PREDLOG

ZAKON O ELEKTRONSKOJ IDENTIFIKACIJI I USLUGAMA POVJERENJA*

I. OSNOVNE ODREDBE

Predmet
Član 1

Ovim zakonom propisuju se uslovi pod kojima se pružaju, priznaju i prihvataju sredstva elektronske identifikacije, a naročito i novčanici digitalnog identiteta i pravila za elektronske usluge povjerenja, kako bi se fizičkim i pravnim licima, odnosno organima vlasti omogućilo i olakšalo ostvarivanje prava na bezbjedno učešće u digitalnom društvu i pristup elektronskim uslugama.

Primjena
Član 2

Ovaj zakon primjenjuje se na sisteme elektronske identifikacije, novčanike digitalnog identiteta i na davaoce usluga povjerenja koji su registrovani u Crnoj Gori.

Izuzeće od primjene
Član 3

Ovaj zakon ne primjenjuje se na pružanje elektronskih usluga povjerenja (u daljem tekstu: usluge povjerenja) koje se koriste isključivo u zatvorenim sistemima između određene grupe učesnika, a koje ne utiču na treća lica, u skladu sa zakonom ili potvrđenim međunarodnim ugovorom.

Ovaj zakon ne utiče na zaključivanje i punovažnost ugovora koji imaju posebne uslove i koji se odnose na formu zaključivanja tih ugovora, u skladu sa zakonom.

Dostupnost licima sa invaliditetom
Član 4

Usluge povjerenja, sredstva elektronske identifikacije, novčanik digitalnog identiteta kao i računarska oprema (hardver) ili računarski program (softver) koji se koriste prilikom vršenja tih usluga, dostupni su licima sa invaliditetom.

Zaštita podataka o ličnosti
Član 5

Podaci o ličnosti koriste se i obrađuju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

Upotreba rodno osjetljivog jezika
Član 6

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

Princip internog tržišta
Član 7

Pružanje usluga povjerenja na području Crne Gore, dozvoljeno je davaocu usluga povjerenja koji je prijavljen u nekoj od država članica Evropske unije.

Proizvodi i usluge povjerenja koji ispunjavaju uslove koje propisuje država članica Evropske unije koriste se slobodno na području Crne Gore.

Pseudonimi u elektronskim transakcijama
Član 8

Upotreba pseudonima koji korisnik izabere u elektronskim transakcijama je dozvoljena, osim ako to zakonom nije zabranjeno.

Značenje izraza
Član 9

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) **elektronska identifikacija** je postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji na jedinstven način predstavljaju fizičko ili pravno lice, odnosno organ vlasti ili fizičko lice koje predstavlja drugo fizičko ili pravno lice, odnosno organ vlasti;

2) **sredstvo elektronske identifikacije** je materijalno i/ili nematerijalno sredstvo koje sadrži lične identifikacione podatke i koje se koristi za autentifikaciju usluga koje se pružaju preko interneta, ili po potrebi usluga koje se ne pružaju preko interneta;

3) **lični podaci** su svi podaci koji su definisani kao lični podaci u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti;

4) **lični identifikacioni podaci** su skup podataka koji se izdaju u skladu sa zakonom i koji omogućavaju utvrđivanje identiteta fizičkog ili pravnog lica, odnosno organa vlasti ili fizičkog lica koje predstavlja drugo fizičko ili pravno lice, odnosno organ vlasti;

5) **autentifikacija** je elektronski postupak kojim se omogućava potvrda elektronske identifikacije fizičkog ili pravnog lica, odnosno organa vlasti ili potvrda porijekla i integriteta podataka u elektronskom obliku;

6) **korisnik** je fizičko ili pravno lice, odnosno organ vlasti ili fizičko lice koje predstavlja drugo fizičko ili pravno lice, odnosno organ vlasti koji koristi usluge povjerenja ili sredstva elektronske identifikacije, u skladu sa ovim zakonom;

7) **pouzdajuća strana** je fizičko ili pravno lice, odnosno organ vlasti koji se pouzdaje u elektronsku identiifikaciju, novčanik digitalnog identiteta ili u drugo sredstvo elektronske identifikacije ili u uslugu povjerenja;

8) **organ vlasti** je državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja;

9) **potpisnik** je fizičko lice koje izrađuje elektronski potpis;

10) **podaci za izradu elektronskog potpisa** su jedinstveni podaci koje potpisnik koristi za izradu elektronskog potpisa;

11) **sertifikat za elektronski potpis** je elektronska potvrda koja povezuje podatke za validaciju elektronskog potpisa sa fizičkim licem i potvrđuje najmanje ime ili pseudonim tog lica;

12) **usluga povjerenja** je elektronska usluga koja se obično pruža uz naknadu, a obuhvata jednu od sljedećih usluga:

- izdavanje sertifikata za elektronske potpise, sertifikata za elektronske pečate, sertifikata za provjeru autentičnosti internet stranice ili sertifikata za pružanje drugih usluga povjerenja,
- validaciju sertifikata za elektronske potpise, sertifikata za elektronske pečate, sertifikata za provjeru autentičnosti internet stranice ili sertifikata za pružanje drugih usluga povjerenja,
- izradu elektronskih potpisa ili elektronskih pečata,

- validaciju elektronskih potpisa ili elektronskih pečata,
- čuvanje elektronskih potpisa, elektronskih pečata, sertifikata za elektronske potpise ili sertifikata za elektronske pečate,
- upravljanje sredstvima za izradu elektronskog potpisa na daljinu ili sredstvima za izradu elektronskog pečata na daljinu,
- izdavanje elektronskih potvrda atributa,
- validaciju elektronskih potvrda atributa,
- izradu elektronskih vremenskih pečata,
- validaciju elektronskih vremenskih pečata,
- pružanje usluga elektronske preporučene dostave,
- validaciju podataka koji se prenose putem usluga elektronske preporučene dostave i povezanih dokaza,
- elektronsko arhiviranje elektronskih podataka i elektronskih dokumenata,
- evidentiranje elektronskih podataka u elektronsku evidenciju;

13) **tijelo za ocjenjivanje usaglašenosti** je pravno lice ili dio pravnog lica koje je u skladu sa zakonom kojim se uređuje akreditacija akreditovano za ocjenjivanje usaglašenosti kvalifikovanih davalaca usluga povjerenja i kvalifikovanih usluga povjerenja koje oni pružaju, kao i za sprovođenje postupka sertifikacije sistema elektronske identifikacije, novčanika digitalnog identiteta ili sredstava elektronske identifikacije;

14) **davalac usluga povjerenja** je fizičko ili pravno lice, odnosno organ vlasti koji pruža jednu ili više usluga povjerenja, bilo kao kvalifikovane ili nekvalifikovane usluge povjerenja;

15) **kvalifikovani davalac usluga povjerenja** je davalac usluga povjerenja koji pruža jednu ili više kvalifikovanih usluga povjerenja i kojem je organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave odobrio status kvalifikovanog davaoca usluga povjerenja;

16) **nekvalifikovani davalac usluga povjerenja** je je davalac usluga povjerenja koji pruža jednu ili više nekvalifikovanih usluga povjerenja;

17) **proizvod je** hardver ili softver ili odgovarajuće komponente hardvera ili softvera, koji su namijenjeni za upotrebu u svrhu pružanja elektronske identifikacije i usluga povjerenja;

18) **hardver je** fizička komponenta koja se koristi u obradi informacija;

19) **softver je** svaki operativni sistem, program, korisnička ili servisna aplikacija;

20) **sredstvo za izradu elektronskog potpisa** je konfigurisani softver ili hardver koji se koristi za izradu elektronskog potpisa;

21) **autor pečata** je pravno lice, odnosno organ vlasti koje izrađuje elektronski pečat;

22) **podaci za izradu elektronskog pečata** su jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata;

23) **sertifikat za elektronski pečat** je elektronska potvrda koja povezuje podatke za validaciju elektronskog pečata sa pravnim licem, odnosno organom vlasti i potvrđuje najmanje ime tog lica, odnosno naziv organa vlasti;

24) **sredstvo za izradu elektronskog pečata** je konfigurisani softver ili hardver koji se koristi za izradu elektronskog pečata;

25) **elektronski dokument je** skup podataka koji su elektronski oblikovani 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, digitalizovani dokument i slično;

26) **podaci za validaciju** su podaci koji se koriste za validaciju elektronskog potpisa ili elektronskog pečata;

27) **validacija** je postupak verifikacije i potvrđivanja da su podaci u elektronskom obliku valjani, u skladu sa ovim zakonom;

28) **atribut** je karakteristika, kvalitet, pravo ili dozvola fizičkog ili pravnog lica, odnosno organa vlasti ili objekta;

29) **autentični izvor** je skladište ili sistem koji je u nadležnosti organa vlasti ili pravnog lica, koji sadrži i pruža atribute o fizičkom ili pravnom licu, odnosno organu vlasti ili objektu i koji se smatra primarnim izvorom tih informacija ili je priznat kao autentičan u skladu sa zakonom;

30) **pouzdana autentifikacija korisnika** je autentifikacija koja se zasniva na upotrebi najmanje dva faktora autentifikacije iz različitih kategorija znanja, odnosno nečega što samo korisnik zna, posjedovanja, odnosno nečega što samo korisnik posjeduje, ili svojstvenosti, odnosno nečega što korisnik jeste, a koji su međusobno nezavisni faktori autentifikacije, tako da narušavanje jednog faktora ne ugrožava pouzdanost drugih i koja je osmišljena na način da zaštiti povjerljivost podataka o autentifikaciji;

31) **uparivanje identiteta** je postupak u kojem se lični identifikacioni podaci ili sredstva elektronske identifikacije spajaju ili povezuju sa postojećim nalogom, koji pripada istom licu;

32) **zapis podataka** podrazumijeva elektronske podatke koji su zabilježeni sa povezanim metapodacima i koji podržavaju obradu podataka;

33) **metapodaci** su podaci koji opisuju karakteristike nekog izvora u digitalnom obliku;

34) **režim van mreže** podrazumijeva interakciju između korisnika i treće strane na fizičkoj lokaciji, koristeći tehnologije u neposrednoj blizini, pri čemu nije potrebno da novčanik digitalnog identiteta ima pristup sistemima na daljinu putem elektronskih komunikacionih mreža, u svrhu interakcije;

35) **interfejs** je zajednička dijeljena granica, posredstvom koje dvije ili više komponenti računarskog sistema vrše razmjenu informacija;

36) **elektronska transakcija** je poslovna aktivnost između dvije ili više strana koja se obavlja elektronskim putem;

37) **interoperabilnost** je sposobnost dva ili više sistema ili njihovih komponenti da razmjenjuju podatke;

38) **ranjivost** je slabost, osjetljivost ili nedostatak nekog resursa, sistema, procesa ili kontrole koji sajber prijetnja može iskoristiti;

39) **ugrađena politika otkrivanja** je skup pravila koja je u elektronsku potvrdu atributa ugradio njen davalac i koja definiše uslove koje pouzdajuća strana novčanika mora ispuniti da bi mogla pristupiti elektronskoj potvrdi atributa.

II. ELEKTRONSKA IDENTIFIKACIJA

Novčanik digitalnog identiteta
Član 10

Novčanik digitalnog identiteta je sredstvo elektronske identifikacije koje korisniku omogućava da bezbjedno skladišti, upravlja i potvrđuje lične identifikacione podatke i elektronske potvrde atributa, u svrhu njihovog pružanja pouzdajućim stranama i drugim korisnicima novčanika digitalnog identiteta, kao i da potpisuje kvalifikovanim elektronskim potpisom.

Davalac novčanika digitalnog identiteta je pravno lice ili organ vlasti koji pruža uslugu novčanika digitalnog identiteta.

Davalac novčanika digitalnog identiteta obezbjeđuje da izvorni kod aplikativnih softverskih komponenti koje su instalirane na korisničkom uređaju mora biti licenciran u otvorenom kodu.

Izuzetno od stava 3 ovog člana, izvorni kod ne mora da bude licenciran u otvorenom kodu, za komponente koje nijesu instalirane na korisničkom uređaju, ako za to postoje opravdani razlozi.

Integritet i funkcionalnost novčanika digitalnog identiteta
Član 11

Integritet i funkcionalnost novčanika digitalnog identiteta omogućavaju korisniku da na njemu prilagođen, transparentan i sljedljiv način:

1) bezbjedno zahtijeva, pribavlja, bira, kombinuje, čuva, briše, dijeli i predstavlja, pod isključivom kontrolom korisnika, lične identifikacione podatke i da se, prema potrebi, u kombinaciji sa elektronskim potvrdama atributa, autentifikuje pouzdajućim stranama na internetu a, gdje je primjenjivo, u režimu van mreže radi pristupa elektronskim uslugama, uz obezbjeđivanje mogućnosti selektivnog otkrivanja podataka;

2) generiše pseudonime i čuva ih lokalno u kriptovanom obliku u novčaniku digitalnog identiteta;

3) bezbjedno izvrši autentifikaciju novčanika digitalnog identiteta drugog lica, kao i da prima i dijeli lične identifikacione podatke i elektronske potvrde atributa, na bezbjedan način između dva novčanika digitalnog identiteta;

4) pristupi evidenciji svih transakcija izvršenih preko novčanika digitalnog identiteta putem zajedničke kontrolne table koja omogućava korisniku da:

- pregleda ažuriranu listu pouzdajućih strana sa kojima je korisnik uspostavio vezu, i gdje je primjenjivo, sve razmijenjene podatke,
- na jednostavan način zahtijeva od pouzdajuće strane brisanje ličnih podataka, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti,
- na jednostavan način prijavi pouzdajuću stranu nadležnom organu za zaštitu podataka o ličnosti, u slučaja kad se dobije nezakonit ili sumnjiv zahtjev za dobijanje ličnih podataka;

5) potpisuje kvalifikovanim elektronskom potpisom, odnosno pečatira kvalifikovanim elektronskim pečatom;

6) preuzme, u mjeri u kojoj je to tehnički izvodljivo, podatke korisnika, elektronske potvrde atributa i konfiguracije;

7) koristi pravo na prenosivost podataka.

Bliža pravila o utvrđivanju integriteta i funkcionalnosti novčanika digitalnog identiteta, kao i druga pitanja od značaja za funkcionisanje novčanika digitalnog identiteta propisuje organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave (u daljem tekstu: Ministarstvo).

Uslovi za novčanik digitalnog identiteta
Član 12

Novčanik digitalnog identiteta naročito treba da:

1) podržava zajedničke protokole i interfejse za:

- izdavanje ličnih identifikacionih podataka, kvalifikovanih i nekvalifikovanih elektronskih potvrda atributa ili kvalifikovanih i nekvalifikovanih sertifikata za novčanik digitalnog identiteta;
- pouzdajuće strane kako bi im se omogućilo da zahtijevaju i potvrde lične identifikacione podatke i elektronske potvrde atributa,
- dijeljenje i predstavljanje pouzdajućim stranama ličnih identifikacionih podataka, elektronske potvrde atributa ili selektivno otkrivenih povezanih podataka na internetu, i po potrebi, u režimu van mreže,
- omogućavanje interakcije korisnika sa novčanikom digitalnog identiteta,
- sigurno uključivanje korisnika upotrebom postojećeg sredstva elektronske identifikacije visokog stepena sigurnosti ili sredstva elektronske identifikacije srednjeg stepena sigurnosti u kombinaciji sa dodatnim postupcima na daljinu koji zajedno ispunjavaju zahtjeve za visok stepen sigurnosti,
- komunikaciju između novčanika digitalnih identiteta dva lica radi bezbjednog primanja, potvrđivanja ispravnosti i dijeljenja ličnih identifikacionih podataka i elektronskih potvrda atributa,

- autentifikaciju i identifikaciju pouzdajućih strana primjenom mehanizma autentifikacije u skladu sa članom 23 ovog zakona,
- pouzdajuće strane kako bi se omogućila provjera autentičnosti i validnosti novčanika digitalnog identiteta,
- slanje zahtjeva pouzdajućoj strani za brisanje ličnih podataka, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti,
- prijavu pouzdajuće strane nadležnom organu za zaštitu podataka o ličnosti ako je primljen nezakonit ili sumnjiv zahtjev za dobijanje ličnih podataka,
- izradu kvalifikovanih elektronskih potpisa, odnosno kvalifikovanih elektronskih pečata pomoću kvalifikovanih sredstava za izradu elektronskih potpisa, odnosno kvalifikovanih sredstava za izradu elektronskih pečata;

2) ne pruža informacije davaocima usluga povjerenja za elektronske potvrde atributa o korišćenju tih elektronskih potvrda;

3) obezbjeđuje da se pouzdajuća strana može autentifikovati i identifikovati primjenom zajedničkog mehanizma autentifikacije u skladu sa članom 23 ovog zakona;

4) ispunjava uslove iz člana 35 ovog zakona, u pogledu visokog stepena sigurnosti, posebno u pogledu zahtjeva za dokazivanje i potvrdu identiteta, kao i za upravljanje sredstvima elektronske identifikacije i autentifikacije;

5) obezbjeđuje da se u slučaju elektronske potvrde atributa sa ugrađenim politikama otkrivanja primjenjuje odgovarajući mehanizam za obavještavanje korisnika da pouzdajuća strana ili korisnik novčanika digitalnog identiteta koji zahtijeva elektronsku potvrdu atributa ima dozvolu za pristup toj potvrdi;

6) obezbjeđuje da lični identifikacioni podaci kojima raspolaže sistem elektronske identifikacije, u skladu sa kojim se obezbjeđuje novčanik digitalnog identiteta na nedvosmislen način predstavljaju fizičko ili pravno lice, odnosno organ vlasti ili fizičko lice koje zastupa drugo fizičko ili pravno lice, odnosno organ vlasti i da su lični identifikacioni podaci povezani sa tim novčanikom digitalnog identiteta;

7) fizičkim licima pruži mogućnost korišćenja besplatnog kvalifikovanog elektronskog potpisa.

Bliža pravila za zajedničke protokole i interfejse, kao i način izdavanja elektronskih potvrda atributa i ličnih identifikacionih podataka koji se izdaju za potrebe novčanika digitalnog identiteta iz stava 1 tač. 5 i 6 ovog člana, kao i druga pitanja od značaja za izdavanje elektronskih potvrda atributa i ličnih identifikacionih podataka, propisuje Ministarstvo.

Interoperabilnost novčanika digitalnog identiteta sa sredstvima elektronske identifikacije

Član 13

Novčanik digitalnog identiteta može da ima dodatne funkcionalnosti, uključujući interoperabilnost sa sredstvima elektronske identifikacije koja su prijavljena u registar iz člana 37 ovog zakona, ako su te funkcionalnosti u skladu sa ovim zakonom.

Validacija novčanika digitalnog identiteta

Član 14

Validacija novčanika digitalnog identiteta vrši se na besplatan način, kako bi se:

1) obezbijedilo da se autentičnost i validnost novčanika digitalnog identiteta mogu provjeriti;

2) korisnicima omogućilo da provjere autentičnost i validnost identiteta pouzdajućih strana koje su upisane u registar iz člana 21 ovog zakona.

Bliži način vršenja validacije iz stava 1 tačka 1 ovog člana propisuje Ministarstvo.

Opoziv validnosti novčanika digitalnog identiteta
Član 15

Validnost novčanika digitalnog identiteta može se opozvati:

1) na izričit zahtjev korisnika;
2) ako je bezbjednost novčanika digitalnog identiteta ugrožena;
3) nakon smrti korisnika ili prestanka rada pravnog lica, odnosno organa vlasti koji je njegov korisnik.

Obaveze davaoca novčanika digitalnog identiteta
Član 16

Davalac novčanika digitalnog identiteta dužan je da obezbijedi korisnicima da mogu lako da zatraže tehničku podršku i prijave tehničke probleme ili incidente koji imaju negativan uticaj na upotrebu novčanika digitalnog identiteta.

Novčanik digitalnog identiteta izdaje se korisnicima u okviru sistema elektronske identifikacije sa visokim stepenom sigurnosti i ima integrisanu sigurnost.

Novčanik digitalnog identiteta izdaje se, upotrebljava i opoziva besplatno za fizička lica.

Davalac novčanika digitalnog identiteta omogućava korisniku da ima punu kontrolu nad upotrebom novčanika digitalnog identiteta, kao i nad podacima koji se nalaze u tom novčaniku.

Davalac novčanika digitalnog identiteta ne prikuplja informacije o upotrebi novčanika digitalnog identiteta koje nijesu neophodne za pružanje usluga novčanika digitalnog identiteta, ne kombinuje lične identifikacione podatke ili bilo koje druge lične podatke, koji se čuvaju ili odnose na korišćenje novčanika digitalnog identiteta, sa ličnim podacima iz bilo koje druge usluge koju pruža taj davalac ili usluga trećih strana koje nijesu neophodne za pružanje usluga novčanika digitalnog identiteta, osim ako korisnik to izričito zatraži.

Lični podaci koji su povezani sa digitalnim novčanikom čuvaju se logički odvojeno od svih drugih podataka koje posjeduje davalac novčanika digitalnog identiteta.

Na davaoca novčanika digitalnog identiteta primjenjuje se odredbe člana 53 stav 1 tačka 2 i tač. 4 do 9 i člana 54 stav 2 ovog zakona.

Upotreba novčanika digitalnog identiteta
Član 17

Upotreba novčanika digitalnog identiteta je dobrovoljna.

Fizičkim i pravnim licima koja ne koriste novčanik digitalnog identiteta ni na koji način se ne smije ograničiti ili otežati korišćenje elektronskih usluga, pristup tržištu rada i slobodi poslovanja.

Fizičkim i pravnim licima iz stava 2 ovog člana pristup elektronskim uslugama mora biti omogućen putem drugih postojećih sredstava identifikacije i autentifikacije.

Tehnički okvir za novčanik digitalnog identiteta
Član 18

Tehnički okvir za novčanik digitalnog identiteta treba da:

1) davaocima usluga povjerenja koji izdaju elektronske potvrde atributa ili bilo kojoj drugoj strani nakon izdavanja elektronske potvrde atributa ne dozvoli da pribavljaju podatke koji omogućavaju praćenje, povezivanje ili upoređivanje elektronskih transakcija ili ponašanje korisnika ili na drugi način dobiju podatke o transakcijama ili ponašanju korisnika, osim ako to korisnik izričito ne zatraži;
2) omogući tehniku za čuvanje privatnosti, kojom se obezbjeđuje nepovezanost sa korisnikom, kad za elektronsku potvrdu atributa nije potrebna identifikacija korisnika.

Izuzetak u pogledu uslova
Član 19

Na novčanik digitalnog identiteta i sistem elektronske identifikacije u okviru kojeg se taj novčanik izdaje ne primjenjuju se uslovi iz čl. 39, 42, 43, 45 i 46 ovog zakona.

Postupak registracije pouzdajućih strana
Član 20

Pouzdajuća strana koja namjerava da za potrebe pružanja elektronskih usluga koristi novčanik digitalnog identiteta, dužna je da se registruje.

Zahtjev za registraciju podnosi se Ministarstvu na propisanom obrascu.

Uz zahtjev za registraciju pouzdajuća strana dostavlja Ministarstvu najmanje sljedeće podatke:

1) informacije neophodne novčaniku digitalnog identiteta, za autentifikaciju pouzdajuće strane, i to:
   - naziv države u kojoj je ta pouzdajuća strana registrovana,
   - naziv pouzdajuće strane,
   - gdje je to primjenjivo registarski broj pouzdajuće strane, kao što je navedeno u službenoj evidenciji, zajedno sa identifikacionim podacima te službene evidencije;
2) kontakt podatke o pouzdajućoj strani (adresa internet stranice ili jedinstvena službena adresa za elektronsku komunikaciju ili kontakt telefon);
3) informacije o namjeni korišćenja novčanika digitalnog identiteta, uz navođenje podataka koje će od korisnika zahtijevati pouzdajuća strana.

Pouzdajuća strana ne smije zahtijevati od korisnika da dostavi druge podatke osim podataka iz stava 2 tačka 3 ovog člana.

Obrazac iz stava 2 ovog člana, bliži način i postupak registracije iz stava 1 ovog člana propisuje Ministarstvo.

Registar pouzdajućih strana
Član 21

Pouzdajuća strana koja je dostavila podatke iz člana 20 stav 2 ovog zakona upisuje se u registar pouzdajućih strana.

Registar iz stava 1 ovog člana sadrži podatke iz člana 20 stav 2 ovog zakona.

Registar iz stava 1 ovog člana vodi Ministarstvo.

Registar iz stava 1 ovog člana vodi se u elektronskom obliku pogodnom za automatsku obradu i objavljuje se na internet stranici Ministarstva.

Registar iz stava 1 ovog člana potpisuje se naprednim elektronskim potpisom, odnosno pečatira naprednim elektronskim pečatom.

Bliži sadržaj registra iz stava 1 ovog člana propisuje Ministarstvo.

Obavještenje o promjeni podataka
Član 22

Pouzdajuća strana koja je upisana u registar iz člana 21 stav 1 ovog zakona dužna je da obavještava Ministarstvo o promjeni podataka iz člana 20 stav 2 ovog zakona, bez odlaganja.

Mehanizam autentifikacije pouzdajućih strana
Član 23

Pouzdajuća strana koja ima namjeru da koristi novčanik digitalnog identiteta identifikuje se uz korišćenje zajedničkog mehanizma autentifikacije, koji obezbjeđuje autentifikaciju i identifikaciju pouzdajućih strana.

Bliži način vršenja autentifikacije iz stava 1 ovog člana propisuje Ministarstvo.

Obaveze pouzdajućih strana
Član 24

Pouzdajuća strana odgovorna je za sprovođenje postupka autentifikacije i validacije ličnih identifikacionih podataka i elektronske potvrde atributa koji su zatraženi iz novčanika digitalnog identiteta.

Pouzdajuća strana dužna je da prihvati upotrebu pseudonima, u slučajevima kad se u skladu sa zakonom ne zahtijeva identifikacija.

Posrednici koji postupaju u ime pouzdajućih strana smatraju se pouzdajućim stranama i ne smiju da čuvaju podatke o sadržaju transakcije.

Sertifikacija novčanika digitalnog identiteta
Član 25

Sertifikacija novčanika digitalnog identiteta podrazumijeva provjeru ispunjenosti uslova iz čl. 11, 12, 14 i 16 st. 4 do 7 ovog zakona i vrši je tijelo za ocjenjivanje usaglašenosti.

Prilikom sertifikacije novčanika digitalnog identiteta provjerava se i usaglašenost novčanika digitalnog identiteta sa odgovarajućim standardima informacione bezbjednosti i zakonom kojim se uređuje informaciona bezbjednost, kao i procjena uticaja na obradu podataka o ličnosti, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

Nakon što tijelo za ocjenjivanje usaglašenosi utvrdi da su ispunjeni uslovi iz st. 1 i 2 ovog člana, davaocu novčanika digitalnog identiteta izdaje se sertifikat.

Sertifikat iz stava 3 ovog člana izdaje se na vrijeme od pet godina, pod uslovom da se svake dvije godine sprovodi procjena ranjivosti.

Ako se procjena ranjivosti iz stava 4 ovog člana ne sprovede, odnosno ako se ranjivost identifikuje i ne otkloni, sertifikat se poništava.

Bliži način sertifikacije novčanika digitalnog identiteta, kao i druga pitanja od značaja za postupak te sertifikacije uređuje Vlada.

Registar novčanika digitalnog identiteta
Član 26

Nakon što je novčanik digitalnog identiteta sertifikovan u skladu sa članom 25 ovog zakona, davalac novčanika digitalnog identiteta podnosi zahtjev za upis u Registar novčanika digitalnog identiteta, na propisanom obrascu.

Uz zahtjev iz stava 1 ovog člana, davalac novčanika digitalnog identiteta dužan je da dostavi informacije o:

1) opisu sistema elektronske identifikacije u okviru kojeg je uspostavljen novčanik digitalnog identiteta;
2) pravnom licu, odnosno organu vlasti koje je uspostavilo sistem elektronske identifikacije i koji je odgovorno za taj sistem;
3) pravilima za suspenziju ili opoziv sistema elektronske identifikacije ili autentifikacije ili kompromitovanih djelova koji se na njih odnose.

Uz zahtjev iz stava 1 ovog člana, dostavlja se i dokumentacija kojom se dokazuje da je novčanik digitalnog identiteta sertifikovan u skladu sa članom 25 ovog zakona, i to:

1) sertifikat kojim se potvrđuje sertifikacija novčanika digitalnog identiteta i sistema elektronske identifikacije u okviru kojeg je izdat taj novčanik;
2) izvještaj o sprovedenom postupku sertifikacije.

Registar iz stava 1 ovog člana vodi Ministarstvo.

Registar iz stav 1 ovog člana vodi se u elektronskom obliku i objavljuje na internet stranici Ministarstva.

Obrazac i sadržaj zahtjeva iz stava 1 ovog člana, dokumentaciju koja se dostavlja, kao i sadržaj registra iz stava 1 ovog člana propisuje Ministarstvo.

Obavještenje o promjenama
Član 27

Davalac novčanika digitalnog identiteta dužan je da u slučaju namjere prestanka izdavanja novčanika digitalnog identiteta, kao i promjene informacija iz člana 26 stav 2 ovog zakona, obavijesti Ministarstvo, bez odlaganja.

Nakon dostavljenog obavještena iz stava 1 ovog člana, Ministarstvo vrši promjene u registru iz člana 26 stav 1 ovog zakona, u roku od deset dana od dana dostavljene promjene.

Narušavanje bezbjednosti novčanika digitalnog identiteta
Član 28

U slučaju povrede ili djelimične kompromitacija novčanika digitalnog identiteta, sistema validacije iz člana 14 ovog zakona, odnosno sistema elektronske identifikacije u okviru kojeg je taj novčanik obezbijeđen, na način koji utiče na njegovu pouzdanost ili pouzdanost drugih novčanika digitalnog identiteta, davalac novčanika digitalnog identiteta o tome obavještava Ministarstvo, bez odlaganja.

Na osnovu obavještenja iz stava 1 ovog člana Ministarstvo suspenduje novčanik digitalnog identiteta.

O suspenziji iz stava 2 ovog člana davalac novčanika digitalnog identiteta obavještava korisnike, a Ministarstvo obavještava pouzdajuće strane upisane u registar iz člana 21 ovog zakona.

Ako se povreda, odnosno kompromitacija iz stava 1 ovog člana ne otklone u roku od tri mjeseca od dana suspenzije, davalac novčanika digitalnog identiteta o tome obavještava Ministarstvo, bez odlaganja.

Na osnovu obavještenja iz stava 4 ovog člana Ministarstvo opoziva novčanik digitalnog identiteta.

O opozivu iz stava 5 ovog člana, davalac novčanika digitalnog identiteta obavještava korisnike, a Ministarstvo obaviještava pouzdajuće strane upisane u registar iz člana 21 ovog zakona.

Ako se povreda ili kompromitacija iz stava 1 ovog člana otkloni, davalac novčanika digitalnog identiteta o tome obavještava Ministarstvo, bez odlaganja, i dostavlja izvještaj o mjerama koje su preduzete za otklanjanje povrede, odnosno kompromitacije.

Na osnovu obavještenja iz st. 1 i 3 ovog člana i dostavljenih izvještaja iz stava 7 ovog člana, Ministarstvo evidentira promjene u registru iz člana 26 ovog zakona.

O promjenama iz stava 7 ovog člana, Ministarstvo će obavijestiti pouzdajuće strane, a davalac novčanika digitalnog identiteta korisnike.

Bliže kriterijume na osnovu kojih se vrši procjena povrede, odnosno kompromitacije iz stava 1 ovog člana, kao i bliži način suspenzije, odnosno opoziva novčanika digitalnog identiteta propisuje Ministarstvo.

Evropski novčanik digitalnog identiteta
Član 29

U cilju obezbjeđivanja da sva fizička i pravna lica, odnosno organi vlasti imaju siguran, pouzdan i nesmetan prekogranični pristup elektronskim uslugama, uz punu kontrolu nad njihovim podacima, Crna Gora obezbjeđuje najmanje jedan evropski novčanik digitalnog identiteta.

Evropski novčanik digitalnog identiteta obezbjeđuje se na jedan ili više sljedećih načina, i to od:

1) Crne Gore;
2) druge države članice Evropske unije;

3) druge države koja nije članica Evropske unije, pod uslovom da je priznat od strane Crne Gore.

EU oznaka pouzdanosti evropskog novčanika digitalnog identiteta je provjerljiva, jednostavna i prepoznatljiva oznaka kojom se na jasan način označava da je EU novčanik digitalnog identiteta usklađen sa Regulativa (EU) br. 910/2014 Evropskog parlamenta i Savjeta od 23. jula 2014. godine o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC i Regulativom (EU) 2024/1183 Evropskog parlamenta i Savjeta od 11. aprila 2024. godine o izmjeni Regulative (EU) br. 910/2024 u pogledu uspostavljanja evropskog okvira za digitalni identitet (u daljem tekstu: Regulativa eIDAS).

Evropski novčanik digitalnog identiteta obezbijeđen od strane privatnih lica u skladu sa stavom 2 tač. 2 i 3 ovog člana pruža se na način koji je funkcionalno odvojen od drugih usluga koje se pružaju.

Prekogranično priznavanje evropskih novčanika digitalnog identiteta

Član 30

Kad Crna Gora zahtijeva elektronsku identifikaciju i autentifikaciju za pristup elektronskim uslugama koje obezbjeđuje organ vlasti prihvatiće evropske digitalne novčanike koji su upisani na Listu sertifikovanih evropskih novčanika digitalnog identiteta koju objavljuje Evropska komisija.

Kad Crna Gora zahtijeva da privatne pouzdajuće strane koje pružaju elektronske usluge, osim mikro i malih preduzeća u skladu sa zakonom kojim se uređuje računovodstvo koriste snažnu autentifikaciju korisnika za elektronsku identifikaciju ili kad je snažna autentifikacija korisnika za elektronsku identifikaciju zahtijevana u skladu sa ugovornim obavezama u oblasti transporta, energetike, bankarstva, finansijskih usluga, socijalne sigurnosti, vode za piće, poštanskih usluga, digitalne infrastrukture, obrazovanja ili telekomunikacija, te pouzdajuće strane će samo na dobrovoljni zahtjev korisnika prihvatiti evropske novčanike koji su na Listi digitalnih novčanika Evropske unije.

Pružaoci veoma velikih internet platformi koji zahtijevaju autentifikaciju korisnika za pristup elektronskim uslugama moraju da prihvate i olakšaju upotrebu evropskih digitalnih novčanika, za autentifikaciju korisnika, samo na dobrovoljan zahtjev korisnika i uz upotrebu minimalnih podataka koji su potrebni za specifičnu elektronsku uslugu, za koju se zahtijeva autentifikacija.

Evropski novčanici digitalnog identiteta koji su upisani na Listu sertifikovanih evropskih novčanika digitalnog identiteta koju objavljuje Evropska komisija priznaju se za identifikaciju za pristup elektronskim uslugama koje se pružaju u Crnoj Gori, na osnovu međunarodnog sporazuma o međusobnom priznavanju evropskih novčanika digitalnog identiteta koji se zasniva na principu reciprociteta, čiji sastavni dio su implementacioni akti za njegovo sprovođenje.

Novčanici digitalnog identiteta koji su upisani na Listu sertifikovanih novčanika digitalnog identiteta u drugoj državi koja nije članica Evropske unije priznaju se za autentifikaciju za pristup elektronskim uslugama koje se pružaju u Crnoj Gori, na osnovu međunarodnog sporazuma o međusobnom priznavanju novčanika digitalnog identiteta na principu reciprociteta, čiji sastavni dio su implementacioni akti za njegovo sprovođenje.

Dostavljanje informacija Evropskoj komisiji

Član 31

Ministarstvo dostavlja Evropskoj komisiji, bez odlaganja, informacije o:

1) organu odgovornom za uspostavljanje i vođenje registra iz člana 21 ovog zakona, kao i lokaciji na kojoj je taj registar dostupan;

2) davaocu evropskog novčanika digitalnog identiteta;

3) organu odgovornom za obezbjeđivanje povezanosti identifikacionih podataka lica sa evropskim digitalnim novčanikom, u skladu sa članom 12 stav 1 tačka 6 ovog zakona;

4) načinu koji omogućava validaciju podataka za identifikaciju lica iz člana 12 stav 1 tačka 6 ovog zakona;

5) mehanizmu autentifikacije kojim se potvrđuje autentičnost i validnost evropskih novčanika digitalnog identiteta u skladu sa članom 14 ovog zakona.

Dostavljanje informacija Evropskoj komisiji o novčanicima digitalnog identiteta
Član 32

Ministarstvo dostavlja Evropskoj komisiji, bez odlaganja, informacije o novčanicima digitalnog identiteta koji su obezbijeđeni u skladu sa ovim zakonom i sertifikovani od strane tijela za ocjenjivanje usaglašenosti u skladu sa članom 25 ovog zakona.

Ministarstvo dostavlja Evropskoj komisiji bez odlaganja, informacije o poništavanju sertifikata novčanika digitalnog identiteta, uz navođenje razloga za poništavanje.

Informacije iz st. 1 i 2 ovog člana, sadrže najmanje podatke o:

1) sertifikatu i izvještaju o procjeni sertifikata sertifikovanog evropskog novčanika digitalnog identiteta;

2) opisu sistema elektronske identifikacije, u okviru kojeg je izdat novčanik digitalnog identiteta;

3) sistemu nadzora koji se primjenjuje i režimu odgovornosti, u odnosu na pravno lice, odnosno organ vlasti koji obezbjeđuje novčanik digitalnog identiteta;

4) pravnom licu, odnosno organu vlasti koji je uspostavio sistem elektronske identifikacije;

5) pravilima za suspenziju ili ukidanje sistema elektronske identifikacije ili autentifikacije ili kompromitovanih djelova koji se na njih odnose.

Ministarstvo može da podnese zahtjev Evropskoj komisiji za brisanje prijavljenog novčanika digitalnog identiteta i sistema elektronske identifikacije sa Liste sertifikovanih evropskih novčanika digitalnog identiteta koju objavljuje Evropska komisija, u skladu sa Regulativom eIDAS.

U slučaju promjene informacija iz stava 1 i 2 ovog člana, Ministarstvo će Evropskoj komisiji dostaviti obavještenje o promjeni.

Obavještavanje Evropske komisije o kršenju bezbjednosti evropskih digitalnih novčanika
Član 33

Kad se desi povreda ili djelimična kompromitacija novčanika digitalnog identiteta, sistema validacije iz člana 14 ovog zakona, odnosno sistema elektronske identifikacije u okviru kojeg je taj novčanik obezbijeđen, na način koji utiče na njegovu pouzdanost, ili pouzdanost drugih evropskih novčanika digitalnog identiteta, Crna Gora, bez odlaganja, suspenduje evropski novčanik digitalnog identiteta.

Crna Gora o suspenziji iz stava 1 ovog člana, bez odlaganja obavještava pouzdajuće strane i Evropsku komisiju.

Davalac evropskog novčanika digitalnog identiteta o suspenziji evropskog novčanika digitalnog identiteta obavještava korisnike.

Ako se povreda ili djelimična kompromitacija iz st. 1 i 2 ovog člana ne otklone u roku od tri mjeseca od dana suspenzije, Crna Gora će opozvati validnost tog novčanika.

Crna Gora o opozvanom evropskom novčaniku digitalnog identiteta, obavještava pouzdajuće strane, Evropsku komisiju i jedinstvene kontakt tačke koje su uspostavljene u skladu sa pravilima Evropske unije, bez odlaganja, a davalac evropskog novčanika digitalnog identiteta obavještava korisnike.

Sistem elektronske identifikacije
Član 34

Sistem elektronske identifikacije je sistem u okviru kojeg se sredstva elektronske identifikacije izdaju fizičkim ili pravnim licima, odnosno organima vlasti ili fizičkim licima koja zastupaju drugo fizičko ili pravno lice, odnosno organ vasti.

Fizičko i pravno lice, odnosno organ vlasti upravlja sistemom elektronske identifikacije u okviru kojeg se izdaje sredstvo elektronske identifikacije (u daljem tekstu: davalac elektronske identifikacije).

Stepen sigurnosti sistema elektronske identifikacije
Član 35

Sistem elektronske identifikacije mora imati određeni stepen sigurnosti koji se odnosi na sredstvo 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, a odlikuje se referencom na tehničke specifikacije, standarde i procedure, koji se odnose na njih, uključujući tehničke kontrole, čija je svrha smanjenje rizika od zloupotrebe ili izmjene identiteta;

2) srednji stepen sigurnosti koji garantuje značajan stepen pouzdanosti sredstva elektronske identifikacije u odnosu na traženi ili utvrđeni identitet lica, a odlikuje se referencom na tehničke specifikacije, standarde i postupke koji se odnose na njih, uključujući tehničke kontrole čija je svrha da se značajno smanji rizik od zloupotrebe ili izmjene identiteta;

3) visok stepen sigurnosti koji garantuje visok stepen pouzdanosti sredstva elektronske identifikacije u odnosu na traženi ili utvrđeni identitet lica, a odlikuje se referencom na tehničke specifikacije, standarde i postupke koji se odnose na njih, uključujući tehničke kontrole čija je svrha sprječavanje zloupotrebe ili izmjene identiteta.

Minimalne tehničke specifikacije, standarde i procedure iz stava 2 ovog člana propisuje Ministarstvo.

Uslovi za sistem za elektronsku identifikaciju
Član 36

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 35 stav 2 ovog zakona;

2) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjedi 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 35 stav 3 ovog zakona za odgovarajući stepen sigurnosti;

3) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjedi 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 35 stav 3 ovog zakona za odgovarajući stepen sigurnosti;

4) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbijedi autentifikaciju pouzdajućim stranama, na način da mogu da potvrde lične identifikacione podatke primljene u elektronskom obliku.

Registar sistema elektronske identifikacije
Član 37

Sistem elektronske identifikacije koji ispunjava uslove iz člana 36 ovog zakona upisuje se u registar sistema elektronske identifikacije, na osnovu zahtjeva koji se podnosi na propisanom obrascu.

Uz zahtjev iz stava 1 ovog člana prilaže se i potrebna dokumentacija.

Registar iz stava 1 ovog člana sadrži informacije o:

1) opisu sistema elektronske identifikacije;

2) stepenu sigurnosti sistema elektronske identifikacije i sredstava elektronske identifikacije koji se izdaju u okviru tog sistema;

3) podacima 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) suspenziji ili opozivu sistema elektronske identifikacije;

5) datumu upisa sistema elektronske identifikacije, kao i izmjene i brisanja iz tog registra.

Registar iz stava 1 ovog člana vodi Ministarstvo.

Registar iz stava 1 ovog člana se vodi u elektronskom obliku pogodnom za automatsku obradu i objavljuje na internet stranici Ministarstva.

Registar iz stava 1 ovog člana potpisuje se naprednim elektronskim potpisom, odnosno pečatira naprednim elektronskim pečatom.

Obrazac i sadržaj zahtjeva iz stava 1 ovog člana, dokumentaciju koja se dostavlja uz zahtjev, kao i bliži sadržaj registra iz stava 1 ovog člana propisuje Ministarstvo.

Korišćenje sistema elektronske identifikacije u komunikaciji sa organom vlasti
Član 38

Za utvrđivanje identiteta korisnika u elektronskoj komunikaciji sa organima vlasti koriste se sistemi elektronske identifikacije sa visokim stepenom sigurnosti iz člana 35 stav 2 tačka 3 ovog zakona u pogledu sredstva elektronske identifikacije, osim ako posebnim zakonom nije drukčije uređeno.

Narušavanje bezbjednosti sistema elektronske identifikacije
Član 39

Kad se za sistem elektronske identifikacije koji je upisan u registar iz člana 37 ovog zakona, odnosno autentifikaciju iz člana 36 stav 1 tačka 4 ovog zakona utvrdi da je došlo do povrede ili djelimične kompromitacije na način koji utiče na pouzdanost autentifikacije tog sistema, davalac elektronske identifikacije, bez odlaganja, suspenduje autentifikaciju i o tome obavještava Ministarstvo.

Na osnovu obavještenja iz stava 1 ovog člana Ministarstvo evidentira suspenziju autentifikacije u registru iz člana 37 ovog zakona.

Ako se povreda, odnosno kompromitacija iz stava 1 ovog člana otkloni, davalac elektronske identifikacije ponovo uspostavlja autentifikaciju i o tome obavještava Ministarstvo, bez odlaganja, i dostavlja izvještaj o mjerama koje su preduzete za otklanjanje povreda, odnosno kompromitacije iz stava 1 ovog člana.

Na osnovu obavještenja iz stava 3 ovog člana Ministarstvo evidentira promjenu u registru iz člana 37 ovog zakona.

Ako se povreda, odnosno kompromitacija iz stava 1 ovog člana ne otklone u roku od tri mjeseca od dana suspenzije, davalac elektronske identifikacije o tome obavještava Ministarstvo, bez odlaganja.

Na osnovu obavještenja iz stava 5 ovog člana, Ministarstvo evidentira opoziv sistema elektronske identifikacije u registru iz člana 37 ovog zakona.

Odgovornost
Član 40

Davalac elektronske identifikacije koji izdaje sredstva elektronske identifikacije odgovoran je za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu, odnosno organu vlasti zbog neispunjavanja uslova propisanih u članu 36 ovog zakona.

Prekogranično uparivanje identiteta
Član 41

Kad postupa kao pouzdajuća strane za prekogranične usluge koje pruža Evropska unija, Crna Gora obezbjeđuje nedvosmisleno uparivanje identiteta za fizička lica koja upotrebljavaju sredstva elektronske identifikacije ili evropski novčanik digitalnog identiteta, koja su prijavljena na Listi sistema elektronske identifikacije koju objavljuje Evropska komisija, odnosno Listi sertifikovanih evropskih novčanika digitalnog identiteta.

Za potrebe korišćenja prekograničnih usluga, Crna Gora obezbjeđuje tehničke i organizacione mjere kako bi se obezbijedio visok nivo zaštite ličnih podataka, koji se koriste za uparivanje identiteta, kako bi se spriječilo profilisanje korisnika.

Interoperabilnost
Član 42

Sistemi elektronske identifikacije koji se prijavljuju na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija, u skladu sa članom 46 ovog zakona, moraju biti interoperabilni.

Za interoperabilnost iz stava 1 ovog člana uspostavlja se okvir interoperabilnosti.

Okvir interoperabilnosti treba da:

1) bude tehnološki neutralan i ne pravi diskriminaciju između bilo kakvih specifičnih nacionalnih tehničkih rješenja za elektronsku identifikaciju;
2) ispuni evropske i međunarodne standarde;
3) olakša implementaciju integrisane privatnosti i sigurnosti.

Okvir interoperabilnosti sastoji se od:

- upućivanja na minimalne tehničke zahtjeve koji se odnose na stepene sigurnosti iz člana 35 stav 3 ovog zakona;
- raspoređivanja stepena sigurnosti iz člana 35 stav 2 ovog zakona drugih država;
- upućivanja na minimalne tehničke zahtjeve za interoperabilnost;
- upućivanja na najmanji set ličnih identifikacionih podataka koji na nedvosmislen način predstavljaju fizičko ili pravno lice ili fizičko lice koje zastupa drugo fizičko ili pravno lice, odnosno organ vlasti, kojim raspolažu sistemi elektronske identfiikacije;
- pravila i procedura;
- načina rješavanja sporova i
- zajedničkih operativnih standarda bezbjednosti.

Ocjenjivanje sistema elektronske identifikacije koji se prijavljuje na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija, u pogledu interoperabilnosti, vrši se u skladu sa Regulativom eIDAS.

Ocjenjivanje sistema elektronske identifikacije u skladu sa stavom 4 ovog člana ne vrši se za sisteme elektronske identifikacije ili djelove tog sistema, koji su sertifikovani u skladu sa članom 43 ovog zakona.

Sertifikacija sistema elektronske identifikacije
Član 43

Sertifikaciju sistema elektronske identifikacije koji se prijavljuje u registar sistema elektronske identifikacije, kao i usklađenost sa stepenom sigurnosti iz člana 35 stav 2 ovog zakona, u pogledu bezbjednosti, vrši tijelo za ocjenjivanje usaglašenosti.

Nakon što tijelo za ocjenjivanje usaglašenosi utvrdi da sistem elektronske identifikacije ispunjava uslove u pogledu usklađenosti sa stepenom sigurnosti iz člana 35 stav 2 ovog zakona, davaocu elektronske identifikacije izdaje sertifikat.

Sertifikat iz stava 2 ovog člana izdaje se na vrijeme od pet godina, pod uslovom da se svake dvije godine sprovodi procjena ranjivosti.

Ako se procjena ranjivosti iz stava 3 ovog člana ne sprovede, sertifikat se poništava.

Bliži način sertifikacije sistema elektronske identifikacije, kao i druga pitanja od značaja za postupak te sertifikacije uređuje Vlada.

Uzajamno priznavanje sredstava elektronske identifikacije
Član 44

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

1) je sredstvo elektronske identifikacije izdato u okviru sistema elektronske identifikacije koji je stavljen na Listu sistema elektronske identifikacije koju objavljuje 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 srednji ili visok stepen sigurnosti u odnosu na pristupanje toj usluzi na internetu.

Kad organ vlasti za uslugu koju pruža na internetu zahtijeva elektronsku identifikaciju pomoću sredstava elektronske identifikacije i autentifikacije radi pristupa toj usluzi, sredstvo elektronske identifikacije izdato u drugoj državi koja nije članica Evropske unije biće priznato za potrebe prekogranične autentifikacije na osnovu međunarodnog sporazuma o međusobnom priznavanju sredstava elektronske identifikacije, na principu reciprociteta, ako:

1) je sredstvo elektronske identifikacije izdato u okviru sistema elektronske identifikacije koji je stavljen na Listu sistema elektronske identifikacije koju objavljuje država sa kojom je Crna Gora potpisala međunarodni sporazum;

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 srednji ili visok stepen sigurnosti u odnosu na pristupanje toj usluzi na internetu.

Prijava sistema elektronske identifikacije Evropskoj komisiji
Član 45

Ministarstvo radi prijave sistema elektronske identifikacije na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija, dostavlja Evropskoj komisiji informacije koje se odnose na:

1) opis sistema elektronske identifikacije i njegove stepene sigurnosti,

2) podatke o fizičkom ili pravnom licu, odnosno organu vlasti koji izdaje sredstva elektronske identifikacije;

3) važeći sistem nadzora i informacije o pravilima i odgovornostima fizičkog ili pravnog lica, odnosno organa vlasti koji izdaje sredstva elektronske identifikacije, odnosno sprovodi proceduru autentifikacije;

4) fizičko ili pravno lice, odnosno organ vlasti koji upravlja registracijom jedinstvenih ličnih identifikacionih podataka;

5) opis načina ispunjavanja tehničkih zahtjeva koji se odnose na okvir interoperabilnosti iz člana 42 ovog zakona;

6) opis autentifikacije iz člana 46 stav 1 tačka 6 ovog zakona;

7) suspenziju ili opoziv sistema elektronske identifikacije.

O promjeni informacija iz stava 1 ovog člana Ministarstvo je dužno da, bez odlaganja, obavijesti Evropsku komisiju.

U slučaju iz člana 39 stav 6 ovog zakona Ministarstvo može da podnese zahtjev Evropskoj komisiji za brisanje sistema elektronske identifikacije sa Liste sistema elektronske identifikacije koju objavljuje Evropska komisija, u skladu sa Regulativom eIDAS.

Prihvatljivost sistema elektronske identifikacije na nivou Evropske unije

Član 46

Sistem elektronske identifikacije može se prijaviti u skladu sa članom 45 ovog zakona ako:

1) su sredstva elektronske identifikacije izdata, na jedan ili više sljedećih načina, i to od:

- Crne Gore,
- druge države članice Evropske unije,
- druge države koja nije članica Evropske unije, pod uslovom da je priznat od strane Crne Gore;

2) sredstva elektronske identifikacije mogu da se koriste za pristup najmanje jednoj usluzi koju pruža organ vlasti, a koja zahtijeva elektronsku identifikaciju u državi članici Evropske unije koja sprovodi prijavljivanje sistema na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija;

3) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema ispunjavaju zahtjeve bilo kojeg stepena sigurnosti iz člana 35 stav 2 ovog zakona;

4) Crna Gora obezbijedi da se identifikacioni podaci, u skladu sa tehničkim specifikacijama, standardima i procedurama za odgovarajući stepen sigurnosti iz člana 35 stav 2 ovog zakona, pripisuju fizičkom ili pravnom licu koje koristi identifikacione podatke u elektronskom obliku u vrijeme kad su sredstva elektronske identifikacije izdata u okviru tog sistema;

5) davalac elektronske identifikacije koji izdaje sredstva elektronske identifikacije u okviru tog sistema obezbijedi da se sredstva elektronske identifikacije pripisuju fizičkom ili pravnom licu koje koristi identifikacione podatke u elektronskom obliku u skladu sa odgovarajućim stepenom sigurnosti iz člana 35 stav 2 ovog zakona;

6) Crna Gora obezbijedi dostupnost autentifikacije na internetu, tako da zainteresovana strana može potvrditi identifikacione podatke primljene u elektronskom obliku.

Najmanje šest mjeseci prije prijavljivanja sistema elektronske identifikacije na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija, Crna Gora dostavlja drugim državama članicama Evropske unije opis sistema elektronske identifikacije radi ocjene tog sistema u skladu sa Regulativom eIDAS.

Narušavanje bezbjednosti sistema elektronske identifikacije na prekograničom nivou

Član 47

U slučaju povrede ili djelimičnog ugrožavanja sistema elektronske identifikacije davaoca elektronske identifikacije koji je prijavljen na Listu sistema elektronske identifikacije koju objavljuje Evropska komisija, na način koji utiče na pouzdanost prekogranične autentifikacije

tog sistema, Crna Gora, bez odlaganja, suspenduje ili opoziva tu prekograničnu autentifikaciju ili ugrožene djelove sistema elektronske identifikacije i obavještava države članice Evropske unije i Evropsku komisiju u skladu sa Regulativom eIDAS.

Kad je povreda ili ugrožavanje iz stava 1 ovog člana otklonjeno, Crna Gora uspostavlja prekograničnu autentifikaciju i, bez odlaganja, obavještava druge države članice Evropske unije i Evropsku komisiju u skladu sa Regulativom eIDAS.

Ako povreda ili ugrožavanje iz stava 1 ovog člana nije otklonjena u roku od tri mjeseca od suspenzije ili opoziva, Crna Gora obavještava druge države članice Evropske unije i Evropsku komisiju o povlačenju sistema elektronske identifikacije u skladu sa Regulativom eIDAS.

Odgovornost na prekograničnom nivou
Član 48

Crna Gora odgovorna je za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveza prilikom prekogranične transakcije u skladu sa članom 46 stav 1 tač. 4 i 6 ovog zakona.

Davalac 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 46 stav 1 tačka 5 ovog zakona.

Davalac 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 46 stav 1 tačka 6 ovog zakona prilikom prekogranične transakcije.

Pristup hardverskim i softverskim funkcijama
Član 49

Kad davaoci evropskih novčanika digitalnog identiteta i davaoci sredstava elektronske identifikacije koji na nivou Evropske unije postupaju u profesionalne i komercijalne svrhe i koriste osnovne usluge platforme, za potrebe pružanja evropskih novčanika digitalnog identiteta i sredstava elektronske identifikacije krajnjih korisnika, predstavljaju poslovne korisnike, pružaoci velikih platformi tim davaocima omogućavaju besplatnu i efikasnu interoperabilnost i u svrhu interoperabilnosti, pristup istom operativnom sistemu, hardveru ili softverskim karakteristikama.

III. USLUGE POVJERENJA

Uslovi za nekvalifikovane davaoce usluga povjerenja
Član 50

Nekvalifikovani davalac usluga povjerenja koji pruža nekvalifikovane usluge povjerenja treba da ispunjava sljedeće uslove, i to da:

1) ima odgovarajuće politike i preduzima odgovarajuće mjere za upravljanje pravnim, poslovnim, operativnim i drugim direktnim ili indirektnim rizicima za pružanje nekvalifikovanih usluga povjerenja koje, bez obzira na mjere informacione bezbjednosti propisane zakonom kojim se uređuje informaciona bezbjednost, uključuju najmanje mjere koje se odnose na:
- procedure registracije i uključivanja za pružanje usluga povjerenja,
- proceduralne ili administrativne provjere potrebne za pružanje usluga povjerenja,
- upravljanje i sprovođenje usluga povjerenja;

2) obavještava Ministarstvo, ugrožene korisnike koje je moguće identifikovati, javnost ako je to od javnog interesa i, ako je to primjenjivo, druga relevantna nadležna tijela, o bilo kakvom

narušavanju bezbjednosti ili poremećajima u pružanju usluga ili u sprovođenju mjera iz tačke 1 ovog člana, koji imaju značajan uticaj na pruženu uslugu povjerenja ili na lične podatke koji se u njoj čuvaju, bez nepotrebnog odlaganja, a najkasnije 24 sata od saznanja o bilo kakvom narušavanju bezbjednosti ili poremećaju.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

Prijava o početku pružanja nekvalifikovanih usluga povjerenja
Član 51

Nekvalifikovane usluge povjerenja može da pruži nekvalifikovani davalac usluga povjerenja koji je upisan u evidenciju nekvalifikovanih davalaca usluga povjerenja, koju vodi Ministarstvo.

Upis u evidenciju iz stava 1 ovog člana vrši se na osnovu prijave o početku pružanja nekvalifikovane usluge povjerenja koju nekvalifikovani davalac usluge povjerenja podnosi Ministarstvu, najmanje osam dana prije dana koji je u prijavi naznačen kao dan početka pružanja nekvalifikovanih usluga povjerenja.

O promjenama u pružanju usluga povjerenja nekvalifikovani davalac usluga povjerenja dužan je da obavijesti Ministarstvo, podnošenjem prijave.

Uz prijave iz st. 2 i 3 ovog člana prilažu se akti o načinu i postupcima pružanja nekvalifikovanih usluga povjerenja i odgovarajuće politike iz člana 50 stav 1 tačka 1 ovog zakona.

Prijave iz st. 2 i 3 ovog člana, podnose se na propisanom obrascu.

Obrazac i bliži sadržaj prijava iz st. 2 i 3 ovog člana propisuje Ministarstvo.

Sadržaj evidencije nekvalifikovanih davalaca usluga povjerenja
Član 52

Evidencija nekvalifikovanih davalaca usluga povjerenja sadrži podatke o nekvalifikovanom davaocu usluga 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 iz stava 1 ovog člana vodi se u elektronskom obliku pogodnom za automatsku obradu i objavljuje na internet stranici Ministarstva.

Bliži sadržaj evidencije iz stava 1 ovog člana propisuje Ministarstvo.

Uslovi za kvalifikovane davaoce usluga povjerenja
Član 53

Kvalifikovani davalac usluga povjerenja koji pruža kvalifikovane usluge povjerenja mora da ispunjava sljedeće uslove, i to da:

1) prilikom izdavanja kvalifikovanog sertifikata ili kvalifikovane elektronske potvrde atributa provjeri identitet ako je primjenjivo, bilo koje specifične atribute fizičkog ili pravnog lica, odnosno organa vlasti, kome treba da se izda kvalifikovani sertifikat ili kvalifikovana elektronska potvrda atributa;

2) 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 i odgovarajućih bezbjednosnih procedura za pružanje kvalifikovanih usluga povjerenja, kao i zaštitu podataka o ličnosti;

3) posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu pružanjem kvalifikovanih usluga povjerenja, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih usluga povjerenja koje je izdao, ako za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete;

4) na jasan, sveobuhvatan i lako dostupan način, na javno dostupnom prostoru i pojedinačno, informiše svako lice koje želi da koristi kvalifikovanu uslugu povjerenja, o preciznim uslovima korišćenja te usluge, uključujući sva ograničenja u pogledu njenog korišćenja;

5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku bezbjednost i pouzdanost procesa, koje ti sistemi podržavaju, uključujući korišćenje kriptografskih tehnika;

6) koristi pouzdane sisteme za čuvanje podataka koji su mu dati, u provjerljivom obliku, tako da:

- oni budu javno dostupni za preuzimanje samo kad je pribavljena saglasnost lica na koju se podaci odnose,
- samo ovlašćena lica mogu da unose i mijenjaju sačuvane podatke,
- se može provjeriti autentičnost podataka;

7) ima odgovarajuće politike i preduzima odgovarajuće mjere za upravljanje pravnim, poslovnim, operativnim i drugim direktnim ili indirektnim rizicima za pružanje kvalifikovanih usluga povjerenja koje, bez obzira na mjere informacione bezbjednosti u skladu sa zakonom kojim se uređuje informaciona bezbjednost, uključuju najmanje mjere koje se odnose na:

- postupke registracije i uključivanja za usluge povjerenja,
- proceduralne ili administrativne provjere potrebne za pružanje usluga povjerenja,
- upravljanje i sprovođenje usluga povjerenja;

8) preduzima odgovarajuće mjere protiv falsifikovanja, krađe ili zloupotrebe podataka ili neovlašćenog brisanja, izmjene ili onemogućavanja pristupa podacima;

9) evidentira i čini dostupnim onoliko dugo koliko je to potrebno, nakon prestanka obavljanja poslova kvalifikovanog davaoca usluga povjerenja, sve bitne informacije povezane sa podacima koje je pružio i primio kvalifikovani davalac usluga povjerenja, za potrebe pružanja dokaza u pravnim postupcima i u svrhu obezbjeđivanja pružanja usluge u kontinuitetu;

10) ima ažuriran plan prekida pružanja kvalifikovane usluge povjerenja radi obezbjeđivanja njenog kontinuiteta;

11) uspostavi i ažurira bazu podataka izdatih sertifikata, za kvalifikovane davaoce usluga povjerenja koji izdaju kvalifikovane sertifikate;

12) obezbijedi da se prostorije i oprema koju koriste za pružanje kvalifikovanih usluga povjerenja nalaze na teritoriji Crne Gore;

13) podatke i dokumenta koja se nalaze u informacionom sistemu ne skladišti na informaciono-komunikacionoj infrastrukturi van Crne Gore, ako posebnim zakonom ili potvrđenim međunarodnim ugovorom nije drukčije utvrđeno.

Provjeru identiteta iz stava 1 tačka 1 ovog člana vrši kvalifikovani davalac usluga povjerenja neposredno ili preko treće strane, na osnovu jedne od sljedećih metoda, ili, kad je to potrebno, njihovom kombinacijom:

- pomoću novčanika digitalnog identiteta ili prijavljenog sredstva elektronske identifikacije koje ispunjava zahtjeve iz člana 35 stav ovog zakona, u pogledu visokog stepena sigurnosti;
- sertifikatom kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata, koji je izdat u skladu sa al. 1, 3 ili 4 ovog stava;
- korišćenjem drugih metoda koje obezbjeđuju identifikaciju lica sa visokim stepenom sigurnosti, čiju usaglašenost potvrđuje tijelo za ocjenjivanje usaglašenosti;
- fizičkim prisustvom fizičkog lica ili ovlašćenog predstavnika pravnog lica, odnosno organa vlasti, na osnovu važeće javne isprave sa fotografijom, koja je izdata u skladu sa zakonom.

Provjeru atributa iz stava 1 tačka 1 ovog člana vrši kvalifikovani davalac usluga povjerenja neposredno ili preko treće strane, na osnovu jedne od sljedećih metoda, ili, kad je to potrebno, njihovom kombinacijom:

- pomoću novčanika digitalnog identiteta ili prijavljenog sredstva elektronske identifikacije, koje ispunjava zahtjeve iz člana 35 stav 2 ovog zakona, u pogledu visokog stepena sigurnosti;
- sertifikatom kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata, koji je izdat u skladu sa stavom 2 al. 1, 3 ili 4 ovog člana;
- putem kvalifikovane elektronske potvrde atributa;
- korišćenjem drugih metoda koje koje obezbjeđuju provjeru atributa sa visokim stepenom sigurnosti, čiju usaglašenost potvrđuje tijelo za ocjenjivanje usaglašenosti;
- fizičkim prisustvom fizičkog lica ili ovlašćenog predstavnika pravnog lica, odnosno organa vlasti, uz pomoć odgovarajućih dokaza i postupaka, u skladu sa zakonom.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

Obaveza obavještavanja o promjenama
Član 54

Kvalifikovani davalac usluga povjerenja dužan je da obavijesti Ministarstvo, najmanje mjesec dana prije sprovođenja bilo kakve promjene u pružanju kvalifikovanih usluga povjerenja ili najmanje tri mjeseca u slučaju namjere da se pružanje tih usluga prekine, o tim promjenanama, odnosno namjeri.

Kvalifikovani davalac usluga povjerenja dužan je da obavijesti Ministarstvo, ugrožene korisnike koja je moguće identifikovati, druge nadležne organe kad je to moguće i na zahtjev Ministarstva javnost, ako je to od javnog interesa, o bilo kakvim kršenjima bezbjednosti ili prekidima u pružanju kvalifikovane usluge povjerenja ili sprovođenju mjera iz člana 53 stav 1 tačka 7 ovog zakona, koje imaju značajan uticaj na pružanje te usluge, bez odlaganja, a najkasnije u roku od 24 sata.

Ministarstvo može od kvalifikovanog davaoca usluga povjerenja u vezi sa pružanjem kvalifikovanih usluga povjerenja zatražiti dodatne informacije u vezi stava 1 ovog člana ili dodatni izvještaj tijela za ocjenjivanje usaglašenosti o ispunjenosti uslova u vezi sa pružanjem kvalifikovanih usluga povjerenja, kojim se potvrđuje da davalac usluga povjerenja ispunjava sve uslove u vezi sa pružanjem kvalifikovanih usluga povjerenja u skladu sa ovim zakonom, kao i zakonom kojim se uređuje informaciona bezbjednost, u pogledu mjera informacione bezbjednosti, a u vezi sa upravljanjem rizicima u oblasti sajber bezbjednosti.

Kad Ministarstvo ne izvrši provjeru ispunjenosti uslova u vezi sa pružanjem kvalifikovanih usluga povjerenja, u skladu sa stavom 3 ovog člana, u roku od tri mjeseca od dana obavještavanja iz st. 1 i 2 ovog člana, Ministarstvo obavještava kvalifikovanog davaoca o razlozima kašnjenja i o roku do kojeg provjera treba da bude završena.

Davaoci usluga povjerenja koji pružaju usluge povjerenja i kvalifikovane usluge povjerenja dužni su da dostavljaju Ministarstvu podatke o broju sertifikata od početka izdavanja, odnosno broju pruženih usluga povjerenja, kao i po potrebi druge informacije, na zahtjev Ministarstva.

Bliži sadržaj obavještenja iz st. 1 i 2 ovog člana propisuje Ministarstvo.

Opoziv i suspenzija sertifikata koje izdaje kvalifikovani davalac usluga povjerenja
Član 55

Kvalifikovani davalac usluga povjerenja dužan je da izvrši opoziv sertifikata u slučaju kad:

1) opoziv sertifikata zahtijeva potpisnik, odnosno autor elektronskog pečata ili njegov ovlašćeni zastupnik;

2) utvrdi da je podatak u sertifikatu pogrešan ili je sertifikat izdat na osnovu pogrešnih podataka;

3) primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice, ili organ vlasti, 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;

4) utvrdi da su podaci za izradu elektronskog potpisa, elektronskog pečata, autentifikaciju internet stranice 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 elektronskog pečata, autentifikaciju internet stranice ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost sertifikata;

6) prestaje sa radom ili mu je rad zabranjen, a izdatim sertifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja ne prenese na drugog davaoca tih usluga;

7) primi sudsku odluku ili upravni akt koji se odnose na važenje sertifikata ili

8) postoje drugi opravdani razlozi.

Kvalifikovani davalac usluga povjerenja dužan je da u roku od 24 sata od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti iz stava 1 ovog člana, izvrši opoziv sertifikata.

Kvalifikovani davalac elektronskih usluga povjerenja dužan je da na svojoj internet stranici objavi status opozvanih sertifikata, a opoziv sertifikata proizvodi dejstvo od trenutka objavljivanja statusa.

Kvalifikovani davalac elektronskih usluga povjerenja može da suspenduje sertifikat u slučajevima i na način koji navede u politikama iz člana 53 stav 1 tačka 7 ovog zakona.

Ako je sertifikat suspendovan, taj sertifikat gubi validnost tokom perioda suspenzije.

Period suspenzije iz stava 5 ovog člana mora biti jasno naznačen u bazi podataka iz člana 53 stav 1 tačka 11 ovog zakona, a status suspenzije mora biti vidljiv za pouzdajuće strane tokom perioda suspenzija.

Ako je kvalifikovani sertifikat za elektronski potpis, odnosno elektronski pečat, autentifikacija internet stranice, opozvan nakon početne aktivacije, on gubi valjanost od trenutka opoziva i njegov se status ni u kojem slučaju ne može vratiti u prijađašnje stanje.

Datum i vrijeme suspenzije i opoziva sertifikata unose se u bazu podataka iz člana 53 stav 1 tačka 11 ovog zakona.

Kvalifikovani davalac usluga povjerenja treba da pruži informacije o validnosti ili opozivu pojedinog sertifikata u svakom trenutku i nakon roka važenja, na automatizovan način koji je pouzdan, besplatan i efikasan.

Opoziv kvalifikovanih elektronskih potvrda atributa vrši se na način iz st. 2, 3 i 9 ovog člana.

Nadzor nad kvalifikovanim davaocima usluga povjerenja od strane tijela za ocjenjivanje usaglašenosti

Član 56

Tijelo za ocjenjivanje usaglašenosti vrši reviziju kvalifikovanih davalaca usluga povjerenja, najmanje svakih 24 mjeseca, o trošku davaoca usluga povjerenja.

Revizijom iz stava 1 ovog člana potvrđuje se da kvalifikovani davaoci usluga povjerenja ispunjavaju sve uslove u vezi sa pružanjem kvalifikovanih usluga povjerenja, u skladu sa ovim zakonom, kao i zakonom kojim se uređuje informaciona bezbjednost u pogledu mjera informacione bezbjednosti, a u vezi sa upravljanjem rizicima u oblasti sajber bezbjednosti.

Kvalifikovani davaoci usluga povjerenja izvještaj tijela za ocjenjivanje usaglašenosti o ispunjenosti uslova u vezi sa pružanjem kvalifikovanih usluga povjerenja dostavljaju Ministarstvu, u roku od tri dana, od dana prijema.

Kvalifikovani davalac usluga povjerenja najkasnije mjesec dana prije planirane revizije, obavještava Ministarstvo o reviziji, i omogućava da Ministarstvo, na osnovu zahtjeva može da učestvuje kao posmatrač tokom vršenja revizije.

Ministarstvo može zahtijevati od kvalifikovanog davaoca usluga povjerenja da tijelo za ocjenjivanje usaglašenosti izvrši ocjenjivanje kvalifikovanog davaoca usluga povjerenja, u bilo kojem trenutku, o trošku tog davaoca usluga povjerenja, kako bi se potvrdilo da kvalifikovani

davalac usluga povjerenja ispunjava sve uslove u vezi sa pružanjem kvalifikovanih usluga povjerenja, u skladu sa ovim zakonom.

Ministarstvo obavještava Evropsku komisiju o imenima, adresama i detaljima o akreditaciji tijela za ocjenjivanje usaglašenosti, kao i o svim promjenama, u skladu sa Regulativom eIDAS.

Ministarstvo će u slučaju postojanja sumnje da je došlo do kršenja pravila o zaštiti podataka o ličnosti, obavijestiti organ nadležan za zaštitu podataka o ličnosti, bez odlaganja.

Ako se tokom revizije iz st. 1 i 5 ovog člana utvrdi da kvalifikovani davalac usluga povjerenja ne ispunjava bilo koji od uslova u skladu sa ovim zakonom, Ministarstvo će, ako je to primjenjivo, zahtijevati od tog davaoca da u određenom roku ispuni te uslove, u skladu sa zakonom.

Ako kvalifikovani davalac usluga povjerenja ne ispuni uslove u roku koji je odredilo Ministarstvo, Ministarstvo će tom davaocu ili usluzi povjerenja koju on pruža ukinuti status kvalifikovanog davaoca usluga povjerenja, odnosno status kvalifikovane usluge povjerenja.

Kad organ nadležan za oblast informacione bezbjednosti u skladu sa zakonom kojim se uređuje informaciona bazbjednost, a koji vrši nadzor kod kvalifikovanog davaoca usluga povjerenja nad primjenom mjera informacione bezbjednosti, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, utvrdi da taj davalac ne ispunjava bilo koju od mjera informacione bezbjednosti, o tome obavještava Ministarstvo, bez odlaganja.

Na osnovu obavještenja iz stava 10 ovog člana, Ministarstvo može izvršiti reviziju ili zahtijevati od kvalifikovanog davaoca elektronskih usluga povjerenja da tijelo za ocjenjivanje usaglašenosti izvrši ocjenjivanje kvalifikovanog davaoca usluga povjerenja, u pogledu primjene mjera informacione bezbjednosti, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, o trošku tog davaoca usluga povjerenja.

Na osnovu revizije, odnosno izvještaja tijela za ocjenjivanje usaglašenosti, u skladu sa stavom 11 ovog člana, Ministarstvo će procijeniti da li kvalifikovanom davaocu usluga povjerenja treba ukinuti status kvalifikovanog davaoca usluga povjerenja ili usluzi povjerenja koju on pruža status kvalifikovane usluge povjerena.

Kad organ za zaštitu podataka o ličnosti koji kod kvalifikovanog davaoca usluga povjerenja, vrši nadzor nad zaštitom podataka o ličnosti, u skladu za zakonom kojim se uređuje zaštita podataka o ličnosti, utvrdi da da kvalifikovani davalac usluga povjerenja ne ispunjava bilo koji od uslova propisanih tim zakonom, o tome obavještava Ministarstvo, bez odlaganja.

Na osnovu obavještenja iz stava 13 ovog člana, Ministarstvo može izvršiti reviziju ili zahtijevati od kvalifikovanog davaoca usluga povjerenja da tijelo za ocjenjivanje usaglašenosti izvrši ocjenjivanje kvalifikovanog davaoca usluga povjerenja, u pogledu zaštite podataka o ličnosti, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti, o trošku tog davaoca usluga povjerenja.

Na osnovu revizije, odnosno izvještaja tijela za ocjenjivanje usaglašenosti, u skladu sa stavom 14 ovog člana, Ministarstvo će procijeniti da li tom davaocu treba ukinuti status kvalifikovanog davaoca usluga povjerenja, ili usluzi koju on pruža.

Ministarstvo obavještava kvalifikovanog davaoca usluga povjerenja o ukidanju statusa kvalifikovanog davaoca usluga povjerenja, bez odlaganja.

Ministarstvo obavještava organ iz st. 10 i 13 ovog člana, o ukinutom statusu kvalifikovanog davaoca usluga povjerenja, bez odlaganja.

Bliža pravila za akreditaciju tijela za ocjenjivanje usaglašenosti i sadržaj izvještaja tijela za ocjenjivanje propisuje Ministarstvo.

Početak pružanja kvalifikovanih usluga povjerenja
Član 57

Davalac usluga povjerenja koji namjerava da pruža kvalifikovane usluge povjerenja, podnosi Ministarstvu zahtjev za upis u Registar kvalifikovanih davalaca usluga povjerenja (u daljem tekstu: Registar).

Uz zahtjev iz stava 1 ovog člana, davalac usluga povjerenja dužan je da dostavi izvještaj tijela za ocjenjivanje usaglašenosti kojim se potvrđuje ispunjenost uslova propisanih ovim zakonom.

Ministarstvo, nakon dostavljanja zahtjeva iz stava 1 ovog člana, kao i izvještaja tijela za ocjenjivanje usaglašenosti iz stava 2 ovog člana, provjerava da li davalac usluga povjerenja ispunjava uslove za pružanje kvalifikovanih usluga povjerenja, u skladu sa ovim zakonom.

Ministarstvo, u cilju dodatne provjere primjene mjera informacione bezbjednosti koje se odnose na upravljanje rizicima u oblasti sajber bezbjednosti, zahtijeva od organa nadležnog za oblast informacione bezbjednosti da u skladu sa zakonom kojim se uređuje informaciona bezbjednost, sprovede stručni nadzor i dostavi izvještaj o izvršenom stručnom nadzoru, bez odlaganja, a najkasnije u roku od dva mjeseca od prijema tog zahtjeva.

Ako nadzor iz stava 4 ovog člana ne bude sproveden u roku iz stava 4 ovog člana, organ iz stava 4 ovog člana obavještava Ministarstvo, uz obrazloženje razloga za kašnjenje i navodi rok do kojeg će sprovesti nadzor.

Ako, na osnovu uvida u podnijeti zahtjev iz stava 1 ovog člana, izvještaj iz stava 2 ovog člana i izvještaj iz stava 4 ovog člana, utvrdi da davalac usluga povjerenja koji namjerava da pruža kvalifikovane usluge povjerenja ispunjava uslove u skladu sa ovim zakonom, Ministarstvo donosi rješenje o ispunjenosti uslova za vršenje kvalifikovanih usluga povjerenja propisanih ovim zakonom.

Rješenje iz stava 6 ovog člana donosi se u roku od tri mjeseca od dana uredno podnijetog zahtjeva.

Ako u roku iz stava 7 ovog člana ne izvrsi provjeru iz stava 6 ovog člana, Ministarstvo o tome obavještava davaoca usluga povjerenja, uz obrazloženje razloga za kašnjenje i navodi rok u kojem će izvršiti provjeru.

Bliži sadržaj obrasca zahtjeva iz stava 1 ovog člana, kao i bliži postupak provjere iz stava 3 ovog člana propisuje Ministarstvo.

Registar kvalifikovanih davalaca usluga povjerenja
Član 58

Na osnovu rješenja iz člana 57 stav 6 ovog zakona, Ministarstvo vrši upis podnosioca zahtjeva u registar kvalifikovanih davalaca usluga povjerenja.

Registar iz stava 1 ovog člana sadrži podatke o kvalifikovanom davaocu usluge povjerenja, i to:

- ime i prezime fizičkog lica, odnosno naziv pravnog lica, odnosno organa vlasti,
- adresu fizičkog lica, odnosno sjedište i adresu pravnog lica,odnosno organa vlasti,
- jedinstvenu službenu adresu za elektronsku komunikaciju,
- jedinstveni matični broj fizičkog lica, šifru djelatnosti i poreski identifikacioni broj pravnog lice, odnosno matični broj organa vlasti,
- registarski broj iz Centralnog registra privrednih subjekata.

Registar iz stava 1 ovog člana vodi se u elektronskom obliku i objavljuje na internet stranici Ministarstva.

Registar iz stava 1 ovog člana potpisuje se naprednim elektronskim potpisom, odnosno pečatira naprednim elektronskim pečatom.

Bliži sadržaj i način vođenja registra iz stava 1 ovog člana propisuje Ministarstvo.

Organi vlasti kao davaoci usluga povjerenja
Član 59

Usluge povjerenja i kvalifikovane usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, pruža Ministarstvo.

Usluge povjerenja i kvalifikovane usluge povjerenja mogu pružati i drugi organi vlasti u okviru poslova iz svoje nadležnosti, u skladu sa posebnim zakonom.

Kad Ministarstvo i organ vlasti pružaju kvalifikovane usluge povjerenja moraju ispunjavati uslove iz člana 53 stav 1 tač. 1 i 2 i tač. 4 do 11 ovog zakona i člana 54 ovog zakona.

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

Lista povjerenja
Član 60

Ministarstvo vodi i objavljuje Listu povjerenja davalaca usluga povjerenja (u daljem tekstu: Lista povjerenja), koja uključuje informacije o kvalifikovanim davaocima usluga povjerenja i nekvalifikovanim davaocima usluga povjerenja, zajedno sa informacijama o uslugama povjerenja koje oni pružaju.

Lista povjerenja vodi se na način pogodan za automatsku obradu i objavljuje na internet stranici Ministarstva, putem bezbjednog kanala.

Lista povjerenja vodi se u skladu sa međunarodnim standardima i potpisuje naprednim elektronskim potpisom, odnosno pečatira naprednim elektronskim pečatom.

Bliži način vođenja Liste povjerenja propisuje Ministarstvo.

EU oznaka povjerenja za kvalifikovane usluge povjerenja
Član 61

Kvalifikovani davalac elektronskih usluga povjerenja, nakon upisa na Listu povjerenja može da koristi EU oznaku povjerenja koja na jednostavan, prepoznatljiv i jasan način označava kvalifikovane usluge povjerenja koje pruža.

Korišćenjem EU oznake povjerenja, kvalifikovani davalac usluga povjerenja obezbjeđuje da veza sa Listom povjerenja bude dostupna na internet stranici tog davaoca.

Odgovornost davaoca usluga povjerenja i teret dokazivanja
Član 62

Davalac usluga povjerenja odgovoran je za štetu koju je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu, ako nije postupio u skladu sa ovim zakonom.

Svako fizičko ili pravno lice koje je pretrpjelo štetu usljed toga što davalac usluga povjerenja nije postupio u skladu sa ovim zakonom ima pravo na naknadu štete, u skladu sa zakonom.

Teret dokazivanja namjere ili nepažnje nekvalifikovanog davaoca usluga poverenja je na fizičkom ili pravnom licu koje zahtijeva naknadu štete iz stava 2 ovog člana.

Namjera ili nepažnja kvalifikovanog davaoca elektronskih usluga povjerenja podrazumijeva se, osim ako taj kvalifikovani davalac usluga povjerenja ne dokaže da je šteta iz stava 1 ovog člana nastala bez namjere ili nepažnje tog kvalifikovanog davaoca usluga povjerenja.

Davalac usluga povjerenja koji je unaprijed obavijestio svoje korisnike o ograničenjima prilikom korišćenja usluga koje pruža, nije odgovoran za štetu nastalu zbog korišćenja usluga kojima se prekoračuju ta ograničenja.

Prekogranično priznavanje usluga povjerenja
Član 63

Usluge povjerenja koje pružaju davaoci usluga povjerenja sa sjedištem u jednoj od država članica Evropske unije imaju jednako pravno dejstvo kao kvalifikovano usluge povjerenja koje pružaju kvalifkovani davaoci usluga povjerenja u Crnoj Gori, kad se usluge povjerenja koje se pružaju od strane davalaca sa sjedištem u jednoj od država članica Evropske unije priznaju na osnovu međunarodnog sporazuma o međusobnom priznavanju usluga povjerenja koji se zasniva na principu reciprociteta, čiji sastavni dio su implementacioni akti za njegovo sprovođenje.

Usluge povjerenja koje pružaju davaoci usluga povjerenja sa sjedištem u drugoj državi koja nije članica Evropske unije imaju jednako pravno dejstvo kao kvalifikovano usluge povjerenja

koje pružaju kvalifkovani davaoci usluga povjerenja u Crnoj Gori, kad se usluge povjerenja, koje se pružaju od strane davalaca sa sjedištem u drugoj državi koja nije članica Evropske unije priznaju na osnovu međunarodnog sporazuma o međusobnom priznavanju usluga povjerenja koji se zasniva na principu reciprociteta, čiji sastavni dio su implementacioni akti za njegovo sprovođenje.

Sporazumi i implementacioni akti iz st. 1 i 2 ovog člana obezbjeđuju ispunjavanje uslova za kvalifikovane davaoce usluga povjerenja, u skladu sa zakonom.

Prekogranično priznavanje kvalifikovanih usluga povjerenja
Član 64

Kvalifikovani elektronski potpis i kvalifikovani elektronski pečat koji se zasnivaju na kvalifikovanom sertifikatu izdati u jednoj državi članici Evropske unije priznaju se kao kvalifikovani elektronski potpis, odnosno kvalifikovani elektronski pečat u Crnoj Gori.

Kvalifikovana sredstva za izradu elektronskih potpisa i kvalifikovana sredstva za izradu elektronskih pečata sertifikovana u jednoj državi članici Evropske unije priznaju se kao kvalifikovana sredstva za izradu elektronskih potpisa, odnosno kvalifikovana sredstva za izradu elektronskih pečata u Crnoj Gori.

Kvalifikovani sertifikat za elektronske potpise, kvalifikovani sertifikat za elektronske pečate, kvalifikovana usluga povjerenja za upravljanje kvalifikovanim sredstvima za izradu elektronskih potpisa na daljinu i kvalifikovana usluga povjerenja za upravljanje kvalifikovanim sredstvima za izradu elektronskih pečata na daljinu koji su pruženi u jednoj državi članici Evropske unije priznaju se kao kvalifikovani sertifikati za elektronske potpise, kvalifikovani sertifikat za elektronske pečate, kvalifikovana usluga povjerenja za upravljanje kvalifikovanim sredstvima za izradu elektronskih potpisa na daljinu, odnosno kvalifikovana usluga povjerenja za upravljanje kvalifikovanim sredstvima za izradu elektronskih pečata na daljinu u Crnoj Gori.

Kvalifikovana usluga validacije kvalifikovanih elektronskih potpisa i kvalifikovana usluga validacije kvalifikovanih elektronskih pečata pružene u jednoj državi članici Evrospke unije priznaju se kao kvalifikovana usluga validacije kvalifikovanih elektronskih potpisa odnosno kvalifikovana usluga validacije kvalifikovanih elektronskih pečata u Crnoj Gori.

Kvalifikovana usluga čuvanja kvalifikovanih elektronskih potpisa i kvalifikovana usluga čuvanja kvalifikovanih elektronskih pečata pružene u jednoj državi članici Evropske unije priznaju se kao kvalifikovana usluga čuvanja kvalifikovanih elektronskih potpisa odnosno kvalifikovana usluga čuvanja kvalifikovanih elektronskih pečata u Crnoj Gori.

Kvalifikovani elektronski vremenski pečat izdat u jednoj državi članici Evropske unije priznaje se kao kvalifikovani elektronski vremenski pečat u Crnoj Gori.

Kvalifikovani sertifikat za autentifikaciju internet stranica izdat u jednoj državi članici Evropske unije priznaje se kao kvalifikovani sertifikat za autentifikaciju internet stranica u Crnoj Gori.

Kvalifikovana usluga elektronske preporučene dostave pružena u jednoj državi članici Evropske unije priznaje se kao kvalifikovana usluga elektronske preporučene dostave u Crnoj Gori.

Kvalifikovana elektronska potvrda atributa izdata u jednoj državi članici Evropskoj uniji priznaje se kao kvalifikovana elektronska potvrda atributa u Crnoj Gori.

Kvalifikovana usluga elektronskog arhiviranja pružena u jednoj državi članici Evropske unije priznaje se kao kvalifikovana usluga elektronskog arhiviranja u Crnoj Gori.

Kvalifikovana elektronska evidencija stavljena na raspolaganje u jednoj državi članici Evropske unije priznaje se kao kvalifikovana elektronska evidencija u Crnoj Gori.

Elektronski, napredni elektronski i kvalifikovani elektronski potpis
Član 65

Elektronski potpis predstavlja podatke u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koje potpisnik koristi za potpisivanje.

Napredni elektronski potpis je elektronski potpis koji ispunjava posebne uslove iz člana 66 ovog zakona.

Kvalifikovani elektronski potpis je napredni elektronski potpis koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog potpisa i koji je zasnovan na kvalifikovanom sertifikatu za elektronski potpis.

Uslovi za napredni elektronski potpis
Član 66

Napredni elektronski potpis mora da ispunjava sljedeće uslove, i to da:

1) je na nedvosmislen način povezan sa potpisnikom;

2) može da identifikuje potpisnika;

3) je izrađen korišćenjem podataka za izradu elektronskog potpisa koje potpisnik može, uz visok nivo sigurnosti, da koristi isključivo pod njegovim nadzorom;

4) je povezan sa podacima na koje se odnosi, i to na način da je bilo koja naknadna promjena podataka uočljiva.

Pravno dejstvo elektronskog potpisa i naprednog elektronskog potpisa
Član 67

Elektronskom potpisu se kao dokazu u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što je u elektronskom obliku ili zbog toga što ne ispunjava sve uslove za kvalifikovani elektronski potpis.

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 68

Kvalifikovani elektronski potpis ima isto pravno dejstvo kao i svojeručni potpis.

Elektronski potpis za prekogranično korišćenje elektronskih usluga
Član 69

Kad se zahtijeva napredni elektronski potpis za korišćenje elektronske usluge koju pruža organ vlasti ili za korišćenje elektronske usluge koja se pruža u ime organa vlasti, organi vlasti će priznati napredni elektronski potpis, napredni elektronski potpis koji su zasnovani na kvalifikovanom sertifikatu za elektronski potpis i kvalifikovane elektronske potpise, najmanje u formatima ili korišćenjem metoda koje je objavila Evropska komisija.

Kad se zahtijeva napredni elektronski potpis koji je zasnovan na kvafikovanom sertifikatu za korišćenje elektronske usluge koju pruža organ vlasti ili elektronske usluge koja se pruža u ime organa vlasti, organ vlasti će priznati napredne elektronske potpise koji se zasnivaju na kvalifikovanom sertifikatu i kvalifikovane potpise najmanje u formatima ili korišćenjem metoda koje je objavila Evropska komisija.

Za prekogranično korišćenje elektronskih usluga koje pruža organ vlasti ne zahtijeva se elektronski potpis višeg nivoa bezbjednosti od kvalifikovanog elektronskog potpisa.

Kvalifikovani sertifikat za elektronski potpis
Član 70

Kvalifikovani sertifikat za elektronski potpis je sertifikat koji izdaje kvalifikovani davalac usluga povjerenja, i koji sadrži:

1) oznaku, najmanje u obliku prikladnom za automatsku obradu, da je sertifikat izdat kao kvalifikovani sertifikat za elektronski potpis;

2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani sertifikat za elektronski potpis, uz navođenje oznake države u kojoj je to lice, odnosno organ vlasti registrovan kao kvalifikovani davalac usluga povjerenja, i to za:

- pravno lice, odnosno organ vlasti: naziv, i kad je to promjenjivo matični, odnosno poreski identifikacioni broj,
- fizičko lice: ime i prezime;

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

4) podatke za validaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa;

5) podatke o početku i kraju perioda važenja tog sertifikata;

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

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

8) lokaciju na kojoj je besplatno dostupan sertifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronskih usluga povjerenja iz tačke 7 ovog stava;

9) informacije ili lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog sertifikata;

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

11) identifikacioni broj.

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.

Kvalifikovani sertifikat za elektronski potpis mora da ispunjava odgovarajuće standarde.

Standarde iz stava 3 ovog člana propisuje Ministarstvo.

Kvalifikovano sredstvo za izradu elektronskog potpisa
Član 71

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) je povjerljivost podataka koji se koriste za izradu elektronskog potpisa u dovoljnoj mjeri obezbijeđena;

2) se podaci za izradu kvalifikovanog elektronskog potpisa sa visokom sigurnošću, mogu pojaviti samo jedanput;

3) se podaci za izradu kvalifikovanog elektronskog potpisa sa visokom sigurnošću, ne mogu utvrditi iz tog potpisa;

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

5) 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.

Generisanje podataka ili upravljanje tim podacima za izradu elektronskog potpisa ili dupliranje takvih podataka za potrebe pravljenja rezervnih sigurnosnih kopija obavlja samo u ime i na zahtjev potpisnika kvalifikovani davalac usluga povjerenja koji pruža kvalifikovanu uslugu povjerenja za upravljanje kvalifikovanim sredstvom za izradu elektronskih potpisa na daljinu.

Uslovi za kvalifikovanu uslugu za upravljanje kvalifikovanim sredstvima za izradu elektronskog potpisa na daljinu

Član 72

Upravljanje kvalifikovanim sredstvom za izradu elektronskog potpisa na daljinu može da vrši samo kvalifikovani davalac usluga povjerenja, koji:

1) generiše ili upravlja podacima za izradu elektronskog potpisa u ime potpisnika;

2) duplira podatke za izradu elektronskog potpisa radi izrade rezervnih kopija, nezavisno od člana 71 sav 2 tačka 5 ovog zakona, pod uslovom da su ispunjeni sljedeći uslovi, i to da:

- sigurnost dupliranih podataka mora biti na istom nivou, kao i sigurnost izvornih podataka,
- broj dupliranih podataka ne prelazi najmanji broj potreban za obezbjeđenje kontinuiteta pružanja usluge;

3) ispunjava sve uslove u vezi sa sertifikacijom iz člana 73 ovog zakona.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

Sertifikacija kvalifikovanih sredstava za izradu elektronskih potpisa

Član 73

Sertifikacija kvalifikovanih sredstava za izradu elektronskih potpisa podrazumijeva postupak provjere usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa sa uslovima iz člana 71 ovog zakona i vrši je tijelo za ocjenjivanje usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa, koje se imenuje u skladu sa zakonom kojim se uređuju tehnički zahtjevi za proizvode i ocjenjivanju usaglašenosti (u daljem tekstu: imenovano tijelo).

Sertifikacija iz stava 1 ovog člana sprovodi se jednim od sljedećih postupaka, i to postupkom:

1) procjenjivanja bezbjednosti, koji se sprovodi u skladu sa jednim od standarda za procjenu bezbjednosti proizvoda informacionih tehnologija koji su obuhvaćeni spiskom standarda za ocjenjivanje bezbjednosti proizvoda informacionih tehnologija ili

2) različitim od postupka iz stava 2 tačka 1 ovog člana, pod uslovom da on koristi uporedive nivoe bezbjednosti i da imenovano tijelo obavijesti Ministarstvo o tom postupku.

Postupak iz stava 2 tačka 2 ovog člana može da se primjenjuje samo u slučaju nepostojanja standarda iz stava 2 tačka 1 ovog člana ili kad je u toku postupak procjene bezbjednosti iz stava 2 tačka 1 ovog člana.

Nakon što imenovano tijelo utvrdi da su ispunjeni uslovi iz stava 1 ovog člana izdaje sertifikat za kvalifikovano sredstavo za izradu elektronskih potpisa.

Sertifikat iz stava 4 ovog člana izdaje se na vrijeme od pet godina, pod uslovom da se svake dvije godine sprovodi procjena ranjivosti.

Ako se procjena ranjivosti iz stava 5 ovog člana ne sprovede, odnosno ako se ranjivost identifikuje i ne otkloni, sertifikat se poništava.

Davalac usluga povjerenja dužan je da o isteku vremena na koji je izdat setifikat iz stava 4 ovog člana kao i o njegovom opozivu, odnosno produžetku važenja, bez odlaganja, obavijesti Ministarstvo.

Bliže uslove koje treba da ispuni imenovano tijelo iz stava 1 ovog člana, kao i postupak sertifikacije propisuje Ministarstvo.

Registar kvalifikovanih sredstava za izradu elektronskih potpisa
Član 74

Zahtjev za upis u Registar kvalifikovanih sredstava za izradu elektronskih potpisa podnosi se Ministarstvu, na propisanom obrascu.

Uz zahtjev iz stava 1 ovog člana podnosi se izvještaj o usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa sa uslovima iz člana 71 ovog zakona, koji sačinjava imenovano tijelo.

Zahtjev iz stava 1 ovog člana može se podnijeti i za kvalifikovano sredstvo za izradu elektronskih potpisa sa Liste sertifikovanih kvalifikovanih sredstava za izradu elektronskog potpisa koju objavljuje Evropska komisija.

Registar iz stava 1 ovog člana vodi Ministarstvo.

Imenovano tijelo, bez odlaganja, a najkasnije u roku od sedam dana, obavještava Ministarstvo o izvršenoj sertifikaciji iz člana 73 ovog zakona, poništavanju sertifikata iz člana 73 stav 4 ovog zakona, odnosno o drugoj nastaloj promjeni.

Kad je kvalifikovano sredstvo za izradu elektronskog potpisa koje je objavljeno na Listi iz stava 3 ovog člana opozvano, podnosilac zahtjeva za upis u Registar iz stava 1 ovog člana, o tome obavještava Ministarstvo, bez odlaganja, a najkasnije u roku od 30 dana nakon opoziva.

Registar iz stava 1 ovog člana vodi se u elektronskom obliku i dostupan je javnosti na internet stranici Ministarstva.

Obrazac i sadržaj zahtjeva iz stava 1 ovog člana, dokumentaciju koja se podnosi uz zahtjev i sadržaj registra iz stava 1 ovog člana propisuje Ministarstvo.

Obavještavanje Evropske komisije o kvalifikovanim sredstvima za izradu elektronskog potpisa
Član 75

Ministarstvo bez odlaganja, a najkasnije mjesec dana nakon završetka sertifikacije iz člana 73 ovog zakona, obavještava Evropsku komisiju o kvalifikovanim sredstvima za izradu elektronskog potpisa, koja su sertifikovani od strane imenovanog tijela.

Ministarstvo bez odlaganja, a najkasnije 30 dana nakon poništenja sertifikata iz člana 73 stav 4 ovog zakona obavještava Evropsku komisiju o informacijama o sredstvima za izradu elektronskog potpisa koja su opozvana.

Uslovi za validaciju kvalifikovanih elektronskih potpisa
Član 76

Postupkom validacije kvalifikovanog elektronskog potpisa potvrđuje se validnost kvalifikovanog elektronskog potpisa, pod uslovom da:

1) je sertifikat na kojem se zasniva elektronski potpis u trenutku potpisivanja bio kvalifikovani sertifikat za elektronski potpis u smislu člana 70 ovog zakona;

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

3) podaci za validaciju potpisa odgovaraju podacima koji se dostavljaju pouzdajućoj strani;

4) je jedinstveni skup podataka koji predstavlja potpisnika u kvalifikovanom sertifikatu za elektronski potpis ispravno dostavljen pouzdajućoj strani;

5) je korišćenje pseudonima, ako je pseudonim korišćen u trenutku potpisivanja, jasno naznačeno pouzdajućoj strani;

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

7) nije ugrožen integritet potpisanih podataka;

8) su uslovi iz člana 66 ovog zakona bili ispunjeni u trenutku izrade elektronskog potpisa.

Sistem koji se koristi za validaciju kvalifikovanog elektronskog potpisa obezbjeđuje pouzdajućoj strani ispravan rezultat postupka validacije i omogućava otkrivanje svih problema koji mogu uticati na bezbjednost.

Postupak validacije kvalifikovanih elektronskih potpisa vrši se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za postupak validacije kvalifikovanih elektronskih potpisa propisuje Ministarstvo.

Uslovi za validaciju naprednih elektronskih potpisa zasnovanih na kvalifikovanim sertifikatima

Član 77

Postupkom validacije naprednog elektronskog potpisa koji se zasniva na kvalifikovanom sertifikatu potvrđuje se validnost naprednog elektronskog potpisa koji se zasniva na kvalifikovanom sertifikatu, pod pod uslovom da:

1) je sertifikat na kojem se zasniva elektronski potpis u trenutku potpisivanja bio kvalifikovani sertifikat za elektronski potpis, u smilu člana 70 ovog zakona;

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

3) podaci za validaciju potpisa odgovaraju podacima koji se dostavljaju pouzdajućoj strani;

4) je jedinstveni skup podataka koji predstavlja potpisnika u kvalifikovanom sertifikatu za elektronski potpis ispravno dostavljen pouzdajućoj strani;

5) je korišćenje pseudonima, ako je pseudonim bio korišćen u trenutku potpisivanja, jasno naznačeno pouzdajućoj strani;

6) nije ugrožen integritet potpisanih podataka;

7) su uslovi iz člana 66 ovog zakona ispunjeni u trenutku izrade potpisa.

Sistem koji se koristi za validaciju naprednog elektronskog potpisa koji se zasniva na kvalifikovanom sertifikatu obezbjeđuje pouzdajućoj strani ispravan rezultat postupka validacije i omogućava otkrivanje svih problema koji mogu uticati na bezbjednost.

Postupak validacije naprednih elektronskih potpisa vrši se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za postupak validacije naprednih elektronskih potpisa propisuje Ministarstvo.

Kvalifikovana usluga validacije za kvalifikovane elektronske potpise

Član 78

Kvalifikovanu uslugu validacije kvalifikovanih elektronskih potpisa može pružati samo kvalifikovani davalac usluga povjerenja, koji:

1) obezbjeđuje validaciju u skladu sa članom 76 ovog zakona;

2) omogućava pouzdajućim stranama da dobiju rezulatat postupka validacije na automatizovan način koji je pouzdan i efikasan;

3) omogućava da je rezultat postupka validacije iz stava 1 tačka 2 ovog člana, potpisan naprednim elektronskim potpisom ili pečatiran naprednim elektronskim pečatom kvalifikovanog davaoca usluge validacije.

Kvalifikovana usluga validacije kvalifikovanih elektronskih potpisa pruža se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovanu uslugu validacije kvalifikovanih elektronskih potpisa propisuje Ministarstvo.

Kvalifikovana usluga čuvanja kvalifikovanih elektronskih potpisa

Član 79

Kvalifikovanu uslugu čuvanja kvalifikovanih elektronskih potpisa može pružati samo kvalifikovani davalac usluga povjerenja koji koristi postupke i tehnologije koje mogu produžiti pouzdanost kvalifikovanog elektronskog potpisa na period koji je duži od perioda tehnološke validnosti.

Kvalifikovana usluga čuvanja kvalifikovanih elektronskih potpisa pruža se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovanu uslugu čuvanja kvalifikovanih elektronskih potpisa propisuje Ministarstvo.

Elektronski, napredni elektronski i kvalifikovani elektronski pečat

Član 80

Elektronski pečat je skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim podacima u elektronskom obliku, kako bi se obezbijedilo porijeklo i integritet tih podataka.

Napredni elektronski pečat je elektronski pečat koji ispunjava posebne uslove iz člana 81 ovog zakona.

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

Uslovi za napredne elektronske pečate

Član 81

Napredni elektronski pečat mora da ispunava sljedeće uslove, i to da:

1) je na nedvosmislen način povezan sa autorom pečata;

2) može da identifikuje autora pečata;

3) je izrađen korišćenjem podataka za izradu elektronskog pečata koje autor pečata može, uz visok nivo sigurnosti, da koristi isključivo pod njegovim nadzorom; i

4) da je povezan sa podacima na koje se odnosi, i to na takav način da je bilo koja naknadna promjena podataka uočljiva.

Pravno dejstvo elektronskih pečata

Član 82

Elektronskom pečatu se kao dokazu u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što je u elektronskom obliku ili zbog toga što ne ispunjava sve uslove za kvalifikovani elektronski pečat.

Za kvalifikovani elektronski pečat podrazumijeva se cjelovitost podataka i tačnost izvora podataka sa kojima je kvalifikovani elektronski pečat povezan.

Elektronski pečat za prekograničnо korišćenje elektronskih pečata

Član 83

Kad se zahtijeva napredni elektronski pečat za korišćenje elektronske usluge koju pruža organ vlasti ili za korišćenje usluge koja se pruža u ime organa vlasti, organ vlasti će priznati napredne elektronske pečate, napredne elektronske pečate koji su zasnovani na kvalifikovanom sertifikatu za elektronski pečat i kvalifikovane elektronske pečate najmanje u formatima ili korišćenjem metoda koje je objavila Evropska komisija.

Kad se zahtijeva napredni elektronski pečat koji je zasnovan na kvafikovanom sertifikatu za korišćenje elektronske usluge koju pruža organ vlasti ili elektronske usluge koja se pruža u ime organa vlasti, organ vlasti će priznati napredne elektronske pečate koji se zasnivaju na kvalifikovanom sertifikatu i kvalifikovane potpise najmanje u formatima ili korišćenjem metoda koje je objavila Evropska komisija.

Za prekogranično korišćenje elektronskih usluga koje pruža organ vlasti ne zahtijeva se elektronski pečat višeg nivoa bezbjednosti od kvalifikovanog elektronskog pečata.

Kvalifikovani sertifikati za elektronske pečate
Član 84

Kvalifikovani sertifikat za elektronske pečate treba da ispunjavaju sljedeće uslove, i to da sadrže:

1) oznaku, najmanje u obliku prikladnom za automatsku obradu, da je sertifikat izdat kao kvalifikovani sertifikat za elektronske pečate;

2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje koji izdaje kvalifikovane sertifikate, uz navođenje oznake države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac usluga povjerenja, i to za:

- pravno lice, odnosno organ vlasti: naziv i, kad je to primjenjivo, matični, odnosno poreski identifikacioni broj,
- fizičko lice: ime i prezime;

3) najmanje naziv autora pečata i, kad je to primjenivo, matični, odnosno poreski identifikacioni broj;

4) podatke za validaciju elektronskog pečata koji odgovaraju podacima za izradu elektronskog pečata;

5) podatke o početku i kraju perioda važenja tog sertifikata;

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

7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga povjerenja koji izdaje sertifikat;

8) lokaciju na kojoj je besplatno dostupan sertifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat iz tačke 7 ovog stava;

9) informacije ili lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog sertifikata;

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

Kvalifikovani sertifikati za elektronske pečate mogu da sadrže i druge podatke koji nijesu obavezni, a da ti podaci ne utiču na interoperabilnost i priznavanje kvalifikovanih elektronskih pečata.

Kvalifikovani sertifikati za elektronske pečate pružaju se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovane sertifikate za elektronske pečate propisuje Ministarstvo.

Shodna primjena
Član 85

Na uslove za kvalifikovana sredstva za izradu elektronskih pečata, sertifikaciju kvalifikovanih sredstava za izradu elektronskih pečata, vođenje i objavljivanje registra kvalifikovanih sredstava za izradu elektronskih pečata, obavještavanje Evropske komisije, kvalifikovanu uslugu za upravljanje kvalifikovanim sredstvima za izradu elektronskog pečata na daljinu, uslove za validaciju kvalifikovanih elektronskih pečata, kvalifikovanu uslugu validacije naprednih elektronskih pečata zasnovanih na kvalifikovanom sertifikatu i kvalifikovanu uslugu čuvanja kvalifikovanih elektronskih pečata, primjenjuju se odredbe čl. 71 do 79 ovog zakona.

Elektronski vremenski pečat i kvalifikovani elektronski vremenski pečat
Član 86

Elektronski vremenski pečat je skup podataka u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određeni vremenom čime se dokazuje da su ti podaci postojali u to vrijeme.

Kvalifikovani elektronski vremenski pečat treba da:

1) povezuje datum i vrijeme sa podacima na način koji isključuje mogućnost neprimjetne promjene podataka koja se ne može otkriti;

2) je zasnovan na preciznom vremenskom izvoru koji je povezan sa preciznim univerzalnim vremenom (UTC); i

3) je potpisan naprednim elektronskim potpisom, odnosno pečatiran naprednim elektronskim pečatom kvalifikovanog davaoca usluga povjerenja ili drugom ekvivalentnom metodom.

Standarde i specifikacije za povezivanje datuma i vremena podataka i za utvrđivanje tačnosti vremenskih pečata propisuje Ministarstvo.

Pravno dejstvo elektronskih vremenskih pečata
Član 87

Elektronskom pečatu se kao dokazu u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što je u elektronskom obliku ili zbog toga što ne ispunjava sve uslove za kvalifikovani elektronski vremenski pečat.

Za kvalifikovani elektronski vremenski pečat podrazumijeva se tačnost datuma i vremena koje označava, kao i integritet podataka sa kojima su povezani datum i vrijeme.

Usluga elektronske preporučene dostave
Član 88

Usluga elektronske preporučene dostave je usluga koja omogućava prenos podataka između trećih lica elektronskim putem i obezbjeđuje dokaze o postupanju sa prenesenim podacima, uključujući dokaz o slanju i prijemu podataka, kao i zaštitu prenijetih podataka od rizika od gubitka, krađe, oštećenja ili drugih neovlašćenih izmjena.

Kvalifikovana usluga elektronske preporučene dostave
Član 89

Kvalifikovana usluga elektronske preporučene dostave treba da ispunjava uslove, i to da:

1) je pruža jedan ili više kvalifikovanih davalaca elektronskih usluga povjerenja;

2) uz visok stepen 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 označavaju kvalifikovanim elektronskim vremenskim pečatom.

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

Davaoci kvalifikovane usluge elektronske preporučene dostave mogu se dogovoriti o interoperabilnosti kvalifikovanih usluga elektronske preporučene dostave koje pružaju, pri čemu moraju biti ispunjeni uslovi iz stava 1 ovog člana.

Usklađenost okvira interoperabilnosti iz stava 3 ovog člana sa zahtjevima iz stava 1 ovog člana potvrđuje tijelo za ocjenjivanje usaglašenosti.

Kvalifikovana usluga elektronske preporučene dostave pruža se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovanu uslugu elektronske preporučene dostave i za interoperabilnost kvalifikovanih usluga elektronske preporučene dostave propisuje Ministarstvo.

Pravno dejstvo usluge preporučene dostave
Član 90

Podacima poslatim i primljenim putem usluge elektronske preporučene dostave ne može se kao dokazu u sudskim postupcima uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što su u elektronskom obliku ili zbog toga što ne ispunjavaju sve uslove za kvalifikovanu uslugu elektronske preporučene dostave.

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

1) integritet 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.

Autentifikacija internet stranica
Član 91

Autentifikacija internet stranica zasniva se na sertifikatu za autentifikaciju internet stranica, odnosno na kvalifikovanom sertifikatu za autentifikaciju internet stranica.

Sertifikat za autentifikaciju internet stranica je elektronska potvrda pomoću koje se može izvršiti autentifikacija internet stranice i kojom se internet stranica povezuje sa fizičkim ili pravnim licem, odnosno organom vlasti kojem je izdat sertifikat.

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

Uslovi za kvalifikovane sertifikate za autentifikaciju internet stranica
Član 92

Kvalifikovani sertifikat za autentifikaciju internet stranice mora da sadrži:

1) oznaku, najmanje u obliku prikladnom za automatsku obradu, da je sertifikat izdat kao kvalifikovani sertifikat za autentifikaciju internet stranice;
2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani sertifikat za autentifikaciju internet stranica, uz navođenje oznake 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 i, kad je to primjenjivo, matični, odnosno poreski identifikacioni broj,
- fizičko lice: ime i prezime;
3) skup identifikacionih podataka o:
- pravnom licu ili organu vlasti kojem je izdat sertifikat: naziv i, gdje je to primjenjivo, matični, odnosno poreski identifikacioni broj i sjedište (minimum naziv grada i države),

- fizičkom licu kome je izdat sertifikat: 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 sertifikat za autentifikaciju internet stranice;

5) podatke o početku i kraju perioda 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 usluga povjerenja koji izdaje sertifikat;

8) lokaciju na kojoj je besplatno dostupan sertifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga povjerenja iz tačke 7 ovog stava;

9) informacije ili lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog sertifikata za autentifikaciju internet stranice.

Kvalifikovani sertifikati za autentifikaciju internet stranica moraju da ispunjavaju odgovarajuće standarde.

Standarde i specifikacije za kvalifikovani sertifikat za autentifikaciju internet stranica propisuje Ministarstvo.

Obaveze pružaoca internet pretraživača
Član 93

Kvalifikovane sertifikate za autentifikaciju internet stranica izdate u skladu sa članom 92 ovog zakona priznaju pružaoci internet pretraživača.

Pružaoci internet pretraživača obezbjeđuju da se podaci o identitetu potvrđeni u sertifikatu za autentifikaciju internet stranice i dodatni potvrđeni atributi prikazuju na način prilagođen korisnicima.

Pružaoci internet pretraživača obezbjeđuju podršku kvalifikovanih sertifikata za autentifikaciju internet stranica, kao i interoperabilnost sa tim sertifikatima, osim mikro i malih preduzeća u skladu sa zakonom kojim se uređuje računovodstvo, i to tokom prvih pet godina njhovog rada kao pružaoca internet pretraživača.

Za kvalifikovane sertifikati za autentifikaciju internet stranica ne smiju se zahtijevati dodatni uslovi, osim uslova iz člana 92 ovog zakona.

Mjere predostrožnosti u pogledu sajber bezbjednosti
Član 94

Pružaoci internet pretraživača ne smiju preduzimati nikakve mjere koje su u suprotnosti sa obavezama iz člana 93 st. 1 do 4 ovog zakona, a posebno u vezi priznavanja kvalifikovanog sertifikata za autentifikaciju internet stranica iz člana 93 stav 1 ovog zakona i prikazivanja dostavljenih podataka o identitetu koji su potvrđeni u sertifikatu na način iz člana 93 stav 2 ovog zakona.

U slučaju da postoje opravdani razlozi u vezi sa narušavanjem bezbjednosti ili gubitkom integriteta sertifikata ili skupa sertifikata, pružaoci internet pretraživača mogu preduzeti mjere predostrožnosti u vezi sa sertifikatom sa stavom 1 ovog člana ili skupom sertifikata.

Ako pružaoci internet pretraživača preduzmu mjere predostrožnosti u skladu sa stavom 2 ovog člana, taj pružalac, bez odlaganja, obavještava Ministarstvo i organ nadležan za sajber bezbjednost u skladu sa zakonom kojim se uređuje informaciona bezbjednost, korisnika kojem je sertifikat izdat i kvalifikovanog davaoca usluga povjerenja koji je izdao taj sertifikat ili skup sertifikata, o svojim aktivnostima, uključujući i mjere predostrožnosti u pogledu sajber bezbjednosti koje je preduzeo.

Nakon prijema obavještenja iz stava 3 ovog člana, organ nadležan za sajber bezbjednost, sprovodi aktivnosti u skladu sa zakonom kojim se uređuje informaciona bezbjednost i o rezultatima sprovedenih aktivnosti obavještava pružaoca internet pretraživača, Ministarstvo i kvalifikovanog davaoca usluga povjerenja koji je izdao sertifikat ili skup sertifikata za autenifikaciju internet stranice.

Ako kvalifikovani davalac usluga povjerenja, na osnovu obavještenja iz stava 4 ovog člana, ne povuče sertifikat ili skup sertifikata za autentifikaciju internet stranice, zavisno od procjene ugroženosti tog sertifikata, o tome organ nadležan za sajber bezbjednost obavještava pružaoca internet pretraživača i nalaže mu da ukine mjere predostrožnosti iz stava 2 ovog člana.

Elektronska potvrda atributa i uslovi za kvalifikovanu elektronsku potvrdu atributa

Član 95

Elektronska potvrda atributa je potvrda u elektronskom obliku kojom se omogućava autentifikacija atributa.

Kvalifikovana elektronska potvrda atributa je potvrda u elektronskom obliku kojom se omogućava potvrđivanje atributa i koja sadrži:

1) oznaku, najmanje u obliku prikladnom za automatsku obradu, da je potvrda izdata kao kvalifikovana elektronska potvrda atributa;

2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovanu elektronsku potvrdu atributa, uz navođenje oznake 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 i, kad je to primjenjivo, matični odnosno poreski identifikacioni broj,
- fizičko lice: ime i prezime;

3) skup identifikacionih podataka koji nedvosmisleno predstavljaju pravno lice, fizičko lice ili organ vlasti na koji se odnose potvrđeni atributi, ili pseudonim koji, ako se koristi, mora biti jasno naznačen;

4) potvrđeni atribut, odnosno potvrđene atribute, uključujući, prema potrebi, informacije potrebne za određivanje onoga što ti atributi obuhvataju;

5) podatke o početku i kraju perioda važenja potvrde atributa;

6) identifikacionu oznaku potvrde atributa koja mora biti jedinstvena za kvalifikovanog davaoca usluga povjerenja i, ako je to primjenjivo, podatak o tome kojem sistemu potvrda pripada ta potvrda atributa;

7) kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat kvalifikovanog davaoca usluga povjerenja koji izdaje tu potvrdu;

8) lokaciju na kojoj je besplatno dostupan sertifikat na kojem se zasniva kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat iz tačke 7 ovog stava;

9) informacije ili lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovane potvrde.

Za kvalifikovanu elektronsku potvrdu atributa ne može se zahtijevati dodatni sadržaj, osim sadržaja iz stava 2 ovog člana.

Elektronska potvrda atributa mora ispunjavati odgovarajuće standarde.

Standarde, specifikacije i procedure za kvalifikovanu elektronsku potvrdu atributa propisuje Ministarstvo.

Pravno dejstvo elektronske potvrde atributa
Član 96

Elektronskoj potvrdi atributa se kao dokazu u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što je u elektronskom obliku ili zbog toga što ne ispunjava sve uslove za kvalifikovanu elektronsku potvrdu atributa.

Kvalifikovana elektronska potvrda atributa i potvrda atributa izdata od strane ili u ime organa vlasti odgovornog za autentični izvor, imaće isto pravno dejstvo kao i potvrde u papirnoj formi, izdate u skladu sa zakonom.

Elektronska potvrda o atributima u elektronskim uslugama Evropske unije
Član 97

Kad se za korišćenje elektronske usluge koju pruža organ vlasti zahtijeva elektronska identifikacija zasnovana na sredstvima za elektronsku identifikaciju i autentifikaciju u skladu sa zakonom, lični identifikacioni podaci u elektronskoj potvrdi atributa ne zamjenjuju elektronsku identifikaciju koja se zasniva na sredstvima elektronske identifikacije i autentifikacije, osim ako država članica Evropske unije to izričito dozvoljava, u kom slučaju se prihvata i kvalifikovana elektronska potvrda atributa iz drugih država članica.

Potvrda atributa koju izdaje nadležni organ druge države članice Evropske unije odgovoran za autentični izvor podataka u toj državi članici ili koja se izdaje u njegovo ime, priznaje se kao potvrda o atributima izdata od strane ili u ime organa vlasti odgovornog za autentični izvor podataka u Crnoj Gori.

Provjera atributa u odnosu na autentične izvore
Član 98

Organi vlasti omogućavaju kvalifikovanim davaocima usluga povjerenja koji izdaju elektronske potvrde atributa da, na zahtjev korisnika, mogu elektronskim putem da provjere autentičnost atributa upoređivanjem sa relevantnim autentičnim izvorom, i to najmanje atribute sa minimalne liste atributa.

Minimalna lista atributa iz stava 1 ovog člana obuhvata sljedeće podatke:

1) adresa;
2) starost;
3) pol;
4) bračni status;
5) sastav porodice;
6) nacionalnost ili državljanstvo;
7) obrazovne kavalifikacije, titule i licence;
8) stručne kvalifikacije, titule i licence;
9) ovlašćenja i mandate za zastupanje fizičkih i pravnih lica;
10) javne dozvole i licence;
11) finansijske i kompanijske podatke za pravna lica.

Bliži način izrade i vođenja minimalne liste atributa iz stava 1 ovog člana, kao i bliži način provjere autentičnosti atributa propisuje Ministarstvo.

Elektronska potvrda atributa izdata od strane ili u ime organa vlasti i uslovi za tu potvrdu
Član 99

Elektronska potvrda atributa izdata od strane ili u ime organa vlasti je elektronsko utvrđivanje atributa izdatih u ime ili od strane organa vlasti koji je odgovoran za autentičan izvor.

Elektronska potvrda atributa iz stava 1 ovog člana mora da sadrži:

1) oznaku, najmanje u obliku prikladnom za automatsku obradu, da je potvrda izdata kao elektronska potvrda atributa koju izdaje organ vlasti odgovoran za autentični izvor ili koja se izdaje u njegovo ime;

2) skup identifikacionih podataka koji nedvosmisleno predstavljaju organ vlasti koji izdaje elektronsku potvrdu atributa, uz navođenje oznake države i naziva organa vlasti i, kad je primjenjivo matičnog broja;

3) skup identifikacionih podataka koji nedvosmisleno predstavljaju pravno lice, fizičko lice ili organ vlasti na koji se odnose potvrđeni atributi ili pseudonim koji, ako se koristi, mora biti jasno naznačen;

4) potvrđeni atribut, odnosno povrđene atribute, uključujući, gdje je to primjenjivo, informacije neophodne za određivanje onoga što ti atributi obuhvataju;

5) podatke o početku i kraju perioda važenja potvrde;

6) identifikacionu oznaku potvrde, koja je jedinstvena za organ vlasti koji izdaje elektronsku potvrdu atributa i, gdje je to primjenjivo, podatak o tome kojem sistemu potvrda pripada ta potvrda atributa;

7) kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat organa vlasti koji izdaje elektronsku potvrdu atributa;

8) lokaciju na kojoj je besplatno dostupan sertifikat koji podržava elektronski potpis ili elektronski pečat iz tačke 7 ovog stava;

9) informacije ili lokaciju usluga koje se mogu koristiti za ispitivanje validnosti potvrde.

Kvalifikovani sertifikat na kojem se zasniva kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat organa vlasti odgovornog za autentičan izvor sadrži skup sertifikovanih atributa u obliku pogodnom za automatsku obradu u kojem se:

- ukazuje na to da je organ vlasti koji izdaje potvrdu u skladu sa zakonom odgovoran za autentični izvor, na osnovu kojeg je izdata elektronska potvrda atributa ili od onoga koji je ovlašćen da izdaje tu potvrdu u ime organa vlasti;
- pruža skup podataka koji nedvosmisleno predstavljaju autentični izvor;
- prepoznaje zakon iz alineje 1 ovog stava.

Organ vlasti koji izdaje elektronske potvrde atributa treba da, u pogledu pouzdanosti i povjerenja, ispunjava nivo koji je jednak kvalifikovanom davaocu usluga povjerenja u skladu sa čl. 53 i 54 ovog zakona.

Organ vlasti obavještava Ministarstvo o ispunjenosti uslove iz čl. 53 i 54 ovog zakona i dostavlja izvještaj koji izdaje tijelo za ocjenu usaglašenosti.

Ministarstvo, na osnovu dostavljenog obavještenja i izvještaja iz stava 5 ovog člana, vodi Listu organa vlasti koji izdaju elektronske potvrde atributa.

Lista iz stava 6 ovog člana vodi se u elektronskom obliku pogodnom za automatsku obradu i objavljuje na internet stranici Ministarstva, putem bezbjednog kanala.

Lista iz stava 6 ovog člana potpisuje se naprednim elektronskim potpisom, odnosno pečatira naprednim elektronskim pečatom.

Ako je elektronska potvrda atributa izdata od organa vlasti koji je odgovoran za autentični izvor ili od onoga koji je ovlašćen da izdaje tu potvrdu u ime organa vlasti, opozvana nakon početnog izdavanja, ta potvrda gubi validnost od trenutka opoziva, bez mogućnosti da opet dobije status validnosti.

Organi javne vlasti koji izdaju elektronske potvrde atributa treba da obezbijede interfejs sa evropskim novčanicima digitalnog identiteta, koji su obezbijeđeni u skladu sa članom 12 ovog zakona.

Specifikacije za elektronske potvrde atributa iz stava 1 ovog člana, propisuje Ministarstvo.

Izdavanje elektronske potvrde atributa za novčanike digitalnog identiteta
Član 100

Davaoci elektronskih potvrda atributa koji izdaju elektronske potvrde atributa moraju da korisnicima novčanika digitalnog identiteta pruže mogućnost da zatraže, nabave, čuvaju i upravljaju elektronskom potvrdom atributa.

Davaoci elektronskih potvrda atributa koji izdaju kvalifikovane elektronske potvrde atributa moraju da obezbijede interfejs sa novčanicima digitalnog identiteta, koji su obezbijeđeni u skladu sa članom 12 ovog zakona.

Dodatna pravila za elektronske potvrde atributa
Član 101

Davaoci usluga povjerenja koji izdaju elektronske potvrde atributa i kvalifikovane elektronske potvrda atribuda ne smiju da kombinuju lične podatke koji se odnose na pružanje tih usluga sa ličnim podacima iz bilo kojih drugih usluga koje pružaju oni ili njihovi komercijalni partneri.

Lični podaci povezani sa pružanjem usluga izdavanja elektronskih potvrda atributa moraju se čuvati logički odvojeno od drugih podataka koje posjeduje davalac elektronske potvrde atributa.

Davaoci usluga povjerenja koji izdaju kvalifikovane elektronske potvrde atributa treba da organizuju pružanje takvih kvalifikovanih usluga povjerenja na način koji je funkcionalno odvojen od drugih usluga koje pružaju.

Elektronsko arhiviranje i kvalifikovano elektronsko arhiviranje
Član 102

Elektronsko arhiviranje je usluga kojom se obezbjeđuje prijem, čuvanje, preuzimanje i brisanje elektronskih podataka i elektronskih dokumenata, kako bi se obezbijedila njihova trajnost i čitljivost, kao i očuvanje njhovog integriteta, povjerljivosti i dokaza o porijeklu tokom perioda čuvanja.

Kvalifikovana usluga elektronskog arhiviranja je usluga elektronskog arhiviranja koju pruža kvalifikovani davalac usluga povjerenja i koja ispunjava uslove iz člana 104 ovog zakona.

Pravno dejstvo elektronskog arhiviranja
Član 103

Elektronskim podacima i elektronskim dokumentima koji se čuvaju uz pomoć usluge elektronskog arhiviranja se u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što su u elektronskom obliku ili zbog toga što nijesu sačuvani upotrebom kvalifikovane usluge elektronskog arhiviranja.

Za elektronske podatke i elektronske dokumente sačuvane pomoću kvalifikovane usluge elektronskog arhiviranja podrazumijeva se njihov integritet i tačnost porijekla, tokom trajanja perioda čuvanja od strane kvalifikovanog davaoca usluga povjerenja.

Uslovi za kvalifikovano elektronsko arhiviranje
Član 104

Kvalifikovana usluga elektronskog arhiviranja mora da ispunjava sljedeće uslove, i to da:

1) je pružaju kvalifikovani davaoci usluga povjerenja;

2) kvalifikovani davaoci usluga povjerenja koriste procedure i tehnologije koje obezbjeđuju trajnost i čitljivost elektronskih podataka i elektronskih dokumenata van perioda tehnološke validnosti i najmanje tokom zakonskog ili ugovornog perioda čuvanja, uz održavanje integriteta i tačnosti njihovog porijekla;

3) kvalifikovani davaoci usluga povjerenja obezbjeđuju da se ti elektronski podaci i elektronski dokumenti čuvaju na takav način, da budu zaštićeni od gubitka i promjena, osim promjena u njihovom medijumu ili elektronskom formatu;

4) kvalifikovani davaoci usluga povjerenja obezbjeđuju ovlašćenim pouzdajućim stranama da dobiju izvještaj na automatizovan način, koji potvrđuje da elektronski podaci i elektronski dokumenti, preuzeti iz kvalifikovane elektronske arhive, podrazumijevaju integritet od početka perioda čuvanja do trenutka preuzimanja.

Izvještaj iz stava 1 tačka 4 ovog člana, treba da bude dostavljen na pouzdan i efikasan način i da je potpisan kvalifikovanim elektronskim potpisom, odnosno pečatiran kvalifikovanim elektronskim pečatom davaoca usluga povjerenja koji pruža kvalifikovanu usluge elektronskog arhiviranja**.**

Kvalifikovana usluga elektronskog arhiviranja pruža se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovanu uslugu elektronskog arhiviranja propisuje Ministarstvo.

Elektronska evidencija i kvalifikovana elektronska evidencija
Član 105

Elektronska evidencija podrazumijeva niz elektronskih zapisa podataka kojima se obezbjeđuje integritet i tačnost hronološkog redosleda tih zapisa.

Kvalifikovana elektronska evidencija je elektronska evidencija koju pruža kvalifikovani davalac usluga povjerenja i koja ispunjava uslove iz člana 107 ovog zakona.

Pravno dejstvo elektronskih evidencija
Član 106

Elektronskoj evidenciji se u sudskim postupcima ne može uskratiti pravno dejstvo i prihvatljivost, samo zbog toga što je u elektronskom obliku ili zbog toga što ne ispunjava uslove za kvalifikovanu elektronsku evidenciju.

Za zapise podataka koji su sadržani u kvalifikovanoj elektronskoj evidenciji podrazumijeva se njihov jedinstven i tačan sekvencijalni hronološki redosljed, kao i njihov integritet.

Uslovi za kvalifikovane elektronske evidencije
Član 107

Kvalifikovane elektronske evidencije moraju da ispunjavaju sljedeće uslove, i to da:

1) ih pruža jedan ili više kvalifikovanih davalaca usluga povjerenja;
2) utvrđuju porijeklo zapisa u evidenciji;
3) obezbjeđuju jedinstveni sekvencijalni hronološki redosljed zapisa podataka u evidenciji;
4) se u elektronskim evidencijama bilježe podaci na takav način da je svaka naknadna promjena podataka odmah uočljiva, čime se obezbjeđuje njihov integritet tokom vremena.

Kvalifikovana elektronska evidencija pruža se u skladu sa odgovarajućim standardima.

Standarde i specifikacije za kvalifikovane elektronske evidencije propisuje Ministarstvo.

IV. JEDINSTVENA KONTAKT TAČKA, PRIKUPLJANJE PODATAKA I POMOĆ ORGANA DRUGIH DRŽAVA ČLANICA EVROPSKE UNIJE

Jedinstvena kontakt tačka
Član 108

Ministarstvo predstavlja jedinstvenu kontakt tačku za usluge povjerenja, novčanik digitalnog identiteta, evropski novčanik digitalnog identiteta i prijavljene sisteme elektronske identifikacije i sarađuje sa jedinstvenim kontakt tačkama drugih država članica Evropske unije.

Prikupljanje statističkih podataka radi izvještavanja Evropske komisije
Član 109

Ministarstvo, za potrebe izvještavanja Evropske komisije prikuplja sve potrebne statističke podatke od davalaca usluga povjerenja, davalaca novčanika digitalnog identiteta i davalaca elektronske identifikacije, u skladu sa Regulativom eIDAS.

Pomoć organa drugih država članica Evropske unije
Član 110

U cilju olakšavanja vršenja nadzora nad sprovođenjem ovog zakona, kao i izvršavanju obaveza propisanih ovim zakonom, Ministarstvo može da zatraži pomoć od organa druge države članice Evropske unije nadležnog za nadzor, u kojoj je osnovan davalac evropskog novčanika digitalnog identiteta ili davalac usluga povjerenja ili gdje se nalaze sistemi elektronske identifikacije ili mrežni i informacioni sistemi ili gdje se pružaju usluge povjerenja.

V. NADZOR

Nadzor nad sprovođenjem zakona
Član 111

Nadzor nad sprovođenjem ovog zakona vrši Ministarstvo.

Inspekcijski nadzor
Član 112

Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja, davalaca novčanika digitalnog identiteta i davalaca elektronske identifikacije vrši Ministarstvo preko inspektora za informaciono društvo, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.

Prilikom vršenja nadzora iz stava 1 ovog člana inspektor je ovlašćen da:

1) kontroliše rad tih davalaca i ispunjenost uslova propisanih ovim zakonom;
2) u slučaju prijema obavještenja da rad tog davaoca nije u skladu sa ovim zakonom, preduzme mjere i sprovodi dodatne aktivnosti u skladu sa zakonom;
3) zahtijeva od davaoca da otkloni utvrđene nepravilnosti u ostavljenom roku;
4) daje predlog Ministarstvu za:
   - opoziv statusa davaoca usluga povjerenja ili status usluge povjerenja koju on pruža,
   - suspenziju ili poništavanje statusa pouzdajuće strane, u slučaju upotrebe novčanika digitalnog identiteta na nezakonit način,
   - opoziv statusa davaoca elektronske identifikacije i davaoca novčanika digitalnog identiteta.

Inspektor je dužan da Ministarstvu dostavi, do 1. marta tekuće za prethodnu kalendarsku godinu, detaljan izvještaj o izvršenom nadzoru i preduzetim aktivnostima iz svoje nadležnosti.

VI. KAZNENE ODREDBE

Član 113

Novčanom kaznom u iznosu od 500 do 40.000 eura kazniće se za prekršaj pravno lice, ako:

1) ne obezbijedi korisnicima da mogu lako da zatraže tehničku podršku i prijave tehničke probleme ili incidente koji imaju negativan uticaj na upotrebu novčanika digitalnog identiteta (član 16 stav 1);

2) ne izdaje, ne upotrebljava i ne opoziva besplatno novčanik digitalnog identiteta za fizička lica (član 16 stav 3);

3) ne omogući korisniku da ima punu kontrolu nad upotrebom novčanika digitalnog identiteta, kao i nad podacima koji se nalaze u tom novčaniku (član 16 stav 4);

4) prikuplja informacije o upotrebi novčanika digitalnog identiteta koje nijesu neophodne za pružanje usluga novčanika digitalnog identiteta, kombinuje lične identifikacione podatke ili bilo koje druge lične podatke, koji se čuvaju ili odnose na korišćenje novčanika digitalnog identiteta, sa ličnim podacima iz bilo koje druge usluge koju pruža taj davalac ili usluga trećih strana koje nijesu neophodne za pružanje usluga novčanika digitalnog identiteta, osim ako korisnik to izričito zatraži (član 16 stav 5);

5) ne čuva lične podatke koji su povezani sa digitalnim novčanikom logički odvojeno od svih drugih podataka koje posjeduje davalac novčanika digitalnog identiteta (član 16 stav 6);

6) fizičkim i pravnim licima koja ne koriste novčanik digitalnog identiteta ograniči ili otežа korišćenje elektronskih usluga, pristup tržištu rada i slobodi poslovanja (član 17 stav 2);

7) ne obavijesti Ministarstvo, bez odlaganja, u slučaju namjere prestanka izdavanja novčanika digitalnog identiteta, kao i promjene informacija iz člana 26 stav 2 ovog zakona (član 27 stav 1);

8) ne obavijesti Ministarstvo, bez odlaganja kad se desi povreda ili djelimična kompromitacija novčanika digitalnog identiteta, sistema validacije iz člana 14 ovog zakona, odnosno sistema elektronske identifikacije u okviru kojeg je taj novčanik obezbijeđen, na način koji utiče na njegovu pouzdanost, ili pouzdanost drugih novčanika digitalnog identiteta davalac novčanika digitalnog identiteta (član 28 stav 1);

9) ne suspenduje autentifikaciju i bez odlaganja o tome ne obavijesti Ministarstvo, kad se za sistem elektronske identifikacije koji je upisan u registar u skladu sa članom 37 ovog zakona, odnosno autentifikacije iz člana 36 stav 1 tačka 4 ovog zakona, utvrdi da je došlo do povrede ili djelimične kompromitacije na način koji utiče na pouzdanost autentifikacije tog sistema, davalac elektronske identifikacije (član 39 stav 1);

10) ne provjeri identitet prilikom izdavanja kvalifikovanog sertifikata ili kvalifikovane elektronske potvrde atributa i, ako je primjenjivo, bilo koje specifične atribute fizičkog ili pravnog lica, odnosno organa vlasti, kome treba da se izda kvalifikovani sertifikat ili kvalifikovana elektronska potvrda atributa (član 53 stav 1 tačka 1);

11) 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 i odgovarajućih sigurnosnih procedura za pružanje kvalifikovanih usluga povjerenja, zaštitu podataka o ličnosti (član 53 stav 1 tačka 2);

12) ne posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu pružanjem kvalifikovanih usluga povjerenja, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih usluga povjerenja koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete (član 53 stav 1 tačka 3);

13) ne informiše svako lice koje želi da koristi kvalifikovanu uslugu povjerenja, na jasan, sveobuhvatan i lako dostupan način, na javno dostupnom prostoru, o preciznim uslovima korišćenja te usluge, uključujući sva ograničenja u pogledu njenog korišćenja (član 53 stav 1 tačka 4);

14) ne koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku bezbjednost i pouzdanost procesa, koje ti sistemi podržavaju, uključujući korišćenje kriptografskih tehnika (član 53 stav 1 tačka 5);

15) ne koristi pouzdane sisteme za čuvanje podataka koji su mu dati, u provjerljivom obliku, tako da: oni budu javno dostupni za preuzimanje samo kad je pribavljena saglasnost osobe

na koju se podaci odnose, samo ovlašćena lica mogu da unose i mijenjaju sačuvane podatke, se može provjeriti autentičnost podataka (član 53 stav 1 tačka 6);

16) nema odgovarajuće politike i ne preduzima odgovarajuće mjere za upravljanje pravnim, poslovnim, operativnim i drugim direktnim ili indirektnim rizicima za pružanje kvalifikovanih usluga povjerenja koje, bez obzira na mjere informacione bezbjednosti, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, uključuju najmanje mjere koje se odnose na: postupke registracije i uključivanja za usluge povjerenja, proceduralne ili administrativne provjere potrebne za pružanje usluga povjerenja, upravljanje i sprovođenje usluga povjerenja (član 53 stav 1 tačka 7);

17) ne preduzima odgovarajuće mjere protiv falsifikovanja, krađe ili zloupotrebe podataka, ili neovlašćenog brisanja, izmjene ili onemogućavanje pristupa podacima (član 53 stav 1 tačka 8);

18) ne evidentira i ne čini dostupnim onoliko dugo koliko je to potrebno, nakon prestanka obavljanja poslova kvalifikovanog davaoca usluga povjerenja, sve bitne informacije povezane s podacima koje je pružio i primio kao kvalifikovani davalac usluga povjerenja, za potrebe pružanja dokaza u pravnim postupcima i u svrhu obezbjeđivanja pružanja usluge u kontinuitetu (član 53 stav 1 tačka 9);

19) nema ažuriran plan prekida pružanja kvalifikovane usluge povjerenja radi obezbjeđivanja njenog kontinuiteta (član 53 stav 1 tačka 10);

20) ne uspostavi i ne ažurira bazu podataka izdatih sertifikata, za kvalifikovane davaoce usluga povjerenja koji izdaju kvalifikovane sertifikate (član 53 stav 1 tačka 11);

21) podatke i dokumenta koja se nalaze u informacionom sistemu skladišti na informaciono-komunikacionoj infrastrukturi van Crne Gore, ako posebnim zakonom ili potvrđenim međunarodnim ugovorom nije drukčije utvrđeno (član 53 stav 1 tačka 13);

22) ne obavijesti Ministarstvo najmanje mjesec dana prije sprovođenja bilo kakve promjene u pružanju kvalifikovanih usluga povjerenja, ili najmanje tri mjeseca, u slučaju namjere da se pružanje tih usluga prekine (član 54 stav 1);

23) ne obavijesti Ministarstvo, ugrožene korisnike koje je moguće identifikovati, druge nadležne organe kad je to moguće i na zahtjev Ministarstva javnost, ako je to od javnog interesa, o bilo kakvim kršenjima bezbjednosti ili prekidima u pružanju kvalifikovane usluge povjerenja ili sprovođenju mjera iz člana 53 stav 1 tačka 7 ovog zakona, koje imaju značajan uticaj na pružanje te usluge, bez odlaganja, a najkasnije 24 sata (član 54 stav 2);

24) ne dostavi Ministarstvu podatke o broju sertifikata izdatih od početka izdavanja, odnosno broju pruženih usluga povjerenja, kao i po potrebi druge informacije, na zahtjev Ministarstva (član 54 stav 5);

25) ne izvrši opoziv sertifikata kad to zahtijeva potpisnik, odnosno autor elektronskog pečata ili njegov ovlašćeni zastupnik (član 55 stav 1 tačka 1);

26) ne izvrši opoziv sertifikata kad utvrdi da je podatak u sertifikatu pogrešan ili je sertifikat izdat na osnovu pogrešnih podataka (član 55 stav 1 tačka 2);

27) ne izvrši opoziv sertifikata kad primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice, ili organ vlasti, 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 55 stav 1 tačka 3);

28) ne izvrši opoziv sertifikata kad utvrdi da su podaci za izradu elektronskog potpisa, elektronskog pečata, autentifikaciju internet stranice 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 55 stav 1 tačka 4);

29) ne izvrši opoziv sertifikata kad utvrdi da su podaci za provjeru elektronskog potpisa elektronskog pečata, autentifikaciju internet stranice ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost sertifikata (član 55 stav 1 tačka 5);

30) 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 prenese na drugog davaoca tih usluga (član 55 stav 1 tačka 6);

31) ne izvrši opoziv sertifikata kad primi sudsku odluku ili upravni akt koji se odnose na važenje sertifikata (član 55 stav 1 tačka 7);

32) ne izvrši opoziv sertifikata ako postoje drugi opravdani razlozi (član 55 stav 1 tačka 8);

33) u roku od 24 sata od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti iz člana 55 stav 1 ovog člana, ne izvrši opoziv sertifikata (član 55 stav 2);

34) ne objavi status opozvanih sertifikata na svojoj internet stranici (član 55 stav 3);

35) jasno ne naznači period suspenzije iz člana 55 stav 5 ovog člana u bazi podataka iz člana 53 stav 1 tačka 11 ovog zakona i ne učini vidljivim status suspenzije za pouzdajuće strane tokom perioda suspenzija (član 55 stav 6);

36) datum i vrijeme suspenzije i opoziva sertifikata nijesu unijeti u bazu podataka iz člana 53 stav 1 tačka 11 ovog zakona (član 55 stav 8);

37) ne pruži informacije o validnosti ili opozivu pojedinog sertifikata u svakom trenutku i nakon roka važenja, na automatizovan način koji je pouzdan, besplatan i efikasan (član 55 stav 9);

38) opoziv kvalifikovanih elektronskih potvrda atributa ne vrši na način iz člana 55 st. 2, 3 i 9 ovog člana (član 55 stav 10);

39) ne obavijesti Ministarstvo, bez odlaganja o isteku vremena na koji je izdat setifikat iz člana 73 stav 4 ovog zakona kao i o njegovom opozivu, odnosno produžetku važenja (član 73 stav 7);

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 4.000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu vlasti novčanom kaznom u iznosu od 30 eura do 4.000 eura.

Član 114

Novčanom kaznom u iznosu od 500 eura do 10.000 eura kazniće se za prekršaj pravno lice ako:

1) fizičkim i pravnim licima koja ne koriste novčanik digitalnog identiteta ne omogući pristup elektronskim uslugama putem drugih postojećih sredstava identifikacije i autentifikacije (član 17 stav 3);

2) ne obavještava Ministarstvo o promjeni podataka iz člana 20 stav 2 ovog zakona, bez odlaganja (član 22);

3) nema odgovarajuće politike i ne preduzima odgovarajuće mjere za upravljanje pravnim, poslovnim, operativnim i drugim direktnim ili indirektnim rizicima za pružanje nekvalifikovanih usluga povjerenja koje, bez obzira na mjere informacione bezbjednosti, koje su propisane u skladu sa zakonom kojim se uređuje informaciona bezbjednost, uključuju najmanje mjere koje se odnose na: procedure registracije i uključivanja za pružanje usluga povjerenja, proceduralne ili administrativne provjere potrebne za pružanje usluga povjerenja i upravljanje i sprovođenje usluga povjerenja (član 50 stav 1 tačka 1);

4) ne obavještava Ministarstvo, ugrožene korisnike koje je moguće identifikovati, javnost ako je to od javnog interesa i, ako je to primjenjivo, druga relevantna nadležna tijela, o bilo kakvom narušavanju bezbjednosti ili poremećajima u pružanju usluga, ili u sprovođenju mjera iz člana 50 stav tačka 1 ovog zakona, koji imaju značajan uticaj na pruženu uslugu povjerenja ili na lične podatke koji se u njoj čuvaju, bez nepotrebnog odlaganja, a najkasnije 24 sata od saznanja o bilo kakvom narušavanju bezbjednosti ili poremećaju (član 50 stav 1 tačka 2);

5) o promjenama u pružanju usluga povjerenja ne obavijesti Ministarstvo, podnošenjem prijave (član 51 stav 3);

6) odbije prijem elektronskog dokumenta sa elektronskim potpisom ili naprednim elektronskim potpisom, samo zato što je u elektronskom obliku (član 67 stav 2);

7) bez odlaganja, a najkasnije u roku od sedam dana, ne obavijesti Ministarstvo o izvršenoj sertifikaciji iz člana 73 ovog zakona, o poništavanju sertifikata iz člana 73 stav 4 ovog zakona, odnosno o drugoj nastaloj promjeni (član 74 stav 5);

8) podnosilac zahtjeva za upis u Registar iz člana 74 stav 1 ovog zakona, ne obavijesti Ministarstvo, bez odlaganja, a najkasnije u roku od 30 dana nakon opoziva, da je kvalifikovano sredstvo za izradu elektronskog potpisa koje je objavljeno na Listi iz člana 74 stav 3 ovog zakona, opozvano (član 74 stav 6);

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 30 eura do 4.000 eura.

Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu vlasti novčanom kaznom u iznosu od 30 eura do 4.000 eura.

VII. PRELAZNE I ZAVRŠNE ODREDBE

Rok za donošenje podzakonskih akata
Član 115

Podzakonski akti za sprovođenje ovog zakona donijeće se u roku od 18 mjeseci od dana stupanja na snagu ovog zakona.

Do donošenja podzakonskih akata iz stava 1 ovog člana primjenjivaće se podzakonski akti donijeti na osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG“, br. 31/17 i 72/19).

Važenje sertifikata izdatih po ranijem zakonu
Član 116

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 sertifikata.

Obaveza usklađivanja poslovanja
Član 117

Davaoci usluga povjerenja i davaoci elektronske identifikacije dužni su da u roku od 24 mjeseca od dana donošenja podzakonskih akata iz člana 115 ovog zakona usklade svoje poslovanje sa odredbama ovog zakona i dostave Ministarstvu izvještaj tijela o ocjenjivanju usaglašenosti o ispunjenosti tih uslova.

Ocjenjivanje usaglašenosti do akreditacije prvog tijela za ocjenjivanje usaglašenosti
Član 118

Do akreditacije prvog tijela za ocjenjivanje usaglašenosti u skladu sa zakonom, ocjenjivanje usaglašenosti u skladu sa ovim zakonom vrši akreditaciono tijelo sa Liste akreditacionih tijela koju vodi i javno objavljuje Evropska komisija, u skladu sa Regulativom eIDAS.

Uspostavljanje novčanika digitalnog identiteta
Član 119

Novčanik digitalnog identiteta Ministarstvo je dužno da uspostavi u roku od 18 mjeseci od dana donošenja podzakonskih akata iz člana 115 ovog zakona.

Odložena primjena pojedinih odredbi

Član 120

Odredbe čl. 7 i 29, člana 30 st. 1, 2 i 3, čl. 31, 32 i 33, čl. 41 i 42, člana 44 stav 1, čl. 45 do 49, člana 56 stav 6, člana 61, člana 63 stav 1 i čl. 64, 69, 75, 83, 97, 108, 109 i 110 ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

Prestanak primjene pojedinih odredbi

Član 121

Odredba člana 53 stav 1 tač. 12 i 13 ovog zakona primjenjivaće se do dana pristupanja Crne Gore Evropskoj uniji.

Prestanak važenja

Član 122

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG“, br. 31/17 i 72/19).

Stupanje na snagu

Član 123

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

---

* Ovaj zakon usklađen je sa Regulativom (EU) br. 910/2014 Evropskog parlamenta i Savjeta od 23. jula 2014. godine, o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC i Regulativom (EU) 2024/1183 Evropskog parlamenta i Savjeta od 11. aprila 2024. godine, o izmjeni Regulative (EU) br. 910/2024 u pogledu uspostavljanja evropskog okvira za digitalni identitet