CRNA GORA
SKUPŠTINA CRNE GORE

PRIMLJENO:	14. 11	20 19 GOD.
KLASIFIKACIONI BROJ:	10-2/19-2	
VEZA:		
EPA:	856 XXVI	
SKRAĆENICA:		PRILOG:

Crna Gora
VLADA CRNE GORE
Broj: 07-5821
Podgorica, 11. novembra 2019. godine

PREDSJEDNIKU SKUPŠTINE CRNE GORE

PODGORICA

Vlada Crne Gore, na sjednici od 31. oktobra 2019. godine, utvrdila je **PREDLOG ZAKONA O IZMJENAMA I DOPUNAMA ZAKONA O ELEKTRONSKOJ IDENTIFIKACIJI I ELEKTRONSKOM POTPISU**, koji Vam u prilogu dostavljamo radi stavljanja u proceduru Skupštine Crne Gore.

Za predstavnike Vlade koji će učestvovati u radu Skupštine i njenih radnih tijela, prilikom razmatranja Predloga ovog zakona, određeni su SUZANA PRIBILOVIĆ, ministarka javne uprave i DUŠAN POLOVIĆ, generalni direktor Direktorata za elektronsku upravu i informatičku bezbjednost u Ministarstvu javne uprave.

PREDSJEDNIK
Duško Marković, s. r.

PREDLOG

ZAKON

O IZMJENAMA I DOPUNAMA ZAKONA O ELEKTRONSKOJ IDENTIFIKACIJI I ELEKTRONSKOM POTPISU

Član 1

U Zakonu o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG", broj 31/17) član 2 mijenja se i glasi:

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

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

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

Član 2

Član 3 mijenja se i glasi:

„Elektronske usluge povjerenja

Član 3

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

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

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

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

Član 3

Član 4 mijenja se i glasi:

„Davaoci elektronske usluge povjerenja

Član 4

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

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

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

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

Član 4

Član 5 mijenja se i glasi:

„Dostupnost elektronskih usluga povjerenja licima sa invaliditetom

Član 5

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

Član 5

U članu 8 stav 1 tač. 1, 3, 4, 6, 8 i 9 mijenjaju se i glase:

„1) **identifikacioni podaci** obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog lica, pravnog lica ili organa vlasti;

3) **korisnik** je fizičko, pravno lice ili organ vlasti koje se oslanja na elektronsku identifikaciju ili elektronsku uslugu povjerenja;

4) **potpisnik** je fizičko lice koje se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica korišćenjem podataka za izradu elektronskog potpisa;

6) **autor elektronskog pečata** je pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata;

8) **certifikat za elektronski pečat** je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili organom vlasti i potvrđuje naziv tog pravnog lica ili organa vlasti;

9) **kvalifikovani certifikat za elektronski pečat** je certifikat za elektronski pečat koji izdaje kvalifikovani davalac elektronske usluge povjerenja;".

Član 6

U članu 15, članu 20 st. 1 i 2, članu 23 stav 1 tačka 2 i stav 3, članu 24 stav 1, članu 26 stav 2 tačka 3, članu 31 stav 1 tač. 1 i 4 i stav 2, član 32 stav 3, nazivu poglavlja V, članu 36, nazivu i članu 37, čl. 41, 42 i 43, nazivu poglavlja VII, nazivu i članu 45, članu 47 stav 1, članu 50 stav 1, članu 52 stav 1, nazivu i članu 53, članu 54, članu 55 stav 1, članu 56, članu 57 st. 1, 3, 4 i 5, članu 58 st. 1, 2, 3, 5 i 6, članu 63 stav 1, članu 72 stav 1 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.

Član 7

Član 16 mijenja se i glasi:

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

1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis u obliku prikladnom za automatsku obradu podataka;

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

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

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

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

5) podatke o periodu važenja tog certifikata;

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

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

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

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

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

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

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

Način određivanja identifikacionog broja uređuje Vlada."

Član 8

U članu 18 stav 2 briše se.

Član 9

Član 27 mijenja se i glasi:

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

Član 10

U članu 29 riječi: "Organ vlasti, odnosno pravno lice" zamjenjuju se riječima: „Fizičko lice, pravno lice, odnosno organ vlasti".

Član 11

Član 33 mijenja se i glasi:

„Kvalifikovani certifikati za autentifikaciju internet stranice
Član 33

Kvalifikovani certifikat za autentifikaciju internet stranice mora da sadrži:

1) oznaku da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranice u elektronskom obliku pogodnom za automatsku obradu;

2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za autentifikaciju internet stranice, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za:

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

3) skup identifikacionih podataka o:

- pravnom licu ili organu vlasti kojem je izdat certifikat: naziv, matični, odnosno poreski identifikacioni broj i sjedište (minimum naziv grada i države),
- fizičkom licu kome je izdat certifikat: ime i prezime ili pseudonim koji, ako se koristi, mora biti jasno naznačen i adresu (minimum naziv grada i države);

4) naziv jednog ili više domena kojim upravlja fizičko lice, pravno lice ili organ vlasti kojem je izdat certifikat za autentifikaciju internet stranice;

5) podatke o periodu važenja kvalifikovanog certifikata za autentifikaciju internet stranice;

6) identifikacionu oznaku izdatog kvalifikovanog certifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca elektronske usluge povjerenja;

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

8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja;

9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za autentifikaciju internet stranice."

Član 12

Član 34 mijenja se i glasi:

„Uslovi u vezi sa kvalifikovanim davaocima elektronske usluge povjerenja

Član 34

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

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

2) obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti;

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

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

5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa;

6) preduzima mjere za sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja certifikate potpisnicima na bezbjedan način;

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

8) posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz

evidencije kvalifikovanih certifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa;

9) koristi pouzdan sistem čuvanja kvalifikovanih certifikata u obliku koji omogućava provjeru, kako bi:

- unos i promjene podataka prilikom pružanja elektronske usluge povjerenja vršila samo ovlašćena lica,
- mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata,
- podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje,
- bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve, bila vidljiva kvalifikovanom davaocu elektronske usluge povjerenja.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo."

Član 13

Član 35 mijenja se i glasi:

„Vršenje kvalifikovanih elektronskih usluga povjerenja za organe vlasti

Član 35

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

Ispunjenost uslova iz stava 1 ovog člana utvrđuje Ministarstvo.

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

Član 14

U članu 38 st. 1 i 2 riječi: „usluge certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske usluge povjerenja".

Stav 3 briše se.

Dosadašnji st. 4 i 5 postaju st. 3 i 4.

Član 15

Član 39 mijenja se i glasi:

„Rješenje o ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja

Član 39

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

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

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

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

Član 16

U članu 40 st. 2 i 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.

Stav 4 briše se.

U stavu 5 poslije riječi „obradu" dodaje se riječ „podataka".

Dosadašnji st. 5 do 8 postaju st. 4 do 7.

Član 17

Članu 44 mijenja se i glasi:

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

Član 18

U nazivu člana 49 i uvodnoj rečenici stava 1 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.

U stavu 1 tač. 2 i 3 mijenjaju se i glase:

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

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

Poslije stava 1 dodaju se tri nova stava koji glase:

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

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

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

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

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

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

U stavu 2 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja".

Dosadašnji stav 2 postaje stav 5.

Član 19

U članu 51 u uvodnoj rečenici stava 1 i u tački 5 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja", a u tački 6 riječi: „usluge certifikovanja" zamjenjuju se riječima: „elektronske usluge povjerenja".

Stav 2 mijenja se i glasi:

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

U stavu 3 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja".

St. 4 i 5 mijenjaju se i glase:

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

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

Član 20

Član 59 mijenja se i glasi:

„Upravljanje sistemom elektronske identifikacije

Član 59

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

Član 21

U članu 60 stav 1 mijenja se i glasi:

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

U stavu 2 riječi: „elektronske tranakcije" zamjenjuju se riječima: „sredstva elektronske identifikacije".

Član 22

Poslije člana 60 dodaju se dva nova člana koji glase:

„Uslovi u vezi sa sistemom za elektronsku identifikaciju

Član 60a

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

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

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

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

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

Ispunjenost uslova iz stava 1 ovog člana utvrđuje Ministarstvo.

„Registar sistema elektronske identifikacije

Član 60b

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

Registar sistema elektronske identifikacije sadrži:

1) opis sistema elektronske identifikacije,

2) stepen sigurnosti sistema elektronske identifikacije i sredstava elektronske identifikacije koji se izdaju u okviru tog sistema,

3) podatke o fizičkom licu, pravnom licu, odnosno organu vlasti koji upravljaju sistemom elektronske identifikacije i to za:

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

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

Registar sistema elektronske identifikacije vodi Ministarstvo.

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

Registar potpisuje Ministarstvo naprednim elektronskim potpisom."

Član 23

Član 61 mijenja se i glasi:

„Interoperabilnost
Član 61

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

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

Čvor uspostavlja i njime upravlja Ministarstvo.

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

Član 24

U članu 62 stav 1 tačka 1 riječi: „evidenciju i registar" zamjenjuju se riječima „registar sistema elektronske identifikacije".

Član 25

U članu 64 stav 1 tačka 1 mijenja se i glasi:

„1) opis sistema elektronske identifikacije i njegove stepene sigurnosti, podatke o fizičkom i pravnom licu, odnosno organu vlasti iz člana 4 st. 3 i 4 ovog zakona koji izdaje sredstva elektronske identifikacije;"

U tač. 2 i 3 riječi: „davaoci usluga certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „fizičko i pravno lice, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona" u odgovarajućem padežu.

Tačka 4 mijenja se i glasi:

4) opis načina ispunjavanja tehničkih i operativnih zahtjeva koji se odnose na okvir interoperabilnosti iz člana 61 stav 4 ovog zakona;"

U stavu 2 riječi: „evidenciju, odnosno u registar" zamjenjuju se riječima: „registar sistema elektronske identifikacije".

Član 26

U članu 65 stav 1 tačka 2 riječi: „certifikovanja za elektronske transakcije" brišu se.

U tački 5 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije".

Član 27

U članu 66 stav 1 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije", a riječi: „evidenciju ili registar," zamjenjuju se riječima: „registar sistema elektronske identifikacije,".

Član 28

U članu 67 st. 2 i 3 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije".

Član 29

U članu 68 stav 2 mijenja se i glasi:

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

Član 30

Član 70 mijenja se i glasi:

„Član 70

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

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

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

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

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

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

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

7) ne posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih certifikata, u iznosu koji može pokriti

rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete (član 34 stav 1 tačka 7);

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

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

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

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

12) o izdatim kvalifikovanim certifikatima ne vodi evidenciju i ne obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju (član 49 stav 1 tačka 2);

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

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

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

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

17) ne izvrši opoziv certifikata kad primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata (član 51 stav 1 tačka 3);

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Član 31

U članu 71 stav 3 riječi: „državnom organu" zamjenjuju se riječima: „organu vlasti".

St. 4, 5 i 6 brišu se.

Član 32

Poslije člana 73 dodaje se novi član koji glasi:

„Član 73a

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

Član 33

U članu 74 riječi: „člana 40 st. 2 i 7," zamjenjuju se riječima: „člana 40 st. 2 i 6,".

Član 34

Poslije člana 75 dodaje se novi član i glasi:

„Član 75a

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

Član 35

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

Obrazloženje

I. Ustavni osnov za donošenje zakona

Ustavni osnov za donošenje ovog zakona sadržan je u odredbi člana 16 Ustava Crne Gore kojim je, između ostalog, propisano da se zakonom uređuju određena pitanja od interesa za Crnu Goru.

II. Razlozi za donošenje zakona

Cilj donošenja ovog zakona je povećanje povjerenja u elektronske transakcije kroz pravni okvir koji uređuje sigurne i pouzdane elektronske transakcije. Izgradnja povjerenja u elektronsko poslovanje je ključna za razvoj informacionog društva kao i za ekonomski i socijalni razvoj praćen modernim tehnologijama. Donošenjem Zakona o izmjenama i dopunama elektronskoj identifikaciji i elektronskom potpisu preciznije se normira pravni osnov za dalji razvoj elektronskog poslovanja u Crnoj Gori. Takođe, vrši se potpuno usaglašavanje normativnog okvira za ovu oblast sa evropskom regulativom.

III. Usaglašenost sa pravnom tekovinom Evropske unije i potvrđenim međunarodnim konvencijama

Predlogom zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu transponuje se Regulativa Evropskog parlamenta i savjeta (EU) broj 910/2014 o elektronskoj identifikaciji i uslugama povjerenja u elektronske transakcije na unutrašnjem tržištu (eIDAS) i prestanku važenja Direktive 1999/93/EZ. Regulativa je donijeta sa ciljem rješavanja glavnih problema koje sprečavaju građane da koriste pogodnosti digitalnog jedinstvenog tržišta i prekograničnih digitalnih usluga. Cilj je brz napredak u ključnim oblastima digitalne ekonomije i promovisanje potpuno jedinstvenog digitalnog tržišta olakšavanjem prekogranične upotrebe usluga na internetu uz pridavanje naročite pažnje olakšavanju sigurne elektronske identifikacije i autentifikacije.

IV. Objašnjenje osnovnih pravnih instituta

Odredbom člana 1 Predloga zakona data je definicija elektronske identifikacije, sistema elektronske identifikacije i sredstva elektronske identifikacije.

Odredbama **člana 2** Predloga zakona definišu se i precizno navode elektronske usluge povjerenja, kao i kvalifikovane elektronske usluge povjerenja.

Odredbama **člana 3** Predloga zakona propisano je da elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove propisane ovim zakonom, dok kvalifikovane elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove za vršenje tih usluga propisane ovim zakonom. Takođe je propisano da elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, vrši organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja, odnosno Ministarstvo.

Članom 4 vrše se izmjene člana iz razloga preciznijeg definisanja proizvoda koji se koriste prilikom pružanja elektronskih usluga povjerenja licima sa invaliditetom.

U **članu 5** se preciznije definišu pojedini izrazi iz člana 8 Predloga zakona iz razloga što se izmjene ovog zakona vrše kako bi se stvorili uslovi da organ vlasti, osim toga što može postati davalac usluga elektronske usluge povjerenja, može biti i autor elektronskog pečata.

Članom 6 izvršena je izmjena riječi „usluge certifikovanja za elektronske transakcije" u različitom padežu u izraz „elektronske usluge povjerenja" u odgovarajućem padežu u članovima u kojima je to bilo potrebno.

Odredbama člana 7 mijenja se član 16 na način da je preciznije propisan sadržaj podataka kvalifikovanog certifikata za elektronski potpis u skladu sa eIDAS Regulativom.

Odredbom **člana 8** u članu 18 briše se stav 2.

Odredbom **člana 9** briše se određeni dio kako bi norma bila prilagođena promjenama koje smo iz razloga preciznosti uveli.

Odredbom **člana 10** normirano je da ni fizičko lice ne može odbiti prijem podataka poslatih i primljenih upotrebom usluge elektronske preporučene dostave samo zato što je u elektronskom obliku ili zbog toga što ne ispunjavaju sve zahtjeve kvalifikovane usluge elektronske preporučene dostave.

Član 11 preciznije uređuje sadržinu podataka na kvalifikovani certifikati za autentifikaciju internet stranica u skladu sa eIDAS Regulativom.

Odredbama **člana 12** se dodatno uređuju uslovi koje treba da ispuni davalac kvalifikovane usluge povjerenja u skladu sa dosadašnjim promjenama.

Članom 13 propisani su uslovi, koje moraju da ispune organ vlasti i Ministarstvo kada vrše kvalifikovane elektronske usluge povjerenja.

Odredbom **člana 14** Predloga zakona u članu 38 st. 1 i 2 riječi „usluge certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske usluge povjerenja", briše se stav 3 iz razloga razdvajanja sistema elektronske identifikacije od elektronskih usluga povjerenja.

Odredbama **člana 15** propisuje se postupak za upis davalaca elektronskih usluga povjerenja u registar kvalifikovanih davalaca elektronskih usluga povjerenja.

Nadalje odredbom **člana 16** Predloga zakona riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu i briše se stav 4 člana 40.

Odredbom **člana 17** omogućeno je i organima vlasti izdavanje kvalifikovanog certifikata na njegov zahtjev, na osnovu utvrđenog identiteta i drugih podataka o pravnom licu, fizičkom licu ili organu vlasti za koje se izdaje kvalifikovani certifikat

Odredbama **člana 18** pored terminološkog usklađivanja, u članu 49 i stavu 1 tačka 2 uvedeno je da se provjera identiteta pored fizičkog lica i pravnog lica vrši i za organ vlasti kojem se izdaje kvalifikovani certifikat, dok je u tački 3 propisano da o izdatim kvalifikovanim certifikatima vodi evidenciju i obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju. Takođe, propisani su i načini kojima se može vršiti provjera identiteta fizičkog, pravnog lica ili organa vlasti.

Odredbama **člana 19** izvršeno je terminološko usklađivanje riječi u stavu 1, kao i preciznije normiranje st. 2, 4 i 5.

Članom 20 propisano je da sistemima elektronske identifikacije upravljaju fizičko, pravno lice ili organ vlasti iz člana 4 st. 3 i 4 ovog zakona.

Odredbama člana 21 izmijenjen je član 60 u smislu prilagođavanja izvršenim izmjenama.

Odredbama člana 22 dodata su dva nova člana 60a i 60b, kojima su propisani uslovi u vezi sa sistemom za eletronsku identifikaciju i sadržaj registra sistema elektronske identifikacije.

Odredbama člana 23 propisana je obaveza uspostavljanja interoperabilnosti sistema elektronske identifikacije.

U **čl, 24, 25, 26, 27 i 28,** izvršene su izmjene iz razloga dosadašnjih izmjena u Predlogu zakona.

Odredbom **člana 29** izvršena je korekcija u u članu 68 stav 2 u cilju preciznijeg normiranja u smislu da inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.

Odredbama **čl. 30 i 31** vrše se izmjene kaznenih odredbi u skladu sa promjenama izvršenim u Predlogu zakona.

Odredbom **člana 32** dodaje se novi član 73a poslije člana 73 kojim se definiše da će se podzakonski akti donijeti na osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG", broj 31/17) uskladiti sa ovim zakonom u roku od 12 mjeseci od dana stupanja na snagu ovog zakona.

Članom 33 izvršena je korekcija tehničke prirode u članu 74, iz razloga promjene, odnosno brisanja stava u članu 40 Predloga zakona.

Odredbom **člana 34** dodaje se novi član 75a poslije člana 75 kojim se definiše da kvalifikovani certifikati i sredstva za izradu elektronskog potpisa, koji se zasniva na tom certifikatu, izdati do dana stupanja na snagu ovog zakona smatraju se kvalifikovanim certifikatima za elektronski potpis, odnosno kvalifikovanim sredstvima za izradu elektronskog potpisa u skladu sa ovim zakonom do datuma isteka roka važenja tih certifikata.

Članom 35 normirano je da ovaj zakon stupa na snagu osmog dana od dana objavljivanja u Službenom listu Crne Gore.

V. Finansijska sredstva za sprovođenje zakona

Za sprovođenje ovog zakona nije potrebno obezbijediti sredstva.

Odredbe Zakona o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG, br. 31/17") koje se mijenjaju

Elektronska identifikacija

Član 2

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

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

Usluge certifikovanja za elektronske transakcije

Član 3

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

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

Ocjenjivanje usaglašenosti kvalifikovanih usluga certifikovanja za elektronske transakcije

Član 4

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

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

Dostupnost usluga certifikovanja za elektronske transakcije licima sa invaliditetom

Član 5

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

Proizvodi koji se koriste prilikom pružanja usluga certifikovanja za elektronske transakcije podrazumijevaju odgovarajuću računarsku opremu (hardver) ili računarski

program (softver) koji su namijenjeni za korišćenje u svrhu pružanja usluga certifikovanja za elektronske transakcije.

Izrazi

Član 8

Izrazi koji se koriste u ovom zakonu imaju sljedeća značenja:

1) **lični identifikacioni podaci** obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica;

2) **autentifikacija** je elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku;

3) **korisnik** je fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili uslugu certifikovanja za elektronske transakcije;

4) **potpisnik** je fizičko lice koje posjeduje sredstvo za izradu elektronskog potpisa kojim se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica;

5) **podaci za izradu elektronskog potpisa** su jedinstveni podaci (kodovi ili privatni kriptografski ključevi), koje potpisnik koristi za izradu elektronskog potpisa;

6) **autor elektronskog pečata** je pravno lice koje posjeduje sredstvo za izradu elektronskog pečata i izrađuje elektronski pečat;

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

8) **certifikat za elektronski pečat** je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem i potvrđuje naziv tog pravnog lica;

9) **kvalifikovani certifikat za elektronski pečat** je certifikat za elektronski pečat koji izdaje kvalifikovani davalac usluge certifikovanja za elektronske transakcije i koji ispunjava posebne uslove propisane ovim zakonom;

10) **sredstvo za izradu elektronskog pečata** je odgovarajuća računarska oprema ili računarski program koji se koristi za izradu elektronskog pečata;

11) **sredstvo za izradu kvalifikovanog elektronskog pečata** je sredstvo za izradu elektronskog pečata koje ispunjava posebne uslove propisane ovim zakonom;

12) **elektronski dokument** je skup podataka koji su elektronski oblikovani, poslati, primljeni ili skladišteni na elektronskom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva pomoću kojih se identifikuje stvaralac, utvrđuje vjerodostojnost sadržaja i dokazuje nepromjenjivost sadržaja u vremenu, a uključuje sve oblike pisanog teksta, podatke, slike, crteže, karte, zvuk, muziku, govor i slično;

13) **podaci za verifikaciju** su podaci koji se koriste za verifikaciju elektronskog potpisa ili elektronskog pečata;

14) **verifikacija** je postupak kojim se potvrđuje da su elektronski potpis ili elektronski pečat validni;

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

16) **domen** je sistem u kome se internet adrese vezuju za određene lokacije na internetu.

Certifikat za elektronski potpis

Član 15

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

Kvalifikovani certifikat za elektronski potpis

Član 16

Kvalifikovani certifikat za elektronski potpis je certifikat za kvalifikovani elektronski potpis koji sadrži podatke propisane ovim zakonom i kojeg izdaje kvalifikovani davalac usluga certifikovanja za elektronske transakcije.

Kvalifikovani certifikat za elektronski potpis mora da sadrži:

1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis;

2) identifikacioni skup podataka o pravnom ili fizičkom licu koje izdaje kvalifikovani certifikat za elektronski potpis uz navođenje države u kojoj je davalac usluga registrovan, i to:

- za pravno lice: naziv, matični broj i poreski identifikacioni broj,
- za fizičko lice: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište;

3) identifikacioni skup podataka o potpisniku (lično ime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište);

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

5) podatke o periodu važenja kvalifikovanog certifikata za elektronski potpis;

6) identifikacionu oznaku izdatog kvalifikovanog certifikata za elektronski potpis koja mora biti jedinstvena za kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;

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

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

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

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

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

Sredstvo za izradu elektronskog potpisa

Član 18

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

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

Kreiranje podataka za izradu elektronskog potpisa

Član 20

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

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

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

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

Zahtjevi za verifikaciju kvalifikovanog elektronskog potpisa

Član 23

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

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

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

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

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

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

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

7) nije ugrožen integritet potpisanih podataka;

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

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

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

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

Način sprovođenja verifikacije kvalifikovanog elektronskog potpisa propisuje Ministarstvo.

Usluga čuvanja kvalifikovanih elektronskih potpisa

Član 24

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

Način vršenja usluge čuvanja kvalifikovanih elektronskih potpisa propisuje Ministarstvo.

Elektronski vremenski pečat i kvalifikovani elektronski vremenski pečat

Član 26

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

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

1) povezuje datum i vrijeme sa podacima tako da se sprječava svaka mogućnost promjene podataka;

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

3) potpisan je naprednim elektronskim potpisom ili pečatiran pomoću naprednog elektronskog pečata kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije.

Shodna primjena

Član 27

Na pravno dejstvo, punovažnost i prihvatljivost elektronskog pečata, elektronskog vremenskog pečata i kvalifikovanog elektronskog pečata, zahtjeve za napredni elektronski pečat, sadržaj kvalifikovanog elektronskog pečata i elektronskog vremenskog pečata, izdavanje, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, kvalifikovana sredstva za izradu elektronskog pečata i elektronskog vremenskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata i sredstva za izradu elektronskog vremenskog pečata, verifikaciju i čuvanje kvalifikovanog sredstva za izradu elektronskog pečata i sredstva za izradu elektronskog vremenskog pečata shodno se primjenjuju odredbe čl. 9 do 24 ovog zakona.

Pravno dejstvo usluge elektronske preporučene dostave

Član 29

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

Kvalifikovana usluga elektronske preporučene dostave

Član 31

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

1) je vrši jedan ili više kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije;

2) uz visok nivo sigurnosti obezbjeđuje identifikaciju pošiljaoca;

3) obezbjeđuje identifikaciju primaoca prije dostave podataka;

4) je slanje i primanje podataka obezbijeđeno naprednim elektronskim potpisom ili naprednim elektronskim pečatom kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije, na način kojim se isključuje mogućnost nezapažene promjene podataka;

5) se pošiljaocu i primaocu podataka jasno naznačava svaka promjena podataka potrebna radi slanja ili primanja podataka;

6) se datum i vrijeme slanja, primanja i eventualne promjene podataka ovjeravaju kvalifikovanim elektronskim vremenskim pečatom.

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

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

Pojam i certifikati

Član 32

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

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

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

Kvalifikovani certifikati za autentifikaciju internet stranica

Član 33

Kvalifikovani certifikat za autentifikaciju internet stranica mora da sadrži:

1) oznaku u elektronskom obliku pogodnom za automatsku obradu da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranica;

2) identifikacioni skup podataka o pravnom ili fizičkom licu koje izdaje kvalifikovani certifikat za elektronski potpis uz navođenje države u kojoj je davalac usluga registrovan, i to:

- za pravno lice: naziv, matični broj i poreski identifikacioni broj;
- za fizičko lice: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište;

3) identifikacioni skup podataka o fizičkom licu kome je izdat certifikat, i to: ime i prezime, ime oca ili majke, pseudonim ako ga ima, datum rođenja, prebivalište, odnosno boravište, adresu, grad i državu;

4) naziv domena kojim upravlja fizičko ili pravno lice kojem je izdat certifikat za autentifikaciju internet stranice;

5) podatke o periodu važenja kvalifikovanog certifikata za autentifikaciju internet stranice;

6) identifikacionu oznaku izdatog kvalifikovanog certifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije;

7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije koji izdaje certifikat;

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

9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za autentifikaciju internet stranica.

V. USLOVI ZA VRŠENjE KVALIFIKOVANIH USLUGA CERTIFIKOVANjA ZA ELEKTRONSKE TRANSAKCIJE

Uslovi u vezi sa kvalifikovanim davaocima usluga certifikovanja za elektronske transakcije

Član 34

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

1) ima ažuriran plan prekida pružanja usluge radi obezbjeđivanja njenog kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona;

2) obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti;

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

4) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje usluga certifikovanja za elektronske transakcije, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka;

5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa;

6) preduzima mjere za sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja certifikate potpisnicima na bezbjedan način;

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

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

9) koristi pouzdan sistem čuvanja kvalifikovanih certifikata u obliku koji omogućava provjeru, kako bi:

- unos i promjene podataka za izradu usluga certifikovanja za elektronske transakcije vršila samo ovlašćena lica,
- mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata,
- podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje,
- bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve, bila vidljiva kvalifikovanom davaocu usluga certifikovanja za elektronske transakcije.

Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo.

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

Član 35

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

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

Pravno dejstvo kvalifikovanih certifikata izdatih u drugoj državi

Član 36

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

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

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

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

3) su u skladu sa međunarodnim ugovorom zaključenim između Crne Gore i druge države ili međunarodne organizacije;

4) su u skladu sa međunarodnim ugovorom zaključenim između Evropske unije i države koja nije članica Evropske unije ili međunarodne organizacije;

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

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

Prijava o početku vršenja usluge certifikovanja za elektronske transakcije

Član 37

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

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

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

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

Upis u evidenciju

Član 38

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

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

Evidencija sadrži i podatke o sistemu elektronske identifikacije uključujući stepene njegove sigurnosti.

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

Bliži sadržaj i način vođenja evidencije propisuje Ministarstvo.

Rješenje o ispunjenosti uslova za pružanje kvalifikovanih usluga certifikovanja za elektronske transakcije

Član 39

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

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

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

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

Upis u registar

Član 40

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

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

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

Registar sadrži i podatke o sistemu elektronske identifikacije uključujući stepene njegove sigurnosti.

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

Registar potpisuje Ministarstvo naprednim elektronskim potpisom.

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

Bliži sadržaj i način vođenja registra propisuje Ministarstvo.

Brisanje iz registra

Član 41

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

Kad Ministarstvo nakon obavještenja iz stava 1 ovog člana utvrdi da kvalifikovani davalac usluge certifikovanja za elektronske transakcije ne ispunjava uslove iz člana 34

ovog zakona, ili prestane da vrši usluge certifikovanja za elektronske transakcije, brisaće tog davaoca usluge iz registra.

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

Naznaka o upisu u registar u certifikatima

Član 42

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

Korišćenje oznake certifikovanja za elektronske transakcije EU

Član 43

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

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

Izdavanje certifikata

Član 44

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

Pravo na izbor davaoca usluga certifikovanja za elektronske transakcije

Član 45

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

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

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

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

Obaveze potpisnika i autora elektronskog pečata

Član 47

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

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

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

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

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

Obaveze davaoca usluge certifikovanja za elektronske transakcije

Član 49

Davalac usluga certifikovanja za elektronske transakcije dužan je da:

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

2) sprovede potpunu provjeru identiteta potpisnika;

3) obezbijedi tačnost i cjelovitost podataka koje unosi u evidenciju izdatih certifikata;

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

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

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

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

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

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

Davanje obavještenja podnosiocima zahtjeva

Član 50

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

Obavještenje iz stava 1 ovog člana obavezno sadrži:

1) izvod iz važećih propisa i internih akata iz člana 37 stav 4 ovog zakona;

2) podatke o eventualnim ograničenjima koja se odnose na korišćenje certifikata;

3) podatke o odgovarajućoj pravnoj zaštiti ili vansudskom poravnanju, ako na njega davalac usluga pristane u slučaju spora;

4) podatke o mjerama koje treba da realizuju potpisnici, odnosno autori elektronskog pečata i o tehnologiji potrebnoj za bezbjednu izradu i provjeru elektronskog potpisa.

Opoziv i suspenzija certifikata

Član 51

Davalac usluga certifikovanja za elektronske transakcije dužan je da izvrši opoziv certifikata u slučaju kad:

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

2) utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka;

3) primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata;

4) utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način;

5) utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca usluga certifikovanja za elektronske transakcije ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata;

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

7) istekne rok važenja certifikata;

8) primi sudsku odluku ili upravni akt koji se odnose na važenje certifikata ili

9) postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 ovog zakona.

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

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

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

Davalac usluga certifikovanja za elektronske transakcije dužan je da obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog koje se certifikat suspenduje, odnosno opoziva.

Mjere zaštite certifikata

Član 52

Davalac usluga certifikovanja za elektronske transakcije dužan je da:

1) primjenjuje organizacione i tehničke mjere zaštite certifikata i podataka vezanih za potpisnike i autore elektronskog pečata;

2) uspostavi i primjenjuje sistem zaštite pristupa evidenciji certifikata i opozvanih i suspendovanih certifikata koji će omogućiti pristup samo ovlašćenim licima i koji obezbjeđuje provjeru tačnosti prenosa podataka i blagovremeni uvid u eventualne greške tehničkih sredstava.

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

Obaveze davaoca usluge certifikovanja za elektronske transakcije u slučaju raskida ugovora

Član 53

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

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

certifikovanja za elektronske transakcije kod drugog davaoca usluge certifikovanja za elektronske transakcije.

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

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

Obaveza povezivanja evidencija

Član 54

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

Osiguranje rizika od odgovornosti

Član 55

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

Najniži iznos osiguranja iz stava 1 ovog člana utvrđuje Ministarstvo.

Odgovornost za štetu

Član 56

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

1) informacija koju sadrži kvalifikovani certifikat nije tačna u trenutku njegovog izdavanja;

2) certifikat ne sadrži sve elemente propisane za kvalifikovani certifikat;

3) nije obezbijedio da potpisnik, odnosno autor elektronskog pečata u trenutku izdavanja certifikata posjeduje podatke za izradu elektronskog potpisa, odnosno elektronskog pečata koji odgovaraju podacima za provjeru elektronskog potpisa, odnosno elektronskog pečata koji su dati, odnosno identifikovani u certifikatu;

4) ne obezbijedi da se podaci za izradu i podaci za provjeru elektronskog potpisa, odnosno elektronskog pečata mogu koristiti komplementarno, u slučaju kad te podatke kreira davalac usluge certifikovanja za elektronske transakcije;

5) propusti da opozove certifikat u skladu sa članom 51 ovog zakona;

6) certifikat ne sadrži informacije o ograničenjima koja se odnose na korišćenje.

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

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

Davalac usluga certifikovanja za elektronske transakcije odgovoran je za štetu pričinjenu potpisniku, odnosno autoru elektronskog pečata ili savjesnom trećem licu zbog

nedostataka ili kašnjenja prilikom omogućavanja uvida u podatke o važenju, isteku ili suspenziji certifikata.

Prikupljanje i obrada podataka o ličnosti

Član 57

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

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

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

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

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

Upravljanje rizicima

Član 58

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

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

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

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

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

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

Sistem elektronske identifikacije

Član 59

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

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

Stepen sigurnosti sistema elektronske identifikacije

Član 60

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

Stepeni sigurnosti iz stava 1 ovog člana su:

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

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

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

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

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

Minimalne tehničke standarde i prateće procedure propisuje Ministarstvo.

Interoperabilnost

Član 61

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

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

1) ima za cilj tehnološku neutralnost i ne pravi razliku između posebnih tehničkih rješenja za elektronsku identifikaciju;

2) se pridržava evropskih i međunarodnih standarda, kad je to moguće;

3) na obradu ličnih podatak primjenjuje propise o zaštiti podataka o ličnosti.

Saradnja

Član 62

Ministarstvo sarađuje sa državama članicama Evropske unije u vezi sa:

1) interoperabilnošću sistema elektronske identifikacije koji su upisani u evidenciju i registar;

2) sigurnošću sistema elektronske identifikacije.

Saradnja iz stava 1 ovog člana podrazumijeva:

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

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

3) razmjenu informacija o ocjenjivanju usaglašenosti sistema elektronske identifikacije.

Priznavanje certifikata i sredstava elektronske identifikacije

Član 63

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

Kad organ vlasti za uslugu koju pruža na internetu zahtijeva elektronsku identifikaciju pomoću sredstava elektronske identifikacije i autentifikacije radi pristupa toj usluzi, u skladu

sa propisima, sredstvo elektronske identifikacije izdato u državi članici Evropske unije priznaje se za potrebe prekogranične autentifikacije ako:

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

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

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

Obavještavanje Evropske komisije

Član 64

Ministarstvo dostavlja Evropskoj komisiji sljedeće informacije i, bez odlaganja, sve naknadne izmjene tih informacija koje se odnose na:

1) opis sistema elektronske identifikacije, uključujući njegove stepene sigurnosti i davaoca, odnosno davaoce usluge certifikovanja za elektronske transakcije sredstava u okviru tog sistema;

2) važeći sistem nadzora i informacije o pravilima i odgovornosti davaoca usluga certifikovanja za elektronske transakcije koji izdaje sredstva elektronske identifikacije, odnosno sprovodi proceduru autentifikacije;

3) davaoce usluga certifikovanja za elektronske transakcije koji upravlja registracijom jedinstvenih ličnih identifikacionih podataka;

4) opis načina ispunjavanja kriterijuma iz člana 61 stav 2 ovog zakona;

5) opis autentifikacije iz člana 65 stav 1 tačka 6 ovog zakona;

6) suspenziju ili opoziv certifikata.

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

Prihvatljivost sistema elektronske identifikacije

Član 65

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

1) su sredstva elektronske identifikacije priznata od strane države članice Evropske unije;

2) sredstva elektronske identifikacije mogu da se koriste za pristup bilo kojoj usluzi certifikovanja za elektronske transakcije koju pruža organ vlasti, a koja zahtijeva elektronsku identifikaciju u državi članici Evropske unije;

3) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema ispunjavaju zahtjeve bilo kojeg stepena sigurnosti iz člana 60 ovog zakona;

4) Ministarstvo obezbijedi da se lični identifikacioni podaci, u skladu sa tehničkim specifikacijama, standardima i procedurama za odgovarajući stepen sigurnosti iz člana 60 ovog zakona, pripisuju fizičkom ili pravnom licu koje koristi lične identifikacione podatke u elektronskom obliku u vrijeme kad su sredstva elektronske identifikacije izdata u okviru tog sistema;

5) davalac usluga certifikovanja za elektronske transakcije koji izdaje sredstva elektronske identifikacije u okviru tog sistema obezbijedi da se sredstva elektronske identifikacije pripisuju fizičkom ili pravnom licu koje koristi lične identifikacione podatke u elektronskom obliku u skladu sa odgovarajućim stepenom sigurnosti iz člana 60 ovog zakona;

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

Povreda sigurnosti

Član 66

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

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

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

Odgovornost

Član 67

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

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

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

Upravni i inspekcijski nadzor

Član 68

Upravni nadzor nad sprovođenjem ovog zakona vrši Ministarstvo.

Inspekcijski nadzor nad radom davalaca usluga certifikovanja za elektronske transakcije i kvalifikovanih davalaca usluga certifikovanja za elektronske transakcije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.

Član 70

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16) ne izvrši opoziv certifikata kad primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata (član 51 stav 1 tačka 3);

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Član 71

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

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

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

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

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

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

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

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

Član 72

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

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

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

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

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

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

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

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

Član 74

Odredbe člana 10 stav 3, čl. 22, 36, člana 40 st. 2 i 7, člana 43, člana 45 stav 4, člana 58 st. 4 i 6, i čl. 62 do 67 ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

OBRAZAC

IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	Ministarstvo javne uprave
NAZIV PROPISA	Predlog zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu

1. Definisanje problema

- **Koje probleme treba da riješi predloženi akt?**
- **Koji su uzroci problema?**
- **Koje su posljedice problema?**
- **Koji su subjekti oštećeni, na koji način i u kojoj mjeri?**
- **Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?**

UVOD:

Nakon donošenja Uredbe EU broj 910/2014 o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije, prestala je da važi Direktiva EU br. 1999/93 o elektronskom potpisu.

U cilju usaglašavanja normativnog okvira za elektronsku identifikaciju i elektronske usluge povjerenja sa navedenom direktivom donešen je Zakon o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG" broj 31/2017), kojim su pravno uređena bitna pitanja iz oblasti elektronskog poslovanja i povećanja povjerenja u elektronske transakcije.

Nakon dve godine sprovođenja Zakona, koji se usklađuje sa najkompleksnijom regulativom EU za oblast informacionog društva, pristupilo se dodatnom normiranju članova kako bi Zakon bio precizniji za sprovođenje, a i prilagođen potrebama Crne Gore, u procesu uvođenja elektronskog identifikacionog dokumenta.

Izmjene i dopune Zakona o elektronskoj identifikaciji i elektronskom potpisu izvršene su, prevashodno, iz razloga prilagođavanja Zakona o elektronskoj identifikaciji i elektronskom potpisu izmjenama Zakona o ličnoj karti, odnosno uvođenja elektronskog identifikacionog dokumenta i jasnijeg normiranja elektronske identifikacije.

Izvršeno je i terminološko usklađivanje sa EIDAS regulativom u smislu da se umjesto pojma usluge certifikovanja za elektronske transakcije uveo pojam elektronske usluge povjerenja, koji je adekvatniji iz razloga što elektronske usluge povjerenja, osim usluga izdavanja certifikata obuhvataju i druge usluge koje ne zahtijevaju izdavanje certifikata, te je novi izraz primjereniji obuhvatu usluga koje normira zakon.

Zakon je značajan za građane, privredu, organe javne vlasti i ostale subjekte, a njegova primjena omogućava intezivnije elektronsko poslovanje.

Osnovni cilj zakonskog uređivanja oblasti elektronske identifikacije i usluga povjerenja u elektronske transakcije je da se omogući i podstakne brže, efikasnije i ekonomičnije poslovanje, razvije tržište usluga povjerenja, građanima i privredi omogući lakša i sugurnija komunikacija i pristup uslugama organa javne vlasti i drugih subjekata.

Pravni okvir

Donošenjem zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu dodatno će se urediti zakonski okvir za sigurno i efikasno elektronsko poslovanje, čime se direktno utiče na jačanje povjerenja u elektronske transakcije na tržištu.

Zakonom o elektronskom dokumentu propisano je da se elektronski dokument izjednačava sa dokumentom u papirnoj formi. Zakonom o informacionoj bezbijednosti propisane su mjere i standardi informacione bezbijednosti.

Takođe, Zakonom o upravnom postupku, Zakonom o elektronskoj upravi i ovim zakonskim rješenjem zaokružuje se pravni okvir i stvaraju preduslovi za elektronsko upravno postupanje razvoj elektronske uprave i povećanje povjerenja u elektronsko poslovanje organa.

Trenutna situacija

Nakon što je donijet Zakon o elektronskoj identifikaciji i elektronskom potpisu, doneseni su svi zakonom propisani podzakoski akti, a to su:

- Pravilnik o najnižem iznosu osiguranja rizika od odgovornosti za štete koje nastanu pružanjem usluga certifikovanja;
- Pravilnik o načinu sprovođenja verifikacije i načinu vršenja usluge čuvanja kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata;
- Pravilnik o sadržini i načinu vođenja evidencije davalaca usluga certifikovanja i registra kvalifikovanih davalaca usluga certifikovanja;
- Pravilnik o okviru za interoperabilnost sistema elektronske identifikacije;
- Pravilnik o načinu ocjenjivanja usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata i sadržaju liste certifikovanih kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata;
- Pravilnik o mjerama i aktivnostima za zaštitu certifikata za elektronski potpis i elektronski pečat;
- Pravilnik o minimalnim tehničkim standardima i pratećim procedurama u odnosu na koje se određuje stepen sigurnosti sistema elektronske identifikacije;
- Pravilnik o bližim zahtjevima koje mora da ispunjava kvalifikovana usluga elektronske preporučene dostave;
- Pravilnik o bližim uslovima koje mora da ispunjava kvalifikovani davalac usluga certifikovanja i
- Uredba o načinu vršenja kvalifikovanih usluga certifikovanja za organe državne uprave.

U registru kvalifikovanih davalaca usluga elektronskih transakcija upisan je jedan davalac kvalifikovanih usluga certifikovanja za elektronske transakcije, a na listi kvalifikovanih sredstava za izradu elektronskog potpisa, odnosno elektronskog pečata upisano je kvalifikovano sredstvo.

Očekivanja su da izmjene i dopune Zakona o elektronskoj identifikaciji i elektronskom potpisu doprinesu većem interesovanju od strane potencijalnih davalaca elektronskih usluga povjerenja, odnosno uspostavljanju sistema elektronske identifikacije.

Predloženi akt treba da riješi problem:

Izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu dodatno će se urediti oblast elektronske identifikacije i elektronskih usluga povjerenja. Sistemi elektronske identifikacije se predloženim izjenama ne vezuju samo za davaoce elektronskih usluga povjerenja, kako je bio slučaj do sada, već se mogu uspostaviti nezavisno uz ispunjavanje propisanih uslova.

Takođe, ovim izmjenama je izvršeno dodatno usglašavanje sa EU regulativom 910/2014 u smislu jasnijeg opisa sadržaja kvalifikovanog certifikata za elektronski potpis, autentifikaciju internet stranica itd.

Uzroci problema su prije svega :

Zakonom o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG" broj 31/2017) propisano je da usluge certifikovanja za elektronske transakcije (elektronske usluge povjerenja) može da pruža samo fizičko ili pravno lice, a za organe državne uprave ove usluge može pružati i organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja. Praksa je pokazala da ovakvo rješenje ne doprinosi masovnijoj primjeni elektronske identifikacije i elektronskih usluga povjerenja te da je potrebno, prije svega, pružanje ovih usluga dozvoliti i ostalim organima javne vlasti.

Zakonom o ličnoj karti ("Službeni list CG", br. 12/2007, 73/2010, 28/2011, 50/2012, 10/2014 i 18/2019) u članu 6 propisano sledeće:

"Lična karta izdaje se na propisanom obrascu, u skladu sa ovim zakonom.Obrazac lične karte sadrži: Grb Crne Gore, naziv "Crna Gora", naziv "Lična karta", oznaku za elektronsku ispravu, zaštitne elemente, rubrike za unos ličnih i drugih podataka, kao i čip u kojem su sadržani fotografija, otisak dva prsta, lični i drugi podaci, certifikat za elektronsku identifikaciju i certifikat za kvalifikovani elektronski potpis.Lični i drugi podaci iz stava 2 ovog člana su: prezime, ime, pol, dan, mjesec i godina rođenja, državljanstvo, jedinstveni matični broj lica, fotografija, potpis, datum izdavanja, datum prestanka važenja, broj lične karte, naziv organa koji je izdao ličnu kartu i mašinski čitljiv zapis.Unošenje podataka i certifikata iz st. 2 i 3 ovog člana ovog člana u obrazac lične karte vrši organ državne uprave nadležan za unutrašnje poslove (u daljem tekstu: Ministarstvo).Tehničke karakteristike čipa iz stava 2 ovog člana moraju da obezbijede cjelovitost, autentičnost i povjerljivost podataka koje sadrži.Podatke koje sadrži mašinski čitljiv zapis utvrđuje Ministarstvo u skladu sa preporukama ISAO Dos 9303.Obrazac lične karte propisuje Ministarstvo, u skladu sa evropskim i međunarodnim standardima."

Imajući u vidu ovaj propis kao i strateška dokumenta iz oblasti elektronske uprave, izmjenama i dopunama zakona o elektronskoj identifikaciji i elektronskom potpisu omogućiti će se organu državne uprave nadležnom za poslove elektronske uprave i elektronskog poslovanja da vrši elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, kao i da elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja mogu vršiti i drugi organi vlasti u okviru poslova iz svoje nadležnosti, u skladu sa posebnim zakonom.

Posledice problema:

- Na tržištu postoji samo jedan kvalifikovani davalac usluga certifikovanja za elektronske transakcije;
- Nemogućnost organa javne vlasti da pružaju elektronske usluge povjerenja i uspostave sisteme elektronske identifikacije;
- Uslijed visoke cijene certifikata, broj izdatih certifikata nije na nivou koji zadovoljava potrebe elektronskog poslovanja koje treba da snažno utiče na privredni i društveni razvoj. Zbog visokih cijena certifikata građani oklijevaju da učestvuju i primjenjuju elektronsko poslovanje. Prisutno je samo djelimično pružanje elektronskih usluga i nemogućnost pružanja kompletnih elektronskih usluga tokom cijelog postupka pred organima javne vlasti.

Koji su subjekti oštećeni, na koji način i u kojoj mjeri?
Oštećeni subjekti su svi učesnici u elektronskom poslovanju, kao i korisnici usluga javne administracije.

Kako bi problem evoluirao bez promjene propisa (status quo)

U slučaju opcije status quo identifikacioni dokumenti građana ne bi mogli da služe za elektronsku identifikaciju ili za elektronsko potpisivanje.

Naime, Zakonom o elektronskoj identifikaciji i elektronskom potpisu propisano je da samo pravna i fizička lica mogu da budu davaoci usluga certifikovanja za elektronske transakcije, odnosno elektronskih usluga

povjerenja. Povodom toga, ukazujemo da na osnovu tog zakona Ministarstvo unutrašnjih poslova kao organ koji je nadležan za poslove u vezi izdavanja identifikacionih dokumenata ne bi mogao da uspostavi sistem elektronske identifikacije i pruža elektronske usluge povjerenja, što je neophodno za poslove izdavanja novih identifikacionih dokumenata.

2. Ciljevi

- Koji ciljevi se postižu predloženim propisom?
- Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo.

Koji ciljevi se postižu predloženim propisom?

Izmjenama i dopunama zakona o elektronskoj identifikaciji i elektronskom potpisu omogućiće se organu državne uprave nadležnom za poslove elektronske uprave i elektronskog poslovanja da vrši elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, kao i da elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja mogu vršiti i drugi organi vlasti u okviru poslova iz svoje nadležnosti, u skladu sa posebnim zakonom.

Ovim zakonskim rješenjem, sistem elektronske identifikacije je odvojen od pružanja elektronskih usluga povjerenja. Samim tim fizička, pravna lica ili organi vlasti koji upravljaju sistemima za elektronsku identifikaciju ispunjavaju uslove koji su propisani izmjenama i dopunama ovog zakona.

Takođe, propisano je da autor elektronskog pečata može biti i organ javne vlasti. Naime, prethodno zakonsko rješenje nije propisivalo mogućnost da autor elektronskog pečata može biti i organ javne vlasti.

Usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo

Strategijom reforme javne uprave Crne Gore 2016 do 2020. godine, u oblasti pružanja usluga predviđeno je uspostavljanje jedinstvenog sistema elektronske identifikacije na Portalu eUprave, kao tačke pristupa elektronskim uslugama koje nude organi javne uprave sa visokim stepenom korisničkog iskustva i korisničkog zadovoljstva kao i elektronsko upravljanje dokumentima.

Strategijom razvoja informacionog društva Crne Gore 2016 do 2020. godine, naglašeno je da elektronska identifikacija predstavlja osnov za pravno funkcionisanje e-usluga. Tehnologije elektronskog identiteta i usluge autentifikacije su od suštinske važnosti za transakcije preko interneta, i u privatnom i u javnom sektoru.

3. Opcije

- Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa).
- Obrazložiti preferiranu opciju?

Ispunjavanje ciljeva i rješavanje problema moguće je postići usvajanjem navedenog propisa. "Status quo" opcija bi podrazumijevala neefikasno otklanjanje uočenih problema ili bi moglo doći do djelimične primjene rješenja što bi svakako uticalo na kvalitet elektronskog poslovanja.

4: Analiza uticaja

- Na koga će i kako će najvjerovatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.
- Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima).
- Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.
- Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.
- Uključiti procjenu administrativnih opterećenja i biznis barijera.

Na koga će i kako će najvjerovatnije uticati rješenja u propisu?

Implementacija Zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu će uticati na javnu upravu, privredu i građane.

Izdavanjem ceritikata za elektronsku identifikaciju i certifikata za kvalifikovani elektronski potpis na ličnim kartama, omogućiće se masovnija primjena elektronske identifikacije i elektronskog potpisa u poslovanju.

Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim I srednjim preduzećima)?

Analizom su razmatrane pozitivne posljedice primjene propisa po građane i privredu. Na portalu elektronske uprave, na dosta niskom transakcionom nivou, trenutno se nalaze 574 elektronske usluge.

Očekuje se da će se masovnijom primjenom elektronske identifikacije i elektronskih usluga povjerenja značajno povećati kvalitet ovih usluga, što će svakako doprinijeti uštedi vremena i novca svih korisnika.

Koristeći primjer iz analize, koja je urađena za potrebe Zakona o elektronskoj upravi, u kome se metodom proračuna standardnog troška izračunalo da se realizacijom samo jedne elektronske usluge „Upis novorođenčeta i vađenje zdravstvene knjižice" na nivou Podgorice godišnje uštedi 58.078 € , očekuje se da će se uvođenjem elektronskog dokument koji će obezbijediti i funkcionlnost zdravstvene knjižice ova ušteda povećati.

Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti?

Odredbama ovog zakonskog rješenja uspostavlja se viši nivo efikasnosti i efektivnosti rada organa na koje se zakon primjenjuje, uz visok stepen pravne sigurnosti čime se formira pogodno poslovno okruženje, naročito za investicije.

Da li se zakonom podržava stvaranje novih privrednih subjekata i tržišna konkurencija?

Očekuje se da će Izmjene i dopune Zakona o elektronskoj identifikaciji i elektronskom potpisu doprinijeti stvaranju novih privrednih subjekata i podržati tržišnu konkurenciju. Ovim zakonskim rješenjem stvaraju se preduslovi za povećanu upotrebu usluga elektronske identifikacije i kvalifikovanih elektronskih usluga povjerenja. Uslijed toga, sasvim realno je očekivati da će se povećati potražnja za ovim uslugama od strane organa javne vlasti, građana i privrede, što može dovesti do stvaranja novih privrednih subjekata, a samim tim i novih radnih mjesta.

Procjena administrativnih opterećenja i biznis barijera.

Izuzimajući troškove koji su povezani sa elektronskim uslugama povjerenja, može se reći da primjena ovog propisa ne izaziva troškove za građane i privredu već donosi uštedu.

Trenutno na tržištu je registrovan jedan komercijalni davalac elektronski usluga povjerenja Certifikaciono tijelo Pošta Crne Gore, koja je do kraja 2018 izdala 21828 certifikata.

Certifikaciono tijelo Pošta CG izdaje sledeće certifikate:

- Kvalifikovani certifikat za kvalifikovani elektronski potpis na kriptografskom tokenu ("QSCD" sredstvo) sa rokom važenja od tri godine, u zavisnosti od količine cijena certifikata iznosi od 90 do 110 €.
- Kvalifikovani certifikat za napredni elektronski potpis sa rokom važenja od tri godine, u zavisnosti od količine cijena certifikata iznosi 25 do 30 €.
- Kvalifikovani certifikat za povjerljivost izdat na "QSCD" sredstvu sa rokom važenja do tri godine, u zavisnosti od količine cijena certifikata iznosi od 90 do 110 €.
- Kvalifikovani certifikat za povjerljivost sa rokom važenja od tri godine, u zavisnosti od količine cijena certifikata iznosi 25 do 30 €.

- Kvalifikovani certifikat za kvalifikovani elektronski pečat izdat na kriptografskom tokenu ("QSCD" sredstvo) sa rokom važenja od tri godine, u zavisnosti od količine cijena certifikata iznosi od 90 do 110 €.
- Kvalifikovani certifikat za napredni elektronski pečat, sa rokom važenja od tri godine,u zavisnosti od količine cijena iznosi 25 do 30 €.
- Kvalifikovani certifikat za autentifikaciju internet stranica, sa rokom važenja od godinu dana iznosi 100 €.
- Certifikat za Microsoft Windows Domain Controllera (DS) server sa rokom važenja od pet godina iznosi 100 €.
- Certifikat za SmartLogon izdat na kriptografskom tokenu (QSCD sredstvo) sa rokom važenja od pet godina, u zavisnosti od količine cijena certifikata iznosi od 90 do 110 €.
- Grupni certifikat na kriptografskom tokenu (QSCD sredstvo) sa rokom važenja od tri godine, u zavisnosti od količine cijena certifikata iznosi od 68 do 110 €.
- Obnova grupnog certifikata na kriptografskom tokenu QSCD za tri godine iznosi od 60 do 80 €.

Povećanjem broja davalaca elektronskih usluga povjerenja i sistema elektronske identifikacije za očekivati je da i cijene certifikata budu niže.

Zakon ne predviđa dodatna administrativna opterećenja i biznis barijere, već ih nasuprot tome smanjuje.

5. Procjena fiskalnog uticaja

- **Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?**
- **Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Obrazložiti.**
- **Da li implementacijom propisa proizilaze međunarodne finansijske obaveze? Obrazložiti.**
- **Da li su neophodna finansijska sredstva obezbijeđena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskanu godinu?**
- **Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteći finansijske obaveze?**
- **Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?**
- **Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.**
- **Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda?**
- **Obrazložiti.**
- **Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?**
- **Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.**

S obzirom da se radi o Zakonu o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu, za implementaciju ovog ovog propisa nije potrebno izdvajati dodatna finansijska sredstva iz budžeta Crne Gore, jer su ona ranije predviđena.

Ne proizilaze finansijske obaveze iz podzakonski akata koja će se donijeti na osnovu ovog propisa.Zakon će pozitivno uticati na rad organa javne vlasti koji će, primjenom kvalifikovanih elektronskih usluga povjerenja, moći da akte koje donose u svom radu izdaju u obliku potpisanog/pečatiranog elektronskog dokumenta. Dostavljanje elektronskih akata moći će da se vrši putem kvalifikovane elektronske preporučene dostave.

Imajući u vidu da se izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu ne zahtijevaju dodatna finansijska sredstva/prihodi od onih koja su predviđena u Zakonu o elektronskoj identifikaciji i elektronskom potpisu, smatramo da nije bilo potrebno raditi obračun finansijskih izdataka/prihoda.

6. Konsultacije zainteresovanih strana

- **Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.**

- Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije). **- Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.**
Prilikom izrade zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu korišćena je eksterna ekspertska podrška.
7. Monitoring i evaluacija - **Koje su potencijalne prepreke za implementaciju propisa?** - **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?** - **Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?** - **Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?**
Potencijalne prepreke za implementaciju propisa su: - Otpor krajnjih korisnika prilikom uvođenja novih tehnologija; - Nezainteresovanost subjekata koji su Zakonom prepoznati kao potencijalni davaoci usluga elektronske identifikacije i elektronskih usluga povjerenja da uspostave sisteme elektronske odentifikacije ili da pružaju elektronske usluge povjerenja; - Nedovoljna upućenost o prednostima uvođenja elektronske identifikacije i elektronskih usluga povjerenja; - Nedostatak stručnih kadrova koji će pratiti i nadgledati primjenu zakonskih rješenja u organima. **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi** Za punu primjenu propisa neophodno je pojačati inspekcijski nadzor nad primjenom ovog zakona. Takođe potrebno je dodatno angažovanje u pogledu promovisanja elektronske identifikacije i elektronskih usluga povjerenja kako bi se široj javnosti pružile neophodne informacije o rešenjima koje predviđa Zakon. Mjerenje ispunjavanja ciljeva vršiće se preko broja izdatih certifikata kao i broja korisnika elektronskih usluga na Portalu eUprave. Monitoring i evaluaciju primjene propisa vršiće Ministarstvo javne uprave i o tome će izvještavati Vladu.

Datum i mjesto

Starješina organa

MINISTARSTVO JAVNE UPRAVE
1
PODGORICA

Crna Gora
Ministarstvo pravde

Crna Gora
MINISTARSTVO JAVNE UPRAVE
Podgorica

Primljeno:				
Org. jed.	Klas. znak	Redni broj	Prilog	Vrijednost
01-011/19-3910/5				

Adresa: Vuka Karadžića 3,
81000 Podgorica, Crna Gora
tel: +382 20 407 501
fax: +382 20 482 926
www.pravda.gov.me

Br: 01-019-7408/19-2

16. jul 2019.

Za: Ministarstvo javne uprave, Suzani Pribilović, ministarki

Veza: Vaš dopis broj: 01-011/19-3910/4 od 12. jula 2019. godine

Predmet: Mišljenje na tekst Predloga zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu

Ministarstvo pravde razmotrilo je tekst Predloga zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu, dostavljen aktom broj: 01-011/19-3910/4 od 12. jula 2019. godine. S tim u vezi, obavještavamo vas da u okviru nadležnosti ovog Ministarstva, nemamo primjedbi na tekst Predloga zakona, budući da su u neposrednoj komunikaciji sa predstavnicima predlagača, sugestije Ministarstva pravde ugrađene u tekst Predloga zakona.

S poštovanjem,

Zoran Pažin
MINISTAR

Dostavljeno:
- Ministarstvo javne uprave
- a/a

Crna Gora
MINISTARSTVO JAVNE UPRAVE
Podgorica

Primljeno	11.07.2019.			
Org. jed.	Klas. znak	Redni broj	Prilog	Vrijednost
01-011/19	3910/3			

Crna Gora
Sekretarijat za zakonodavstvo

Broj: 02-673/2
Podgorica, 10. jula 2019. godine

MINISTARSTVO JAVNE UPRAVE
- gospođi Suzani Pribilović, ministarki -

PODGORICA

Na inovirani tekst **PREDLOGA ZAKONA O IZMJENAMA I DOPUNAMA ZAKONA O ELEKTRONSKOJ IDENTIFIKACIJI I ELEKTRONSKOM POTPISU** (dostavljen Vašim aktom, broj 01-011/19-3910/2 od 9. jula 2019. godine), iz okvira nadležnosti ovog Sekretarijata, nemamo primjedaba, budući da su primjedbe i sugestije Sekretarijata date predstavnicima obrađivača u neposrednoj saradnji od 2. do 5. jula 2019. godine, ugrađene u predloženi tekst zakona.

SEKRETARKA
Dušanka Jauković

Vuka Karadžića broj 3 81000 Podgorica
Tel.: (+382) 20 231-535 Fax: (+382) 20 231-592
e-mail: szz@szz.gov.me

Crna Gora
MINISTARSTVO JAVNE UPRAVE
Podgorica

Primljeno:	14.10.2019.			
Org. jed.	Klas. znak	Redni broj	Prilog	Vrijednost
01-	011/19-	5847/2	1	

Vlada Crne Gore
Kabinet predsjednika
Kancelarija za evropske integracije

Br: 01-004-2689/2

Podgorica, 14. oktobar 2019. godine

MINISTARSTVO JAVNE UPRAVE
ministarki Suzani Pribilović

Poštovana gospođo Pribilović,

Dopisom broj 01-011/19-5847 od 14. oktobra 2019. godine tražili ste mišljenje o usklađenosti **Predloga zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu** sa pravnom tekovinom Evropske unije.

Nakon upoznavanja sa sadržinom predloga propisa, a u skladu sa nadležnostima definisanim članom 40 stav 1 alineja 2 Poslovnika Vlade Crne Gore („Sl. list CG", br. 3/12, 31/15, 48/17 i 62/18) Kancelarija za evropske integracije je saglasna sa navodima u obrascu usklađenosti predloga propisa s pravnom tekovinom Evropske unije.

S poštovanjem,

GLAVNI PREGOVARAČ

Aleksandar Drljević

- Sačinio: Luka Stanković, šef Grupe
- Odobrila: Nevenka Vulićević, načelnik Odsjeka za usklađivanje propisa s pravnom tekovinom EU

81000 Podgorica, Bulevar revolucije 15
Tel: +382 20 481 301
E-mail: kei@gsv.gov.me; www.kei.gov.me

IZJAVA O USKLAĐENOSTI NACRTA/PREDLOGA PROPISA CRNE GORE S PRAVNOM TEKOVINOM EVROPSKE UNIJE

Identifikacioni broj Izjave	**MJU-IU/PZ/19/06**
1. Naziv nacrta/predloga propisa	
- na crnogorskom jeziku	Predlog zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu
- na engleskom jeziku	Proposal of the Law on amendments to the Law on electronic identification and electronic signature
2. Podaci o obrađivaču propisa	
a) Organ državne uprave koji priprema propis	
Organ državne uprave	Ministarstvo javne uprave
- Sektor/odsjek	Direktorat za elektronsku upravu i informatičku bezbjednost
- odgovorno lice (ime, prezime, telefon, e-mail)	Dušan Polović +382 67 637 267 dusan.polovic@mju.gov.me
- kontakt osoba (ime, prezime, telefon, e-mail)	Bojana Bajić +382 68 312 331
b) Pravno lice s javnim ovlašćenjem za pripremu i sprovođenje propisa	
- Naziv pravnog lica	/
- odgovorno lice (ime, prezime, telefon, e-mail)	/
- kontakt osoba (ime, prezime, telefon, e-mail)	/
3. Organi državne uprave koji primjenjuju/sprovode propis	
- Organ državne uprave	Svi organi državne uprave
4. Usklađenost nacrta/predloga propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropske unije i njenih država članica, s jedne strane i Crne Gore, s druge strane (SSP)	
a) Odredbe SSPa s kojima se usklađuje propis	
Glava VIII Politika saradnje, član 105 Informatičko društvo	
b) Stepen ispunjenosti obaveza koje proizilaze iz navedenih odredbi SSPa	
☒	ispunjava u potpunosti
☐	djelimično ispunjava
☐	ne ispunjava
c) Razlozi za djelimično ispunjenje, odnosno neispunjenje obaveza koje proizilaze iz navedenih odredbi SSPa	
/	
5. Veza nacrta/predloga propisa s Programom pristupanja Crne Gore Evropskoj uniji (PPCG)	
- PPCG za period	2019-2020
- Poglavlje, potpoglavlje	10: Informatičko društvo i mediji, 1. Planovi i potrebe, 1.2. Zakonodavni okvir, B) Usluge informatičkog društva
- Rok za donošenje propisa	II kvartal
- Napomena	Do probijanja roka došlo je zbog međuresorskog usklađivanja.
6. Usklađenost nacrta/predloga propisa s pravnom tekovinom Evropske unije	
a) Usklađenost s primarnim izvorima prava Evropske unije	
Ne postoji odredba primarnih izvora prava EU s kojom bi se predlog propisa mogao uporediti radi dobijanja stepena njegove usklađenosti.	
b) Usklađenost sa sekundarnim izvorima prava Evropske unije	
32014R0910 Regulativa (EU) Evropskog parlamenta i Savjeta (EU) br. 910/2014 od 23. jula 2014. o elektronskoj identifikaciji i uslugama certifikovanja za elektronske transakcije na unutrašnjem tržištu i prestanku važenja	

Direktive 1999/93/EZ / Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC *(OJ L 257, 28.8.2014)* **Potpuno uskađeno/fully harmonized**
c) Usklađenost s ostalim izvorima prava Evropske unije
Ne postoji izvor prava EU ove vrste s kojim bi se predlog propisa mogao uporediti radi dobijanja stepena njegove usklađenosti.
6.1. Razlozi za djelimičnu usklađenost ili neusklađenost nacrta/predloga propisa Crne Gore s pravnom tekovinom Evropske unije i rok u kojem je predviđeno postizanje potpune usklađenosti
/
7. Ukoliko ne postoje odgovarajući propisi Evropske unije s kojima je potrebno obezbijediti usklađenost konstatovati tu činjenicu
/
8. Navesti pravne akte Savjeta Evrope i ostale izvore međunarodnog prava korišćene pri izradi nacrta/predloga propisa

Ne postoje izvori međunarodnog prava sa kojima je potrebno uskladiti predlog zakona.	/

9. Navesti da li su navedeni izvori prava Evropske unije, Savjeta Evrope i ostali izvori međunarodnog prava prevedeni na crnogorski jezik (prevode dostaviti u prilogu)
Navedeni izvor prava EU preveden je na crnogorski jezik.
10. Navesti da li je nacrt/predlog propisa iz tačke 1 Izjave o usklađenosti preveden na engleski jezik (prevod dostaviti u prilogu)
Predlog zakona o izmjenama i dopunama zakona o elektronskoj identifikaciji i elektronskom potpisu je preveden na engleski jezik.
11.Učešće konsultanata u izradi nacrta/predloga propisa i njihovo mišljenje o usklađenosti
Rudi Ponikvar, OSI d.o.o. Ljubljana, Slovenija

Potpis / ovlašćeno lice obrađivača propisa	**Potpis** / glavni pregovarač
Datum:	Datum:

Prilog obrasca:

1. Prevodi propisa Evropske unije
2. Prevod nacrta/predloga propisa na engleskom jeziku (ukoliko postoji)

TABELA USKLAĐENOSTI

1. Identifikacioni broj (IB) nacrta/predloga propisa	1.1. Identifikacioni broj izjave o usklađenosti i datum utvrđivanja nacrta/predloga propisa na Vladi
MJU-TU/PZ/19/06	MJU-IU/PZ/19/06

2. Naziv izvora prava Evropske unije i CELEX oznaka

Regulativa (EU) Evropskog parlamenta i Savjeta (EU) br. 910/2014 od 23. jula 2014. o elektronskoj identifikaciji i uslugama certifikovanja za elektronske transakcije na unutrašnjem tržištu i prestanku važenja Direktive 1999/93/EZ - 32014R0910

3. Naziv nacrta/predloga propisa Crne Gore

Na crnogorskom jeziku	Na engleskom jeziku
Predlog zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu	Proposal of the Law on amendments to the Law on electronic identification and electronic signature

4. Usklađenost nacrta/predloga propisa sizvorima prava Evropske unije

a)	b)	c)	d)	e)
Odredba i tekst odredbe izvora prava Evropske unije (član, stav, tačka)	Odredba i tekst odredbenacrta/predloga propisa Crne Gore (član, stav, tačka)	Usklađenost odredbe nacrta/ predloga propisa Crne Gore s odredbom izvora prava Evropske unije	Razlog za djelimičnu usklađenost ili neusklađenost	Rok za postizanje potpune usklađenosti
Regulativa 910/2014				
POGLAVLJE I **OPŠTE ODREDBE** *Član 1* **Predmet** Radi obezbjeđenja ispravnog funkcionisanja unutrašnjeg tržišta, istovremeno težeći odgovarajućem stepenu sigurnosti sredstava elektronske identifikacije i usluga povjerenja, ovom regulativom: (a) utvrđuju se uslovi pod kojim države članice priznaju sredstva elektronske identifikacije fizičkih i pravnih lica koja su obuhvaćena notifikovanim sistemom elektronske identifikacije druge države članice; (utvrđuju se pravila za usluge povjerenja, naročito za b elektronske transakcije; i)	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 1 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(c) uspostavlja se pravni okvir za elektronske potpise, elektronske pečate, elektronske vremenske pečate, elektronske dokumente, usluge elektronske preporučene dostave i usluge certifikovanja za autentifikaciju internet stranica.				
Član 2 **Područje primjene** 1. Ova regulativa primjenjuje se na sisteme elektronske identifikacije koje je notifikovala država članica, kao i na davaoce usluga povjerenja osnovane u Uniji. 2. Ova regulativa ne primjenjuje se na pružanje usluga povjerenja koje se isključivo koriste unutar zatvorenih sistema koji proizilaze iz domaćih zakona ili sporazumâ unutar utvrđene grupe učesnika. 3. Ova regulativa ne utiče na domaće pravo ili pravo Unije koje se odnosi na zaključivanje i valjanost ugovorâ ili drugih pravnih ili proceduralnih obaveza u pogledu forme.	Nema odgovarajuće odredbe	Neprenosivo		
Član 3 **Značenje izraza** Za potrebe ove regulative podrazumijeva se da je/su: 1. **elektronska identifikacija** – postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji na jedinstven način predstavljaju fizičko ili pravno lice ili fizičko lice koje predstavlja pravno lice; 2. **sredstvo elektronske identifikacije** – materijalna i/ili nematerijalna jedinica koja sadrži lične identifikacione podatke i koja se koristi za autentifikaciju usluge na internetu; 3. **lični identifikacioni podaci** – skup podataka koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica ili fizičkog lica koje predstavlja pravno lice; 4. **sistem elektronske identifikacije** – sistem za elektronsku identifikaciju u okviru kojeg se izdaju sredstva elektronske identifikacije fizičkim ili pravnim licima ili fizičkim licima koja predstavljaju pravna lica; 5. **autentifikacija** – elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku;	**Član 1** **Član 2 mijenja se i glasi:** „Elektronska identifikacija je postupak korišćenja identifikacionih podataka u elektronskom obliku koji na jedinstven način predstavljaju fizičko lice, pravno lice ili organ vlasti. Sistem elektronske identifikacije je sistem za izdavanje sredstava elektronske identifikacije fizičkim licima, pravnim licima, organima vlasti, odnosno fizičkim licima koja zastupaju pravna lica ili organe vlasti. Sredstvo elektronske identifikacije može biti skup podataka, računarska oprema (hardver) ili računarski program (softver) koji sadrže identifikacione podatke u elektronskom obliku ili povezuju fizičko lice, pravno lice ili organ vlasti sa tim podacima, a koji se koriste za autentifikaciju za uslugu u elektronskom obliku." **Član 2** **Član 3 mijenja se i glasi:** „Elektronske usluge povjerenja Radi korišćenja elektronskog potpisa, elektronskog pečata, elektronskog vremenskog pečata i usluge elektronske preporučene dostave u pravnom	Potpuno usklađeno	Potpuno usklađeno članovima 8, 9, 10, 11, 12, 18, 25, 26, 38, 40, 51, 65, 66,67 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

6. **strana korisnica** – fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili uslugu povjerenja; 7. **organ javnog sektora** – državni, regionalni ili lokalni organ, organ javnog prava ili udruženje koje čini jedan ili nekoliko takvih organa ili jedan ili nekoliko takvih organa javnog prava ili privatni subjekat koji je ovlastio barem jedan od tih organa uprave, organa ili udruženja za pružanje javnih usluga kada djeluju u okviru takvog ovlašćenja; 8. **organ javnog prava** – organ definisan u članu 2 stav 1 tačka 4 Direktive 2014/24/EU Evropskog parlamenta i Savjeta; 9. **potpisnik** – fizičko lice koje izrađuje elektronski potpis; 10. **elektronski potpis** – podaci u elektronskom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektronskom obliku i koje potpisnik koristi za potpisivanje; 11. **napredni elektronski potpis** – elektronski potpis koji ispunjava zahtjeve navedene u članu 26; 12. **kvalifikovani elektronski potpis** – napredni elektronski potpis koji je izrađen pomoću kvalifikovanih sredstava za izradu elektronskog potpisa i zasniva se na kvalifikovanom certifikatu za elektronske potpise; 13. **podaci za izradu elektronskog potpisa** – jedinstveni podaci koje potpisnik koristi za izradu elektronskog potpisa; 14. **certifikat za elektronski potpis** – elektronska potvrda koja povezuje podatke za validaciju elektronskog potpisa s fizičkim licem i potvrđuje barem ime ili pseudonim tog lica; 15. **kvalifikovani certifikat za elektronski potpis** – certifikat za elektronske potpise koji izdaje kvalifikovani davalac usluga povjerenja i koji ispunjava zahtjeve utvrđene u Aneksu I; 16. **usluga povjerenja** – elektronska usluga koja se po pravilu pruža uz naknadu i koja se sastoji od: (a) izrade, verifikacije i validacije elektronskih potpisa, elektronskih pečata ili elektronskih vremenskih pečata, usluge elektronske preporučene dostave i certifikata koji se odnose na te usluge; ili	prometu, upravnim, sudskim i drugim postupcima, kao i certifikata za autentifikaciju internet stranice, fizičko i pravno lice i organ vlasti oslanjaju se na elektronsku uslugu povjerenja. Elektronske usluge povjerenja su usluge kojima se omogućava visok nivo pouzdanosti razmjene i obrade podataka u elektronskom obliku. Elektronske usluge povjerenja su: izrada certifikata za elektronski potpis, elektronski pečat i autentifikaciju internet stranice; izrada elektronskog vremenskog pečata; usluga elektronske preporučene dostave; verifikacija elektronskog potpisa i elektronskog pečata; čuvanje elektronskog potpisa, elektronskih pečata ili certifikata koji se odnose na te usluge. Elektronske usluge povjerenja koje ispunjavaju posebne uslove propisane ovim zakonom su kvalifikovane elektronske usluge povjerenja." **Član 3** **Član 4 mijenja se i glasi:** „Davaoci elektronske usluge povjerenja Elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove propisane ovim zakonom (u daljem tekstu: davalac elektronske usluge povjerenja). Kvalifikovane elektronske usluge povjerenja vrši fizičko ili pravno lice koje ispunjava uslove za vršenje tih usluga propisane ovim zakonom (u daljem tekstu: kvalifikovani davalac elektronske usluge povjerenja). Elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja za organe državne uprave, a kad je to propisano zakonom i za druge organe vlasti, vrši organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja (u daljem tekstu: Ministarstvo). Elektronske usluge povjerenja i kvalifikovane elektronske usluge povjerenja mogu vršiti i drugi organi vlasti u okviru poslova iz svoje nadležnosti, u skladu sa posebnim zakonom." **Član 5**			

(b) izrade, verifikacije i validacije certifikata za autentifikaciju internet stranica; ili (c) čuvanje elektronskih potpisa, pečata ili certifikata koji se odnose na te usluge; 17. **kvalifikovana usluga povjerenja** – usluga povjerenja koja ispunjava odgovarajuće zahtjeve utvrđene u ovoj regulativi; 18. **organ za ocjenjivanje usaglašenosti** – organ u smislu člana 2 tačka 13 Regulative (EZ) br. 765/2008 koji je u skladu s tom regulativom ovlašćen kao nadležan za sprovođenje ocjenjivanja usaglašenosti kvalifikovanog davaoca usluga povjerenja i kvalifikovanih usluga povjerenja koje on pruža; 19. **davalac usluga povjerenja** – fizičko ili pravno lice koja pruža jednu ili više usluga povjerenja bilo kao kvalifikovani ili nekvalifikovani davalac usluga povjerenja; 20. **kvalifikovani davalac usluga povjerenja** – davalac usluga povjerenja koji pruža jednu ili više kvalifikovanih usluga povjerenja i kojem je nadzorni organ odobrio kvalifikovani status; 21. **proizvod** – hardver ili softver ili odgovarajuće komponente hardvera ili softvera koji su namijenjeni za korišćenje u svrhu pružanja usluga povjerenja; 22. **sredstvo za izradu elektronskog potpisa** – konfigurisani softver ili hardver koji se koristi za izradu elektronskog potpisa; 23. **kvalifikovano sredstvo za izradu elektronskog potpisa** – sredstvo za izradu elektronskog potpisa koje ispunjava zahtjeve utvrđene u Aneksu II; 2 **autor pečata** – pravno lice koje izrađuje elektronski 4. pečat; 25. **elektronski pečat** – podaci u elektronskom obliku koji su pridruženi drugim podacima u elektronskom obliku ili su logički povezani s njima radi obezbjeđenja porijekla i integriteta tih podataka; 26. **napredni elektronski pečat** – elektronski pečat koji ispunjava zahtjeve navedene u članu 36; 27. **kvalifikovani elektronski pečat** – napredan elektronski pečat koji je izrađen pomoću kvalifikovanog sredstva za	**U članu 8 stav 1 tač. 1, 3, 4, 6, 8 i 9 mijenjaju se i glase:** „1) identifikacioni podaci obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog lica, pravnog lica ili organa vlasti; 3) korisnik je fizičko, pravno lice ili organ vlasti koje se oslanja na elektronsku identifikaciju ili elektronsku uslugu povjerenja; 4) potpisnik je fizičko lice koje se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica korišćenjem podataka za izradu elektronskog potpisa; 6) autor elektronskog pečata je pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata; 8) certifikat za elektronski pečat je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili organom vlasti i potvrđuje naziv tog pravnog lica ili organa vlasti; 9) kvalifikovani certifikat za elektronski pečat je certifikat za elektronski pečat koji izdaje kvalifikovani davalac elektronske usluge povjerenja;“. **Član 4** **Član 5 mijenja se i glasi:** **Član 5** **„Dostupnost elektronskih usluga povjerenja licima sa invaliditetom** Elektronske usluge povjerenja, kao i računarska oprema (hardver) ili računarski program (softver) koji se koriste prilikom vršenja tih usluga, kad je to moguće, dostupni su licima sa invaliditetom.“ **Član 7** **Član 16 mijenja se i glasi:** **Član 16** „Kvalifikovani certifikat za elektronski potpis je certifikat koji izdaje kvalifikovani davalac elektronske usluge povjerenja, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona i koji sadrži:			

izradu elektronskog pečata i koji se zasniva na kvalifikovanom certifikatu za elektronski pečat; 28. **podaci za izradu elektronskog pečata** – jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata; 29. **certifikat za elektronski pečat** – elektronska potvrda koja povezuje podatke za validaciju elektronskog pečata s pravnim licem i potvrđuje naziv tog lica; 30. **kvalifikovani certifikat za elektronski pečat** – certifikat za elektronski pečat koji izdaje kvalifikovani davalac usluge povjerenja i koji ispunjava zahtjeve utvrđene u Aneksu III; 31. **sredstvo za izradu elektronskog pečata** – konfigurisani softver ili hardver koji se koristi za izradu elektronskog pečata; 32. **sredstvo za izradu kvalifikovanog elektronskog pečata** – sredstvo za izradu elektronskog pečata koje mutatis mutandis ispunjava zahtjeve utvrđene u Aneksu II; 33. **elektronski vremenski pečat** – podaci u elektronskom obliku koji povezuju druge podatke u elektronskom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme; 34. **kvalifikovani elektronski vremenski pečat** – elektronski vremenski pečat koji ispunjava zahtjeve navedene u članu 42; 35. **elektronski dokument** – svaki sadržaj koji je sačuvan u elektronskom obliku, a naročito kao tekstualni ili zvučni, vizuelni ili audiovizuelni zapis; 36. **usluga elektronske preporučene dostave** – usluga koja omogućava prenos podataka među trećim stranama pomoću elektronskih sredstava i pruža dokaz o postupanju s prenesenim podacima, uključujući dokaz o slanju i prijemu podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja ili bilo kakvih neovlašćenih prepravki; 37. **kvalifikovana usluga elektronske preporučene dostave** – usluga elektronske preporučene dostave koja ispunjava zahtjeve utvrđene u članu 44; 38. **certifikat za autentifikaciju internet stranice** – potvrda pomoću koje je moguće izvršiti autentifikaciju internet	1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis u obliku prikladnom za automatsku obradu podataka; 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za elektronski potpis, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj; - fizičko lice: ime i prezime i poreski identifikacioni broj; 3) skup identifikacioni podataka o potpisniku (ime i prezime ili pseudonim) koji, ako se koristi, mora biti jasno naznačen; 4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa i koji su pod kontrolom potpisnika; 5) podatke o periodu važenja tog certifikata; 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za elektronski potpis koja mora biti jedinstvena za kvalifikovanog davaoca elektronskih usluga povjerenja; 7) napredni elektronski potpis kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje taj certifikat; 8) lokaciju na kojoj je besplatno dostupan taj certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronskih usluga povjerenja; 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti tog certifikata; 10) odgovarajuću naznaku, u obliku pogodnom za automatsku obradu podataka, ako se podaci za izradu elektronskog potpisa koji su povezani sa podacima za verifikaciju elektronskog potpisa nalaze u kvalifikovanom sredstvu za izradu elektronskog potpisa.			

stranice i kojom se internet stranica povezuje s fizičkim ili pravnim licem kojem je izdat certifikat; 39. **kvalifikovani certifikat za autentifikaciju internet stranice** - certifikat za autentifikaciju internet stranice koji izdaje kvalifikovani davalac usluga povjerenja i koji ispunjava zahtjeve utvrđene u Aneksu IV; 40. **podaci za validaciju** – podaci koji se koriste za validaciju elektronskog potpisa ili elektronskog pečata; 41. **validacija** – postupak verifikacije i potvrđivanja da su elektronski potpis ili pečat validni.	Kvalifikovani certifikat 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." **Član 6** U članu 26 stav 2 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. **Član 14** U članu 38 st. 1 i 2 riječi: „usluge certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske usluge povjerenja". Stav 3 briše se. Dosadašnji st. 4 i 5 postaju st. 3 i 4. **Član 16** U članu 40 st. 2 i 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. Stav 4 briše se. U stavu 5 poslije riječi „obradu" dodaje se riječ „podataka". Dosadašnji st. 5 do 8 postaju st. 4 do 7. **Član 51** U članu 51 u uvodnoj rečenici stava 1 i u tački 5 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja", a u tački 6 riječi: „usluge certifikovanja" zamjenjuju se riječima: „elektronske usluge povjerenja". Stav 2 mijenja se i glasi: "Davalac elektronskih usluga povjerenja dužan je da na svojoj internet stranici objavi listu opozvanih certifikata, a opoziv certifikata proizvodi dejstvo od trenutka objavljivanja ove liste." U stavu 3 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja".			

	St. 4 i 5 mijenjaju se i glase: „Datum i vrijeme suspenzije i opoziva certifikata unose se u evidenciju iz člana 49 stav 1 tačka 5 ovog zakona: Davalac elektronskih usluga povjerenja dužan je da obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti iz stava 1 ovog člana." **Član 26** U članu 65 stav 1 tačka 2 riječi: „certifikovanja za elektronske transakcije" brišu se. U tački 5 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije". **Član 27** U članu 66 stav 1 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije", a riječi: „evidenciju ili registar," zamjenjuju se riječima: „registar sistema elektronske identifikacije," **Član 28** U članu 67 st. 2 i 3 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije".			
Član 4 **Načelo unutrašnjeg tržišta** 1. Pružanje usluga povjerenja na teritoriji države članice od strane davaoca usluge povjerenja osnovanog u drugoj državi članici ne ograničava se zbog razloga koji ulaze u područje primjene ove regulative. 2. Proizvodima i uslugama povjerenja koji su u skladu s ovom regulativom dozvoljava se da slobodno cirkulišu na unutrašnjem tržištu.	**Član 6** U članu 36 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 36 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 5 **Obrada i zaštita podataka** 1. Obrada ličnih podataka sprovodi se u skladu s Direktivom 95/46/EZ.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 6 Zakona o elektronskoj identifikaciji i	

2. Ne dovodeći u pitanje pravna dejstva koja pseudonimi imaju prema domaćem pravu, korišćenje pseudonima u elektronskim transakcijama nije zabranjeno.			elektronskom potpisu („Sl. list CG", broj 31/17)	
POGLAVLJE II **ELEKTRONSKA IDENTIFIKACIJA** *Član 6* **Uzajamno priznavanje** 1. Kada se prema domaćem pravu ili domaćoj administrativnoj praksi zahtijeva elektronska identifikacija pomoću sredstva elektronske identifikacije i autentifikacije radi pristupa usluzi koju organ javnog sektora pruža na internetu u jednoj državi članici, sredstvo elektronske identifikacije izdato u drugoj državi članici priznaje se u prvoj državi članici za potrebe prekogranične autentifikacije na tu uslugu na internetu, pod uslovom da su ispunjeni sljedeći uslovi: (a) sredstvo elektronske identifikacije izdato je u okviru sistema elektronske identifikacije koji je uvršten u listu koju je objavila Komisija na osnovu člana 9; (b) stepen sigurnosti tih sredstava elektronske identifikacije odgovara stepenu sigurnosti koji je jednak ili viši od stepena sigurnosti koji zahtijeva nadležni organ javnog sektora radi pristupa toj usluzi na internetu u prvoj državi članici ili viši od tog stepena, pod uslovom da stepen sigurnosti tih sredstava elektronske identifikacije odgovara značajnom ili visokom stepenu sigurnosti; (c) odgovarajući organ javnog sektora primjenjuje značajan ili visok stepen sigurnosti u odnosu na pristupanje toj usluzi na internetu. Takvo priznavanje mora da uslijedi najkasnije 12 mjeseci nakon što Komisija objavi listu iz podstava 1 tačka a. 2. Sredstvo elektronske identifikacije koje se izdaje u okviru sistema elektronske identifikacije uvrštenog na listu koju je objavila Komisija na osnovu člana 9 i koje odgovara niskom stepenu sigurnosti, organi javnog sektora mogu priznati za potrebe prekogranične autentifikacije na uslugu koju ti organi pružaju na internetu.	**Član 6** U članu 63 stav 1, članu 72 stav 1 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 63 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

Član 7 **Prihvatljivost sistema elektronske identifikacije za notifikaciju** Sistem elektronske identifikacije prihvatljiv je za notifikaciju na osnovu člana 9 stav 1 pod uslovom da budu ispunjeni svi sljedeći uslovi: (a) sredstva elektronske identifikacije u okviru sistema elektronske identifikacije izdata su: i. od strane države članice koja vrši notifikaciju; ii. u okviru mandata države članice koja vrši notifikaciju; ili iii. nezavisno od države članice koja vrši notifikaciju, a priznata su od strane te države članice; (b) sredstva elektronske identifikacije u okviru sistema elektronske identifikacije mogu da se koriste za pristup barem jednoj usluzi koju pruža organ javnog sektora i koja zahtijeva elektronsku identifikaciju u državi članici koja vrši notifikaciju; (c) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema ispunjavaju zahtjeve barem jednog od stepena sigurnosti utvrđenih u aktu za sprovođenje iz člana 8 stav 3; (d) država članica koja vrši notifikaciju obezbjeđuje da se lični identifikacioni podaci koji jedinstveno predstavljaju lice o kojem je riječ, u skladu s tehničkim specifikacijama, standardima i procedurama za odgovarajući stepen sigurnosti utvrđen u aktu za sprovođenje iz člana 8 stav 3, pripisuju fizičkom ili pravnom licu iz člana 3 tačka 1 u vrijeme kada su sredstva elektronske identifikacije izdata u okviru tog sistema; (e) strana koja izdaje sredstva elektronske identifikacije u okviru tog sistema obezbjeđuje da se sredstva elektronske identifikacije pripisuju licu iz tačke d ovog člana u skladu s tehničkim specifikacijama, standardima i procedurama za odgovarajući stepen sigurnosti utvrđen u aktu za sprovođenje iz člana 8 stav 3; (f) država članica koja vrši notifikaciju obezbjeđuje dostupnost autentifikacije na internetu, tako da svaka strana korisnica osnovana na teritoriji druge države članice	Poslije člana 60 dodaje se novi član koji glasi: **„Uslovi u vezi sa sistemom za elektronsku identifikaciju** **Član 60a** Sistem elektronske identifikacije mora da ispunjava sljedeće uslove, i to da: 1) sistem elektronske identifikacije i sredstva elektronske identifikacije izdata u okviru tog sistema, ispunjavaju zahtjeve najmanje jednog od stepena sigurnosti iz člana 60 stav 2 ovog zakona; 2) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjeđuje da identifikacioni podaci na osnovu kojih se izdaju sredstva elektronske identifikacije nedvosmisleno predstavljaju fizičko lice, pravno lice, odnosno organ vlasti kojem se to sredstvo izdaje, u momentu izdavanja, u skladu sa tehničkim standardima i procedurama iz člana 60 stav 3 ovog zakona za odgovarajući stepen sigurnosti; 3) fizičko lice, pravno lice, odnosno organ vlasti koji izdaje sredstva elektronske identifikacije obezbjeđuje da ta sredstva budu izdata fizičkom licu, pravnom licu, odnosno organu vlasti na osnovu čijih identifikacionih podataka je sredstvo izdato, u skladu sa tehničkim standardima i procedurama iz člana 60 stav 3 ovog zakona za odgovarajući stepen sigurnosti i 4) sistem elektronske identifikacije ispunjava tehničke i operativne zahtjeve iz člana 61 stav 1 ovog zakona. Ispunjenost uslova iz stava 1 ovog člana utvrđuje Ministarstvo. **Član 26** U članu 65 stav 1 tačka 2 riječi: „certifikovanja za elektronske transakcije" brišu se. U tački 5 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije".	Potpuno usklađeno	Potpuno usklađeno i članom 65 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

	može potvrditi lične identifikacione podatke primljene u elektronskom obliku. Za strane korisnice koje nijesu organi javnog sektora, država članica koja vrši notifikaciju može utvrditi uslove pristupa toj autentifikaciji. Prekogranična autentifikacija pruža se bez naknade kada se sprovodi na internetu u vezi s uslugom koju pruža organ javnog sektora. Države članice ne nameću bilo kakve posebne nesrazmjerne tehničke zahtjeve stranama korisnicama koje namjeravaju da sprovedu takvu autentifikaciju ako takvi zahtjevi sprečavaju ili znatno ograničavaju interoperabilnost notifikovanih sistema elektronske identifikacije; (g) najmanje šest mjeseci prije notifikacije na osnovu člana 9 stav 1, za potrebe obaveze prema članu 12 stav 5, država članica koja vrši notifikaciju drugoj državi članici dostavlja opis tog sistema u skladu s proceduralnim aranžmanima koji su utvrđeni aktima za sprovođenje iz člana 12 stav 7; (h) sistem elektronske identifikacije ispunjava zahtjeve utvrđene u aktu za sprovođenje iz člana 12 stav 8.				
	Član 8 **Stepeni sigurnosti sistema elektronske identifikacije**				
	1. Sistem elektronske identifikacije koji je notifikovan na osnovu člana 9 stav 1 određuje nizak, značajan i/ili visok stepen sigurnosti koji se pripisuje sredstvima elektronske identifikacije koja su izdata u okviru tog sistema. 2. Nizak, značajan i visok stepen sigurnosti moraju ispunjavati sljedeće kriterijume: (a) nizak stepen sigurnosti odnosi se na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koji pruža ograničen stepen povjerenja u odnosu na traženi ili utvrđeni identitet lica i karakteriše se pozivanjem na tehničke specifikacije, standarde i prateće procedure, uključujući tehničke kontrole čija je svrha smanjenje rizika od zloupotrebe ili promjene identiteta; (b) značajan stepen sigurnosti odnosi se na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koji pruža značajan stepen povjerenja u odnosu na traženi ili utvrđeni identitet lica i karakteriše se	**Član 21** U članu 60 stav 1 mijenja se i glasi: „Sistem elektronske identifikacije može imati nizak, značajan ili visok stepen sigurnosti koji se odnosi i na sredstva elektronske identifikacije". U stavu 2 riječi: „elektronske tranakcije" zamjenjuju se riječima: „sredstva elektronske identifikacije".	Potpuno usklađeno	Potpuno usklađeno članom 60 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

pozivanjem na tehničke specifikacije, standarde i prateće procedure, uključujući tehničke kontrole čija je svrha značajno smanjenje rizika od zloupotrebe ili promjene identiteta; (c) visok stepen sigurnosti odnosi se na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koji pruža viši stepen povjerenja u odnosu na traženi ili utvrđeni identitet lica od sredstava elektronske identifikacije sa značajnim stepenom sigurnosti i karakteriše ga pozivanje na tehničke specifikacije, standarde i s njima povezane postupke, uključujući tehničke kontrole čija je svrha značajno smanjenje rizika od zloupotrebe ili promjene identiteta. 3. Komisija, uzevši u obzir odgovarajuće međunarodne standarde i zavisno od stava 2, aktima za sprovođenje do 18. septembra 2015. godine određuje minimalne tehničke specifikacije, standarde i procedure u odnosu na koje se za sredstva elektronske identifikacije u smislu stava 1 utvrđuju nizak, značajan i visok stepen sigurnosti. Te minimalne tehničke specifikacije, standardi i procedure određuju se pozivanjem na pouzdanost i kvalitet sljedećih elemenata: (a) procedure radi dokazivanja i verifikacije identiteta fizičkog ili pravnog lica koje podnosi zahtjev za izdavanje sredstava elektronske identifikacije; (b) procedure za izdavanje traženih sredstava elektronske identifikacije; (c) mehanizma autentifikacije putem kojeg fizičko ili pravno lice koristi sredstva elektronske identifikacije za potvrđivanje svog identiteta strani korisnici; (d) organa koji izdaje sredstvo elektronske identifikacije; (e) svakog drugog organa uključenog u podnošenje zahtjeva za izdavanje sredstava elektronske identifikacije; i (f) tehničkih i sigurnosnih specifikacija izdatih sredstava elektronske identifikacije. Ti akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				

Član 9 **Notifikacija** 1. Država članica koja vrši notifikaciju prijavljuje Komisiji sljedeće informacije i, bez odlaganja, sve njihove naknadne izmjene: (a) opis sistema elektronske identifikacije, uključujući njegove stepene sigurnosti i izdavaoca ili izdavaoce sredstava elektronske identifikacije u okviru sistema; (b) važeći sistem nadzora i informacije o pravilima o odgovornosti u pogledu sljedećeg: i. strane koja izdaje sredstvo elektronske identifikacije; i ii. strane koja sprovodi proceduru autentifikacije; (c) organ ili organi odgovorni za sistem elektronske identifikacije; (d) informacije o subjektu ili subjektima koji upravljaju registracijom jedinstvenih ličnih identifikacionih podataka; (e) opis načina ispunjavanja zahtjeva određenih u aktima za sprovođenje iz člana 12 stav 8; (f) opis autentifikacije iz člana 7 tačka f; (g) dogovori za suspenziju ili opoziv notifikovanog sistema elektronske identifikacije ili autentifikacije ili ugroženih djelova o kojima je riječ.	**Član 22** **Poslije člana 60 dodaje se novi član koji glasi:** **„Registar sistema elektronske identifikacije** **Član 60b** Sistem elektronske identifikacije koji ispunjava uslove iz člana 60a ovog zakona upisuje se u registar sistema elektronske identifikacije. Registar sistema elektronske identifikacije sadrži: 1) opis sistema elektronske identifikacije, 2) stepen sigurnosti sistema elektronske identifikacije i sredstava elektronske identifikacije koji se izdaju u okviru tog sistema, 3) podatke o fizičkom licu, pravnom licu, odnosno organu vlasti koji upravljaju sistemom elektronske identifikacije i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj; - fizičko lice: ime i prezime i poreski identifikacioni broj; 4) datum upisa sistema elektronske identifikacije, kao i izmjene i brisanja iz registra. Registar sistema elektronske identifikacije vodi Ministarstvo.	Potpuno usklađeno	Potpuno usklađeno i članom 64 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
2. Godinu dana od dana primjene akata za sprovođenje iz člana 8 stav 3 i člana 12 stav 8, Komisija u Službenom listu Evropske unije objavljuje listu sistemâ elektronske identifikacije koji su notifikovani na osnovu stava 1 ovog člana i osnovne informacije o njima. 3. Ako Komisija primi notifikaciju nakon isteka perioda iz stava 2, ona u Službenom listu Evropske unije objavljuje izmjene i dopune liste iz stava 2, u roku od dva mjeseca od datuma prijema te notifikacije. 4. Država članica može Komisiji da podnese zahtjev za uklanjanje sistema elektronske identifikacije koji je notifikovala ta država članica s liste iz stava 2. Komisija objavljuje odgovarajuće izmjene i dopune liste u Službenom listu Evropske unije u roku od mjesec dana od datuma prijema zahtjeva države članice.	Registar se vodi u elektronskom obliku pogodnom za automatsku obradu i dostupan je javnosti na internet stranici Ministarstva. Registar potpisuje Ministarstvo naprednim elektronskim potpisom." **Član 25** **U članu 64 stav 1 tačka 1 mijenja se i glasi:** „1) opis sistema elektronske identifikacije i njegove stepene sigurnosti, podatke o fizičkom i pravnom licu, odnosno organu vlasti iz člana 4 st. 3 i 4 ovog zakona koji izdaje sredstva elektronske identifikacije;" U tač. 2 i 3 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: "elektronskih usluga povjerenja". Tačka 4 mijenja se i glasi:			

5. Komisija može aktima za sprovođenje da utvrdi okolnosti, oblike i procedure notifikacije u skladu sa stavom 1. Ti akti za sprovođenje donose se u skladu s procedurom ispitivanja iz člana 48 stav 2.	4) opis načina ispunjavanja tehničkih i operativnih zahtjeva koji se odnose na okvir interoperabilnosti iz člana 61 stav 4 ovog zakona;" U stavu 2 riječi: „evidenciju, odnosno u registar" zamjenjuju se riječima: „registar sistema elektronske identifikacije".			
Član 10 **Povreda sigurnosti** 1. U slučaju povrede ili djelimičnog ugrožavanja sistema elektronske identifikacije koji je notifikovan na osnovu člana 9 stav 1 ili autentifikacije iz člana 7 tačka f na način koji utiče na pouzdanost prekogranične autentifikacije tog sistema, država članica koja vrši notifikaciju bez odlaganja suspenduje ili opoziva tu prekograničnu autentifikaciju ili ugrožene djelove o kojima je riječ i obavještava ostale države članice i Komisiju. 2. Kada je povreda ili ugrožavanje iz stava 1 otklonjeno, država članica koja vrši notifikaciju ponovo uspostavlja prekograničnu autentifikaciju i bez odlaganja obavještava ostale države članice i Komisiju. 3. Ako povreda ili ugrožavanje iz stava 1 nije otklonjeno u roku od 3 mjeseca od suspenzije ili opoziva, država članica koja vrši notifikaciju obavještava druge države članice i Komisiju o povlačenju sistema elektronske identifikacije. Komisija u Službenom listu Evropske unije bez odlaganja objavljuje odgovarajuće izmjene i dopune liste iz člana 9 stav 2.	**Član 27** U članu 66 stav 1 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije", a riječi: „evidenciju ili registar," zamjenjuju se riječima: „registar sistema elektronske identifikacije,"	Potpuno usklađeno	Potpuno usklađeno članom 66 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 11 **Odgovornost** 1. Država članica koja vrši notifikaciju odgovorna je za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveza prilikom prekogranične transakcije u skladu s članom 7 tač. d i f. 2. Strana koja izdaje sredstva elektronske identifikacije odgovara za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu nepoštovanjem obaveza prilikom prekogranične transakcije iz člana 7 tačka e. 3. Strana koja sprovodi postupak autentifikacije odgovorna je za štetu koja je namjerno ili nepažnjom prouzrokovana	**Član 28** U članu 67 st. 2 i 3 riječi: „certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronske identifikacije.	Potpuno usklađeno	Potpuno usklađeno članom 67 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

svakom fizičkom ili pravnom licu nepoštovanjem obaveze obezbjeđenja ispravnog sprovođenja autentifikacije iz člana 7 tačka f prilikom prekogranične transakcije. 4. St. 1, 2 i 3 primjenjuju se u skladu s domaćim pravilima o odgovornosti. 5. St. 1, 2 i 3 ne dovode u pitanje odgovornost prema domaćem pravu strana u transakciji u kojoj se koriste sredstva elektronske identifikacije obuhvaćena sistemom elektronske identifikacije notifikovanim na osnovu člana 9 stav 1.				
Član 12 **Saradnja i interoperabilnost** 1. Domaći sistemi elektronske identifikacije notifikovani na osnovu člana 9 stav 1 moraju da budu interoperabilni. 2. Za potrebe stava 1, uspostavlja se okvir za interoperabilnost. 3. Okvir za interoperabilnost mora da ispunjava sljedeće kriterijume: (a) ima za cilj tehnološku neutralnost i ne pravi razliku između bilo kojih posebnih domaćih tehničkih rješenja za elektronsku identifikaciju unutar određene države članice; (b) pridržava se evropskih i međunarodnih standarda, kada je to moguće; (c) olakšava sprovođenje načela „ugrađene zaštite privatnosti"; i (d) obezbjeđuje obradu ličnih podataka u skladu s Direktivom 95/46/EZ. 4. Okvir za interoperabilnost sastoji se od: (a) pozivanja na minimalne tehničke zahtjeve koji se odnose na stepen sigurnosti prema članu 8; (b) raspoređivanje domaćih stepena sigurnosti notifikovanih sistema elektronske identifikacije na stepene sigurnosti u skladu s članom 8; (c) pozivanja na minimalne tehničke zahtjeve za interoperabilnost; (d) pozivanja na najmanji skup ličnih identifikacionih podataka koji na nedvosmislen način predstavljaju fizičko ili pravno lice i kojim raspolažu sistemi elektronske identifikacije; (e) poslovnika;	**Član 61 mijenja se i glasi:** **„Interoperabilnost** **Član 61** Sistemi elektronske identifikacije koji su upisani u registar sistema elektronske identifikacije moraju da ispunjavaju minimalne tehničke standarde i procedure iz člana 60 stav 3 ovog zakona i tehničke i operativne zahtjeve koji se odnose na čvor, operatera čvora i podatke o identitetu korisnika, i proces uspostavljanja okvira interoperabilnosti. Čvor je mjesto priključenja sistema elektronske identifikacije, koji je dio strukture interoperabilnosti sistema elektronske identifikacije i ima mogućnost prepoznavanja i obrade, odnosno prosljeđivanja prenosa podataka na druge čvorove i povezivanja sa sistemima elektronske identifikacije drugih država. Čvor uspostavlja i njime upravlja Ministarstvo. Tehničke i operativne zahtjeve koji se odnose na čvor, operatera čvora i podatke o identitetu korisnika, i proces uspostavljanja okvira interoperabilnosti propisuje Ministarstvo." **Član 24** U članu 62 stav 1 tačka 1 riječi: „evidenciju i registar" zamjenjuju se riječima „registar sistema elektronske identifikacije".	Potpuno usklađeno	Potpuno usklađeno i članom 62 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(f) dogovorâ za rješavanje sporova; i (g) zajedničkih operativnih sigurnosnih standarda. 5. Države članice sarađuju u vezi sa sljedećim: (a) interoperabilnošću sistema elektronske identifikacije koji su notifikovani na osnovu člana 9 stav 1 i sistema elektronske identifikacije koje države članice namjeravaju da notifikuju; i (b) sigurnošću sistemâ elektronske identifikacije. 6. Saradnja između država članica sastoji se od: (a) razmjene informacija, iskustva i dobre prakse u vezi sa sistemima elektronske identifikacije i naročito u vezi s tehničkim zahtjevima koji se odnose na interoperabilnost i stepene sigurnosti; (b) razmjene informacija, iskustva i dobre prakse u vezi s radom sa stepenima sigurnosti sistemâ elektronske identifikacije u skladu s članom 8; (c) stručnog pregleda sistema elektronske identifikacije obuhvaćenih ovom regulativom; i (d) pregleda odgovarajućih kretanja u sektoru elektronske identifikacije. 7. Komisija aktima za sprovođenje do 18. marta 2015. godine uspostavlja potrebne proceduralne aranžmane kako bi olakšala saradnju između država članica iz st. 5 i 6, s ciljem podsticanja visokog stepena povjerenja i sigurnosti koji odgovara stepenu rizika. 8. Komisija u svrhu određivanja jednakih uslova za sprovođenje zahtjeva na osnovu stava 1 do 18. septembra 2015. godine donosi akte za sprovođenje o okviru za interoperabilnost kako je utvrđeno u stavu 4, u skladu s kriterijumima iz stava 3 i uzimajući u obzir rezultate saradnje između država članica. 9. Akti za sprovođenje iz st. 7 i 8 ovog člana donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
POGLAVLJE III **USLUGE POVJERENJA** ***ODSJEK 1*** ***Opšte odredbe*** *Član 13* **Odgovornost i teret dokazivanja**	**Član 6** U članu 56 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.		Potpuno usklađeno članom 56 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

	1. Ne dovodeći u pitanje stav 2, davaoci usluga povjerenja odgovorni su za štetu koja je namjerno ili nepažnjom prouzrokovana svakom fizičkom ili pravnom licu zbog nepoštovanja obaveza na osnovu ove regulative. Teret dokazivanja namjere ili nepažnje nekvalifikovanog davaoca usluga povjerenja je na fizičkom ili pravnom licu koje zahtijeva naknadu štete iz podstava 1. Namjera ili nepažnja kvalifikovanog davaoca usluga povjerenja pretpostavlja se, osim ako kvalifikovani davalac usluga povjerenja dokaže da je šteta iz podstava 1 nastala bez namjere ili nepažnje tog kvalifikovanog davaoca usluga povjerenja. 2. U slučaju kada davaoci usluga povjerenja propisno i unaprijed obavijeste svoje korisnike o ograničenjima prilikom korišćenja usluga koje pružaju i kada su ta ograničenja prepoznatljiva za treće strane, davaoci usluga povjerenja ne odgovaraju za štete koje nastanu zbog korišćenja usluga kojim se prekoračuju navedena ograničenja. 3. St. 1 i 2 primjenjuju se u skladu s domaćim pravilima o odgovornosti.		Potpuno usklađeno		
	Član 14 **Međunarodni aspekti**				
	1. Usluge povjerenja koje pružaju davaoci usluga povjerenja osnovani u trećoj zemlji priznaju se kao pravno jednake kvalifikovanim uslugama povjerenja koje pružaju kvalifikovani davaoci usluga povjerenja osnovani u Uniji kada su usluge povjerenja iz treće zemlje priznate u okviru sporazuma zaključenog između Unije i treće zemlje o kojoj je riječ ili određene međunarodne organizacije u skladu s članom 218 UFEU. 2. Sporazumi iz stava 1 naročito obezbjeđuju da: (a) davaoci usluga povjerenja u trećoj zemlji ili međunarodne organizacije s kojima je zaključen sporazum i usluge povjerenja koje oni pružaju ispunjavaju zahtjeve koji se primjenjuju na kvalifikovane davaoce usluga povjerenja osnovane u Uniji i na kvalifikovane usluge povjerenja koje oni pružaju;	**Član 6** U članu 36 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 36 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(b) kvalifikovane usluge povjerenja koje pružaju kvalifikovani davaoci usluga povjerenja osnovani u Uniji budu priznate kao pravno jednake uslugama povjerenja koje pružaju davaoci usluga povjerenja u trećoj zemlji ili koje pružaju međunarodne organizacije s kojima je zaključen sporazum.				
Član 15 **Pristupačnost za lica s invaliditetom** Kada je to moguće, usluge povjerenja i proizvodi za krajnje korisnike korišćeni prilikom pružanja tih usluga pristupačni su za lica s invaliditetom.	**Član 5 mijenja se i glasi:** **„Dostupnost elektronskih usluga povjerenja licima sa invaliditetom"** **Član 5** Elektronske usluge povjerenja, kao i računarska oprema (hardver) ili računarski program (softver) koji se koriste prilikom vršenja tih usluga, kad je to moguće, dostupni su licima sa invaliditetom."	Potpuno usklađeno		
Član 16 **Sankcije** Države članice utvrđuju pravila o sankcijama koje se primjenjuju na povrede ove regulative. Te sankcije moraju da budu djelotvorne, srazmjerne i odvraćajuće.	**Član 70 mijenja se i glasi:** **„Član 70** Novčanom kaznom od 1.000 do 10.000 eura kazniće se za prekršaj pravno lice, ako: 1) nema ažuriran plan prekida pružanja usluge radi obezbjeđivanja njenog kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona (član 34 stav 1 tačka 1); 2) ne obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti (član 34 stav 1 tačka 2); 3) ne obezbijedi, na odgovarajući način i u skladu sa ovim zakonom i internim aktima iz člana 37 stav 4 ovog zakona, provjeru identiteta potpisnika i, po potrebi, drugog obilježja fizičkog i pravnog lica, kojima se izdaje kvalifikovani certifikat za elektronski potpis, odnosno kvalifikovani certifikat za elektronski pečat (član 34 stav 1 tačka 3); 4) nema zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje elektronskih usluga povjerenja, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka (član 34 stav 1 tačka 4);	Potpuno usklađeno	Potpuno usklađeno i i članovima 71, 72 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

		5) ne koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa (član 34 stav 1 tačka 5); 6) ne preduzima mjere za sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, ne garantuje tajnost procesa kreiranja tih podataka i ne dostavlja certifikate potpisnicima na bezbjedan način (član 34 stav 1 tačka 6); 7) ne posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih certifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete (član 34 stav 1 tačka 7); 8) ne posjeduje sistem čuvanja svih relevantnih informacija koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih certifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa (član 34 stav 1 tačka 8); 9) ne koristi pouzdan sistem čuvanja kvalifikovanih certifikata u obliku koji omogućava provjeru podataka, kako bi unos i promjene podataka za izradu elektronskih usluga povjerenja vršila samo ovlašćena lica, kako bi mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata, kako bi podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje i kako bi bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve bila vidljiva kvalifikovanom davaocu elektronskih usluga povjerenja (član 34 stav 1 tačka 9);			

	10) ne podnese Ministarstvu prijavu o promjenama u vršenju elektronskih usluga povjerenja (član 37 stav 3); 11) ne sprovede potpunu provjeru identiteta fizičkog lica, pravnog lica, odnosno organa vlasti kojem se izdaje kvalifikovani certifikat (član 49 stav 1 tačka 2); 12) o izdatim kvalifikovanim certifikatima ne vodi evidenciju i ne obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju (član 49 stav 1 tačka 2); 13) ne vodi ažurnu, tačnu i sigurnosnim mjerama zaštićenu evidenciju o validnosti certifikata (član 49 stav 1 tačka 5); 14) ne da obavještenje pravnom ili fizičkom licu, koje je podnijelo zahtjev za izdavanje certifikata o svim važnim okolnostima za njegovo korišćenje, prije zaključivanja ugovora iz člana 45 stav 3 ovog zakona (član 50); 15) ne izvrši opoziv certifikata na zahtjev potpisnika, odnosno autora elektronskog pečata ili njegovog ovlašćenog zastupnika (član 51 stav 1 tačka 1); 16) ne izvrši opoziv certifikata kad utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka (član 51 stav 1 tačka 2); 17) ne izvrši opoziv certifikata kad primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata (član 51 stav 1 tačka 3); 18) ne izvrši opoziv certifikata kad utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način (član 51 stav 1 tačka 4);			

		19) ne izvrši opoziv certifikata kad utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata (član 51 stav 1 tačka 5); 20) ne izvrši opoziv certifikata kad prestaje sa radom ili mu je rad zabranjen, a izdatim certifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja ne prenese na drugog davaoca tih usluga (član 51 stav 1 tačka 6); 21) ne izvrši opoziv certifikata kad istekne rok važenja certifikata (član 51 stav 1 tačka 7); 22) ne izvrši opoziv certifikata kad primi sudsku odluku ili upravni akt koji se odnose na važenje certifikata (član 51 stav 1 tačka 8); 23) ne izvrši opoziv certifikata kad postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 ovog zakona (član 51 stav 1 tačka 9); 24) ne objavi na svojoj internet stranici listu opozvanih certifikata (član 51 stav 2); 25) bez odlaganja ne suspenduje certifikat do utvrđivanja činjenica iz člana 51 stav 1 ovog zakona, ako se činjenice ne mogu odmah utvrditi na nesumnjiv način (član 51 stav 3); 26) ne obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu certifikata u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog kojih se certifikat suspenduje odnosno opoziva (član 51 stav 5); 27) ne primjenjuje organizacione i tehničke mjere zaštite certifikata i podataka vezanih za potpisnike i autore elektronskog pečata (član 52 stav 1 tačka 1); 28) ne uspostavi i ne primjenjuje sistem zaštite pristupa evidenciji certifikata i opozvanih i suspendovanih certifikata koji će omogućiti pristup samo ovlašćenim licima i koji obezbjeđuje provjeru tačnosti prenosa podataka i blagovremeni uvid u			

		eventualne greške tehničkih sredstava (član 52 stav 1 tačka 2); 29) ne obavijesti potpisnika, odnosno autora elektronskog pečata i Ministarstvo, najmanje tri mjeseca prije dana predviđenog za raskid ugovora, da raskida ugovor iz člana 45 stav 3 ovog zakona, zbog mogućeg stečaja ili potrebe, odnosno namjere prestanka poslovanja, (član 53 stav 1); 30) ne obezbijedi nastavak vršenja elektronskih usluga povjerenja za potpisnike, odnosno autore elektronskog pečata, kojima je izdao certifikate kod drugog davaoca usluga kojem dostavlja kompletnu dokumentaciju u vezi sa vršenjem elektronskih usluga povjerenja, a potpisnike, odnosno autore elektronskog pečata ne obavijesti o uslovima elektronskih usluga povjerenja kod drugog davaoca elektronske usluge povjerenja(član 53 stav 2); 31) ne opozove sve izdate certifikate i o tome, odmah, a najkasnije u roku od 48 časova, ne obavijesti Ministarstvo i ne dostavi mu kompletnu dokumentaciju u vezi sa izvršenim elektronskim uslugama povjerenja ako ne obezbijedi nastavak vršenja tih usluga kod drugog davaoca elektronske uslugepovjerenja, (član 53 stav 3); 32) ne omogući povezanost svoje evidencije izdatih i evidencije opozvanih i suspendovanih certifikata sa drugim davaocima elektronskih usluga povjerenja uz primjenu dostupne informacione tehnologije i uz upotrebu tehničkih i programskih sredstava čije je djelovanje u skladu sa važećim međunarodnim standardima (član 54); 33) ne osigura rizik od odgovornosti za štete koje nastanu vršenjem elektronskih usluga povjerenja (član 55 stav 1); 34) ne da podatke o identitetu potpisnika državnom organu koji je zakonom ovlašćen za njihovo prikupljanje i obradu, na njegov zahtjev (član 57 stav 4).			

	Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom od 150 eura do 2 000 eura. Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u organu vlasti novčanom kaznom od 150 eura do 2 000 eura. Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom od 150 do 1000 eura. " **Član 31** U članu 71 stav 3 riječi: „državnom organu" zamjenjuju se riječima: „organu vlasti". St. 4, 5 i 6 brišu se. **Član 6** U članu 72 stav 1 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.			
ODSJEK 2 ***Nadzor*** ***Član 17*** **Nadzorni organ** 1. Države članice imenuju nadzorni organ osnovan na njihovoj teritoriji ili, prema uzajamnom dogovoru s drugom državom članicom, nadzorni organ osnovan u toj drugoj državi članici. Taj organ je odgovoran za zadatke nadzora u državi članici koja ga imenuje. Nadzornim organima dodjeljuju se potrebna ovlašćenja i odgovarajuća sredstva za ostvarivanje njihovih zadataka. 2. Države članice obavještavaju Komisiju i druge države članice o nazivima i adresama svojih nadzornih organa koje su imenovale. 3. Uloga nadzornog organa je sljedeća: (a) da nadzire kvalifikovane davaoce usluga povjerenja osnovan na teritoriji države članice koja ga imenuje kako bi se obezbijedilo, putem prethodnih (ex ante) i naknadnih (ex post) aktivnosti nadzora, da ti kvalifikovani davaoci usluga povjerenja i kvalifikovane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj regulativi;	**Član 29** U članu 68 stav 2 mijenja se i glasi: „Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom."	Potpuno usklađeno	Potpuno usklađeno i članovima 68 i 69 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(b) da, prema potrebi, preduzima mjere u odnosu na nekvalifikovane davaoce usluga povjerenja osnovane na teritoriji države članice koja ga imenuje, putem naknadnih (ex post) aktivnosti nadzora, kada primi obavještenje da ti nekvalifikovani davaoci usluga povjerenja ili usluge povjerenja koje oni pružaju navodno ne ispunjavaju zahtjeve utvrđene u ovoj regulativi.				
4. Za potrebe stava 3 i podložno u njemu predviđenim ograničenjima, zadaci nadzornog organa naročito uključuju: (a) saradnju s drugim nadzornim organima i pružanje pomoći tim organima u skladu s članom 18; (b) analiziranje izvještajâ o ocjenjivanju usaglašenosti iz člana 20 stav 1 i člana 21 stav 1; (c) obavještavanje drugih nadzornih organa i javnosti o povredama sigurnosti ili gubitku integriteta u skladu s članom 19 stav 2; (d) izvještavanje Komisije o svojim glavnim aktivnostima u skladu sa stavom 6 ovog člana; (e) sprovođenje revizija ili zahtijevanje od organa za ocjenjivanje usaglašenosti da sprovode ocjenjivanje usaglašenosti kvalifikovanih davalaca usluga povjerenja u skladu s članom 20 stav 2;				
(f) saradnja s organima za zaštitu podataka, a naročito njihovim obavještavanjem, bez odlaganja, o rezultatima revizija kvalifikovanih davalaca usluga povjerenja, u slučaju kada se čini da je došlo do povrede pravila o zaštiti ličnih podataka; (g) dodjeljivanje kvalifikovanog statusa davaocima usluga povjerenja i uslugama koje oni pružaju i ukidanje tog statusa u skladu s čl. 20 i 21; (h) obavještavanje organa odgovornog za domaću pouzdanu listu iz člana 22 stav 3 o odlukama o dodjeljivanju ili ukidanju kvalifikovanog statusa, osim ako je taj organ istovremeno i nadzorni organ;				
(i) provjeravanje postojanja i pravilne primjene odredaba o planovima prekida u slučajevima kada kvalifikovani davalac usluga povjerenja prekine svoje aktivnosti,				

uključujući način na koji se održava dostupnost informacija u skladu s članom 24 stav 2 tačka h; (j) zahtijevanje od davalaca usluga povjerenja da otklone svako nepoštovanje zahtjeva utvrđenih u ovoj regulativi. 5. Države članice mogu od nadzornog organa da zahtijevaju da uspostavi, održava i ažurira infrastrukturu povjerenja u skladu s uslovima na osnovu domaćeg prava. 6. Do 31. marta svake godine, svaki nadzorni organ podnosi Komisiji izvještaj o svojim glavnim aktivnostima u prethodnoj kalendarskoj godini, zajedno s kratkim pregledom notifikacija o povredama koje je primio od davalaca usluga povjerenja u skladu s članom 19 stav 2. 7. Komisija stavlja na raspolaganje državama članicama godišnji izvještaj iz stava 6. 8. Komisija može aktima za sprovođenje da utvrdi oblike i procedure za izvještaj iz stava 6. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 18 **Uzajamna pomoć** 1. Nadzorni organi sarađuju s ciljem razmjene dobre prakse. Nadzorni organ, po prijemu obrazloženog zahtjeva drugog nadzornog organa, tom organu pruža pomoć kako bi se aktivnosti nadzornih organa mogle sprovoditi na dosljedan način. Uzajamna pomoć može naročito obuhvatati zahtjeve za informacijama i nadzorne mjere, kao što su zahtjevi za sprovođenje kontrola koje se odnose na izvještaje o ocjenjivanju usaglašenosti, kako je navedeno u čl. 20 i 21. 2. Nadzorni organ kojem je upućen zahtjev za pomoć može odbiti taj zahtjev zbog bilo kojeg od sljedećih razloga: (nadzorni organ nije nadležan za pružanje tražene a pomoći;) (b) tražena pomoć nije srazmjerna aktivnostima nadzora nadzornog organa koje se sprovode u skladu s članom 17;	**Član 24** U članu 62 stav 1 tačka 1 riječi: „evidenciju i registar" zamjenjuju se riječima: „registar sistema elektronske identifikacije".	Potpuno usklađeno	Potpuno usklađeno članom 62 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(pružanje tražene pomoći ne bi bilo u skladu s ovom c regulativom.) 3. Prema potrebi, države-članice mogu da ovlaste svoje nadzorne organe da sprovode zajedničke istrage u kojima učestvuje osoblje nadzornih organa iz drugih država članica. Dogovore i postupke za takva zajednička djelovanja dogovaraju i uspostavljaju odnosne države članice u skladu sa svojim domaćim pravima.				
Član 19 **Sigurnosni zahtjevi koji se primjenjuju na davaoce usluga povjerenja** 1. Kvalifikovani i nekvalifikovani davaoci usluga povjerenja preduzimaju odgovarajuće tehničke i organizacione mjere za upravljanje rizicima koji prijete sigurnosti usluga povjerenja koje oni pružaju. Imajući u vidu najnovija tehnološka rješenja, tim mjerama se obezbjeđuje da stepen sigurnosti odgovara stepenu rizika. Naročito se preduzimaju mjere za sprečavanje i smanjivanje uticaja sigurnosnih incidenata i za obavještavanje aktera o neželjenim uticajima bilo kakvih incidenata te vrste. 2. Kvalifikovani i nekvalifikovani davaoci usluga povjerenja obavještavaju nadzorni organ bez odlaganja, ali u svakom slučaju u roku od 24 sata od saznanja, i, prema potrebi, druge odgovarajuće organe, kao što su nadležni državni organ za sigurnost informacija ili organ za zaštitu podataka, o svakoj povredi sigurnosti ili gubitku integriteta koji imaju značajan uticaj na pruženu uslugu povjerenja ili u njoj sadržane lične podatke. Ako je vjerovatno da bi povreda sigurnosti ili gubitak integriteta mogli nepovoljno da utiču na fizičko ili pravno lice kojem su pružene usluge povjerenja, davalac usluga povjerenja o povredi ili gubitku integriteta bez odlaganja obavještava i fizičko ili pravno lice. Prema potrebi, naročito ako se povreda sigurnosti ili gubitak integriteta odnosi na dvije države-članice ili više njih, notifikovani nadzorni organ obavještava nadzorne organe u drugim državama članicama na koje se to odnosi i ENISA-u.	**Član 6** U članu 58 st. 1, 2, 3, 5 i 6 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno i članom 58 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

Notifikovani nadzorni organ obavještava javnost ili zahtijeva od davaoca usluga povjerenja da to učini ako utvrdi da je otkrivanje povrede sigurnosti ili gubitka integriteta u javnom interesu. 3. Nadzorni organ jednom godišnje dostavlja ENISA-i kratak pregled notifikacija o povredi sigurnosti i gubitku integriteta koje je primio od davalaca usluga povjerenja. 4. Komisija može aktima za sprovođenje: (a dalje da precizira mjere iz stava 1; i) (b) da definiše oblike i procedure, uključujući rokove, koji važe za potrebe stava 2. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
ODSJEK 3 ***Kvalifikovane usluge povjerenja*** ***Član 20*** Nadzor kvalifikovanih davalaca usluga povjerenja 1. Organ za ocjenjivanje usaglašenosti vrši reviziju davalaca kvalifikovanih usluga povjerenja o njihovom trošku i najmanje svaka 24 mjeseca. Svrha revizija sastoji se u potvrđivanju da kvalifikovani davaoci usluga povjerenja i kvalifikovane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj regulativi. Kvalifikovani davaoci usluga povjerenja nadzornom organu podnose izvještaj o ocjenjivanju usaglašenosti u roku od tri radna dana od njegovog prijema. 2. Ne dovodeći u pitanje stav 1, nadzorni organ može u bilo kojem trenutku da izvrši reviziju ili zahtijeva od organa za ocjenjivanje usaglašenosti da sprovedu ocjenjivanje usaglašenosti davalaca kvalifikovanih usluga povjerenja, o trošku tih davalaca usluga povjerenja, kako bi se potvrdilo da davaoci usluga povjerenja i kvalifikovane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj regulativi. U slučaju kada se čini da je došlo do povrede pravila o zaštiti ličnih podataka, nadzorni organ obavještava organ za zaštitu podataka o rezultatima svojih revizija. 3. U slučaju kada nadzorni organ zahtijeva od davaoca kvalifikovanih usluga povjerenja da otkloni bilo kakvo	**Član 29** U članu 68 stav 2 mijenja se i glasi: „Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i ovim zakonom.”	Potpuno usklađeno	Potpuno usklađeno i članovima 68 i 69 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG“, broj 31/17)	

nepoštovanje zahtjeva u skladu s ovom regulativom i kada davalac usluge ne postupi u skladu s tim zahtjevom, i ako je to primjenljivo i u roku koji odredi nadzorni organ, nadzorni organ može, naročito uzimajući u obzir obim, trajanje i posljedice tog nepoštovanja, da ukine kvalifikovani status tog davaoca usluge ili obuhvaćene usluge koje on pruža i može za potrebe ažuriranja pouzdanih lista iz člana 22 stav 1 da obavijesti organ iz člana 22 stav 3. Nadzorni organ obavještava kvalifikovanog davaoca usluga povjerenja o ukidanju njegovog kvalifikovanog statusa ili kvalifikovanog statusa odnosne usluge. 4. Komisija može aktima za sprovođenje da utvrdi referentne brojeve sljedećih standarda: (a) akreditacije organa za ocjenu usaglašenosti i za izvještaj o ocjenjivanju usaglašenosti iz stava 1; (b) pravila revizije prema kojim će organi za ocjenjivanje usaglašenosti sprovoditi ocjenjivanje usaglašenosti kvalifikovanih davalaca usluga povjerenja kako je navedeno u stavu 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 21 Početak pružanja kvalifikovane usluge povjerenja 1. Ako davaoci usluga povjerenja bez kvalifikovanog statusa namjeravaju da započnu pružanje kvalifikovanih usluga povjerenja, oni nadzornom organu podnose notifikaciju o svojoj namjeri zajedno s izvještajem o ocjenjivanju usaglašenosti koji je izdao organ za ocjenjivanje usaglašenosti. 2. Nadzorni organ provjerava da li je davalac usluga povjerenja usaglašen odnosno da li su usluge povjerenja koje on pruža usaglašene sa zahtjevima utvrđenim u ovoj regulativi a naročito sa zahtjevima za kvalifikovane davaoce usluga povjerenja i za kvalifikovane usluge povjerenja koje oni pružaju. Ako nadzorni organ zaključi da su davalac usluga povjerenja i usluge povjerenja koje on pruža usklađeni sa zahtjevima iz podstava 1, nadzorni organ odobrava kvalifikovani status davaocu usluga povjerenja i uslugama	**Član 15** **Član 39 mijenja se i glasi:** „Rješenje o ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja Davalac elektronskih usluga povjerenja koji je upisan u evidenciju može podnijeti zahtjev za upis u registar kvalifikovanih davalaca elektronskih usluga povjerenja (u daljem tekstu: registar), koji vodi Ministarstvo. Uz zahtjev iz stava 1 ovog člana, davalac elektronskih usluga povjerenja dužan je da priloži dokumentaciju kojom dokazuje da ispunjava uslove iz člana 34 ovog zakona. O ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja propisanih ovim zakonom Ministarstvo donosi rješenje, na osnovu uvida u priloženu dokumentaciju	Potpuno usklađeno	Potpuno usklađeno i članom 41 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

povjerenja koje on pruža i obavještava organ iz člana 22 stav 3 u svrhu ažuriranja pouzdanih lista iz člana 22 stav 1, najkasnije tri mjeseca nakon notifikacije u skladu sa stavom 1 ovog člana. Ako verifikacija nije izvršena u roku od tri mjeseca od notifikacije, nadzorni organ o tome obavještava davaoca usluga povjerenja, navodeći razloge za kašnjenje i rok do kojeg verifikacija mora biti izvršena. 3. Davaoci kvalifikovanih usluga povjerenja mogu da započnu pružanje kvalifikovane usluge povjerenja nakon što kvalifikovani status bude naznačen u pouzdanim listama iz člana 22 stav 1. 4. Komisija može aktima za sprovođenje da utvrdi oblike i procedure za potrebe st. 1 i 2. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	iz stava 1 ovog člana i, po potrebi, na osnovu neposrednog uvida. Rješenje iz stava 3 ovog člana donosi se, u roku od 15 dana od dana podnošenja urednog zahtjeva." **Član 6** U članu 41 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.			
Član 22 **Pouzdane liste** 1. Svaka država članica izrađuje, vodi i objavljuje pouzdane liste, uključujući informacije o kvalifikovanim davaocima usluga povjerenja za koje je ta država članica odgovorna, zajedno s informacijama o kvalifikovanim uslugama povjerenja koje oni pružaju. 2. Države članice u obliku pogodnom za automatizovanu obradu i na siguran način sastavljaju, vode i objavljuju elektronski potpisane ili pečatirane pouzdane liste iz stava 1. 3. Države članice bez odlaganja obavještavaju Komisiju o podacima o organu odgovornom za izradu, vođenje i objavljivanje domaćih pouzdanih lista i pojedinostima o tome gdje se takve liste objavljuju, certifikatima korišćenim za potpisivanje ili pečatiranje pouzdanih lista i svim njihovim izmjenama. 4. Komisija stavlja na raspolaganje javnosti informacije iz stava 3 na siguran način, u elektronski potpisanom ili pečatiranom formatu pogodnom za automatsku obradu. 5. Do 18. septembra 2015. godine, Komisija putem akata za sprovođenje navodi informacije iz stava 1 i utvrđuje tehničke specifikacije i formate za pouzdane liste koje se primjenjuju za potrebe st. 1 do 4. Ovi akti za sprovođenje	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članovima 21 i 22 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 23 **Oznaka povjerenja EU za kvalifikovane usluge povjerenja** 1. Nakon što je kvalifikovani status iz člana 21 stav 2 podstav 2 naznačen na listi davalaca usluga povjerenja iz člana 22 stav 1, davaoci kvalifikovanih usluga povjerenja mogu da koriste oznaku povjerenja EU kako bi na jednostavan, prepoznatljiv i jasan način naznačili kvalifikovane usluge povjerenja koje pružaju. 2. Prilikom korišćenja oznake povjerenja EU za kvalifikovane usluge povjerenja iz stava 1, kvalifikovani davaoci usluga povjerenja obezbjeđuju da je na njihovim internet stranicama dostupan link za odgovarajuću listu davalaca usluga povjerenja. 3. Komisija do 1. jula 2015. godine, aktima za sprovođenje propisuje specifikacije u odnosu na oblik i naročito izgled, sastav, veličinu i dizajn oznake povjerenja EU za kvalifikovane usluge povjerenja. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	**Član 6** U članu 43 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 43 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 24 **Zahtjevi u vezi s kvalifikovanim davaocima usluga povjerenja** 1. Prilikom izdavanja kvalifikovanog certifikata za uslugu povjerenja kvalifikovani davalac usluga povjerenja provjerava, na odgovarajući način i u skladu s domaćim pravom, identitet i, ako je to primjenljivo, posebne karakteristike fizičkog ili pravnog lica kojem se izdaje kvalifikovani certifikat. Informacije iz podstava 1 provjerava kvalifikovani davalac usluga povjerenja bilo neposredno ili oslanjajući se na treće lice u skladu s domaćim pravom: (a) fizičkim prisustvom fizičkog lica ili ovlašćenog predstavnika pravnog lica; ili (b) na daljinu, pomoću sredstava elektronske identifikacije, za koja je prije izdavanja kvalifikovanog certifikata obezbijeđeno fizičko prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica i koje ispunjava	**Član 12** **Član 34 mijenja se i glasi:** **„Uslovi u vezi sa kvalifikovanim davaocima elektronske usluge povjerenja** Kvalifikovani davalac elektronske usluge povjerenja mora da ispunjava sljedeće uslove, i to da: 1) ima ažuriran plan prekida pružanja elektronske usluge povjerenja radi obezbjeđivanja njenog kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona; 2) obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti; 3) obezbijedi, na odgovarajući način i u skladu sa ovim zakonom i internim aktima iz člana 37 stav 4 ovog zakona, provjeru identiteta potpisnika i, po potrebi, drugog obilježja fizičkog i pravnog lica, kojima se izdaje kvalifikovani certifikat za elektronski potpis, odnosno kvalifikovani certifikat za elektronski pečat;	Potpuno usklađeno	Potpuno usklađeno i članovima 49, 50, 51, 53, 54, 55 i 57 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

zahtjeve utvrđene u članu 8 u pogledu „značajnog" ili „visokog" stepena sigurnosti; ili (c) pomoću certifikata kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata izdatog u skladu s tačkom a ili b; ili (d) pomoću drugih metoda identifikacije priznatih na državnom nivou koja po pitanju pouzdanosti obezbjeđuju sigurnost jednaku fizičkom prisustvu. Jednaku sigurnost potvrđuje organ za ocjenjivanje usaglašenosti. 2. Kvalifikovani davalac usluga povjerenja: (a) obavještava nadzorni organ o svim promjenama u vezi s pružanjem svojih kvalifikovanih usluga povjerenja i o namjeri prestanka obavljanja te djelatnosti; (b) zapošljava osoblje i, ako je to primjenljivo, podizvođače koji posjeduju potrebno stručno znanje, pouzdanost, iskustvo i kvalifikacije i koji su prošli odgovarajuće obuke u vezi s sigurnošću i propisima o zaštiti ličnih podataka i primjenjuju upravne i upravljačke postupke u skladu s evropskim ili međunarodnim standardima; (c) u pogledu rizika od odgovornosti za štetu u skladu s članom 13, raspolaže dovoljnim finansijskim sredstvima i/ili je pribavio odgovarajuće osiguranje od odgovornosti, u skladu s domaćim pravom; (d) prije stupanja u ugovorni odnos, obavještava, na jasan i sveobuhvatan način, svako lice koje želi da koristi kvalifikovanu uslugu povjerenja o tačnim uslovima korišćenja te usluge, uključujući bilo kakva ograničenja korišćenja; (e) koristi pouzdane sisteme i proizvode koji su zaštićeni od izmjena i obezbjeđuju tehničku sigurnost i pouzdanost postupaka koje ti sistemi i proizvodi podržavaju; (f) koristi pouzdane sisteme za čuvanje podataka koji su mu dostavljeni, u obliku koji se može provjeriti, kako bi: i. ti podaci bili javno dostupni za pronalaženje samo uz pristanak lica na koje se ti podaci odnose; ii. samo ovlašćena lica mogu da unose nove podatke u sačuvane podatke i da ih mijenjaju; iii. se mogla provjeriti autentičnost podataka;	4) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje elektronskih usluga povjerenja, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka; 5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa; 6) preduzima mjere za sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja certifikate potpisnicima na bezbjedan način; 7) posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih certifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete; 8) posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih certifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa; 9) koristi pouzdan sistem čuvanja kvalifikovanih certifikata u obliku koji omogućava provjeru, kako bi: - unos i promjene podataka prilikom pružanja elektronske usluge povjerenja vršila samo ovlašćena lica, - mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata,			

(g) preduzima odgovarajuće mjere protiv krivotvorenja i krađe podataka; (h) evidentira i čini dostupnim u toku odgovarajućeg perioda, uključujući period nakon prestanka obavljanja djelatnosti kvalifikovanog davaoca usluga povjerenja, sve bitne informacije u vezi s podacima koje izdaje i prima kvalifikovani davalac usluga povjerenja, a naročito za potrebe predlaganja dokaza u sudskim postupcima i u svrhu obezbjeđenja kontinuiteta usluge. Takvo evidentiranje može se obavljati elektronskim putem; (i) ima ažuriran plan prekida pružanja usluge radi obezbjeđenja njenog kontinuiteta u skladu s odredbama koje je potvrdio nadzorni organ iz člana 17 stav 4 tačka i; (j) obezbjeđuje zakonitu obradu ličnih podataka u skladu s Direktivom 95/46/EZ; (k) ako je riječ o kvalifikovanim davaocima usluga povjerenja koji izdaju kvalifikovane certifikate, uspostavlja i ažurira bazu podataka certifikata. 3. Ako kvalifikovani davalac usluga povjerenja koji izdaje kvalifikovane certifikate odluči da opozove certifikat, on registruje opoziv certifikata u svojoj bazi podataka certifikata i blagovremeno objavljuje status opoziva certifikata, a u svakom slučaju unutar 24 sata nakon prijema zahtjeva. Opoziv stupa na snagu odmah nakon njegovog objavljivanja. 4. Imajući u vidu stav 3, kvalifikovani davaoci usluga povjerenja koji izdaju kvalifikovane certifikate pružaju bilo kojoj strani korisnici informacije o statusu validnosti ili opoziva kvalifikovanih certifikata koje su izdali. Te informacije moraju biti dostupne barem za pojedinačne certifikate, u svakom trenutku i nakon isteka perioda validnosti certifikata, na automatizovan način koji je pouzdan, besplatan i djelotvoran. 5. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za pouzdane sisteme i proizvode koji ispunjavaju zahtjeve u skladu sa stavom 2 tač. e i f ovog člana. Ako pouzdani sistemi i proizvodi zadovoljavaju te standarde, smatra se da su ispunjeni zahtjevi iz ovog člana. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	- podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje, - bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve, bila vidljiva kvalifikovanom davaocu elektronske usluge povjerenja. Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo." **Član 18** U nazivu člana 49 i uvodnoj rečenici stava 1 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. U stavu 1 tač. 2 i 3 mijenjaju se i glase: „2) sprovede potpunu provjeru identiteta fizičkog lica, pravnog lica, odnosno organa vlasti kojem se izdaje kvalifikovani certifikat; 3) o izdatim kvalifikovanim certifikatima vodi evidenciju i obezbijedi tačnost i cjelovitost podataka koji se unose u tu evidenciju;" Poslije stava 1 dodaju se tri nova stava koji glase: „Provjeru identiteta iz stava 1 tačka 2 ovog člana, kvalifikovani davalac elektronske usluge povjerenja vrši dobijanjem podataka na osnovu kojih se vrši provjera neposredno od fizičkog lica ili ovlašćenog predstavnika pravnog lica ili organa vlasti ili od drugog lica. Provjera identiteta iz stava 1 tačka 2 ovog člana vrši se na neki od sljedećih načina: 1) uz prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica ili organa vlasti; 2) na daljinu, pomoću sredstava elektronske identifikacije, za koja je prije izdavanja kvalifikovanog certifikata obezbijeđeno prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica, ili organa vlasti i ako sistem za elektronsku identifikaciju iz kojeg su izdata ta sredstva ispunjavaju zahtjeve iz člana 60			

	ovog zakona u pogledu stepena sigurnosti „značajan" ili „visok"; 3) pomoću certifikata kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata, koji je izdat uz provjeru na način iz tačke 1 ili tačke 2 ovog stava; ili 4) primjenom drugih metoda identifikacije koje u pogledu pouzdanosti pružaju sigurnost provjere identiteta jednaku provjeri identiteta na osnovu fizičkog prisustva. Prije primjene metoda iz stava 3 tačka 4 ovog člana kvalifikovani davalac elektronskih usluga povjerenja dužan je da pribavi saglasnost Ministarstva za primjenu te metode." U stavu 2 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja". Dosadašnji stav 2 postaje stav 5. **Član 6** U članu 50 stav 1 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima:„elektronske usluge povjerenja" u odgovarajućem padežu.			
	Član 19 U članu 51 u uvodnoj rečenici stava 1 i u tački 5 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja", a u tački 6 riječi: „usluge certifikovanja" zamjenjuju se riječima: „elektronske usluge povjerenja". Stav 2 mijenja se i glasi: "Davalac elektronskih usluga povjerenja dužan je da na svojoj internet straniči objavi listu opozvanih certifikata, a opoziv certifikata proizvodi dejstvo od trenutka objavljivanja ove liste." U stavu 3 riječi: „usluga certifikovanja za elektronske transakcije" zamjenjuju se riječima: „elektronskih usluga povjerenja". St. 4 i 5 mijenjaju se i glase:			

	„Datum i vrijeme suspenzije i opoziva certifikata unose se u evidenciju iz člana 49 stav 1 tačka 5 ovog zakona. Davalac elektronskih usluga povjerenja dužan je da obavijesti potpisnika, odnosno autora elektronskog pečata o suspenziji ili opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti iz stava 1 ovog člana."			
	Član 6 U članu 53 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. **Član 6** U članu 54 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. **Član 6** U članu 55 stav 1 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. **Član 6** U članu 57 st. 1, 3, 4 i 5 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.			
ODSJEK 4 **Elektronski potpisi** **Član 25** **Pravna dejstva elektronskih potpisa** 1. Elektronskom potpisu kao dokazu u sudskim postupcima ne smije biti uskraćeno pravno dejstvo i prihvatljivost samo zbog toga što je u elektronskom obliku ili zbog toga što ne zadovoljava sve zahtjeve za kvalifikovani elektronski potpis.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članovima 12, 13 i 14 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

2. Kvalifikovani elektronski potpis ima jednako pravno dejstvo kao svojeručni potpis. 3. Kvalifikovani elektronski potpis koji je zasnovan na kvalifikovanom certifikatu izdatom u jednoj državi članici priznaje se kao kvalifikovani elektronski potpis u svim ostalim državama članicama.				
Član 26 **Zahtjevi za napredne elektronske potpise** Napredni elektronski potpis mora da ispunjava sljedeće zahtjeve: (povezan je s potpisnikom na jedinstven način; a) (omogućava identifikaciju potpisnika; b) (c) izrađen je korišćenjem podataka za izradu elektronskog potpisa koje potpisnik može, uz visok stepen povjerenja, da koristi pod svojom isključivom kontrolom; i (d) povezan je s potpisanim podacima na takav način da se može otkriti bilo koja naknadna izmjena podataka.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 10 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 27 **Elektronski potpisi u javnim službama** 1. Ako država članica zahtijeva napredni elektronski potpis za korišćenje usluge na internetu koju nudi organ javnog sektora ili usluge koja se nudi u ime organa javnog sektora, ta država članica priznaje napredne elektronske potpise, napredne elektronske potpise koji se zasnivaju na kvalifikovanom certifikatu za elektronske potpise i kvalifikovane elektronske potpise barem u formatima ili korišćenjem metoda koji su definisane u aktima za sprovođenje iz stava 5. 2. Ako država članica zahtijeva napredni elektronski potpis koji se zasniva na kvalifikovanom certifikatu za korišćenje usluge na internetu koju nudi organ javnog sektora ili usluge koja se nudi u ime organa javnog sektora, ta država članica priznaje napredne elektronske potpise koji se zasnivaju na kvalifikovanom certifikatu i kvalifikovane elektronske potpise barem u formatima ili korišćenjem	**Član 6** U članu 36 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu	Potpuno usklađeno	Potpuno usklađeno članovima 14 i 36 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

metoda koje su definisane u aktima za sprovođenje iz stava 5. 3. Za prekograničnо korišćenje usluge na internetu koju nudi organ javnog sektora države članice ne zahtijevaju elektronski potpis čiji je stepen sigurnosti viši od kvalifikovanog elektronskog potpisa. 4. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za napredne elektronske potpise. Ako napredni elektronski potpis zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima za napredne elektronske potpise iz st. 1 i 2 ovog člana i člana 26. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2. 5. Komisija, imajući u vidu postojeću praksu, standarde i pravne akte Unije, putem akata za sprovođenje, do 18. septembra 2015. godine utvrđuje referentne formate naprednih elektronskih potpisa ili referentne metode ako se koriste alternativni formati. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 28 **Kvalifikovani certifikati za elektronske potpise** 1. Kvalifikovani certifikati za elektronske potpise moraju da ispune zahtjeve utvrđene u Aneksu I. 2. Kvalifikovani certifikati za elektronske potpise ne smiju da podliježu obaveznim zahtjevima koji prelaze zahtjeve utvrđene u Aneksu I. 3. Kvalifikovani certifikati za elektronske potpise mogu da uključuju dodatne posebne karakteristike koje nijesu obavezne. Te karakteristike ne utiču na interoperabilnost i priznavanje kvalifikovanih elektronskih potpisa. 4. Ako je kvalifikovani certifikat za elektronske potpise opozvan nakon početne aktivacije, on gubi validnost od trenutka opoziva i njegov status se ni u kojem slučaju ne može vratiti u prethodno stanje. 5. Države članice mogu da utvrde domaća pravila o privremenoj suspenziji kvalifikovanih certifikata za elektronski potpis u skladu sa sljedećim uslovima:	**Član 17** **Član 16 mijenja se i glasi:** „Kvalifikovani certifikat za elektronski potpis je certifikat koji izdaje kvalifikovani davalac elektronske usluge povjerenja, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona i koji sadrži: 1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis u obliku prikladnom za automatsku obradu podataka; 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za elektronski potpis, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj; - fizičko lice: ime i prezime i poreski identifikacioni broj;	Potpuno usklađeno	Potpuno usklađeno i i članom 17 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(a) ako je kvalifikovani certifikat za elektronski potpis privremeno suspendovan, taj certifikat gubi validnost u toku perioda suspenzije; (b) period suspenzije jasno je naznačen u bazi podataka certifikata, a status suspenzije je tokom perioda suspenzije vidljiv iz usluge u okviru koje se pružaju informacije o statusu certifikata. 6. Komisija može aktima za sprovođenje utvrditi referentne brojeve standarda za kvalifikovane certifikate za elektronski potpis. Ako kvalifikovani certifikat za elektronski potpis zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u Aneksu I. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	3) skup identifikacioni podataka o potpisniku (ime i prezime ili pseudonim) koji, ako se koristi, mora biti jasno naznačen; 4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa i koji su pod kontrolom potpisnika; 5) podatke o periodu važenja tog certifikata; 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za elektronski potpis koja mora biti jedinstvena za kvalifikovanog davaoca elektronskih usluga povjerenja; 7) napredni elektronski potpis kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje taj certifikat; 8) lokaciju na kojoj je besplatno dostupan taj certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronskih usluga povjerenja; 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti tog certifikata; 10) odgovarajuću naznaku, u obliku pogodnom za automatsku obradu podataka, ako se podaci za izradu elektronskog potpisa koji su povezani sa podacima za verifikaciju elektronskog potpisa nalaze u kvalifikovanom sredstvu za izradu elektronskog potpisa. Kvalifikovani certifikat 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."			
Član 29 **Zahtjevi za kvalifikovana sredstva za izradu elektronskih potpisa** 1. Kvalifikovana sredstva za izradu elektronskih potpisa moraju da ispune zahtjeve utvrđene u Aneksu II. 2. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za kvalifikovana sredstva za izradu elektronskih potpisa. Ako kvalifikovano sredstvo za izradu elektronskog potpisa zadovoljava te standarde,	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 19 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u Aneksu II. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 30 **Certifikovanje kvalifikovanih sredstava za izradu elektronskih potpisa** 1. Usaglašenost kvalifikovanih sredstava za izradu elektronskih potpisa sa zahtjevima utvrđenim u Aneksu II potvrđuju odgovarajući javni ili privatni organi koje imenuju države članice. 2. Države članice obavještavaju Komisiju o nazivima i adresama javnih ili privatnih organa iz stava 1. Komisija stavlja te informacije na raspolaganje državama članicama. 3. Certifikacija iz stava 1 zasniva se na jednom od sljedećeg: (a) postupku evaluacije sigurnosti u skladu s jednim od standarda za ocjenu sigurnosti proizvoda informacione tehnologije uključenih na listu sastavljenu u skladu s podstavom 2; ili (b) postupku različitom od postupka iz tačke a, pod uslovom da on koristi uporedive stepene sigurnosti i pod uslovom da javni ili privatni organ iz stava 1 obavijesti Komisiju o tom postupku. Taj postupak se može koristiti samo u slučaju nepostojanja standarda navedenih u tački a ili kada je postupak evaluacije sigurnosti iz tačke a u toku. Komisija aktima za sprovođenje utvrđuje listu standarda za ocjenu sigurnosti proizvoda informacione tehnologije iz tačke a. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2. 4. Komisija je ovlašćena da donosi delegirane akte u skladu s članom 47, u vezi s utvrđivanjem posebnih kriterijuma koje moraju ispuniti organi iz stava 1 ovog člana koji su imenovani.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 21 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 31 **Objavljivanje liste certifikovanih kvalifikovanih sredstava za izradu elektronskog potpisa** 1. Države članice obavještavaju Komisiju, bez odlaganja, a najkasnije u roku od mjesec dana nakon završetka certifikacije, o informacijama o sredstvima za izradu kvalifikovanog elektronskog potpisa koja su certifikovali organi iz člana 30 stav 1. One obavještavaju i Komisiju, bez	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 22 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

odlaganja, a najkasnije u roku od mjesec dana nakon poništenja certifikacije, o informacijama o sredstvima za izradu elektronskog potpisa koja više nijesu certifikovana. 2. Na osnovu primljenih informacija Komisija izrađuje, objavljuje i vodi listu certifikovanih kvalifikovanih sredstava za izradu elektronskog potpisa. 3. Komisija može aktima za sprovođenje da utvrdi važeće formate i postupke za potrebe stava 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stava 2.				
Član 32 **Zahtjevi za validaciju kvalifikovanih elektronskih potpisa** 1. Postupkom validacije kvalifikovanog elektronskog potpisa potvrđuje se validnost kvalifikovanog elektronskog potpisa pod sljedećim uslovima: (a) certifikat koji podržava potpis je u trenutku potpisivanja bio kvalifikovani certifikat za elektronski potpis koji je u skladu s Aneksom I; (b) kvalifikovani certQifikat izdao je kvalifikovani davalac usluga povjerenja i bio je validan u trenutku potpisivanja; (c) podaci za validaciju potpisa odgovaraju podacima koji se pružaju strani korisnici; (d) jedinstveni skup podataka koji predstavlja potpisnika u certifikatu ispravno je dostavljen strani korisnici; (e) korišćenje pseudonima, ako je pseudonim bio korišćen u trenutku potpisivanja, jasno je naznačeno strani korisnici; (f) elektronski potpis izrađen je sredstvom za izradu kvalifikovanog elektronskog potpisa; (g) nije ugrožen integritet potpisanih podataka; (h) zahtjevi predviđeni u članu 26 bili su ispunjeni u trenutku potpisivanja. 2. Sistem koji se upotrebljava za potvrđivanje kvalifikovanog elektronskog potpisa obezbjeđuje strani korisnici tačan rezultat postupka validacije i omogućava joj otkrivanje svih poteškoća bitnih za sigurnost. 3. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za validaciju kvalifikovanih	Član 6 U članu 23 stav 1 tačka 2 i stav 3, riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 23 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

elektronskih potpisa. Ako validacija kvalifikovanih elektronskih potpisa zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u stavu 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.				
Član 33 **Kvalifikovana usluga validacije za kvalifikovane elektronske potpise** 1. Kvalifikovanu uslugu validacije kvalifikovanih elektronskih potpisa može pružati samo kvalifikovani davalac usluga povjerenja koji: (pruža validaciju u skladu s članom 32 stav 1; i a) (b) omogućava stranama korisnicama da dobiju rezultate postupka validacije na automatizovani način koji je pouzdan, djelotvoran i nosi napredan elektronski potpis ili napredan elektronski pečat kvalifikovanog davaoca usluge validacije. 2. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za kvalifikovanu uslugu validacije iz stava 1. Ako usluga validacije kvalifikovanih elektronskih potpisa zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u stavu 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	**Član 6** U članu 23 stav 1 tačka 2 i stav 3, riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno članom 23 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Član 34 **Kvalifikovana usluga čuvanja kvalifikovanih elektronskih potpisa** 1. 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 tehnološkog roka važenja. 2. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za kvalifikovanu uslugu čuvanja kvalifikovanih elektronskih potpisa. Ako dogovori za kvalifikovanu uslugu čuvanja kvalifikovanih elektronskih potpisa zadovoljavaju te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u stavu	**Član 24** U članu 24 stav 1 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu. **Član 12** **Član 34 mijenja se i glasi:** **„Uslovi u vezi sa kvalifikovanim davaocima elektronske usluge povjerenja** Kvalifikovani davalac elektronske usluge povjerenja mora da ispunjava sljedeće uslove, i to da: 1) ima ažuriran plan prekida pružanja elektronske usluge povjerenja radi obezbjeđivanja njenog	Potpuno usklađeno	Potpuno usklađeno članom 24 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	kontinuiteta, koji donosi u skladu sa internim aktima iz člana 37 stav 4 ovog zakona; 2) obezbijedi obradu podataka o ličnosti u skladu sa propisima o zaštiti podataka o ličnosti; 3) obezbijedi, na odgovarajući način i u skladu sa ovim zakonom i internim aktima iz člana 37 stav 4 ovog zakona, provjeru identiteta potpisnika i, po potrebi, drugog obilježja fizičkog i pravnog lica, kojima se izdaje kvalifikovani certifikat za elektronski potpis, odnosno kvalifikovani certifikat za elektronski pečat; 4) ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za pružanje elektronskih usluga povjerenja, a naročito u odnosu na: sposobnosti na upravljačkom nivou, stručnost u primjeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura, zaštitu podataka o ličnosti i primjenu upravnog postupka; 5) koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmjena i koji obezbjeđuju tehničku i kriptografsku sigurnost procesa; 6) preduzima mjere za sprječavanje falsifikovanja certifikata, a u slučajevima u kojima kreira podatke za izradu elektronskog potpisa, garantuje tajnost procesa kreiranja tih podataka i dostavlja certifikate potpisnicima na bezbjedan način; 7) posjeduje finansijska sredstva za osiguranje od rizika i odgovornosti za moguću štetu nastalu izdavanjem kvalifikovanih certifikata, u iznosu koji može pokriti rizik od štete i odgovornosti nastalih korišćenjem kvalifikovanih certifikata koje je izdao, ukoliko za štetu nije odgovoran potpisnik ili je zaključio ugovor o osiguranju od rizika i odgovornosti za tu vrstu štete; 8) posjeduje sistem čuvanja svih relevantnih podataka koji se odnose na kvalifikovane certifikate u određenom vremenskom periodu, a naročito radi davanja tih podataka iz evidencije kvalifikovanih certifikata za potrebe sudskih i drugih pravnih postupaka, pri čemu se ti podaci mogu čuvati i u			

	elektronskom obliku, na način koji omogućava provjeru elektronskih potpisa; 9) koristi pouzdan sistem čuvanja kvalifikovanih certifikata u obliku koji omogućava provjeru, kako bi: - unos i promjene podataka prilikom pružanja elektronske usluge povjerenja vršila samo ovlašćena lica, - mogla biti provjerena autentičnost podataka iz kvalifikovanog certifikata, - podaci bili javno dostupni za pretraživanje na brz i siguran način samo u onim slučajevima za koje je registrovani potpisnik dao odobrenje, - bilo koja tehnička promjena, koja bi mogla narušiti sigurnosne zahtjeve, bila vidljiva kvalifikovanom davaocu elektronske usluge povjerenja. Bliže uslove iz stava 1 ovog člana propisuje Ministarstvo."			
ODSJEK 5 ***Elektronski pečati*** ***Član 35*** **Pravna dejstva elektronskih pečata** 1. Elektronskom pečatu kao dokazu u sudskim postupcima ne smije se uskratiti pravno dejstvo i prihvatljivost samo zbog toga što je on u elektronskom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalifikovani elektronski pečat. 2. Kvalifikovani elektronski pečat uživa pretpostavku integriteta podataka i ispravnosti porijekla tih podataka na koji je povezan kvalifikovani elektronski pečat. 3. Kvalifikovani elektronski pečat koji se zasniva na kvalifikovanom certifikatu izdatom u jednoj državi članici priznaje se kao kvalifikovani elektronski pečat u svim ostalim državama članicama. ***Član 36*** **Zahtjevi za napredne elektronske pečate** Napredni elektronski pečat mora zadovoljiti sljedeće zahtjeve:	**Član 9** **Član 27 mijenja se i glasi:** „Na punovažnost, prihvatljivost i pravno dejstvo elektronskog pečata, elektronskog vremenskog pečata, kvalifikovanog elektronskog pečata i kvalifikovanog elektronskog vremenskog pečata, zahtjeve za napredni elektronski pečat, sadržaj i izdavanje certifikata za kvalifikovani elektronski pečat, gubitak validnosti, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata, verifikaciju i čuvanje elektronskog pečata, shodno se primjenjuju odredbe čl. 10, 12, 13, 14 i čl.16 do 24 ovog zakona."	Potpuno usklađeno		

(na jedinstven način je povezan s autorom pečata; a).				
(omogućava identifikaciju autora pečata; b)				
(c) izrađen je korišćenjem podataka za izradu elektronskog pečata koje autor pečata može, uz visok stepen povjerenja i pod svojom kontrolom, koristiti za izradu elektronskog pečata; i				
(d) ezan je s podacima na koje se odnosi na takav način da može otkriti bilo koja naknadna izmjena podataka. ***Član 37*** **Elektronski pečati u javnim službama** ako država članica zahtijeva napredan elektronski pečat korišćenje na internetu usluge koju nudi organ javnog tora ili usluge koja se nudi u ime organa javnog sektora, država članica priznaje napredne elektronske pečate, redne elektronske pečate koji se zasnivaju na lifikovanom certifikatu za elektronske pečate i lifikovane elektronske pečate barem u formatima ili išćenjem metoda koje su definisane u aktima za ovođenje iz stava 5. ako država članica zahtijeva napredan elektronski pečat se zasniva na kvalifikovanom certifikatu za korišćenje internetu usluge koju nudi organ javnog sektora ili uge koja se nudi u ime organa javnog sektora, ta država ica priznaje napredne elektronske pečate koji se nivaju na kvalifikovanom certifikatu i kvalifikovanom ktronskom potpisu barem u formatima ili korišćenjem toda koje su definisane u aktima za sprovođenje iz stava za prekogranično korišćenje na internetu usluge koju li organ javnog sektora države članice ne zahtijevaju ktronski pečat višeg stepena sigurnosti od lifikovanog elektronskog pečata. Komisija može aktima za sprovođenje da utvrdi erentne brojeve standarda za napredne elektronske ate. Ako napredni elektronski pečat zadovoljava te ndarde, smatra se da je postignuta usaglašenost sa				

tjevima za napredne elektronske pečate iz st. 1 i 2 ovog ıa i člana 36. Ovi akti za sprovođenje donose se u skladu ɔstupkom ispitivanja iz člana 48 stav 2. Komisija, uzimajući u obzir postojeću praksu, standarde avne akte Unije, do 18. septembra 2015. godine aktima sprovođenje utvrđuje referentne formate naprednih ‹tronskih pečata ili referentne metode ako se koriste ırnativni formati. Ovi akti za sprovođenje donose se u ıdu s postupkom ispitivanja iz člana 48 stava 2.				
Član 38 **Kvalifikovani certifikati za elektronske pečate** 1. Kvalifikovani certifikati za elektronske pečate moraju zadovoljiti zahtjeve utvrđene u Aneksu III. 2. Kvalifikovani certifikati za elektronske pečate ne smiju da podliježu obaveznim zahtjevima koji prelaze zahtjeve utvrđene u Aneksu III. 3. Kvalifikovani certifikati za elektronske pečate mogu uključivati dodatne posebne karakteristike koje nijesu obavezne. Te karakteristike ne utiču na interoperabilnost i priznavanje kvalifikovanih elektronskih pečata. 4. Ako je kvalifikovani certifikat za elektronski pečat opozvan nakon početne aktivacije, on gubi validnost od trenutka opoziva i njegov status ni u kojem slučaju ne može se vratiti u prethodno stanje. 5. Države članice mogu da utvrde domaća pravila o privremenoj suspenziji kvalifikovanih certifikata za elektronske pečate pod sljedećim uslovima: (a) ako je kvalifikovani certifikat za elektronski pečat privremeno suspendovan, taj certifikat gubi svoju validnost za vrijeme perioda suspenzije; (b) period suspenzije jasno je naznačen u bazi podataka certifikata, a status suspenzije je tokom perioda suspenzije vidljiv iz usluge u okviru koje se pružaju informacije o statusu certifikata.				
Komisija može aktima za sprovođenje da utvrdi ɜrentne brojeve standarda za kvalifikovane certifikate elektronske pečate. Ako kvalifikovani certifikat za ‹tronski pečat zadovoljava te standarde, smatra se da postignuta usaglašenost sa zahtjevima utvrđenim u				

ıksu III. Ovi akti za sprovođenje donose se u skladu s tupkom ispitivanja iz člana 48 stav 2. **Član 39** **Kvalifikovana sredstva za izradu elektronskog pečata** 1. Član 29 primjenjuje se mutatis mutandis na zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata. 2. Član 30 primjenjuje se mutatis mutandis na certifikaciju kvalifikovanih sredstva za izradu elektronskog pečata. 3. Član 31 primjenjuje se mutatis mutandis na objavu liste certifikovanih kvalifikovanih sredstava za izradu elektronskih pečata. **Član 40** **Validacija i čuvanje kvalifikovanih elektronskih pečata** 32, 33 i 34 primjenjuju se mutatis mutandis na validaciju vanje kvalifikovanih elektronskih pečata.				
ODSJEK 6 **Elektronski vremenski pečati** **Član 41** **Pravno dejstvo elektronskih vremenskih pečata** 1. Elektronskom vremenskom pečatu ne smije da bude uskraćeno pravno dejstvo i prihvatljivost kao dokaza u sudskom postupku isključivo na osnovu toga što je u elektronskom obliku ili što ne ispunjava sve uslove za kvalifikovani elektronski vremenski pečat. 2. Kvalifikovani elektronski vremenski pečat uživa pretpostavku o tačnosti datuma i vremena na koje ukazuje i integritet podataka za koje su datum i vrijeme vezani. 3. Kvalifikovani elektronski vremenski pečat izdat u jednoj državi članici priznaje se kao kvalifikovani elektronski vremenski pečat u svim državama članicama.	Član 9 **Član 27 mijenja se i glasi:** „Na punovažnost, prihvatljivost i pravno dejstvo elektronskog pečata, elektronskog vremenskog pečata, kvalifikovanog elektronskog pečata i kvalifikovanog elektronskog vremenskog pečata, zahtjeve za napredni elektronski pečat, sadržaj i izdavanje certifikata za kvalifikovani elektronski pečat, gubitak validnosti, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata, verifikaciju i čuvanje elektronskog pečata, shodno se primjenjuju odredbe čl. 10, 12, 13, 14 i čl.16 do 24 ovog zakona." **Član 26** U članu 26 stav 2 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno i članovima 25 i 26 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

Član 42 **Zahtjevi za kvalifikovane elektronske vremenske pečate** 1. Kvalifikovani elektronski vremenski pečat mora ispunjavati sljedeće zahtjeve: (a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka; (b) zasniva se na izvoru tačnog vremena povezanim s koordinisanim univerzalnim vremenom; i (c) potpisan je pomoću naprednog elektronskog potpisa ili zapečaćen pomoću naprednog elektronskog pečata kvalifikovanog davaoca usluga povjerenja ili ekvivalentnom metodom. 2. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za povezivanje datuma i vremena s podacima i za izvore tačnog vremena. Ako povezivanje datuma i vremena s podacima i izvor tačnog vremena zadovoljavaju te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u stavu 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	**Član 9** **Član 27 mijenja se i glasi:** „Na punovažnost, prihvatljivost i pravno dejstvo elektronskog pečata, elektronskog vremenskog pečata, kvalifikovanog elektronskog pečata i kvalifikovanog elektronskog vremenskog pečata, zahtjeve za napredni elektronski pečat, sadržaj i izdavanje certifikata za kvalifikovani elektronski pečat, gubitak validnosti, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata, verifikaciju i čuvanje elektronskog pečata, shodno se primjenjuju odredbe čl. 10, 12, 13, 14 i čl.16 do 24 ovog zakona." **Član 6** U članu 26 stav 2 tačka 3 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.	Potpuno usklađeno	Potpuno usklađeno i članovima 25 i 26 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
ODSJEK 7 **Usluge elektronske preporučene dostave**			Potpuno usklađeno	
Član 43 **Pravno dejstvo usluge elektronske preporučene dostave** 1. Podacima poslatim i primljenim pomoću usluge za elektronsku preporučenu dostavu ne smije biti uskraćeno pravno dejstvo i prihvatljivost kao dokaza u sudskom postupku isključivo na osnovu toga što su u elektronskom obliku ili zbog toga što ne ispunjavaju uslove kvalifikovane usluge elektronske preporučene dostave. 2. Podaci poslati i primljeni korišćenjem kvalifikovane usluge elektronske preporučene dostave uživaju pretpostavku integriteta podataka, slanje tih podataka od strane identifikovanog pošiljaoca, njihov prijem od strane identifikovanog primaoca i tačnost datuma i vremena slanja i prijema naznačeni su kvalifikovanom uslugom elektronske preporučene dostave.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članovima 30 i 31 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

Član 44 **Zahtjevi za kvalifikovane usluge elektronske preporučene dostave** 1. Kvalifikovane usluge elektronske preporučene dostave moraju ispuniti sljedeće zahtjeve: (a) pruža ih jedan kvalifikovani davalac usluga povjerenja ili više njih; (b) uz visok stepen povjerenja obezbjeđuju identifikaciju pošiljaoca;	**Član 6** U članu 31 stav 1 tač. 1 i 4 i stav 2 riječi: „usluge certifikovanja za elektronske transakcije" u različitom padežu zamjenjuju se riječima: „elektronske usluge povjerenja" u odgovarajućem padežu.			
(c) obezbjeđuju identifikaciju primaoca prije dostave podataka; (d) slanje i primanje podataka obezbjeđeno je naprednim elektronskim potpisom ili naprednim elektronskim pečatom kvalifikovanog davaoca usluga povjerenja na način kojim se isključuje mogućnost nezapažene promjene podataka; (e) pošiljaocu i primaocu podataka jasno se naznačava svaka promjena podataka potrebna radi slanja ili primanja podataka; (f) datum i vrijeme slanja, primanja i eventualne promjene podataka naznačavaju se kvalifikovanim elektronskim vremenskim pečatom. U slučaju prenosa podataka između dva kvalifikovana davaoca usluga povjerenja ili više njih, zahtjevi iz tač. a do f primjenjuju se na sve kvalifikovane davaoce usluga povjerenja. 2. Komisija može aktima za sprovođenje utvrditi referentne brojeve standarda za postupke slanja i primanja podataka. Ako postupak slanja i primanja podataka zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u stavu 1. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.		Potpuno usklađeno	Potpuno usklađeno članom 31 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
ODSJEK 8 **Autentifikacija internet stranica** **Član 45** **Zahtjevi za kvalifikovane certifikate za autentifikaciju internet stranica** 1. Kvalifikovani certifikati za autentifikaciju internet stranica moraju da ispune zahtjeve utvrđene u Aneksu IV.	**Član 33 mijenja se i glasi:** **„Kvalifikovani certifikati za autentifikaciju internet stranice** **Član 33** Kvalifikovani certifikat za autentifikaciju internet stranice mora da sadrži:	Potpuno usklađeno		

2. Komisija može aktima za sprovođenje da utvrdi referentne brojeve standarda za kvalifikovane certifikate za autentifikaciju internet stranica. Ako kvalifikovani certifikat za autentifikaciju internet stranica zadovoljava te standarde, smatra se da je postignuta usaglašenost sa zahtjevima utvrđenim u Aneksu IV. Ovi akti za sprovođenje donose se u skladu s postupkom ispitivanja iz člana 48 stav 2.	1) oznaku da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranice u elektronskom obliku pogodnom za automatsku obradu; 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za autentifikaciju internet stranice, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj, - fizičko lice: ime i prezime i poreski identifikacioni broj; 3) skup identifikacionih podataka o: - pravnom licu ili organu vlasti kojem je izdat certifikat: naziv, matični, odnosno poreski identifikacioni broj i sjedište (minimum naziv grada i države), - fizičkom licu kome je izdat certifikat: ime i prezime ili pseudonim koji, ako se koristi, mora biti jasno naznačen i adresu (minimum naziv grada i države); 4) naziv jednog ili više domena kojim upravlja fizičko lice, pravno lice ili organ vlasti kojem je izdat certifikat za autentifikaciju internet stranice; 5) podatke o periodu važenja kvalifikovanog certifikata za autentifikaciju internet stranice; 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca elektronske usluge povjerenja; 7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje certifikat; 8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja;			

	9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za autentifikaciju internet stranice."			
POGLAVLJE IV **ELEKTRONSKI DOKUMENTI** ***Član 46*** **Pravna dejstva elektronskih dokumenata** Elektronskom dokumentu ne smije biti uskraćeno pravno dejstvo i prihvatljivost kao dokaza u sudskom postupku isključivo na osnovu toga što je u elektronskom obliku.	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 13 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	
Čl. 47-52	Nema odgovarajuće odredbe	Neprenosivo		
PRILOG I. **ZAHTJEVI ZA KVALIFIKOVANE CERTIFIKATE ZA ELEKTRONSKE POTPISE** Kvalifikovani certifikati za elektronske potpise sadrže: (a) indikaciju, barem u obliku pogodnom za automatsku obradu, da je certifikat izdat kao kvalifikovani certifikat za elektronske potpise; (b) skup podataka koji nedvosmisleno predstavlja kvalifikovanog davaoca usluga povjerenja koji izdaje kvalifikovane certifikate uključujući barem državu članicu u kojoj je davalac osnovan i — za pravno lice: naziv i, gdje je to moguće, matični broj kako je navedeno u službenoj evidenciji, — za fizičko lice: ime lica; (c) barem ime potpisnika, ili pseudonim; ako se koristi pseudonimom, on se mora jasno navesti; (d) podatke za validaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa; (podatke o početku i završetku roka validnosti certifikata; e) (f) identifikacionu oznaku certifikata koja mora biti jedinstvena za kvalifikovanog davaoca usluga povjerenja; (g) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga povjerenja koji izdaje certifikat;	**Član 7** **Član 16 mijenja se i glasi:** „Kvalifikovani certifikat za elektronski potpis je certifikat koji izdaje kvalifikovani davalac elektronske usluge povjerenja, odnosno organ vlasti iz člana 4 st. 3 i 4 ovog zakona i koji sadrži: 1) oznaku da se radi o kvalifikovanom certifikatu za elektronski potpis u obliku prikladnom za automatsku obradu podataka; 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za elektronski potpis, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj; - fizičko lice: ime i prezime i poreski identifikacioni broj; 3) skup identifikacioni podataka o potpisniku (ime i prezime ili pseudonim) koji, ako se koristi, mora biti jasno naznačen; 4) podatke za verifikaciju elektronskog potpisa koji odgovaraju podacima za izradu elektronskog potpisa i koji su pod kontrolom potpisnika; 5) podatke o periodu važenja tog certifikata; 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za elektronski potpis koja	Potpuno usklađeno		

(h)lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredan elektronski potpis ili napredan elektronski pečat iz tačke g; (i)lokaciju usluga koje se mogu koristiti za ispitivanje statusa validnosti kvalifikovanog certifikata; (j)ako se podaci za izradu elektronskog potpisa koji su povezani s podacima za validaciju elektronskog potpisa nalaze u kvalifikovanom sredstvu za izradu elektronskog potpisa, odgovarajuću naznaku navedenog, barem u obliku pogodnom za automatsku obradu.	mora biti jedinstvena za kvalifikovanog davaoca elektronskih usluga povjerenja; 7) napredni elektronski potpis kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje taj certifikat; 8) lokaciju na kojoj je besplatno dostupan taj certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronskih usluga povjerenja; 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti tog certifikata; 10) odgovarajuću naznaku, u obliku pogodnom za automatsku obradu podataka, ako se podaci za izradu elektronskog potpisa koji su povezani sa podacima za verifikaciju elektronskog potpisa nalaze u kvalifikovanom sredstvu za izradu elektronskog potpisa. Kvalifikovani certifikat 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."			
PRILOG II. **ZAHTJEVI ZA KVALIFIKOVANA SREDSTVA ZA IZRADU ELEKTRONSKIH POTPISA** 1. Kvalifikovana sredstva za izradu elektronskih potpisa moraju pomoću odgovarajućih tehničkih i proceduralnih sredstava obezbijediti barem da: (a)je u razumnoj mjeri osigurana povjerljivost podataka za izradu elektronskog potpisa koji se upotrebljavaju za izradu elektronskog potpisa; (b)se podaci za izradu elektronskog potpisa koji se upotrebljavaju za izradu elektronskog potpisa praktično mogu pojaviti samo jedanput; (c)se podaci za izradu elektronskog potpisa koji se upotrebljavaju za izradu elektronskog potpisa ne mogu, uz razuman stepen garancije, iz njega izvesti, i da je elektronski potpis pouzdano zaštićen od krivotvorenja korišćenjem trenutno dostupne tehnologije;	Nema odgovarajuće odredbe	Potpuno usklađeno	Potpuno usklađeno članom 19 Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", broj 31/17)	

(d)da zakoniti potpisnik može pouzdano da zaštiti podatke za izradu elektronskog potpisa koji se koriste za izradu elektronskog potpisa od korišćenja od strane drugih lica. 2.Kvalifikovana sredstva za izradu elektronskih potpisa ne smiju da mijenjaju podatke koji se potpisuju niti da spriječe prikazivanje takvih podataka potpisniku prije potpisivanja. 3.Generisanje ili upravljanje podacima za izradu elektronskog potpisa u ime potpisnika može obavljati isključivo kvalifikovani davalac usluga povjerenja. 4.Ne dovodeći u pitanje stav 1 tačka d, kvalifikovani davaoci usluga povjerenja koji upravljaju podacima za izradu elektronskog potpisa u ime potpisnika mogu da dupliraju podatke za izradu elektronskog potpisa isključivo u svrhu izrade rezervnih kopija pod uslovom da su ispunjeni sljedeći zahtjevi: (a)sigurnost dupliranih skupova podataka mora da bude na nivou koji je jednak stepenu sigurnosti izvornih skupova podataka; (b)broj dupliranih skupova podataka ne prelazi broj neophodan za obezbjeđenje kontinuiteta usluge.				
PRILOG III. **ZAHTJEVI ZA KVALIFIKOVANE CERTIFIKATE ZA ELEKTRONSKE PEČATE** Kvalifikovani certifikati za elektronske pečate sadrže: (a)naznaku, barem u obliku prikladnom za automatsku obradu, da je certifikat izdat kao kvalifikovani certifikat za elektronske pečate; (b)skup podataka koji nedvosmisleno predstavljaju kvalifikovanog davaoca usluga povjerenja koji izdaje kvalifikovane certifikate, uključujući barem državu članicu u kojoj je davalac osnovan i —za pravno lice: naziv i, gdje je to moguće, matični broj kako je navedeno u službenoj evidenciji, —za fizičko lice: ime lica; (c)barem naziv autora pečata i, gdje je to moguće, matični broj kako je navedeno u službenoj evidenciji; (d)podatke za validaciju elektronskog pečata koji odgovaraju podacima za izradu elektronskog pečata;	**Član 9** **Član 27 mijenja se i glasi:** „Na punovažnost, prihvatljivost i pravno dejstvo elektronskog pečata, elektronskog vremenskog pečata, kvalifikovanog elektronskog pečata i kvalifikovanog elektronskog vremenskog pečata, zahtjeve za napredni elektronski pečat, sadržaj i izdavanje certifikata za kvalifikovani elektronski pečat, gubitak validnosti, opoziv i privremenu suspenziju certifikata za elektronski pečat i certifikata za kvalifikovani elektronski pečat, zahtjeve za kvalifikovana sredstva za izradu elektronskog pečata, ocjenu usaglašenosti kvalifikovanog sredstva za izradu elektronskog pečata, verifikaciju i čuvanje elektronskog pečata, shodno se primjenjuju odredbe čl. 10, 12, 13, 14 i čl.16 do 24 ovog zakona.”	Potpuno usklađeno	

(podatke o početku i kraju roka validnosti certifikata; e) (f) identifikacionu oznaku certifikata koja mora biti jedinstvena za tog kvalifikovanog davaoca usluga povjerenja; (g) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga povjerenja koji izdaje certifikat;				
(h) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredni elektronski potpis ili napredni elektronski pečat iz tačke g; (i) lokaciju usluga koje se mogu koristiti za ispitivanje statusa validnosti kvalifikovanog certifikata; (j) kada se podaci za izradu elektronskog pečata koji su povezani s podacima za validaciju elektronskog pečata nalaze u kvalifikovanom sredstvu za izradu elektronskog pečata, odgovarajuću naznaku navedenog, barem u obliku prikladnom za automatsku obradu.				
PRILOG IV. **ZAHTJEVI ZA KVALIFIKOVANE CERTIFIKATE ZA AUTENTIKACIJU MREŽNIH STRANICA** Kvalifikovani certifikati za autentifikaciju internet stranica sadrže:	**Član 11** **Član 33 mijenja se i glasi:** **„Kvalifikovani certifikati za autentifikaciju internet stranice** Kvalifikovani certifikat za autentifikaciju internet stranice mora da sadrži:			
(a) naznaku, barem u obliku prikladnom za automatsku obradu, da je certifikat izdat kao kvalifikovani certifikat za autentifikaciju internet stranica; (b) skup podataka koji nedvosmisleno predstavljaju kvalifikovanog davaoca usluga povjerenja koji izdaje kvalifikovane certifikate, uključujući barem državu članicu u kojoj je davalac osnovan i —za pravno lice: naziv i, gdje je to moguće, matični broj kako je navedeno u službenoj evidenciji, —za fizičko lice: ime lica; (c) za fizička lica: barem ime lica kojem je izdat certifikat ili pseudonim. Ako se koristi pseudonim, on mora biti jasno naveden; za pravna lica: barem naziv pravnog lica kojem je izdat certifikat i, gdje je to moguće, matični broj kako je navedeno u službenoj evidenciji;	1) oznaku da se radi o kvalifikovanom certifikatu za autentifikaciju internet stranice u elektronskom obliku pogodnom za automatsku obradu; 2) skup identifikacionih podataka o pravnom licu, fizičkom licu ili organu vlasti koji izdaje kvalifikovani certifikat za autentifikaciju internet stranice, uz navođenje naziva države u kojoj je to lice odnosno organ vlasti registrovan kao kvalifikovani davalac elektronskih usluga povjerenja, i to za: - pravno lice, odnosno organ vlasti: naziv, matični, odnosno poreski identifikacioni broj, - fizičko lice: ime i prezime i poreski identifikacioni broj; 3) skup identifikacionih podataka o:	Potpuno usklađeno		

(d) elemente adrese, uključujući barem grad i državu, fizičkog ili pravnog lica kojem je izdat certifikat i, gdje je to moguće, kako je navedeno u službenoj evidenciji; (e) naziv(e) domena(â) kojim(ima) upravlja fizičko ili pravno lice kojem je izdat certifikat; (f podatke o početku i kraju roka važenja certifikata;) (g) identifikacionu oznaku certifikata koja mora biti jedinstvena za kvalifikovanog davaoca usluga povjerenja; (h) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca usluga povjerenja koji izdaje certifikat; (i) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredni elektronski potpis ili napredni elektronski pečat iz tačke h; (j) lokaciju usluga statusa validnosti certifikata koje se mogu koristiti za ispitivanje statusa validnosti kvalifikovanog certifikata.	- pravnom licu ili organu vlasti kojem je izdat certifikat: naziv, matični, odnosno poreski identifikacioni broj i sjedište (minimum naziv grada i države), - fizičkom licu kome je izdat certifikat: ime i prezime ili pseudonim koji, ako se koristi, mora biti jasno naznačen i adresu (minimum naziv grada i države); 4) naziv jednog ili više domena kojim upravlja fizičko lice, pravno lice ili organ vlasti kojem je izdat certifikat za autentifikaciju internet stranice; 5) podatke o periodu važenja kvalifikovanog certifikata za autentifikaciju internet stranice; 6) identifikacionu oznaku izdatog kvalifikovanog certifikata za autentifikaciju internet stranice koja mora biti jedinstvena za kvalifikovanog davaoca elektronske usluge povjerenja; 7) napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja koji izdaje certifikat; 8) lokaciju na kojoj je besplatno dostupan certifikat na kojem se zasniva napredni elektronski potpis ili napredni elektronski pečat kvalifikovanog davaoca elektronske usluge povjerenja; 9) lokaciju usluga koje se mogu koristiti za ispitivanje validnosti kvalifikovanog certifikata za autentifikaciju internet stranice."			

Crna Gora
Ministarstvo finansija

Crna Gora
MINISTARSTVO JAVNE UPRAVE
Podgorica

Primljeno: 15.10.2019.				
Org. jed.	Klas. znak	Redni broj	Prilog	Vrijednost
01-011/19		4375/2		

Adresa: ul. Stanka Dragojevića 2,
81000 Podgorica, Crna Gora
tel: +382 20 242 835
fax: +382 20 224 450
www.mif.gov.me

Br:02-03-11878/1

Podgorica, 15. 10. 2019. godine

MINISTARSTVO JAVNE UPRAVE
-n/r ministarke, g-đe Suzane Pribilović-

Poštovana gospođo Pribilović,

Na osnovu Vašeg akta broj: 01-011/19-4375, kojim se traži mišljenje na tekst Predloga zakona o izmjenama i dopunama Zakona o elektronskoj identifikaciji i elektronskom potpisu, Ministarstvo finansija daje sljedeće:

MIŠLJENJE

Predlogom Zakona dodatno se uređuje oblast elektronske identifikacije i elektronskih usluga povjerenja. Sistemi elektronske identifikacije, predloženim izmjenama se ne vezuju samo za davaoce elektronskih usluga povjerenja, već se mogu uspostaviti nezavisno uz ispunjavanje propisanih uslova. Takođe, predloženim izmjenama izvršeno je dodatno usaglašavanje sa EU regulativom.

Na tekst Predloga zakona i pripremljeni Izvještaj o analizi uticaja propisa sa aspekta uticaja na poslovni ambijent, nemamo primjedbi.

Uvidom u dostavljeni tekst Predloga zakona i Izvještaj o sprovedenoj analizi procjene uticaja propisa utvrđeno je da implementacija istog ne zahtijeva dodatna izdvajanja finansijskih sredstava iz Budžeta države.

S poštovanjem,

MINISTAR
dr Darko Radunović

CRNA GORA MINISTARSTVO FINANSIJA 1 PODGORICA