifikata u obliku koji omogućava njihovu provjeru kako bi:
 1. unos i promjene radila samo ovlaštena lica,
 2. mogla biti utvrđena provjera autentičnosti informacija iz certifikata,
 3. elektronski certifikat bio javno raspoloživ za pretraživanje samo u onim slučajevima za koje je vlasnik certifikata, odnosno korisnik dao saglasnost i
 4. bilo koja tehnička promjena koja bi mogla da naruši bezbjednosne zahtjeve bila poznata certifikacionom tijelu.

(2) Ministar pravilnikom detaljnije propisuje uslove koje moraju ispunjavati certifikaciona tijela iz ovog člana i člana 19. ovog zakona, kao i najniži iznos obaveznog osiguranja iz stava 1. tačka 8) ovog

člana kojim je certifikaciono tijelo obavezno da osigura rizik od odgovornosti za štetu koja nastane obavljanjem usluga elektronske certifikacije.

Član 22.

(1) Certifikaciono tijelo iz člana 21. ovog zakona, koje izdaje kvalifikovane elektronske certifikate, može da obavlja usluge na osnovu dozvole koju izdaje Ministarstvo.

(2) Na osnovu zahtjeva certifikacionog tijela za izdavanje dozvole, ministar imenuje Komisiju za provjeru ispunjenosti uslova za obavljanje usluga izdavanja kvalifikovanih elektronskih certifikata (u daljem tekstu: Komisija), koja ima tri člana.

(3) U Komisiju se imenuju stručnjaci iz oblasti informacionih tehnologija, koji imaju iskustvo u oblasti primjene elektronskog potpisa i koji poznaju sistem infrastrukture javnog ključa.

(4) Članovi Komisije imaju pravo na naknadu za svoj rad, koja se utvrđuje rješenjem ministra.

(5) Na osnovu preporuke Komisije, ministar donosi rješenje kojim se rješava po zahtjevu za izdavanje dozvole.

(6) Dozvola za izdavanje kvalifikovanih elektronskih certifikata (u daljem tekstu: dozvola) ima značenje rješenja izdatog u upravnom postupku.

(7) Dozvola se izdaje u roku od 30 dana od dana podnošenja urednog zahtjeva.

(8) U postupku za izdavanje dozvole, u pitanjima koja nisu uređena ovim zakonom primjenjuju se odredbe Zakona o opštem upravnom postupku.

Član 23.

(1) Zajedno sa izdavanjem dozvole iz člana 22. stav 5. ovog zakona, certifikaciono tijelo se upisuje se u Registar certifikacionih tijela u Republici Srpskoj (u daljem tekstu: Registar), koji vodi Ministarstvo i koji je javno dostupan.

(2) Certifikaciono tijelo može početi da obavlja usluge danom upisa u Registar.

(3) Certifikaciona tijela koja su upisana u Registar mogu to da naznače u izdatim kvalifikovanim elektronskim certifikatima.

(4) Ministar pravilnikom propisuje sadržaj i način vođenja Registra, obrasce zahtjeva za izdavanje dozvole i potrebnih priloga uz zahtjev, obrasce zahtjeva za upis promjena i potrebnih priloga, kao i postupak izdavanja dozvole i upisa u Registar.

Član 24.

(1) Elektronske certifikate može izdavati i organ uprave, ako ispunjava sve uslove propisane ovim zakonom i propisima donesenim na osnovu ovog zakona.

(2) Djelokrug, sadržaj i nosioci poslova elektronske certifikacije u organima uprave i za organe uprave utvrđuju se uredbom Vlade Republike Srpske.

GLAVA VI

PRAVA, OBAVEZE I ODGOVORNOSTI KORISNIKA I CERTIFIKACIONIH TIJELA

Član 25.

(1) Korisnici su slobodni u izboru certifikacionog tijela.

(2) Korisnik može koristiti usluge certifikacije od jednog certifikacionog tijela ili više njih.

(3) Korisnici mogu koristiti i usluge certifikacionog tijela u inostranstvu.

(4) Korisnici koriste usluge certifikacije na osnovu ugovora sa odabranim certifikacionim tijelom.

Član 26.

(1) Elektronski certifikat može se izdati svakom korisniku na njegov zahtjev, na osnovu nesumnjivo utvrđenog identiteta i ostalih podataka o korisniku koji je podnio zahtjev.

(2) Identitet korisnika se utvrđuje na osnovu lične karte, putne isprave ili drugog identifikacionog dokumenta korisnika ili ovlaštenog predstavnika korisnika, koji sadrži fotografiju lica i koji je važeći u trenutku podnošenja zahtjeva.

(3) Certifikaciono tijelo izdaje elektronski certifikat za svakog pojedinačnog korisnika na osnovu ugovora potpisanog sa korisnikom.

Član 27.

(1) Svaki korisnik obavezan je da preduzme sve potrebne organizacione i tehničke mjere zaštite od gubitaka i štete koje može uzrokovati drugim korisnicima, certifikacionom tijelu ili trećim licima.

(2) Obaveza korisnika je da sredstva i podatke za izradu elektronskog potpisa i elektronskog pečata koristi pažljivo i u skladu sa odredbama ovog zakona, te da ih zaštiti i čuva od neovlaštenog pristupa i upotrebe.

Član 28.

(1) Sve potrebne podatke i informacije o promjenama koje utiču ili mogu uticati na tačnost certifikata korisnik je obavezan da odmah prijavi, odnosno dostavi certifikacionom tijelu.

(2) Korisnik je obavezan da odmah zatraži opoziv svog certifikata u svim slučajevima gubitka ili oštećenja sredstava ili podataka za izradu elektronskog potpisa i elektronskog pečata.

Član 29.

Korisnik je odgovoran za nepravilnosti koje su nastale zbog neispunjavanja obaveza utvrđenih odredbama čl. 27. i 28. ovog zakona.

Član 30.

Certifikaciono tijelo koje izdaje kvalifikovane elektronske certifikate ima obavezu da:

- 1) osigura da svaki kvalifikovani elektronski certifikat sadrži sve potrebne podatke u skladu sa čl. 16, 17. i 18. ovog zakona,
- 2) utvrdi identitet korisnika za kojeg sprovodi usluge certifikacije,
- 3) osigura tačnost i cjelovitost podataka koje unosi u evidenciju izdatih certifikata,
- 4) u svaki certifikat unese osnovne podatke o svom identitetu,
- 5) omogući svakom zainteresovanom licu uvid u identifikacione podatke certifikacionog tijela i uvid u dozvolu za izdavanje kvalifikovanih elektronskih certifikata,
- 6) vodi tačnu i zaštićenu evidenciju elektronskih certifikata,
- 7) vodi tačnu i zaštićenu evidenciju opozvanih elektronskih certifikata,
- 8) osigura vidljiv podatak o tačnom datumu i vremenu (sat i minuta) izdavanja, odnosno opoziva elektronskih certifikata u evidenciji izdatih elektronskih certifikata,
- 9) čuva sve podatke i dokumentaciju o izdatim i opozvanim elektronskim certifikatima, u skladu sa važećim propisima, kao sredstvo dokazivanja u sudskim, upravnim i drugim postupcima, pri čemu podaci i prateća dokumentacija mogu biti i u elektronskom obliku i
- 10) primjenjuje odredbe zakona i drugih propisa kojima je uređena zaštita ličnih podataka.

Član 31.

(1) Certifikaciono tijelo obavezno je da izvrši opoziv certifikata, najkasnije u roku od 24 časa, korisnicima:

- 1) koji su to izričito zatražili,
- 2) za koje je utvrđena netačnost ili nepotpunost podataka u evidenciji certifikata,
- 3) za koje je primljena službena obavijest o gubitku poslovne sposobnosti i
- 4) za koje je primljena službena obavijest o smrti.

(2) Opoziv stupa na snagu odmah nakon njegovog objavljivanja u evidenciji opozvanih certifikata.

(3) Certifikaciono tijelo obavezno je da ažurno vodi evidenciju svih opozvanih elektronskih certifikata.

(4) Obaveza certifikacionog tijela je da obavijesti korisnika o opozivu certifikata u roku od 24 časa od primljenog obavještenja, odnosno nastanka okolnosti zbog kojih se elektronski certifikat opoziva.

(5) Od trenutka kada je opozvan, certifikat gubi pravno dejstvo i njegov status se ne može ponovo aktivirati.

Član 32.

(1) Certifikaciono tijelo obavezno je da, u slučaju prestanka poslovanja, o namjeri raskida ugovora obavijesti svakog korisnika, kao i da prestanak poslovanja prijavi Ministarstvu.

(2) Obaveza certifikacionog tijela je da osigura kod drugog certifikacionog tijela nastavak obavljanja usluga certifikacije za korisnike kojima je izdalo certifikate najmanje za period važenja originalnog certifikata, a ukoliko za to nema mogućnosti, dužno je da opozove sve izdate certifikate.

(3) Certifikaciono tijelo koje prestaje da pruža usluge elektronske certifikacije obavezno je da dostavi svu dokumentaciju u vezi sa obavljenim uslugama certifikacije drugom certifikacionom tijelu na koga prenosi obaveze obavljanja usluga certifikacije.

Član 33.

(1) Kvalifikovani certifikati koje su izdala certifikaciona tijela sa sjedištem u jednoj od zemalja članica Evropske unije imaju istu pravnu snagu kao i kvalifikovani certifikati izdati u Republici Srpskoj.

(2) Kvalifikovani certifikati koje su izdala certifikaciona tijela sa sjedištem u inostranstvu izvan Evropske unije imaju istu pravnu snagu kao i kvalifikovani certifikati izdati u Republici Srpskoj, u slučaju da je ispunjen najmanje jedan od sljedećih uslova:

1) certifikaciono tijelo ispunjava uslove propisane ovim zakonom za izdavanje kvalifikovanih certifikata i registrovano je u Republici Srpskoj,

2) domaće certifikaciono tijelo koje je upisano u Registar garantuje za takav kvalifikovani certifikat,

3) bilateralnim ili multilateralnim sporazumom između Republike Srpske ili Bosne i Hercegovine i drugih zemalja ili međunarodnih organizacija određeno je da se priznaje i

4) kvalifikovani certifikat ili certifikaciono tijelo priznato je na osnovu bilateralnog ili multilateralnog sporazuma između Evropske unije i trećih zemalja ili međunarodnih organizacija.

GLAVA VII NADZOR

Član 34.

(1) Nadzor nad primjenom ovog zakona i radom certifikacionih tijela vrši Republička uprava za inspeksijske poslove posredstvom nadležnih inspektora.

(2) Nadzor nad radom certifikacionih tijela na poslovima prikupljanja, upotrebe i zaštite ličnih podataka vrše organi određeni propisima kojima se uređuje zaštita ličnih podataka.

Član 35.

U okviru inspekcijskog nadzora certifikacionih tijela inspektor:

- 1) utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donesenim na osnovu ovog zakona,
- 2) kontroliše pravilnost primjene propisanih postupaka i organizaciono-tehničkih mjera, primjenu internih pravila koja su u vezi sa uslovima propisanim ovim zakonom i propisima donesenim na osnovu ovog zakona,
- 3) vrši kontrolu postupka izdavanja, čuvanja i opoziva elektronskih certifikata i
- 4) vrši kontrolu zakonitosti obavljanja drugih usluga certifikacionih tijela.

Član 36.

- (1) U vršenju inspekcijskog nadzora inspektor ima pravo i dužnost da:
 - 1) pregleda akte i dokumentaciju koja je povezana sa djelatnošću izdavanja certifikata,
 - 2) provjerava poslovne prostorije certifikacionog tijela, informacioni sistem, računarsku mrežu, ostalu opremu, tehničku dokumentaciju, kao i bezbjednosne mjere koje se preduzimaju i
 - 3) izvrši uvid u cjelokupnu dokumentaciju radi obezbjeđivanja dokaza ili tačnog utvrđivanja eventualne neregularnosti.
- (2) Inspektor je dužan da čuva kao službenu tajnu sve podatke o certifikatima i lične podatke o korisniku certifikata.
- (3) Certifikaciono tijelo je dužno da u cilju sprovođenja inspekcijskog nadzora omogući inspektoru pristup u svoje poslovne prostorije i omogući uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika i računarskoj opremi i uređajima koji se primjenjuju u postupku izdavanja certifikata.

Član 37.

- (1) Nadležni inspektor rješenjem:
 - 1) zabranjuje primjenu neadekvatnih postupaka i infrastrukture i daje rok certifikacionom tijelu u kojem je ono dužno da obezbijedi adekvatne postupke i infrastrukturu,
 - 2) zabranjuje licima koja ne posjeduju specijalistička znanja, iskustvo i stručne kvalifikacije potrebne za vršenje usluge izdavanja elektronskih certifikata, rad na poslovima izdavanja certifikata i daje rok za obezbjeđenje adekvatnog kadra,
 - 3) privremeno zabranjuje poslovanje certifikacionog tijela do otklanjanja neadekvatnosti postupaka i infrastrukture,
 - 4) nalaže opoziv jednog ili više certifikata izdatih od certifikacionog tijela, ako postoji osnovana sumnja da je riječ o neadekvatnom postupku ili falsifikatu i
 - 5) nalaže opoziv svih certifikata izdatih od certifikacionog tijela, što dovodi do prestanka rada certifikacionog tijela, ako postoji osnovana sumnja da je riječ o neadekvatnom postupku ili falsifikatu.
- (2) U slučaju privremene zabrane poslovanja certifikacionog tijela iz stava 1. tačka 3) ovog člana, certifikati izdati do dana nastanka uzroka zbog kojih je izrečena mjera zabrane i dalje važe.
- (3) U slučaju opoziva svih certifikata, odnosno prestanka rada certifikacionog tijela iz stava 1. tačka 5) ovog člana, inspektor će odmah obavijestiti Ministarstvo i zatražiti brisanje iz evidencije, odnosno Registra.
- (4) Ukoliko se tokom inspekcijske kontrole utvrdi da certifikaciono tijelo koje izdaje kvalifikovane elektronske certifikate i koje je upisano u Registar više ne ispunjava uslove propisane ovim zakonom, nadležni inspektor o tome odmah obavještava Ministarstvo.

(5) Ministarstvo je dužno da certifikaciono tijelo, odmah po dobijanju obavještenja od strane nadležnog inspektora, briše iz Registra.

GLAVA VIII KAZNE NE ODREDBE

Član 38.

Novčanom kaznom od 500 KM do 1.500 KM kazniće se za prekršaj fizičko lice koje neovlašteno pristupi i upotrijebi podatke i sredstva za izradu elektronskog potpisa i kvalifikovanog elektronskog potpisa.

Član 39.

(1) Novčanom kaznom od 500 KM do 1.500 KM kazniće se za prekršaj korisnik – fizičko lice ili samostalni preduzetnik koji:

1) nepažljivo i neodgovorno koristi sredstva i podatke za izradu elektronskog potpisa i elektronskog pečata (član 27. stav 2),

2) certifikacionom tijelu ne dostavi potrebne podatke i informacije o promjenama koje utiču ili mogu uticati na tačnost elektronskog certifikata (član 28. stav 1) i

3) odmah ne dostavi certifikacionom tijelu zahtjev za opoziv certifikata (član 28. stav 2).

(2) Za prekršaj iz stava 1. ovog člana korisnik – pravno lice će se kazniti novčanom kaznom od 1.000 KM do 3.000 KM.

(3) Odgovorno lice u pravnom licu kazniće se za prekršaj iz stava 1. ovog člana novčanom kaznom od 500 KM do 1.000 KM.

Član 40.

(1) Novčanom kaznom od 1.000 KM do 15.000 KM kazniće se za prekršaj certifikaciono tijelo koje:

1) izdaje kvalifikovani elektronski certifikat koji ne sadrži sve potrebne podatke (član 16. stav 2, čl. 17. i 18),

2) ne prijavi Ministarstvu početak obavljanja usluga elektronske certifikacije (član 20. stav 2),

3) čuva i kopira podatke iz certifikata (član 21. stav 1. tačka 10),

4) ne obavijesti korisnika kojem izdaje elektronski certifikat o svim bitnim uslovima upotrebe izdatog certifikata (član 21. stav 1. tačka 11),

5) ne utvrdi identitet korisnika kojem izdaje kvalifikovani elektronski certifikat (član 30. tačka 2),

6) ne vodi ažurno i bezbjednosnim mjerama zaštićenu evidenciju certifikata (član 30. tačka 6),

7) ne prekine usluge certifikacije, odnosno ne izvrši opoziv izdatih certifikata u propisanim slučajevima (član 31. stav 1),

8) ne vodi ažurno evidenciju svih opozvanih certifikata (član 31. stav 2),

9) ne obavijesti u propisanom roku korisnika o izvršenom opozivu elektronskog certifikata (član 31. stav 3),

10) ne čuva kompletnu dokumentaciju o izdatim i opozvanim certifikatima u predviđenom roku (član 30. tačka 9),

11) blagovremeno ne obavijesti korisnike kojima je izdao elektronske certifikate i Ministarstvo o prestanku poslovanja (član 32. stav 1) i

12) ne omogući nadležnim inspekcijskim organima pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika, računarskoj opremi i uređajima (član 36. stav 3).

(2) Odgovorno lice u certifikacionom tijelu kazniće se za prekršaj iz stava 1. ovog člana novčanom kaznom od 500 KM do 1.000 KM.

Član 41.

(1) Novčanom kaznom od 1.000 KM do 15.000 KM kazniće se za prekršaj certifikaciono tijelo – izdavalac vremenskog žiga koji:

1) formira vremenski žig koji ne sadrži sve podatke propisane zakonom i podzakonskim aktima donesenim na osnovu ovog zakona (član 11. stav 2),

2) ne čuva na bezbjedan način i u propisanim rokovima podatke o izdatim vremenskim žigovima (član 12. stav 2) i

3) ne omogući nadležnim inspekcijskim organima pristup u svoje poslovne prostorije i ne omogući uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika, računarskoj opremi i uređajima (član 36. stav 3).

(2) Odgovorno lice u certifikacionom tijelu kazniće se za prekršaj iz stava 1. ovog člana novčanom kaznom od 500 KM do 1.000 KM.

GLAVA IX

PRELAZNE I ZAVRŠNE ODREDBE

Član 42.

Vlada Republike Srpske donijeće uredbu iz člana 24. stav 2. ovog zakona u roku od tri mjeseca od dana stupanja na snagu ovog zakona.

Član 43.

Ministar će u roku od šest mjeseci od dana stupanja na snagu ovog zakona donijeti:

1) Pravilnik o tehničko-tehnološkim postupcima za izradu kvalifikovanog elektronskog potpisa i drugih usluga povjerenja i mjerama zaštite elektronskog potpisa i drugih usluga povjerenja (član. 8. stav 4),

2) Pravilnik o izdavanju vremenskog žiga (član 12. stav 4),

3) Pravilnik o evidenciji certifikacionih tijela (član 20. stav 4),

4) Pravilnik o posebnim uslovima koje moraju da ispunjavaju certifikaciona tijela (član 21. stav 2) i

5) Pravilnik o postupku izdavanja dozvole i upisa u registar certifikacionih tijela za izdavanje kvalifikovanih elektronskih certifikata (član 23. stav 4).

Član 44.

Do donošenja podzakonskih akata iz čl. 42. i 43. ovog zakona primjenjivaće se podzakonski akti doneseni na osnovu ranije važećeg Zakona, ako nisu u suprotnosti sa odredbama ovog zakona.

Član 45.

Stupanjem na snagu ovog zakona prestaje da važi Zakon o elektronskom potpisu Republike Srpske („Službeni glasnik Republike Srpske“, br. 59/08 i 68/13).

Član 46.

Ovaj zakon stupa na snagu osmoga dana od dana objavljivanja u „Službenom glasniku Republike Srpske“.

Broj: 02/1-021-1563/15
Datum: 10. decembar 2015. godine

Po ovlaštenju
Predsjednika Narodne skupštine

Nenad Stevandić