

Zakon o elektronskoj identifikaciji i elektronskom potpisu

Zakon je objavljen u "Službenom listu CG", br. [31/2017](#) i [72/2019](#).

I. OSNOVNE ODREDBE

Predmet

Član 1

Ovim zakonom uređuju se uslovi za korišćenje elektronskog potpisa, elektronskog pečata, elektronskog vremenskog pečata i usluge elektronske preporučene dostave u pravnom prometu, upravnim, sudskim i drugim postupcima i certifikovanje za autentifikaciju internet stranice, kao i sistem elektronske identifikacije i uslovi za priznavanje sredstava elektronske identifikacije drugih država.

Elektronska identifikacija

Član 2

Elektronska identifikacija je postupak korišćenja identifikacionih podataka u elektronskom obliku koji na jedinstven način predstavljaju fizičko lice, pravno lice ili organ vlasti.

Sistem elektronske identifikacije je sistem za izdavanje sredstava elektronske identifikacije fizičkim licima, pravnim licima, organima vlasti, odnosno fizičkim licima koja zastupaju pravna lica ili organe vlasti.

Sredstvo elektronske identifikacije može biti skup podataka, računarska oprema (hardver) ili računarski program (softver) koji sadrže identifikacione podatke u elektronskom obliku ili povezuju fizičko lice, pravno lice ili organ vlasti sa tim podacima, a koji se koriste za autentifikaciju za uslugu u elektronskom obliku.

Elektronske usluge povjerenja

Član 3

Radi korišćenja elektronskog potpisa, elektronskog pečata, elektronskog vremenskog pečata i usluge elektronske preporučene dostave u pravnom prometu, upravnim, sudskim i drugim postupcima, kao i sertifikata za autentifikaciju internet stranice, fizičko i pravno lice i organ vlasti oslanjaju se na elektronsku uslugu povjerenja.

Elektronske usluge povjerenja su usluge kojima se omogućava visok nivo pouzdanosti razmjene i obrade podataka u elektronskom obliku.

Elektronske usluge povjerenja su: izrada sertifikata za elektronski potpis, elektronski pečat i autentifikaciju internet stranice; izrada elektronskog vremenskog pečata; usluga elektronske preporučene dostave; verifikacija elektronskog potpisa i elektronskog pečata; čuvanje elektronskog potpisa, elektronskih pečata ili sertifikata koji se odnose na te usluge.

Elektronske usluge povjerenja koje ispunjavaju posebne uslove propisane ovim zakonom su kvalifikovane elektronske usluge povjerenja.

Davaoci elektronske usluge povjerenja

Član 4

Elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove propisane ovim zakonom (u daljem tekstu: davalac elektronske usluge povjerenja).

Kvalifikovane elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove za vršenje tih usluga propisane ovim zakonom (u daljem tekstu: kvalifikovani davalac elektronske usluge povjerenja).

Elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, vrši organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja (u daljem tekstu: Ministarstvo).

Elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja mogu vršiti i dragi organi vlasti u okviru poslova iz svoje nadležnosti, u skladu sa posebnim zakonom.

Dostupnost elektronskih usluga povjerenja licima sa invaliditetom

Član 5

Elektronske usluge povjerenja, kao i računarska oprema (hardver) ili računarski program (softver) koji se koriste prilikom vršenja tih usluga, kad je to moguće, dostupni su licima sa invaliditetom.

Zaštita podataka o ličnosti

Član 6

Na obradu podataka o ličnosti primjenjuju se propisi kojima se uređuje zaštita podataka o ličnosti. Korišćenje pseudonima u elektronskim transakcijama nije zabranjeno.

Upotreba rodno osjetljivog jezika

Član 7

Izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

Izrazi

Član 8

Izrazi koji se koriste u ovom zakonu imaju sljedeća značenja:

- 1) **identifikacioni podaci** obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog lica, pravnog lica ili organa vlasti;
- 2) **autentifikacija** je elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku;
- 3) **korisnik** je fizičko, pravno lice ili organ vlasti koje se oslanja da elektronsku identifikaciju ili elektronsku uslugu povjerenja;
- 4) **potpisnik** je fizičko lice koje se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica korišćenjem podataka za izradu elektronskog potpisa;
- 5) **podaci za izradu elektronskog potpisa** su jedinstveni podaci (kodovi ili privatni kriptografski ključevi), koje potpisnik koristi za izradu elektronskog potpisa;
- 6) **autor elektronskog pečata** je pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata;
- 7) **podaci za izradu elektronskog pečata** su jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata;
- 8) **certifikat za elektronski pečat** je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili organom vlasti i potvrđuje naziv tog pravnog lica ili organa vlasti;
- 9) **kvalifikovani certifikat** za elektronski pečat je sertifikat za elektronski pečat koji izdaje kvalifikovani davalac elektronske usluge povjerenja;
- 10) **sredstvo za izradu elektronskog pečata** je odgovarajuća računarska oprema ili računarski program koji se koristi za izradu elektronskog pečata;
- 11) **sredstvo za izradu kvalifikovanog elektronskog pečata** je sredstvo za izradu elektronskog pečata koje ispunjava posebne uslove propisane ovim zakonom;
- 12) **elektronski dokument** je skup podataka koji su elektronski oblikovani, poslani, primljeni ili skladišteni na elektronskom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva pomoću kojih se identifikuje stvaralac, utvrđuje vjerodostojnost sadržaja i dokazuje nepromjenjivost sadržaja u vremenu, a uključuje sve oblike pisanog teksta, podatke, slike, crteže, karte, zvuk, muziku, govor i slično;
- 13) **podaci za verifikaciju** su podaci koji se koriste za verifikaciju elektronskog potpisa ili elektronskog pečata;
- 14) **verifikacija** je postupak kojim se potvrđuje da su elektronski potpis ili elektronski pečat validni;
- 15) **organ vlasti** je državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja;
- 16) **domen** je sistem u kome se internet adrese vezuju za određene lokacije na internetu.

II. ELEKTRONSKI POTPIS I ELEKTRONSKI PEČAT

Elektronski potpis

Član 9

Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i služe za potpis i elektronsku identifikaciju potpisnika.

Elektronski potpis se izrađuje pomoću sredstva za izradu elektronskog potpisa i zasniva se na certifikatu za izradu

elektronskog potpisa.

Napredni elektronski potpis

Član 10

Napredni elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika i integritet elektronskog dokumenta, a koji ispunjava uslove propisane ovim zakonom.

Napredni elektronski potpis mora da:

- 1) bude isključivo povezan sa potpisnikom;
- 2) nedvosmisleno identifikuje potpisnika;
- 3) nastaje korišćenjem sredstva za izradu elektronskog potpisa kojim potpisnik može samostalno da upravlja i koje je isključivo pod njegovim nadzorom;
- 4) sadrži direktnu povezanost sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmjenu izvornih podataka.

Napredni elektronski potpis koji se zasniva na elektronskom certifikatu izdatom u državi članici Evropske unije priznaje se kao napredni elektronski potpis u Crnoj Gori, ako su ispunjeni uslovi iz stava 2 ovog člana.

Kvalifikovani elektronski potpis

Član 11

Kvalifikovani elektronski potpis je napredni elektronski potpis koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog potpisa i zasniva se na kvalifikovanom certifikatu za elektronski potpis.

Punovažnost elektronskog potpisa

Član 12

Elektronskom potpisu ne može se osporiti punovažnost i prihvatljivost samo zbog toga što:

- 1) je u elektronskom obliku;
- 2) se ne zasniva na kvalifikovanom certifikatu za elektronski potpis.

Pravno dejstvo elektronskog potpisa i naprednog elektronskog potpisa

Član 13

Organ vlasti odnosno pravno lice ne može odbiti prijem elektronskog dokumenta sa elektronskim potpisom ili naprednim elektronskim potpisom samo zato što je u elektronskom obliku.

Pravno dejstvo kvalifikovanog elektronskog potpisa

Član 14

Kvalifikovani elektronski potpis ima jednako pravno dejstvo kao svojeručni potpis, odnosno svojeručni potpis i pečat u odnosu na podatke u papirnom obliku i prihvatljiv je kao dokazno sredstvo u postupcima pred državnim organima, organima državne uprave, organima lokalne samouprave i lokalne uprave i pravnim licima koja vrše javna ovlašćenja.

Certifikat za elektronski potpis

Član 15

Certifikat za elektronski potpis je dokument u elektronskom obliku potpisan od davaoca elektronskih usluga povjerenja koji povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.

Kvalifikovani certifikat za elektronski potpis

Član 16

Kvalifikovani certifikat za elektronski potpis je certifikat koji izdaje kvalifikovani davalac elektronske usluge povjerenja, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona i koji sadrži:

- 1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis u obliku prikladnom za automatsku obradu podataka;
- 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za elektronski potpis, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za:

- pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj;

- fizičko lice: ime i prezime i poreski identifikacioni broj;

3) skup identifikacionih podataka o potpisniku (ime i prezime ili pseudonim) koji, ako se koristi, mora biti jasno naznačen;

4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa i koji su pod kontrolom potpisnika;

5) podatke o periodu važenja tog sertifikata;

6) identifikacionu oznaku izdatog kvalifikovanog sertifikata za elektronski potpis koja mora biti jedinstvena za kvalifikovanog davaoca elektronskih usluga povjerenja;

7) napredni elektronski potpis kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje taj sertifikat;

8) lokaciju na kojoj je besplatno dostupan taj sertifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronskih usluga povjerenja;

9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti tog sertifikata;

10) odgovarajuću naznaku, u obliku pogodnom za automatsku obradu podataka, ako se podaci za izradu elektronskog potpisa koji su povezani sa podacima za verifikaciju elektronskog potpisa nalaze u kvalifikovanom sredstvu za izradu elektronskog potpisa.

Kvalifikovani sertifikat za elektronski potpis pored podataka iz stava 1 ovog člana sadrži i identifikacioni broj potpisnika koji određuje organ državne uprave nadležan za unutrašnje poslove.

Kvalifikovani sertifikat za elektronski potpis, pored podataka iz stava 1 ovog člana, može da sadrži i druge podatke o potpisniku ako to potpisnik zahtijeva, a ti podaci ne utiču na interoperabilnost i priznavanje kvalifikovanih elektronskih potpisa.

Način određivanja identifikacionog broja uređuje Vlada Crne Gore.

Gubitak validnosti kvalifikovanog sertifikata za elektronski potpis i privremena suspenzija

Član 17

Kvalifikovani elektronski potpis gubi validnost ako je kvalifikovani sertifikat za elektronski potpis na kojem se zasniva opozvan nakon aktivacije, u skladu sa članom 51 stav 1 ovog zakona, i to od trenutka opoziva sertifikata.

U slučaju iz stava 1 ovog člana, elektronski potpis se ne može ponovo aktivirati.

Kvalifikovani elektronski potpis gubi validnost za vrijeme suspenzije kvalifikovanog sertifikata za elektronski potpis iz člana 51 stav 3 ovog zakona.

U slučaju iz stava 3 ovog člana, elektronski potpis se može ponovo aktivirati, kad se utvrdi da nijesu ispunjeni uslovi za opoziv kvalifikovanog sertifikata iz člana 51 stav 1 ovog zakona.

Sredstvo za izradu elektronskog potpisa

Član 18

Sredstvo za izradu elektronskog potpisa je odgovarajuća računarska oprema ili računarski program koji se koristi prilikom izrade elektronskog potpisa uz korišćenje podataka za izradu elektronskog potpisa.

Kvalifikovano sredstvo za izradu elektronskog potpisa

Član 19

Kvalifikovano sredstvo za izradu elektronskog potpisa je sredstvo za izradu kvalifikovanog elektronskog potpisa koje ispunjava posebne uslove propisane ovim zakonom.

Kvalifikovano sredstvo za izradu elektronskog potpisa mora da obezbijedi da:

1) se podaci za izradu kvalifikovanog elektronskog potpisa mogu pojaviti samo jedanput i da je ostvarena njihova sigurnost;

2) se podaci za izradu kvalifikovanog elektronskog potpisa ne mogu utvrditi iz tog potpisa;

3) kvalifikovani elektronski potpis bude zaštićen od falsifikovanja upotrebom trenutno dostupne tehnologije;

4) podatke za izradu kvalifikovanog elektronskog potpisa potpisnik može pouzdano zaštititi od neovlašćenog korišćenja.

Kvalifikovano sredstvo za izradu elektronskog potpisa ne smije, prilikom izrade kvalifikovanog elektronskog potpisa, promijeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke prije procesa izrade kvalifikovanog elektronskog potpisa.

Odredbe st. 1 i 2 ovog člana, shodno se primjenjuju na sredstvo za izradu elektronskog potpisa.

Kreiranje podataka za izradu elektronskog potpisa

Član 20

Kreiranje podataka za izradu elektronskog potpisa i upravljanje tim podacima u ime potpisnika može vršiti isključivo kvalifikovani davalac elektronske usluge povjerenja.

Kvalifikovani davalac elektronskih usluga povjerenja može da duplira podatke za izradu elektronskog potpisa isključivo u svrhu izrade rezervnih kopija, ako obezbijedi da:

1) sigurnost dupliranih skupova podataka za izradu elektronskog potpisa bude na istom nivou kao sigurnost izvornih skupova podataka za izradu elektronskog potpisa; i

2) broj dupliranih skupova podataka za izradu elektronskog potpisa ne prelazi broj neophodan za obezbjeđenje kontinuiteta usluge izrade kvalifikovanog elektronskog potpisa.

Certifikovanje kvalifikovanog sredstva za izradu elektronskog potpisa

Član 21

Usaglašenost kvalifikovanih sredstava za izradu elektronskih potpisa sa zahtjevima iz člana 19 ovog zakona ocjenjuje Ministarstvo.

Kvalifikovana sredstva za izradu elektronskih potpisa za koje se utvrdi da su usaglašena sa zahtjevima iz člana 19 ovog zakona, Ministarstvo stavlja na listu certifikovanih kvalifikovanih sredstava za izradu elektronskih potpisa.

Kvalifikovano sredstvo za izradu elektronskog potpisa koje se nalazi na listi iz stava 2 ovog člana, Ministarstvo može brisati sa liste ako, u skladu sa stavom 1 ovog člana, utvrdi da nije usaglašeno sa zahtjevima iz člana 19 ovog zakona.

Lista iz stava 2 ovog člana objavljuje se na internet stranici Ministarstva.

Način ocjenjivanja usaglašenosti iz stava 1 ovog člana, kao i sadržaj liste iz stava 2 ovog člana propisuje Ministarstvo.

Obavješćavanje Evropske komisije

Član 22

O nadležnosti da ocjenjuje usaglašenost kvalifikovanih sredstava za izradu elektronskih potpisa iz člana 21 ovog zakona Ministarstvo dostavlja Evropskoj komisiji obavještenje.

Ministarstvo, najkasnije u roku od 30 dana od ocjenjivanja usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa sa zahtjevima iz člana 19 ovog zakona, obavješćava o tome Evropsku komisiju.

Zahtjevi za verifikaciju kvalifikovanog elektronskog potpisa

Član 23

Validnost kvalifikovanog elektronskog potpisa potvrđuje se verifikacijom kvalifikovanog elektronskog potpisa, koja obuhvata utvrđivanje da:

1) je certifikat na kojem se zasniva elektronski potpis u trenutku potpisivanja bio kvalifikovani certifikat za elektronski potpis izdat u skladu sa ovim zakonom;

2) je kvalifikovani certifikat za elektronski potpis izdao kvalifikovani davalac elektronske usluge povjerenja i da je validan u trenutku potpisivanja;

3) podaci za verifikaciju potpisa odgovaraju podacima koji se daju korisniku;

4) je jedinstveni skup podataka koji predstavljaju potpisnika u kvalifikovanom certifikatu za elektronski potpis ispravno dostavljen korisniku;

5) je korišćenje pseudonima, ako je pseudonim korišćen u trenutku potpisivanja, naznačeno korisniku;

6) je kvalifikovani elektronski potpis izrađen kvalifikovanim sredstvom za izradu elektronskog potpisa;

7) nije ugrožen integritet potpisanih podataka;

8) su zahtjevi iz člana 10 ovog zakona ispunjeni u trenutku izrade potpisa.

Verifikacija kvalifikovanog elektronskog potpisa sprovodi se na način koji korisniku obezbjeđuje tačan rezultat verifikacije.

Kvalifikovanu uslugu verifikacije kvalifikovanih elektronskih potpisa može vršiti samo kvalifikovani davalac elektronskih usluga povjerenja koji verifikaciju vrši u skladu sa stavom 1 ovog člana i omogućava korisniku da dobije rezultate postupka verifikacije automatski, na način koji je pouzdan.

Rezultati postupka verifikacije potpisuju se naprednim elektronskim potpisom ili naprednim elektronskim pečatom davaoca usluge verifikacije.

Način sprovođenja verifikacije kvalifikovanog elektronskog potpisa propisuje Ministarstvo.

Usluga čuvanja kvalifikovanih elektronskih potpisa

Član 24

Uslugu čuvanja kvalifikovanih elektronskih potpisa može pružiti samo kvalifikovani davalac elektronskih usluga povjerenja koji koristi postupke i tehnologije koje mogu produžiti pouzdanost kvalifikovanog elektronskog potpisa na period koji je duži od tehnološkog roka važenja.

Način vršenja usluge čuvanja kvalifikovanih elektronskih potpisa propisuje Ministarstvo.

Elektronski, napredni elektronski i kvalifikovani elektronski pečat

Član 25

Elektronski pečat je skup podataka u elektronskom obliku koji su pridruženi drugim podacima u elektronskom obliku ili su logički povezani sa njima radi obezbjeđenja porijekla i integriteta tih podataka i zasniva se na certifikatu za elektronski pečat.

Napredni elektronski pečat je elektronski pečat koji ispunjava posebne zahtjeve u skladu sa ovim zakonom.

Kvalifikovani elektronski pečat je napredni elektronski pečat koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog pečata i zasniva se na kvalifikovanom certifikatu za elektronski pečat.

Elektronski vremenski pečat i kvalifikovani elektronski vremenski pečat

Član 26

Elektronski vremenski pečat je skup podataka u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.

Kvalifikovani elektronski vremenski pečat je elektronski vremenski pečat koji ispunjava posebne zahtjeve, i to:

- 1) povezuje datum i vrijeme sa podacima tako da se sprječava svaka mogućnost promjene podataka;
- 2) zasnovan je na preciznom vremenskom izvoru koji je povezan sa koordiniranim univerzalnim vremenom (UTC); i
- 3) potpisan je naprednim elektronskim potpisom ili pečatiran pomoću naprednog elektronskog pečata kvalifikovanog davaoca elektronskih usluga povjerenja.

Shodna primjena

Član 27

Na punovažnost, prihvatljivost i pravno dejstvo elektronskog pečata, elektronskog vremenskog pečata, kvalifikovanog elektronskog pečata i kvalifikovanog elektronskog vremenskog pečata, zahtjeve za napredni elektronski pečat, sadržaj i izdavanje sertifikata za kvalifikovani elektronski pečat, gubitak validnosti, opoziv i privremenu suspenziju sertifikata za elektronski pečat i sertifikata za kvalifikovani elektronski pečat, zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata, verifikaciju i čuvanje elektronskog pečata, shodno se primjenjuju odredbe čl. 10, 12, 13, 14 i čl. 16 do 24 ovog zakona.

III. USLUGA ELEKTRONSKE PREPORUČENE DOSTAVE

Usluga elektronske preporučene dostave

Član 28

Usluga elektronske preporučene dostave je usluga koja omogućava prenos podataka pomoću elektronskih sredstava i pruža dokaz o postupanju sa prenesenim podacima, uključujući dokaz o slanju i prijemu podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja ili bilo kakvih neovlašćenih prepravki.

Pravno dejstvo usluge elektronske preporučene dostave

Član 29

Fizičko lice, pravno lice, odnosno organ vlasti ne može odbiti prijem podataka poslatih i primljenih upotrebom usluge elektronske preporučene dostave samo zato što je u elektronskom obliku ili zbog toga što ne ispunjavaju sve zahtjeve kvalifikovane usluge elektronske preporučene dostave.

Uslovi za slanje podataka korišćenjem kvalifikovane usluge elektronske preporučene dostave

Član 30

Za podatke poslate i primljene korišćenjem kvalifikovane usluge elektronske preporučene dostave podrazumijeva se:

- 1) cjelovitost podataka;
- 2) slanje podataka od strane identifikovanog pošiljaoca;
- 3) prijem podataka od strane identifikovanog primaoca;
- 4) tačnost datuma i vremena slanja i prijema podataka kako su naznačeni kvalifikovanom uslugom elektronske preporučene dostave.

Kvalifikovana usluga elektronske preporučene dostave

Član 31

Kvalifikovana usluga elektronske preporučene dostave je usluga elektronske preporučene dostave koja ispunjava posebne zahtjeve, i to da:

- 1) je vrši jedan ili više kvalifikovanih davalaca elektronskih usluga povjerenja;
- 2) uz visok nivo sigurnosti obezbjeđuje identifikaciju pošiljaoca;
- 3) obezbjeđuje identifikaciju primaoca prije dostave podataka;
- 4) je slanje i primanje podataka obezbijeđeno naprednim elektronskim potpisom ili naprednim elektronskim pečatom kvalifikovanog davaoca elektronskih usluga povjerenja, na način kojim se isključuje mogućnost nezapažene promjene podataka;
- 5) se pošiljaocu i primaocu podataka jasno naznačava svaka promjena podataka potrebna radi slanja ili primanja podataka;
- 6) se datum i vrijeme slanja, primanja i eventualne promjene podataka ovjeravaju kvalifikovanim elektronskim vremenskim pečatom.

U slučaju prenosa podataka između dva ili više kvalifikovanih davalaca elektronskih usluga povjerenja, zahtjevi iz stava 1 ovog člana odnose se na sve kvalifikovane davaoce elektronskih usluga povjerenja.

Bliže zahtjeve koje mora da ispunjava kvalifikovana usluga elektronske preporučene dostave propisuje Ministarstvo.

IV. AUTENTIFIKACIJA INTERNET STRANICA

Pojam i certifikati

Član 32

Autentifikacija internet stranica je elektronski postupak koji omogućava potvrđivanje cjelovitosti podataka internet stranice i pouzdanosti korišćenja internet stranice i zasniva se na certifikatu za autentifikaciju internet stranica, odnosno na kvalifikovanom certifikatu za autentifikaciju internet stranica.

Certifikat za autentifikaciju internet stranice je potvrda pomoću koje se može izvršiti autentifikacija internet stranice i kojom se internet stranica povezuje sa fizičkim ili pravnim licem kojem je izdat certifikat.

Kvalifikovani certifikat za autentifikaciju internet stranice je certifikat za autentifikaciju internet stranice koji izdaje davalac elektronske usluge povjerenja, a koji ispunjava posebne uslove propisane ovim zakonom.

Kvalifikovani certifikati za autentifikaciju internet stranica

Član 33

Kvalifikovani certifikat za autentifikaciju internet stranice mora da sadrži:

- 1) oznaku da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranice u elektronskom obliku pogodnom za automatsku obradu;
- 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za autentifikaciju internet stranice, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za:
 - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj,
 - fizičko lice: ime i prezime i poreski identifikacioni broj;
- 3) skup identifikacionih podataka o:
 - pravnom licu ili organu vlasti kojem je izdat certifikat: naziv, matični, odnosno poreski identifikacioni broj i sjedište (minimum naziv grada i države),
 - fizičkom licu kome je izdat certifikat: ime i prezime ili pseudonim koji, ako se koristi, mora biti jasno naznačen i adresu (minimum naziv grada i države);
- 4) naziv jednog ili više domena kojim upravlja fizičko lice, pravno lice ili organ vlasti kojem je izdat certifikat za autentifikaciju internet stranice;
- 5) podatke o periodu važenja kvalifikovanog sertifikata za autentifikaciju internet stranice;
- 6) identifikacionu oznaku izdatog kvalifikovanog sertifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca elektronske usluge povjerenja;
- 7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje certifikat;
- 8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja;
- 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog sertifikata za autentifikaciju internet stranice.

V. USLOVI ZA VRŠENJE KVALIFIKOVANIH ELEKTRONSKIH USLUGA POVJERENJA

Uslovi u vezi sa kvalifikovanim davaocima elektronske usluge povjerenja

Član 34

Kvalifikovani davalac elektronske usluge povjerenja mora da ispunjava sljedeće uslove, i to da:

- 1) ima ažuriran plan prekida pružanja elektronske usluge povjerenja radi obezbjeđivanja njenog kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona;
 - 2) obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti;
 - 3) obezbijedi, na odgovarajući način i u skladu sa ovim zakonom i internim aktima iz člana 37 stav 4 ovog zakona, provjeru identiteta potpisnika i, po potrebi, drugog obilježja fizičkog i pravnog lica, kojima se izdaje kvalifikovani sertifikat za elektronski potpis, odnosno kvalifikovani sertifikat za elektronski pečat;
 - 4) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje elektronskih usluga povjerenja, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka;
 - 5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa;
 - 6) preduzima mjere za sprječavanje falsifikovanja sertifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja sertifikate potpisnicima na bezbjedan način;
 - 7) posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih sertifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih sertifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete;
 - 8) posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane sertifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih sertifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa;
 - 9) koristi pouzdan sistem čuvanja kvalifikovanih sertifikata u obliku koji omogućava provjeru, kako bi:
 - unos i promjene podataka prilikom pružanja elektronske usluge povjerenja vršila samo ovlašćena lica,
 - mogla biti provjerena autentičnost podataka iz kvalifikovanog sertifikata,
 - podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje,
 - bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve, bila vidljiva kvalifikovanom davaocu elektronske usluge povjerenja.
- Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

Vršenje kvalifikovanih elektronskih usluga povjerenja za organe vlasti

Član 35

Kad Ministarstvo i organ vlasti iz člana 4 stav 4 ovog zakona vrše kvalifikovane elektronske usluge povjerenja moraju ispunjavati uslove iz člana 34 stav 1 tač. 1 do 6 i tač. 8 i 9 ovog zakona.

Ispunjenost uslova iz stava 1 ovog člana utvrđuje Ministarstvo.

Način vršenja elektronskih usluga povjerenja i kvalifikovanih elektronskih usluga povjerenja za organe državne uprave propisuje Ministarstvo.

Pravno dejstvo kvalifikovanih sertifikata izdatih u drugoj državi

Član 36

Kvalifikovane elektronske usluge povjerenja u Crnoj Gori mogu vršiti i davaoci elektronskih usluga povjerenja sa sjedištem u drugoj državi.

Kvalifikovani sertifikati koje izdaju davaoci elektronskih usluga povjerenja sa sjedištem u drugoj državi koja nije članica Evropske unije, imaju isto pravno dejstvo kao i kvalifikovani sertifikati izdati u Crnoj Gori, ako:

- 1) davalac elektronskih usluga povjerenja ispunjava uslove propisane ovim zakonom za izdavanje kvalifikovanih sertifikata i upisan je u registar kvalifikovanih davalaca elektronskih usluga povjerenja u Crnoj Gori ili je registrovan u državi članici Evropske unije;
- 2) kvalifikovani davalac elektronskih usluga povjerenja koji je upisan u registar kvalifikovanih davalaca elektronskih usluga povjerenja u Crnoj Gori ili je registrovan u državi članici Evropske unije garantuje za takav kvalifikovani sertifikat;
- 3) su u skladu sa međunarodnim ugovorom zaključenim između Crne Gore i druge države ili međunarodne organizacije;
- 4) su u skladu sa međunarodnim ugovorom zaključenim između Evropske unije i države koja nije članica Evropske unije ili međunarodne organizacije;

5) davalac elektronskih usluga povjerenja ispunjava uslove utvrđene propisima Evropske unije za izdavanje kvalifikovanih certifikata i ako je registrovan u državi članici Evropske unije;

Certifikati davaoca elektronskih usluga povjerenja sa sjedištem u državi članici Evropske unije, koji ne ispunjavaju uslove za izdavanje kvalifikovanog certifikata u skladu sa ovim zakonom, imaju isto pravno dejstvo kao i certifikati izdati u Crnoj Gori u skladu sa ovim zakonom.

VI. EVIDENCIJE I REGISTRI

Prijava o početku vršenja elektronske usluge povjerenja

Član 37

Elektronske usluge povjerenja može da vrši davalac elektronske usluge povjerenja koji je upisan u evidenciju davalaca elektronskih usluga povjerenja (u daljem tekstu: evidencija), koju vodi Ministarstvo.

Upis u evidenciju vrši se na osnovu prijave o početku vršenja elektronske usluge povjerenja koju davalac elektronske usluge povjerenja podnosi Ministarstvu, najmanje osam dana prije dana koji je u prijavi naznačen kao dan početka vršenja elektronskih usluga povjerenja.

Davalac elektronske usluge povjerenja dužan je da o promjenama u vršenju elektronskih usluga povjerenja Ministarstvu podnese prijavu.

Uz prijave iz st. 1 i 3 ovog člana, prilažu se interna akta o načinu i postupcima pružanja elektronskih usluga povjerenja, bezbjednosnom sistemu i tehničkoj infrastrukturi.

Upis u evidenciju

Član 38

Upis u evidenciju vrši se odmah nakon podnošenja prijave o početku obavljanja elektronske usluge povjerenja.

Evidencija sadrži podatke o davaocu elektronske usluge povjerenja koji je podnio prijavu, i to: ime i prezime fizičkog lica, odnosno naziv pravnog lica, adresu i elektronsku adresu, šifru djelatnosti i poreski identifikacioni broj, odnosno jedinstveni matični broj za fizičko lice, registarski broj iz Centralnog registra privrednih subjekata.

Evidencija se vodi u elektronskom obliku pogodnom za automatsku obradu i dostupna je javnosti na internet stranici Ministarstva.

Bliži sadržaj i način vođenja evidencije propisuje Ministarstvo.

Rješenje o ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja

Član 39

Davalac elektronskih usluga povjerenja koji je upisan u evidenciju može podnijeti zahtjev za upis u registar kvalifikovanih davalaca elektronskih usluga povjerenja (u daljem tekstu: registar), koji vodi Ministarstvo.

Uz zahtjev iz stava 1 ovog člana, davalac elektronskih usluga povjerenja dužan je da priloži dokumentaciju kojom dokazuje da ispunjava uslove iz člana 34 ovog zakona.

O ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja propisanih ovim zakonom Ministarstvo donosi rješenje, na osnovu uvida u priloženu dokumentaciju iz stava 1 ovog člana i, po potrebi, na osnovu neposrednog uvida.

Rješenje iz stava 3 ovog člana donosi se, u roku od 15 dana od dana podnošenja urednog zahtjeva.

Upis u registar

Član 40

Na osnovu rješenja kojim se utvrđuje da podnosilac zahtjeva za upis u registar ispunjava uslove iz člana 34 ovog zakona, odmah nakon njegovog donošenja, Ministarstvo vrši upis podnosioca zahtjeva u registar.

U registar se upisuju i davaoci elektronskih usluga povjerenja koji imaju sjedište u drugoj državi, na njihov zahtjev, ako ispunjavaju uslove iz člana 34 ovog zakona.

Registar sadrži podatke o kvalifikovanom davaocu elektronske usluge povjerenja koji je upisan u registar, i to: ime i prezime fizičkog lica, odnosno naziv pravnog lica, adresu i elektronsku adresu, šifru djelatnosti i poreski identifikacioni broj, odnosno jedinstveni matični broj za fizičko lice, registarski broj iz Centralnog registra privrednih subjekata.

Registar se vodi u elektronskom obliku pogodnom za automatsku obradu podataka i dostupan je javnosti na internet stranici Ministarstva.

Registar potpisuje Ministarstvo naprednim elektronskim potpisom.

Ministarstvo dostavlja Evropskoj komisiji podatke o svojoj nadležnosti da vodi i objavljuje registar, kao i o tome gdje se podaci o registru objavljuju, certifikatima korišćenim za potpisivanje ili pečatiranje registra, kao i o svim njegovim izmjenama.

Bliži sadržaj i način vođenja registra propisuje Ministarstvo.

Brisanje iz registra

Član 41

O svim promjenama u vezi sa vršenjem kvalifikovanih elektronskih usluga povjerenja, kao i o namjeri da prestane da vrši te usluge, kvalifikovani davalac elektronske usluge povjerenja dužan je da obavijesti Ministarstvo.

Kad Ministarstvo nakon obavještenja iz stava 1 ovog člana utvrdi da kvalifikovani davalac elektronske usluge povjerenja ne ispunjava uslove iz člana 34 ovog zakona, ili prestane da vrši elektronske usluge povjerenja, brisaće tog davaoca usluge iz registra.

Brisanje iz registra se može izvršiti i u drugim slučajevima kad se utvrdi da kvalifikovani davalac elektronske usluge povjerenja ne ispunjava uslove iz člana 34 ovog zakona.

Naznaka o upisu u registar u certifikatima

Član 42

Kvalifikovani davalac elektronske usluge povjerenja koji je upisan u registar može tu činjenicu naznačiti u certifikatima koje izdaje.

Korišćenje oznake certifikovanja za elektronske transakcije EU

Član 43

Nakon upisa u registar, kvalifikovani davalac elektronskih usluga povjerenja može da koristi oznaku certifikovanja EU kako bi na jednostavan, prepoznatljiv i jasan način naznačio kvalifikovane elektronske usluge povjerenja.

VII. PRAVA, OBAVEZE I ODGOVORNOSTI POTPISNIKA, AUTORA ELEKTRONSKOG PEČATA I DAVALACA ELEKTRONSKIH USLUGA POVJERENJA

Izdavanje certifikata

Član 44

Kvalifikovani certifikat može se izdati pravnom licu, fizičkom licu ili organu vlasti, na njegov zahtjev, na osnovu utvrđenog identiteta i drugih podataka o pravnom licu, fizičkom licu ili organu vlasti za koje se izdaje kvalifikovani certifikat.

Pravo na izbor davaoca elektronskih usluga povjerenja

Član 45

Pravno ili fizičko lice samostalno vrši izbor davaoca elektronskih usluga povjerenja.

Pravno ili fizičko lice može koristiti elektronske usluge povjerenja jednog ili više davalaca elektronskih usluga povjerenja.

Pravno ili fizičko lice koristi elektronski potpis, elektronski pečat i elektronski vremenski pečat, odnosno elektronske usluge povjerenja na osnovu ugovora sa odabranim davaocem elektronske usluge povjerenja.

Pravno ili fizičko lice može koristiti elektronske usluge povjerenja davaoca elektronske usluge povjerenja koji ima sjedište u drugoj državi.

Obaveza čuvanja sredstava i podataka za izradu elektronskog potpisa ili elektronskog pečata

Član 46

Potpisnik, odnosno autor elektronskog pečata dužan je da pažljivo čuva sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata, kao i podatke za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata od neovlašćenog pristupa i upotrebe i da ih koristi u skladu sa ovim zakonom.

Niko ne smije neovlašćeno da pristupi i upotrijebi sredstva za izradu elektronskog potpisa, elektronskog pečata ili elektronskog vremenskog pečata, kao ni podatke za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata.

Obaveze potpisnika i autora elektronskog pečata

Član 47

Potpisnik, odnosno autor elektronskog pečata dužan je da dostavi davaocu elektronske usluge povjerenja sve potrebne podatke i informacije o promjenama koje utiču ili mogu uticati na tačnost utvrđivanja njegovog identiteta, odmah, a najkasnije u roku od 48 časova od nastanka promjene.

Potpisnik, odnosno autor elektronskog pečata dužan je da odmah zahtijeva opoziv ili suspenziju certifikata koji mu je izdat u slučaju:

1) gubitka ili oštećenja sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata ili gubitka podataka za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata;

2) kad posumnja u povjerljivost podataka za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata.

Kad je u certifikatu za elektronski potpis navedeno da potpisnik potpisuje u ime drugog fizičkog ili pravnog lica, obavezu da zahtijeva opoziv ili suspenziju certifikata u slučajevima iz stava 2 ovog člana, ima i to lice.

Odgovornost potpisnika i autora elektronskog pečata

Član 48

Potpisnik, odnosno autor elektronskog pečata odgovara za nepravilnosti koje su nastale zbog neispunjavanja obaveza iz čl. 46 i 47 ovog zakona.

Potpisnik, odnosno autor elektronskog pečata nije odgovoran za nepravilnosti iz stava 1 ovog člana, ako dokaže da oštećeno lice nije preduzelo ili je pogrešno preduzelo radnje vezane za provjeru elektronskog potpisa, elektronskog pečata, odnosno elektronskog vremenskog pečata.

Obaveze davaoca elektronske usluge povjerenja

Član 49

Davalac elektronskih usluga povjerenja dužan je da:

1) obezbijedi da svaki kvalifikovani certifikat sadrži podatke iz člana 16 ovog zakona;

2) sprovede potpunu provjeru identiteta fizičkog lica, pravnog lica, odnosno organa vlasti kojem se izdaje kvalifikovani certifikat;

3) o izdatim kvalifikovanim certifikatima vodi evidenciju i obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju;

4) u svaki certifikat unese osnovne podatke o svom identitetu i omogući svakom zainteresovanom licu uvid u te podatke;

5) vodi ažurnu, tačnu i sigurnosnim mjerama zaštićenu evidenciju o validnosti certifikata;

6) obezbijedi vidljiv podatak o tačnom datumu i vremenu (čas i minut) izdavanja, suspenzije, isteka roka i opoziva certifikata, najmanje do dana isteka roka važenja koji je naveden u certifikatu;

7) čuva sve podatke i dokumentaciju o izdatim, suspendovanim, isteklim i opozvanim certifikatima za potrebe dokazivanja i verifikacije u sudskim, upravnim i drugim postupcima, najmanje deset godina od prestanka njihovog važenja, pri čemu podaci i prateća dokumentacija mogu biti u elektronskom obliku;

8) primjenjuje odredbe zakona i drugih propisa kojima je uređena zaštita podataka ličnosti.

Provjeru identiteta iz stava 1 tačka 2 ovog člana, kvalifikovani davalac elektronske usluge povjerenja vrši dobijanjem podataka na osnovu kojih se vrši provjera neposredno od fizičkog lica ili ovlašćenog predstavnika pravnog lica ili organa vlasti ili od drugog lica.

Provjera identiteta iz stava 1 tačka 2 ovog člana vrši se na neki od sljedećih načina:

1) uz prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica ili organa vlasti;

2) na daljinu, pomoću sredstava elektronske identifikacije, za koja je prije izdavanja kvalifikovanog certifikata obezbijeđeno prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica, ili organa vlasti i ako sistem za elektronsku identifikaciju iz kojeg su izdata ta sredstva ispunjavaju zahtjeve iz člana 60 ovog zakona u pogledu stepena sigurnosti "značajan" ili "visok";

3) pomoću certifikata kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata, koji je izdat uz provjeru na način iz tačke 1 ili tačke 2 ovog stava; ili

4) primjenom drugih metoda identifikacije koje u pogledu pouzdanosti pružaju sigurnost provjere identiteta jednaku provjeri identiteta na osnovu fizičkog prisustva.

Prije primjene metoda iz stava 3 tačka 4 ovog člana kvalifikovani davalac elektronskih usluga povjerenja dužan je da pribavi saglasnost Ministarstva za primjenu te metode.

Davalac elektronskih usluga povjerenja utvrđuje cijene elektronskih usluga povjerenja, uz prethodnu saglasnost Ministarstva.

Davanje obavještenja podnosiocima zahtjeva

Član 50

Davalac elektronskih usluga povjerenja, prije zaključivanja ugovora iz člana 45 stav 3 ovog zakona, mora dati obavještenje pravnom ili fizičkom licu koje je podnijelo zahtjev za izdavanje certifikata o svim važnim okolnostima za njegovo korišćenje.

Obavještenje iz stava 1 ovog člana obavezno sadrži:

- 1) izvod iz važećih propisa i internih akata iz člana 37 stav 4 ovog zakona;
- 2) podatke o eventualnim ograničenjima koja se odnose na korišćenje certifikata;
- 3) podatke o odgovarajućoj pravnoj zaštiti ili vansudskom poravnanju, ako na njega davalac usluga pristane u slučaju spora;
- 4) podatke o mjerama koje treba da realizuju potpisnici, odnosno autori elektronskog pečata i o tehnologiji potrebnoj za bezbjednu izradu i provjeru elektronskog potpisa.

Opoziv i suspenzija certifikata

Član 51

Davalac elektronskih usluga povjerenja dužan je da izvrši opoziv certifikata u slučaju kad:

- 1) opoziv certifikata zahtijeva potpisnik, odnosno autor elektronskog pečata ili njegov ovlašćeni zastupnik;
- 2) utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka;
- 3) primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata;
- 4) utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način;
- 5) utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata;
- 6) prestaje sa radom ili mu je rad zabranjen, a izdatim certifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja ne prenesu na drugog davaoca tih usluga;
- 7) istekne rok važenja certifikata;
- 8) primi sudsku odluku ili upravni akt koji se odnose na važenje certifikata ili
- 9) postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 ovog zakona.

Davalac elektronskih usluga povjerenja dužan je da na svojoj internet stranici objavi listu opozvanih certifikata, a opoziv certifikata proizvodi dejstvo od trenutka objavljivanja ove liste.

Ako se činjenice iz stava 1 ovog člana ne mogu odmah utvrditi na nesumnjiv način, davalac elektronskih usluga povjerenja dužan je da bez odlaganja suspenduje certifikat do utvrđivanja tih činjenica.

Datum i vrijeme suspenzije i opoziva certifikata unose se u evidenciju iz člana 49 stav 1 tačka 5 ovog zakona.

Davalac elektronskih usluga povjerenja dužan je da obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti iz stava 1 ovog člana.

Mjere zaštite certifikata

Član 52

Davalac elektronskih usluga povjerenja dužan je da:

- 1) primjenjuje organizacione i tehničke mjere zaštite certifikata i podataka vezanih za potpisnike i autore elektronskog pečata;
- 2) uspostavi i primjenjuje sistem zaštite pristupa evidenciji certifikata i opozvanih i suspendovanih certifikata koji će omogućiti pristup samo ovlašćenim licima i koji obezbjeđuje provjeru tačnosti prenosa podataka i blagovremeni uvid u eventualne greške tehničkih sredstava.

Mjere i aktivnosti iz stava 1 ovog člana, propisuje Ministarstvo.

Obaveze davaoca elektronske usluge povjerenja u slučaju raskida ugovora

Član 53

U slučaju da davalac elektronskih usluga povjerenja, zbog mogućeg stečaja ili potrebe, odnosno namjere prestanka poslovanja, raskida ugovor iz člana 45 stav 3 ovog zakona, dužan je da o tome obavijesti potpisnika, odnosno autora elektronskog pečata i Ministarstvo, najmanje tri mjeseca prije dana predviđenog za raskid ugovora.

Davalac elektronskih usluga povjerenja dužan je da obezbijedi nastavak vršenja elektronskih usluga povjerenja za potpisnike, odnosno autore elektronskog pečata kojima je izdao certifikate kod drugog davaoca usluga kojem dostavlja kompletnu dokumentaciju u vezi sa vršenjem elektronskih usluga povjerenja, a potpisnike, odnosno autore elektronskog pečata obavijesti o elektronskim uslugama povjerenja kod drugog davaoca elektronske usluge povjerenja.

Ako davalac elektronskih usluga povjerenja ne obezbijedi nastavak vršenja tih usluga kod drugog davaoca elektronske usluge povjerenja, dužan je da opozove sve izdate certifikate i o tome, odmah, a najkasnije u roku od 48 časova, obavijesti Ministarstvo i dostavi mu kompletnu dokumentaciju u vezi sa izvršenim elektronskim uslugama povjerenja.

Ministarstvo je dužno da odmah izvrši opoziv svih certifikata koje je izdao davalac elektronske usluge povjerenja koji iz bilo kog razloga nije opozvao izdate certifikate, a na trošak davaoca elektronske usluge povjerenja.

Obaveza povezivanja evidencija

Član 54

Davalac elektronskih usluga povjerenja dužan je da omogući povezanost svoje evidencije izdatih i evidencije opozvanih i suspendovanih certifikata sa drugim davaocima elektronskih usluga povjerenja uz primjenu dostupne informacione tehnologije i uz upotrebu tehničkih i programskih sredstava čije je djelovanje u skladu sa važećim međunarodnim standardima.

Osiguranje rizika od odgovornosti

Član 55

Kvalifikovani davalac elektronske usluge povjerenja dužan je da osigura rizik od odgovornosti za štete koje nastanu vršenjem elektronskih usluga povjerenja.

Najniži iznos osiguranja iz stava 1 ovog člana utvrđuje Ministarstvo.

Odgovornost za štetu

Član 56

Davalac elektronskih usluga povjerenja koji izdaje kvalifikovane certifikate ili garantuje za kvalifikovane certifikate drugog davaoca elektronskih usluga povjerenja odgovoran je za štetu pričinjenu licu koje se pouzdalo u taj certifikat, ako:

- 1) informacija koju sadrži kvalifikovani certifikat nije tačna u trenutku njegovog izdavanja;
- 2) certifikat ne sadrži sve elemente propisane za kvalifikovani certifikat;
- 3) nije obezbijedio da potpisnik, odnosno autor elektronskog pečata u trenutku izdavanja certifikata posjeduje podatke za izradu elektronskog potpisa, odnosno elektronskog pečata koji odgovaraju podacima za provjeru elektronskog potpisa, odnosno elektronskog pečata koji su dati, odnosno identifikovani u certifikatu;
- 4) ne obezbijedi da se podaci za izradu i podaci za provjeru elektronskog potpisa, odnosno elektronskog pečata mogu koristiti komplementarno, u slučaju kad te podatke kreira davalac elektronske usluge povjerenja;
- 5) propusti da opozove certifikat u skladu sa članom 51 ovog zakona;
- 6) certifikat ne sadrži informacije o ograničenjima koja se odnose na korišćenje.

Davalac elektronskih usluga povjerenja nije odgovoran za štetu iz stava 1 ovog člana, ako pred sudom ili drugim nadležnim organom dokaže da je postupao sa pažnjom dobrog privrednika.

Davalac elektronskih usluga povjerenja nije odgovoran za štetu koja je nastala zbog korišćenja certifikata mimo ograničenja, ukoliko su ta ograničenja jasno naznačena u certifikatu.

Davalac elektronskih usluga povjerenja odgovoran je za štetu pričinjenu potpisniku, odnosno autoru elektronskog pečata ili savjesnom trećem licu zbog nedostataka ili kašnjenja prilikom omogućavanja uvida u podatke o važenju, isteku ili suspenziji certifikata.

Prikupljanje i obrada podataka o ličnosti

Član 57

Davalac elektronskih usluga povjerenja može prikupljati podatke o ličnosti koji su neophodni za izdavanje i održavanje certifikata, neposredno od potpisnika ili posredno uz njegovu izričitu saglasnost.

Podaci prikupljeni u skladu sa stavom 1 ovog člana ne mogu biti obrađivani ili korišćeni za druge namjene bez izričite saglasnosti potpisnika.

Davalac elektronskih usluga povjerenja, na zahtjev potpisnika, može u certifikatu, umjesto punog imena potpisnika, unijeti njegov pseudonim nakon provjere njegovog identiteta.

Davalac elektronskih usluga povjerenja dužan je da podatke o identitetu potpisnika da državnom organu koji je zakonom ovlašćen za njihovo prikupljanje i obradu, na njegov zahtjev.

Davalac elektronskih usluga povjerenja može podatke iz stava 1 ovog člana prikupljati neposredno ili angažovanjem drugih fizičkih ili pravnih lica.

Upravljanje rizicima

Član 58

Davaoci elektronskih usluga povjerenja upravljaju rizicima i preduzimaju mjere u cilju povećanja stepena sigurnosti.

O povredi sigurnosti ili gubitku integriteta koji utiču na elektronsku uslugu povjerenja, davaoci elektronskih usluga povjerenja obavještavaju Ministarstvo, najkasnije u roku od 24 časa od saznanja za takvu povredu ili gubitak integriteta.

U slučaju da povreda sigurnosti i gubitak integriteta nepovoljno utiču na fizičko ili pravno lice kojem su pružene elektronske usluge povjerenja, davalac elektronskih usluga povjerenja obavještava to fizičko ili pravno lice.

U slučaju da se povreda sigurnosti ili gubitak integriteta iz stava 2 ovog člana odnosi na dvije ili više država članica Evropske unije, Ministarstvo obavještava nadzorne organe u drugim državama članicama na koje se to odnosi i Evropsku agenciju za mreže i informacionu bezbjednost (ENISA).

Ministarstvo obavještava javnost ili zahtijeva od davalaca elektronskih usluga povjerenja da to učine ako utvrdi da je otkrivanje povrede sigurnosti ili gubitka integriteta iz stava 2 ovog člana u javnom interesu.

Ministarstvo jednom godišnje dostavlja izvještaj o povredama sigurnosti i gubitku integriteta iz stava 2 ovog člana koje je primio od davaoca elektronskih usluga povjerenja Evropskoj agenciji za mreže i informacionu bezbjednost (ENISA).

VIII. ELEKTRONSKA IDENTIFIKACIJA

Upravljanje sistemom elektronske identifikacije

Član 59

Sistemima elektronske identifikacije upravljaju fizičko i pravno lice, kao i organ vlasti iz člana 4 st. 3 i 4 ovog zakona, u okviru kojih se izdaju sredstva elektronske identifikacije.

Stepen sigurnosti sistema elektronske identifikacije

Član 60

Sistem elektronske identifikacije može imati nizak, značajan ili visok stepen sigurnosti koji se odnosi i na sredstva elektronske identifikacije.

Stepeni sigurnosti iz stava 1 ovog člana su:

1) nizak stepen sigurnosti koji garantuje ograničen stepen pouzdanosti sredstva elektronske identifikacije u odnosu na traženi ili utvrđeni identitet lica;

2) značajan stepen sigurnosti koji garantuje značajan stepen pouzdanosti sredstva elektronske identifikacije u odnosu na traženi ili utvrđeni identitet lica;

3) visok stepen sigurnosti koji garantuje visok stepen pouzdanosti sredstva elektronske identifikacije u odnosu na traženi ili utvrđeni identitet lica.

Stepeni sigurnosti iz stava 2 ovog člana, podrazumijevaju pozivanje na tehničke specifikacije, standarde i prateće procedure, kao i tehničke kontrole čija je svrha smanjenje rizika od zloupotrebe ili promjene identiteta.

Stepene sigurnosti iz stava 2 ovog člana, određuje Ministarstvo u odnosu na minimalne tehničke standarde i prateće procedure.

Minimalne tehničke standarde i prateće procedure propisuje Ministarstvo.

Uslovi u vezi sa sistemom za elektronsku identifikaciju

Član 60a

Sistem elektronske identifikacije mora da ispunjava sljedeće uslove, i to da:

1) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema, ispunjavaju zahtjeve najmanje jednog od stepena sigurnosti iz člana 60 stav 2 ovog zakona;

2) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjeđuje da identifikacioni podaci na osnovu kojih se izdaju sredstva elektronske identifikacije nedvosmisleno predstavljaju fizičko lice, pravno lice, odnosno organ vlasti kojem se to sredstvo izdaje, u momentu izdavanja, u skladu sa tehničkim standardima i procedurama iz člana 60 stav 3 ovog zakona za odgovarajući stepen sigurnosti;

3) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjeđuje da ta sredstva budu izdata fizičkom licu, pravnom licu, odnosno organu vlasti na osnovu čijih identifikacionih podataka je sredstvo izdato, u skladu sa tehničkim standardima i procedurama iz člana 60 stav 3 ovog zakona za odgovarajući stepen sigurnosti i

4) sistem elektronske identifikacije ispunjava tehničke i operativne zahtjeve iz člana 61 stav 1 ovog zakona.

Ispunjenost uslova iz stava 1 ovog člana utvrđuje Ministarstvo.

Registar sistema elektronske identifikacije

Član 60b

Sistem elektronske identifikacije koji ispunjava uslove iz člana 60a ovog zakona upisuje se u registar sistema

elektronske identifikacije.

Registar sistema elektronske identifikacije sadrži:

- 1) opis sistema elektronske identifikacije,
- 2) stepen sigurnosti sistema elektronske identifikacije i sredstava elektronske identifikacije koji se izdaju u okviru tog sistema,
- 3) podatke o fizičkom licu, pravnom licu, odnosno organu vlasti koji upravljaju sistemom elektronske identifikacije i to za:

- pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj;

- fizičko lice: ime i prezime i poreski identifikacioni broj;

- 4) datum upisa sistema elektronske identifikacije, kao i izmjene i brisanja iz registra.

Registar sistema elektronske identifikacije vodi Ministarstvo.

Registar se vodi u elektronskom obliku pogodnom za automatsku obradu i dostupan je javnosti na internet stranici Ministarstva.

Registar potpisuje Ministarstvo naprednim elektronskim potpisom.

Interoperabilnost

Član 61

Sistemi elektronske identifikacije koji su upisani u registar sistema elektronske identifikacije moraju da ispunjavaju minimalne tehničke standarde i procedure iz člana 60 stav 3 ovog zakona i tehničke i operativne zahtjeve koji se odnose na čvor, operatera čvora i podatke o identitetu korisnika, i proces uspostavljanja okvira interoperabilnosti.

Čvor je mjesto priključenja sistema elektronske identifikacije, koji je dio strukture interoperabilnosti sistema elektronske identifikacije i ima mogućnost prepoznavanja i obrade, odnosno prosleđivanja prenosa podataka na druge čvorove i povezivanja sa sistemima elektronske identifikacije drugih država.

Čvor uspostavlja i njime upravlja Ministarstvo.

Tehničke i operativne zahtjeve koji se odnose na čvor, operatera čvora i podatke o identitetu korisnika, i proces uspostavljanja okvira interoperabilnosti propisuje Ministarstvo.

Saradnja

Član 62

Ministarstvo saraduje sa državama članicama Evropske unije u vezi sa:

- 1) interoperabilnošću sistema elektronske identifikacije koji su upisani u registar sistema elektronske identifikacije;
- 2) sigurnošću sistema elektronske identifikacije.

Saradnja iz stava 1 ovog člana podrazumijeva:

1) razmjenu informacija, iskustava i dobre prakse u vezi sa sistemima elektronske identifikacije, a naročito u vezi sa tehničkim zahtjevima koji se odnose na interoperabilnost i stepene sigurnosti koji se odnose na sisteme elektronske identifikacije;

2) razmjenu informacija, iskustva i dobre prakse u vezi sa stepenima sigurnosti koji se odnosi na sisteme elektronske identifikacije;

3) razmjenu informacija o ocjenjivanju usaglašenosti sistema elektronske identifikacije.

Priznavanje certifikata i sredstava elektronske identifikacije

Član 63

Kvalifikovani certifikati koje izdaju davaoci elektronskih usluga povjerenja sa sjedištem u jednoj od država članica Evropske Unije imaju isto pravno dejstvo kao i kvalifikovani certifikati izdati u Crnoj Gori.

Kad organ vlasti za uslugu koju pruža na internetu zahtijeva elektronsku identifikaciju pomoću sredstava elektronske identifikacije i autentifikacije radi pristupa toj usluzi, u skladu sa propisima, sredstvo elektronske identifikacije izdato u državi članici Evropske unije priznaje se za potrebe prekogranične autentifikacije ako:

1) je sredstvo elektronske identifikacije izdato u okviru sistema elektronske identifikacije koji je stavljen na listu notifikovanih sistema elektronske identifikacije koju je objavila Evropska komisija;

2) stepen sigurnosti sredstava elektronske identifikacije odgovara stepenu sigurnosti koji je jednak ili viši od stepena sigurnosti koji zahtijeva organ vlasti za pristup toj usluzi na internetu;

3) organ vlasti primjenjuje značajan ili visok stepen sigurnosti u odnosu na pristupanje toj usluzi na internetu.

Obavješćavanje Evropske komisije

Član 64

Ministarstvo dostavlja Evropskoj komisiji sljedeće informacije i, bez odlaganja, sve naknadne izmjene tih informacija

koje se odnose na:

- 1) opis sistema elektronske identifikacije i njegove stepene sigurnosti, podatke o fizičkom i pravnom licu, odnosno organu vlasti iz člana 4 st. 3 i 4 ovog zakona koji izdaje sredstva elektronske identifikacije;
- 2) važeći sistem nadzora i informacije o pravilima i odgovornosti fizičkog i pravnog lica, odnosno organa vlasti iz člana 4 st. 3 i 4 ovog zakona koji izdaje sredstva elektronske identifikacije, odnosno sprovodi proceduru autentifikacije;
- 3) fizičko i pravno lice, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona koji upravlja registracijom jedinstvenih ličnih identifikacionih podataka;
- 4) opis načina ispunjavanja tehničkih i operativnih zahtjeva koji se odnose na okvir interoperabilnosti iz člana 61 stav 4 ovog zakona;
- 5) opis autentifikacije iz člana 65 stav 1 tačka 6 ovog zakona;
- 6) suspenziju ili opoziv certifikata.

Ministarstvo može da podnese zahtjev Evropskoj komisiji za brisanje sistema elektronske identifikacije koji je upisan u registar sistema elektronske identifikacije sa liste notifikovanih sistema koju objavljuje Evropska komisija.

Prihvatljivost sistema elektronske identifikacije

Član 65

Sistem elektronske identifikacije prihvatljiv je za obavlještavanje iz člana 64 ovog zakona ako:

- 1) su sredstva elektronske identifikacije priznata od strane države članice Evropske unije;
- 2) sredstva elektronske identifikacije mogu da se koriste za pristup bilo kojoj usluzi koju pruža organ vlasti, a koja zahtijeva elektronsku identifikaciju u državi članici Evropske unije;
- 3) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema ispunjavaju zahtjeve bilo kojeg stepena sigurnosti iz člana 60 ovog zakona;
- 4) Ministarstvo obezbijedi da se lični identifikacioni podaci, u skladu sa tehničkim specifikacijama, standardima i procedurama za odgovarajući stepen sigurnosti iz člana 60 ovog zakona, pripisuju fizičkom ili pravnom licu koje koristi lične identifikacione podatke u elektronskom obliku u vrijeme kad su sredstva elektronske identifikacije izdata u okviru tog sistema;
- 5) davalac usluga elektronske identifikacije koji izdaje sredstva elektronske identifikacije u okviru tog sistema obezbijedi da se sredstva elektronske identifikacije pripisuju fizičkom ili pravnom licu koje koristi lične identifikacione podatke u elektronskom obliku u skladu sa odgovarajućim stepenom sigurnosti iz člana 60 ovog zakona;
- 6) Ministarstvo obezbijedi dostupnost autentifikacije na internetu, tako da zainteresovana strana može potvrditi lične identifikacione podatke primljene u elektronskom obliku.

Povreda sigurnosti

Član 66

U slučaju povrede ili djelimičnog ugrožavanja sistema elektronske identifikacije davaoca usluga elektronske identifikacije koji je upisan u registar sistema elektronske identifikacije, odnosno autentifikacije iz člana 65 stav 1 tačka 6 ovog zakona, na način koji utiče na pouzdanost prekogranične autentifikacije tog sistema, Ministarstvo, bez odlaganja, suspenduje ili opoziva tu prekograničnu autentifikaciju ili ugrožene djelove sistema elektronske identifikacije i obavještava države članice Evropske unije i Evropsku komisiju.

Kad je povreda ili ugrožavanje iz stava 1 ovog člana otklonjeno, Ministarstvo uspostavlja prekograničnu autentifikaciju i, bez odlaganja, obavještava druge države članice Evropske unije i Evropsku komisiju.

Ako povreda ili ugrožavanje iz stava 1 ovog člana nije otklonjeno u roku od tri mjeseca od suspenzije ili opoziva, Ministarstvo obavještava druge države članice Evropske unije i Evropsku komisiju o povlačenju sistema elektronske identifikacije.

Odgovornost

Član 67

Ministarstvo je odgovorno za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveza prilikom prekogranične transakcije u skladu sa članom 65 stav 1 tač. 4 i 6 ovog zakona.

Davalac usluga elektronske identifikacije koji izdaje sredstva elektronske identifikacije odgovoran je za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveza prilikom prekogranične transakcije iz člana 65 stav 1 tačka 5 ovog zakona.

Davalac usluga elektronske identifikacije koji sprovodi postupak autentifikacije odgovoran je za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveze obezbjeđenja ispravnog sprovođenja autentifikacije iz člana 65 stav 1 tačka 6 ovog zakona prilikom prekogranične transakcije.

IX. NADZOR

Upravni i inspekcijski nadzor

Član 68

Upravni nadzor nad sprovođenjem ovog zakona vrši Ministarstvo.

Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.

Obaveze inspekcije za usluge informacionog društva

Član 69

Inspekcija za usluge informacionog društva dužna je da Ministarstvu dostavi, do 1. marta tekuće za prethodnu kalendarsku godinu, izvještaj o aktivnostima iz svoje nadležnosti.

X. KAZNE NE ODREDBE

Član 70

Novčanom kaznom u iznosu od 1.000 do 10.000 eura kazniće se za prekršaj pravno lice, ako:

1) nema ažuriran plan prekida pružanja elektronske usluge povjerenja radi obezbjeđivanja njenog kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona (član 34 stav 1 tačka 1);

2) ne obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti (član 34 stav 1 tačka 2);

3) ne obezbijedi, na odgovarajući način i u skladu sa ovim zakonom i internim aktima iz člana 37 stav 4 ovog zakona, provjeru identiteta potpisnika i, po potrebi, drugog obilježja fizičkog i pravnog lica, kojima se izdaje kvalifikovani sertifikat za elektronski potpis, odnosno kvalifikovani sertifikat za elektronski pečat (član 34 stav 1 tačka 3);

4) nema zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje elektronskih usluga povjerenja, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka (član 34 stav 1 tačka 4);

5) ne koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa (član 34 stav 1 tačka 5);

6) ne preduzima mjere za spriječavanje falsifikovanja sertifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, ne garantuje tajnost procesa kreiranja tih podataka i ne dostavlja sertifikate potpisnicima na bezbjedan način (član 34 stav 1 tačka 6);

7) ne posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih sertifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih sertifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete (član 34 stav 1 tačka 7);

8) ne posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane sertifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih sertifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa (član 34 stav 1 tačka 8);

9) ne koristi pouzdan sistem čuvanja kvalifikovanih sertifikata u obliku koji omogućava provjeru podataka, kako bi unos i promjene podataka za izradu elektronskih usluga povjerenja vršila samo ovlašćena lica, kako bi mogla biti provjerena autentičnost podataka iz kvalifikovanog sertifikata, kako bi podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje i kako bi bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve bila vidljiva kvalifikovanom davaocu elektronskih usluga povjerenja (član 34 stav 1 tačka 9);

10) ne podnese Ministarstvu prijavu o promjenama u vršenju elektronskih usluga povjerenja (član 37 stav 3);

11) ne sprovede potpunu provjeru identiteta fizičkog lica, pravnog lica, odnosno organa vlasti kojem se izdaje kvalifikovani sertifikat (član 49 stav 1 tačka 2);

12) o izdatim kvalifikovanim sertifikatima ne vodi evidenciju i ne obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju (član 49 stav 1 tačka 3);

13) ne vodi ažurnu, tačnu i sigurnosnim mjerama zaštićenu evidenciju o validnosti sertifikata (član 49 stav 1 tačka 5);

14) ne da obavještenje pravnom ili fizičkom licu, koje je podnijelo zahtjev za izdavanje sertifikata o svim važnim okolnostima za njegovo korišćenje, prije zaključivanja ugovora iz člana 45 stav 3 ovog zakona (član 50);

15) ne izvrši opoziv sertifikata na zahtjev potpisnika, odnosno autora elektronskog pečata ili njegovog ovlašćenog zastupnika (član 51 stav 1 tačka 1);

16) ne izvrši opoziv sertifikata kad utvrdi daje podatak u sertifikatu pogrešan ili je sertifikat izdat na osnovu pogrešnih podataka (član 51 stav 1 tačka 2);

17) ne izvrši opoziv sertifikata kad primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime

potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje sertifikata (član 51 stav 1 tačka 3);

18) ne izvrši opoziv sertifikata kad utvrdi da su podaci za izradu elektronskog potpisa ili informacijski sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način (član 51 stav 1 tačka 4);

19) ne izvrši opoziv sertifikata kad utvrdi da su podaci za provjeru elektronskog potpisa ili informacijski sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost sertifikata (član 51 stav 1 tačka 5);

20) ne izvrši opoziv sertifikata kad prestaje sa radom ili mu je rad zabranjen, a izdatim sertifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja ne prenesu na drugog davaoca tih usluga (član 51 stav 1 tačka 6);

21) ne izvrši opoziv sertifikata kad istekne rok važenja sertifikata (član 51 stav 1 tačka 7);

22) ne izvrši opoziv sertifikata kad primi sudsku odluku ili upravni akt koji se odnose na važenje sertifikata (član 51 stav 1 tačka 8);

23) ne izvrši opoziv sertifikata kad postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 ovog zakona (član 51 stav 1 tačka 9);

24) ne objavi na svojoj internet stranici listu opozvanih sertifikata (član 51 stav 2);

25) bez odlaganja ne suspenduje sertifikat do utvrđivanja činjenica iz člana 51 stav 1 ovog zakona, ako se činjenice ne mogu odmah utvrditi na nesumnjiv način (član 51 stav 3);

26) ne obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu sertifikata u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog kojih se sertifikat suspenduje odnosno opoziva (član 51 stav 5);

27) ne primjenjuje organizacione i tehničke mjere zaštite sertifikata i podataka vezanih za potpisnike i autore elektronskog pečata (član 52 stav 1 tačka 1);

28) ne uspostavi i ne primjenjuje sistem zaštite pristupa evidenciji sertifikata i opozvanih i suspendovanih sertifikata koji će omogućiti pristup samo ovlašćenim licima i koji obezbjeđuje provjeru tačnosti prenosa podataka i blagovremeni uvid u eventualne greške tehničkih sredstava (član 52 stav 1 tačka 2);

29) ne obavijesti potpisnika, odnosno autora elektronskog pečata i Ministarstvo, najmanje tri mjeseca prije dana predviđenog za raskid ugovora, da raskida ugovor iz člana 45 stav 3 ovog zakona, zbog mogućeg stečaja ili potrebe, odnosno namjere prestanka poslovanja (član 53 stav 1);

30) ne obezbijedi nastavak vršenja elektronskih usluga povjerenja za potpisnike, odnosno autore elektronskog pečata, kojima je izdao sertifikate kod drugog davaoca usluga kojem dostavlja kompletnu dokumentaciju u vezi sa vršenjem elektronskih usluga povjerenja, a potpisnike, odnosno autore elektronskog pečata ne obavijesti o uslovima elektronskih usluga povjerenja kod drugog davaoca elektronske usluge povjerenja (član 53 stav 2);

31) ne opozove sve izdate sertifikate i o tome, odmah, a najkasnije u roku od 48 časova, ne obavijesti Ministarstvo i ne dostavi mu kompletnu dokumentaciju u vezi sa izvršenim elektronskim uslugama povjerenja ako ne obezbijedi nastavak vršenja tih usluga kod drugog davaoca elektronske usluge povjerenja, (član 53 stav 3);

32) ne omogući povezanost svoje evidencije izdatih i evidencije opozvanih i suspendovanih sertifikata sa drugim davaocima elektronskih usluga povjerenja uz primjenu dostupne informacione tehnologije i uz upotrebu tehničkih i programskih sredstava čije je djelovanje u skladu sa važećim međunarodnim standardima (član 54);

33) ne osigura rizik od odgovornosti za štete koje nastanu vršenjem elektronskih usluga povjerenja (član 55 stav 1);

34) ne da podatke o identitetu potpisnika državnom organu koji je zakonom ovlašćen za njihovo prikupljanje i obradu, na njegov zahtjev (član 57 stav 4).

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 150 eura do 2 000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu vlasti novčanom kaznom u iznosu od 150 eura do 2 000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom u iznosu od 150 do 1000 eura.

Član 71

Novčanom kaznom u iznosu od 500 eura do 5.000 eura kazniće se za prekršaj pravno lice ako:

1) odbije prijem elektronskog dokumenta sa elektronskim potpisom ili naprednim elektronskim potpisom, samo zato što je u elektronskom obliku (član 13);

2) odbije prijem podataka poslatih i primljenih upotrebom usluge elektronske preporučene dostave, samo zato što je u elektronskom obliku ili zbog toga što ne ispunjavaju sve zahtjeve kvalifikovane usluge elektronske preporučene dostave (član 29).

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 2 000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu vlasti novčanom kaznom u iznosu od 30 eura do 2 000 eura.

Član 72

Novčanom kaznom u iznosu od 500 do 5.000 eura kazniće se za prekršaj pravno lice, ako:

1) ne čuva pažljivo sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata, kao i podatke za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata od neovlašćenog pristupa i upotrebe i ne koristi ih u skladu sa ovim zakonom (član 46 stav 1);

2) neovlašćeno pristupi i upotrijebi sredstva za izradu elektronskog potpisa, elektronskog pečata ili elektronskog vremenskog pečata kao i podatke za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata (član 46 stav 2);

3) davaocu elektronskih usluga povjerenja, ne dostavi sve potrebne podatke i informacije o promjenama koje utiču ili mogu uticati na tačnost utvrđivanja njegovog identiteta, odmah, a najkasnije u roku od 48 časova od nastanka promjene (član 47 stav 1);

4) odmah ne zahtijeva opoziv ili suspenziju certifikata u slučaju gubitka ili oštećenja sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata ili gubitka podataka za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata (član 47 stav 2 tačka 1);

5) odmah ne zahtijeva opoziv ili suspenziju certifikata koji mu je izdat kad posumnja u povjerljivost podataka za izradu elektronskog potpisa, odnosno elektronskog pečata ili elektronskog vremenskog pečata (član 47 stav 2 tačka 2).

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 2 000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom u iznosu od 30 do 1000 eura.

XI. PRELAZNE I ZAVRŠNE ODREDBE

Član 73

Podzakonski akti za sprovođenje ovog zakona donijeće se u roku od 12 mjeseci od dana stupanja na snagu ovog zakona.

Član 73a

Podzakonski akti donijeti na osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu ("Službeni list CG", broj 31/17) uskladiće se sa ovim zakonom u roku od 12 mjeseci od dana stupanja na snagu ovog zakona.

Član 74

Odredbe člana 10 stav 3, čl. 22, 36, člana 40 st. 2 i 6, člana 43, člana 45 stav 4, člana 58 st. 4 i 6, i čl. 62 do 67 ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

Član 75

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o elektronskom potpisu ("Službeni list RCG" broj 55/03 i "Službeni list CG", br. 41/10 i 40/11).

Član 75a

Kvalifikovani sertifikati za elektronski potpis i sredstva za izradu elektronskog potpisa, koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis, izdati do dana stupanja na snagu ovog zakona smatraju se kvalifikovanim sertifikatima za elektronski potpis, odnosno kvalifikovanim sredstvima za izradu elektronskog potpisa u skladu sa ovim zakonom do datuma isteka roka važenja tih certifikata.

Član 76

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".