

Na osnovu člana 95 tačka 3 Ustava Crne Gore donosim

U K A Z
O PROGLAŠENJU ZAKONA O ELEKTRONSKOJ
IDENTIFIKACIJI I ELEKTRONSKOM POTPISU

Proglašavam **Zakon o elektronskoj identifikaciji i elektronskom potpisu**, koji je donijela Skupština Crne Gore 26. saziva, na Petoj sjednici Prvog redovnog (proljećnjeg) zasijedanja u 2017. godini, dana 27. aprila 2017. godine.

Broj: 01-447/2

Podgorica, 08.05.2017.



Na osnovu člana 82 stav 1 tačka 2 i člana 91 stav 1 Ustava Crne Gore, Skupština Crne Gore 26. saziva, na Petoj sjednici Prvog redovnog (proljećnjeg) zasijedanja u 2017. godini, dana 27. aprila 2017. godine, donijela je

ZAKON O ELEKTRONSKOJ IDENTIFIKACIJI I ELEKTRONSKOM POTPISU

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

Korišćenje elektronskog potpisa, elektronskog pečata, elektronskog vremenskog pečata, elektronskog dokumenta i usluge elektronske preporučene dostave u pravnom prometu, upravnim, sudskim i drugim postupcima podrazumijeva elektronsku identifikaciju fizičkih i pravnih lica koja koriste te usluge, u skladu sa ovim zakonom.

Elektronska identifikacija je postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koje na jedinstven način predstavljaju fizičko ili pravno lice.

Usluge certifikovanja za elektronske transakcije

Član 3

Usluge izrade, verifikacije i čuvanja elektronskih potpisa, elektronskih pečata i elektronskih vremenskih pečata, usluge elektronske preporučene dostave i izdavanje certifikata koji se odnose na te usluge, izradu i verifikaciju certifikata za autentifikaciju internet stranice i usluge čuvanja elektronskih potpisa, elektronskog pečata i izdavanje certifikata koji se odnose na te usluge (u daljem tekstu: usluge certifikovanja za elektronske transakcije) vrši pravno ili fizičko lice, koje ispunjava uslove propisane ovim zakonom (u daljem tekstu: davalac usluge certifikovanja za elektronske transakcije).

Usluge certifikovanja za elektronske transakcije za organe državne uprave može vršiti i organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja (u daljem tekstu: Ministarstvo).

Ocjenjivanje usaglašenosti kvalifikovanih usluga certifikovanja za elektronske transakcije

Član 4

Ocjenjivanje usaglašenosti usluga certifikovanja za elektronske transakcije za koje su ovim zakonom propisani posebni zahtjevi (u daljem tekstu: kvalifikovane usluge certifikovanja za elektronske transakcije), kao i uslova koje u skladu sa ovim zakonom moraju ispunjavati pravno ili fizičko lice koje vrši kvalifikovanu uslugu certifikovanja za elektronske transakcije (u daljem tekstu: kvalifikovani davalac usluge certifikovanja za elektronske transakcije) vrši Ministarstvo.

Kvalifikovani davalac usluge certifikovanja za elektronske transakcije upisuje se u registar davalaca kvalifikovane usluge certifikovanja za elektronske transakcije, koji vodi Ministarstvo.

Dostupnost usluga certifikovanja za elektronske transakcije licima sa invaliditetom

Član 5

Usluge certifikovanja za elektronske transakcije i proizvodi koji se koriste prilikom pružanja tih usluga, kad je to moguće, dostupni su licima sa invaliditetom.

Proizvodi koji se koriste prilikom pružanja usluga certifikovanja za elektronske transakcije podrazumijevaju odgovarajuću računarsku opremu (hardver) ili računarski program (softver) koji su namijenjeni za korišćenje u svrhu pružanja usluga certifikovanja za elektronske transakcije.

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) **lični identifikacioni podaci** obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica;
- 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 ili pravno lice koje se oslanja na elektronsku identifikaciju ili uslugu certifikovanja za elektronske transakcije;
- 4) **potpisnik** je fizičko lice koje posjeduje sredstvo za izradu elektronskog potpisa kojim se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica;
- 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 koje posjeduje sredstvo za izradu elektronskog pečata i izrađuje elektronski pečat;
- 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 i potvrđuje naziv tog pravnog lica;
- 9) **kvalifikovani certifikat za elektronski pečat** je certifikat za elektronski pečat koji izdaje kvalifikovani davalac usluge certifikovanja za elektronske transakcije i koji ispunjava posebne uslove propisane ovim zakonom;
- 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 usluga certifikovanja za elektronske transakcije 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 za kvalifikovani elektronski potpis koji sadrži podatke propisane ovim zakonom i kojeg izdaje kvalifikovani davalac usluga certifikovanja za elektronske transakcije.

Kvalifikovani certifikat za elektronski potpis mora da sadrži:

- 1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis;
- 2) identifikacioni skup podataka o pravnom ili fizičkom licu koje izdaje kvalifikovani certifikat za elektronski potpis uz navođenje države u kojoj je davalac usluga registrovan, i to:
 - za pravno lice: naziv, matični broj i poreski identifikacioni broj,
 - za fizičko lice: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište;
- 3) identifikacioni skup podataka o potpisniku (lično ime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište);
- 4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa i koji su pod kontrolom potpisnika;
- 5) podatke o periodu važenja kvalifikovanog certifikata za elektronski potpis;
- 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za elektronski potpis koja mora biti jedinstvena za kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;

7) napredni elektronski potpis kvalifikovanog davaoca usluge certifikovanja za elektronske transakcije koji izdaje certifikat;

8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;

9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za elektronski potpis;

10) odgovarajuću naznaku, u obliku pogodnom za automatsku obradu, 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 certifikat, 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.

Gubitak validnosti kvalifikovanog certifikata za elektronski potpis i privremena suspenzija

Član 17

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

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

Kvalifikovani elektronski potpis gubi validnost za vrijeme suspenzije kvalifikovanog certifikata 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 certifikata 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.

Sredstva iz stava 1 ovog člana izdaju se fizičkim ili pravnim licima putem sistema elektronske identifikacije koji koristi davalac usluga certifikovanja za elektronske transakcije za vršenje usluga certifikovanja za elektronske transakcije.

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 usluge certifikovanja za elektronske transakcije.

Kvalifikovani davalac usluga certifikovanja za elektronske transakcije 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.

Obavještanje 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, obavještava 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 usluge certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije 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 pružati samo kvalifikovani davalac usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije.

Shodna primjena

Član 27

Na pravno dejstvo, punovažnost i prihvatljivost elektronskog pečata, elektronskog vremenskog pečata i kvalifikovanog elektronskog pečata, zahtjeve za napredni elektronski pečat, sadržaj kvalifikovanog elektronskog pečata i elektronskog vremenskog pečata, izdavanje, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, kvalifikovana sredstva za izradu elektronskog pečata i elektronskog vremenskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata i sredstva za izradu elektronskog vremenskog pečata, verifikaciju i čuvanje kvalifikovanog sredstva za izradu elektronskog pečata i sredstva za izradu elektronskog vremenskog pečata shodno se primjenjuju odredbe čl. 9 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

Organ vlasti, odnosno pravno lice 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 usluga certifikovanja za elektronske transakcije;
- 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 usluga certifikovanja za elektronske transakcije, 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 usluga certifikovanja za elektronske transakcije, zahtjevi iz stava 1 ovog člana odnose se na sve kvalifikovane davaoce usluga certifikovanja za elektronske transakcije.

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 kvalifikovane usluge certifikovanja za elektronske transakcije, a koji ispunjava posebne uslove propisane ovim zakonom.

Kvalifikovani certifikati za autentifikaciju internet stranica

Član 33

Kvalifikovani certifikat za autentifikaciju internet stranica mora da sadrži:

- 1) oznaku u elektronskom obliku pogodnom za automatsku obradu da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranica;
- 2) identifikacioni skup podataka o pravnom ili fizičkom licu koje izdaje kvalifikovani certifikat za elektronski potpis uz navođenje države u kojoj je davalac usluga registrovan, i to:
 - za pravno lice: naziv, matični broj i poreski identifikacioni broj;
 - za fizičko lice: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište;
- 3) identifikacioni skup podataka o fizičkom licu kome je izdat certifikat, i to: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište, adresu, grad i državu;
- 4) naziv domena kojim upravlja fizičko ili pravno lice kojem je izdat certifikat za autentifikaciju internet stranice;
- 5) podatke o periodu važenja kvalifikovanog certifikata za autentifikaciju internet stranice;
- 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;
- 7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije koji izdaje certifikat;
- 8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;
- 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za autentifikaciju internet stranica.

V. USLOVI ZA VRŠENJE KVALIFIKOVANIH USLUGA CERTIFIKOVANJA ZA ELEKTRONSKE TRANSAKCIJE

Uslovi u vezi sa kvalifikovanim davaocima usluga certifikovanja za elektronske transakcije

Član 34

Kvalifikovani davalac usluga certifikovanja za elektronske transakcije mora da ispunjava sljedeće uslove, i to da:

- 1) ima ažuriran plan prekida pružanja usluge 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 certifikat za elektronski potpis, odnosno kvalifikovani certifikat za elektronski pečat;

4) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje usluga certifikovanja za elektronske transakcije, 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 certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja certifikate potpisnicima na bezbjedan način;

7) posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih certifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik;

8) posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih certifikata 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 certifikata u obliku koji omogućava provjeru, kako bi:

- unos i promjene podataka za izradu usluga certifikovanja za elektronske transakcije vršila samo ovlašćena lica,
- mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata,
- 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 usluga certifikovanja za elektronske transakcije.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

Uslovi za vršenje kvalifikovanih usluga certifikovanja za elektronske transakcije za organe državne uprave

Član 35

Ako kvalifikovane usluge certifikovanja za elektronske transakcije za organe državne uprave vrši Ministarstvo, moraju biti ispunjeni uslovi iz člana 34 stav 1 tač. 1 do 6 i tač. 8 i 9 ovog zakona.

Način vršenja kvalifikovanih usluga certifikovanja za elektronske transakcije iz stava 1 ovog člana propisuje Vlada Crne Gore.

Pravno dejstvo kvalifikovanih certifikata izdatih u drugoj državi

Član 36

Kvalifikovane usluge certifikovanja za elektronske transakcije u Crnoj Gori mogu vršiti i davaoci usluga certifikovanja za elektronske transakcije sa sjedištem u drugoj državi.

Kvalifikovani certifikati koje izdaju davaoci usluga certifikovanja za elektronske transakcije sa sjedištem u drugoj državi koja nije članica Evropske unije, imaju isto pravno dejstvo kao i kvalifikovani certifikati izdati u Crnoj Gori, ako:

1) davalac usluga certifikovanja za elektronske transakcije ispunjava uslove propisane ovim zakonom za izdavanje kvalifikovanih certifikata i upisan je u registar kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije u Crnoj Gori ili je registrovan u državi članici Evropske unije;

2) kvalifikovani davalac usluga certifikovanja za elektronske transakcije koji je upisan u registar kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije u Crnoj Gori ili je registrovan u državi članici Evropske unije garantuje za takav kvalifikovani certifikat;

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 usluga certifikovanja za elektronske transakcije ispunjava uslove utvrđene propisima Evropske unije za izdavanje kvalifikovanih certifikata i ako je registrovan u državi članici Evropske unije;

Certifikati davaoca usluga certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije

Član 37

Usluge certifikovanja za elektronske transakcije može da vrši davalac usluge certifikovanja za elektronske transakcije koji je upisan u evidenciju davalaca usluga certifikovanja za elektronske transakcije (u daljem tekstu: evidencija), koju vodi Ministarstvo.

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

Davalac usluge certifikovanja za elektronske transakcije dužan je da o promjenama u vršenju usluga certifikovanja za elektronske transakcije Ministarstvu podnese prijavu.

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

Upis u evidenciju

Član 38

Upis u evidenciju vrši se odmah nakon podnošenja prijave o početku obavljanja usluge certifikovanja za elektronske transakcije.

Evidencija sadrži podatke o davaocu usluge certifikovanja za elektronske transakcije 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 sadrži i podatke o sistemu elektronske identifikacije uključujući stepene njegove sigurnosti.

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 pružanje kvalifikovanih usluga certifikovanja za elektronske transakcije

Član 39

Davalac usluga certifikovanja za elektronske transakcije koji je upisan u evidenciju, može Ministarstvu podnijeti zahtjev za upis u registar kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije (u daljem tekstu: registar).

Uz zahtjev iz stava 1 ovog člana, davalac usluga certifikovanja za elektronske transakcije dužan je da priloži dokumentaciju kojom dokazuje da ispunjava uslove iz člana 34 ovog zakona.

O ispunjenosti uslova za pružanje kvalifikovanih usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije koji imaju sjedište u drugoj državi, na njihov zahtjev, ako ispunjavaju uslove iz člana 34 ovog zakona.

Registar sadrži podatke o kvalifikovanom davaocu usluge certifikovanja za elektronske transakcije 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 sadrži i podatke o sistemu elektronske identifikacije uključujući stepene njegove sigurnosti.

Registar se vodi u elektronskom obliku pogodnom za automatsku obradu 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 usluga certifikovanja za elektronske transakcije, kao i o namjeri da prestane da vrši te usluge, kvalifikovani davalac usluge certifikovanja za elektronske transakcije dužan je da obavijesti Ministarstvo.

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

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

Naznaka o upisu u registar u certifikatima

Član 42

Kvalifikovani davalac usluge certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije može da koristi oznaku certifikovanja EU kako bi na jednostavan, prepoznatljiv i jasan način naznačio kvalifikovane usluge certifikovanja za elektronske transakcije.

VII. PRAVA, OBAVEZE I ODGOVORNOSTI POTPISNIKA, AUTORA ELEKTRONSKOG PEČATA I DAVALACA USLUGA CERTIFIKOVANJA ZA ELEKTRONSKE TRANSAKCIJE

Izdavanje certifikata

Član 44

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

Pravo na izbor davaoca usluga certifikovanja za elektronske transakcije

Član 45

Pravno ili fizičko lice samostalno vrši izbor davaoca usluga certifikovanja za elektronske transakcije.

Pravno ili fizičko lice može koristiti usluge certifikovanja za elektronske transakcije jednog ili više davalaca usluga certifikovanja za elektronske transakcije.

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

Pravno ili fizičko lice može koristiti usluge certifikovanja za elektronske transakcije davaoca usluge certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije

Član 49

Davalac usluga certifikovanja za elektronske transakcije dužan je da:

- 1) obezbijedi da svaki kvalifikovani certifikat sadrži podatke iz člana 16 ovog zakona;
- 2) sprovede potpunu provjeru identiteta potpisnika;
- 3) obezbijedi tačnost i cjelovitost podataka koje unosi u evidenciju izdatih certifikata;
- 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.

Davalac usluga certifikovanja za elektronske transakcije utvrđuje cijene usluga certifikovanja za elektronske transakcije, uz prethodnu saglasnost Ministarstva.

Davanje obavještenja podnosiocima zahtjeva

Član 50

Davalac usluga certifikovanja za elektronske transakcije, 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 usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije ugroženi na način koji utiče na pouzdanost i pouzdanost certifikata;
- 6) prestaje sa radom ili mu je rad zabranjen, a izdatim certifikatima nije istekao rok važenja, osim ako usluge certifikovanja ne prenesu na drugog davaoca tih usluga;

- 7) istekne rok važenja certifikata;
- 8) primi sudsku odluku ili upravni akt koji se odnose na vađenje certifikata ili
- 9) postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 ovog zakona.

Davalac usluga certifikovanja za elektronske transakcije dužan je da na svojoj internet stranici objavi listu opozvanih certifikata.

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

Suspenzija i opoziv certifikata obavezno sadrže datum i vrijeme donošenja, a proizvode dejstvo od trenutka unošenja u evidenciju suspendovanih i opozvanih certifikata.

Davalac usluga certifikovanja za elektronske transakcije 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 zbog koje se certifikat suspenduje, odnosno opoziva.

Mjere zaštite certifikata

Član 52

Davalac usluga certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije u slučaju raskida ugovora

Član 53

U slučaju da davalac usluga certifikovanja za elektronske transakcije, 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 usluga certifikovanja za elektronske transakcije dužan je da obezbijedi nastavak vršenja usluga certifikovanja za elektronske transakcije za potpisnike, odnosno autore elektronskog pečata kojima je izdao certifikate kod drugog davaoca usluga kojem dostavlja kompletnu dokumentaciju u vezi sa vršenjem usluga certifikovanja za elektronske transakcije, a potpisnike, odnosno autore elektronskog pečata obavijesti o uslovima certifikovanja za elektronske transakcije kod drugog davaoca usluge certifikovanja za elektronske transakcije.

Ako davalac usluga certifikovanja za elektronske transakcije ne obezbijedi nastavak vršenja tih usluga kod drugog davaoca usluge certifikovanja za elektronske transakcije, 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 uslugama certifikovanja za elektronske transakcije.

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

Obaveza povezivanja evidencija

Član 54

Davalac usluga certifikovanja za elektronske transakcije dužan je da omogući povezanost svoje evidencije izdatih i evidencije opozvanih i suspendovanih certifikata sa drugim davaocima usluga certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije dužan je da osigura rizik od odgovornosti za štete koje nastanu vršenjem usluga certifikovanja za elektronske transakcije.

Najniži iznos osiguranja iz stava 1 ovog člana utvrđuje Ministarstvo.

Odgovornost za štetu

Član 56

Davalac usluga certifikovanja za elektronske transakcije koji izdaje kvalifikovane certifikate ili garantuje za kvalifikovane certifikate drugog davaoca usluga certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije;
- 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 usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije nije odgovoran za štetu koja je nastala zbog korišćenja certifikata mimo ograničenja, ukoliko su ta ograničenja jasno naznačena u certifikatu.

Davalac usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije, na zahtjev potpisnika, može u certifikatu, umjesto punog imena potpisnika, unijeti njegov pseudonim nakon provjere njegovog identiteta.

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

Davalac usluga certifikovanja za elektronske transakcije može podatke iz stava 1 ovog člana prikupljati neposredno ili angažovanjem drugih fizičkih ili pravnih lica.

Upravljanje rizicima

Član 58

Davaoci usluga certifikovanja za elektronske transakcije upravljaju rizicima i preduzimaju mjere u cilju povećanja stepena sigurnosti.

O povredi sigurnosti ili gubitku integriteta koji utiču na uslugu certifikovanja za elektronske transakcije, davaoci usluga certifikovanja za elektronske transakcije 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 usluge certifikovanja za elektronske transakcije, davalac usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije 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 usluga certifikovanja za elektronske transakcije Evropskoj agenciji za mreže i informacionu bezbjednost (ENISA).

VIII. ELEKTRONSKA IDENTIFIKACIJA

Sistem elektronske identifikacije

Član 59

Sistem elektronske identifikacije je sistem za izdavanje sredstava elektronske identifikacije, prilikom pružanja usluga certifikovanja za elektronske transakcije.

Sredstvo elektronske identifikacije je računarska oprema (hardver) ili računarski program (softver), koje sadrži lične identifikacione podatke u elektronskom obliku, a koji se koriste za autentifikaciju usluga u elektronskom obliku

Stepen sigurnosti sistema elektronske identifikacije

Član 60

Sistem elektronske identifikacije davaoca usluga certifikovanja za elektronske transakcije koji je upisan u evidenciju, odnosno u registar može imati nizak, značajan ili visok stepen sigurnosti koji se odnosi na sredstva elektronske identifikacije.

Stepeni sigurnosti iz stava 1 ovog člana su:

- 1) nizak stepen sigurnosti koji garantuje ograničen stepen pouzdanosti elektronske transakcije u odnosu na traženi ili utvrđeni identitet lica;
- 2) značajan stepen sigurnosti koji garantuje značajan stepen pouzdanosti elektronske transakcije u odnosu na traženi ili utvrđeni identitet lica;
- 3) visok stepen sigurnosti koji garantuje visok stepen pouzdanosti elektronske transakcije 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.

Interoperabilnost

Član 61

Sistemi elektronske identifikacije davalaca usluga certifikovanja koji su upisani u evidenciju, odnosno u registar moraju da budu interoperabilni.

U cilju uspostavljanja interoperabilnosti iz stava 1 ovog člana, Ministarstvo propisuje okvir za interoperabilnost koji mora da ispunjava sljedeće kriterijume i to da:

- 1) ima za cilj tehnološku neutralnost i ne pravi razliku između posebnih tehničkih rješenja za elektronsku identifikaciju;
- 2) se pridržava evropskih i međunarodnih standarda, kad je to moguće;
- 3) na obradu ličnih podataka primjenjuje propise o zaštiti podataka o ličnosti.

Saradnja

Član 62

Ministarstvo saraduje sa državama članicama Evropske unije u vezi sa:

- 1) interoperabilnošću sistema elektronske identifikacije koji su upisani u evidenciju i registar;
- 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 usluga certifikovanja za elektronske transakcije 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 prístup toj usluzi na internetu;

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

Obavještanje 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, uključujući njegove stepene sigurnosti i davaoca, odnosno davaoca usluge certifikovanja za elektronske transakcije sredstava u okviru tog sistema;
- 2) važeći sistem nadzora i informacije o pravilima i odgovornosti davaoca usluga certifikovanja za elektronske transakcije koji izdaje sredstva elektronske identifikacije, odnosno sprovodi proceduru autentifikacije;
- 3) davaoca usluga certifikovanja za elektronske transakcije koji upravlja registracijom jedinstvenih ličnih identifikacionih podataka;
- 4) opis načina ispunjavanja kriterijuma iz člana 61 stav 2 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 evidenciju, odnosno u registar sa liste notifikovanih sistema koju objavljuje Evropska komisija.

Prihvatljivost sistema elektronske identifikacije

Član 65

Sistem elektronske identifikacije prihvatljiv je za obavještanje 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 certifikovanja za elektronske transakcije 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 certifikovanja za elektronske transakcije 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 certifikovanja za elektronske transakcije koji je upisan u evidenciju ili registar, 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 certifikovanja za elektronske transakcije 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 certifikovanja za elektronske transakcije 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 inspeksijski nadzor

Član 68

Upravni nadzor nad sprovođenjem ovog zakona vrši Ministarstvo.

Inspeksijski nadzor nad radom davalaca usluga certifikovanja za elektronske transakcije i kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspeksijski 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. KAZNENE 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 usluge 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 certifikat za elektronski potpis, odnosno kvalifikovani certifikat za elektronski pečat (član 34 stav 1 tačka 3);

4) nema zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje usluga certifikovanja za elektronske transakcije, 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 sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, ne garantuje tajnost procesa kreiranja tih podataka i ne dostavlja certifikate 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 certifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik (član 34 stav 1 tačka 7);

8) ne posjeduje sistem čuvanja svih relevantnih informacija koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih certifikata 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 certifikata u obliku koji omogućava provjeru podataka, kako bi unos i promjene podataka za izradu usluga certifikovanja za elektronske transakcije vršila samo ovlašćena lica, kako bi mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata, 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 usluga certifikovanja za elektronske transakcije (član 34 stav 1 tačka 9);

10) ne podnese Ministarstvu prijavu o promjenama u vršenju usluga certifikovanja za elektronske transakcije (član 37 stav 3);

11) ne sprovede potpunu provjeru identiteta potpisnika (član 49 stav 1 tačka 2);

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

13) ne da obavještenje pravnom ili fizičkom licu, koje je podnijelo zahtjev za izdavanje certifikata o svim važnim okolnostima za njegovo korišćenje, prije zaključivanja ugovora iz člana 45 stav 3 ovog zakona (član 50 stav 1);

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

15) ne izvrši opoziv certifikata kad utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka (član 51 stav 1 tačka 2);

16) ne izvrši opoziv certifikata 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 certifikata (član 51 stav 1 tačka 3);

17) ne izvrši opoziv certifikata kad 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 (član 51 stav 1 tačka 4);

18) ne izvrši opoziv certifikata kad utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca usluga certifikovanja za elektronske transakcije ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata (član 51 stav 1 tačka 5);

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

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

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

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

23) ne objavi na svojoj internet stranici listu opozvanih certifikata. (član 51 stav 2);

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

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

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

27) ne uspostavi i ne 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 (član 52 stav 1 tačka 2);

28) 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);

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

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

31) ne omogući povezanost svoje evidencije izdatih i evidencije opozvanih i suspendovanih certifikata sa drugim davaocima usluga certifikovanja za elektronske transakcije uz primjenu dostupne informacione tehnologije i uz upotrebu tehničkih i programskih sredstava čije je djelovanje u skladu sa važećim međunarodnim standardima (član 54);

32) ne osigura rizik od odgovornosti za štete koje nastanu vršenjem usluga certifikovanja za elektronske transakcije (član 55 stav 1);

33) 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 državne uprave 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 državnom organu novčanom kaznom u iznosu od 30 eura do 2 000 eura.

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

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

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu lokalne uprave 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 stav2);

3) davaocu usluga certifikovanja za elektronske transakcije, 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 74

Odredbe člana 10 stav 3, čl. 22, 36, člana 40 st. 2 i 7, 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 76

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

Broj: 10-2/17-1/4

EPA 105 XXVI

Podgorica, 27. aprila 2017. godine

SKUPŠTINA CRNE GORE 26. SAZIVA

