PREDLOG

Z A K O N

O ELEKTRONSKOM DOKUMENTU, ELEKTRONSKOJ IDENTIFIKACIJI I USLUGAMA OD POVERENJA U ELEKTRONSKOM POSLOVANJU

I. UVODNE ODREDBE

Predmet

Član 1.

Ovim zakonom uređuju se elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju.

Značenje pojedinih izraza

Član 2.

Pojedini izrazi, u smislu ovog zakona, imaju sledeće značenje:

1) elektronsko poslovanje je upotreba podataka u elektronskom obliku, sredstava elektronske komunikacije i elektronske obrade podataka u obavljanju poslova fizičkih i pravnih lica, uključujući organe javne vlasti;
2) elektronski oblik podataka je digitalni zapis podataka pogodan za elektronsku obradu i prenos putem sredstava elektronske komunikacije;
3) elektronska transakcija je poslovna aktivnost između dve ili više strana koja se obavlja elektronskim putem;
4) elektronski dokument je skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video materijala, u elektronskom obliku;
5) proizvod je hardver, softver odnosno hardver sa pripadajućim softverom, ili njihove odgovarajuće komponente, namenjen elektronskoj obradi, elektronskom prenosu odnosno čuvanju podataka;
6) interoperabilnost je sposobnost dva ili više sistema ili njihovih komponenti da razmenjuju podatke i omoguće zajedničku upotrebu podataka i znanja;
7) organ javne vlasti je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, preduzeća, ustanove, organizacije i pojedinci kojima su povereni poslovi iz nadležnosti Republike Srbije, odnosno javna ovlašćenja;
8) fizičko lice u svojstvu registrovanog subjekta je fizičko lice koje registrovano za obavljanje određene delatnosti u skladu sa zakonom;
9) autentikacija je proces provere identiteta pravnog lica, fizičkog lica ili fizičkog lica u svojstvu registrovanog subjekta uključujući proveru integriteta i porekla podataka za koje se pretpostavlja da ih je to lice stvorilo, odnosno poslalo;
10) identifikacioni podaci predstavljaju skup podataka na osnovu kojih je moguće jednoznačno utvrditi identitet pravnog lica, fizičkog lica ili fizičkog lica u svojstvu registrovanog subjekta;

11) elektronska identifikacija je postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji jednoznačno određuju pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta;

12) sredstvo elektronske identifikacije je materijalno odnosno nematerijalno sredstvo koje sadrži identifikacione podatke i kojim se dokazuje identitet prilikom autentikacije;

13) šema elektronske identifikacije je sistem izdavanja sredstva elektronske identifikacije pravnom licu, fizičkom licu ili fizičkom licu u svojstvu registrovanog subjekta;

14) usluga elektronske identifikacije je usluga koja omogućava korišćenje određene šeme elektronske identifikacije u elektronskim transakcijama pri čemu se u okviru te usluge pružaju garancije da identifikacioni podaci iz sredstva elektronske identifikacije odgovaraju licu kome je sredstvo izdato;

15) usluga od poverenja je elektronska usluga koja olakšava poslovnu aktivnost između dve ili više strana pri čemu se zasniva na tome da pružalac usluge stranama garantuje verodostojnost pojedinih podataka, a koja je kao takva određena ovim zakonom;

16) pružalac usluga od poverenja je pravno lice ili fizičko lice u svojstvu registrovanog subjekta koje pruža jednu ili više usluga od poverenja;

17) pouzdajuća strana je pravno ili fizičko lice koje se pouzdaje u uslugu elektronske identifikacije odnosno uslugu od poverenja;

18) kvalifikovana usluga od poverenja je usluga od poverenja koja ispunjava uslove utvrđene ovim zakonom za kvalifikovanu uslugu od poverenja;

19) pružalac kvalifikovane usluge od poverenja je pravno lice ili fizičko lice u svojstvu registrovanog subjekta koje pruža jednu ili više kvalifikovanih usluga od poverenja;

20) elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (potpisanim) podacima u elektronskim obliku tako da se elektronskim potpisom potvrđuje integritet tih podataka i identitet potpisnika;

21) elektronski pečat je skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (pečatiranim) podacima u elektronskim obliku tako da se elektronskim pečatom potvrđuje integritet tih podataka i identitet pečatioca;

22) podaci za kreiranje elektronskog potpisa odnosno pečata su jedinstveni podaci koje koristi potpisnik odnosno pečatilac za kreiranje elektronskog potpisa odnosno pečata i koji su logički povezani sa odgovarajućim podacima za validaciju elektronskog potpisa odnosno pečata;

23) podaci za validaciju elektronskog potpisa odnosno pečata su podaci na osnovu kojih se proverava da li elektronski potpis odnosno pečat odgovara podacima koji su potpisani odnosno pečatirani;

24) sertifikat za elektronski potpis odnosno pečat je elektronska potvrda kojim se potvrđuje veza između podataka za validaciju elektronskog potpisa odnosno pečata i identiteta potpisnika odnosno pečatioca;

25) potpisnik je fizičko lice koje je kreiralo elektronski potpis i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski potpis, to jest sertifikatu kojim se potvrđuje veza između

identiteta tog potpisnika i podataka za validaciju elektronskog potpisa koji odgovaraju podacima za kreiranje elektronskog potpisa koje je potpisnik koristio pri kreiranju tog elektronskog potpisa;

26) pečatilac je pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta u čije ime se kreira elektronski pečat i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski pečat, odnosno u sertifikatu kojim se potvrđuje veza između identiteta tog pečatioca i podataka za validaciju elektronskog pečata koji odgovaraju podacima za kreiranje elektronskog pečata koji su po ovlašćenju pečatioca korišćeni pri kreiranju tog elektronskog pečata;

27) sredstvo za kreiranje elektronskog potpisa odnosno pečata je tehničko sredstvo (softver odnosno hardver) koje se koristi za kreiranje elektronskog potpisa odnosno pečate uz korišćenje podataka za kreiranje elektronskog potpisa odnosno pečata;

28) validacija je postupak provere i potvrđivanja ispravnosti elektronskog potpisa odnosno elektronskog pečata;

29) napredni elektronski potpis je elektronski potpis koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta potpisnika u skladu sa ovim zakonom;

30) kvalifikovani elektronski potpis je napredni elektronski potpis koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog potpisa i koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis;

31) kvalifikovano sredstvo za kreiranje elektronskog potpisa je sredstvo koji ispunjava uslove propisane ovim zakonom;

32) kvalifikovani sertifikat za elektronski potpis je sertifikat za elektronski potpis koji izdaje kvalifikovani pružalac usluga od poverenja i koji ispunjava uslove predviđene ovim zakonom;

33) napredni elektronski pečat je elektronski pečat koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta pečatioca u skladu sa ovim zakonom;

34) kvalifikovani elektronski pečat je napredni elektronski pečat koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog pečata i koji je zasnovan na kvalifikovanom sertifikatu za elektronski pečat;

35) kvalifikovano sredstvo za kreiranje elektronskog pečata je sredstvo koji ispunjava uslove propisane ovim zakonom;

36) kvalifikovani sertifikat za elektronski pečat je sertifikat za elektronski pečat koji izdaje kvalifikovani pružalac usluga od poverenja i ispunjava uslove predviđene ovim zakonom;

37) sertifikat za autentikaciju veb sajta je potvrda pomoću koje je moguće izvršiti autentikaciju veb sajta i kojom se veb sajt povezuje sa identitetom fizičkog ili pravnog lica kome je sertifikat izdat;

38) kvalifikovani sertifikat za autentikaciju veb sajta je sertifikat za autentikaciju veb sajta koju izdaje kvalifikovani pružalac usluga od poverenja i ispunjava uslove predviđene ovim zakonom;

39) elektronski vremenski žig je zvanično vreme pridruženo podacima u elektronskom obliku kojim se potvrđuje da su ti podaci postojali u tom vremenskom trenutku;

40) kvalifikovani elektronski vremenski žig je elektronski vremenski žig koji ispunjava uslove utvrđene ovim zakonom za kvalifikovani elektronski vremenski žig;

41) usluga elektronske dostave je usluga prenosa podataka elektronskim putem u okviru koje pružalac usluge obezbeđuje dokaze o postupanju sa prenesenim podacima, uključujući dokaz slanja i prijema podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja odnosno bilo kojih neovlašćenih promena;

42) konverzija je prevođenje dokumenta iz jednog oblika u drugi tako da je očuvan sadržaj dokumenta;

43) digitalizacija je konverzija dokumenta iz oblika koji nije elektronski u elektronski oblik;

44) digitalizovani dokument je dokument koji je nastao digitalizacijom izvornog dokumenata;

45) telo za ocenjivanje usaglašenosti je telo ovlašćeno za sprovođenje ocenjivanja usaglašenosti kvalifikovanog pružaoca usluga od poverenja i kvalifikovane usluge od poverenja koju on pruža sa uslovima za pružanje kvalifikovanih usluga od poverenja.

Primena

Član 3.

Pružalac usluga od poverenja pruža usluge od poverenja u skladu sa ovim zakonom.

Odredbe ovog zakona ne primenjuju se na usluge od poverenja koje se pružaju u okviru zatvorenog sistema, odnosno ograničenog kruga učesnika, koji može biti određen sporazumom, internim aktom ili propisom, i koje nemaju uticaj na treće strane, odnosno ne obavezuju treća lica van tog sistema.

Obrada i zaštita podataka

Član 4.

Pružalac usluga od poverenja odnosno usluge elektronske identifikacije prilikom obrade podataka o ličnosti postupa u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

U okviru elektronske transakcije strane se mogu predstavljati pseudonimom ako propisom, ugovorom ili na drugi obavezujući način nije drugačije određeno.

Pristanak na identifikaciju i autentikaciju

Član 5.

Postupak elektronske identifikacije i autentikacije može biti pokrenut samo na zahtev pravnog ili fizičkog lica koje je predmet identifikacije, osim ako je propisom drugačije određeno.

Dostupnost i pristup osobama sa invaliditetom

Član 6.

Usluge od poverenja, usluge elektronske identifikacije i proizvodi koji se koriste za pružanje tih usluga treba da su dostupni osobama sa invaliditetom, u meri u kojoj je to moguće.

II. ELEKTRONSKI DOKUMENT

Punovažnost i dokazna snaga elektronskog dokumenta

Član 7.

Elektronskom dokumentu ne može se osporiti punovažnost, dokazna snaga, kao ni pisana forma samo zato što je u elektronskom obliku.

Izrada elektronskog dokumenta

Član 8.

Elektronski dokument se izrađuje primenom bilo koje dostupne i upotrebljive informaciono komunikacione tehnologije, ako zakonom nije drugačije određeno.

Elektronski dokument koji predstavlja arhivsku građu izrađuje se u formi koja zadovoljava uslove propisane ovim zakonom za pouzdanu pripremu za elektronsko čuvanje.

Forma prikaza elektronskog dokumenta

Član 9.

Elektronski dokument sadrži unutrašnju i spoljnu formu prikaza.

Unutrašnja forma prikaza sastoji se od tehničko-programske forme zapisivanja sadržine elektronskog dokumenta.

Spoljna forma prikaza sastoji se od vizuelnog ili drugog razumljivog prikaza sadržine elektronskog dokumenta.

Ako dokument sadrži elektronski potpis ili elektronski pečat, ta činjenica treba da bude jasno iskazana u spoljnoj formi elektronskog dokumenta.

Original i kopija

Član 10.

Elektronski dokument koji je izvorno nastao u elektronskom obliku smatra se originalom.

Elektronski dokument koji ima istovetan digitalni zapis originalnom elektronskom dokumentu smatra se originalom.

Kopija elektronskog dokumenta na papiru izrađuje se štampanjem spoljne forme elektronskog dokumenta.

Elektronski dokument koji je nastao digitalizacijom izvornog dokumenta čija forma nije elektronska, smatra se kopijom izvornog dokumenta.

Overa digitalizovanog akta

Član 11.

Akt koji je digitalizovan ima istu dokaznu snagu kao originalni akt ako su kumulativno ispunjeni sledeći uslovi i to:

1) da je digitalizacija akta obavljena, na jedan od sledećih načina, odnosno pod nadzorom:

(1) fizičkog odnosno ovlašćenog lica fizičkog lica u svojstvu registrovanog subjekta ili ovlašćenog lica pravnog lica čiji je to akt, ili

(2) lica koje je ovlašćeno za overu potpisa, rukopisa i prepisa u skladu sa zakonom koji uređuje overu potpisa, rukopisa i prepisa, ili

(3) lica koje je posebnim zakonom ovlašćeno za overu digitalizovanog akta;

2) da je istovetnost digitalizovanog akta sa originalom potvrđena kvalifikovanim elektronskim pečatom ili kvalifikovanom elektronskim potpisom lica iz podtač. (1) - (3) ovog stava ili lica na koga su prenete nadležnosti na osnovu kojih je akt donet.

Organi javne vlasti u postupcima koje sprovode u vršenju javnih ovlašćenja mogu izvršiti overu digitalizovanog akta, pod nadzorom organa javne vlasti, na način iz stava 1. tačka 2) ovog člana, kojom potvrđuju istovetnost digitalizovanog akta sa originalnom ispravom.

Digitalizovani akt koji je overen od strane organa iz stava 2. ovog člana ima istu dokaznu snagu kao original u okviru sprovođenja tog postupka.

Overa odštampanog primerka elektronskog dokumenta

Član 12.

Odštampani primerak elektronskog dokumenta ima istu dokaznu snagu kao originalni akt, ako su kumulativno ispunjeni sledeći uslovi i to:

1) da je štampanje elektronskog dokumenta izvršeno pod nadzorom:

(1) fizičkog lica, ovlašćenog lica fizičkog lica u svojstvu registrovanog subjekta, odnosno ovlašćenog lica pravnog lica čiji je to akt, ili

(2) lica koje je ovlašćeno za overu potpisa, rukopisa i prepisa u skladu sa zakonom koji uređuje overu potpisa, rukopisa i prepisa;

2) da je istovetnost odštampanog primerka elektronskog dokumenta sa originalom potvrđena, uz naznaku da je reč o odštampanom primerku elektronskog dokumenta:

(1) svojeručnim potpisom fizičkog lica, ili

(2) svojeručnim potpisom ovlašćenog lica fizičkog lica u svojstvu registrovanog subjekta, odnosno ovlašćenog lica pravnog lica, kao i pečatom fizičkog lica u svojstvu registrovanog subjekta, odnosno pravnog lica, ako postoji zakonska obaveza da akt sadrži pečat, ili

(3) od strane lica koje je ovlašćeno za overu potpisa, rukopisa i prepisa u skladu sa zakonom koji uređuje overu potpisa, rukopisa i prepisa.

Organi javne vlasti u postupcima koje sprovode u vršenju javnih ovlašćenja mogu izvršiti overu odštampanog primerka elektronskog dokumenta na način iz stava 1. tačka 2) podtačka (2) ovog člana, pri čemu odštampani primerak elektronskog

dokumenta obavezno sadrži pečat utvrđen zakonom kojim se uređuje pečat državnih i drugih organa.

Odštampani primerak elektronskog dokumenta koji je overen od strane organa iz stava 2. ovog člana ima istu dokaznu snagu kao original u okviru sprovođenja tog postupka.

Potvrda o prijemu elektronskog dokumenta

Član 13.

Potvrda o prijemu elektronskog dokumenta je dokaz da je taj dokument primljen od strane primaoca.

Potvrdu o prijemu elektronskog dokumenta izdaje primalac elektronskog dokumenta ili pružalac usluge elektronske dostave.

Potvrda o prijemu elektronskog dokumenta može biti sačinjena u formi elektronskog dokumenta.

Obaveza izdavanja potvrde o prijemu elektronskog dokumenta i elementi sadržaja potvrde uređuju se propisima ili voljom stranaka, ako zakonom nije drugačije određeno.

Dupliranje elektronskih dokumenata

Član 14.

Svaki primljeni elektronski dokument smatra se posebnim dokumentom, osim ako je više puta primljen istovetan dokument i primalac je znao ili je morao znati da je reč o istovetnom dokumentu.

Dostavljanje elektronskih dokumenata između organa javne vlasti i stranaka

Član 15.

Podnesak izrađen kao elektronski dokument fizička i pravna lica (stranke) dostavljaju organima javne vlasti putem elektronske pošte na adresu elektronske pošte koja je od strane organa javne vlasti određena za prijem elektronskih podnesaka, putem usluge kvalifikovane elektronske dostave na adresu za kvalifikovanu elektronsku dostavu koja je od strane organa javne vlasti određena za prijem elektronskih dokumenata ili drugim elektronskim putem ako je zakonom koji uređuje taj postupak predviđena mogućnost elektronskog opštenja, odnosno ako pitanje elektronske dostave tim zakonom nije drugačije uređeno.

Elektronski dokument iz stava 1. ovog člana organ javne vlasti dostavlja stranci na adresu elektronske pošte, odnosno adresu za kvalifikovanu elektronsku dostavu, koja je od strane stranke određena za prijem elektronskih dokumenata ili drugim elektronskim putem, u skladu sa propisom.

Dostavljanje elektronskih dokumenata između organa javne vlasti

Član 16.

Dostavljanje elektronskih dokumenata između organa javne vlasti obavlja se putem elektronske pošte, servisne magistrale organa, usluge kvalifikovane elektronske dostave ili drugim elektronskim putem, u skladu sa propisom.

III. ELEKTRONSKA IDENTIFIKACIJA

1. Šeme elektronske identifikacije

Uslovi koje mora da ispunjava šema elektronske identifikacije

Član 17.

Šema elektronske identifikacije mora:

1) da sadrži podatke za identifikaciju lica na izdatim sredstvima za identifikaciju, koji jedinstveno određuju pravno ili fizičko lice;

2) da obezbedi da izdavalac sredstava elektronske identifikacije obezbedi identifikacione podatke u okviru sredstva elektronske identifikacije koji odgovaraju licu kome je sredstvo izdato;

3) da jasno definiše tehničke i druge uslove koji omogućavaju pouzdajućoj strani proveru identiteta;

4) da ispunjava uslove za nivo pouzdanosti u koji se razvrstava, iz člana 18. ovog zakona.

Nivoi pouzdanosti šema elektronske identifikacije

Član 18.

Šeme elektronske identifikacije razvrstavaju se prema nivou pouzdanosti na:

1) šeme osnovnog nivoa pouzdanosti, koje obezbeđuju ograničeno poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija svrha je da smanje rizik zloupotrebe odnosno neistinitog predstavljanja;

2) šeme srednjeg nivoa pouzdanosti, koje obezbeđuju značajno poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija svrha je da značajno smanje rizik zloupotrebe odnosno neistinitog predstavljanja;

3) šeme visokog nivoa pouzdanosti, koje obezbeđuju visoko poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija svrha je da onemoguće zloupotrebu odnosno neistinito predstavljanje.

Vlada, na predlog ministarstva nadležnog za poslove informacionog društva (u daljem tekstu: Ministarstvo), uređuje bliže uslove koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti, a naročito:

1) način dokazivanja i provere identiteta fizičkog odnosno pravnog lica koje zahteva izdavanje sredstava elektronske identifikacije;

2) način izdavanja sredstava elektronske identifikacije;

3) mehanizam autentikacije, putem koga fizičko odnosno pravno lice korišćenjem sredstava identifikacije potvrđuje svoj identitet drugoj strani u elektronskoj transakciji;

4) uslove koje treba da ispuni izdavalac sredstava elektronske identifikacije;

5) uslove koje treba da ispune drugi učesnici koji su uključeni u postupak izdavanja sredstava elektronske identifikacije;

6) tehničke i bezbednosne karakteristike sredstava elektronske identifikacije koja se izdaju;

7) minimalne tehničke i organizacione uslove u cilju obezbeđivanja interoperabilnosti šema elektronske identifikacije u skladu sa domaćim i međunarodnim standardima iz ove oblasti.

Registar pružalaca usluga elektronske identifikacije i šema elektronske identifikacije

Član 19.

Pružalac usluge elektronske identifikacije podnosi Ministarstvu zahtev za upis u Registar pružalaca usluga elektronske identifikacije i šema elektronske identifikacije, koji vodi Ministarstvo.

Registar iz stava 1. ovog člana od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkciju i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte.

Ministarstvo propisuje sadržaj i način vođenja registra iz stava 1. ovog člana, kao i način podnošenja zahteva za upis u registar, u skladu sa zakonom koji uređuje opšti upravni postupak, potrebnu dokumentaciju uz zahtev, obrazac zahteva i način objavljivanja podataka iz registra.

Korišćenje šema elektronske identifikacije u elektronskom poslovanju i u opštenju sa organom javne vlasti

Član 20.

Za utvrđivanje identiteta u elektronskom poslovanju mogu se koristiti šeme elektronske identifikacije koje su upisane u registar iz člana 19. ovog zakona, kao i šeme elektronske identifikacije koje nisu upisane u registar.

Iskaz volje ne može se osporiti samo zato što su, umesto potpisa, korišćene šeme elektronske identifikacije iz stava 1. ovog člana.

Šema elektronske identifikacije koja je upisana u registar iz člana 19. ovog zakona (u daljem tekstu: registrovana šema elektronske identifikacije) može se koristiti za utvrđivanje identiteta stranke u opštenju sa organom javne vlasti.

U opštenju stranke sa organima javne vlasti identitet stranke utvrđen na osnovu registrovane šeme elektronske identifikacije visokog nivoa pouzdanosti zamenjuje potpis stranke na podnesku.

Propisom može biti određeno da se u slučaju iz stava 4. ovog člana može koristiti šema elektronske identifikacije srednjeg ili osnovnog nivoa pouzdanosti ako su rizik od zloupotrebe i moguća šteta od zloupotrebe takvi da nije neophodno koristiti šemu visokog nivoa pouzdanosti.

Odgovornost pri elektronskoj identifikaciji

Član 21.

Izdavalac sredstava elektronske identifikacije odgovoran je za štetu koja je nastala zbog toga što sredstvo za identifikaciju nije izdato u skladu sa šemom elektronske identifikacije koja ispunjava uslove iz člana 17. ovog zakona.

Za štetu nastalu usled neispravno sprovedenog postupka autentikacije odgovorna je strana koja sprovodi taj postupak, ako je štetu prouzrokovala namerno ili nepažnjom.

Bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga elektronske identifikacije

Član 22.

Pružaoci usluga elektronske identifikacije, preduzimaju potrebne tehničke, fizičke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga.

Tehničkim i organizacionim merama osigurava se da nivo bezbednosti odgovara stepenu rizika i predviđenom nivou pouzdanosti šeme elektronske identifikacije, uzimajući u obzir najnovija dostupna tehnološka rešenja, a posebno se preduzimaju mere za sprečavanje bezbednosnih incidenata i ograničavanje štetnih posledica eventualnih incidenata, kao i za obaveštavanje zainteresovanih strana o neželjenim efektima bezbednosnih incidenata.

2. Prekogranična saradnja u oblasti elektronske identifikacije

Interoperabilnost tehničkih sistema

Član 23.

Ministarstvo sarađuje sa nadležnim telima Evropske unije po pitanjima prekogranične interoperabilnosti šema elektronske identifikacije i preduzima mere iz svoje nadležnosti kako bi se uspostavio što viši nivo interoperabilnosti šema elektronske identifikacije na nacionalnom nivou.

Prijavljivanje

Član 24.

Ministarstvo Evropskoj komisiji prijavljuje registrovane šeme elektronskog identiteta koje ispunjavaju uslove iz Uredbe EU br. 910/2014 Evropskog parlamenta i Saveta (u daljem tekstu: Uredba eIDAS).

IV. USLUGE OD POVERENjA

1. Opšte odredbe

Odgovornost pružaoca usluga od poverenja i teret dokazivanja

Član 25.

Pružalac usluge od poverenja odgovoran je za štetu nastalu usled toga što nije postupio u skladu sa ovim zakonom ukoliko je štetu prouzrokovao namerno ili nepažnjom.

Teret dokazivanja namere ili nepažnje pružaoca usluga od poverenja ja na fizičkom ili pravnom licu koje zahteva naknadu štete iz stava 1. ovog člana.

Teret dokazivanja da šteta nije nastala usled namere ili nepažnje kvalifikovanog pružaoca usluga od poverenja iz stava 1. ovog člana je na tom pružaocu usluga.

Pružalac usluga od poverenja nije odgovoran za štetu nastalu zbog korišćenja usluge kojom je prekoračeno naznačeno ograničenje, ako je korisnik usluge od poverenja o takvom ograničenju unapred obavešten.

Odgovornost korisnika usluga od poverenja za čuvanje sredstava i podataka za formiranje elektronskog potpisa odnosno pečata

Član 26.

Korisnik usluge od poverenja dužan je da čuva sredstva i podatke za formiranje elektronskog potpisa odnosno pečata od neovlašćenog pristupa i upotrebe, i da iste koristi u skladu sa odredbama ovog zakona.

Bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga od poverenja

Član 27.

Pružaoci usluga od poverenja, uključujući pružaoce kvalifikovanih usluga od poverenja, preduzimaju potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga od poverenja.

Tehničkim i organizacionim merama osigurava se da nivo bezbednosti odgovara stepenu rizika, uzimajući u obzir najnovija dostupna tehnološka rešenja, a posebno se preduzimaju mere za sprečavanje bezbednosnih incidenata i ograničavanje štetnih posledica eventualnih incidenata, kao i za obaveštavanje zainteresovanih strana o neželjenim efektima bezbednosnih incidenata.

Pružaoci usluga od poverenja, uključujući pružaoce kvalifikovanih usluga od poverenja, bez odlaganja, a najkasnije u roku od 24 sata od saznanja, obaveštavaju Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge koji imaju značajan uticaj na pružanje usluga od poverenja ili na zaštitu podataka o ličnosti koji se obrađuju u okviru pružanja usluge. U slučaju kada se narušena bezbednost odnosi na zaštitu podataka o ličnosti pružalac usluge od poverenja obaveštava i Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

Ako bi ugrožavanje bezbednosti ili gubitak integriteta usluge od poverenja mogli nepovoljno uticati na korisnike usluga od poverenja, pružalac usluga od poverenja o povredi bezbednosti ili gubitku integriteta usluge, bez odlaganja, obaveštava korisnika usluga od poverenja.

Ministarstvo obaveštava javnost ili zahteva od pružaoca usluga od poverenja da to učini, ako utvrdi da je objavljivanje podataka o povredi bezbednosti ili gubitka integriteta usluge u javnom interesu.

Ministarstvo će ostvariti saradnju sa odgovarajućim institucijama drugih država po pitanju razmene podataka o narušavanju bezbednosti i integriteta, u skladu sa odgovarajućim potvrđenim međunarodnim sporazumima.

Nadležnost Ministarstva

Član 28.

Ministarstvo vrši sledeće poslove:

1) vodi registar pružaoca kvalifikovanih usluga od poverenja;

2) razmatra izveštaje o proveri ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja;

3) vrši inspekcijski nadzor nad radom pružaoca usluga od poverenja;

4) nalaže vanrednu proveru ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja, u skladu sa zakonom;

5) sarađuje sa nadležnim organom za zaštitu podataka o ličnosti, i obaveštava ga bez odlaganja ukoliko dođe do saznanja da pružaoci kvalifikovanih usluga od poverenja ne postupaju u skladu sa propisima o zaštiti podataka o ličnosti;

6) proverava postojanje i pravilnu primenu odredaba o planovima prekida aktivnosti u slučajevima kada pružalac kvalifikovane usluge od poverenja prekine svoje aktivnosti, uključujući način na koji se održava dostupnost informacija koje izdaje i prima pružalac kvalifikovane usluge od poverenja;

7) sarađuje sa nadzornim telima iz člana 17. Uredbe eIDAS;

8) obaveštava javnost o ugrožavanju bezbednosti ili gubitku celovitosti usluga od poverenja koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke.

Nadležnosti Ministarstva u okviru prekogranične saradnje u oblasti usluga od poverenja

Član 29.

Ministarstvo obavlja i poslove:

1) obaveštava nadležna tela država članica Evropske unije o ugrožavanju bezbednosti ili gubitku celovitosti koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke;

2) izveštava Evropsku komisiju o svojim aktivnostima u skladu sa Uredbom eIDAS.

2. Opšte odredbe za kvalifikovane usluge od poverenja

Uspostavljanje odnosa između pružaoca i korisnika kvalifikovane usluge od poverenja

Član 30.

O pružanju kvalifikovane usluge od poverenja zaključuje se ugovor između pružaoca i korisnika kvalifikovane usluge od poverenja, na zahtev korisnika.

Pružalac kvalifikovane usluge od poverenja dužan je da, pre zaključivanja ugovora iz stava 1. ovog člana, obavesti lice koje je podnelo zahtev za pružanje kvalifikovane usluge od poverenja o svim važnim okolnostima korišćenja usluge, a naročito o:

1) propisima i pravilima koji se odnose na korišćenje kvalifikovane usluge od poverenja;

2) eventualnim ograničenjima u korišćenju kvalifikovane usluge od poverenja;

3) merama koje treba da realizuju korisnici kvalifikovane usluge od poverenja i o potrebnoj tehnologiji za bezbedno korišćenje kvalifikovane usluge od poverenja.

Korisnik kvalifikovane usluge od poverenja može koristiti usluge od poverenja jednog ili više pružalaca usluga od poverenja.

Uslovi za pružanje kvalifikovanih usluga od poverenja

Član 31.

Pružalac kvalifikovanih usluga od poverenja mora:

1) imati zaposlene koji poseduju neophodnu stručnost, iskustvo i kvalifikacije za primenu administrativnih i upravljačkih procedura koje odgovaraju domaćim i međunarodnim standardima i koji su prošli odgovarajuću obuku u oblasti informacione bezbednosti i zaštite podataka o ličnosti;

2) biti osiguran od odgovornosti za štetu nastalu vršenjem kvalifikovane usluge od poverenja;

3) koristiti sigurne uređaje i proizvode koji su zaštićeni od neovlašćene promene i garantuju tehničku bezbednost i pouzdanost procesa koje podržavaju;

4) koristiti sigurne sisteme za čuvanje podataka koji su mu povereni tako:

(1) da su javno raspoloživi samo kada je dobijena saglasnost lica čiji su to podaci,

(2) da samo ovlašćena lica mogu unositi podatke i vršiti izmene,

(3) da se može proveravati autentičnost podataka;

5) sprovoditi mere protiv falsifikovanja i krađe podataka;

6) čuvati u odgovarajućem vremenskom periodu sve relevantne informacije koje se odnose na podatke koji su kreirani ili primljeni od strane pružaoca kvalifikovanih usluga od poverenja, a posebno za svrhu pružanja dokaza u pravnim postupcima. Čuvanje se može vršiti elektronskim putem;

7) voditi ažurnu, tačnu i bezbednim merama zaštićenu bazu podataka izdatih elektronskih sertifikata;

8) imati ažuran plan završetka rada koji osigurava kontinuitet kvalifikovanih usluga od poverenja;

9) osigurati obradu ličnih podataka u skladu sa zakonima Republike Srbije.

Pružalac kvalifikovane usluge od poverenja dužan je da donese akta kojima određuje:

1) opšte uslove za pružanje usluge koji su javno dostupni ;

2) procedure i postupke koje pružalac kvalifikovane usluge od poverenja koristi kako bi obezbedio pružanje usluge u skladu sa propisima i opštim uslovima iz tačke 1) ovog stava.

Vlada, na predlog Ministarstva, bliže uređuje uslove za pružanje kvalifikovane usluge od poverenja iz stava 1. ovog člana i sadržaj akata iz stava 2. ovog člana, uključujući određivanje međunarodnih standarda koji se primenjuju.

Osiguranje od profesionalne odgovornosti

Član 32.

Ministarstvo propisuje najniži iznos osiguranja od rizika odgovornosti za štetu nastalu vršenjem usluge kvalifikovane usluge od poverenja.

Provera identiteta korisnika kvalifikovane usluge od poverenja

Član 33.

Pri izdavanju kvalifikovanog sertifikata za usluge od poverenja pružalac kvalifikovane usluge od poverenja proverava podatke o identitetu fizičkog odnosno pravnog lica koji su sadržani u kvalifikovanom sertifikatu, u skladu sa zakonom.

Proveru podataka iz stava 1. ovog člana pružalac kvalifikovane usluge od poverenja vrši:

1) uz fizičko prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica ili
2) putem javne isprave koja služi kao sredstvo identifikacije na daljinu, u skladu sa zakonom.

O promeni podataka iz stava 1. ovog člana, fizičko odnosno pravno lice dužno je da, bez odlaganja, obavesti pružaoca kvalifikovane usluge od poverenja.

Ocenjivanje ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja

Član 34.

Ocenjivanje ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja (u daljem tekstu: ocenjivanje ispunjenosti uslova) obavlja telo za ocenjivanje usaglašenosti koje je, u skladu sa zakonom kojim se uređuje akreditacija, akreditovano za ocenjivanje usaglašenosti pružaoca kvalifikovanih usluga od poverenja i kvalifikovanih usluga od poverenja koje oni pružaju.

Nakon sprovedenog ocenjivanja ispunjenosti uslova telo za ocenjivanje usaglašenosti sačinjava izveštaj o ocenjivanju usaglašenosti.

Ocenjivanje ispunjenosti uslova vrši se pre početka pružanja kvalifikovanih usluga od poverenja i najmanje jednom u 24 meseca.

Nakon završenog ocenjivanja ispunjenosti uslova pružalac usluge od poverenja dostavlja Ministarstvu izveštaj o ocenjivanju usaglašenosti, u roku od tri radna dana od dana kada ga je primio.

Ministarstvo može naložiti vanredno ocenjivanje ispunjenosti uslova alo se utvrde nepravilnosti u pružanju kvalifikovanih usluga od poverenja ili ako nastupi incident koji je u značajnoj meri ugrozio ili narušio informacionu bezbednost.

Vanredno ocenjivanje ispunjenosti uslova vrši telo za ocenjivanje usaglašenosti koje nije povezano sa vršenjem prethodnog ocenjivanja.

Troškove ocenjivanja ispunjenosti uslova, uključujući vanredna ocenjivanja, snosi pružalac kvalifikovane usluge od poverenja.

Ministarstvo utvrđuje listu standarda koje mora da ispuni telo za ocenjivanje usaglašenosti, obaveznu sadržinu izveštaja o ocenjivanju usaglašenosti i postupak ocenjivanja ispunjenosti uslova odnosno ocenjivanja usaglašenosti kvalifikovanih usluga od poverenja.

Početak pružanja kvalifikovanih usluga od poverenja

Član 35.

Pružalac kvalifikovanih usluga od poverenja podnosi Ministarstvu zahtev za upis u Registar pružalaca kvalifikovanih usluga od poverenja, koji vodi Ministarstvo.

Pružalac kvalifikovanih usluga od poverenja mora biti upisan u registar iz stava 1. ovog člana pre otpočinjanja pružanja kvalifikovanih usluga od poverenja.

Uz zahtev iz stava 1. ovog člana prilažu se dokazi o činjenicama iskazanim u zahtevu uključujući izveštaj o ocenjivanju usaglašenosti iz člana 34. stav 4. ovog zakona kojim je ocenjeno da podnosilac zahteva i kvalifikovane usluge od poverenja koje on namerava da pruža ispunjavaju uslove iz ovog zakona.

Ministarstvo rešava o upisu pružaoca kvalifikovanih usluga od poverenja u registar iz stava 1. ovog člana u roku od 60 dana od dana podnošenja urednog zahteva.

U postupku rešavanja iz stava 4. ovog člana Ministarstvo može zahtevati prilaganje dodatnih dokaza, kao i dodatnu proveru tehničkih i bezbednosnih komponenti i operativnog rada.

Ako pružalac usluga prestane da ispunjava uslove propisane ovim zakonom Ministarstvo donosi rešenje o njegovom brisanju iz registra iz stava 1. ovog člana.

Registar iz stava 1. ovog člana od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkciju i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte.

Ministarstvo propisuje sadržaj i način vođenja registra iz stava 1. ovog člana, način podnošenja zahteva za upis u registar iz stava 1. ovog člana u skladu sa propisima koji uređuju opšti upravni postupak, potrebnu dokumentaciju uz zahtev, obrazac zahteva i način provere ispunjenosti uslova za pružanje kvalifikovane usluge od poverenja.

Prestanak pružanja usluge izdavanja kvalifikovanih elektronskih sertifikata

Član 36.

Izdavalac kvalifikovanih elektronskih sertifikata koji namerava da prestane sa obavljanjem delatnosti dužan je da o nameri raskida ugovora obavesti svakog korisnika kvalifikovane usluge od poverenja i Ministarstvo, najmanje tri meseca pre nastanka nameravanog prestanka obavljanja delatnosti.

Izdavalac kvalifikovanih elektronskih sertifikata koji prestaje sa obavljanjem poslova dužan je da obezbedi kod drugog pružaoca usluga od poverenja nastavak obavljanja usluge za korisnike kvalifikovane usluge od poverenja kojima je izdao sertifikat, a ako za to nema mogućnosti, dužan je da opozove sve izdate sertifikate i o preduzetim merama odmah obavesti Ministarstvo.

Izdavalac kvalifikovanih elektronskih sertifikata dužan je da dostavi svu dokumentaciju i neophodna tehnička sredstva u vezi sa obavljanjem usluga od poverenja drugom izdavaocu na koga prenosi obaveze obavljanja jedne ili više usluga od poverenja, odnosno Ministarstvu.

Ako izdavalac kvalifikovanih elektronskih sertifikata ne postupi u skladu sa stavom 3. ovog člana, Ministarstvo će izvršiti opoziv svih sertifikata, bez odlaganja, a na trošak izdavaoca kvalifikovanih elektronskog sertifikata.

U slučaju privremene zabrane vršenja usluga, sertifikati izdati do dana nastanka uzroka zbog kojih je izrečena mera zabrane, ostaju u važnosti.

Državni organ kao pružalac kvalifikovanih usluga od poverenja

Član 37.

Državni organ može postati pružalac usluga od poverenja na osnovu uredbe Vlade ako ispunjava sve uslove za pružanje usluga predviđenih zakonom.

Uredba treba da sadrži vrstu usluge od poverenja koju može da pruža organ iz stava 1. ovog člana, način obavljanja i bliže određenje postupka obavljanja poverenih usluga od poverenja.

Javna lista kvalifikovanih usluga od poverenja

Član 38.

Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja, u elektronskom obliku koji je pogodan za automatsku obradu.

Podaci u Javnoj listi kvalifikovanih usluga od poverenja izvode se iz Registra iz člana 35. ovog zakona.

Javna lista kvalifikovanih usluga od poverenja potpisuje se naprednim elektronskim pečatom.

Formu i način objavljivanja Javne liste kvalifikovanih usluga od poverenja propisuje Ministarstvo.

Forma i način objavljivanja Javne liste kvalifikovanih usluga od poverenja iz stava 4. ovog člana treba da budu usklađeni sa tehničkim uslovima za liste od poverenja iz člana 22. Uredbe eIDAS.

Znak pouzdanosti za kvalifikovane usluge od poverenja

Član 39.

Znak pouzdanosti za kvalifikovane usluge od poverenja (u daljem tekstu: Znak pouzdanosti) je znak kojim se na jednostavan, prepoznatljiv i jasan način označava kvalifikovana usluga od poverenja.

Registrovani pružaoci kvalifikovanih usluga od poverenja imaju pravo da koriste Znak pouzdanosti za kvalifikovane usluge od poverenja koje pružaju.

Znak pouzdanosti iz stava 1. koristi se do stupanja Republike Srbije u članstvo u Evropskoj uniji.

Ministarstvo propisuje izgled, sastav, veličinu i dizajn Znaka pouzdanosti za kvalifikovane usluge od poverenja.

Prekogranično priznavanje kvalifikovanih usluga od poverenja

Član 40.

Kvalifikovana usluga od poverenja koju pruža strani pružalac usluge od poverenja ravnopravna je sa domaćom uslugom od poverenja ukoliko je tako regulisano potvrđenim međunarodnim sporazumom.

V. POJEDINE VRSTE USLUGA OD POVERENjA

Vrste usluga

Član 41.

Usluge od poverenja se pružaju u oblastima:

1) elektronskog potpisa i elektronskog pečata;

2) elektronskog vremenskog žiga;

3) elektronske dostave;

4) autentikacije veb sajtova;

5) elektronskog čuvanja dokumenata.

Kvalifikovane usluge od poverenja su:

1) izdavanje kvalifikovanih sertifikata za elektronski potpis;

2) usluga upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa;

3) usluga validacije kvalifikovanog elektronskog potpisa;

4) izdavanje kvalifikovanih sertifikata za elektronski pečat;

5) usluga upravljanja kvalifikovanim sredstvom za kreiranje elektronskog pečata;

6) usluga validacije kvalifikovanog elektronskog pečata;

7) izdavanje kvalifikovanih elektronskih vremenskih žigova;

8) usluga kvalifikovane elektronske dostave;

9) usluga izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova;

10) usluga kvalifikovanog elektronskog čuvanja dokumenata.

Pružalac usluga od poverenja odnosno kvalifikovanih usluga od poverenja može pružati jednu ili više usluga iz st. 1. i 2. ovog člana.

1. Elektronski potpis i elektronski pečat

Napredni elektronski potpis i napredni elektronski pečat

Član 42.

Napredni elektronski potpis odnosno napredni elektronski pečat mora:

1) na nedvosmislen način da bude povezan sa potpisnikom odnosno pečatiocem;

2) da omogućava utvrđivanje identiteta potpisnika, odnosno pečatioca;

3) da bude izrađen korišćenjem podataka za izradu elektronskog potpisa odnosno elektronskog pečata koje potpisnik odnosno pečatilac može, uz visok nivo pouzdanosti, koristi pod svojom isključivom kontrolom;

4) da bude povezan sa elektronski potpisanim odnosno elektronski pečatiranim podacima, na način da se može utvrditi bilo koja naknadna izmena tih podataka.

Sadržaj kvalifikovanog elektronskog sertifikata

Član 43.

Kvalifikovani elektronski sertifikat mora da sadrži:

1) oznaku, u formi pogodnoj za automatsku obradu, da se elektronski sertifikat koristi kao kvalifikovani sertifikat za elektronski potpis, odnosno pečat;

2) skup podataka koji jedinstveno identifikuju kvalifikovanog pružaoca usluge od poverenja za izdavanje kvalifikovanog elektronskog sertifikata uključujući, najmanje, zemlju porekla pružaoca i naziv pružaoca;

3) skup podataka koji jedinstveno identifikuju potpisnika odnosno pečatioca uključujući najmanje:

(1) za potpisnika:

- ime i prezime ili pseudonim , a ukoliko je upotrebljen pseudonim to mora biti jasno obeleženo u okviru kvalifikovanog elektronskog sertifikata;
- JMBG, ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG,

(2) za pečatioca: naziv, država i matični broj odnosno jedinstvena identifikaciona oznaka u skladu sa pravnom regulativom te države, ukoliko postoji;

4) podatke za proveru elektronskog potpisa odnosno elektronskog pečata, koji odgovaraju podacima za kreiranje tog elektronskog potpisa odnosno elektronskog pečata;

5) podatke o početku i kraju važenja kvalifikovanog elektronskog sertifikata;

6) serijski broj kvalifikovanog elektronskog sertifikata, koji mora biti jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata;

7) napredni elektronski potpis ili napredni elektronski pečat izdavaoca kvalifikovanog elektronskog sertifikata;

8) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 7) ovog stava;

9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata;

10) oznaku da su podaci za kreiranje elektronskog potpisa odnosno pečata, koji odgovaraju podacima za proveru elektronskog potpisa odnosno pečata iz kvalifikovanog elektronskog sertifikata, sadržani u kvalifikovanom sredstvu za kreiranje elektronskog potpisa odnosno pečata, ukoliko je taj uslov ispunjen.

Kvalifikovani elektronski sertifikati, pored obeležja iz stava 1. ovog člana, mogu uključivati dodatna obeležja.

Ministarstvo bliže propisuje uslove koje mora da ispunjavaju kvalifikovani elektronski sertifikati iz stava 1. ovog člana.

Opoziv i suspenzija kvalifikovanog elektronskog sertifikata

Član 44.

Izdavalac kvalifikovanih sertifikata dužan je da izvrši opoziv izdatih sertifikata, kada:

1) opoziv sertifikata zahteva vlasnik sertifikata ili njegov punomoćnik;

2) vlasnik sertifikata izgubi poslovnu sposobnost, ili je prestao da postoji ili su se promenile okolnosti koje bitno utiču na važenje sertifikata;

3) utvrdi da je podatak u sertifikatu pogrešan;

4) utvrdi da su podaci za proveru kvalifikovanog elektronskog potpisa odnosno pečata ili sistem pružaoca kvalifikovanih usluga od poverenja ugroženi na način koji utiče na bezbednost i pouzdanost sertifikata;

5) utvrdi da su podaci za elektronsko potpisivanje odnosno pečatiranje ili sistem vlasnika sertifikata ugroženi na način koji utiče na pouzdanost i bezbednost elektronskog potpisa;

6) prestaje sa radom ili mu je rad zabranjen.

Izdavalac kvalifikovanih sertifikata dužan je da obavesti korisnika kvalifikovane usluge od poverenja o opozivu sertifikata u roku od 24 časa od primljenog obaveštenja, odnosno nastanka okolnosti zbog kojih se sertifikat opoziva.

Korisnik kvalifikovane usluge od poverenja dužan je da odmah zatraži opoziv svog kvalifikovanog elektronskog sertifikata u slučaju gubitka ili oštećenja uređaja ili podataka za kreiranje sertifikata.

U slučaju opoziva kvalifikovani elektronski sertifikat trajno prestaje da važi od trenutka opoziva.

U slučaju suspenzije kvalifikovani elektronski sertifikat gubi važnost tokom perioda trajanja suspenzije.

Podaci o suspenziji i periodu trajanja suspenzije kvalifikovanog elektronskog sertifikata upisuju se u bazu podataka izdatih sertifikata koju vodi izdavalac kvalifikovanih elektronskih sertifikata i moraju biti vidljivi tokom trajanja suspenzije u okviru usluga kojima se pružaju informacije o statusu sertifikata.

Čuvanje dokumentacije o izdatim i opozvanim kvalifikovanim sertifikatima

Član 45.

Izdavalac kvalifikovanih elektronskih sertifikata dužan je da čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima, kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima, najmanje deset godina po prestanku važenja sertifikata.

Podaci iz stava 1. ovog člana mogu se čuvati u elektronskoj formi.

Kvalifikovana sredstva za kreiranje elektronskog potpisa i pečata

Član 46.

Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata mora da, pomoću odgovarajućih tehničkih rešenja i postupaka, obezbedi:

1) poverljivost podataka za kreiranje elektronskog potpisa odnosno pečata;

2) da se podaci za kreiranje elektronskog potpisa, odnosno pečata pojavljuju samo jednom;

3) da se podaci za kreiranje elektronskog potpisa, odnosno pečata ne mogu dobiti izvan sredstva za kreiranje elektronskog potpisa, odnosno pečata upotrebom dostupne tehnologije u razumnom vremenu;

4) da je elektronski potpis, odnosno pečat pouzdano zaštićen od falsifikovanja upotrebom dostupne tehnologije;

5) mogućnost pouzdane zaštite podataka za kreiranje elektronskog potpisa, odnosno pečata od neovlašćenog korišćenja.

Sredstva za kreiranje kvalifikovanog elektronskog potpisa, odnosno pečata, prilikom kreiranja elektronskog potpisa odnosno pečata, ne smeju promeniti podatke koji se potpisuju odnosno pečatiraju ili onemogućiti potpisniku, odnosno pečatiocu uvid u te podatke pre procesa kreiranja kvalifikovanog elektronskog potpisa odnosno pečata.

Kvalifikovano sredstvo za kreiranje elektronskog potpisa, odnosno pečata korisnik kvalifikovane usluge od poverenja može koristiti putem usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, odnosno pečata, što takođe predstavlja kvalifikovanu uslugu od poverenja.

Izuzetno od stava 1. ovog člana, kvalifikovani pružalac usluga od poverenja iz stava 3. ovog člana može izraditi kopiju podataka za izradu elektronskog potpisa, odnosno pečata u svrhu zaštite od gubitka podataka ako:

1) izrada i čuvanje kopija podataka za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata ne umanjuju propisani nivo zaštite tih podataka;

2) broj izrađenih kopija podataka za kreiranje elektronskog potpisa odnosno pečata nije veći nego što je to neophodno za obezbeđivanje kontinuiteta pružanja usluge.

Ministarstvo bliže propisuje uslove koje mora da ispunjava sredstvo za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata.

Sertifikacija kvalifikovanih sredstava za kreiranje elektronskog potpisa odnosno pečata

Član 47.

U skladu sa zakonom kojim se uređuju tehnički zahtevi za proizvode i ocenjivanje usaglašenosti, Ministarstvo imenuje telo za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata sa propisom iz člana 46. (u daljem tekstu: imenovano telo).

Propisom iz člana 46. se, takođe, bliže uređuju uslovi koje mora da ispunjava imenovano telo.

Ministarstvo vodi Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata na osnovu izveštaja koje dobija od imenovanih tela.

Imenovano telo bez odlaganja, a najkasnije u roku od 7 dana od nastale promene, obaveštava Ministarstvo o izdatim i povučenim potvrdama o usaglašenosti sredstava za kreiranje elektronskih potpisa odnosno pečata.

Ministarstvo u elektronskom obliku objavljuje podatke iz Registra kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata.

U Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata upisuju se i kvalifikovana sredstva za kreiranje elektronskog potpisa i elektronskog pečata sa spiska koji prema članu 31. Uredba eIDAS koji objavljuje Evropska komisija.

Ministarstvo propisuje sadržaj i način vođenja registra iz stava 3. ovog člana, način podnošenja zahteva za upis u registar u skladu sa propisima koji uređuju opšti upravni postupak, potrebnu dokumentaciju uz zahtev i obrazac zahteva.

Postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

Član 48.

Postupkom validacije utvrđuje se da elektronski potpis predstavlja ispravan kvalifikovani elektronski potpis kada:

1) je utvrđeno da je sertifikat koji prati elektronski potpis u trenutku potpisivanja predstavljao kvalifikovani elektronski sertifikat;

2) je utvrđeno da je kvalifikovani elektronski sertifikat izdat od strane pružaoca usluge izdavanja kvalifikovanih sertifikata za elektronski potpis i da je važio u trenutku potpisivanja;

3) je utvrđeno da podaci za validaciju elektronskog potpisa iz kvalifikovanog elektronskog sertifikata odgovaraju kombinaciji elektronskog potpisa i podataka koji su potpisani elektronskim potpisom;

4) je pouzdajućoj strani tačno prikazan skup podataka iz kvalifikovanog elektronskog sertifikata koji jedinstveno identifikuju potpisnika;

5) su pouzdajućoj strani tačno prikazani podaci koji su potpisani elektronskim potpisom;

6) je korišćenje pseudonima jasno naznačeno pouzdajućoj strani, u slučaju da je prilikom elektronskog potpisivanja korišćen pseudonim;

7) je utvrđeno da je elektronski potpis kreiran korišćenjem kvalifikovanog sredstva za kreiranje elektronskog potpisa;

8) je utvrđeno da nije narušen integritet podataka koji su potpisani elektronskim potpisom;

9) je utvrđeno da elektronski potpis ispunjava uslove za napredni elektronski potpis iz ovog zakona.

Sistem koji se koristi za validaciju kvalifikovanog elektronskog potpisa obezbeđuje tačan rezultat postupka validacije pouzdajućoj strani i omogućava joj identifikovanje bilo kog problema od značaja za pouzdanost.

Odredbe st. 1. i 2. ovog člana shodno se primenjuju na elektronski pečat.

Ministarstvo bliže propisuje uslove za postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

Usluga kvalifikovane validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata

Član 49.

Pružalac usluge kvalifikovane validacije kvalifikovanih elektronskih potpisa odnosno pečata obezbeđuje:

1) validaciju kvalifikovanog elektronskog potpisa odnosno pečata u skladu sa članom 48. ovog zakona;

2) da pouzdajuća strana koja koristi uslugu dobije rezultat postupka validacije elektronskim putem na automatizovan način, koji je pouzdan i efikasan;

3) da je rezultat postupka validacije iz tačke 2) ovog stava pečatiran naprednim elektronskim pečatom ili potpisan naprednim elektronskim potpisom pružaoca usluge.

Ministarstvo bliže propisuje uslove za pružanje usluge kvalifikovane validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata.

Pravno dejstvo elektronskog potpisa

Član 50.

Elektronskom potpisu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovani elektronski potpis.

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

Kvalifikovani elektronski potpis može da zameni overu svojeručnog potpisa, ako je to propisano posebnim zakonom.

Odredbe st. 1. i 2. ovog člana ne primenjuju se na formu testamenta, menicu, ček kao ni na druge pravne poslove za koje je posebnim zakonom predviđeno da se ne mogu preduzeti u elektronskoj formi.

Ugovori i drugi pravni poslovi za koje je posebnim zakonom predviđeno da se sačinjavaju u formi overe potpisa, javno potvrđene (solemnizovane) isprave, ili u formi javnobeležničkog zapisa ne mogu se sačiniti u skladu sa st. 1. i 2. ovog člana već u skladu sa propisima kojima se uređuje overa potpisa, potvrđivanje, i sačinjavanje isprava o pravnim poslovima.

Pravno dejstvo elektronskog pečata

Član 51.

Elektronskom pečatu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovan elektronski pečat.

Za kvalifikovani elektronski pečat važi pravna pretpostavka očuvanosti integriteta i tačnosti porekla podataka za koje je vezan.

Akt organa javne vlasti koji se donosi u vršenju javnih ovlašćenja u obliku elektronskog dokumenta umesto pečata odnosno potpisa službenog lica i pečata sadrži kvalifikovani elektronski pečat tog organa.

Podnesak stranke u postupku koji organi javne vlasti sprovode u vršenju javnih ovlašćenja u obliku elektronskog dokumenta sadrži kvalifikovani elektronski pečat ili kvalifikovani elektronski potpis.

Kvalifikovani elektronski pečat na podnesku u postupku koji organi javne vlasti sprovode u vršenju javnih ovlašćenja u obliku elektronskog dokumenta ima isto pravno dejstvo kao i svojeručni potpis, odnosno pečat.

Odredbe st. 1-5. ovog člana ne primenjuju se na menicu, ček kao ni na druge pravne poslove za koje je posebnim zakonom predviđeno da se ne mogu preduzeti u elektronskoj formi.

Ugovori i drugi pravni poslovi za koje je posebnim zakonom predviđeno da se sačinjavaju u formi overe potpisa, javno potvrđene (solemnizovane) isprave, ili u formi javnobeležničkog zapisa ne mogu se sačiniti u skladu sa st. 1-5. ovog člana već u skladu sa propisima kojima se uređuje overa potpisa, potvrđivanje, i sačinjavanje isprava o pravnim poslovima.

2. Elektronski vremenski žig

Uslovi za kvalifikovane elektronske vremenske žigove

Član 52.

Kvalifikovani elektronski vremenski žig mora:

1) da je povezan sa koordiniranim univerzalnim vremenom (UTC) tako da se sprečava svaka mogućnost promene podataka koja se ne može otkriti;

2) da je zasnovan na preciznom vremenskom izvoru;

3) da je izdat od strane pružaoca usluge izdavanja kvalifikovanog vremenskog žiga;

4) da je potpisan, odnosno pečatiran od strane pružaoca usluge izdavanja kvalifikovanog vremenskog žiga pomoću naprednog elektronskog potpisa ili naprednog elektronskog pečata.

Ministarstvo propisuje bliže uslove za kvalifikovane elektronske vremenske žigove.

Pravno dejstvo elektronskog vremenskog žiga

Član 53.

Elektronskom vremenskom žigu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovan vremenski žig.

Za kvalifikovani elektronski vremenski žig i podatke kojima je taj vremenski žig pridružen važi pravna pretpostavka tačnosti datuma i vremena iskazanog u vremenskom žigu i očuvanosti integriteta tih podataka u odnosu na taj vremenski trenutak.

3. Elektronska dostava

Uslovi za usluge kvalifikovane elektronske dostave

Član 54.

Usluga kvalifikovane elektronske dostave mora:

1) da je pružana od strane jednog ili više pružaoca kvalifikovanih usluga od poverenja;

2) da, uz visok nivo pouzdanosti, obezbeđuje identifikaciju pošiljaoca;

3) da obezbeđuje identifikaciju primaoca prilikom dostave podataka;

4) u procesu slanja i prijema elektronske poruke, da koristi napredni elektronski potpis ili napredni elektronski pečat pružaoca usluge kvalifikovane elektronske dostave u svrhu sprečavanja neprimećene promene podataka;

5) da obezbedi da izmena podataka izvršena u svrhu slanja ili prijema podataka mora biti jasno naznačena pošiljaocu i primaocu;

6) da obezbedi da vreme i datum slanja, prijema i eventualne izmene podataka moraju biti naznačeni kvalifikovanim elektronskim vremenskim žigom;

7) da, u slučaju da se podaci prenose između dva ili više pružalaca usluge kvalifikovane elektronske dostave, obezbedi da se uslovi iz ovog stava primenjuju na svakog od njih.

Potvrda o elektronskoj dostavi

Član 55.

Pružalac usluge kvalifikovane elektronske dostave pošiljaocu elektronske poruke izdaje:

1) potvrdu prijema elektronske poruke od strane pružaoca usluge;

2) potvrdu dostave elektronske poruke primaocu.

Potvrde iz stava 1. ovog člana pružalac usluge dostavlja automatski u elektronskom obliku potpisane naprednim elektronskim pečatom, a na zahtev ih može izdati u elektronskom ili papirnom obliku.

Potvrda iz stava 1. tač. 1) i 2) ovog člana sadrži:

1) identifikacionu oznaku elektronske poruke koju je dodelio pružalac usluge;

2) podatke o pošiljaocu i primaocu, koji od podataka o ličnosti mogu da sadrže podatke iz član 43. stav 1. tačka 3) ovog zakona kao i adresu za elektronsku dostavu;

3) podatke koji povezuju potvrdu sa sadržajem elektronske poruke;

4) datum i vreme prijema elektronske poruke od strane pružaoca usluge, odnosno datum i vreme dostave elektronske poruke pružaocu usluge.

Potvrda iz stava 1. tačka 2) ovog člana smatra se dostavnicom u elektronskom obliku u smislu zakona kojim se uređuje upravni postupak, pri čemu se datum i vreme dostave iz stava 3. tačka 4) ovog člana smatraju datumom i vremenom uručenja.

Datum i vreme prijema podneska koji je stranka u upravnom postupku uputila organu putem kvalifikovane elektronske dostave smatra se da je datum i vreme dostave iz stava 3. tačka 4) ovog člana.

Ako dođe do tehničkih problema prilikom elektronskog dostavljanja odnosno prijema podataka, pružalac usluge kvalifikovane elektronske dostave dužan je da o tome obavesti pošiljaoca i primaoca.

Ministarstvo propisuje bliže uslove za usluge kvalifikovane elektronske dostave iz člana 54. ovog zakona i sadržaj potvrda iz stava 3. ovog člana.

Razmena elektronskih poruka između pružalaca usluge kvalifikovane elektronske dostave

Član 56.

Ako se elektronska poruka prenosi preko dva ili više pružalaca usluga kvalifikovane elektronske dostave, tada se između pružalaca usluga elektronska poruka razmenjuje putem Centralnog sistema za razmenu poruka kvalifikovane elektronske dostave (u daljem tekstu: Centralni sistem).

Pružaoci usluge kvalifikovane elektronske dostave u obavezi su:

1) da obezbede povezivanje sa Centralnim sistemom;

2) da u okviru svoje usluge omoguće prijem i slanje poruka i kada je pošiljalac ili primalac poruke korisnik drugog pružaoca usluge kvalifikovane elektronske dostave.

Centralni sistem uspostavlja i o njegovom funkcionisanju stara se Ministarstvo.

Pravno dejstvo usluge elektronske dostave

Član 57.

Podacima poslatim ili primljenim putem usluge elektronske dostave ne može se osporiti pravna snaga i dopuštenost kao dokaz u pravnom prometu samo iz razloga što su u elektronskoj formi ili iz razloga što ne ispunjavaju sve uslove usluge kvalifikovane elektronske dostave.

Za podatke iz elektronske poruke poslate ili primljene putem usluge kvalifikovane elektronske dostave važi pravna pretpostavka integriteta podataka, slanja podataka od naznačenog pošiljaoca, prijem od strane naznačenog primaoca, pouzdanosti datuma i vremena slanja ili primanja.

4. Autentikacija veb sajtova

Kvalifikovani sertifikati za autentikaciju veb sajtova

Član 58.

Autentikacija veb sajta koristi se za potvrdu identiteta veb sajta od strane korisnika kvalifikovane usluge od poverenja, kojom se garantuje njegova pouzdanost korišćenja.

Za autentikaciju veb sajtova koriste se kvalifikovani sertifikati koje izdaje pružalac kvalifikovanih usluga od poverenja.

Kvalifikovani sertifikat za autentikaciju veb sajta mora da ispunjava uslove iz člana 59. ovog zakona.

Sadržaj kvalifikovanih sertifikata za autentikaciju veb sajtova

Član 59.

Kvalifikovani sertifikati za autentikaciju veb sajtova sadrže:

1) oznaku, koja se može prepoznati pri automatskoj obradi, da je sertifikat izdat kao kvalifikovani sertifikat za autentikaciju veb sajtova;

2) skup podataka koji nedvosmisleno predstavljaju pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova, što obavezno uključuje državu sedišta, poslovno ime i matični broj tog pružaoca usluge;

3) ime i prezime ili pseudonim fizičkog lica kome je izdat sertifikat, odnosno poslovne ime i matični broj pravnog lica kome je izdat sertifikat;

4) adresu, odnosno sedište fizičkog ili pravnog lica kome je izdat sertifikat;

5) naziv internet domena fizičkog ili pravnog lica kome je izdat sertifikat;

6) podatke o početku i kraju roka važenja sertifikata;

7) identifikacionu oznaku sertifikata koja mora da bude jedinstvena za pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova;

8) napredan elektronski potpis ili napredan elektronski pečat pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova;

9) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 8) ovog stava;

10) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata

5. Elektronsko čuvanje dokumenta

Priprema dokumenata za elektronsko čuvanje

Član 60.

Priprema dokumenata za elektronsko čuvanje odnosi se na:

1) dokumenta koja su izvorno nastala u elektronskom obliku koji je pogodan za čuvanje;

2) konverziju dokumenta u drugačiji elektronski oblik pogodan za čuvanje;

3) digitalizaciju dokumenta koja su izvorno nastala u obliku koji nije elektronski u oblik pogodan za čuvanje.

Dokument pripremljen za elektronsko čuvanje može obuhvatiti i dodatne podatke koji opisuju dokument ili su izvedeni iz dokumenta.

Priprema dokumenata za pouzdano elektronsko čuvanje

Član 61.

Priprema dokumenta za pouzdano elektronsko čuvanje mora:

1) da obezbedi da svi bitni elementi sadržaja izvornog dokumenta budu verno preneti u dokument pripremljen za elektronsko čuvanje, uzimajući u obzir prirodu i svrhu dokumenta, tj. očuvan je integritet sadržaja dokumenta;

2) da obezbedi da je očuvana upotrebljivost sadržaja izvornog dokumenta;

3) da obezbedi da su uključeni svi elementi sadržaja izvornog dokumenta koji su od značaja za autentičnost;

4) da obezbedi potvrdu vernosti izvornog dokumenta i tačnost dodatno uključenih podataka kvalifikovanim elektronskim pečatom ili potpisom sa pridruženim vremenskim žigom;

5) da obezbedi sprovođenje kontrole tačnosti i kvaliteta konverzije kao i otklanjanje grešaka nastalih u postupku konverzije;

6) da obezbedi da se dopune sadržaja, unete zabeležbe i podaci o preduzetim radnjama čuvaju odvojeno od izvornih dokumenata;

7) da obezbedi da se o preduzetim radnjama u postupku pripreme za elektronsko čuvanje vodi uredna evidencija.

Ako je propisani rok za čuvanje dokumenta duži od pet godina, dokument pripremljen za čuvanje treba da bude u formatu koji je pogodan za dugoročno čuvanje.

Vlada, na predlog Ministarstva, uređuje bliže uslove koje mora da ispunjava pouzdana priprema dokumenta za elektronsko čuvanje i formate dokumenta koji su pogodni za dugotrajno čuvanje.

Pouzdano elektronsko čuvanje dokumenta

Član 62.

Pouzdano elektronsko čuvanje dokumenata koji u izvornom obliku sadrže kvalifikovani elektronski potpis odnosno pečat, kao potvrdu integriteta i porekla tih dokumenata, vrši se tako da se tokom čuvanja koriste postupci i tehnološka rešenja kojima se obezbeđuje mogućnost dokazivanja validnosti kvalifikovanog elektronskog potpisa odnosno pečata tokom celog perioda čuvanja.

Pouzdano elektronsko čuvanje dokumenata pripremljenih u skladu sa članom 61. ovog zakona, kojima je kvalifikovanim elektronskim potpisom odnosno pečatom iz člana 61. stav 1. tačka 4) potvrđena vernost izvornom dokumentu i tačnost dodatno uključenih podataka, vrši se tako da se tokom čuvanja koriste postupci i tehnološka rešenja kojima se obezbeđuje mogućnost dokazivanja validnosti kvalifikovanog elektronskog potpisa odnosno pečata tokom celog perioda čuvanja.

Ministarstvo propisuje bliže uslove za postupke i tehnološka rešenja iz st. 1. i 2. ovog člana.

Ministarstvo nadležno za poslove kulture uređuje bliže uslove, zadatke, poslove, standarde i procese digitalizacije kulturnog nasleđa i savremenog stvaralaštva koji se odnose na postupke i tehnološka rešenja iz čl. 61 i 62. ovog zakona.

Usluga kvalifikovanog elektronskog čuvanja dokumenata

Član 63.

Usluga kvalifikovanog elektronskog čuvanja dokumenata je kvalifikovana usluga od poverenja putem koje se pruža pouzdano elektronsko čuvanje dokumenata u skladu sa čl. 60. do 62. ovog zakona.

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenta može se opredeliti da uslugu kvalifikovanog elektronskog čuvanja dokumenata ograniči samo na čuvanje dokumenata koji u izvornom obliku sadrže kvalifikovani elektronski potpis odnosno pečat.

Za dokument koji se čuva u okviru usluge kvalifikovanog elektronskog čuvanja dokumenata važi pravna pretpostavka vernosti izvornom dokumentu, o čemu pružalac usluge kvalifikovanog elektronskog čuvanja dokumenta izdaje potvrdu.

Ako se dokument čuva u okviru usluge kvalifikovanog elektronskog čuvanja dokumenata tako da period čuvanja predviđen tom uslugom obuhvata propisani period čuvanja datog dokumenta, izvorni dokument može biti uništen, osim ako nije drugačije propisano.

VI. INSPEKCIJSKI NADZOR

Poslovi inspekcije za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju

Član 64.

Inspekcija za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju vrši inspekcijski nadzor nad primenom ovog zakona i radom pružalaca usluga elektronske identifikacije i pružalaca usluga od poverenja (u daljem tekstu: pružaoci usluga) preko inspektora za elektronsku identifikaciju i usluge od poverenja (u daljem tekstu: inspektor)

U okviru inspekcijskog nadzora pružalaca usluga inspektor utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim za sprovođenje ovog zakona.

Ovlašćenja inspektora

Član 65.

Inspektor je ovlašćen da u postupku inspekcijskog nadzora:

1) nalaže otklanjanje utvrđenih nepravilnosti i za to ostavi rok;

2) zabranjuje upotrebu neadekvatnih postupaka i infrastrukture, i daje rok pružaocu usluga u kojem je dužan da obezbedi adekvatne postupke i infrastrukturu;

3) privremeno zabranjuje vršenje usluge pružaoca usluga do otklanjanja neadekvatnosti postupaka i infrastrukture;

4) naređuje privremeni opoziv nekog ili svih sertifikata izdatih od strane pružaoca usluge, ako postoji osnovana sumnja da se radi o neadekvatnom postupku ili falsifikatu.

VII. KAZNENE, PRELAZNE I ZAVRŠNE ODREDBE

Član 66.

Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj pružalac kvalifikovane usluge od poverenja – pravno lice ako:

1) ne preduzima potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga od poverenja (član 27. stav 1);

2) bez odlaganja, a najkasnije u roku od 24 sata od saznanja, ne obavesti Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge koji imaju značajan uticaj na pružanje usluga od poverenja ili na zaštitu podataka o ličnosti koji se obrađuju u okviru pružanja usluge (član 27. stav 3);

3) o povredi bezbednosti ili gubitku integriteta usluge, bez odlaganja, ne obavesti korisnika usluge od poverenja, ako bi ugrožavanje bezbednosti ili gubitak integriteta usluge od poverenja moglo nepovoljno uticati na korisnike usluga od poverenja (član 27. stav 4);

4) pre zaključenja ugovora iz člana 30. stav 1. ovog zakona ne obavesti lice koje je podnelo zahtev za pružanje kvalifikovane usluge po poverenja o svim važnim okolnostima korišćenja usluge iz člana 30. stav 2. tač. 1) - 3) ovog zakona (član 30. stav 2);

5) ne ispunjava uslove iz člana 31. (član 31);

6) pri izdavanju kvalifikovanog sertifikata za usluge od poverenja ne proveri podatke o identitetu fizičkog odnosno pravnog lica koji su sadržani u kvalifikovanom sertifikatu, u skladu sa članom 33. stav 2. zakona (član 33. st. 1. i 2);

7) ne izvrši proveru ispunjenosti uslova pre početka pružanja kvalifikovanih usluga od poverenja, odnosno najmanje jednom u 24 meseca (član 34. stav 3.);

8) ne izvrši nalog za vanredno ocenjivanje ispunjenosti uslova (član 34. stav 5);

9) pre otpočinjanja pružanja kvalifikovanih usluga od poverenja ne bude upisan u Registar pružaoca kvalifikovanih usluga od poverenja (član 35. stav 2);

10) izdavalac kvalifikovanih elektronskih sertifikata, koji namerava da prestane sa obavljanjem delatnosti, o nameri raskida ugovora ne obavesti svakog korisnika kvalifikovane usluge od poverenja i Ministarstvo najmanje tri meseca pre nastanka o nameravanom prestanku obavljanja delatnosti (član 36. stav 1);

11) u slučaju prestanka sa obavljanjem poslova ne obezbedi kod drugog pružaoca usluga od poverenja nastavak obavljanja usluge za korisnike kojima je izdao sertifikat, ili ne opozove sve izdate sertifikate i o preduzetim merama odmah ne obavesti Ministarstvo (član 36. stav 2);

12) ne dostavi svu dokumentaciju u vezi sa obavljanjem usluga od poverenja drugom izdavaocu na koga prenosi obaveze obavljanja jedne ili više usluga od poverenja, odnosno Ministarstvu (član 36. stav 3);

13) kvalifikovani elektronski sertifikat ne sadrži sve podatke iz člana 43. stav 1. ovog zakona (član 43. stav 1);

14) izdavalac kvalifikovanih sertifikata ne izvrši opoziv izdatih sertifikata, u slučajevima iz člana 44. stav 1. (član 44. stav 1);

15) izdavalac kvalifikovanih sertifikata ne obavesti korisnika kvalifikovane usluge od poverenja o opozivu sertifikata u roku od 24 časa od primljenog obaveštenja, odnosno nastanka okolnosti zbog kojih se sertifikat opoziva (član 44. stav 2);

16) izdavalac kvalifikovanih sertifikata ne čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovani sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja sertifikata (član 45);

17) ne obezbedi povezivanje sa Centralnim sistemom i ne omogući prijem i slanje poruka i u slučaju kada je pošiljalac ili primalac poruke korisnik drugog pružaoca usluge kvalifikovane elektronske dostave (član 56. stav 2);

18) pouzdano elektronsko čuvanje dokumenata pripremljenih u skladu sa članom 61. ovog zakona, kojima je kvalifikovanim elektronskim potpisom odnosno pečatom iz člana 61. stav 1. tačka 4) potvrđena vernost izvornom dokumentu i tačnost dodatno uključenih podataka, se ne vrši tako da se tokom čuvanja koriste postupci i tehnološka rešenja kojima se obezbeđuje mogućnost dokazivanja validnosti kvalifikovanog elektronskog potpisa odnosno pečata tokom celog perioda čuvanja (član 62. stav 2).

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice pružaoca usluge od poverenja novčanom kaznom od 5.000 do 100.000 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge od poverenja - fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara.

Član 67.

Novčanom kaznom od 50.000 do 200.000 dinara kazniće se za prekršaj korisnik kvalifikovane usluge od poverenja – pravno lice ako:

1) u slučaju promene podataka iz stava 1. člana 33. ovog zakona ne obavesti bez odlaganja pružaoca kvalifikovane usluge od poverenja (član 33. stav 3);

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom od 5.000 do 50.000 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se korisnik usluge od poverenja - fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 100.000 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se korisnik usluge od poverenja - fizičko lice novčanom kaznom od 5.000 do 50.000 dinara.

Član 68.

Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj registrovan pružalac usluge elektronske identifikacije – pravno lice ako:

1) šema elektronske identifikacije ne ispunjava uslove iz člana 17. (član 17);

2) ne preduzima potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga iz člana 22. stav 2. ovog zakona (član 22. st. 1. i 2);

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice pružaoca usluge elektronske identifikacije novčanom kaznom od 5.000 do 100.000 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge elektronske identifikacije – fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara.

Član 69.

Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj pružalac usluge iz člana 64. ovog zakona ako ne postupi po nalogu inspektora u ostavljenom roku iz člana 65. stav 1. ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice pružaoca usluge novčanom kaznom od 5.000 do 100.000 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge – fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara.

2. Prelazne i završne odredbe

Sprovođenje zakona

Član 70.

Podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona.

Prestanak važenja dosadašnjih propisa, nastavak primene podzakonskih akata i nastavak rada na osnovu prethodne registracije

Član 71.

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o elektronskom potpisu („Službeni glasnik RS”, broj 135/04) i Zakon o elektronskom dokumentu (Službeni glasnik RS”, broj 51/09).

Podzakonski akti doneti na osnovu zakona iz stava 1. ovog člana primenjivaće se i posle prestanka važenja navedenih zakona, sve do donošenja odgovarajućih propisa saglasno ovom zakonu, osim ako su u suprotnosti sa odredbama ovog zakona.

Danom stupanja na snagu ovog zakona sertifikaciona tela za izdavanje kvalifikovanih elektronskih sertifikata koja su registrovana na osnovu Zakon o elektronskom potpisu nastavljaju sa radom kao kvalifikovani pružaoci usluge izdavanje kvalifikovanih sertifikata za elektronski potpis.

Danom stupanja na snagu ovog zakona izdavaoci vremenskog žiga koji su registrovani na osnovu Zakona o elektronskom dokumentu nastavljaju sa radom kao kvalifikovani pružaoci usluge izdavanja kvalifikovanih elektronskih vremenskih žigova.

Sertifikaciona tela iz stava 3. ovog člana i izdavaoci vremenskog žiga iz stava 4. ovog člana dužni su da u roku od 12 meseci od dana stupanja na snagu ovog zakona usklade svoje poslovanje sa odredbama ovog zakona i dostave Ministarstvu izveštaj o ocenjivanju usaglašenosti iz člana 34. ovog zakona.

Ministarstvo vrši ocenjivanje usaglašenosti iz člana 34. ovog zakona do akreditacije prvog tela za ocenjivanje usaglašenosti, u skladu sa propisima.

Stupanje na snagu zakona

Član 72.

Ovaj zakon stupa na snagu osam dana od dana objavljivanja u „Službenom glasniku Republike Srbije”.

O B R A Z L O Ž E NJ E

I. USTAVNI OSNOV ZA DONOŠENjE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u članu 97. tač. 6. i 17. Ustava Republike Srbije, kojima je, između ostalog, propisano da Republika Srbija uređuje i obezbeđuje sistem obavljanja pojedinih privrednih i drugih delatnosti, kao i druge odnose od interesa za Republiku Srbiju.

II. RAZLOZI ZA DONOŠENjE ZAKONA

Republika Srbija je donošenjem Zakona o elektronskom potpisu („Službeni glasnik RS”, broj 135/04) i Zakona o elektronskom dokumentu („Službeni glasnik RS”, broj 51/09) započela proces razvoja pravnog okvira neophodnog za razvoj elektronskog poslovanja u našoj zemlji. Elektronski potpis, a posebno kvalifikovani elektronski potpis, postao je zakonom prepoznato sredstvo potvrde autentičnosti elektronskog dokumenta. Kvalifikovani elektronski potpis u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

U ovoj oblasti Evropska unija donela je Uredbu br. 910/2014 od 23. jula 2014. godine o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu, kojom je derogirana Direktiva 1999/93/EC o elektronskom potpisu. Uredbom se uređuju šeme elektronske identifikacije i usluge od poverenja u elektronskom poslovanju, koje uključuju elektronski potpis, elektronski pečat i druge vrste usluga od poverenja. U procesu pristupanja Evropskoj uniji Republika Srbija je u obavezi da izvrši usklađivanje svog zakonodavstva sa pravnom regulativom Evropske unije. Shodno tome, predloženim zakonom obuhvaćena su pravna rešenja predviđena navedenom uredbom.

Donošenjem zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju čini se korak dalje u pravnom uređivanju elektronskog poslovanja i to upravo uređivanje onih pitanja koja su bitna za praksu odnosno funkcionisanje elektronskog poslovanja u stvarnosti.

Pošto se informacione tehnologije i načini poslovanja izuzetno brzo menjaju, ocenjena je potreba da zakonska rešenja budu fleksibilna i otvorena za nova tehnološka dostignuća, da se zasnivaju na rešenjima sadržanim u međunarodnim dokumentima, propisima i standardima Evropske unije, a posebno na rešenjima tehnološki razvijenih zemalja.

Osnovni cilj zakonskog uređivanja je da se omogući i podstakne brže i efikasnije poslovanje i smanjenje troškova poslovanja, razvije tržište usluga od poverenja, modernizuje i, usled toga, učini efikasnijim rad organa javnih vlasti i privrednih subjekata, omogući građanima lakši i sigurniji pristup uslugama organa javne vlasti i drugih subjekata i pristup većem broju navedenih usluga, kao i pouzdano čuvanje elektronskih dokumenata, što će doprineti smanjenju troškova za čuvanje dokumentacije.

Posebni ciljevi zakonskog uređivanja sastoje se u tome da se pravnim uređenjem ove materije otvori prostor za intenzivnije elektronsko poslovanje, stvori poverenje najšire javnosti u upotrebu i razmenu elektronskih dokumenata, upotrebu

usluga od poverenja u elektronskom poslovanju i postigne konkurentnost na svetskim tržištima.

Ovaj zakon je podjednako značajan za građane, privredu, državnu upravu, lokalnu samoupravu i ostale subjekte, a njegova primena omogućava napredak i u međunarodnom položaju i delovanju.

Ključna zakonska rešenja uređuju sledeće oblasti:

- Elektronski dokument;
- Elektronska identifikacija;
- Usluge od poverenja;
- Elektronski potpis i elektronski pečat;
- Vremenski žig;
- Elektronska dostava;
- Autentikacija veb sajtova;
- Elektronsko čuvanje dokumenata.

U delu Predloga zakona kojim se uređuje elektronski dokument, utvrđeno je da se elektronskom dokumentu ne može osporiti punovažnost, dokazna snaga ili pisana forma samo zato što je u elektronskom obliku. Pored toga, predviđene su odredbe o izradi, formi prikaza, originalu i kopiji elektronskog dokumenta. Predlog zakona određuje da digitalizovani akt fizičkog ili pravnog lica (akt koji je izvorno u papirnom obliku i koji je primenom odgovarajućih postupaka konvertovan u elektronski oblik) ima istu dokaznu snagu kao originalni akt ukoliko je digitalizacija obavljena pod propisanim nadzorom i ako je istovetnost potvrđena kvalifikovanim elektronskim pečatom ili kvalifikovanim elektronskim potpisom. Digitalizacijom dokumenta postiže se smanjenje upotrebe dokumenata u papirnom obliku, veća pristupačnost dokumenata, i omogućava se i lakše pretraživanje, korišćenje i publikovanje dokumenata, što je posebno značajno i za efikasnije ostvarivanje prava građana na dostupnost informacija od javnog značaja. Predlog zakona predviđa i odredbu o dostavljanju elektronskih dokumenata između organa vlasti i stranaka, kojom je predviđeno da podnesak izrađen kao elektronski dokument fizička i pravna lica (stranke) dostavljaju organima vlasti putem elektronske pošte na adresu elektronske pošte koja je od strane organa vlasti određena za prijem elektronskih podnesaka, putem usluge kvalifikovane elektronske dostave ili drugim elektronskim putem, u skladu sa propisom, i ako je to predviđeno zakonima koji uređuju određene postupke. Dostavljanje dokumenata između organa vlasti obavlja se putem elektronske pošte, servisne magistrale organa putem usluge kvalifikovane elektronske dostave ili drugim elektronskim putem, u skladu sa posebnim propisom.

Prilikom pružanja svojih usluga elektronskim putem, organi javne vlasti, kao i drugi subjekti, mogu da vrše elektronsku identifikaciju lica kojima se usluga pruža. Elektronska identifikacija predstavlja postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji jednoznačno određuju pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta. Radi identifikovanja stranke kojoj se usluga pruža elektronskim putem, mogu se koristiti različite šeme identifikacije, koje pružaju visok, srednji ili osnovni nivo pouzdanosti u postupku elektronske identifikacije. Nivo pouzdanosti obično zavisi od toga da li koristimo jedan ili više faktora autentikacije i koliko su pouzdani pojedini faktori. Na primer, ako se koristi samo korisničko ime i lozinka to nije naročito visok nivo pouzdanosti. Ako se za uspešnu autentikaciju, pored lozinke, koristi i SMS poruka sa dodatnom jednokratnom šifrom, tada imamo dva faktora autentikacije i to je viši nivo pouzdanosti. Najviši nivoi pouzdanosti obično kao jedan faktor autentikacije uključuju karticu ili drugi uređaj koji je nemoguće iskopirati.

Predlog zakona predviđa uspostavljanje i vođenje registra pružalaca usluga elektronske identifikacije i šema elektronske identifikacije, u kome se vodi evidencija

o pružaocima usluga elektronske identifikacije, kao i o šemama elektronske identifikacije. Šema elektronske identifikacije koje su upisane u registar mogu se koristiti za utvrđivanje identiteta stranke u opštenju sa organom javne vlasti. Ukoliko je identitet stranke utvrđen putem registrovane šeme visokog nivoa pouzdanosti, takva identifikacija ima isto dejstvo kao potpis stranke na podnesku. U slučaju kada je to određeno posebnim propisom, identifikacija putem šeme srednjeg ili osnovnog nivoa može da ima isto dejstvo kao potpis stranke na podnesku, pod uslovom da su rizik od zloupotrebe i moguća šteta od zloupotrebe takvi da nije neophodno koristiti šemu visokog nivoa pouzdanosti.

Ovim zakonom uređuju se usluge od poverenja u elektronskom poslovanju, koje se zasnivaju na tome da pružalac usluge garantuje verodostojnost pojedinih podataka i koja je kao takva određena ovim zakonom. U elektronskom poslovanju je veoma važno da postoji pouzdanje u verodostojnost pojedinih podataka. Shodno tome, pružaoci usluga od poverenja imaju određene odgovornosti i moraju da ispune propisane uslove kako bi njihova usluga mogla da se smatra uslugom od poverenja. Usluge od poverenja mogu da se pružaju i kao kvalifikovane usluge od poverenja, i u tom slučaju pružalac kvalifikovane usluge od poverenja mora da ispuni posebne tehničke, organizacione i bezbednosne uslove, kako bi obezbedio viši nivo pouzdanosti usluge koju pruža. Kvalifikovanim uslugama od poverenja se obezbeđuje pravno dejstvo i dokazna snaga dokumenata i podataka koji se koriste u elektronskom obliku. Da bi obavljao kvalifikovanu uslugu od poverenja, pružalac kvalifikovanih usluga od poverenja je u obavezi da se upiše u registar koji vodi ministarstvo nadležno za primenu ovog zakona.

Predlog zakona uređuje usluge od poverenja u oblasti elektronskog potpisa, elektronskog pečata, elektronskog vremenskog žiga, elektronske dostave, autentikacije veb sajtova i elektronskog čuvanja dokumenta.

Elektronski potpis odnosno pečat predstavljaju skup podataka u elektronskom obliku kojima se potvrđuje integritet tih podataka i identitet potpisnika, odnosno pečatioca.

Osnovna usluga od poverenja u oblasti elektronskog potpisa, odnosno pečata jeste izdavanje kvalifikovanog elektronskog sertifikata. Kvalifikovani sertifikat predstavlja elektronsku potvrdu kojom se potvrđuje veza između podataka za validaciju elektronskog potpisa odnosno pečata i identiteta potpisnika odnosno pečatioca.

Prilikom izdavanja kvalifikovanog elektronskog sertifikata izdaju se i odgovarajući podaci za kreiranje elektronskog potpisa odnosno pečata pohranjeni u okviru kvalifikovanog sredstva za kreiranje elektronskog potpisa odnosno pečata.

Kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata kreira se kvalifikovani elektronski potpis odnosno pečat tako da bude pridružen podacima koji se potpisuju odnosno pečatiraju.

Ispravnost kvalifikovanog elektronskog potpisa odnosno pečata, uz uzimanje u obzir i podataka koji su potpisani odnosno pečatirani, proverava se u odnosu na kvalifikovani elektronski sertifikat u postupku validacije.

Potpisivanje odnosno pečatiranje vrši potpisnik odnosno pečatilac kome je izdat elektronski sertifikat i u čijem je posedu sredstvo za kreiranje elektronskog potpisa odnosno pečata, a proveru ispravnosti potpisa odnosno pečata (validaciju) vrši pouzdajuća strana.

Pored usluge izdavanja kvalifikovanih elektronskih sertifikata, u oblasti elektronskog potpisa i elektronskog pečata uređene su još po dve kvalifikovane usluge od poverenja:

- usluga kvalifikovane validacije kvalifikovanog elektronskog potpisa odnosno pečata i
- usluga upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata;

Predmet usluge kvalifikovane validacije je postupak validacije, pri čemu pružalac usluge poseduje tehnološka sredstva i stručna znanja potrebna za pravilnu validaciju.

Usluga upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa znači da se sredstvo za kreiranje elektronskog potpisa čuva kod pružaoca usluge, tako da pružalac usluge na zahtev korisnika tehnički formira elektronski potpis koji je formalno kreiran u ime korisnika usluge kao potpisnika.

Ovim zakonom se predviđaju uslovi za kvalifikovane elektronske sertifikate, odnosno njihov sadržaj, opoziv i suspenziju, kao i čuvanje dokumentacije o izdatim i opozvanim kvalifikovanim sertifikatima.

Za kreiranje elektronskog potpisa i pečata koriste se kvalifikovana sredstva za kreiranje elektronskog potpisa i pečata (tehnička sredstva - softver odnosno hardver). Ovim zakonom su predviđeni uslovi koje moraju da ispune ta sredstva, i njihova sertifikacija.

Kvalifikovane usluge od poverenja u oblasti elektronskog potpisa i elektronskog pečata obezbeđuju punovažnost i dokaznu snagu kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata, i ne može im se osporiti punovažnost i dokazna snaga samo što su u elektronskom obliku.

Pojam naprednog elektronskog potpisa odnosno pečata je uveden zbog uređenja slučajeva kada je potreban visok nivo pouzdanosti elektronskog potpisa odnosno pečata, a iz formalnih ili praktičnih razloga nije primereno predvideti kvalifikovani elektronski potpis odnosno pečat. Primer je napredni elektronski pečat na Javnoj listi kvalifikovanih usluga od poverenja, jer takvu listu nije primereno potpisivati na bazi sertifikata koji je izdat od strane pružaoca usluga sa liste.

Napredni elektronski potpis odnosno pečat predstavlja širi pojam od kvalifikovanog elektronskog potpisa odnosno pečata, što znači da svi uslovi koji važe za napredni elektronski potpis odnosno pečat, važe i za kvalifikovani elektronski potpis odnosno pečat, uz dodatak da kvalifikovani elektronski potpis odnosno pečat treba da je kreiran kvalifikovanim sredstvom i na bazi kvalifikovanog elektronskog sertifikata.

Predlog zakona uređuje uslugu elektronske dostave, koja predstavlja uslugu prenosa podataka elektronskim putem u okviru koje pružalac usluge obezbeđuje dokaze o postupanju sa prenesenim podacima, uključujući dokaz slanja i prijema podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja odnosno bilo kojih neovlašćenih promena.

Predlogom zakona su propisani i uslovi za elektronsko čuvanje dokumenata. Uređuje se priprema dokumenta za pouzdano elektronsko čuvanje, čime se obezbeđuje da svi bitni elementi sadržaja izvornog dokumenta budu preneti u dokument koji se elektronski čuva, odnosno da dokument koji se elektronski čuva bude veran izvornom dokumentu. Pouzdano elektronsko čuvanje obezbeđuje mogućnost dokazivanja validnosti kvalifikovanog elektronskog potpisa odnosno pečata tokom celog perioda čuvanja.

III. OBJAŠNjENjE OSNOVNIH PRAVNIH INSTITUTA I POJEDINAČNIH REŠENjA

Članom 1. ovog zakona definisan je predmet zakona.

Članom 2. ovog zakona određeno je značenje izraza koji se koriste u smislu ovog zakona.

Članom 3. ovog zakona određena je primena ovog zakona.

Članom 4. ovog zakona utvrđeno je postupanje koje se odnosi na obradu i zaštitu podataka.

Članom 5. ovog zakona propisano je da postupak elektronske identifikacije i autentikacije može biti pokrenut samo na zahtev pravnog ili fizičkog lica koje je predmet identifikacije, osim ako je propisom drugačije određeno.

Članom 6. ovog zakona definiše se dostupnost i pristup usluga od poverenja, usluga elektronske identifikacije i proizvoda osobama sa invaliditetom.

Članom 7. ovog zakona utvrđuje se punovažnost i dokazna snaga elektronskog dokumenta.

Članom. 8. ovog zakona definiše se izrada elektronskog dokumenta.

Članom 9. ovog zakona definiše se forma prikaza elektronskog dokumenta.

Članom 10. ovog zakona uređuju se original i kopija elektronskog dokumenta.

Članom 11. ovog zakona utvrđuje se overa digitalizovanog akta.

Članom 12. ovog zakona uređuje se overa kopije elektronskog akta na papiru.

Članom 13. ovog zakona uređuje se potvrda o prijemu elektronskog dokumenta.

Članom 14. ovog zakona određeno je da se svaki primljeni elektronski dokument smatra posebnim dokumentom, osim ako je više puta primljen istovetan dokument i primalac je znao ili je morao znati da je reč o istovetnom dokumentu.

Članom 15. ovog zakona predviđeno je dostavljanje elektronskih dokumenata između organa vlasti i stranaka.

Članom 16. ovog zakona utvrđuje se dostavljanje elektronskih dokumenata između organa vlasti.

Članom 17. ovog zakona definišu se uslovi koje mora da ispunjava šema elektronske identifikacije.

Članom 18. ovog zakona određuju se nivoi pouzdanosti šema elektronske identifikacije.

Članom 19. ovog zakona određuje se Registar pružalaca usluga elektronske identifikacije i šema elektronske identifikacije.

Članom 20. ovog zakona određuje se korišćenje šema elektronske identifikacije u elektronskom poslovanju i u opštenju sa organima javne vlasti.

Članom 21. ovog zakona određuje se odgovornost pri elektronskoj identifikaciji.

Članom 22. ovog zakona utvrđuju se bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga elektronske identifikacije.

Članom 23. ovog zakona definiše se saradnja Ministarstva sa nadležnim telima EU u pogledu interoperabilnosti tehničkih sistema.

Članom 24. ovog zakona utvrđuje se prijavljivanje registrovanih šema elektronskog identiteta koje ispunjavaju uslove iz Uredbe EU br. 910/2014 Evropskog parlamenta i Saveta (Uredba eIDAS).

Članom 25. ovog zakona uređuje se odgovornost pružaoca usluga od poverenja i teret dokazivanja.

Članom 26. ovog zakona utvrđuje se odgovornost korisnika usluga od poverenja za čuvanje sredstava i podataka za formiranje elektronskog potpisa odnosno pečata.

Članom 27. ovog zakona definišu se bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga od poverenja.

Članom 28. ovog zakona utvrđuje se nadležnost ministarstva nadležnog za poslove informacionog društva u primeni ovog zakona.

Članom 29. ovog zakona utvrđuju se nadležnosti Ministarstva u okviru prekogranične saradnje u oblasti usluga od poverenja.

Članom 30. ovog zakona utvrđuje se uspostavljanje odnosa između pružaoca kvalifikovane usluge od poverenja i korisnika kvalifikovane usluge od poverenja.

Članom 31. ovog zakona utvrđuju se uslovi za pružanje kvalifikovanih usluga od poverenja.

Članom 32. ovog zakona utvrđuje se propisivanje najnižeg iznosa osiguranja od rizika odgovornosti za štetu nastalu vršenjem usluge kvalifikovane usluge od poverenja.

Članom 33. ovog zakona definiše se provera identiteta korisnika kvalifikovane usluge od poverenja.

Članom 34. ovog zakona uređuje se ocenjivanje ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja.

Članom 35. ovog zakona uređuje se početak pružanja kvalifikovanih usluga od poverenja.

Članom 36. ovog zakona uređuje se postupanje u slučaju prestanka pružanja usluge izdavanja kvalifikovanih elektronskih sertifikata.

Članom 37. ovog zakona utvrđuje se da državni organ može postati pružalac usluga od poverenja na osnovu uredbe Vlade ukoliko ispunjava sve uslove za pružanje usluga predviđenih zakonom.

Članom 38. ovog zakona reguliše se objavljivanje Javne liste kvalifikovanih usluga od poverenja.

Članom 39. ovog zakona definiše se znak pouzdanosti za kvalifikovane usluge od poverenja.

Članom 40. ovog zakona utvrđuje se prekogranično priznavanje kvalifikovanih usluga od poverenja.

Članom 41. ovog zakona definišu se usluge od poverenja i kvalifikovane usluge od poverenja.

Članom 42. ovog zakona utvrđuju se uslovi za napredni elektronski potpis i napredni elektronski pečat.

Članom 43. ovog zakona utvrđuje se sadržaj kvalifikovanog elektronskog sertifikata.

Članom 44. ovog zakona uređuje se opoziv i suspenzija kvalifikovanog elektronskog sertifikata.

Članom 45. ovog zakona propisuje se čuvanje dokumentacije o izdatim i opozvanim kvalifikovanim sertifikatima.

Članom 46. ovog zakona definišu se uslovi koje moraju da ispune kvalifikovana sredstva za kreiranje elektronskog potpisa i pečata.

Članom 47. ovog zakona definiše se sertifikacija sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata.

Članom 48. ovog zakona utvrđuje se postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

Članom 49. ovog zakona definišu se uslovi za uslugu kvalifikovane validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata.

Članom 50. ovog zakona utvrđuje se pravno dejstvo kvalifikovanog elektronskog potpisa.

Članom 51. ovog zakona utvrđuje se pravno dejstvo kvalifikovanog elektronskog pečata.

Članom 52. ovog zakona utvrđuju se uslovi za kvalifikovane elektronske vremenske žigove.

Članom 53. ovog zakona utvrđuje se pravno dejstvo elektronskog vremenskog žiga.

Članom 54. ovog zakona utvrđuju se uslovi za uslugu kvalifikovane elektronske dostave.

Članom 55. ovog zakona uređuje se potvrda o elektronskoj dostavi.

Članom 56. ovog zakona propisuje se razmena elektronskih poruka između pružalaca usluge kvalifikovane elektronske dostave.

Članom 57. ovog zakona utvrđuje se pravno dejstvo usluge elektronske dostave.

Članom 58. ovog zakona uređuju se kvalifikovani sertifikati za autentikaciju veb sajtova.

Članom 59. ovog zakona utvrđuje se sadržaj kvalifikovanih sertifikata za autentikaciju veb sajtova.

Članom 60. ovog zakona definiše se priprema dokumenta za elektronsko čuvanje.

Članom 61. ovog zakona propisuju se uslovi za pripremu dokumenta za pouzdano elektronsko čuvanje.

Članom 62. ovog zakona definiše se pouzdano elektronsko čuvanje.

Članom 63. ovog zakona definiše se usluga kvalifikovanog elektronskog čuvanja dokumenta.

Članom 64. ovog zakona utvrđuju se poslovi inspekcije za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju.

Članom 65. ovog zakona utvrđuju se ovlašćenja inspektora.

Čl. 66, 67, 68. i 69. ovog zakona propisuju se kaznene odredbe.

Članom 70. ovog zakona utvrđuje se rok za donošenje podzakonskih akata.

Članom 71. ovog utvrđuje se prestanak važenja dosadašnjih propisa, nastavak primene podzakonskih akata i nastavak rada na osnovu prethodne registracije.

Članom 72. ovog zakona uređuje se stupanje na snagu zakona osmog dana od objavljivanja u „Službenom glasniku Republike Srbije".

IV. SREDSTVA POTREBNA ZA SPROVOĐENjE ZAKONA

Sredstva za realizaciju zakona u narednim godinama realizovaće se u skladu sa bilansnim mogućnostima budžeta Republike Srbije i predviđenim limitima.

Za sprovođenje ovog zakona potrebno je obezbediti sredstva u budžetu Republike Srbije za 2017, 2018. i 2019. godinu u iznosu od 22.901.000,00 dinara, odnosno 12.225.000,00 dinara u 2017. godini i po 5.338.000,00 dinara u 2018. i 2019. godini na razdelu Ministarstva trgovine, turizma i telekomunikacija.

Predlogom zakona predviđeno je da se Ministarstvo stara o Centralnom sistemu za razmenu poruka kvalifikovane elektronske dostave. Usled toga, za uspostavljanje Centralnog sistema za razmenu poruka kvalifikovane elektronske dostave predviđeno je 10.000.000,00 dinara u 2017. godini i po 2.000.000 dinara u 2018. i 2019. godini za održavanje Centralnog sistema.

Predlogom zakona predviđeni su inspekcijski poslovi koje bi trebalo da obavljaju tri državna službenika na mestu rada inspektora za inspekcijski nadzor ali za navedene poslove neće biti potrebe za novozaposlenima, već će se sagledati mogućnosti da se od postojećeg broja zaposlenih izvrši preraspodela poslova u navedenom ministarstvu, imajući u vidu ograničenje novog zapošljavanja i postupak započete racionalizacije u javnom sektoru.

Troškovi	2017	2018	2019	UKUPNO
Rashodi za zaposlene	2.225.000,00	3.338.000,00	3.338.000,00	8.901.000,00
Osnovna sredstva	10.000.000,00	2.000.000,00	2.000.000,00	14.000.000,00
UKUPNO	**12.225.000,00**	**5.338.000,00**	**5.338.000,00**	**22.901.000,00**

V. ANALIZA EFEKATA ZAKONA

1. Problemi koje akt treba da reši

Republika Srbija je donošenjem Zakona o elektronskom potpisu („Službeni glasnik RS", broj 135/04) i Zakona o elektronskom dokumentu („Službeni glasnik RS", broj 51/09) započela proces razvoja pravnog okvira neophodnog za razvoj elektronskog poslovanja u našoj zemlji.

Problemi koje donošenje zakona treba da reši su:

- Delimična neusklađenost sa EU regulativom;

- Nedovoljna interoperabilnost usluga od poverenja u RS sa uslugama od poverenja EU;
- Potreba za većim nivoom pouzdanosti usluga od poverenja u elektronskom poslovanju;
- Izjednačavanje poslovanja elektronskim putem sa klasičnim poslovanjem.

U ovoj oblasti Evropska unija donela je Uredbu br. 910/2014 od 23. jula 2014. godine o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu, kojom je derogirana Direktiva 1999/93/EC o elektronskom potpisu. Uredbom se uređuju šeme elektronske identifikacije i usluge od poverenja u elektronskom poslovanju, koje uključuju elektronski potpis, elektronski pečat i druge vrste usluga od poverenja. U procesu pristupanja Evropskoj uniji Republika Srbija je u obavezi da izvrši usklađivanje svog zakonodavstva sa pravnom regulativom Evropske unije. Kako trenutni zakonski okvir u ovoj oblasti u Republici Srbiji ne sadrži sva rešenja predviđena propisom EU, shodno tome, Predlogom zakona celokupna materija iz navedene uredbe, odnosno izvršeno je usklađivanje sa EU regulativom.

Pošto se informacione tehnologije i načini poslovanja izuzetno brzo menjaju, ocenjena je potreba da zakonska rešenja budu fleksibilna i otvorena za nova tehnološka dostignuća, da se zasnivaju na rešenjima sadržanim u međunarodnim dokumentima, propisima i standardima Evropske unije, a posebno na rešenjima tehnološki razvijenih zemalja. Definisanje usluga od poverenja u Predlogu zakona omogućuje interoperabilnost sa uslugama od poverenja u zemljama EU, čime se otvara mogućnost da Srbija bude u istom rangu sa zemljama EU kada je u pitanju elektronsko poslovanje. Takođe, ovaj zakon će omogućiti da se, nakon ulaska u Evropsku uniju, šeme elektronske identifikacije i kvalifikovane usluge od poverenja registrovane u Republici Srbiji ravnopravno koriste i priznaju u Evropskoj uniji.

U Republici Srbiji u ovom trenutku regulisane su dve vrste usluga u ovoj oblasti: izdavanje kvalifikovanih elektronskih sertifikata za elektronski potpis i izdavanje vremenskog žiga. Pružaoci ovih usluga dužni su da, pre početka obavljanja usluga, budu upisani u registar koje vodi ministarstvo nadležno za poslove informacionog društva. Da bi bili upisani u registar, ovi subjekti moraju da ispune tehničke, organizacione i bezbednosne uslove koje se zahtevaju u Zakonu o elektronskom potpisu, odnosno Zakonu o elektronskom dokumentu, kao i podzakonskim aktima donetim na osnovu ovog zakona. U Registar izdavalaca kvalifikovanih elektronskih sertifikata upisano je šest izdavalaca:

R.br.	Naziv sertifikacionog tela
1.	Javno preduzeće „Pošta Srbije” – Sertifikaciono telo Pošte
2.	Privredna komora Srbije – PKC CA
3.	MUP RS – Sertifikaciono telo MUP RS
4.	HALCOM BG CA
5.	„E-Smart Systems” d.o.o. – ESS CA
6.	Sertifikaciono telo Ministarstva odbrane i Vojske Srbije

U Republici Srbiji je do sada izdato oko 300.000 kvalifikovanih elektronskih sertifikata.

U Registar izdavalaca vremenskog žiga upisana su 2 izdavalaca:

R.br.	Naziv izdavaoca
1.	Direkcija za elektronsku upravu
2.	Javno preduzeće „Pošta Srbije" – Sertifikaciono telo Pošte

Novi zakon povećava broj usluga od poverenja u elektronskom poslovanju i reguliše uslove za njihovo obavljanje. Ovim zakonom uređuju se usluge od poverenja u elektronskom poslovanju, koje predstavljaju elektronske usluge koje olakšavaju poslovnu aktivnost između dve ili više strana pri čemu se zasnivaju na tome da pružalac usluge stranama garantuje verodostojnost pojedinih podataka, a koje su kao takva određena ovim zakonom. U elektronskom poslovanju je veoma važno da postoji pouzdanje u verodostojnost pojedinih podataka. Shodno tome, Predlogom zakona je predviđeno da pružaoci usluga od poverenja imaju određene odgovornosti i moraju da ispune propisane uslove kako bi njihova usluga mogla da se smatra uslugom od poverenja. Usluge od poverenja mogu da se pružaju i kao kvalifikovane usluge od poverenja, i u tom slučaju pružalac kvalifikovane usluge od poverenja mora da ispuni posebne tehničke, organizacione i bezbednosne uslove, kako bi obezbedio viši nivo pouzdanosti usluge koju pruža. Definisanjem uslova za pružanje kvalifikovanih usluga od poverenja u skladu sa evropskim standardima obezbeđuje se viši nivo pouzdanosti ovih usluga i sigurnost elektronskog poslovanja. Pored toga, izuzetno je značajno što se Predlogom zakona uspostavlja praksa interoperabilne i jednostavne upotrebe kvalifikovanih elektronskih sertifikata, koja je jednostavna za korisnike sertifikata, za one koji verifikuju elektronski potpis formiran na bazi sertifikata, kao i za one koji razvijaju tehnička rešenja bazirana na elektronskim sertifikatima i elektronskom potpisu. Uspostavljanje interoperabilnosti u okviru Republike Srbije, od značaja je za prekograničnu interoperabilnost usluga od poverenja, a posebno sa članicama EU.

Ovim zakonom se uspostavlja sistemska zakonska osnova i za izjednačavanje klasičnog sa elektronskim poslovanjem i ujedno se utiče na povećanje obima elektronskog poslovanja u Republici Srbiji tako što zakon predviđa nove usluge od poverenja, odnosno šeme elektronske identifikacije i kvalifikovane usluge od poverenja, kojima se obezbeđuje pravno dejstvo i dokazna snaga ekvivalentna odgovarajućim radnjama u klasičnom poslovanju. Naime, iako je do sada kvalifikovanom elektronskom potpisu bilo priznato jednako dejstvo i dokazna snaga kao i svojeručnom potpisu, to nije bilo dovoljno da se obezbedi potpun prelazak sa klasičnog na elektronsko poslovanje. Na primer, nedostatak uređenja pouzdane elektronske dostave i čuvanja elektronskog dokumenta doveo je do toga da se postupci pred organima javne vlasti otežano sprovode elektronskim putem, s obzirom da je u mnogim slučajevima neophodna garancija da su dokumenti i podaci poslati ili primljeni u vreme čija je tačnost pouzdana. Predlogom zakona su uvedene nove usluge – elektronski pečat, elektronska dostava i čuvanje elektronskih dokumenata, putem kojih će se pouzdano garantovati tačnost određenih podataka.

2. Ciljevi koji se aktom postižu

Donošenjem Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju čini se korak dalje u pravnom uređivanju elektronskog poslovanja i to upravo uređivanje onih pitanja koja su bitna za praksu odnosno funkcionisanje elektronskog poslovanja u stvarnosti.

Osnovni cilj zakonskog uređivanja je da se regulisanjem šema elektronske identifikacije i razvojem tržišta usluga od poverenja uklone barijere da se sa klasičnog pređe na elektronsko poslovanje, čime se postiže:

- brže i efikasnije poslovanje i smanjenje troškova poslovanja privrednih subjekata, organa javne vlasti i građana,
- modernizacija i efikasniji rad organa javnih vlasti,
- lakši i sigurniji pristup uslugama organa javne vlasti i drugih subjekata koje se pružaju elektronskim putem, kao i pristup većem broju tih usluga.

Primenom zakonskih rešenja omogućiće se brže i efikasnije poslovanje, budući da se korišćenjem usluga predviđenih zakonom značajno smanjuje vreme koje je potrebno za izvršenje određenih poslova i transakcija. Poslovi će lakše moći da se obavljaju elektronski, bez potrebe odlaska na šaltere, u određene institucije, i bez fizičkog kontakta čime se štede materijalni resursi (troškovi prevoza, papira i sl.) i vreme koje je potrebno u klasičnom poslovanju.

Očekuje se da će zakon doprineti modernizaciji i efikasnijem radu organa javne vlasti, jer će se unaprediti preduslovi za izradu akata u elektronskom obliku, urediti elektronski prijem i dostava dokumenata u postupcima koje sprovode i obezbediti pouzdano elektronsko čuvanje dokumenata.

Regulisanjem šema elektronskih identifikacija i usluga od poverenja omogućiće se lakši i sigurniji pristup uslugama organa javne vlasti i drugih subjekata koji se pružaju elektronskim putem, s obzirom da će se propisati uslovi za pružanje ovih usluga koji obezbeđuju poverenje u verodostojnost podataka koji se pružaju i da će se odrediti odgovarajuće pravno dejstvo tih usluga. To će uticati da se broj usluga koje se vrše elektronskim putem poveća, da korisnici više upotrebljavaju ove usluge i tako će se značajno uticati na povećanje obima elektronskog poslovanja u Republici Srbiji.

3. Razmatrane mogućnosti da se problem reši i bez donošenja akta

Postojeća rešenja u važećim propisima ne uređuju sva ključna pitanja od značaja za prelazak sa klasičnog na elektronsko poslovanje koja su prepoznata u aktuelnom zakonodavnom okviru EU, iz čega proizlazi da je donošenje novog zakona neophodno. Trenutno važeći propisi regulišu pravno dejstvo kvalifikovanog elektronskog potpisa, a predmetnim Predlogom zakona je regulisano i pravno dejstvo elektronske identifikacije i novih usluga od poverenja. Takođe, priznavanje punovažnosti i dokazne snage elektronskog dokumenta i usluga od poverenja mora da bude uređeno zakonom, kako bi se elektronsko poslovanje moglo da obavlja jednako kao i klasično poslovanje. Pored toga, postojala je neophodnost da se ovim propisom urede uslovi za pružanje usluga kvalifikovanih usluga od poverenja i stvori mehanizam nadzora nad primenom zakonskih normi.

Imajući u vidu da je u postupku pridruživanja Evropskoj uniji Republika Srbija preuzela obavezu da do 2018. godine uskladi svoje zakonodavstvo sa propisima EU, potrebno je izvršiti usklađivanje zakonodavstva donošenjem ovog zakona i time ispuniti preuzete obaveze. Evropska unija je 2014. godine donela gore

navedenu uredbu koja predstavlja novi pravni okvir u ovoj oblasti i sa kojom se vrši usklađivanje u ovoj oblasti.

4. Zašto je donošenje akta najbolji način za rešavanje problema

U delu koji se tiče kvalifikovanih usluga od poverenja, Predlogom zakona su predviđeni tehnički, organizacioni i bezbednosni uslovi koje moraju da ispune pružaoci ovih usluga, i koji su u skladu sa međunarodnim propisima i standardima u ovoj oblasti. Propisivanjem obaveza pružaocima kvalifikovanih usluga od poverenja postiže se neophodan nivo pouzdanosti usluga koje pružaju, čime se stvara osnov za pouzdano elektronsko poslovanje. Dalje, zakonom je predviđena obaveza za pružaoce kvalifikovanih usluga od poverenja da se upišu u registar koji vodi nadležno ministarstvo, što je jedan od uslova za pružanje ovih usluga. Objavljivanjem registra, odnosno Javne liste kvalifikovanih usluga od poverenja, omogućava se da korisnici i pouzdajuće strane imaju informaciju o tome koji su pružaoci usluga od poverenja kvalifikovani, odnosno koji se smatraju pouzdanim za vršenje usluga od poverenja. Takođe, ulaskom u Evropsku uniju, Javna lista kvalifikovanih usluga od poverenja biće dostupna korisnicima i trećim licima iz država članica EU.

Kako bi se vršila pravovremena provera ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja, Predlogom zakona je predviđen inspekcijski nadzor, što je neophodno predvideti zakonom.

Pored toga, Predlogom zakona će se izvršiti neophodno usklađivanje sa propisima EU u ovoj oblasti, čime će Republika Srbija ispuniti svoje obaveze u postupku pridruživanja Evropskoj uniji. Uslovi za pružanje usluga elektronske identifikacije i usluga od poverenja biće u skladu sa evropskim propisima i standardima, što će doprineti postizanju interoperabilnosti, odnosno priznavanju dejstva ovih usluga kada Republika Srbija postane članica EU.

Kako je za sva navedena rešenja problema neophodno dopuniti zakonsko uređenje, to je donošenje zakona najbolji način za rešavanje problema, a pošto u datoj oblasti postoji EU uredba, a s obzirom na utvrđenu politiku pristupanja EU, ocenjujemo da je najbolji način za rešavanje problema donošenje zakona koji je harmonizovan sa odgovarajućim propisima EU.

5. Na koga će i kako će najverovatnije uticati rešenja u zakonu

Zakon je podjednako značajan za građane, privredu, državnu upravu, lokalnu samoupravu i ostale subjekte, a njegova primena omogućava napredak i u međunarodnom položaju i delovanju.

Građani i privreda će imati koristi od rešenja u ovom zakonu zato što će se regulisanjem elektronske identifikacije i usluga od poverenja u elektronskom poslovanju stvoriti prostor za povećano korišćenje elektronskih servisa, odnosno međusobnih elektronskih transakcija. Naime, propisivanjem uslova za šeme elektronske identifikacije i kvalifikovane usluge od poverenja zahteva se od pružaoca ovih usluga da ispune zahteve čijim ostvarivanjem se može pouzdano garantovati verodostojnost podataka (podaci o identitetu fizičkog, odnosno pravnog lica, vremenu izrade dokumenta, vremenu slanja, odnosno prijema podataka itd.). Pružaoci usluga će morati da ispune tehničke, bezbednosne i organizacione uslove kako bi mogli da pružaju usluge elektronske identifikacije i kvalifikovane usluge od poverenja. Zakon utvrđuje da se ovim uslugama ne može osporiti punovažnost ili dokazna snaga samo zato što su u elektronskom obliku, što im daje pravno dejstvo na osnovu koga se elektronsko poslovanje putem ovih

usluga može vršiti ravnopravno sa klasičnim poslovanjem, i omogućava da se podaci generisani putem ovih usluga ne mogu osporiti samo zato što su u elektronskom obliku. To će sve omogućiti da stranke (fizička i pravna lica) mogu da koriste usluge koji će pouzdano potvrditi verodostojnost određenih podataka prilikom elektronskih transakcija.

U zakonu su prepoznate dve grupe pružaoca usluga od poverenja, i to: kvalifikovani (upisani u odgovarajući registar) i pružaoci usluga od poverenja koji nisu upisani u registar. Pružaoci usluga od poverenja, i pružaoci kvalifikovanih usluga od poverenja imaju obavezu da ispune bezbednosne uslove za pružanje usluga od poverenja. Oni su dužni da preduzimaju tehničke i organizacione mere kojima se osigurava da nivo bezbednosti odgovara stepenu rizika, uzimajući u obzir najnovija dostupna tehnološka rešenja, a posebno se preduzimaju mere za sprečavanje bezbednosnih incidenata i ograničavanje štetnih posledica eventualnih incidenata, kao i za obaveštavanje zainteresovanih strana o neželjenim efektima bezbednosnih incidenata.

S druge strane, pružaoci kvalifikovanih usluga od poverenja, pored bezbednosnih uslova, moraju da ispune i druge uslove predviđene zakonom, kako bi bili upisani u Registar kvalifikovanih pružalaca usluga od poverenja. Kvalifikovani pružaoci usluga od poverenja vrše svoje usluge u oblastima elektronskog potpisa, elektronskog pečata, elektronske dostave, autentikacije veb sajtova i elektronskog čuvanja dokumenata. Zakon propisuje opšte uslove koje će morati da ispune svi pružaoci kvalifikovanih usluga od poverenja, kao i posebne uslove koji treba da se ispune u oblasti u kojoj se usluga pruža. Radi se o tehničkim, bezbednosnim i organizacionim uslovima čijim ispunjenjem se postiže poverenje u uslugu koju pružalac pruža i daje se status kvalifikovane usluge, koja ima pravno dejstvo izjednačeno sa klasičnim poslovanjem, kao i dokaznu snagu. Da bi stekli status kvalifikovanih pružaoca usluga od poverenja, pružaoci ovih usluga moraju da se upišu u navedeni registar. Jedan od uslova za upis u registar je dostavljanje izveštaja o ocenjivanju usaglašenosti, koje izrađuje telo za ocenjivanje usaglašenosti koje je, u skladu sa zakonom kojim se uređuje akreditacija, akreditovano za ocenjivanje usaglašenosti pružaoca kvalifikovanih usluga od poverenja i kvalifikovanih usluga od poverenja koje oni pružaju.

Zakon će uticati na organe javne vlasti i privredne subjekte, koji će u većoj meri, primenom kvalifikovanih usluga od poverenja, moći da akte koje donose u svom radu (rešenja, odluke, zaključke, potvrde…) izdaju u obliku elektronskog dokumenta. Elektronske dokumente će organi javne vlasti moći da dostavljaju drugim organima javne vlasti, kao i građanima, što će omogućiti veću efikasnost u sprovođenju različitih postupaka. Zakon će uticati na rad organa javne vlasti i drugih subjekata tako što će se omogućiti i digitalizacija akata koji su nastali u papirnom obliku (digitalizovani akti). Imajući u vidu da je digitalizacija dokumenata koji su nastali u papiru veoma značajna za ispunjenje ciljeva zakona, predviđeno je da digitalizovani akt fizičkog ili pravnog lica (akt koji je izvorno u papirnom obliku i koji je primenom odgovarajućih postupaka konvertovan u elektronski oblik) ima istu dokaznu snagu kao originalni akt ukoliko je digitalizacija obavljena pod propisanim nadzorom i ako je istovetnost potvrđena kvalifikovanim elektronskim pečatom ili kvalifikovanim elektronskim potpisom. Digitalizacijom dokumenta postiže se smanjenje upotrebe dokumenata u papirnom obliku, veća pristupačnost dokumenata, i omogućava se i lakše pretraživanje, korišćenje i publikovanje dokumenata, što je posebno značajno i za efikasnije ostvarivanje

prava građana na dostupnost informacija od javnog značaja. Takođe, organi javne vlasti i privredni subjekti imaju veliku potrebu za regulisanjem čuvanja elektronskih dokumenata, s obzirom na obaveze i potrebe da se elektronski dokumenti nastali u radu čuvaju u određenom vremenskom periodu. Zakon propisuje uslove koji su neophodni za pouzdano čuvanje dokumenata i reguliše važan segment poslovanja navedenih subjekata. Ova pravila su važna i za čuvanje javne arhivske građe i dokumentarnog materijala u elektronskom obliku.

Zakon će doprineti da organi javne vlasti omoguće veći broj svojih usluga koje pružaju elektronskim putem, gde su posebno bitne odredbe o elektronskoj identifikaciji. Naime, prilikom pružanja svojih usluga elektronskim putem, organi javne vlasti, kao i drugi subjekti, mogu da vrše elektronsku identifikaciju lica kojima se usluga pruža. Elektronska identifikacija predstavlja postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji jednoznačno određuju pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta. Radi identifikovanja stranke kojoj se usluga pruža elektronskim putem, mogu se koristiti različite šeme identifikacije, koje pružaju visok, srednji ili nizak nivo pouzdanosti u postupku elektronske identifikacije. Najviši nivoi pouzdanosti obično kao jedan faktor autentikacije uključuju karticu ili drugi uređaj koji je nemoguće iskopirati. Predlogom zakona je predloženo da u opštenju stranke sa organima javne vlasti identitet stranke utvrđen na osnovu registrovane šeme elektronske identifikacije visokog nivoa pouzdanosti zamenjuje potpis stranke na podnesku, što će stvoriti preduslove da građani koriste usluge elektronskim putem u svim onim slučajevima gde je predviđeno da se podnesak stranke mora potpisati, kao i da organi vlasti priznaju ovakav način identifikacije ravnopravno sa identifikacijom putem potpisa u klasičnom poslovanju.

6. Kakve troškove će primena zakona stvoriti građanima i privredi (naročito malim i srednjim preduzećima)

Primena zakona neće stvoriti veće troškove građanima i privredi. Troškovi korišćenja usluga elektronske identifikacije i usluga od poverenja će omogućiti srazmero efikasnije i jeftinije obavljanje poslova, što neće dovesti do ukupnog povećanja troškova. Na primer, troškovi elektronske dostave će biti manji od troškova fizičke dostave koja se zamenjuje elektronskom.

Trenutni troškovi koje snose sertifikaciona tela za kvalifikovani elektronski potpis, odnosno izdavaoci vremenskog žiga, za upis u registre koje vode Ministarstvo, odnose se na uplatu republičke administrativne takse za upis, promenu podataka ili brisanje iz registra. Naime, za rešenje o upisu u Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih potpisa uplaćuju se sledeće takse:

1) rešenje po zahtevu za utvrđivanje ispunjenosti uslova za početak rada i obavljanje delatnosti sertifikacionih tela	440.200
2) rešenje po žalbi na rešenje o odbijanju zahteva za upis u Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji	2.200
3) rešenje o upisu promene podataka u Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji	2.200
4) rešenje o brisanju sertifikacionih tela iz Registra sertifikacionih tela za izdavanje kvalifikovanih elektronskih	2.200

sertifikata u Republici Srbiji	

Troškovi koje snose izdavaoci vremenskog žiga radi naplate republičke administrativne takse:

1) po zahtevu za upis u registar	1.470
2) po zahtevu za upis promena u registar	720
3) po zahtevu za brisanje iz registra	1.470
4) Za uverenje o podacima upisanim u registar, ako ovim zakonom nije drukčije propisano	720

Privredni subjekti koji su obavljali delatnosti iz ove oblasti na osnovu Zakona o elektronskom potpisu i Zakona o elektronskom dokumentu (sertifikaciona tela za izdavanje kvalifikovanog elektronskog potpisa, izdavaoci vremenskog žiga) neće imati značajnije troškove kako bi se usaglasili sa novim zakonom. Ovi privredni subjekti će biti dužni da Ministarstvu dostave izveštaj o oceni usaglašenosti, koje izrađuju tela za ocenjivanje usaglašenosti. Troškovi pribavljanja izveštaja se u ovom trenutku ne mogu proceniti, s obzirom da se ocena usaglašenosti od ovakvih tela do sada nije obavljala (procenu usaglašenosti je vršilo Ministarstvo), kao i da će se tek donošenjem zakona pojaviti potreba za njihovom akreditacijom, nakon čega će biti poznati i troškovi za izradu navedenih izveštaja. Pored toga, za rešenje koje se donosi u vezi sa upisom u Registar pružalaca kvalifikovanih usluga od poverenja, pružaoci kvalifikovanih usluga od poverenja moraće da uplate republičku administrativnu taksu (za upis u registar – 1.470 dinara, za upis promena u registar – 720 dinara, za brisanje iz registra – 1.470 dinara). Iste troškove će snositi i pružaoci usluga elektronske identifikacije, radi upisa u Registar pružalaca usluga elektronske identifikacije i šema elektronske identifikacije.

Zakonom je predviđeno da proveru ispunjenosti uslova za obavljanje kvalifikovanih usluga od poverenja vrše tela za ocenjivanje usaglašenosti, koja su, u skladu sa zakonom kojim se uređuje akreditacija, akreditovana za ocenjivanje usaglašenosti pružaoca kvalifikovanih usluga od poverenja i kvalifikovanih usluga od poverenja koje oni pružaju. Zakonom o akreditaciji („Službeni glasnik RS”, br. 73/10) predviđeno je da u Republici Srbiji poslove akreditacije vrši Akreditaciono telo Srbije. U skladu sa Zakonom o republičkim administrativnim taksama („Službeni glasnik RS”, br. 43/03, 51/03 - ispr., 61/05, 101/05 - dr. zakon, 5/09, 54/09, 50/11, 70/11 - usklađeni din. izn., 55/12 - usklađeni din. izn., 93/12, 47/13 - usklađeni din. izn., 65/13 - dr. zakon, 57/14 - usklađeni din. izn., 45/15 - usklađeni din. izn., 83/15, 112/15 i 50/16 - usklađeni din. izn.), za prijavu za akreditaciju plaća se naknada u iznosu od 1.190 dinara. Pored toga, Odlukom o visini troškova akreditacije („Službeni glasnik RS”, broj 43/13) predviđeni su sledeći troškovi akreditacije:

Troškovi	Dinara
1) troškovi obrade prijave za otpočinjanje prve akreditacije	48.000

2) troškovi obrade prijave za proširenje obima akreditacije	30.000
3) troškovi obrade prijave za ponovnu akreditaciju	36.000
4) troškovi preliminarne posete	36.000
5) troškovi ocenjivanja po dan/ocenjivaču	48.000
6) troškovi održavanja akreditacije (godišnja naknada):	
6.1 za laboratorije za ispitivanje, etaloniranje, medicinske laboratorije:	
- do 25 akreditovanih metoda	30.000
- od 26 do 100 akreditovanih metoda	60.000
- preko 100 akreditovanih metoda	120.000
6.2 za kontrolna tela:	
- do 10 oblasti kontrolisanja	60.000
- preko 10 oblasti kontrolisanja	90.000
6.3 za sertifikaciona tela za sertifikaciju proizvoda:	
- do 10 proizvoda/grupe proizvoda	60.000
- preko 10 proizvoda/grupe proizvoda	90.000
6.4 za sertifikaciju sistema menadžmenta:	
- do 10 oblasti industrijsko-ekonomskog sektora	60.000
- preko 10 oblasti industrijsko-ekonomskog sektora	90.000
6.5 za sertifikaciona tela za sertifikaciju osoba:	
- do 10 oblasti	60.000

Pored toga, zakonom je predviđeno da Ministarstvo imenuje tela za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata. Prema Zakonu o republičkim administrativnim taksama, za spise i radnje koji se vrše u skladu sa propisima kojima se uređuju tehnički zahtevi za proizvode i ocenjivanje usaglašenosti proizvoda sa propisanim zahtevima, plaćaju se administrativne takse (za zahtev za imenovanja tela za ocenjivanje usaglašenosti – 2.410 dinara, za prijavu za ovlašćivanje tela za ocenjivanje usaglašenosti – 2.410 dinara, za rešenje koje se donosi po zahtevu podnetom za imenovanje tela za ocenjivanje usaglašenosti – 11.550 dinara i za rešenje koje se donosi po prijavi podnetoj za ovlašćivanje tela za ocenjivanje usaglašenosti – 11.550 dinara). Proizvođači koji budu zahtevali sertifikaciju svojih proizvoda imaće troškove koje u ovom trenutku nije moguće proceniti, s obzirom da tela za ocenu usaglašenosti tek treba da započnu sa radom i da cene nisu formirane.

Ministarstvo trgovine, turizma i telekomunikacija, koje vode registre navedene u odgovoru na ovo pitanje, neće imati troškove za njihovo uspostavljanje.

U obrazloženju Predloga zakona, odeljku IV Finansijska sredstva, prikazani su troškovi za realizaciju zakona u naredne dve godine, koji će se finansirati iz budžeta Republike Srbije.

7. *Da li su pozitivne posledice donošenja zakona takve da opravdavaju troškove koje će on stvoriti*

Pozitivne posledice donošenja zakona su brojne i opravdavaju troškove koje će on stvoriti. Kao što je već navedeno, zakon će doprineti bržem i efikasnijem poslovanju i smanjenju troškova poslovanja privrednih subjekata, organa javne vlasti i građana, modernizaciji i efikasnijem radu organa javnih vlasti, lakši i sigurniji pristup uslugama organa javne vlasti i drugih subjekata koje se pružaju elektronskim putem, kao i pristupu većem broju tih usluga.

Troškovi koji nastaju donošenjem zakona su neophodni za jačanje uloge nadležnog organa u ovoj oblasti i primenu zakona u potpunom obimu, kako bi se poslovi tog organa obavljali na način koji će omogućiti adekvatnu primenu ovog zakona. U tom smislu, neophodno je povećanje kapaciteta inspekcije za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju, kao i uspostavljanja Centralnog sistema za razmenu poruka kvalifikovane elektronske dostave, kako bi se obezbedila nesmetana elektronska dostava u slučaju kada korisnici usluge koriste različite pružaoce usluga kvalifikovane elektronske dostave.

Zakonom se uvodi novo rešenje u vezi sa ocenjivanjem usaglašenosti uslova za pružanje kvalifikovanih usluga od poverenja, tako što se određuje da ovu ocenu vrši telo za ocenjivanje usaglašenosti. Ovo rešenje će dovesti do toga da ocenu usaglašenosti vrše tela koja ispunjavaju odgovarajuće standarde u ovoj oblasti, i da se ocena vrši od strane stručnih lica koja mogu da garantuju da pružalac kvalifikovanih usluga od poverenja ispunjava sve zahteve predviđene propisima. Takođe, zakon uvodi sertifikaciju sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata, koja je veoma značajna, s obzirom da ova sredstva moraju da ispune bezbednosne uslove kako ne bi došlo do njihove zloupotrebe. Shodno tome, tela za ocenjivanje usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata, koja ispunjavaju standarde u ovoj oblasti, garantovaće da navedena sredstva ispunjavaju uslove predviđene propisima, a javnim objavljivanjem registra sertifikovanih sredstava biće dostupne informacije o sredstvima koja ispunjavaju ove uslove.

8. *Da li se zakonom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija*

Očekuje se da će zakonska rešenja uticati na stvaranje novih privrednih subjekata na tržištu i tržišnu konkurenciju. Zakonom se uvode nove usluge u elektronskom poslovanju, što može dovesti do povećanog interesovanja privrednih subjekata za obavljanje ove delatnosti. Takođe, predmetni zakon stvara preduslove za povećanu upotrebu usluga elektronske identifikacije i kvalifikovanih usluga od poverenja, imajući u vidu pravno dejstvo koje im se priznaje. Usled toga, očekuje se da će postojati povećana potražnja za ovim uslugama od strane organa javne vlasti, građana i privrede, što može dovesti do stvaranja novih privrednih subjekata na tržištu i povećanje broja novih radnih mesta.

Pored toga, s obzirom da se zakonom predviđa da se ocenjivanje usaglašenosti za obavljanje kvalifikovanih usluga od poverenja, kao i ocenjivanje usaglašenosti kvalifikovanih sredstava za kreiranje elektronskog potpisa odnosno pečata vrši od strane tela za ocenjivanje usaglašenosti, očekuje se da će se uspostaviti i razviti tržište usluga na kojem će poslovati ovi privredni subjekti. S obzirom da je zakonska obaveza pružaoca usluga od poverenja da podnesu Ministarstvu izveštaj o oceni usaglašenosti kvalifikovanih usluga od poverenja koji izrađuje telo za ocenjivanje usaglašenosti, kao i da sredstva za kreiranje elektronskog potpisa odnosno pečata budu sertifikovana od strane tela za ocenjivanje usaglašenosti, izvesno je da će postojati potražnja za ovim uslugama, što će doprineti razvoju tržišta u ovoj oblasti.

9. Da li su sve zainteresovane strane imale priliku da se izjasne o zakonu

Na osnovu zaključka Odbora za privredu i finansije Vlade 05 Broj: 011-8026/2016-1 od 7. septembra 2016. godine, Ministarstvo trgovine, turizma i telekomunikacija sprovelo je javnu raspravu o tekstu Nacrta zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju u periodu od 7. septembra 2016. godine do 30. septembra 2016. godine. Tekst Nacrta zakona sa obrazloženjem objavljen je na sajtu Ministarstva www.mtt.gov.rs i Portalu eUprava www.euprava.gov.rs. Sva zainteresovana lica mogla su da preuzmu tekst Nacrta zakona i da svoje komentare dostave Ministarstvu poštom i elektronskim putem. Okrugli sto o Nacrtu zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju održan je u utorak, 13. septembra 2016. godine, u prostorijama Privredne komore Srbije, Resavska 15, Beograd. Skup je bio veoma posećen, i na njemu su, pored članova radne grupe koja je izradila Nacrt zakona, prisustvovali predstavnici državnih organa, privrede, nevladinih organizacija, akademske zajednice, eminentni stručnjaci u ovoj oblasti i druga zainteresovana lica. Oni su mogli da iznesu svoje komentare na tekst Nacrt zakona, kao i da dobiju detaljnije informacije i obrazloženja u vezi sa predloženim zakonskim normama.

Tokom javne rasprave upućeni su sledeći komentari i sugestije:

- Republički geodetski zavod i NALED su predložili da se dopune odredbe o overi digitalizovanog dokumenta, tako što će se predvideti slučaj kada se dokumenti izdati od strane jednog organa preuzimaju od strane drugog. Ova sugestija je prihvaćena i uneta u tekst zakona;
- Dragan Spasić, veštak informacionih tehnologija i predstavnik sertifikacionog tela „Pošta Srbije" izneo je mišljenje da matični broj sertifikacionog tela ne treba da bude obavezan element kvalifikovanog elektronskog sertifikata, što je i predviđeno Nacrtom zakona. Naime, u odredbi koja propisuje sadržaj kvalifikovanog elektronskog sertifikata, predviđeno je da se JMBG nalazi u sertifikatu ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG. To znači da je JMBG sastavni deo sertifikata samo ukoliko je korisnik to tražio. Takođe, izrazio je mišljenje da elektronski potpis „u klaudu", koji se pruža putem usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, nije dovoljno bezbedan. Povodom toga, ukazujemo da je zakonom predviđeno da pružaoci usluga kvalifikovanih usluga od poverenja, uključujući i pružaoce ove usluge, moraju da ispune bezbednosne uslove za njihovo vršenje;

- Učesnici su smatrali da je potrebno preispitati odredbu po kojoj državni organ može postati pružalac usluga od poverenja na osnovu uredbe Vlade Republike Srbije ukoliko ispunjava sve uslove za pružanje usluga predviđenih zakonom, s obzirom da bi za državne organe trebao da važi jednak režim kao i za ostale subjekte. Povodom toga, ističemo da je u članu 37. Nacrta zakona propisano da državni organ može postati pružalac usluga od poverenja ukoliko ispunjava sve uslove za pružanje usluga predviđene zakonom, iz čega proizlazi da državni organi moraju da pružaju usluge od poverenja pod jednakim uslovima kao i subjekti koji nisu državni organi. Ukazujemo da je zakonsko rešenje iste prirode već predviđeno članom 21. Zakona o elektronskom potpisu („Službeni glasnik RS”, broj 135/04), kojim je propisano da izdavanje kvalifikovanih elektronskih sertifikata može obavljati i organ državne uprave, u skladu sa posebnim propisima. Na osnovu ovog člana, doneta je Uredba o određivanju Ministarstva unutrašnjih poslova za izdavanje kvalifikovanih elektronskih sertifikata („Službeni glasnik RS”, broj 111/09) i Uredba o određivanju Ministarstva odbrane za izdavanje kvalifikovanih elektronskih sertifikata („Službeni glasnik RS”, broj 77/14);
- Više učesnika je iznelo stav da je potrebno zakonom, a ne podzakonskim aktom, bliže urediti uslove koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti. Povodom toga, mišljenja smo da je celishodnije ovu materiju regulisati podzakonskim aktom, s obzirom da se u većem delu u podzakonskim aktima predviđa bliže uređenje tehničkih uslova za vršenje ovih usluga, u skladu sa EU standardima, koji se, usled brzog tehnološkog napretka, često menjaju;
- Istaknuto je da bi sve usluge od poverenja trebale da budu definisane tako da dozvoljavaju konstantna tehnička poboljšanja, kao i da budu dostupne kako za hardverska, tako i softverska rešenja, nezavisno od operativne platforme.
- Predloženo je da se skrati rok za donošenje podzakonskih akata, koji iznosi 12 meseci, što nije prihvaćeno, s obzirom da zakon predviđa donošenje velikog broja podzakonskih akata i da je 12 meseci objektivan rok za njihovo donošenje;
- Predstavnici NALED-a predložili su da se zakonom uvede još jedna usluga od poverenja – usluga kvalifikovane digitalizacije dokumenta, koja nije prepoznata u evropskoj regulativi, i usled toga zakon nije regulisao ovo pitanje;
- Arhiv Srbije je predložio da se u zakonu preformuliše definicija pojma „arhivske građe”, što je prihvaćeno i definisano na predloženi način;
- JP „Elektromreža Srbije” predložilo je da se prilagodi definicija „organa javne vlasti” na koje se ovaj zakon odnosi, imajući u vidu prirodu poslova koji će ovi organi vršiti elektronskim putem, i predložena izmena je usvojena.

10. Koje će se mere tokom primene zakona preduzeti da bi se ostvarilo ono što se donošenjem zakona namerava

Kako bi se ostvarilo ono što se donošenjem zakona namerava, planirano je da se u Ministarstvu trgovine, turizma i telekomunikacija uspostavi Centralni sistem za razmenu poruka kvalifikovane elektronske dostave i poveća kapacitet inspekcije za elektronsku identifikaciju i usluge od poverenja. Usled toga, kako bi se navedeni poslovi mogli izvršavati u skladu sa zakonom, potrebno je da se zaposle tri državna službenika na radnom mestu inspektora za inspekcijski nadzor 2017. godini usled čega bi ukupni godišnji rashodi za zaposlene iznosili 2.225.000,00 dinara u 2017. godini i 3.338.000,00 u 2018. godini, a

godišnji rashodi za uspostavljanje Centralnog sistema za razmenu poruka kvalifikovane elektronske dostave 10.000.000,00 dinara u 2017. godini i 2.000.000 dinara u 2018. godini za održavanje Centralnog sistema.

Zakonom se ne uspostavljaju nove institucije, niti se ukidaju postojeće. Takođe, nije potrebno menjati organizacionu strukturu postojećih organa i organizacija.

Zakon predviđa odredbe o nadležnosti Ministarstva u pogledu saradnje sa telima Evropske unije i nadležnim institucijama država članica Evropske unije. Naime, prema Uredbi EU, države članice EU dužne su da prijavljuju Evropskoj komisiji svoje šeme elektronske identifikacije, radi upisa u registar, na osnovu koga će se omogućiti da se šeme elektronske identifikacije priznaju u zemlji u kojoj nisu izdate. Po stupanju u EU, Republika Srbija će prijavljivati šeme elektronske identifikacije registrovane u našoj zemlji, i to elektronskim putem, prema formatima, standardima i obrascima koje je propisala EU. Takođe, navedena uredba predviđa i razmenu podatka o bezbednosnim incidentima koje ugrožavaju korisnike u dve ili više država članica EU. U tim slučajevima, Ministarstvo će elektronskim putem biti dužno da obavesti nadležna tela o ovim incidentima.

Kao što je gore već navedeno, u skladu sa ovim zakonom biće uvedeni novi registri:

1) Registar pružalaca usluga elektronske identifikacije i šema elektronske identifikacije;

2) Registar pružalaca kvalifikovanih usluga od poverenja:

3) Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata.

Vođenje ovih registara finansiraće se u okviru finansijskih sredstava namenjenih za redovno poslovanje Ministarstva.

Registri koji se vode na osnovu Zakona o elektronskom potpisu (Evidencija sertifikacionih tela, Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji) i na osnovu Zakona o elektronskom dokumentu (Registar izdavalaca vremenskog žiga) prestaju da postoje.

Nakon usvajanja ovog zakona, nadležno ministarstvo planira upoznavanje javnosti sa zakonom, kako u okviru svojih redovnih informativnih kampanja, tako i putem namenskih okruglih stolova i drugih vidova informisanja kojima će se građanima Republike Srbije pružiti neophodne informacije o rešenjima koja predviđa zakon.

Radi izvršavanja ovog zakona, planirano je donošenje sledećih podzakonskih akata:

Član Nacrta zakona	**Naziv podzakonskog akta**
Član 18.	Uredba o uslovima za šeme elektronske identifikacije prema nivou pouzdanosti;

Član 19.	Pravilnik o Registru pružalaca usluga elektronske identifikacije i šema elektronske identifikacije;
Član 31.	Uredba o uslovima za pružanje kvalifikovanih usluga od poverenja
Član 34.	Pravilnik o utvrđivanju liste standarda koje mora da ispuni telo za ocenjivanje usaglašenosti, sadržini izveštaja o ocenjivanju usaglašenosti i postupku provere ispunjenosti uslova i ocenjivanja usaglašenosti kvalifikovanih usluga od poverenja
Član 35.	Pravilnik o sadržaju i načinu vođenja Registra kvalifikovanih usluga od poverenja
Član 38.	Pravilnik o tehničkim uslovima za formu i način objavljivanja Javne liste kvalifikovanih usluga od poverenja
Član 39.	Pravilnik o izgledu, sastavu, veličini i dizajnu Znaka pouzdanosti za kvalifikovane usluge od poverenja
Član 43.	Pravilnik o bližem uslovima za kvalifikovane elektronske sertifikate i usluge
Član 46.	Pravilnik o bližim uslovima za sredstva za kreiranje kvalifikovanog elektronskog potpisa i pečata i uslovima za telo za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa i pečata
Član 47.	Pravilnik o sadržaju i načinu vođenja Registra kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata
Član 48.	Pravilnik o bližim uslovima za postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata
Član 49.	Pravilnik o bližim uslovima za pružanje usluge kvalifikovane validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata
Član 52.	Pravilnik o bližim uslovima za kvalifikovane elektronske vremenske žigove
Čl. 54. i 55.	Pravilnik o bližim uslovima za usluge kvalifikovane preporučene elektronske dostave i sadržaju potvrde o prijemu elektronske poruke od strane pružaoca usluga i potvrdu dostave elektronske poruke
Član 61.	Uredba o bližim uslovima za pouzdanu pripremu dokumenata za elektronsko čuvanje
Član 62.	Pravilnik o bližim uslovima za postupke i tehnološka rešenja za pouzdano elektronsko čuvanje dokumenata
Član 62.	Pravilnik o bližim uređenju uslova, zadataka, poslova, standarda i procesa digitalizacije kulturnog nasleđa i savremenog stvaralaštva.

Prema članu 71. Predloga zakona, podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona.

1. Naziv propisa Evropske unije : 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 Uredba Evropskog parlamenta i Evropskog saveta broj 910/2014 od 23. jula 2014. godine o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu, koja zamenjuje Direktivu 1999/93/EC	2. „CELEX" oznaka EU propisa 32014R0910
3. Organ državne uprave, odnosno drugi ovlašćeni predlagač propisa: Vlada	4. Datum izrade tabele:
Obrađivač - Ministarstvo trgovine, turizma i telekomunikacija	31.10.2016. godine
5. Naziv (nacrta, predloga) propisa čije odredbe su predmet analize usklađenosti sa propisom Evropske unije: Predlog zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju Draft Law on Electronic Document, Electronic Identification and trust services in electronic business	6. Brojčane oznake (šifre) planiranih propisa iz baze NPAA: 2016-481
7. Usklađenost odredbi propisa sa odredbama propisa EU:	

a)	a1)	b)	b1)	v)	g)	d)
Odredba propisa EU	Sadržina odredbe	Odredbe propisa R. Srbije	Sadržina odredbe	Usklađenost[1]	Razlozi za delimičnu usklađenost, neusklađenost ili neprenosivost	Napomena o usklađenosti
1.1.1.a	With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation: (a) lays down the conditions under which Member States recognise electronic identification			NP	Odredbom je utvrđeno da ova uredba reguliše uslove na osnovu kojih države članice priznaju sredstva elektronske identifikacije fizičkih i pravnih lica koja se koriste u okviru šeme	

[1] Potpuno usklađeno - PU, delimično usklađeno - DU, neusklađeno - NU, neprenosivo – NP

a)	a1)	b)	b1)	v)	g)	d)
	means of natural and legal persons falling under a notified electronic identification scheme of another Member State;				elektronske identifikacije druge države članice. Imajući u vidu da Republika Srbija nije članica EU, ovakva odredba nije prenosiva.	
1.1.1.b	(b) lays down rules for trust services, in particular for electronic transactions; and	1.	Ovim zakonom uređuje se elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju.	PU		
1.1.1.c	(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.	1.	Ovim zakonom uređuje se elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju.	PU		
2.1.	This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.			NP	Odredba je neprenosiva u propis Republike Srbije, jer se njom određuje primena uredbe u državama članicama Evropske unije.	
2.2.	This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.	3.2.	Odredbe ovog zakona se ne primenjuju na usluge od poverenja koje se pružaju u okviru ograničenog kruga učesnika i nemaju uticaj na treće strane.	PU		
2.3.	This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.			NP	Odredba je neprenosiva, jer se odnosi na domašaj primene ove uredbe kada je pravom EU ili nacionalnim pravom predviđena posebna forma za ugovore i druge akte.	
3.1.1.	For the purposes of this Regulation, the following definitions apply: 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person	2.1.12.	**elektronska identifikacija** je postupak korišćenja ličnih identifikacionih podataka u elektronskom obliku koji jednoznačno određuju pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta	PU		
3.1.2.	'electronic identification means' means a material and/or immaterial unit containing person	2.1.13.	**sredstvo elektronske identifikacije** je materijalno odnosno nematerijalno sredstvo koje sadrži	PU		

a)	a1)	b)	b1)	v)	g)	d)
	identification data and which is used for authentication for an online service		identifikacione podatke i kojim se dokazuje identitet prilikom autentikacije			
3.1.3.	'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;	2.1.11.	**identifikacioni podaci** predstavljaju skup podataka na osnovu kojih je moguće jednoznačno utvrditi identitet pravnog lica, fizičkog lica ili fizičkog lica u svojstvu registrovanog subjekta	PU		
3.1.4.	'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;	2.1.14.	**šema elektronske identifikacije** je sistem izdavanja sredstva elektronske identifikacije pravnom licu, fizičkom licu ili fizičkom licu u svojstvu registrovanog subjekta	PU		
3.1.5.	'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;	2.1.10.	**autentikacija** je proces provere identiteta pravnog lica, fizičkog lica ili fizičkog lica u svojstvu registrovanog subjekta uključujući proveru integriteta i porekla podataka za koje se pretpostavlja da ih je to lice stvorilo, odnosno poslalo	PU		
3.1.6.	'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;	2.1.18.	**pouzdajuća strana** je pravno ili fizičko lice koje se pouzdaje u uslugu elektronske identifikacije odnosno uslugu od poverenja	PU		
3.1.7.	'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;	2.1.8.	**organ javne vlasti** je državni organ, organ teritorijalne autonomije, organ jedinice lokalne samouprave, kao i pravno ili fizičko lice kojem su poverena javna ovlašćenja	PU		
3.1.8.	'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council;	2.1.8.	**organ javne vlasti** je državni organ, organ teritorijalne autonomije, organ jedinice lokalne samouprave, kao i pravno ili fizičko lice kojem su poverena javna ovlašćenja	PU		
3.1.9.	'signatory' means a natural person who creates an electronic signature;	2.1.26.	**potpisnik** je fizičko lice koje je kreiralo elektronski potpis i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski potpis, to jest sertifikatu kojim se potvrđuje veza između identiteta tog potpisnika i podataka za validaciju elektronskog potpisa koji odgovaraju podacima za kreiranje elektronskog potpisa koje je potpisnik koristio pri kreiranju tog elektronskog potpisa	PU		

a)	a1)	b)	b1)	v)	g)	d)
3.1.10.	'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;	2.1.21.	**elektronski potpis** je skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (potpisanim) podacima u elektronskim obliku tako da se elektronskim potpisom potvrđuje integritet tih podataka i identitet potpisnika.	PU		
3.1.11.	'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26	2.1.30.	**napredni elektronski potpis** je elektronski potpis koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta potpisnika u skladu sa ovim zakonom	PU		
3.1.12.	'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;	2.1.31.	**kvalifikovani elektronski potpis** je napredni elektronski potpis koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog potpisa i koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis	PU		
3.1.13.	'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature	2.1.23.	**podaci za kreiranje elektronskog potpisa odnosno pečata** su jedinstveni podaci koje koristi potpisnik odnosno pečatilac za kreiranje elektronskog potpisa odnosno pečata i koji su logički povezani sa odgovarajućim podacima za validaciju elektronskog potpisa odnosno pečata	PU		
3.1.14.	'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person	2.1.25.	**sertifikat za elektronski potpis odnosno pečat** je elektronska potvrda kojim se potvrđuje veza između podataka za validaciju elektronskog potpisa odnosno pečata i identiteta potpisnika odnosno pečatioca	PU		
3.1.15.	'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;	2.1.33.	**kvalifikovani sertifikat za elektronski potpis** je sertifikat za elektronski potpis koji izdaje kvalifikovani pružalac usluga od poverenja i koji ispunjava uslove predviđene ovim zakonom	PU		
3.1.16.a 3.1.16.b. 3.1.16.c.	'trust service' means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services	2.1.16. 41.1.	**usluga od poverenja** je elektronska usluga koja olakšava poslovnu aktivnost između dve ili više strana pri čemu se zasniva na tome da pružalac usluge stranama garantuje verodostojnost pojedinih podataka, a koja je kao takva određena ovim zakonom; Usluge od poverenja se pružaju u oblastima: 1) elektronskog potpisa i elektronskog pečata 2) elektronskog vremenskog žiga 3) elektronske dostave 4) autentikacije veb sajtova 5) elektronskog čuvanja dokumenata	PU		

a)	a1)	b)	b1)	v)	g)	d)
3.1.17.	'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation	2.1.19.	**kvalifikovana usluga od poverenja** je usluga od poverenja koja ispunjava uslove utvrđene ovim zakonom za kvalifikovanu uslugu od poverenja	PU		
3.1.18.	'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;	2.1.46.	**telo za ocenjivanje usaglašenosti** je telo ovlašćeno za sprovođenje ocenjivanja usaglašenosti kvalifikovanog pružaoca usluga od poverenja i kvalifikovane usluge od poverenja koju on pruža sa uslovima za pružanje kvalifikovanih usluga od poverenja	PU		
3.1.19.	'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider	2.1.17.	**pružalac usluga od poverenja** je pravno ili fizičko lice koje pruža jednu ili više usluga od poverenja	PU		
3.1.20.	'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;	2.1.20.	**pružalac kvalifikovane usluge od poverenja** je pravno ili fizičko lice koje pruža jednu ili više kvalifikovanih usluga od poverenja	PU		
3.1.21.	'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services	2.1.6.	**proizvod je** hardver, softver odnosno hardver sa pripadajućim softverom, ili njihove odgovarajuće komponente, namenjen elektronskoj obradi, elektronskom prenosu odnosno čuvanju podataka	PU		
3.1.22.	'electronic signature creation device' means configured software or hardware used to create an electronic signature;	2.1.28.	**sredstvo za kreiranje elektronskog potpisa odnosno pečata** je tehničko sredstvo (softver odnosno hardver) koje se koristi za kreiranje elektronskog potpisa odnosno pečata uz korišćenje podataka za kreiranje elektronskog potpisa odnosno pečata	PU		
3.1.23.	qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;	2.1.32.	**kvalifikovano sredstvo za kreiranje elektronskog potpisa** je sredstvo koji ispunjava uslove propisane ovim zakonom	PU		
3.1.24.	'creator of a seal' means a legal person who creates an electronic seal	2.1.27.	**pečatilac** je pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta u čije ime se kreira elektronski pečat i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski pečat, to jest sertifikatu kojim se potvrđuje	PU		

a)	a1)	b)	b1)	v)	g)	d)
			veza između identiteta tog pečatioca i podataka za validaciju elektronskog pečata koji odgovaraju podacima za kreiranje elektronskog pečata koji su po ovlašćenju pečatioca korišćeni pri kreiranju tog elektronskog pečata			
3.1.25.	'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity	2.1.22.	**elektronski pečat** je skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (pečatiranim) podacima u elektronskim obliku tako da se elektronskim pečatom potvrđuje integritet tih podataka i identitet pečatioca	PU		
3.1.26.	'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;	2.1.34.	**napredni elektronski pečat** je elektronski pečat koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta pečatioca u skladu sa ovim zakonom	PU		
3.1.27.	'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;	2.1.34.	**kvalifikovani elektronski pečat** je napredni elektronski pečat koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog pečata i koji je zasnovan na kvalifikovanom sertifikatu za elektronski pečat	PU		
3.1.28.	'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;	2.1.23.	**podaci za kreiranje elektronskog potpisa odnosno pečata** su jedinstveni podaci koje koristi potpisnik odnosno pečatilac za kreiranje elektronskog potpisa odnosno pečata i koji su logički povezani sa odgovarajućim podacima za validaciju elektronskog potpisa odnosno pečata	PU		
3.1.29.	'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;	2.1.25.	**sertifikat za elektronski potpis odnosno pečat** je elektronska potvrda kojim se potvrđuje veza između podataka za validaciju elektronskog potpisa odnosno pečata i identiteta potpisnika odnosno pečatioca	PU		
3.1.30.	'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;	2.1.37.	**kvalifikovani sertifikat za elektronski pečat** je sertifikat za elektronski pečat koji izdaje kvalifikovani pružalac usluga od poverenja i ispunjava uslove predviđene ovim zakonom	PU		
3.1.31.	'electronic seal creation device' means configured software or hardware used to create an electronic seal;	2.1.28.	**sredstvo za kreiranje elektronskog potpisa odnosno pečata** je tehničko sredstvo (softver odnosno hardver) koje se koristi za kreiranje elektronskog potpisa odnosno pečate uz korišćenje podataka za kreiranje elektronskog potpisa odnosno pečata	PU		

a)	a1)	b)	b1)	v)	g)	d)
3.1.32.	'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II	2.1.36.	**kvalifikovano sredstvo** za kreiranje elektronskog pečata je sredstvo koji ispunjava uslove propisane ovim zakonom	PU		
3.1.33.	'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time	2.1.40.	**elektronski vremenski žig** je zvanično vreme pridruženo podacima u elektronskom obliku kojim se potvrđuje da su ti podaci postojali u tom vremenskom trenutku	PU		
3.1.34.	'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42	2.1.41.	**kvalifikovani elektronski vremenski žig je** elektronski vremenski žig koji ispunjava uslove utvrđene ovim zakonom za kvalifikovani elektronski vremenski žig	PU		
3.1.35.	'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording	2.1.4.	**elektronski dokument** je skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video materijala, u elektronskom obliku	PU		
3.1.36.	'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;	2.1.42.	**usluga elektronske dostave** je usluga prenosa podataka elektronskim putem u okviru koje pružalac usluge obezbeđuje dokaze o postupanju sa prenesenim podacima, uključujući dokaz slanja i prijema podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja odnosno bilo kojih neovlašćenih promena	PU		
3.1.37.	'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44	41.1.8. 54.	Kvalifikovane usluge od poverenja su: 8) usluga kvalifikovane elektronske dostave. Usluga kvalifikovane elektronske dostave mora da ispuni sledeće uslove: 1) da je pružana od strane jednog ili više pružaoca kvalifikovanih usluga od poverenja; 2) da uz visok nivo pouzdanosti obezbeđuje identifikaciju pošiljaoca; 3) da obezbeđuje identifikaciju primaoca prilikom dostave podataka; 4) da se u procesu slanja i prijema elektronske poruke koristi napredni elektronski potpis ili napredni elektronski pečat pružaoca usluge kvalifikovane elektronske dostave u svrhu sprečavanja neprimećene promene podataka; 5) da izmena podataka izvršena u svrhu slanja ili prijema podataka mora biti jasno naznačena	PU	Pojam ove kvalifikovane usluge se ne nalazi u članu u kome su definisani pojmovi iz zakona, ali je članom 41. ovog zakona utvrđeno da je usluga kvalifikovane elektronske dostave jedna od kvalifikovanih usluga od poverenja, a uslovi za njeno vršenje utvrđeni su u članu 54. ovog zakona, te smatramo da ovde postoji potpuna usklađenost.	

a)	a1)	b)	b1)	v)	g)	d)
			pošiljaocu i primaocu; 6) da vreme i datum slanja, prijema i eventualne izmene podataka moraju biti naznačeni kvalifikovanim elektronskim vremenskim žigom. 7) u slučaju da se podaci prenose između dva ili više pružalaca usluge kvalifikovane elektronske dostave uslovi iz ovog stava se primenjuju na svakog od njih.			
3.1.38.	'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;	2.1.38.	**sertifikat za autentikaciju veb sajta** je potvrda pomoću koje je moguće izvršiti autentikaciju veb sajta i kojom se veb sajt povezuje sa identitetom fizičkog ili pravnog lica kome je sertifikat izdat	PU		
3.1.39.	'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;	2.1.39.	**kvalifikovani sertifikat za autentikaciju veb sajta** je sertifikat za autentikaciju veb sajta koju izdaje kvalifikovani pružalac usluga od poverenja i ispunjava uslove predviđene ovim zakonom	PU		
3.1.40.	'validation data' means data that is used to validate an electronic signature or an electronic seal	2.1.24.	**podaci za validaciju elektronskog potpisa odnosno pečata** su podaci na osnovu kojih se proverava da li elektronski potpis odnosno pečat odgovara podacima koji su potpisani odnosno pečatirani	PU		
3.1.41.	'validation' means the process of verifying and confirming that an electronic signature or a seal is valid	2.1.29.	**validacija** je postupak provere i potvrđivanja ispravnosti elektronskog potpisa odnosno elektronskog pečata	PU		
4.1.	There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.			NP	Odredba je neprenosiva, jer uređuje pitanje pružanja usluga od poverenja na teritoriji države članice EU u slučaju kada pružalac nije osnovan u toj državi članici.	
4.2.	Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.			NP	Odredba je neprenosiva, jer uređuje promet usluga od poverenja na unutrašnjem tržištu Evropske unije.	
5.1.	Processing of personal data shall be carried out in accordance with Directive 95/46/EC.	4.1.	Pružalac usluga od poverenja odnosno usluge elektronske identifikacije prilikom obrade podataka o ličnosti postupa u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.	PU		

a)	a1)	b)	b1)	v)	g)	d)
5.2.	Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.	4.2.	U okviru elektronske transakcije strane se mogu predstavljati pseudonimom ukoliko propisom, ugovorom ili na drugi obavezujući način nije drugačije određeno.	PU		
6.	1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met: (a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9; (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high; (c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online. Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph. 2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.			NP	Odredba je neprenosiva, jer se odnosi na priznavanje šema elektronske identifikacije između država članica EU, i to šema koje su prijavljene Evropskoj komisiji. Napominjemo da je članom 24. ovog zakona predviđeno da Ministarstvo Evropskoj komisiji prijavljuje registrovane šeme elektronskog identiteta koje ispunjavaju uslove iz Uredbe EU br. 910/2014 Evropskog parlamenta i Saveta, a ta odredba stupa na snagu od dana pristupanja Republike Srbije Evropskoj uniji.	
7.	An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that			NP	Odredba je neprenosiva, jer se	

a)	a1)	b)	b1)	v)	g)	d)
	all of the following conditions are met: (a) the electronic identification means under the electronic identification scheme are issued: (i) by the notifying Member State; (ii) under a mandate from the notifying Member State; or (iii) independently of the notifying Member State and are recognised by that Member State; (b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State; (c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3); (d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued; (e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3); (f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form. For relying parties other than public sector bodies the notifying Member State may define terms of access to				odnosi na uslove za prijavljivanje šema elektronske identifikacije, koje države članice EU prijavljuju Evropskoj komisiji.	

a)	a1)	b)	b1)	v)	g)	d)
	that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body. Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes; (g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7); (h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).					
8.1.	An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.	18.1.	Šeme elektronske identifikacije se razvrstavaju prema nivou pouzdanosti na: 1) šeme niskog nivoa pouzdanosti, koje obezbeđuju ograničeno poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija je svrha da smanje rizik zloupotrebe odnosno neistinitog predstavljanja; 2) šeme srednjeg nivoa pouzdanosti, koje obezbeđuju značajno poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija je svrha da značajno smanje rizik zloupotrebe odnosno neistinitog predstavljanja; 3) šeme visokog nivoa pouzdanosti, koje obezbeđuju visoko poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija je svrha da onemoguće zloupotrebu odnosno neistinito predstavljanje.	PU		
8.2.a.	The assurance levels low, substantial and high shall meet respectively the following criteria: (a) assurance level low shall refer to an electronic identification means in the context of an electronic	18.1.1.	Šeme elektronske identifikacije se razvrstavaju prema nivou pouzdanosti na: 1) šeme niskog nivoa pouzdanosti, koje obezbeđuju ograničeno poverenje u identitet kojim se lice	PU		

a)	a1)	b)	b1)	v)	g)	d)
	identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity		predstavlja i koriste sredstva i procedure čija je svrha da smanje rizik zloupotrebe odnosno neistinitog predstavljanja			
8.2.b.	(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity	18.1.2.	2) šeme srednjeg nivoa pouzdanosti, koje obezbeđuju značajno poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija je svrha da značajno smanje rizik zloupotrebe odnosno neistinitog predstavljanja	PU		
8.2.c.	(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity	18.1.3.	3) šeme visokog nivoa pouzdanosti, koje obezbeđuju visoko poverenje u identitet kojim se lice predstavlja i koriste sredstva i procedure čija je svrha da onemoguće zloupotrebu odnosno neistinito predstavljanje	PU		
8.3.	By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.			NP	Odredba je neprenosiva, jer se njom daje ovlašćenje Evropskoj komsiji da donese akte za implementaciju odredaba o šemama elektronske identifikacije. Napominjemo da je članom 18. stav 2. Zakona predviđeno da Vlada, na predlog ministarstva nadležnog za poslove informacionog društva, bliže uređuje uslove koje moraju da	

a)	a1)	b)	b1)	v)	g)	d)
					ispune šeme elektronske identifikacije za određene nivoe pouzdanosti. Taj akt će urediti materiju koja odgovara aktima za implementaciju koje će doneti Evropska komisija.	
8.4.a	Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements: (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;	18.2.1.	Vlada, na predlog ministarstva nadležnog za poslove informacionog društva (u daljem tekstu: Ministarstvo) bliže uređuje uslove koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti, a posebno: 1) način dokazivanja i provere identiteta fizičkog odnosno pravnog lica koje zahteva izdavanje sredstava elektronske identifikacije;	PU		
8.4.b	(b) the procedure for the issuance of the requested electronic identification means;	18.2.2.	2) način izdavanja sredstava elektronske identifikacije;	PU		
8.4.c	(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;	18.2.3.	3) mehanizam autentikacije, putem koga fizičko odnosno pravno lice korišćenjem sredstava identifikacije potvrđuje svoj identitet drugoj strani u elektronskoj transakciji;	PU		
8.4.d	(d) the entity issuing the electronic identification means;	18.2.4.	4) uslove koje treba da ispuni izdavalac sredstava elektronske identifikacije	PU		
8.4.e	(e) any other body involved in the application for the issuance of the electronic identification means;	18.2.5.	5) uslove koje treba da ispune drugi učesnici koji su uključeni u postupak izdavanja sredstava elektronske identifikacije;	PU		
8.4.f	(f) the technical and security specifications of the issued electronic identification means.	18.2.6.	6) tehničke i bezbednosne karakteristike sredstava elektronske identifikacije koja se izdaju;	PU		
8.5.	Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredbom se upućuje na proceduru koja sprovodi Evropska komisija u postupku usvajanja akata za implementaciju.	

a)	a1)	b)	b1)	v)	g)	d)
9.	1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto: (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme; (b) the applicable supervisory regime and information on the liability regime with respect to the following: (i) the party issuing the electronic identification means; and (ii) the party operating the authentication procedure; (c) the authority or authorities responsible for the electronic identification scheme; (d) information on the entity or entities which manage the registration of the unique person identification data; (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met; (f) a description of the authentication referred to in point (f) of Article 7; (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned. 2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon. 3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification. 4. A Member State may submit to the Commission a			NP	Odredbe su neprenosive, s obzirom da regulišu obavezu država članica EU da prijave šeme elektronske identifikacije Evropskoj komisiji. Napominjemo da je članom 24. ovog zakona predviđeno da Ministarstvo Evropskoj komisiji prijavljuje registrovane šeme elektronskog identiteta koje ispunjavaju uslove iz Uredbe EU br. 910/2014 Evropskog parlamenta i Saveta, a ta odredba stupa na snagu od dana pristupanja Republike Srbije Evropskoj uniji.	

a)	a1)	b)	b1)	v)	g)	d)
	request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request. 5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
10.	1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission. 2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay. 3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.			NP	Odredba je neprenosiva, jer reguliše obaveze država članica EU kada se desi narušavanje bezbednosti šema elektronske identifikacije, u kom slučaju to prijavljuju drugim državama članicama i Evropskoj komisiji.	
11.1.	The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with			NP	Odredba određuje odgovornost države članice koja ne ispuni	

a)	a1)	b)	b1)	v)	g)	d)
	its obligations under points (d) and (f) of Article 7 in a cross-border transaction.				obaveze koje se odnose na prekogranične transakcije u okviru šema elektronske identifikacije.	
11.2.	The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.	21.1.	Izdavalac sredstava elektronske identifikacije je odgovoran za štetu koja je nastala zbog toga što sredstvo za identifikaciju nije izdato u skladu sa šemom elektronske identifikacije koja ispunjava uslove iz člana 17. ovog zakona.	PU		
11.3.	The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.	21.2.	Za štetu nastalu usled neispravno sprovedenog postupka autentikacije odgovorna je strana koja sprovodi taj postupak, ukoliko je štetu prouzrokovala namerno ili nepažnjom.	PU		
11.4.	Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.			NP	Odredba je neprenosiva, jer upućuje da se odredbe čl.11. st. 1-3. uredbe vrše u skladu sa nacionalnim propisima o odgovornosti za štetu.	
11.5.	Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.			NP	Odredba je neprenosiva, jer upućuje da se odredbe čl.11. st. 1-3. uredbe vrše u skladu sa nacionalnim propisima o odgovornosti za štetu.	
12.	1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable. 2. For the purposes of paragraph 1, an interoperability framework shall be established. 3. The interoperability framework shall meet the following criteria: (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within			NP	Odredba reguliše interoperabilnost šema elektronske identifikacije koje države članice EU prijavljuju Evropskoj komisiji. Ukazujemo da je članom 23. ovog zakona predviđeno da Ministarstvo sarađuje sa	

a)	a1)	b)	b1)	v)	g)	d)
	a Member State; (b) it follows European and international standards, where possible; (c) it facilitates the implementation of the principle of privacy by design; and (d) it ensures that personal data is processed in accordance with Directive 95/46/EC. 4. The interoperability framework shall consist of: (a) a reference to minimum technical requirements related to the assurance levels under Article 8; (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8; (c) a reference to minimum technical requirements for interoperability; (d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes; (e) rules of procedure; (f) arrangements for dispute resolution; and (g) common operational security standards. 5. Member States shall cooperate with regard to the following: (a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and (b) the security of the electronic identification schemes. 6. The cooperation between Member States shall consist of: (a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels; (b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8; (c) peer review of electronic identification				nadležnim telima Evropske unije po pitanjima prekogranične interoperabilnosti šema elektronske identifikacije i preduzima mere iz svoje nadležnosti kako bi se uspostavio što viši nivo interoperabilnosti šema elektronske identifikacije na nacionalnom nivou. Međutim, imajući u vidu da su članom 12. predmetne uredbe predviđene obaveze koje isključivo preduzimaju države članice EU, odnosno Evropska komisija, te odredbe nisu mogle da se prenesu u domaći propis.	

a)	a1)	b)	b1)	v)	g)	d)
	schemes falling under this Regulation; and (d) examination of relevant developments in the electronic identification sector. 7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk. 8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4. 9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
13.1.	Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph. The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.	25.1. 25.2. 25.3.	Pružalac usluge od poverenja odgovoran je za štetu nastalu usled toga što nije postupio u skladu sa ovim zakonom ukoliko je štetu prouzrokovao namerno ili nepažnjom. Teret dokazivanja namere ili nepažnje pružaoca usluga od poverenja ja na fizičkom ili pravnom licu koje zahteva naknadu štete iz stava 1. ovog člana. Teret dokazivanja da šteta nije nastala usled namere ili nepažnje kvalifikovanog pružaoca usluga od poverenja iz stava 1. ovog člana je na tom pružaocu usluga.	PU		
13.2.	Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.	25.4.	Pružalac usluga od poverenja nije odgovoran za štetu nastalu zbog korišćenja usluge kojim je prekoračeno naznačeno ograničenje ukoliko je korisnik usluge od poverenja o takvom ograničenju unapred obavešten.	PU		

a)	a1)	b)	b1)	v)	g)	d)
13.3.	Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.			NP	Odredba upućuje da se čl.13. st. 1. i 2. Uredbe primenjuje u skladu sa nacionalnim propisima država članica EU o odgovornosti za štetu, zbog čega nije prenosiva.	
14.	1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU. 2. Agreements referred to in paragraph 1 shall ensure, in particular, that: (a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide; (b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.			NP	Odredba je neprenosiva, jer se njome utvrđuju postupci i uslovi koje Evropska unija predviđa radi priznavanja dejstva usluga od poverenja koje vrše pružaoci usluga iz trećih zemalja. Ukazujemo da je članom 40. ovog zakona predviđeno da je kvalifikovana usluga od poverenja koju pruža strani pružalac usluge od poverenja ravnopravna sa domaćom uslugom od poverenja ukoliko je tako regulisano potvrđenim međunarodnim sporazumom.	
15.	Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.	6.	U meri u kojoj je to moguće, usluge od poverenja, usluge elektronske identifikacije i proizvodi koji se koriste za pružanje tih usluge treba da su dostupni osobama sa invaliditetom.	PU		
16.	Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.	68.	Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj pružalac kvalifikovane usluge od poverenja – pravno lice ako: 1) ne preduzima potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga od poverenja	PU		

a)	a1)	b)	b1)	v)	g)	d)
			(član 27. stav 1.); 2) bez odlaganja, a najkasnije u roku od 24 sata od saznanja, ne obavesti Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge koji imaju značajan uticaj na pružanje usluga od poverenja ili na zaštitu podataka o ličnosti koji se obrađuju u okviru pružanja usluge (član 27. stav 3.); 3) o povredi bezbednosti ili gubitku integriteta usluge bez odlaganja ne obavesti korisnika usluge od poverenja ukoliko bi ugrožavanje bezbednosti ili gubitak integriteta usluge od poverenja moglo nepovoljno uticati na korisnike usluga od poverenja (član 27. stav 4.); 4) pre zaključenja ugovora iz člana 30. stav 1. ovog zakona ne obavesti lice koje je podnelo zahtev za pružanje kvalifikovane usluge po poverenja o svim važnim okolnostima korišćenja usluge iz člana 30. stav 2. tač. 1) do 3) ovog zakona (član 30. stav 2.); 5) ne ispunjava uslove iz člana 31. (član 31.); 6) pri izdavanju kvalifikovanog sertifikata za usluge od poverenja ne proveri podatke o identitetu fizičkog odnosno pravnog lica koji su sadržani u kvalifikovanom sertifikatu, u skladu sa članom 33. stav 2. zakona (član 33. st. 1. i 2.); 7) ne izvrši proveru ispunjenosti uslova pre početka pružanja kvalifikovanih usluga od poverenja, odnosno najmanje jednom u 24 meseca (član 34. stav 4.); 8) ne izvrši nalog za vanredno ocenjivanje ispunjenosti uslova (član 34. stav 5); 9) pre otpočinjanja pružanja kvalifikovanih usluga od poverenja ne izvrši upis u Registar pružaoca kvalifikovanih usluga od poverenja (član 35. stav 2.); 10) izdavalac kvalifikovanih elektronskih sertifikata, koji namerava da prestane sa obavljanjem delatnosti, o nameri raskida ugovora ne obavesti svakog korisnika kvalifikovane usluge od poverenja i Ministarstvo najmanje tri meseca pre nastanka o nameravanom prestanku obavljanja delatnosti (član 36. stav 1.); 11) u slučaju prestanka sa obavljanjem poslova ne obezbedi kod drugog pružaoca usluga od poverenja nastavak obavljanja usluge za korisnike kojima je			

a)	a1)	b)	b1)	v)	g)	d)
			izdao sertifikat, ili ne opozove sve izdate sertifikate i o preduzetim merama odmah ne obavesti Ministarstvo (član 36. stav 2.); 12) ne dostavi svu dokumentaciju u vezi sa obavljanjem usluga od poverenja drugom izdavaocu na koga prenosi obaveze obavljanja jedne ili više usluga od poverenja, odnosno Ministarstvu (član 36. stav 3.); 13) kvalifikovani elektronski sertifikat ne sadrži sve podatke iz člana 43. stav 1. ovog zakona (član 43. stav 1.); 14) izdavalac kvalifikovanih sertifikata ne izvrši opoziv izdatih sertifikata, u slučajevima iz člana 44. stav 1. (član 44. stav 1.); 15) izdavalac kvalifikovanih sertifikata ne obavesti korisnika kvalifikovane usluge od poverenja o opozivu sertifikata u roku od 24 časa od primljenog obaveštenja, odnosno nastanka okolnosti zbog kojih se sertifikat opoziva (član 44. stav 2.); 16) izdavalac kvalifikovanih sertifikata ne čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovani sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja sertifikata (član 45.); 17) ne obezbedi povezivanje sa Centralnim sistemom i ne omogući prijem i slanje poruka i u slučaju kada je pošiljalac ili primalac poruke korisnik drugog pružaoca usluge kvalifikovane elektronske dostave (član 56. stav 2); 18) pouzdano elektronsko čuvanje dokumenata pripremljenih u skladu sa članom 62. ovog zakona, kojima je kvalifikovanim elektronskim potpisom odnosno pečatom iz člana 62. stav 1. tačka 4) potvrđena vernost izvornom dokumentu i tačnost dodatno uključenih podataka, se ne vrši tako da se tokom čuvanja koriste postupci i tehnološka rešenja kojima se obezbeđuje mogućnost dokazivanja validnosti kvalifikovanog elektronskog potpisa odnosno pečata tokom celog perioda čuvanja (član 63. stav 2). Za prekršaj iz stava 1. ovog člana kazniće se i			

a)	a1)	b)	b1)	v)	g)	d)
			odgovorno lice pružaoca usluge od poverenja novčanom kaznom od 5.000 do 100.000 dinara. Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge od poverenja - fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara. Novčanom kaznom od 50.000 do 200.000 dinara kazniće se za prekršaj korisnik kvalifikovane usluge od poverenja – pravno lice ako: 1) u slučaju promene podataka iz stava 1. člana 33. ovog zakona ne obavesti bez odlaganja pružaoca kvalifikovane usluge od poverenja (član 33. stav 3.); Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom od 5.000 do 50.000 dinara. Za prekršaj iz stava 1. ovog člana kazniće se korisnik usluge od poverenja - fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 100.000 dinara. Za prekršaj iz stava 1. ovog člana kazniće se korisnik usluge od poverenja - fizičko lice novčanom kaznom od 5.000 do 50.000 dinara. Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj registrovan pružalac usluge elektronske identifikacije – pravno lice ako: 1) šema elektronske identifikacije ne ispunjava uslove iz člana 17. (član 17); 2) ne preduzima potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga iz člana 22. stav 2. ovog zakona (član 22. stav 1. i 2.); Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice pružaoca usluge elektronske identifikacije novčanom kaznom od 5.000 do 100.000 dinara. Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge elektronske identifikacije – fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara.			

a)	a1)	b)	b1)	v)	g)	d)
		69. 70.	Novčanom kaznom od 50.000 do 2.000.000 dinara kazniće se za prekršaj pružalac usluge iz člana 66. ovog zakona ukoliko ne postupi po nalogu inspektora u ostavljenom roku iz člana 67. stav 1. ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice pružaoca usluge novčanom kaznom od 5.000 do 100.000 dinara. Za prekršaj iz stava 1. ovog člana kazniće se pružalac usluge – fizičko lice u svojstvu registrovanog subjekta novčanom kaznom od 10.000 do 500.000 dinara.			

a)	a1)	b)	b1)	v)	g)	d)
		71.				
17.1.	Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.	28.	Ministarstvo nadležno za poslove informacionog društva vrši sledeće poslove: 1) vodi registar pružaoca kvalifikovanih usluga od poverenja; 2) razmatra izveštaje o proveri ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja; 3) vrši inspekcijski nadzor nad radom pružaoca usluga od poverenja; 4) nalaže vanrednu proveru ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja, u skladu sa zakonom; 5) sarađuje sa nadležnim organom za zaštitu podataka o ličnosti, i obaveštava ga bez odlaganja ukoliko dođe	PU		

a)	a1)	b)	b1)	v)	g)	d)
		29.	do saznanja da pružaoci kvalifikovanih usluga od poverenja ne postupaju u skladu sa propisima o zaštiti podataka o ličnosti; 6) proverava postojanje i pravilnu primenu odredaba o planovima prekida aktivnosti u slučajevima kada pružalac kvalifikovane usluge od poverenja prekine svoje aktivnosti, uključujući način na koji se održava dostupnost informacija koje izdaje i prima pružalac kvalifikovane usluge od poverenja; 7) sarađuje sa nadzornim telima iz člana 17. Uredbe eIDAS; 8) obaveštava javnost o ugrožavanju bezbednosti ili gubitku celovitosti usluga od poverenja koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke. Ministarstvo obavlja i poslove: 1) obaveštava nadležna tela država članica Evropske unije o ugrožavanju bezbednosti ili gubitku celovitosti koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke; 2) izveštava Evropsku komisiju o svojim aktivnostima u skladu sa Uredbom eIDAS.			
17.2.	Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.			NP	Odredba se odnosi na obavezu država članica EU da obaveste Evropsku komisiju o nadležnom organu. Takva obaveza se isključivo može odnositi na države članice i ne može se preneti u domaći propis.	

a)	a1)	b)	b1)	v)	g)	d)
17.3.a	The role of the supervisory body shall be the following: (a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;	28.1.3.	Ministarstvo nadležno za poslove informacionog društva vrši sledeće poslove: 3) vrši inspekcijski nadzor nad radom pružaoca usluga od poverenja;	PU		
17.3.b	to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.	66. 67.	Inspekcija za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju vrši inspekcijski nadzor nad primenom ovog zakona i radom pružalaca usluga elektronske identifikacije i pružalaca usluga od poverenja (u daljem tekstu: pružaoci usluga) preko inspektora za elektronsku identifikaciju i usluge od poverenja (u daljem tekstu: inspektor) Inspektor je ovlašćen da u postupku inspekcijskog nadzora: 1) nalaže otklanjanje utvrđenih nepravilnosti i za to ostavi rok; 2) zabranjuje upotrebu neadekvatnih postupaka i infrastrukture, i daje rok pružaocu usluga u kojem je dužan da obezbedi adekvatne postupke i infrastrukturu; 3) privremeno zabranjuje vršenje usluge pružaoca usluga do otklanjanja neadekvatnosti postupaka i infrastrukture; 4) naređuje privremeni opoziv nekog ili svih sertifikata izdatih od strane pružaoca usluge, ako postoji osnovana sumnja da se radi o neadekvatnom postupku ili falsifikatu.	PU		
17.4.a	For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular: (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;	28.1.7.	Ministarstvo nadležno za poslove informacionog društva vrši sledeće poslove: 7) sarađuje sa nadzornim telima iz člana 17. Uredbe eIDAS;	PU		

a)	a1)	b)	b1)	v)	g)	d)
17.4.b	(b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);	28.1.2.	2) razmatra izveštaje o proveri ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja;	PU		
17.4.c	(c) inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);	28.1.8. 29.1.1.	8) obaveštava javnost o ugrožavanju bezbednosti ili gubitku celovitosti usluga od poverenja koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke; Ministarstvo obavlja i poslove: 1) obaveštava nadležna tela država članica Evropske unije o ugrožavanju bezbednosti ili gubitku celovitosti koji imaju značajan uticaj na pruženu uslugu od poverenja ili u njoj sadržane lične podatke	PU		
17.4.d	(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;	29.1.2.	2) izveštava Evropsku komisiju o svojim aktivnostima u skladu sa Uredbom eIDAS.	PU		
17.4.e	(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);	28.1.3. 28.1.4.	3) vrši inspekcijski nadzor nad radom pružaoca usluga od poverenja; 4) nalaže vanrednu proveru ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja, u skladu sa zakonom;	PU		
17.4.f	(f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;	28.1.5.	5) sarađuje sa nadležnim organom za zaštitu podataka o ličnosti, i obaveštava ga bez odlaganja ukoliko dođe do saznanja da pružaoci kvalifikovanih usluga od poverenja ne postupaju u skladu sa propisima o zaštiti podataka o ličnosti;	PU		
17.4.g	(g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;	28.1.1.	1) vodi registar pružaoca kvalifikovanih usluga od poverenja;	PU		
17.4.h	(h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;	38.1.	Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja u elektronskom obliku koji je pogodan za automatsku obradu.	PU	Sa ovom odredbom postoji usklađenost, s obzirom da je Ministarstvo nadležni organ za primenu ovog zakona i organ koji objavljuje Javnu listu kvalifikovanih usluga od poverenja.	
17.4.i	(i) to verify the existence and correct application of provisions on termination plans in cases where the	28.1.6.	6) proverava postojanje i pravilnu primenu odredaba o planovima prekida aktivnosti u slučajevima kada	PU		

a)	a1)	b)	b1)	v)	g)	d)
	qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);		pružalac kvalifikovane usluge od poverenja prekine svoje aktivnosti, uključujući način na koji se održava dostupnost informacija koje izdaje i prima pružalac kvalifikovane usluge od poverenja;			
17.4.j	(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.	66.2. 67.1.1.	U okviru inspekcijskog nadzora pružalaca usluga inspektor utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim za sprovođenje ovog zakona. Inspektor je ovlašćen da u postupku inspekcijskog nadzora: 1) nalaže otklanjanje utvrđenih nepravilnosti i za to ostavi rok	PU		
17.5.	Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.			NP	Odredba je diskreciona i odnosi se na mogućnost države članice da uspostavi infrastrukturu od poverenja.	
17.6.	By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).			NP	Odredba se odnosi na obavezu država članica EU da podnose izveštaje Evropskoj komisiji.	
17.7.	The Commission shall make the annual report referred to in paragraph 6 available to Member States.			NP	Odredba se odnosi na izradu godišnjih izveštaja od strane Evropske komisije.	
17.8.	The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva u propis Republike Srbije, jer uređuje ovlašćenje Evropske komisije da donese akt za primenu propisa.	

a)	a1)	b)	b1)	v)	g)	d)
18.	1. Supervisory bodies shall cooperate with a view to exchanging good practice. A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21. 2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds: (a) the supervisory body is not competent to provide the requested assistance; (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17; (c) providing the requested assistance would be incompatible with this Regulation. 3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law			NP	Odredbe se odnose na postupanje država članica EU u pogledu uzajamne pomoći u ovoj oblasti, određuje njihovo postupanje i primenjivaće se u Republici Srbiji od dana pristupanja Evropskoj uniji.	
19.1.	Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.	27.1. 27.2.	Pružaoci usluga od poverenja, uključujući kvalifikovane usluge od poverenja, preduzimaju potrebne tehničke i organizacione mere za upravljanje rizicima koji ugrožavaju pouzdano i bezbedno pružanje tih usluga od poverenja. Tehničkim i organizacionim merama osigurava se da nivo bezbednosti odgovara stepenu rizika, uzimajući u obzir najnovija dostupna tehnološka rešenja, a posebno se preduzimaju mere za sprečavanje bezbednosnih incidenata i ograničavanje štetnih posledica eventualnih incidenata, kao i za	PU		

a)	a1)	b)	b1)	v)	g)	d)
			obaveštavanje zainteresovanih strana o neželjenim efektima bezbednosnih incidenata.			
19.2.1.	Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.	27.3.	Pružaoci usluga od poverenja, uključujući pružaoce kvalifikovanih usluga od poverenja, bez odlaganja, a najkasnije u roku od 24 sata od saznanja, obaveštavaju Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge koji imaju značajan uticaj na pružanje usluga od poverenja ili na zaštitu podataka o ličnosti koji se obrađuju u okviru pružanja usluge.	PU		
19.2.2.	Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.	27.4.	Ukoliko bi ugrožavanje bezbednosti ili gubitak integriteta usluge od poverenja moglo nepovoljno uticati na korisnike usluga od poverenja, pružalac usluga od poverenja o povredi bezbednosti ili gubitku integriteta usluge bez odlaganja obaveštava korisnika usluga od poverenja.	PU		
19.2.3.	Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.	27.6.	Ministarstvo će ostvariti saradnju sa odgovarajućim institucijama drugih država po pitanju razmene podataka o narušavanju bezbednosti i integriteta, u skladu sa odgovarajućim potvrđenim međunarodnim sporazumima.	PU		
19.2.4.	The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.	27.5.	Ministarstvo obaveštava javnost ili zahteva od pružaoca usluga od poverenja da to učini ako utvrdi da je objavljivanje podataka o povredi bezbednosti ili gubitka integriteta usluge u javnom interesu.	PU		
19.3.	The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.			NP	Odredba se odnosi na izveštavanje Evropske agencije za mrežnu i informacionu bezbednost od strane nadležnih tela država članica.	
19.4.	The Commission may, by means of implementing acts: (a) further specify the measures referred to in paragraph 1; and (b) define the formats and procedures,			NP	Odredbe se odnose na ovlašćenje Evropske komisije da donosi akta za primenu navedenih odredbi.	

a)	a1)	b)	b1)	v)	g)	d)
	including deadlines, applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
20.1.	Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.	34.1. 34.3. 34.4.	Ocenjivanje ispunjenosti uslova za pružanje kvalifikovanih usluga od poverenja (u daljem tekstu: ocenjivanje ispunjenosti uslova) obavlja telo za ocenjivanje usaglašenosti koje je, u skladu sa zakonom kojim se uređuje akreditacija, akreditovano za ocenjivanje usaglašenosti pružaoca kvalifikovanih usluga od poverenja i kvalifikovanih usluga od poverenja koje oni pružaju. Ocenjivanje ispunjenosti uslova vrši se pre početka pružanja kvalifikovanih usluga od poverenja i najmanje jednom u 24 meseca. Nakon završenog ocenjivanja ispunjenosti uslova pružalac usluge od poverenja dostavlja Ministarstvu izveštaj o ocenjivanju usaglašenosti u roku od tri radna dana od dana kada ga je primio.	PU		
20.2.	Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.	34.5. 34.7.	Ministarstvo može naložiti vanredno ocenjivanje ispunjenosti uslova ukoliko se utvrde nepravilnosti u pružanju kvalifikovanih usluga od poverenja ili u slučaju incidenta koji je u značajnoj meri ugrozio ili narušio informacionu bezbednost. Troškove ocenjivanja ispunjenosti uslova, uključujući vanredna ocenjivanja, snosi pružalac kvalifikovane usluge od poverenja. Ministarstvo nadležno za poslove informacionog društva vrši sledeće poslove:	PU		

a)	a1)	b)	b1)	v)	g)	d)
		28.1.5.	5) sarađuje sa nadležnim organom za zaštitu podataka o ličnosti, i obaveštava ga bez odlaganja ukoliko dođe do saznanja da pružaoci kvalifikovanih usluga od poverenja ne postupaju u skladu sa propisima o zaštiti podataka o ličnosti			
20.3.	Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.	35.6. 38.2.	Ako pružalac usluga prestane da ispunjava uslove propisane ovim zakonom Ministarstvo donosi rešenje o njegovom brisanju iz registra iz stava 1. ovog člana. Podaci u Javnoj listi kvalifikovanih usluga od poverenja izvode se iz Registra iz člana 35. ovog zakona.	PU		
20.4. 20.5.	The Commission may, by means of implementing acts, establish reference number of the following standards: (a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1; (b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba se odnose na ovlašćenje Evropske komisije da donosi akta za primenu navedenih odredbi.	
21.1.	Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a	35.1.	Pružalac kvalifikovanih usluga od poverenja podnosi Ministarstvu zahtev za upis u Registar pružalaca kvalifikovanih usluga od poverenja, koji vodi	PU		

a)	a1)	b)	b1)	v)	g)	d)
	notification of their intention together with a conformity assessment report issued by a conformity assessment body.	35.2. 35.3.	Ministarstvo. Pružalac kvalifikovanih usluga od poverenja mora biti upisan u registar iz stava 1. ovog člana pre otpočinjanja pružanja kvalifikovanih usluga od poverenja. Uz zahtev iz stava 1. ovog člana prilažu se dokazi o činjenicama iskazanim u zahtevu uključujući izveštaj o ocenjivanju usaglašenosti iz člana 34. stav 4. ovog zakona kojim je ocenjeno da podnosilac zahteva i kvalifikovane usluge od poverenja koje on namerava da pruža ispunjavaju uslove iz ovog zakona.			
21.2.1.	The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.	35.4. 35.5.	Ministarstvo rešava o upisu pružaoca kvalifikovanih usluga od poverenja u registar iz stava 1. ovog člana u roku od 60 dana od dana podnošenja urednog zahteva. U postupku rešavanja iz stava 4. ovog člana Ministarstvo može zahtevati prilaganje dodatnih dokaza, kao i dodatnu proveru tehničkih i bezbednosnih komponenti i operativnog rada.	PU		
21.2.2.	If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.	35.4. 38.1. 38.2.	Ministarstvo rešava o upisu pružaoca kvalifikovanih usluga od poverenja u registar iz stava 1. ovog člana u roku od 60 dana od dana podnošenja urednog zahteva. Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja u elektronskom obliku koji je pogodan za automatsku obradu. Podaci u Javnoj listi kvalifikovanih usluga od poverenja izvode se iz Registra iz člana 35. ovog zakona.	PU		
21.2.3.	If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.			DU	Davanje statusa kvalifikovanog pružaoca usluga od poverenja vrši se u upravnom postupku. Imajući u vidu da je Zakonom o opštem upravnom postupku predviđeno da je rok za izdavanje rešenja u upravnom postupku 60 dana, u slučaju kada se o	

a)	a1)	b)	b1)	v)	g)	d)
					upravnoj stvari ne odlučuje u postupku neposrednog odlučivanja, mišljenja smo da nije bilo neophodno prenositi predmetnu odredbu Uredbe u tekst ovog zakona.	
21.3.	Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).	35.2. 38.1. 38.2.	Pružalac kvalifikovanih usluga od poverenja mora biti upisan u registar iz stava 1. ovog člana pre otpočinjanja pružanja kvalifikovanih usluga od poverenja. Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja u elektronskom obliku koji je pogodan za automatsku obradu. Podaci u Javnoj listi kvalifikovanih usluga od poverenja izvode se iz Registra iz člana 35. ovog zakona.	PU		
21.4.	The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba se odnose na ovlašćenje Evropske komisije da donosi akta za primenu navedenih odredbi.	
22.1.	Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.	38.1. 38.2.	Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja u elektronskom obliku koji je pogodan za automatsku obradu. Podaci u Javnoj listi kvalifikovanih usluga od poverenja izvode se iz Registra iz člana 35. ovog zakona.	PU		
22.2.	Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.	38.1. 38.3.	Ministarstvo objavljuje Javnu listu kvalifikovanih usluga od poverenja u elektronskom obliku koji je pogodan za automatsku obradu. Javna lista kvalifikovanih usluga od poverenja potpisuje se naprednim elektronskim pečatom.	PU		

a)	a1)	b)	b1)	v)	g)	d)
22.3. 22.4. 22.5.	Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba se odnosi na obavezu država članica Evropske unije da obaveste Evropsku komisiju o telu koje je nadležno za javne liste kvalifikovanih usluga od poverenja. Pored toga, odredbom se predviđa ovlašćenje Evropske komisije da donese akte za primenu predmetnih odredbi na nivou Evropske unije.	
23.1. 23.2. 23.3.	1.After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide. 2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website. 3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva, s obzirom da se njom predviđa izdavanje EU znaka pouzdanosti za pružaoce usluga od poverenja iz EU.	
24.1.1.	When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national	33.1.	Pri izdavanju kvalifikovanog sertifikata za usluge od poverenja pružalac kvalifikovane usluge od poverenja proverava podatke o identitetu fizičkog odnosno	PU		

a)	a1)	b)	b1)	v)	g)	d)
	law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.		pravnog lica koji su sadržani u kvalifikovanom sertifikatu, u skladu sa zakonom.			
24.1.2.a.	The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law: (a) by the physical presence of the natural person or of an authorised representative of the legal person; or	33.2.1.	Proveru podataka iz stava 1. ovog člana pružalac kvalifikovane usluge od poverenja vrši u skladu sa zakonom, i to: 1) uz fizičko prisustvo fizičkog lica ili ovlašćenog predstavnika pravnog lica;	PU		
24.1.2.b. 24.1.2.c. 24.1.2.d.	(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b) (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.	33.2.2.	2) putem javne isprave koja služi kao sredstva identifikacije na daljinu, u skladu sa zakonom.	PU		
24.2.2.a	A qualified trust service provider providing qualified trust services shall: (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;	36.1.	Izdavalac kvalifikovanih elektronskih sertifikata koji namerava da prestane sa obavljanjem delatnosti dužan je da o nameri raskida ugovora obavesti svakog korisnika kvalifikovane usluge od poverenja i Ministarstvo najmanje tri meseca pre nastanka nameravanog prestanka obavljanja delatnosti.	PU		
24.2.2.b	(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;	31.1.1.	Pružalac kvalifikovanih usluga od poverenja mora: 1) imati zaposlene koji poseduju neophodnu stručnost, iskustvo i kvalifikacije za primenu administrativnih i upravljačkih procedura koje odgovaraju evropskim i međunarodnim standardima i koji su prošli odgovarajuću obuku u oblasti informacione bezbednosti i zaštite podataka o ličnosti;	PU		

a)	a1)	b)	b1)	v)	g)	d)
24.2.2.c.	(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;	31.1.2.	2) biti osiguran od odgovornosti za štetu nastalu vršenjem kvalifikovane usluge od poverenja;	PU		
24.2.2.d	(d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;	30.2.	Pružalac kvalifikovane usluge od poverenja je dužan da, pre zaključivanja ugovora iz stava 1. ovog člana, obavesti lice koje je podnelo zahtev za pružanje kvalifikovane usluge od poverenja o svim važnim okolnostima korišćenja usluge, a posebno o: 1) propisima i internim pravilima koji se odnose na korišćenje kvalifikovane usluge od poverenja; 2) eventualnim ograničenjima u korišćenju kvalifikovane usluge od poverenja; 3) merama koje treba da realizuju korisnici kvalifikovane usluge od poverenja i o potrebnoj tehnologiji za bezbedno korišćenje kvalifikovane usluge od poverenja.	PU		
24.2.2.e	(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;	31.1.3.	Pružalac kvalifikovanih usluga od poverenja mora: 3) koristiti sigurne uređaje i proizvode koji su zaštićeni od neovlašćene promene i garantuju tehničku bezbednost i pouzdanost procesa koje podržavaju;	PU		
24.2.2.f	(f) use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity;	31.1.4.	4) koristiti sigurne sisteme za čuvanje podataka koji su mu povereni tako: (1) da su javno raspoloživi samo kada je dobijena saglasnost lica čiji su to podaci, (2) da samo ovlašćena lica mogu unositi podatke i vršiti izmene, (3) da se može proveravati autentičnost podataka;	PU		
24.2.2.g	(g) take appropriate measures against forgery and theft of data;	31.1.5.	5) sprovoditi mere protiv falsifikovanja i krađe podataka	PU		
24.2.2.h	(h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service	31.1.6.	6) čuvati u odgovarajućem vremenskom periodu sve relevantne informacije koje se odnose na podatke koji su kreirani ili primljeni od strane pružaoca kvalifikovanih usluga od poverenja, a posebno za svrhu pružanja dokaza u pravnim postupcima.	PU		

a)	a1)	b)	b1)	v)	g)	d)
	provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;		Čuvanje se može vršiti elektronskim putem;			
24.2.2.i	(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);	31.1.8.	8) imati ažuran plan završetka rada koji osigurava kontinuitet kvalifikovanih usluga od poverenja;	PU		
24.2.2.j	(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;	31.1.9.	9) osigurati obradu ličnih podataka u skladu sa zakonima Republike Srbije	PU		
24.2.2.k	(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.	31.1.7.	7) voditi ažurnu, tačnu i bezbednim merama zaštićenu bazu podataka izdatih elektronskih sertifikata koja mora da bude javno dostupna, osim u slučajevima kada vlasnik sertifikata izričito zahteva da njegovi podaci ne budu javno dostupni;	PU		
24.3.	If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.	44.2. 44.4. 45.1.	Izdavalac kvalifikovanih sertifikata je dužan da obavesti korisnika kvalifikovane usluge od poverenja o opozivu sertifikata u roku od 24 časa od primljenog obaveštenja, odnosno nastanka okolnosti zbog kojih se sertifikat opoziva. U slučaju opoziva kvalifikovani elektronski sertifikat trajno prestaje da važi od trenutka opoziva. Izdavalac kvalifikovanih elektronskih sertifikata je dužan da čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja sertifikata. Podaci iz stava 1. ovog člana mogu se čuvati u elektronskoj formi.	PU		

a)	a1)	b)	b1)	v)	g)	d)
		45.2.				
24.4.	With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.	43.1.9. 45.1. 45.2.	Kvalifikovani elektronski sertifikat mora da sadrži: 9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata Izdavalac kvalifikovanih elektronskih sertifikata je dužan da čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja sertifikata. Podaci iz stava 1. ovog člana mogu se čuvati u elektronskoj formi.	PU		
24.5.	The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba se odnosi na ovlašćenje Evropske komisije da donese akte za primenu ovih odredaba na nivou EU.	
25.1.	An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.	50.1.	Elektronskom potpisu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovani elektronski potpis.	PU		

a)	a1)	b)	b1)	v)	g)	d)
25.2.	A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.	50.2.	Kvalifikovani elektronski potpis ima isto pravno dejstvo kao i svojeručni potpis.	PU		
25.3.	A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.			NP	Odredba se odnosi na priznavanje kvalifikovanih potpisa države članice EU.	
26.1.a	An advanced electronic signature shall meet the following requirements: (a) it is uniquely linked to the signatory;	42.1.1.	Napredni elektronski potpis odnosno napredni elektronski pečat mora ispunjavati sledeće uslove: 1) na nedvosmislen način je povezan sa potpisnikom odnosno pečatiocem;	PU		
26.2.b	(b) it is capable of identifying the signatory;	42.1.2.	2) omogućava utvrđivanje identiteta potpisnika odnosno autora pečata;	PU		
26.2.c	(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and	42.1.3.	3) izrađen je korišćenjem podataka za izradu elektronskog potpisa odnosno elektronskog pečata koje potpisnik odnosno pečatilac može, uz visok nivo pouzdanosti, koristi pod svojom isključivom kontrolom;	PU		
26.2.d	(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.	42.1.4.	4) povezan je sa elektronski potpisanim odnosno elektronski pečatiranim podacima na način da se može utvrditi bilo koja naknadna izmena tih podataka.	PU		
27.1. 27.2.	If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.			NP	Odredbe se odnose na postupanje država članica EU u pogledu međusobnog priznavanja naprednih elektronskih potpisa i kvalifikovanih elektronskih potpisa prilikom korišćenja usluga organa javne vlasti. Takođe, odredbe se odnose i na ovlašćenje Evropske komisije da donese akta za primenu odredaba na nivou EU.	

a)	a1)	b)	b1)	v)	g)	d)
27.3. 27.4. 27.5.	Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
28.1. 28.2.	Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.	43.1.	Kvalifikovani elektronski sertifikat mora da sadrži: 1) oznaku, u formi pogodnoj za automatsku obradu, da se elektronski sertifikat koristi kao kvalifikovani sertifikat za elektronski potpis, odnosno pečat; 2) skup podataka koji jedinstveno identifikuju kvalifikovanog pružaoca usluge od poverenja za izdavanje kvalifikovanog elektronskog sertifikata uključujući najmanje zemlju porekla pružaoca i naziv	PU		

a)	a1)	b)	b1)	v)	g)	d)
			pružaoca; 3) skup podataka koji jedinstveno identifikuju potpisnika odnosno pečatioca uključujući najmanje: (1) za potpisnika: - ime i prezime ili pseudonim , a ukoliko je upotrebljen pseudonim to mora biti jasno obeleženo u okviru kvalifikovanog elektronskog sertifikata; - JMBG, ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG; (2) za pečatioca: naziv, država i matični broj odnosno jedinstvena identifikaciona oznaka u skladu sa pravnom regulativom te države, ukoliko postoji; 4) podatke za proveru elektronskog potpisa odnosno elektronskog pečata koji odgovaraju podacima za kreiranje tog elektronskog potpisa odnosno elektronskog pečata; 5) podatke o početku i kraju važenja kvalifikovanog elektronskog sertifikata; 6) serijski broj kvalifikovanog elektronskog sertifikata koji mora biti jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata; 7) napredni elektronski potpis ili napredni elektronski pečat izdavaoca kvalifikovanog elektronskog sertifikata; 8) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 7); 9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata; 10) oznaku da su podaci za kreiranje elektronskog potpisa odnosno pečata, koji odgovaraju podacima za proveru elektronskog potpisa odnosno pečata iz kvalifikovanog elektronskog sertifikata, sadržani u kvalifikovanom sredstvu za kreiranje elektronskog potpisa odnosno pečata, ukoliko je taj uslov ispunjen.			
28.3.	Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.	43.2.	Kvalifikovani elektronski sertifikati mogu uključivati dodatna obeležja pored obeležja iz stava 1. ovog člana.	PU		
28.4.	If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its	44.4.	U slučaju opoziva kvalifikovani elektronski sertifikat trajno prestaje da važi od trenutka opoziva.	PU		

a)	a1)	b)	b1)	v)	g)	d)
	validity from the moment of its revocation, and its status shall not in any circumstances be reverted.					
28.5.a	Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature: (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;	44.5.	U slučaju suspenzije kvalifikovani elektronski sertifikat gubi važnost tokom perioda trajanja suspenzije.	PU		
28.5.b.	(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate	44.6.	Podaci o suspenziji i periodu trajanja suspenzije kvalifikovanog elektronskog sertifikata upisuju se u bazu podataka izdatih sertifikata koju vodi izdavalac kvalifikovanih elektronskih sertifikata i moraju biti vidljivi tokom trajanja suspenzije u okviru usluga kojima se pružaju informacije o statusu sertifikata.	PU		
28.6.	The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredbom se daje ovlašćenje Evropskoj komisiji da donese akte za primenu na nivou EU. Ukazujemo da je članom 43. stav 3. ovog zakona predviđeno da Ministarstvo bliže propisuje uslove koje mora da ispunjavaju kvalifikovani elektronski sertifikati.	
29.1.	Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.	46.1.	Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata mora da, pomoću odgovarajućih tehničkih rešenja i postupaka, obezbedi: 1) poverljivost podataka za kreiranje elektronskog potpisa odnosno pečata; 2) da se podaci za kreiranje elektronskog potpisa odnosno pečata pojavljuju samo jednom; 3) da se podaci za kreiranje elektronskog potpisa odnosno pečata ne mogu dobiti izvan sredstva za kreiranje elektronskog potpisa odnosno pečata upotrebom dostupne tehnologije u razumnom vremenu;	PU		

a)	a1)	b)	b1)	v)	g)	d)
		46.2. 46.3. 46.4.	4) da je elektronski potpis odnosno pečat pouzdano zaštićen od falsifikovanja upotrebom dostupne tehnologije; 5) mogućnost pouzdane zaštite podataka za kreiranje elektronskog potpisa odnosno pečata od neovlašćenog korišćenja. Sredstva za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata, prilikom kreiranja elektronskog potpisa odnosno pečata, ne smeju promeniti podatke koji se potpisuju odnosno pečatiraju ili onemogućiti potpisniku odnosno autoru pečata uvid u te podatke pre procesa kreiranja kvalifikovanog elektronskog potpisa odnosno pečata. Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata korisnik kvalifikovane usluge od poverenja može koristiti putem usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata. Izuzetno od stava 1. ovog člana kvalifikovani pružalac usluga od poverenja iz stava 3. ovog člana može izraditi kopiju podataka za izradu elektronskog potpisa odnosno pečata u svrhu zaštite od gubitka podataka ukoliko su ispunjeni sledeći uslovi: 1) izrada i čuvanje kopija podataka za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata ne umanjuju propisani nivo zaštite tih podataka; 2) broj izrađenih kopija podataka za kreiranje elektronskog potpisa odnosno pečata nije veći nego što je to neophodno za obezbeđivanje kontinuiteta pružanja usluge.			
29.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for				Odredba je neprenosiva, jer se njom daje ovlašćenje Evropskoj	

a)	a1)	b)	b1)	v)	g)	d)
	qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	komisiji da donese akta za primenu na nivou EU.	
30.1.	Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.	47.1.	U skladu sa zakonom kojim se uređuju tehnički zahtevi za proizvode i ocenjivanje usaglašenosti Ministarstvo imenuje telo za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata sa tehničkim propisom iz člana 46.	PU		
30.2.	Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.			NP	Odredba je neprenosiva, s obzirom da se njom zadužuju države članice EU da prijavljuju Evropskoj komisiji tela za ocenjivanje usaglašenosti koja su imenovali.	
30.3.1.a	The certification referred to in paragraph 1 shall be based on one of the following: (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or	47.1. 47.2 46.5.	U skladu sa zakonom kojim se uređuju tehnički zahtevi za proizvode i ocenjivanje usaglašenosti Ministarstvo imenuje telo za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata sa tehničkim propisom iz člana 46. (u daljem tekstu: imenovano telo). Tehničkim propisom iz člana 46. se takođe bliže uređuju uslovi koje mora da ispunjava imenovano telo. Ministarstvo bliže propisuje uslove koje mora da ispunjava sredstvo za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata tehničkim propisom.	PU		
30.3.1.b	(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the			NP	Odredba je u vezi sa prijavljivanjem procesa sertifikacije Evropskoj komisiji.	

a)	a1)	b)	b1)	v)	g)	d)
	Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.					
30.3.2. 30.4.	The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.				Odredbe su neprenosive, jer se članom 30. stav. 3. podstav 2. daje ovlašćenje Evropskoj komisiji za donošenje akta za primenu na nivou EU, a članom 30. stav 4. vrši se prenos nadležnosti Evropskoj komsiji za donošenje akta.	
31.1. 31.2. 31.3.	Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva, jer se odnosi na prijavljivanje informacija o sertifikovanim sredstvima za izdavanje kvalifikovanog elektronskog potpisa Evropskoj komisiji, kao i na ovlašćenje Evropske komisije da donosi akte za primenu na nivou EU. Ukazujemo da je članom 47. ovog zakona predviđeno da Ministarstvo vodi Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata na osnovu izveštaja koje dobija od imenovanih tela, kao i da se u taj registar upisuju i kvalifikovana sredstva za kreiranje elektronskog potpisa i elektronskog pečata sa spiska koji prema članu 31. Regulative koji objavljuje Evropska komisija.	

a)	a1)	b)	b1)	v)	g)	d)
32.1.a	The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that: (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	48.1.1.	Postupkom validacije se utvrđuje da elektronski potpis predstavlja ispravan kvalifikovani elektronski potpis kada su ispunjeni sledeći uslovi: 1) utvrđeno je da je sertifikat koji prati elektronski potpis u trenutku potpisivanja predstavljao kvalifikovani elektronski sertifikat;	PU		
32.1.b	(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	48.1.2.	2) utvrđeno je da je kvalifikovani elektronski sertifikat izdat od strane pružaoca usluge izdavanja kvalifikovanih sertifikata za elektronski potpis i važio je u trenutku potpisivanja;	PU		
32.1.c	(c) the signature validation data corresponds to the data provided to the relying party;	48.1.3.	3) utvrđeno je da podaci za validaciju elektronskog potpisa iz kvalifikovanog elektronskog sertifikata odgovaraju kombinaciji elektronskog potpisa i podataka koji su potpisani elektronskim potpisom;	PU		
32.1.d	(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	48.1.4.	4) pouzdajućoj strani je tačno prikazan skup podataka iz kvalifikovanog elektronskog sertifikata koji jedinstveno identifikuju potpisnika;	PU		
32.1.e	(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	48.1.6.	6) korišćenje pseudonima je jasno naznačeno pouzdajućoj strani, u slučaju da je je prilikom elektronskog potpisivanja korišćen pseudonim;	PU		
32.1.f	(f) the electronic signature was created by a qualified electronic signature creation device;	48.1.7.	7) utvrđeno je da je elektronski potpis kreiran korišćenjem kvalifikovanog sredstva za kreiranje elektronskog potpisa;	PU		
32.1.g	(g) the integrity of the signed data has not been compromised;	48.1.8.	8) utvrđeno je da nije narušen integritet podataka koji su potpisani elektronskim potpisom;	PU		
32.1.h	(h) the requirements provided for in Article 26 were met at the time of signing.	48.1.9.	9) utvrđeno je da elektronski potpis ispunjava uslove za napredni elektronski potpis iz ovog zakona.	PU		
32.2.	The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	48.2.	Sistem koji se koristi za validaciju kvalifikovanog elektronskog potpisa obezbeđuje tačan rezultat postupka validacije pouzdajućoj strani i omogućava joj identifikovanje bilo kog problema od značaja za pouzdanost.	PU		

a)	a1)	b)	b1)	v)	g)	d)
32.3.	The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva, jer se njome daje ovlašćenje Evropskoj komisiji da donosi akte za primenu predmetnog člana. Napominjemo da je članom 48. ovog zakona predviđeno da će Ministarstvo bliže propisuje uslove za postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.	
33.1.a	A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who: (a) provides validation in compliance with Article 32(1); and	49.1.1.	Pružalac usluge kvalifikovane validacije kvalifikovanih elektronskih potpisa odnosno pečata obezbeđuje: 1) validaciju kvalifikovanog elektronskog potpisa odnosno pečata u skladu sa članom 48. ovog zakona;	PU		
33.1.b	(b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	49.1.2. 49.1.3.	2) da pouzdajuća strana koja koristi uslugu dobije rezultat postupka validacije elektronskim putem na automatizovan način koji je pouzdan i efikasan; 3) da je rezultat postupka validacije iz tačke 2) ovog stava pečatiran naprednim elektronskim pečatom ili potpisan naprednim elektronskim potpisom pružaoca usluge.	PU		
33.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva, jer se odnosi na ovlašćenje Evropske komisije da donese akt za primenu navedenog člana. Ukazujemo da je članom 49. ovog zakona predviđeno da Ministarstvo bliže propisuje uslove za pružanje usluge kvalifikovane validacije kvalifikovanih elektronskih	

a)	a1)	b)	b1)	v)	g)	d)
					potpisa i kvalifikovanih elektronskih pečata.	
34.1.	A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.	65.1.	Usluga kvalifikovanog elektronskog čuvanja dokumenata je kvalifikovana usluga od poverenja putem koje se pruža pouzdano elektronsko čuvanje dokumenata u skladu sa čl. 62. i 63. ovog zakona.	PU		
34.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredba je neprenosiva, jer se odnosi na ovlašćenje Evropske komisije da donese akt za primenu navedenog člana. Ukazujemo da je čl. 62. i 63. ovog zakona predviđeno bliže uređenje ove materije od strane Vlade.	
35.1.	An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.	51.1.	Elektronskom pečatu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovan elektronski pečat.	PU		
35.2.	A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.	51.2.	Za kvalifikovani elektronski pečat važi pravna pretpostavka da obezbeđuje poreklo i integritet podataka za koje je vezan.	PU		
35.3.	A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.			NP	Odredba je neprenosiva, jer propisuje da se kvalifikovani elektronski pečati iz države članice EU priznaju u drugim državama članicama EU.	
36.1.a	An advanced electronic seal shall meet the following requirements: (a) it is uniquely linked to the creator of the seal;	42.1.1.	Napredni elektronski potpis odnosno napredni elektronski pečat mora ispunjavati sledeće uslove: 1) na nedvosmislen način je povezan sa potpisnikom odnosno pečatiocem;	PU		

a)	a1)	b)	b1)	v)	g)	d)
36.1.b	(b) it is capable of identifying the creator of the seal;	42.1.2.	2) omogućava utvrđivanje identiteta potpisnika odnosno autora pečata;	PU		
36.1.c	(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and	42.1.3.	3) izrađen je korišćenjem podataka za izradu elektronskog potpisa odnosno elektronskog pečata koje potpisnik odnosno pečatilac može, uz visok nivo pouzdanosti, koristi pod svojom isključivom kontrolom;	PU		
36.1.d	(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.	42.1.4.	4) povezan je sa elektronski potpisanim odnosno elektronski pečatiranim podacima na način da se može utvrditi bilo koja naknadna izmena tih podataka.	PU		
37.1. 37.2. 37.3.	If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall			NP	Odredbe se odnose na postupanje država članica EU u pogledu međusobnog priznavanja naprednih elektronskih potpisa i kvalifikovanih elektronskih potpisa prilikom korišćenja usluga organa javne vlasti. Takođe, odredbe se odnose i na ovlašćenje Evropske komisije da donese akta za primenu odredaba na nivou EU.	

a)	a1)	b)	b1)	v)	g)	d)
37.4. 37.5.	be adopted in accordance with the examination procedure referred to in Article 48(2). By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
38.1. 38.2.	Qualified certificates for electronic seals shall meet the requirements laid down in Annex III. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.	43.1.	Kvalifikovani elektronski sertifikat mora da sadrži: 1) oznaku, u formi pogodnoj za automatsku obradu, da se elektronski sertifikat koristi kao kvalifikovani sertifikat za elektronski potpis, odnosno pečat; 2) skup podataka koji jedinstveno identifikuju kvalifikovanog pružaoca usluge od poverenja za izdavanje kvalifikovanog elektronskog sertifikata uključujući najmanje zemlju porekla pružaoca i naziv pružaoca; 3) skup podataka koji jedinstveno identifikuju potpisnika odnosno pečatioca uključujući najmanje: (1) za potpisnika: - ime i prezime ili pseudonim , a ukoliko je upotrebljen pseudonim to mora biti jasno obeleženo u okviru kvalifikovanog elektronskog sertifikata; - JMBG, ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG; (2) za pečatioca: naziv, država i matični broj odnosno jedinstvena identifikaciona oznaka u skladu sa pravnom regulativom te države, ukoliko postoji; 4) podatke za proveru elektronskog potpisa odnosno	PU		

a)	a1)	b)	b1)	v)	g)	d)
			elektronskog pečata koji odgovaraju podacima za kreiranje tog elektronskog potpisa odnosno elektronskog pečata; 5) podatke o početku i kraju važenja kvalifikovanog elektronskog sertifikata; 6) serijski broj kvalifikovanog elektronskog sertifikata koji mora biti jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata; 7) napredni elektronski potpis ili napredni elektronski pečat izdavaoca kvalifikovanog elektronskog sertifikata; 8) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 7); 9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata; 10) oznaku da su podaci za kreiranje elektronskog potpisa odnosno pečata, koji odgovaraju podacima za proveru elektronskog potpisa odnosno pečata iz kvalifikovanog elektronskog sertifikata, sadržani u kvalifikovanom sredstvu za kreiranje elektronskog potpisa odnosno pečata, ukoliko je taj uslov ispunjen.			
38.3.	Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.	43.2.	Kvalifikovani elektronski sertifikati mogu uključivati dodatna obeležja pored obeležja iz stava 1. ovog člana.	PU		
38.4.	If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	44.4.	U slučaju opoziva kvalifikovani elektronski sertifikat trajno prestaje da važi od trenutka opoziva.	PU		
38.5.a	Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals: (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;	44.5.	U slučaju suspenzije kvalifikovani elektronski sertifikat gubi važnost tokom perioda trajanja suspenzije.	PU		
38.5.b.	(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of	44.7.	Podaci o suspenziji i periodu trajanja suspenzije kvalifikovanog elektronskog sertifikata upisuju se u bazu podataka izdatih sertifikata koju vodi izdavalac	PU		

a)	a1)	b)	b1)	v)	g)	d)
	suspension, from the service providing information on the status of the certificate.		kvalifikovanih elektronskih sertifikata i moraju biti vidljivi tokom trajanja suspenzije u okviru usluga kojima se pružaju informacije o statusu sertifikata.			
38.6.	The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredbom se daje ovlašćenje Evropskoj komisiji da donese akte za primenu na nivou EU. Ukazujemo da je članom 43. stav 3. ovog zakona predviđeno da Ministarstvo bliže propisuje uslove koje mora da ispunjavaju kvalifikovani elektronski sertifikati.	
39.1.	Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.	46.1.	Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata mora da, pomoću odgovarajućih tehničkih rešenja i postupaka, obezbedi: 1) poverljivost podataka za kreiranje elektronskog potpisa odnosno pečata; 2) da se podaci za kreiranje elektronskog potpisa odnosno pečata pojavljuju samo jednom; 3) da se podaci za kreiranje elektronskog potpisa odnosno pečata ne mogu dobiti izvan sredstva za kreiranje elektronskog potpisa odnosno pečata upotrebom dostupne tehnologije u razumnom vremenu; 4) da je elektronski potpis odnosno pečat pouzdano zaštićen od falsifikovanja upotrebom dostupne tehnologije; 5) mogućnost pouzdane zaštite podataka za kreiranje elektronskog potpisa odnosno pečata od neovlašćenog korišćenja. Sredstva za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata, prilikom kreiranja elektronskog potpisa odnosno pečata, ne smeju promeniti podatke koji se potpisuju odnosno pečatiraju ili onemogućiti potpisniku odnosno autoru pečata uvid u te podatke pre procesa kreiranja kvalifikovanog elektronskog potpisa odnosno pečata.	PU		

a)	a1)	b)	b1)	v)	g)	d)
		46.2. 46.3. 46.4. 46.5.	Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata korisnik kvalifikovane usluge od poverenja može koristiti putem usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata. Izuzetno od stava 1. ovog člana kvalifikovani pružalac usluga od poverenja iz stava 3. ovog člana može izraditi kopiju podataka za izradu elektronskog potpisa odnosno pečata u svrhu zaštite od gubitka podataka ukoliko su ispunjeni sledeći uslovi: 1) izrada i čuvanje kopija podataka za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata ne umanjuju propisani nivo zaštite tih podataka; 2) broj izrađenih kopija podataka za kreiranje elektronskog potpisa odnosno pečata nije veći nego što je to neophodno za obezbeđivanje kontinuiteta pružanja usluge. Ministarstvo bliže propisuje uslove koje mora da ispunjava sredstvo za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata tehničkim propisom.			

a)	a1)	b)	b1)	v)	g)	d)
39.2.	Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.	47.1. 47.2 46.5.	U skladu sa zakonom kojim se uređuju tehnički zahtevi za proizvode i ocenjivanje usaglašenosti Ministarstvo imenuje telo za ocenu usaglašenosti sredstava za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata sa tehničkim propisom iz člana 46. (u daljem tekstu: imenovano telo). Tehničkim propisom iz člana 46. se takođe bliže uređuju uslovi koje mora da ispunjava imenovano telo. Ministarstvo bliže propisuje uslove koje mora da ispunjava sredstvo za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata tehničkim propisom.	PU		
39.3.	Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.			NP	Odredba je neprenosiva, jer se odnosi na prijavljivanje informacija o sertifikovanim sredstvima za izdavanje kvalifikovanog elektronskog potpisa Evropskoj komisiji, kao i na ovlašćenje Evropske komisije da donosi akte za primenu na nivou EU. Ukazujemo da je članom 47. ovog zakona predviđeno da Ministarstvo vodi Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata na osnovu izveštaja koje dobija od imenovanih tela, kao i da se u taj	

a)	a1)	b)	b1)	v)	g)	d)
					registar upisuju i kvalifikovana sredstva za kreiranje elektronskog potpisa i elektronskog pečata sa spiska koji prema članu 31. Regulative koji objavljuje Evropska komisija.	
40.	Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	48.1.	Postupkom validacije se utvrđuje da elektronski potpis predstavlja ispravan kvalifikovani elektronski potpis kada su ispunjeni sledeći uslovi: 1) utvrđeno je da je sertifikat koji prati elektronski potpis u trenutku potpisivanja predstavljao kvalifikovani elektronski sertifikat; 2) utvrđeno je da je kvalifikovani elektronski sertifikat izdat od strane pružaoca usluge izdavanja kvalifikovanih sertifikata za elektronski potpis i važio je u trenutku potpisivanja; 3) utvrđeno je da podaci za validaciju elektronskog potpisa iz kvalifikovanog elektronskog sertifikata odgovaraju kombinaciji elektronskog potpisa i podataka koji su potpisani elektronskim potpisom; 4) pouzdajućoj strani je tačno prikazan skup podataka iz kvalifikovanog elektronskog sertifikata koji jedinstveno identifikuju potpisnika; 5) pouzdajućoj strani su tačno prikazani podaci koji su potpisani elektronskim potpisom; 6) korišćenje pseudonima je jasno naznačeno pouzdajućoj strani, u slučaju da je je prilikom elektronskog potpisivanja korišćen pseudonim; 7) utvrđeno je da je elektronski potpis kreiran korišćenjem kvalifikovanog sredstva za kreiranje elektronskog potpisa; 8) utvrđeno je da nije narušen integritet podataka koji su potpisani elektronskim potpisom; 9) utvrđeno je da elektronski potpis ispunjava uslove za napredni elektronski potpis iz ovog zakona. Sistem koji se koristi za validaciju kvalifikovanog elektronskog potpisa obezbeđuje tačan rezultat postupka validacije pouzdajućoj strani i omogućava joj identifikovanje bilo kog problema od značaja za	PU		

a)	a1)	b)	b1)	v)	g)	d)
			pouzdanost. Odredbe iz st. 1. i 2.. ovog člana shodno se primenjuju na elektronski pečat. Pružalac usluge kvalifikovane validacije kvalifikovanih elektronskih potpisa odnosno pečata obezbeđuje: 1) validaciju kvalifikovanog elektronskog potpisa odnosno pečata u skladu sa članom 48. ovog zakona; 2) da pouzdajuća strana koja koristi uslugu dobije rezultat postupka validacije elektronskim putem na automatizovan način koji je pouzdan i efikasan; 3) da je rezultat postupka validacije iz tačke 2) ovog stava pečatiran naprednim elektronskim pečatom ili potpisan naprednim elektronskim potpisom pružaoca usluge.			
		48.2.	Usluga kvalifikovanog elektronskog čuvanja dokumenata je kvalifikovana usluga od poverenja putem koje se pruža pouzdano elektronsko čuvanje dokumenata u skladu sa čl. 62. i 63. ovog zakona.			
		48.3.				
		49.1.				

a)	a1)	b)	b1)	v)	g)	d)
		65.1.				
41.1.	An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.	53.1.	Elektronskom vremenskom žigu ne može se osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovan vremenski žig.	PU		
41.2.	A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.	53.2.	Za kvalifikovani elektronski vremenski žig i podatke kojima je taj vremenski žig pridružen važi pravna pretpostavka tačnosti datuma i vremena iskazanog u vremenskom žigu i očuvanosti integriteta tih podataka u odnosu na taj vremenski trenutak.	PU		
41.3.	A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.			NP	Odredba se utvrđuje da je kvalifikovani vremenski žig izdat u jednoj državi članici EU važi u svim državama članicama EU, i njena primena je vezana isključivo za države članice EU, zbog čega je odredba neprenosiva.	
42.1.a.	A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;	52.1.1.	Kvalifikovani elektronski vremenski žig mora da zadovolji sledeće uslove: 1) da je povezan sa koordiniranim univerzalnim vremenom (UTC) tako da se sprečava svaka mogućnost promene podataka koja se ne može otkriti;	PU		
42.1.b.	(b) it is based on an accurate time source linked to Coordinated Universal Time; and	52.1.2.	2) da je zasnovan na preciznom vremenskom izvoru;	PU		

a)	a1)	b)	b1)	v)	g)	d)
42.1.c.	(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.	52.1.3. 52.1.4.	3) da je izdat od strane pružaoca usluge izdavanja kvalifikovanog vremenskog žiga; 4) da je potpisan odnosno pečatiran od strane pružaoca usluge izdavanja kvalifikovanog vremenskog žiga pomoću naprednog elektronskog potpisa ili naprednog elektronskog pečata.	PU		
42.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).		.	NP	Odredbom je dato ovlašćenje Evropskoj komisiji da svojim aktom bliže uredi standarde za vremenski žig. Ukazujemo da je članom 52. stav 2. ovog zakona predviđeno da Ministarstvo bliže propisuje uslove za kvalifikovane elektronske vremenske žigove.	
43.1.	Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.	58.1.	Podacima poslatim ili primljeni putem usluge elektronske dostave ne može se osporiti pravna snaga i dopuštenost kao dokaz u pravnom prometu samo iz razloga što su u elektronskoj formi ili iz razloga što ne ispunjavaju sve uslove usluge kvalifikovane elektronske dostave.	PU		
43.2.	Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.	58.2.	Za podatke iz elektronske poruke poslate ili primljene putem usluge kvalifikovane elektronske dostave važi pravna pretpostavka integriteta podataka, slanja podataka od naznačenog pošiljaoca, prijem od strane naznačenog primaoca, pouzdanosti datuma i vremena slanja ili primanja.	PU		
44.1.1.a	Qualified electronic registered delivery services shall meet the following requirements: (a) they are provided by one or more qualified trust service provider(s);	54.1.1.	Usluga kvalifikovane elektronske dostave mora da ispuni sledeće uslove: 1) da je pružana od strane jednog ili više pružaoca kvalifikovanih usluga od poverenja;	PU		

a)	a1)	b)	b1)	v)	g)	d)
44.1.1.b	(b) they ensure with a high level of confidence the identification of the sender;	54.1.2.	2) da uz visok nivo pouzdanosti obezbeđuje identifikaciju pošiljaoca;	PU		
44.1.1.c	(c) they ensure the identification of the addressee before the delivery of the data;	54.1.3.	3) da obezbeđuje identifikaciju primaoca prilikom dostave podataka;	PU		
44.1.1.d	(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;	54.1.4.	4) da se u procesu slanja i prijema elektronske poruke koristi napredni elektronski potpis ili napredni elektronski pečat pružaoca usluge kvalifikovane elektronske dostave u svrhu sprečavanja neprimećene promene podataka;	PU		
44.1.1.e	(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;	54.1.5.	5) da izmena podataka izvršena u svrhu slanja ili prijema podataka mora biti jasno naznačena pošiljaocu i primaocu;	PU		
44.1.1.f	(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.	54.1.6.	6) da vreme i datum slanja, prijema i eventualne izmene podataka moraju biti naznačeni kvalifikovanim elektronskim vremenskim žigom.	PU		
44.1.2.	In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.	54.1.7.	7) u slučaju da se podaci prenose između dva ili više pružalaca usluge kvalifikovane elektronske dostave uslovi iz ovog stava se primenjuju na svakog od njih.	PU		
44.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredbom se daje ovlašćenje Evropskoj komsiji da donosi akte kojim se bliže uređuje navedeno pitanje, zbog čega je odredba neprenosiva. Ukazujemo da je članom 55. stav 7. predviđeno da Ministarstvo bliže propisuje uslove za usluge kvalifikovane elektronske dostave.	
45.	Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.	60.	Kvalifikovani sertifikati za autentikaciju veb sajtova sadrže: 1) oznaku, koja se može prepoznati pri automatskoj obradi, da je sertifikat izdat kao kvalifikovani sertifikat za autentikaciju veb sajtova; 2) skup podataka koji nedvosmisleno predstavljaju pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova, što obavezno uključuje	PU		

a)	a1)	b)	b1)	v)	g)	d)
			državu sedišta, poslovno ime i matični broj tog pružaoca usluge; 3) ime i prezime ili pseudonim fizičkog lica kome je izdat sertifikat, odnosno poslovne ime i matični broj pravnog lica kome je izdat sertifikat; 4) adresu, odnosno sedište fizičkog ili pravnog lica kome je izdat sertifikat; 5) naziv internet domena fizičkog ili pravnog lica kome je izdat sertifikat; 6) podatke o početku i kraju roka važenja sertifikata; 7) identifikacionu oznaku sertifikata koja mora da bude jedinstvena za pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova; 8) napredan elektronski potpis ili napredan elektronski pečat pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova; 9) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 8); 10) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata			
45.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			NP	Odredbom se daje ovlašćenje Evropskoj komsiji da donosi akte kojim se bliže uređuje navedeno pitanje, zbog čega je odredba neprenosiva.	
46.	An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.	7.	Elektronskom dokumentu ne može se osporiti punovažnost ili dokazna snaga samo zato što je u elektronskom obliku.	PU		
47.1. 47.2.	The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.			NP	Odredba uređuje pitanje poveravanja nadležnosti Evropskoj komisiji za donošenje akata na osnovu predmetne uredbe.	

a)	a1)	b)	b1)	v)	g)	d)
47.3. 47.4. 47.5.	The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.					
48.	The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.			NP	Odredbom se uređuje obrazovanje komiteta koji obavlja poslove zajedno sa Evropskom komisijom u vezi sa sprovođenjem ove uredbe.	
49.1.	The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this			NP	Odredbom se uređuje da Evropska komisija ispituje primenu ove uredbe i izveštava Evropski parlament i Savet o	

a)	a1)	b)	b1)	v)	g)	d)
49.2. 49.3.	Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.				tome, zbog čega je ova odredba neprenosiva u propis Republike Srbije.	
50.1. 50.2.	Directive 1999/93/EC is repealed with effect from 1 July 2016. References to the repealed Directive shall be construed as references to this Regulation.			NP	Odredbom se predviđa prestanak važenja direktive EU, zbog čega je odredba neprenosiva.	
51.1.	Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.			NU	Dosadašnji propisi u ovoj oblasti nisu predviđali ocenu usaglašenosti sredstava za kreiranje elektronskog potpisa, usled čega se ova odredba nije mogla preneti.	
51.2.	Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.	73.3.	Danom stupanja na snagu ovog zakona sertifikaciona tela za izdavanje kvalifikovanih elektronskih sertifikata koja su registrovana na osnovu Zakon o elektronskom potpisu nastavljaju sa radom kao kvalifikovani pružaoci usluge izdavanje kvalifikovanih sertifikata za elektronski potpis.	PU		
51.3.	A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification- service-provider shall be considered as qualified trust service provider under this Regulation.	73.3.	Danom stupanja na snagu ovog zakona sertifikaciona tela za izdavanje kvalifikovanih elektronskih sertifikata koja su registrovana na osnovu Zakon o elektronskom potpisu nastavljaju sa radom kao kvalifikovani pružaoci usluge izdavanje kvalifikovanih sertifikata za elektronski potpis.	PU		

a)	a1)	b)	b1)	v)	g)	d)
51.4.	If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.	73.3.	Danom stupanja na snagu ovog zakona sertifikaciona tela za izdavanje kvalifikovanih elektronskih sertifikata koja su registrovana na osnovu Zakon o elektronskom potpisu nastavljaju sa radom kao kvalifikovani pružaoci usluge izdavanje kvalifikovanih sertifikata za elektronski potpis.	DU	Odredba samo nije usklađena u pogledu roka za dostavu izveštaja o oceni usaglašenosti. Pružaoci kvalifikovanih usluga od poverenja biti dužni da dostave predmetni izveštaj kada se donesu podzakonska akta za primenu ovog zakona.	
52.1. 52.2. 52.3.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. This Regulation shall apply from 1 July 2016, except for the following: (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014; (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8); (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.EN 28.8.2014 Official Journal of the European Union L 257/109 Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member			NP	Odredba predviđa stupanje na snagu ove uredbe, zbog čega je neprenosiva u domaći propis.	

a)	a1)	b)	b1)	v)	g)	d)
52.4. 52.5.	State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public. This Regulation shall be binding in its entirety and directly applicable in all Member States.					
aI.1.a	Qualified certificates for electronic signatures shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;	43.1.1.	Kvalifikovani elektronski sertifikat mora da sadrži: 1) oznaku, u formi pogodnoj za automatsku obradu, da se elektronski sertifikat koristi kao kvalifikovani sertifikat za elektronski potpis, odnosno pečat;	PU		
aI.1.b	(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name;	43.1.2.	2) skup podataka koji jedinstveno identifikuju kvalifikovanog pružaoca usluge od poverenja za izdavanje kvalifikovanog elektronskog sertifikata uključujući najmanje zemlju porekla pružaoca i naziv pružaoca;	PU		
aI.1.c	(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;	43.1.3.	3) skup podataka koji jedinstveno identifikuju potpisnika odnosno pečatioca uključujući najmanje: (1) za potpisnika: - ime i prezime ili pseudonim , a ukoliko je upotrebljen pseudonim to mora biti jasno obeleženo u okviru kvalifikovanog elektronskog sertifikata; - JMBG, ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG; (2) za pečatioca: naziv, država i matični broj odnosno jedinstvena identifikaciona oznaka u skladu sa pravnom regulativom te države, ukoliko postoji;	PU		
aI.1.d	(d) electronic signature validation data that corresponds to the electronic signature creation data;	43.1.4.	4) podatke za proveru elektronskog potpisa odnosno elektronskog pečata koji odgovaraju podacima za	PU		

a)	a1)	b)	b1)	v)	g)	d)
			kreiranje tog elektronskog potpisa odnosno elektronskog pečata;			
aI.1.e	(e) details of the beginning and end of the certificate's period of validity;	43.1.5.	5) podatke o početku i kraju važenja kvalifikovanog elektronskog sertifikata;	PU		
aI.1.f	(f) the certificate identity code, which must be unique for the qualified trust service provider;	43.1.6.	6) serijski broj kvalifikovanog elektronskog sertifikata koji mora biti jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata;	PU		
aI.1.g	(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	43.1.7.	7) napredni elektronski potpis ili napredni elektronski pečat izdavaoca kvalifikovanog elektronskog sertifikata;	PU		
aI.1.h	(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;	43.1.8.	8) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 7);	PU		
aI.1.i	(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;	43.1.9.	9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata;	PU		
aI.1.j	(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.	43.1.10.	10) oznaku da su podaci za kreiranje elektronskog potpisa odnosno pečata, koji odgovaraju podacima za proveru elektronskog potpisa odnosno pečata iz kvalifikovanog elektronskog sertifikata, sadržani u kvalifikovanom sredstvu za kreiranje elektronskog potpisa odnosno pečata, ukoliko je taj uslov ispunjen.	PU		
aII.1.a	Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;	46.1.1.	Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata mora da, pomoću odgovarajućih tehničkih rešenja i postupaka, obezbedi: 1) poverljivost podataka za kreiranje elektronskog potpisa odnosno pečata;	PU		
aII.1.b	(b) the electronic signature creation data used for electronic signature creation can practically occur only once;	46.1.2.	2) da se podaci za kreiranje elektronskog potpisa odnosno pečata pojavljuju samo jednom;	PU		
aII.1.c	(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;	46.1.3. 46.1.4.	3) da se podaci za kreiranje elektronskog potpisa odnosno pečata ne mogu dobiti izvan sredstva za kreiranje elektronskog potpisa odnosno pečata upotrebom dostupne tehnologije u razumnom vremenu; 4) da je elektronski potpis odnosno pečat pouzdano	PU		

a)	a1)	b)	b1)	v)	g)	d)
			zaštićen od falsifikovanja upotrebom dostupne tehnologije;			
aII.1.d	(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.	46.1.5.	5) mogućnost pouzdane zaštite podataka za kreiranje elektronskog potpisa odnosno pečata od neovlašćenog korišćenja.	PU		
aII.2	Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.	46.2.	Sredstva za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata, prilikom kreiranja elektronskog potpisa odnosno pečata, ne smeju promeniti podatke koji se potpisuju odnosno pečatiraju ili onemogućiti potpisniku odnosno autoru pečata uvid u te podatke pre procesa kreiranja kvalifikovanog elektronskog potpisa odnosno pečata.	PU		
aII.3	Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.	46.3.	Kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata korisnik kvalifikovane usluge od poverenja može koristiti putem usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata.	PU		
aII.4.a	Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: (a) the security of the duplicated datasets must be at the same level as for the original datasets;	46.4.1.	Izuzetno od stava 1. ovog člana kvalifikovani pružalac usluga od poverenja iz stava 3. ovog člana može izraditi kopiju podataka za izradu elektronskog potpisa odnosno pečata u svrhu zaštite od gubitka podataka ukoliko su ispunjeni sledeći uslovi: 1) izrada i čuvanje kopija podataka za kreiranje kvalifikovanog elektronskog potpisa odnosno pečata ne umanjuju propisani nivo zaštite tih podataka;	PU		
aII.4.b	(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.	46.4.2.	2) broj izrađenih kopija podataka za kreiranje elektronskog potpisa odnosno pečata nije veći nego što je to neophodno za obezbeđivanje kontinuiteta pružanja usluge.	PU		
aIII.1.a	Qualified certificates for electronic seals shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;	43.1.1.	Kvalifikovani elektronski sertifikat mora da sadrži: 1) oznaku, u formi pogodnoj za automatsku obradu, da se elektronski sertifikat koristi kao kvalifikovani sertifikat za elektronski potpis, odnosno pečat;	PU		
aIII.1.b	(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member	43.1.2.	2) skup podataka koji jedinstveno identifikuju kvalifikovanog pružaoca usluge od poverenja za izdavanje kvalifikovanog elektronskog sertifikata	PU		

a)	a1)	b)	b1)	v)	g)	d)
	State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name;		uključujući najmanje zemlju porekla pružaoca i naziv pružaoca;			
aIII.1.c	(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;	43.1.3.	3) skup podataka koji jedinstveno identifikuju potpisnika odnosno pečatioca uključujući najmanje: (1) za potpisnika: - ime i prezime ili pseudonim , a ukoliko je upotrebljen pseudonim to mora biti jasno obeleženo u okviru kvalifikovanog elektronskog sertifikata; - JMBG, ukoliko je u zahtevu za izdavanje sertifikata potpisnik zahtevao da sertifikat sadrži JMBG; (2) za pečatioca: naziv, država i matični broj odnosno jedinstvena identifikaciona oznaka u skladu sa pravnom regulativom te države, ukoliko postoji;	PU		
aIII.1.d	(d) electronic seal validation data, which corresponds to the electronic seal creation data;	43.1.4.	4) podatke za proveru elektronskog potpisa odnosno elektronskog pečata koji odgovaraju podacima za kreiranje tog elektronskog potpisa odnosno elektronskog pečata;	PU		
aIII.1.e	(e) details of the beginning and end of the certificate's period of validity;	43.1.5.	5) podatke o početku i kraju važenja kvalifikovanog elektronskog sertifikata;	PU		
aIII.1.f	(f) the certificate identity code, which must be unique for the qualified trust service provider;	43.1.6.	6) serijski broj kvalifikovanog elektronskog sertifikata koji mora biti jedinstven u okviru izdavaoca kvalifikovanog elektronskog sertifikata;	PU		
aIII.1.g	(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	43.1.7.	7) napredni elektronski potpis ili napredni elektronski pečat izdavaoca kvalifikovanog elektronskog sertifikata;	PU		
aIII.1.h	(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;	43.1.8.	8) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 7);	PU		
aIII.1.i	(i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;	43.1.9.	9) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata;	PU		
aIII.1.j	(j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form	43.1.10.	10) oznaku da su podaci za kreiranje elektronskog potpisa odnosno pečata, koji odgovaraju podacima za proveru elektronskog potpisa odnosno pečata iz kvalifikovanog elektronskog sertifikata, sadržani u	PU		

a)	a1)	b)	b1)	v)	g)	d)
	suitable for automated processing.		kvalifikovanom sredstvu za kreiranje elektronskog potpisa odnosno pečata, ukoliko je taj uslov ispunjen.			
aIV.1.a	Qualified certificates for website authentication shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;	60.1.1.	Kvalifikovani sertifikati za autentikaciju veb sajtova sadrže: 1) oznaku, koja se može prepoznati pri automatskoj obradi, da je sertifikat izdat kao kvalifikovani sertifikat za autentikaciju veb sajtova;	PU		
aIV.1.b	(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name;	60.1.2.	2) skup podataka koji nedvosmisleno predstavljaju pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova, što obavezno uključuje državu sedišta, poslovno ime i matični broj tog pružaoca usluge;	PU		
aIV.1.c	(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; or legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;	60.1.3.	3) ime i prezime ili pseudonim fizičkog lica kome je izdat sertifikat, odnosno poslovne ime i matični broj pravnog lica kome je izdat sertifikat;	PU		
aIV.1.d	(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;	60.1.4.	4) adresu, odnosno sedište fizičkog ili pravnog lica kome je izdat sertifikat;	PU		
aIV.1.e	(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;	60.1.5.	5) naziv internet domena fizičkog ili pravnog lica kome je izdat sertifikat;	PU		
aIV.1.f	(f) details of the beginning and end of the certificate's period of validity;	60.1.6.	6) podatke o početku i kraju roka važenja sertifikata;	PU		
aIV.1.g	(g) the certificate identity code, which must be unique for the qualified trust service provider;	60.1.7.	7) identifikacionu oznaku sertifikata koja mora da bude jedinstvena za pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova;	PU		
aIV.1.h	(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	60.1.8.	8) napredan elektronski potpis ili napredan elektronski pečat pružaoca usluge izdavanja kvalifikovanih sertifikata za autentikaciju veb sajtova;	PU		

a)	a1)	b)	b1)	v)	g)	d)
aIV.1.i	(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;	60.1.9.	9) lokaciju na kojoj je, bez naknade, dostupan sertifikat naprednog elektronskog potpisa odnosno naprednog elektronskog pečata iz tačke 8);	PU		
aIV.1.j	(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.	60.1.10	10) lokaciju usluge putem koje se proverava status validnosti kvalifikovanog elektronskog sertifikata	PU		