

ЗАКОН

О ЕЛЕКТРОНСКОМ ДОКУМЕНТУ, ЕЛЕКТРОНСКОЈ ИДЕНТИФИКАЦИЈИ И УСЛУГАМА
ОД ПОВЕРЕЊА У ЕЛЕКТРОНСКОМ ПОСЛОВАЊУ

I. УВОДНЕ ОДРЕДБЕ

Предмет

Члан 1.

Овим законом уређују се електронски документ, електронска идентификација и услуге од поверења у електронском пословању.

Значење појединих израза

Члан 2.

Поједини изрази, у смислу овог закона, имају следеће значење:

- 1) електронско пословање је употреба података у електронском облику, средстава електронске комуникације и електронске обраде података у обављању послова физичких и правних лица;
- 2) електронски облик података је дигитални запис података погодан за електронску обраду и пренос путем средстава електронске комуникације;
- 3) електронска трансакција је пословна активност између две или више страна која се обавља електронским путем;
- 4) електронски документ је скуп података састављен од слова, бројева, симбола, графичких, звучних и видео материјала, у електронском облику;
- 5) производ је хардвер, софтвер односно хардвер са припадајућим софтвером, или њихове одговарајуће компоненте, намењен електронској обради, електронском преносу односно чувању података који омогућава пружање услуга електронске идентификације и услуга од поверења;
- 6) интероперабилност је способност два или више система или њихових компоненти да размењују податке и омогуће заједничку употребу података и знања;
- 7) орган јавне власти је државни орган и организација, орган и организација аутономне покрајине, орган и организација јединице локалне самоуправе, јавно предузеће, установа, посебни орган преко кога се остварује регулаторна функција и правно и физичко лице коме је поверено јавно овлашћење;
- 8) физичко лице у својству регистрованог субјекта је физичко лице које је регистровано за обављање одређене делатности у складу са законом;
- 9) корисник је правно или физичко лице, физичко лице у својству регистрованог субјекта, као и њихов заступник, који користи услуге од поверења или средства електронске идентификације у складу са овим законом;
- 10) аутентификација је процес који обезбеђује потврду електронске идентификације правног лица, физичког лица, или физичког лица у својству регистрованог субјекта, или потврду интегритета и порекла података у електронској форми;
- 11) идентификациони подаци представљају скуп података на основу којих је могуће недвосмислено утврдити идентитет правног лица, физичког лица, или физичког лица у својству регистрованог субјекта, као и њиховог заступника;
- 12) електронска идентификација је поступак коришћења идентификационих података у електронском облику који недвосмислено одређују правно лице, физичко лице, или физичко лице у својству регистрованог субјекта, као и њиховог заступника;
- 13) средство електронске идентификације је материјално, односно нематеријално средство које садржи идентификационе податке и којим се врши аутентификација лица;

14) шема електронске идентификације је систем издавања средства електронске идентификације правном лицу, физичком лицу или физичком лицу у својству регистрованог субјекта;

15) услуга електронске идентификације је услуга која омогућава коришћење одређене шеме електронске идентификације у електронским трансакцијама при чему се у оквиру те услуге пружају гаранције да идентификациони подаци из средства електронске идентификације одговарају лицу коме је средство издато;

16) чвор (енг. node) представља тачка приступа инфраструктури електронске идентификације (у даљем тексту: чвор) је место прикључења националној инфраструктури електронске идентификације путем које се омогућава прекогранична аутентификација лица, која има функцију препознавања и обраде, односно интероперабилни пренос идентификационих података у друге, као и из других држава;

17) услуга од поверења је електронска услуга која олакшава пословну активност између две или више страна којом пружалац услуге странама гарантује веродостојност података, а која је као таква одређена овим законом;

18) пружалац услуга од поверења је правно лице, или физичко лице у својству регистрованог субјекта које пружа једну или више услуга од поверења;

19) поуздајућа страна је правно или физичко лице које, се поуздаје у услугу електронске идентификације, дигитални идентификациони новчаник или друго средство електронске идентификације, односно услугу од поверења;

20) квалификована услуга од поверења је услуга од поверења која испуњава услове утврђене овим законом за квалификовану услугу од поверења;

21) пружалац квалификоване услуге од поверења је правно лице, или физичко лице у својству регистрованог субјекта које пружа једну или више квалификованих услуга од поверења, у складу са овим законом;

22) електронски потпис је скуп података у електронском облику који су придружени или логички повезани са другим подацима у електронском облику, а које потписник користи за потписивање;

23) електронски печат је скуп података у електронском облику који су придружени или логички повезани са другим подацима у електронском облику, а које печатац користи за печатање;

24) подаци за креирање електронског потписа односно печата су јединствени подаци које користи потписник односно печатац за креирање електронског потписа односно печата и који су логички повезани са одговарајућим подацима за валидацију електронског потписа односно печата;

25) подаци за валидацију електронског потписа односно печата су подаци који се користе за валидацију, односно проверу и потврђивање исправности електронског потписа, односно печата;

26) сертификат за електронски потпис је електронска потврда којом се потврђује веза између података за валидацију електронског потписа и идентитета потписника, потврђујући најмање лично име или псеудоним потписника;

27) сертификат за електронски печат је електронска потврда којом се потврђује веза између података за валидацију електронског печата и правног лица чији је печат;

28) потписник је физичко лице које је креирало електронски потпис и чији су идентификациони подаци садржани у сертификату на основу кога је креиран тај електронски потпис, то јест сертификату којим се потврђује веза између идентитета тог потписника и података за валидацију електронског потписа;

29) печатац је правно лице, физичко лице у својству регистрованог субјекта, физичко лице коме је поверено вршење јавних овлашћења или физичко лице које у обављању делатности у складу са посебним прописима има право на коришћење печата (нпр. лица која имају лиценцу за вршење послова или обављање делатности), за чије потребе се креира електронски печат и чији су идентификациони подаци наведени у сертификату на основу кога је креиран тај електронски печат, односно у сертификату којим се потврђује веза између идентитета тог печатноца и података за валидацију електронског печата;

30) средство за креирање електронског потписа, односно печата је техничко средство (софтвер, односно хардвер) које се користи за креирање електронског потписа, односно печата уз коришћење података за креирање електронског потписа односно печата;

31) квалификовано средство за креирање електронског потписа на даљину је квалификовано средство за креирање електронског потписа којим у име потписника управља пружалац квалификованих услуга од поверења у складу са овим законом;

32) квалификовано средство за креирање електронског печата на даљину је квалификовано средство за креирање електронског печата којим у име печатиоца управља пружалац квалификованих услуга од поверења у складу са овим законом;

33) валидација је поступак провере и потврђивања исправности података у електронском облику у складу са овим законом;

34) напредни електронски потпис је електронски потпис који испуњава додатне услове за обезбеђивање вишег нивоа поузданости потврђивања интегритета података и идентитета потписника у складу са овим законом;

35) квалификовани електронски потпис је напредни електронски потпис који је креиран квалификованим средством за креирање електронског потписа и који се заснива на квалификованом сертификату за електронски потпис и који је издат од стране пружаоца квалификоване услуге од поверења у складу са овим законом;

36) квалификовано средство за креирање електронског потписа је средство које испуњава услове прописане овим законом;

37) квалификовани сертификат за електронски потпис је сертификат за електронски потпис који издаје пружалац квалификоване услуге од поверења и који испуњава услове предвиђене овим законом;

38) напредни електронски печат је електронски печат који испуњава додатне услове за обезбеђивање вишег нивоа поузданости потврђивања интегритета података и идентитета печатиоца у складу са овим законом;

39) квалификовани електронски печат је напредни електронски печат који је креиран квалификованим средством за креирање електронског печата и који је заснован на квалификованом сертификату за електронски печат;

40) квалификовано средство за креирање електронског печата је средство које испуњава услове прописане овим законом;

41) квалификовани сертификат за електронски печат је сертификат за електронски печат који издаје пружалац квалификоване услуге од поверења и који испуњава услове предвиђене овим законом;

42) услуга управљања квалификованим средством за креирање електронског потписа на даљину је услуга израде квалификованог електронског потписа на даљину путем средства за креирање електронског потписа којим у име потписника управља пружалац квалификоване услуге од поверења и гарантује да се подаци за израду електронског потписа користе под искључивом контролом потписника, у складу са овим законом;

43) услуга управљања квалификованим средством за креирање електронског печата на даљину је услуга израде квалификованог електронског печата на даљину путем средства за креирање електронског печата којим у име печатиоца управља пружалац квалификоване услуге од поверења и гарантује да се подаци за израду електронског печата користе под искључивом контролом печатиоца, у складу са овим законом;

44) сертификат за аутентификацију веб сајта је потврда помоћу које је могуће извршити аутентификацију веб сајта и којом се веб сајт повезује са идентитетом физичког или правног лица коме је сертификат издат;

45) квалификовани сертификат за аутентификацију веб сајта је сертификат за аутентификацију веб сајта коју издаје пружалац квалификоване услуге од поверења и испуњава услове предвиђене овим законом;

46) електронски временски жиг је време придружено подацима у електронском облику којим се потврђује да су ти подаци постојали у том временском тренутку;

47) квалификовани електронски временски жиг је електронски временски жиг који испуњава услове утврђене овим законом;

48) услуга електронске доставе је услуга преноса података електронским путем у оквиру које пружалац услуге обезбеђује доказе о поступању са пренесеним подацима, укључујући доказ слања и пријема података, којом се пренесени подаци штите од ризика губитка, крађе, оштећења односно било којих неовлашћених промена;

49) услуга квалификоване електронске доставе је услуга пружаоца квалификоване услуге од поверења која испуњава услове за квалификовану електронску доставу утврђене овим законом;

50) конверзија је превођење документа из једног облика у други тако да је очуван садржај документа;

51) дигитализација је конверзија документа из облика који није електронски у електронски облик;

52) дигитализовани документ је документ који је настао дигитализацијом изворног документа;

53) тело за оцењивање усаглашености је правно лице или део правног лица које је овлашћено да обавља послове оцењивања усаглашености пружаоца квалификоване услуге од поверења и квалификоване услуге од поверења коју он пружа са условима за пружање квалификованих услуга од поверења, као и оцењивање усаглашености дигиталног идентификационог новчаника или другог средстава електронске идентификације, у складу са овим законом и законом којим се уређују технички захтеви за производе и оцењивање усаглашености, односно поступак акредитације и примену релевантних стандарда;

54) дигитални идентификациони новчаник је средство електронске идентификације које омогућава кориснику да на безбедан начин чува, управља и валидира личне идентификационе податке и електронске потврде атрибута, са циљем да их приказује поуздајућим странама и другим корисницима дигиталног идентификационог новчаника, као и да омогући корисницима употребу квалификованог електронског потписа, односно печата;

55) атрибут је својство, карактеристика, квалитет, право или овлашћење физичког или правног лица, као и својство, односно карактеристика материјалног или нематеријалног објекта, односно ствари;

56) електронска потврда атрибута је потврда у електронском облику којом се на поуздан начин омогућава аутентификација атрибута;

57) квалификована електронска потврда атрибута је електронска потврда атрибута коју издаје пружалац квалификоване услуге од поверења, а која испуњава услове утврђене овим законом;

58) електронска потврда атрибута органа јавне власти је електронска потврда издата од стране или у име органа јавне власти надлежног за вођење или управљање евиденцијом, односно регистром који је извор података о атрибутима, у складу са законом;

59) извор података о атрибутима је евиденција, односно регистар и други аутентичан извор који садржи податке о атрибутима физичког или правног лица, односно објекта и који је одређен као извор тих података;

60) услуга чувања квалификованог електронског потписа, односно квалификованог електронског печата је услуга коју врши пружалац квалификоване услуге од поверења и која испуњава услове утврђене овим законом.

61) услуга електронског архивирања је услуга која обезбеђује пријем, складиштење, претрагу и брисање електронских података и електронских докумената у циљу обезбеђења њихове трајности и употребљивости, као и очувања њиховог интегритета, поверљивости и доказа о пореклу током читавог периода чувања.

62) квалификовано електронско архивирање је услуга електронског архивирања коју врши пружалац квалификоване услуге од поверења и која испуњава услове утврђене овим законом;

63) аутентификација вишег нивоа поузданости корисника је аутентификација заснована на употреби најмање два фактора аутентификације из различитих категорија који означавају нешто што само корисник зна, поседује или што корисник јесте, а који су међусобно независни, тако да компромитовање једног фактора не угрожава поузданост осталих, и која је креирана тако да штити поверљивост података за аутентификацију;

64) услуга вођења електронске евиденције означава бележење низа електронских записа података, којима се обезбеђује интегритет тих записа и тачност хронолошког редоследа бележења тих записа;

65) квалификована услуга вођења електронске евиденције је услуга пружаоца квалификоване услуге од поверења која испуњава услове утврђене овим законом;

66) податак о личности је сваки податак у смислу закона којим се уређује заштита података о личности;

67) упаривање идентитета је процес у којем се подаци за идентификацију лица или средства за електронску идентификацију упоређују или повезују са постојећим налогом који припада том лицу;

68) запис података су подаци у електронском облику који су забележени са повезаним метаподацима који подржавају обраду тих података, у смислу овог закона;

69) режим „ван мреже” омогућава коришћење дигиталног идентификационог новчаника без потребе за повезивањем са удаљеним системима преко електронских комуникационих мрежа, при чему се интеракција између корисника и треће стране на физичкој локацији врши уз употребу технологија кратког домета.

Сви појмови који се користе у овом закону у мушком роду, обухватају исте појмове у женском роду.

Примена

Члан 3.

Пружалац услуга од поверења пружа услуге од поверења у складу са овим законом.

Одредбе овог закона не примењују се на услуге од поверења које се пружају искључиво у оквиру затвореног система, односно ограниченог круга учесника, који може бити одређен споразумом, интерним актом или прописом, и које немају утицај на треће стране, односно не обавезују трећа лица ван тог система.

Обрада и заштита података

Члан 4.

Пружалац услуга од поверења односно услуге електронске идентификације приликом обраде података о личности поступа у складу са законом којим се уређује заштита података о личности, нарочито поштујући начело минимизације.

Сврха обраде података при пружању услуга из става 1. овог члана је идентификација лица коришћењем средства електронске идентификације, као и пружање услуга од поверења физичким и правним лицима при електронском пословању.

Подаци који се обрађују при електронској идентификацији, као и пружању услуга од поверења прописаних овим законом чувају се највише десет година од тренутка идентификације, односно пружања услуге од поверења, осим ако посебним законом није другачије уређено.

Подаци о личности који се воде у електронској евиденцији, односно регистру, чувају се у складу са законом којим се утврђује та евиденција, односно онолико дуго колико је руковалац одредио, а која одговара сврси обраде.

Подаци садржани у електронском потпису на документу чувају се у складу са прописима којима се уређује рок чувања тог документа.

У оквиру електронске трансакције стране се могу представљати псеудонимом ако прописом, уговором или на други обавезујући начин није другачије одређено.

Пристанак на идентификацију и аутентификацију

Члан 5.

Поступак електронске идентификације и аутентификације може бити покренут само на захтев правног или физичког лица које је предмет идентификације, осим ако је прописом другачије одређено.

Доступност и приступ особама са инвалидитетом

Члан 6.

Услуге од поверења, услуге електронске идентификације и производи који се користе за пружање тих услуга једнако су доступни и особама с инвалидитетом.

II. ЕЛЕКТРОНСКИ ДОКУМЕНТ

Пуноважност и доказна снага електронског документа

Члан 7.

Електронском документу не може се оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику.

Израда електронског документа

Члан 8.

Електронски документ се израђује применом једне од доступних и употребљивих информационо-комуникационих технологија, ако законом није другачије одређено.

Електронски документ који представља архивску грађу израђује се у форми која задовољава услове прописане овим законом за поуздану припрему за електронско чување.

Форма приказа електронског документа

Члан 9.

Електронски документ садржи унутрашњу и спољну форму приказа.

Унутрашња форма приказа састоји се од техничко-програмске форме записивања садржине електронског документа.

Спољна форма приказа састоји се од визуелног или другог разумљивог приказа садржине електронског документа.

Ако документ садржи електронски потпис или електронски печат, та чињеница треба да буде јасно исказана у спољној форми електронског документа.

Уколико електронски документ садржи електронски потпис или печат физичког лица или овлашћеног лица правног субјекта, свака друга форма потписа или печата истог физичког лица или овлашћеног лица правног субјекта је излишна.

Оригинал и копија

Члан 10.

Електронски документ који је изворно настао у електронском облику сматра се оригиналом.

Електронски документ који има истоветан дигитални запис оригиналном електронском документу сматра се оригиналом.

Копија електронског документа на папиру израђује се штампањем спољне форме електронског документа.

Електронски документ који је настао дигитализацијом изворног документа чија форма није електронска, сматра се копијом изворног документа.

Овера дигитализованог акта

Члан 11.

Акт који је дигитализован има исту доказну снагу као оригинални акт ако су кумулативно испуњени следећи услови и то:

1) да је дигитализација акта обављена на један од следећих начина, односно под надзором:

(1) физичког односно овлашћеног лица физичког лица у својству регистрованог субјекта или овлашћеног лица правног лица чији је то акт, или

(2) лица које је овлашћено за оверу потписа, рукописа и преписа у складу са законом који уређује оверу потписа, рукописа и преписа, или

(3) лица које је посебним законом овлашћено за оверу дигитализованог акта;

2) да је истоветност дигитализованог акта са оригиналом потврђена квалификованим електронским печатом или квалификованим електронским потписом лица из подтач. (1)–(3) овог става или лица на кога су пренете надлежности на основу којих је акт донет.

Овлашћено лице органа јавне власти може у поступцима који се спроводе у вршењу јавних овлашћења дигитализовати акт и оверити дигитализовани акт квалификованим електронским печатом органа или својим квалификованим електронским потписом, чиме се потврђује истоветност дигитализованог акта са оригиналном исправом.

Дигитализовани акт који је оверен од стране органа из става 2. овог члана има исту доказну снагу као оригинал у оквиру спровођења тог поступка.

Овера одштампаног примерка електронског документа

Члан 12.

Одштампани примерак електронског документа има исту доказну снагу као оригинални акт, ако су кумулативно испуњени следећи услови и то:

1) да је штампање електронског документа извршено под надзором:

(1) физичког лица, овлашћеног лица физичког лица у својству регистрованог субјекта, односно овлашћеног лица правног лица чији је то акт, или

(2) лица које је овлашћено за оверу потписа, рукописа и преписа у складу са законом који уређује оверу потписа, рукописа и преписа;

2) да је истоветност одштампаног примерка електронског документа са оригиналом потврђена, уз назнаку да је реч о одштампаном примерку електронског документа:

(1) својеручним потписом физичког лица, или

(2) својеручним потписом овлашћеног лица физичког лица у својству регистрованог субјекта, односно овлашћеног лица правног лица, као и печатом физичког лица у својству регистрованог субјекта, односно правног лица, ако постоји законска обавеза да акт садржи печат, или

(3) од стране лица које је овлашћено за оверу потписа, рукописа и преписа у складу са законом који уређује оверу потписа, рукописа и преписа.

Овлашћено лице органа јавне власти може у поступцима који се спроводе у вршењу јавних овлашћења одштампати електронски документ на папиру и оверити одштампани примерак електронског документа на начин из става 1. тачка 2) подтачка (2) овог члана, при чему одштампани примерак електронског документа обавезно садржи печат утврђен законом којим се уређује печат државних и других органа.

Одштампани примерак електронског документа који је оверен од стране органа из става 2. овог члана има исту доказну снагу као оригинал у оквиру спровођења тог поступка.

Потврда о пријему електронског документа

Члан 13.

Потврда о пријему електронског документа је доказ да је тај документ примљен од стране примаоца.

Потврду о пријему електронског документа издаје прималац електронског документа или пружалац услуге електронске доставе.

Обавеза издавања потврде о пријему електронског документа и елементи садржаја потврде уређују се прописима или вољом странака, ако законом није другачије одређено.

Дуплирање електронских докумената

Члан 14.

Сваки примљени електронски документ сматра се посебним документом, осим ако је више пута примљен истоветан документ и прималац је знао или је морао знати да је реч о истоветном документу.

III. ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

1. Дигитални идентификациони новчаник

Својства дигиталног идентификационог новчаника

Члан 15.

Дигитални идентификациони новчаник омогућава кориснику да на једноставан и транспарентан начин:

1) под искључивом контролом корисника, на безбедан начин захтева, добија, бира, комбинује, чува, брише, дели и представља личне идентификационе податке, и када је то потребно, у комбинацији са електронском потврдом атрибута, да се аутентификује поуздајућим странама, у режиму рада на мрежи и када је то прикладно, у режиму рада ван мреже, ради приступања јавним и приватним услугама, уз могућност селективног откривања података;

2) креира псеудониме и чува их у криптованом облику, локално, на свом уређају, у оквиру дигиталног идентификационог новчаника;

3) безбедно изврши аутентификацију дигиталног идентификационог новчаника другог лица, прима и дели личне идентификационе податке и електронске потврде атрибута, на сигуран начин, између два дигитална идентификациона новчаника;

4) приступи евиденцији свих трансакција извршених употребом дигиталног идентификационог новчаника, коришћењем контролне табле дигиталног идентификационог новчаника, која кориснику омогућава да:

(1) прегледа ажуран попис поуздајућих страна са којима је посредством дигиталног идентификационог новчаника остварио конекцију, а где је то могуће и све размењене податке;

(2) на једноставан начин захтева да поуздајућа страна обрише његове податке о личности у складу са законом којим се уређује заштита података о личности;

(3) на једноставан начин пријави поуздајућу страну органу надлежном за заштиту података о личности, ако посумња да је примио незаконит или сумњив захтев за подацима;

5) врши потписивање коришћењем квалификованог електронског потписа, односно печатање коришћењем квалификованог електронског печата;

6) преузме, у мери у којој је то технички изводљиво, податке корисника, електронске потврде атрибута и конфигурације;

7) остварује право корисника на преносивост података.

Дигитални идентификациони новчаник посебно треба да:

1) подржава опште протоколе и интерфејсе:

(1) за издавање личних идентификационих података, квалификованих и неквалификованих електронских потврда атрибута, или квалификованих и неквалификованих електронских сертификата дигиталном идентификационом новчанику;

(2) како би се поуздајућој страни омогућило да захтева и потврђује валидност личних идентификационих података и електронских потврда атрибута;

(3) за дељење и приказивање поуздајућој страни личних идентификационих података, електронских потврда атрибута, или селективно откривених података, у режиму рада на мрежи и када је то прикладно, у режиму рада ван мреже;

(4) омогући безбедно укључивање корисника, употребом средстава електронске идентификације високог нивоа поузданости, у складу са овим законом;

(5) за комуникацију дигиталних идентификационих новчаника два корисника, у сврху безбедног преузимања, валидације и размене личних идентификационих података и електронских потврда атрибута;

(6) за аутентификацију и идентификацију поуздајућих страна, кроз успостављање аутентификационих механизма утврђених овим законом;

(7) како би се поуздајућим странама омогућила провера аутентичности и валидности дигиталних идентификационих новчаника;

(8) како би се од поуздајуће стране могло захтевати брисање личних идентификационих података, у складу са законом којим се уређује заштита података о личности;

(9) за пријаву поуздајуће стране органу надлежном за заштиту података о личности, у случају сумње да је примљен незаконит или сумњив захтев за подацима;

(10) за креирање квалификованог електронског потписа, односно печата, употребом квалификованог средства за креирање електронског потписа, односно печата;

2) пружаоцима услуга од поверења који издају електронске потврде атрибута не пружа информације о употреби тих потврда коришћењем дигиталног идентификационог новчаника;

3) обезбеђује аутентификацију и идентификацију поуздајућих страна, кроз успостављање аутентификационих механизма утврђених овим законом;

4) испуњава услове прописане чланом 17. овог закона за шеме високог нивоа поузданости, нарочито када је реч о доказивању поузданости идентитета и управљању средствима електронске идентификације и њихове аутентификације;

5) у случају електронске потврде атрибута са уграђеним политикама откривања, примењује одговарајући механизам обавештавања корисника да поуздајућа страна или корисник дигиталног идентификационог новчаника, који су поднели захтев за ту електронску потврду атрибута имају овлашћења за приступ тој потврди;

6) обезбеђује да лични идентификациони подаци који су садржани у средству електронске идентификације посредством које је дигитални идентификациони новчаник обезбеђен, јединствено представљају физичко или правно лице, односно физичко лице у својству регистрованог субјекта, као и њиховог заступника;

7) омогућава свим физичким лицима бесплатно коришћење квалификованог електронског потписа.

Корисник дигиталног идентификационог новчаника има потпуну контролу над његовим коришћењем и коришћењем података у оквиру њега.

Издавање, коришћење и опозив дигиталног идентификационог новчаника

Члан 16.

Дигитални идентификациони новчаник издаје орган државне управе надлежан за пројектовање, усклађивање, развој и функционисање система електронске управе (у даљем тексту: канцеларија), као средство електронске идентификације, коришћењем шеме електронске идентификације високог нивоа поузданости.

Канцеларија обезбеђује интероперабилност и коришћење дигиталног идентификационог новчаника у складу са условима за издавање средства електронске идентификације утврђених овим законом.

Подаци о личности на основу којих се користи дигитални идентификациони новчаник чувају се логички одвојено од свих других података које чува пружалац услуге од поверења.

Издавање, коришћење и опозив дигиталног идентификационог новчаника, као и механизме за валидацију података садржаних у дигиталном идентификационом новчанику врши се без накнаде.

Канцеларија може опозвати дигитални идентификациони новчаник:

- 1) на изричит захтев корисника;
- 2) ако је угрожена сигурност дигиталног идентификационог новчаника;
- 3) након смрти корисника или престанка обављања делатности правног лица, односно физичког лица у својству регистрованог субјекта.

Дигитални идентификациони новчаник израђује се у складу са домаћим и међународним стандардима информационе безбедности.

Канцеларија омогућава корисницима да на једноставан начин могу пријавити техничке проблеме или друге инциденте који негативно утичу на коришћење Дигиталног идентификационог новчаника и пружа им техничку подршку у њиховом отклањању.

Канцеларија обезбеђује техничке мере које пружаоцима електронских потврда атрибута као и другој страни, након издавања електронске потврде атрибута, онемогућава праћење, повезивање или корелацију трансакција или понашања корисника.

Канцеларија без одлагања обавештава све кориснике дигиталног идентификационог новчаника о сваком безбедносном инциденту који би могао компромитовати или угрозити дигитални идентификациони новчаник или податке садржане у њему, нарочито ако је дошло до опозива или суспензије дигиталног идентификационог новчаника у складу са одредбама овог закона.

Физичким и правним лицима који не користе дигитални идентификациони новчаник не сме се ограничити нити отежати приступ услугама, тржишту рада и слобода предузетништва.

Влада, на предлог министарства надлежног за послове информационог друштва (у даљем тексту: Министарство), уређује ближе услове за издавање, коришћење и опозив дигиталног идентификационог новчаника.

Регистрација поуздајуће стране за коришћење дигиталног идентификационог новчаника

Члан 17.

Поуздајућа страна која намерава да користи дигитални идентификациони новчаник за пружање услуга својим корисницима, дужна је да се за такву врсту услуге региструје у јавном регистру поуздајућих страна који успоставља и води Канцеларија.

Приликом регистрације, поуздајућа страна дужна је да приложи:

- 1) податке неопходне за аутентификацију, и то: пословно име и седиште, матични број, порески идентификациони број;
- 2) идентификационе податке овлашћеног лица, и то: име и презиме, јединствен матични број и адресу електронске поште;
- 3) начин и сврху коришћења дигиталног идентификационог новчаника укључујући податке који ће се у пружању услуге захтевати од корисника.

Поуздајућа страна без одлагања пријављује Канцеларији сваку промену података из става 2. овог члана.

Поуздајућа страна приликом пружања услуга не сме тражити друге податке од корисника садржаних у дигиталном идентификационом новчанику осим оних које је приликом регистрације пријавила, у складу са ставом 2. тачка 3. овог члана.

Канцеларија у оквиру дигиталног идентификационог новчаника обезбеђује механизам за аутентификацију поуздајуће стране приликом коришћења личних идентификационих података и електронских потврда атрибута.

Поуздајућа страна одговорна је за спровођење поступка аутентификације и валидације личних идентификационих података, као и електронске потврде атрибута које преузима из дигиталног идентификационог новчаника корисника.

Поуздајућа страна прихвата коришћење псеудонима ако приликом пружања услуга није неопходна идентификација корисника.

Посредник који реализује услугу у име поуздајуће стране има исте обавезе као и поуздајућа страна и не сме чувати податке о садржају трансакције.

Министарство прописује садржај и начин вођења регистра из става 1. овог члана, начин подношења захтева за упис у регистар, садржину и форму захтева, потребну документацију и начин објављивања података из регистра.

Сертификација дигиталног идентификационог новчаника

Члан 18.

Оцену усаглашености дигиталног идентификационог новчаника и средстава електронске идентификације у оквиру којег се они стављају на располагање, са условима прописаних у чл. 15. и 16. Овог закона, врши тело за оцењивање усаглашености које је акредитовано у складу са законом којим се уређује поступак акредитације.

При оцени усаглашености дигиталног идентификационог новчаника, проверава се усаглашеност са техничким и безбедносним стандардима.

Сертификација из става 1. овог члана важи пет година, уз спровођење процене рањивости на сваке две године.

Ако се приликом процене утврди рањивост сертификација се поништава.

Листу акредитованих тела за оцену усаглашености из става 1. овог члана утврђује Министарство.

Министарство прописује ближе услове за оцену усаглашености из ст. 1. и 2. овог члана.

Безбедносни инциденти у вези са дигиталним новчаником

Члан 19.

Ако се утврди неправилност, рањивост односно безбедносни инцидент при коришћењу дигиталног идентификационог новчаника, механизма за валидацију или средства електронске идентификације у оквиру које се користи дигитални идентификациони новчаник, на начин који утиче на њихову поузданост или на поузданост других дигиталних идентификационих новчаника, Канцеларија без одлагања привремено обуставља коришћење дигиталног идентификационог новчаника.

Ако је неправилност, рањивост односно безбедносни инцидент из става 1. изазвао или може да изазове озбиљне последице по безбедност дигиталног идентификационог новчаника, Канцеларија повлачи из употребе дигитални идентификациони новчаник.

Када се неправилност, рањивост, односно безбедносни инцидент при коришћењу дигиталног идентификационог новчаника из става 1. овог члана отклони и стекну услови за безбедно и поуздано коришћење дигиталног новчаника, Канцеларија га поново ставља на располагање.

Ако се неправилност, рањивост, односно безбедносни инцидент из става 1. овог члана не отклони у року од 90 дана од дана привремене обуставе, Канцеларија повлачи из употребе дигитални идентификациони новчаник и опозива његову ваљаност.

О инцидентима и предузетим мерама из ст. 1-3. овог члана Канцеларија обавештава кориснике, поуздајуће стране који их користе, као и Министарство.

Министарство ближе прописује мере из ст. 1-4. овог члана.

2. Шеме електронске идентификације

Услови које мора да испуњава шема електронске идентификације

Члан 20.

Шема електронске идентификације мора:

1) да садржи податке за идентификацију лица на издатим средствима за електронску идентификацију, који јединствено одређују правно или физичко лице;

- 2) да обезбеди да пружалац услуге електронске идентификације обезбеди идентификационе податке у оквиру средства електронске идентификације који одговарају лицу коме је средство издато;
- 3) да јасно дефинише техничке и друге услове који омогућавају поуздајућој страни проверу идентитета;
- 4) да испуњава услове за ниво поузданости у који се разврстава, из члана 21. овог закона.

Нивои поузданости шема електронске идентификације

Члан 21.

Шеме електронске идентификације разврставају се према нивоу поузданости на:

- 1) шеме основног нивоа поузданости, које обезбеђују ограничено поверење у идентитет којим се лице представља и користе средства и процедуре чија сврха је да смање ризик злоупотребе односно неистинитог представљања;
- 2) шеме средњег нивоа поузданости, које обезбеђују значајно поверење у идентитет којим се лице представља и користе средства и процедуре чија сврха је да значајно смање ризик злоупотребе односно неистинитог представљања;
- 3) шеме високог нивоа поузданости, које обезбеђују високо поверење у идентитет којим се лице представља и користе средства и процедуре чија сврха је да онемогуће злоупотребу односно неистинито представљање.

Влада, на предлог Министарства, уређује ближе услове које морају да испуне шеме електронске идентификације за одређене нивое поузданости, а нарочито:

- 1) начин доказивања и провере идентитета физичког односно правног лица које захтева издавање средстава електронске идентификације;
- 2) начин издавања средстава електронске идентификације;
- 3) механизам аутентификације, путем кога физичко односно правно лице коришћењем средстава идентификације потврђује свој идентитет другој страни у електронској трансакцији;
- 4) услове које треба да испуни пружалац услуге електронске идентификације;
- 5) услове који се односе на податке који се користе у процесу прекограничне сарадње за физичка и правна лица приликом коришћења регистрованих шема електронске идентификације, а који од података о личности садрже име и презиме, датум рођења, адресу становања и пол а у сврху поуздане провере идентитета лица;
- 6) услове које треба да испуне други учесници који су укључени у поступак издавања средстава електронске идентификације;
- 7) техничке и безбедносне карактеристике средстава електронске идентификације која се издају;
- 8) минималне техничке и организационе услове у циљу обезбеђивања интероперабилности шема електронске идентификације у складу са домаћим и међународним стандардима из ове области.

Упис у Регистар пружалаца услуга електронске идентификације и шема електронске идентификације

Члан 22.

Регистар пружалаца услуга електронске идентификације и шема електронске идентификације представља скуп података о пружаоцима услуге електронске идентификације и о шемама електронске идентификације, који води Министарство.

Пружалац услуге електронске идентификације подноси Министарству захтев и потребну документацију за упис у Регистар пружалаца услуга електронске идентификације и шема електронске идентификације.

Регистар из става 1. овог члана од података о личности садржи податке о одговорним лицима, и то: име, презиме, функцију и контакт податке као што су службена адреса, број службеног телефона и

службена адреса електронске поште у сврху доступности података корисницима услуге о пружаоцу услуге електронске идентификације.

Саставни део Регистра из става 1. овог члана су и шеме електронске идентификације са листе коју, у складу са чланом 9. Уредбе ЕУ бр. 1183/2024 Европског парламента и Савета (у даљем тексту: Уредба eIDAS), објављује Европска комисија.

Министарство прописује садржај и начин вођења Регистра из става 1. овог члана, као и начин подношења захтева за упис у тај регистар, у складу са законом који уређује општи управни поступак, потребну документацију уз захтев, образац захтева и начин објављивања података из тог регистра.

Сертификација шема електронске идентификације

Члан 23.

Тело за оцењивање усаглашености, које је акредитовано у складу са законом којим се уређује поступак акредитације издаје сертификат којим потврђује усклађеност шема електронске идентификације са безбедносним и техничким захтевима прописаним овим законом.

Оцена усклађености, односно сертификација обухвата техничке, организационе и безбедносне аспекте шема електронске идентификације.

Сертификација се врши у складу са:

- 1) захтевима из овог закона и прописа донетих на основу њега;
- 2) националним стандардима за безбедност и заштиту података;
- 3) међународним стандардима као што су ISO/IEC 27001 и ISO/IEC 29115,
- 4) препорукама надлежних међународних тела за информациону безбедност.

Пружалац услуге електронске идентификације уз захтев за сертификацију шеме електронске идентификације доставља:

- 1) техничку спецификацију система;
- 2) опис мера за заштиту података;
- 3) извештај о процени ризика и рањивости;
- 4) опис процедура за надзор и отклањање рањивости и
- 5) доказ о усклађености са релевантним стандардима.

Сертификат о усаглашености важи највише пет година, уз обавезу спровођења редовне процене рањивости најмање сваке две године.

Ако се утврди рањивост издате шеме електронске идентификације, тело које је издало шему без одлагања га суспендује.

Када се рањивост из става 6. овог члана отклони шема електронске идентификације се поново ставља на располагање кориснику.

Ако се рањивост из става 6. овог члана не отклони у року од 90 дана од суспензије сертификат се опозива и повлачи из употребе.

Тело које је издало сертификат обавештава корисника, Канцеларију, као и Министарство о безбедносним инцидентима и предузетим мерама из ст. 6-8. овог члана.

Министарство:

- 1) води регистар акредитованих тела за оцену усаглашености из става 1. овог члана;
- 2) надзире рад акредитованих тела за оцену усаглашености кроз редовне извештаје и инспекције;
- 3) осигурава транспарентност процеса сертификације кроз објављивање информација о сертифицикованим шемама електронске идентификације у јавном регистру.

Министарство ближе уређује услове и критеријуме за сертификацију у складу са технолошким развојем и препорукама међународних тела.

Коришћење шема електронске идентификације у електронском пословању и у општењу са органом јавне власти

Члан 24.

За утврђивање идентитета у електронском пословању могу се користити шеме електронске идентификације које су уписане у регистар из члана 22. овог закона, као и шеме електронске идентификације које нису уписане у регистар.

Исказ воље не може се оспорити само зато што су, уместо потписа, коришћене шеме електронске идентификације из става 1. овог члана.

Шема електронске идентификације која је уписана у регистар из члана 22. овог закона (у даљем тексту: регистрована шема електронске идентификације) може се користити за утврђивање идентитета странке у општењу са органом јавне власти.

У општењу странке са органима јавне власти идентитет странке утврђен на основу регистроване шеме електронске идентификације високог нивоа поузданости замењује потпис странке на поднеску.

Прописом може бити одређено да се у случају из става 4. овог члана може користити шема електронске идентификације средњег или основног нивоа поузданости, ако су ризик од злоупотребе и могућа штета од злоупотребе такви да није неопходно користити шему високог нивоа поузданости.

Одговорност при електронској идентификацији

Члан 25.

Издавалац средства електронске идентификације одговоран је за штету насталу услед тога што је издао средство електронске идентификације противно условима прописаним овим законом и шемом електронске идентификације.

Страна која спроводи поступак аутентификације одговара за штету насталу услед непрописно спроведеног поступка аутентификације.

Лица која учествују у поступку електронске идентификације одговарају за штету коју проузрокују својим радњама или пропустима, у складу са својим овлашћењима и одговорностима утврђеним овим законом.

Одредбе овог члана примењују се у складу са законом којим се уређују облигациони односи.

У случају међународне сарадње у области електронске идентификације, примењују се одредбе утврђене међународним споразумима.

Безбедносни услови које треба да испуњавају пружаоци услуга електронске идентификације

Члан 26.

Пружалац услуга електронске идентификације предузима потребне техничке, физичке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга.

Техничким и организационим мерама осигурава се да ниво безбедности одговара степену ризика и предвиђеном нивоу поузданости шеме електронске идентификације, узимајући у обзир најновија доступна технолошка решења, а посебно се предузимају мере за спречавање безбедносних инцидената и ограничавање штетних последица евентуалних инцидената, као и за обавештавање заинтересованих страна о нежељеним ефектима безбедносних инцидената.

Пружалац услуга електронске идентификације дужан је да најмање једном годишње спроводи процену ризика, идентификује претње и слабости, утврди и ревидира мере заштите које су примерене степену ризика и нивоу поузданости шеме.

Резултати процене и мере из става 3. овог члана морају бити документовани и доступни Министарству, у складу са прописима, техничким стандардима, добром праксом и технолошким достигнућима.

3. Прекогранична сарадња у области електронске идентификације

Члан 27.

Министарство сарађује са надлежним међународним телима по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставила интероперабилност шема електронске идентификације на националном нивоу.

Ради остваривања прекограничне интероперабилности успоставља се оквир интероперабилности који:

- 1) је технолошки неутралан;
- 2) примењује одговарајуће европске и међународне стандарде, нарочито у области информационе безбедности;
- 3) омогућава примену приватности по дизајну, укључујући минималну обраду података, селективно откривање идентитета, криптографску заштиту и спречавање профилисања, у складу са прописима о заштити података о личности.

Канцеларија успоставља и управља чвором у оквиру интероперабилности који омогућава прекограничну аутентификацију лица, чиме се обезбеђује да се инфраструктура електронске идентификације Републике Србије повеже са инфраструктуром електронске идентификације друге државе.

У процесу управљања чвором из става 3. овог члана Канцеларија:

- 1) обезбеђује повезивање са чворовима других држава кроз оквир интероперабилности чије су шеме електронске идентификације саставни део Регистра из члана 22. овог закона, односно које су признате на основу међународног споразума;
- 2) примењује техничке и организационе мере заштите ради спречавања неовлашћеног приступа подацима који се размењују и обезбеђује интегритет податка, који се преносе између чворова употребом одговарајућих техничких решења и праксе;
- 3) обезбеђује да се подаци о личности не чувају или задржавају у чвору;
- 4) користи техничка решења која обезбеђују интегритет и аутентичност података, а која се користе приликом прекограничне размене података;
- 5) обезбеђује да чвор испуњава прописане услове који се односе на формат порука, структуру података и протоколе размене, у складу са важећим националним стандардима и регулативом, чиме се обезбеђује техничка интероперабилност и правна ваљаност прекограничне електронске идентификације;
- 6) обезбеђује достављање метаподатака о управљању чвором у стандардизованом, машински читљивом облику који је погодан за аутоматску обраду података, на безбедан и поуздан начин;
- 7) обезбеђује аутоматску обраду параметара који се односе на безбедност, уз примену техничких и организационих мера које омогућавају континуирано праћење, евидентирање, анализу и реаговање на безбедносне догађаје, у складу са важећим националним стандардима и регулативом, без угрожавања приватности или интегритета података;
- 8) чува податке који би у случају инцидента омогућавали утврђивање места и врсте инцидента у законском року.
- 9) омогућава пренос података који обезбеђују поуздано представљање физичког или правног лица, на основу употребе регистроване шеме електронске идентификације приликом прекограничне сарадње у складу са законом.

У поступцима прекограничне електронске идентификације примењују се технолошка решења која омогућавају недвосмислено утврђивање и упаривање идентитета физичких и правних лица, на основу електронских идентификационих средстава издатих у складу са признатим и регистрованим шемама електронске идентификације, а у складу са важећим техничким стандардима и прописима.

Канцеларија спроводи техничке и организационе мере у чвору на начин који спречава профилисање корисника и обезбеђује заштиту података о личности, у складу са прописима којима се уређује заштита података о личности и електронска идентификација у прекограничном контексту.

Прописом Владе из члана 21. став 2. овог закона ближе се уређују услови из става 4. овог члана који се односе на чвор.

Приступ хардверским и софтверским функцијама

Члан 28.

Канцеларија је дужна да издаваоцима средстава за електронску идентификацију који та средства стављају у промет омогући:

1) интероперабилност, укључујући техничке, организационе и правне мере неопходне за обезбеђивање приступа оперативним системима, хардверским и софтверским функцијама релевантним за пружање услуга електронске идентификације;

2) бесплатан приступ оперативним системима, хардверским и софтверским функцијама из тачке 1 овог става.

Обавезе из овог члана тумаче се у складу са принципима равноправног приступа, транспарентности и недискриминације, узимајући у обзир прописе и одговарајуће међународне стандарде.

Пријављивање

Члан 29.

Министарство може признати сертификате издате у иностранству, под условом да су усклађени са међународним стандардима и да су издати од стране тела која испуњавају захтеве прописане овим законом.

Министарство Европској комисији може пријављивати регистроване шеме електронског идентитета које испуњавају услове из Уредбе eIDAS.

IV. УСЛУГЕ ОД ПОВЕРЕЊА

1. Опште одредбе

Одговорност пружаоца услуга од поверења и терет доказивања

Члан 30.

Пружалац услуге од поверења одговоран је за штету насталу услед тога што није поступио у складу са овим законом уколико је штету проузроковао намерно или непажњом.

Терет доказивања намере или непажње пружаоца услуга од поверења је на физичком или правном лицу које захтева накнаду штете из става 1. овог члана.

Терет доказивања да штета није настала услед намере или непажње квалификованог пружаоца услуга од поверења из става 1. овог члана је на том пружаоцу услуга.

Пружалац услуга од поверења није одговоран за штету насталу због коришћења услуге којом је прекорачено назначено ограничење, ако је корисник услуге од поверења о таквом ограничењу унапред обавештен, и ако су та ограничења позната трећим лицима.

Одговорност корисника услуга од поверења за чување средстава и података за формирање електронског потписа односно печата

Члан 31.

Корисник услуге од поверења дужан је да чува средства и податке за формирање електронског потписа односно печата од неовлашћеног приступа и употребе, и да исте користи у складу са одредбама овог закона.

Услови које треба да испуњавају пружаоци услуга од поверења

Члан 32.

Пружаоци услуга од поверења треба да усвоје одговарајуће политике и процедуре и предузму друге релевантне мере у циљу управљања правним, пословним, оперативним и другим директним или индиректним ризицима по пружање услуге од поверења и да поред предузимања мера из закона који уређује информациону безбедност обухвата мере управљања ризиком приликом:

- 1) регистрације и приступа корисника услугама од поверења;
- 2) спровођења административних провера неопходних за пружање услуга од поверења;
- 3) управљања и спровођења услуга од поверења.

Пружаоци услуга од поверења без одлагања, а најкасније 24 сата од сазнања, обавештавају Министарство и друге надлежне органе, угрожене кориснике, као и јавност уколико је то у јавном интересу, о свакој безбедносној компромитацији или сметњама у пружању услуге или примени мера из става 2. овог члана које имају значајан утицај на пружање услуге од поверења или на заштиту података о личности који се обрађују у оквиру пружања услуге.

Ако би угрожавање безбедности или губитак интегритета услуге од поверења могли неповољно утицати на кориснике услуга од поверења, пружалац услуга од поверења о повреди безбедности или губитку интегритета услуге, без одлагања, обавештава корисника услуга од поверења, а ако би појединачно обавештавање представљало неразуман утрошак времена и средстава, путем средстава јавног информисања, веб презентације министарства и на други погодан начин.

Министарство обавештава јавност или захтева од пружаоца услуга од поверења да то учини, ако утврди да је објављивање података о повреди безбедности или губитку интегритета услуге у јавном интересу.

Министарство сарађује са надлежним органима других држава у вези са разменом података о нарушавању безбедности и интегритета услуга од поверења, у складу са међународним споразумима.

Министарство прописује стандарде, техничке спецификације и процедуре за испуњење услова из става 1. овог члана.

Надлежност Министарства

Члан 33.

Министарство врши следеће послове:

- 1) води регистар пружаоца квалификованих услуга од поверења;
- 2) разматра извештаје о провери испуњености услова за пружање квалификованих услуга од поверења;
- 3) врши инспекцијски надзор над радом пружаоца услуга од поверења;
- 4) налаже ванредну проверу испуњености услова за пружање квалификованих услуга од поверења, у складу са законом;
- 5) сарађује са надлежним органом за заштиту података о личности, и обавештава га без одлагања уколико дође до сазнања да пружаоци квалификованих услуга од поверења не поступају у складу са прописима о заштити података о личности;
- 6) проверава постојање и правилну примену одредаба о плановима прекида активности у случајевима када пружалац квалификоване услуге од поверења прекине своје активности, укључујући начин на који се одржава доступност информација које издаје и прима пружалац квалификоване услуге од поверења;
- 7) сарађује са надзорним телима Европске уније;
- 8) обавештава јавност о угрожавању безбедности или губитку целовитости услуга од поверења који имају значајан утицај на пружену услугу од поверења или у њој садржане личне податке.

Надлежности Министарства у оквиру прекограничне сарадње у области услуга од поверења

Члан 34.

Министарство обавља и послове:

- 1) обавештава надлежна тела страних држава о угрожавању безбедности или губитку целовитости који имају значајан утицај на пружену услугу од поверења или у њој садржане личне податке;
- 2) извештава Европску комисију о својим активностима у складу са Уредбом eIDAS, почев од дана ступања Републике Србије у чланство у Европској унији.

2. Квалификоване услуге од поверења

Успостављање односа између пружаоца и корисника квалификоване услуге од поверења

Члан 35.

О пружању квалификоване услуге од поверења закључује се уговор између пружаоца и корисника квалификоване услуге од поверења, на захтев корисника.

Пружалац квалификоване услуге од поверења дужан је да, пре закључивања уговора из става 1. овог члана, на свеобухватан и лако доступан начин, у разумљивом облику, обавести лице које је поднело захтев за пружање квалификоване услуге од поверења о свим важним околностима коришћења услуге, а нарочито о:

- 1) прописима и правилима који се односе на коришћење квалификоване услуге од поверења;
- 2) евентуалним ограничењима у коришћењу квалификоване услуге од поверења;
- 3) мерама које треба да реализују корисници квалификоване услуге од поверења и о потребној технологији за безбедно коришћење квалификоване услуге од поверења.

Корисник квалификоване услуге од поверења може користити услуге од поверења једног или више пружалаца услуга од поверења.

Услови за пружање квалификованих услуга од поверења

Члан 36.

Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона:

1) има запослене који поседују неопходну стручност, искуство и квалификације за примену административних и управљачких процедура које одговарају домаћим и међународним стандардима и који су прошли одговарајућу обуку у области информационе безбедности и заштите података о личности, у односу на услугу коју пружа;

2) се осигура од одговорности за штету насталу пружањем квалификоване услуге од поверења;

3) користи поуздане уређаје и производе који су заштићени од неовлашћене промене и гарантују техничку безбедност и поузданост процеса које подржавају, укључујући коришћење одговарајућих криптографских техника;

4) користи поуздане системе за чување података који су му поверени тако:

- (1) да су подаци доступни само уз сагласност лица чији су то подаци,
- (2) да само овлашћена лица могу уносити податке и вршити измене,
- (3) да се може проверавати аутентичност података;

5) спроводи мере против злоупотребе и крађе података;

6) чува у одговарајућем временском периоду, не дужем од десет година, све релевантне информације које се односе на податке који су креирани или примљени од стране пружаоца квалификованих услуга од поверења, а посебно за сврху пружања доказа у правним поступцима, осим ако посебним законом није предвиђен другачији период чувања;

7) води ажурну, тачну и безбедним мерама заштићену базу података издатих електронских сертификата у случају када пружа услугу издавања квалификованих електронских сертификата, као и

базу података који су креирани или примљени од стране пружаоца квалификованих услуга од поверења у оквиру пружања квалификованих услуга од поверења;

8) има ажуран план завршетка рада који осигурава континуитет квалификованих услуга од поверења;

9) осигура обраду личних података у складу са законом;

10) обезбеди да се просторије и опрема коју користи за пружање квалификованих услуга од поверења налазе на територији Републике Србије;

11) податке и документа која се налазе у његовом информационом систему не преноси ван територије Републике Србије, осим ако другачије није предвиђено прописима и међународним уговорима.

Пружалац квалификоване услуге од поверења дужан је да донесе акта којима уређује:

1) опште услове за пружање услуге који су јавно доступни;

2) политике пружања услуга и практична правила за пружање услуга које пружалац квалификоване услуге од поверења користи како би обезбедио пружање услуге у складу са прописима и општим условима из тачке 1) овог става;

3) информациону безбедност.

Пружалац квалификованих услуга од поверења дужан је да писаним путем обавести Министарство о свакој планираној измени у пружању квалификованих услуга од поверења најкасније 30 дана пре увођења те измене, односно о намери престанка обављања делатности најкасније 90 дана пре престанка.

Пружалац услуга од поверења који издаје квалификоване електронске сертификате дужан је да доставља Министарству податке о броју сертификата издатих од почетка пружања услуге до 31. децембра календарске године и податке о броју важећих сертификата на дан 31. децембар календарске године.

Ажурни подаци из става 3. овог члана достављају се редовно, најкасније до 15. јануара за претходну годину, као и по потреби, ванредно, на захтев Министарства.

Влада, на предлог Министарства, ближе уређује услове за пружање квалификоване услуге од поверења из става 1. овог члана и садржај аката из става 2. овог члана, укључујући одређивање међународних стандарда који се примењују.

Осигурање од професионалне одговорности

Члан 37.

Министарство прописује најнижи износ осигурања од ризика одговорности за штету насталу вршењем услуге квалификоване услуге од поверења.

Провера идентитета корисника квалификоване услуге од поверења издавања квалификованог сертификата

Члан 38.

Пружалац квалификованих услуга од поверења приликом пружања услуга дужан је да приликом издавања квалификованог сертификата или квалификоване електронске потврде атрибута провери идентитет физичког или правног лица којем се сертификат, односно потврда атрибута издаје, уз примену једне или више метода, и то:

1) коришћењем дигиталног идентификационог новчаника или другог средства електронске идентификације у оквиру шеме електронске идентификације високог нивоа поузданости;

2) коришћењем квалификованог електронског потписа, односно печата;

3) коришћењем других метода идентификације којима се обезбеђује висок ниво поузданости;

4) уз присуство физичког лица, односно овлашћеног представника правног лица уз подношење одговарајућих доказа као што је лична карта или путна исправа, односно други идентификациони документ са фотографијом.

Провера идентитета корисника квалификоване услуге од поверења издавања квалификоване електронске потврде атрибута

Члан 39.

Пружалац квалификованих услуга од поверења приликом издавања квалификоване електронске потврде атрибута, поред провере идентитета на начин из члана 38. овог закона, за проверу атрибута:

- 1) користи дигитални идентификациони новчаник или друга средства електронске идентификације у оквиру шеме електронске идентификације високог нивоа поузданости;
- 2) користи квалификован електронски потпис, односно печат;
- 3) користи квалификовану електронску потврду атрибута која садржи информацију о атрибуту;
- 4) проверава атрибуте присутног физичког лица која захтева услугу у своје име, односно у име правног лица на основу поднетих одговарајућих доказа.

Пружалац квалификоване услуге од поверења дужан је да обезбеди периодичну проверу података и сертификата, а нарочито о статусу физичког и правног лица којем је издао квалификовани сертификат, као и да изврши опозив сертификата у случају промене података у складу са законом.

Оцењивање испуњености услова за пружање квалификованих услуга од поверења

Члан 40.

Оцењивање испуњености услова за пружање квалификованих услуга од поверења (у даљем тексту: оцењивање испуњености услова) обавља тело за оцењивање усаглашености које је, у складу са законом којим се уређује акредитација, акредитовано за оцењивање усаглашености пружаоца квалификованих услуга од поверења и квалификованих услуга од поверења које они пружају.

Након спроведеног оцењивања испуњености услова тело за оцењивање усаглашености сачињава извештај о оцењивању усаглашености.

Оцењивање испуњености услова врши се пре почетка пружања квалификованих услуга од поверења и најмање једном у 24 месеца.

Након завршеног оцењивања испуњености услова пружалац услуге од поверења доставља Министарству извештај о оцењивању усаглашености, у року од три радна дана од дана када га је примио.

Министарство може захтевати ванредно оцењивање испуњености услова како би потврдило да пружалац квалификованих услуга од поверења и квалификоване услуге од поверења које он пружа испуњавају услове прописане овим законом, а посебно ако се утврде неправилности у пружању квалификованих услуга од поверења, односно ако наступи инцидент који је у значајној мери угрозио или нарушио информациону безбедност.

Ванредно оцењивање испуњености услова врши тело за оцењивање усаглашености које није повезано са вршењем претходног оцењивања.

Трошкове оцењивања испуњености услова, укључујући ванредна оцењивања, сноси пружалац квалификоване услуге од поверења.

Ако пружалац квалификоване услуге од поверења не испуњава неки од услова прописаних овим законом, Министарство му налаже отклањање утврђених недостатака у року не дужем од 90 дана.

Ако пружалац квалификоване услуге од поверења у задатом року не отклони утврђене неправилности и не испуни прописане услове, Министарство доноси решење о укидању статуса квалификованог пружаоца услуга од поверења и обустављању пружања одговарајуће услуге од поверења коју пружа и доставља га, у складу са законом.

Ако орган надлежан за заштиту података о личности приликом вршења надзора утврди да је пружалац квалификоване услуге од поверења вршио обраду података о личности супротно закону и

донесе решење којим се захтева престанак обраде, Министарство привремено предузима одговарајуће мере у складу са овим законом и законом којим се уређује инспекцијски надзор.

Сваку измену квалификованог статуса из ст. 9-10. овог члана Министарство ажурира у регистру пружалаца квалификованих услуга од поверења.

Министарство утврђује листу стандарда које мора да испуни тело за оцењивање усаглашености, обавезну садржину извештаја о оцењивању усаглашености и поступак оцењивања испуњености услова односно оцењивања усаглашености квалификованих услуга од поверења.

Упис у Регистар пружалаца квалификованих услуга од поверења

Члан 41.

Регистар пружалаца квалификованих услуга од поверења представља скуп података о пружаоцима квалификованих услуга од поверења и о квалификованим услугама од поверења који води Министарство.

Пружалац квалификованих услуга од поверења подноси Министарству захтев за упис у Регистар пружалаца квалификованих услуга од поверења.

Уз захтев из става 1. овог члана прилажу се докази о чињеницама исказаним у захтеву укључујући извештај о оцењивању усаглашености из члана 40. став 4. овог закона којим је оцењено да подносилац захтева и квалификоване услуге од поверења које он намерава да пружа испуњавају услове из овог закона.

Министарство решава о упису пружаоца квалификованих услуга од поверења у регистар из става 1. овог члана у року од 60 дана од дана подношења уредног захтева.

У поступку решавања из става 4. овог члана Министарство може захтевати прилагање додатних доказа, као и додатну проверу техничких и безбедносних компоненти и оперативног рада.

Ако пружалац квалификованих услуга од поверења испуњава услове утврђене овим законом, Министарство решењем утврђује врсту услуге коју пружа, и врши упис у регистар из става 1. овог члана.

Пружалац квалификованих услуга од поверења може почети да пружа квалификовану услугу од поверења након уписа у регистар из става 5. овог члана.

Ако пружалац услуга престане да испуњава услове прописане овим законом Министарство доноси решење о његовом брисању из регистра из става 1. овог члана.

Регистар из става 1. овог члана од података о личности садржи податке о одговорним лицима, и то: име, презиме, функцију и контакт податке као што су службена адреса, службени број телефона и службена адреса електронске поште у сврху доступности података о пружаоцу квалификоване услуге од поверења са којим се закључује уговор о пружању услуге.

Министарство прописује садржај и начин вођења регистра из става 1. овог члана, начин подношења захтева за упис у регистар из става 1. овог члана у складу са прописима који уређују општи управни поступак, потребну документацију уз захтев, образац захтева и начин провере испуњености услова за пружање квалификоване услуге од поверења.

Престанак пружања услуге издавања квалификованих електронских сертификата

Члан 42.

Издавалац квалификованих електронских сертификата који намерава да престане са обављањем делатности дужан је да о намери раскида уговора обавести сваког корисника квалификоване услуге од поверења и Министарство, најмање 90 дана пре настанка намераваног престанка обављања делатности.

Издавалац квалификованих електронских сертификата који престаје са обављањем послова дужан је да обезбеди код другог пружаоца услуга од поверења наставак обављања услуге за кориснике квалификоване услуге од поверења којима је издао сертификат, а ако за то нема могућности, дужан је да опозове све издате сертификате и о предузетим мерама одмах обавести Министарство.

Издавалац квалификованих електронских сертификата дужан је да достави сву документацију и неопходна техничка средства у вези са обављањем услуга од поверења другом издаваоцу на кога преноси обавезе обављања једне или више услуга од поверења.

Ако издавалац квалификованих електронских сертификата не поступи у складу са ставом 3. овог члана, дужан је да достави сву документацију Министарству које ће извршити опозив свих сертификата, без одлагања, а на трошак издаваоца квалификованих електронских сертификата.

У случају привремене забране вршења услуга, сертификати издати до дана настанка узрока због којих је изречена мера забране, остају у важности.

Употреба квалификованих електронских сертификата и квалификованих електронских временских жигова у софтверским решењима органа јавне власти

Члан 43.

Орган јавне власти дужан је да у пружању услуга електронске управе у смислу закона којим се уређује електронска управа у софтверским решењима омогући употребу квалификованих електронских сертификата и квалификованих електронских временских жигова издатих од свих пружалаца квалификованих услуга од поверења уписаних у Регистар из члана 35. овог закона.

Државни орган као пружалац квалификованих услуга од поверења

Члан 44.

Државни орган може пружати квалификоване услуге од поверења уколико испуњава услове за пружање услуга предвиђене овим законом.

Оцењивање испуњености услова државног органа за пружање услуге од поверења врши министарство, односно инспектор за електронску идентификацију и услуге од поверења, након поднетог захтева.

Изузетно од става 2. овог члана оцењивање испуњености услова врши се на основу интерне контроле у сарадњи са надлежним министарством само у случају када је пружалац квалификоване услуге од поверења министарство надлежно за послове одбране, уз обавезу достављања извештаја о извршеној интерној контроли надлежном министарству.

Након провере испуњености услова Влада уредбом утврђује да државни орган може да обавља квалификовану услугу од поверења која је била предмет оцењивања из става 2. овог члана.

Министарство врши упис државног органа у регистар из члана 35. овог закона, на основу уредбе из става 4. овог члана.

Јавна листа квалификованих услуга од поверења

Члан 45.

Јавна листа квалификованих услуга од поверења на аутоматизован начин поуздајућој страни обезбеђује поуздану информацију о статусу пружаоца квалификованих услуга од поверења и њихових квалификованих услуга у складу са подацима уписаним у регистар из члана 41. овог закона.

Јавна листа квалификованих услуга од поверења садржи информацију о релевантним протеклим догађајима у вези са статусом садашњих и бивших пружалаца и њихових услуга током времена, укључујући информацију о почетку пружања, губитку целovitости услуге од поверења, привременој забрани, престанку пружања услуге, брисању из регистра и другим догађајима забележеним у оквиру послова вођења регистра, инспекцијског надзора или догађајима пријављеним од стране пружаоца, а који утичу на прихватљивост квалификоване услуге од поверења и поступак утврђивања њеног статуса у одређеном временском тренутку.

У Јавну листу квалификованих услуга од поверења уписују се подаци из ст. 1. и 2. овог члана као и други подаци утврђени прописом Министарства из става 6. овог члана и одговарајућим стандардима.

Пружалоци квалификованих услуга од поверења дужни су да, на захтев Министарства, у року од седам дана, доставе податке из става 3. овог члана, као и да о свакој промени података из става 3. овог члана обавесте Министарство без одлагања.

Подаци о сертификату којим је подржан потпис Јавне листе квалификованих услуга од поверења, укључујући sha-256 отисак објављују се у „Службеном гласнику Републике Србије”.

Министарство прописује техничке услове, форму и начин објављивања јавне листе квалификованих услуга од поверења и услове које министарство надлежно за објављивање јавне листе квалификованих услуга од поверења мора да обезбеди при њеном формирању, потписивању и објављивању.

Форма и начин објављивања јавне листе квалификованих услуга од поверења из става 6. овог члана треба да буду усклађени са техничким условима за листе од поверења из члана 22. Уредбе eIDAS.

Знак поузданости за квалификоване услуге од поверења

Члан 46.

Знак поузданости за квалификоване услуге од поверења (у даљем тексту: Знак поузданости) је знак којим се на једноставан, препознатљив и јасан начин означава квалификована услуга од поверења.

Регистровани пружаоци квалификованих услуга од поверења имају право да користе Знак поузданости за квалификоване услуге од поверења које пружају.

Знак поузданости из става 1. користи се до ступања Републике Србије у чланство у Европској унији.

Министарство прописује изглед, састав, величину и дизајн Знака поузданости за квалификоване услуге од поверења.

Прекогранично признавање квалификованих услуга од поверења

Члан 47.

Услуге од поверења које пружају пружаоци квалификованих услуга од поверења основани у другој држави или међународној организацији могу бити признате као правно еквивалентне квалификованим услугама од поверења које пружају пружаоци квалификованих услуга од поверења регистровани у републици србији, ако је то предвиђено међународним споразумом који закључи Република Србија са другом државом или међународном организацијом, као и актом Владе.

Услуге од поверења из става 1 овог члана признаће се ако:

- 1) друга држава или међународна организација успоставе, одржавају и објављују јавну листу квалификованих услуга од поверења у машински читљивом формату;
- 2) су услови за пружаоце услуга од поверења и услуге које они пружају одговарају условима који важе за квалификоване пружаоце услуга од поверења у Републици Србији.

Став 1. овог члана не примењује се на услугу електронског архивирања.

Влада, на предлог министарства, прописује поступак међусобног признавања услуга од поверења из других држава по принципу реципроцитета.

V. ПОЈЕДИНЕ ВРСТЕ УСЛУГА ОД ПОВЕРЕЊА

Врсте услуга

Члан 48.

Услуге од поверења се пружају у областима:

- 1) електронског потписа и електронског печата;
- 2) електронског временског жига;
- 3) електронске доставе;
- 4) аутентификације веб сајтова;
- 5) електронског архивирања;

- 6) електронске потврде атрибута;
- 7) вођења електронских евиденција.

Квалификоване услуге од поверења су:

- 1) издавање квалификованих сертификата за електронски потпис;
- 2) услуга управљања квалификованим средством за креирање електронског потписа на даљину;
- 3) услуга валидације квалификованог електронског потписа;
- 4) издавање квалификованих сертификата за електронски печат;
- 4б) услуга чувања квалификованог електронског потписа;
- 5) услуга управљања квалификованим средством за креирање електронског печата на даљину;
- 6) услуга валидације квалификованог електронског печата;
- 6а) услуга чувања квалификованог електронског печата;
- 7) издавање квалификованих електронских временских жигова;
- 8) услуга квалификоване електронске доставе;
- 9) услуга издавања квалификованих сертификата за аутентификацију веб сајтова;
- 9а) услуга издавања квалификованих електронских потврда атрибута;
- 10) услуга квалификованог електронског архивирања;
- 10а) услуга вођења електронске евиденције;

Пружалац услуга од поверења односно квалификованих услуга од поверења може пружати једну или више услуга из ст. 1. и 2. овог члана.

1. Електронски потпис и електронски печат

Напредни електронски потпис и напредни електронски печат

Члан 49.

Напредни електронски потпис односно напредни електронски печат мора:

- 1) на недвосмислен начин да буде повезан са потписником, односно печатиоцем;
- 2) да омогућава утврђивање идентитета потписника, односно печатиоца;
- 3) да буде израђен коришћењем података за израду електронског потписа односно електронског печата које потписник односно печатилац може, уз висок ниво поузданости, користити под својом искључивом контролом;
- 4) да буде повезан са електронски потписаним односно електронски печатираним подацима, на начин да се може утврдити било која накнадна измена тих података.

Садржај квалификованог електронског сертификата

Члан 50.

Квалификовани електронски сертификат мора да садржи:

- 1) ознаку, у форми погодној за аутоматску обраду, да се електронски сертификат користи као квалификовани сертификат за електронски потпис, односно печат;
- 2) скуп података који јединствено идентификују квалификованог пружаоца услуге од поверења за издавање квалификованог електронског сертификата укључујући, најмање, земљу порекла пружаоца и назив пружаоца;
- 3) скуп података који јединствено идентификују потписника односно печатиоца укључујући најмање:

- (1) за потписника:

– име и презиме или псеудоним, а уколико је употребљен псеудоним то мора бити јасно обележено у оквиру квалификованог електронског сертификата;

– ЈМБГ, уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ;

– евиденцијски број странца уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи евиденцијски број странца;

– број стране путне исправе из машински чиљиве зоне путне исправе, односно број стране личне карте и ознаку земље издаваоца путне исправе, односно стране личне карте, као идентификациону ознаку странца коју додељује Република Србија;

(2) за печатноца: назив, држава и матични број односно јединствена идентификациона ознака у складу са правном регулативом те државе, уколико постоји;

4) податке за проверу електронског потписа односно електронског печата, који одговарају подацима за креирање тог електронског потписа односно електронског печата;

5) податке о почетку и крају важења квалификованог електронског сертификата;

6) серијски број квалификованог електронског сертификата, који мора бити јединствен у оквиру издаваоца квалификованог електронског сертификата;

7) напредни електронски потпис или напредни електронски печат издаваоца квалификованог електронског сертификата;

8) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа односно напредног електронског печата из тачке 7) овог става;

9) информацију о сервисима који врше проверу валидности сертификата;

10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата;

11) ознаку да су подаци за креирање електронског потписа односно печата, који одговарају подацима за проверу електронског потписа односно печата из квалификованог електронског сертификата, садржани у квалификованом средству за креирање електронског потписа односно печата, уколико је тај услов испуњен.

Квалификовани електронски сертификати, поред обележја из става 1. овог члана, могу укључивати додатна обележја.

Министарство ближе прописује услове које морају да испуњавају квалификовани електронски сертификати из става 1. овог члана.

Опозив и суспензија квалификованог електронског сертификата

Члан 51.

Издавалац квалификованих сертификата дужан је да изврши опозив издатих сертификата, када:

- 1) опозив сертификата захтева власник сертификата или његов пуномоћник;
- 2) власник сертификата изгуби пословну способност, или је престао да постоји или су се промениле околности које битно утичу на важење сертификата;
- 3) утврди да је податак у сертификату погрешан;
- 4) утврди да су подаци за проверу квалификованог електронског потписа односно печата или систем пружаоца квалификованих услуга од поверења угрожени на начин који утиче на безбедност и поузданост сертификата;
- 5) утврди да су подаци за електронско потписивање односно печатање или систем власника сертификата угрожени на начин који утиче на поузданост и безбедност електронског потписа;
- 6) престаје са радом или му је рад забрањен.

Издавалац квалификованих сертификата дужан је да обавести корисника квалификоване услуге од поверења о опозиву сертификата у року од 24 часа од примљеног обавештења, односно настанка околности због којих се сертификат опозива.

Корисник квалификоване услуге од поверења дужан је да одмах затражи опозив свог квалификованог електронског сертификата у случају губитка или оштећења уређаја или података за креирање сертификата.

У случају опозива квалификовани електронски сертификат трајно престаје да важи од тренутка опозива.

У случају суспензије квалификовани електронски сертификат губи важност током периода трајања суспензије.

Подаци о суспензији и периоду трајања суспензије квалификованог електронског сертификата уписују се у базу података издатих сертификата коју води издавалац квалификованих електронских сертификата и морају бити видљиви током трајања суспензије у оквиру услуга којима се пружају информације о статусу сертификата.

Чување документације о издатим и опозваним квалификованим сертификатима

Члан 52.

Издавалац квалификованих електронских сертификата дужан је да чува комплетну документацију о издатим и опозваним квалификованим електронским сертификатима, као средство за доказивање и верификацију у управним, судским и другим поступцима, најмање десет година по престанку важења сертификата.

Подаци из става 1. овог члана могу се чувати у електронској форми.

Квалификована средства за креирање електронског потписа и печата

Члан 53.

Квалификовано средство за креирање електронског потписа односно печата мора да, помоћу одговарајућих техничких решења и поступака, обезбеди:

- 1) поверљивост података за креирање електронског потписа односно печата;
- 2) да се подаци за креирање електронског потписа, односно печата појављују само једном;
- 3) да се подаци за креирање електронског потписа, односно печата не могу добити изван средства за креирање електронског потписа, односно печата употребом доступне технологије у разумном времену;
- 4) да је електронски потпис, односно печат поуздано заштићен од фалсификовања употребом доступне технологије;
- 5) могућност поуздане заштите података за креирање електронског потписа, односно печата од неовлашћеног коришћења.

Средства за креирање квалификованог електронског потписа, односно печата, приликом креирања електронског потписа односно печата, не смеју променити податке који се потписују односно печатају или онемогућити потписнику, односно печатиоцу увид у те податке пре процеса креирања квалификованог електронског потписа односно печата.

Квалификовано средство за креирање електронског потписа, односно печата на даљину (у даљем тексту: услуга управљања квалификованим средством на даљину) корисник квалификоване услуге од поверења може користити путем услуге управљања квалификованим средством за креирање електронског потписа, односно печата, што такође представља квалификовану услугу од поверења.

Изузетно од става 1. овог члана, квалификовани пружалац услуга од поверења из става 3. овог члана може израдити копију података за израду електронског потписа, односно печата у сврху заштите од губитка података ако:

- 1) израда и чување копија података за креирање квалификованог електронског потписа односно печата не умањују прописани ниво заштите тих података;

2) број израђених копија података за креирање електронског потписа односно печата није већи него што је то неопходно за обезбеђивање континуитета пружања услуге.

Пружалац квалификоване услуге од поверења који пружа услугу управљања квалификованим средствима за креирање електронског потписа на даљину креира, односно управља подацима за креирање квалификованог електронског потписа и, на захтев корисника, израђује резервне копије тих података у сврху заштите од губитка података.

Министарство ближе прописује услове које мора да испуњава средство за креирање квалификованог електронског потписа односно печата.

Квалификована услуга управљања квалификованим средствима за креирање електронског потписа, односно печата, на даљину

Члан 54.

Пружалац услуге од поверења који управља квалификованим средствима за креирање електронског потписа на даљину је дужан да:

1) креира или управља подацима за креирање електронског потписа на захтев потписника и искључиво у његово име;

2) прави резервне копије података за креирање електронског потписа само у сврху заштите од губитка података, под следећим условима:

(1) да се безбедност резервних копија података одржава на истом нивоу као и безбедност изворних података;

(2) да је број резервних копија података ограничен на минимум неопходан за осигурање континуитета услуге;

3) испуњава све захтеве утврђене за сертификат за квалификовано средство на даљину за креирање електронског потписа, у складу са прописима.

На пружаоца услуге од поверења који управља квалификованим средствима за креирање електронског печата на даљину сходно се примењује став 1. овог члана.

Министарство прописује ближе услове, стандарде и процедуре које морају да испуњавају пружаоци квалификоване услуге од поверења за управљање квалификованим средствима за креирање електронског потписа, односно печата, на даљину.

Сертификација квалификованих средстава за креирање електронског потписа односно печата и упис у Регистар квалификованих средстава за креирање електронских потписа и електронских печата

Члан 55.

У складу са законом којим се уређују технички захтеви за производе и оцењивање усаглашености, Министарство именује тело за оцењивање усаглашености средстава за креирање квалификованог електронског потписа односно печата (у даљем тексту: именовано тело) које врши оцену усаглашености у складу са прописом из члана 53. овог закона.

Прописом из члана 53. овог закона ближе се уређују и услови које мора да испуњава именовано тело.

Министарство води Регистар квалификованих средстава за креирање електронских потписа и електронских печата.

Захтев за упис у Регистар из става 5. овог закона подноси се Министарству, на основу извештаја, односно издате потврде о усаглашености које добија од именованих тела.

Именовано тело без одлагања, а најкасније у року од седам дана од настале промене, обавештава Министарство о издатим и повученим потврдама о усаглашености средстава за креирање електронских потписа односно печата.

Потврда о усаглашености квалификованог средства за креирање електронског потписа или печата важи највише пет година, под условом да се процена рањивости врши најмање једном у две године.

Рањивости које утврде приликом вршења процене из става 6. Овог члана могу се отклонити у року од 30 дана или се потврда о усаглашености поништава.

Саставни део Регистра из става 3. овог члана су и квалификована средства за креирање електронског потписа и електронског печата са листе коју објављује Европска комисија.

За квалификована средства за креирање електронских потписа и електронских печата из става 8. овог члана не подноси се захтев за упис у Регистар квалификованих средстава за креирање електронских потписа и електронских печата.

Министарство прописује садржај и начин вођења Регистра из става 3. овог члана, начин подношења захтева за упис у тај регистар у складу са прописима који уређују општи управни поступак, потребну документацију уз захтев и образац захтева.

Валидација квалификованог електронског потписа и квалификованог електронског печата

Члан 56.

Поступком валидације утврђује се да електронски потпис представља исправан квалификовани електронски потпис када:

1) је утврђено да је сертификат који прати електронски потпис у тренутку потписивања представљао квалификовани електронски сертификат;

2) је утврђено да је квалификовани електронски сертификат издат од стране пружаоца услуге издавања квалификованих сертификата за електронски потпис и да је важио у тренутку потписивања;

3) је утврђено да подаци за валидацију електронског потписа из квалификованог електронског сертификата одговарају комбинацији електронског потписа и података који су потписани електронским потписом;

4) је поуздајућој страни тачно приказан скуп података из квалификованог електронског сертификата који јединствено идентификују потписника;

5) су поуздајућој страни тачно приказани подаци који су потписани електронским потписом;

6) је коришћење псеудонима јасно назначено поуздајућој страни, у случају да је приликом електронског потписивања коришћен псеудоним;

7) је утврђено да је електронски потпис креиран коришћењем квалификованог средства за креирање електронског потписа;

8) је утврђено да није нарушен интегритет података који су потписани електронским потписом;

9) је утврђено да електронски потпис испуњава услове за напредни електронски потпис из овог закона.

Систем који се користи за валидацију квалификованог електронског потписа обезбеђује тачан резултат поступка валидације поуздајућој страни и омогућава јој идентификовање било ког проблема од значаја за поузданост.

Одредбе ст. 1. и 2. овог члана сходно се примењују на електронски печат.

Министарство ближе прописује услове за поступак валидације квалификованог електронског потписа и квалификованог електронског печата.

Валидација напредних електронских потписа и напредних електронских печата заснованих на квалификованим сертификатима

Члан 57.

Валидација напредног електронског потписа заснованог на квалификованом сертификату потврђује исправност потписа, ако су испуњени следећи услови:

1) сертификат који прати електронски потпис је у време потписивања представљао квалификовани сертификат за електронски потпис;

2) квалификовани сертификат је издат од стране пружаоца квалификоване услуге од поверења и био је важећи у време потписивања;

3) подаци за валидацију потписа одговарају подацима достављеним поуздајућој страни;

4) јединствени сет података који идентификује потписника је исправно достављен поуздајућој страни;

5) коришћење псеудонима је јасно назначено поуздајућој страни, у случају да је приликом електронског потписивања коришћен псеудоним;

6) обезбеђен је интегритет потписаних података;

7) захтеви за напредне електронске потписе су били испуњени у време потписивања.

Систем који се користи за валидацију напредног електронског потписа мора да омогући кориснику да сазна тачан резултат процеса валидације и открије све безбедносне неправилности.

Одредбе ст. 1. и 2. овог члана сходно се примењују на електронски печат.

Министарство ближе прописује стандарде, спецификације и процедуре за валидацију напредних електронских потписа заснованих на квалификованим сертификатима.

Квалификована услуга валидације квалификованих електронских потписа и квалификованих електронских печата

Члан 58.

Пружалац квалификоване услуге валидације квалификованих електронских потписа односно печата обезбеђује:

1) валидацију квалификованог електронског потписа односно печата у складу са чланом 56. овог закона;

2) да поуздајућа страна која користи услугу добије резултат поступка валидације електронским путем на аутоматизован начин, који је поуздан и ефикасан;

3) да је резултат поступка валидације из тачке 2) овог става печатиран напредним електронским печатом или потписан напредним електронским потписом пружаоца услуге.

Министарство ближе прописује услове и начин, односно стандарде, спецификације и процедуре за пружање квалификоване услуге валидације квалификованих електронских потписа и квалификованих електронских печата.

Квалификована услуга чувања квалификованих електронских потписа и квалификованих електронских печата

Члан 59.

Пружалац квалификоване услуге чувања електронских потписа, односно печата обезбеђује поузданост квалификованог електронског потписа, односно печата и након његовог престанка важења.

Министарство ближе прописује стандарде, спецификације и процедуре за пружање квалификоване услуге чувања електронских потписа, односно печата.

Правно дејство електронског потписа

Члан 60.

Електронском потпису не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификовани електронски потпис.

Квалификовани електронски потпис има исто правно дејство као и својеручни потпис.

Квалификовани електронски потпис може да замени оверу својеручног потписа, ако је то прописано посебним законом.

Одредбе ст. 1. и 2. овог члана не примењују се на правне послове за које је посебним законом предвиђено да се не могу предузети у електронској форми.

Уговори и други правни послови за које је посебним законом предвиђено да се сачињавају у форми овере потписа, јавно потврђене (солемнизоване) исправе, или у форми јавнобележничког записа не могу се сачинити у складу са ст. 1. и 2. овог члана већ у складу са прописима којима се уређује овера потписа, потврђивање и сачињавање исправа о правним пословима.

Правно дејство електронског печата

Члан 61.

Електронском печату не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификовани електронски печат.

За квалификовани електронски печат важи правна претпоставка очуваности интегритета и тачности порекла података за које је везан.

Одредбе ст. 1–2. овог члана не примењују се на правне послове за које је посебним законом предвиђено да се не могу предузети у електронској форми.

Уговори и други правни послови за које је посебним законом предвиђено да се сачињавају у форми овере потписа, јавно потврђене (солемнизоване) исправе, или у форми јавнобележничког записа не могу се сачинити у складу са ст. 1–2. овог члана већ у складу са прописима којима се уређује овера потписа, потврђивање и сачињавање исправа о правним пословима.

2. Електронски временски жиг

Услови за квалификоване електронске временске жигове

Члан 62.

Квалификовани електронски временски жиг мора:

- 1) да је повезан са координисаним универзалним временом (UTC) тако да се спречава свака могућност промене података која се не може открити;
- 2) да је заснован на прецизном временском извору;
- 3) да је издат од стране пружаоца услуге издавања квалификованог временског жига;
- 4) да је потписан, односно печатиран од стране пружаоца услуге издавања квалификованог временског жига помоћу напредног електронског потписа или напредног електронског печата.

Министарство прописује ближе услове за квалификоване електронске временске жигове.

Правно дејство електронског временског жига

Члан 63.

Електронском временском жигу не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификован временски жиг.

За квалификовани електронски временски жиг и податке којима је тај временски жиг придружен важи правна претпоставка тачности датума и времена исказаног у временском жигу и очуваности интегритета тих података у односу на тај временски тренутак.

3. Електронска достава

Услови за пружање услуге квалификоване електронске доставе

Члан 64.

Услуга квалификоване електронске доставе мора:

- 1) да је пружана од стране једног или више пружаоца квалификованих услуга од поверења;
- 2) да, уз висок ниво поузданости, обезбеђује идентификацију пошиљаоца;
- 3) да обезбеђује идентификацију примаоца приликом доставе података;

4) у процесу слања и пријема електронске поруке, да користи напредни електронски потпис или напредни електронски печат пружаоца услуге квалификоване електронске доставе у сврху спречавања непримећене промене података;

5) да обезбеди да измена података извршена у сврху слања или пријема података мора бити јасно назначена пошиљаоцу и примаоцу;

6) да обезбеди да време и датум слања, пријема и евентуалне измене података морају бити назначени квалификованим електронским временским жигом;

7) да, у случају да се подаци преносе између два или више пружалаца услуге квалификоване електронске доставе, обезбеди да се услови из овог става примењују на сваког од њих.

Ако поступак слања и пријема података испуњава норме и стандарде прописане у члану 65. став 7. сматра се да су испуњени услови из става 1. овог члана.

Потврда о електронској достави

Члан 65.

Пружалац услуге је у обавези да приликом пружања услуге квалификоване електронске доставе изда две потврде пошиљаоцу, и то:

- 1) потврду да је примио електронску поруку пошиљаоца и проследио је примаоцу;
- 2) потврду да је прималац преузео достављену електронску поруку.

Потврде из става 1. овог члана пружалац услуге доставља аутоматски у електронском облику потписане напредним електронским печатом, а на захтев их може издати у електронском или папирном облику.

Потврда из става 1. тач. 1) и 2) овог члана садржи:

- 1) идентификациону ознаку електронске поруке коју је доделио пружалац услуге;
- 2) податке о пошиљаоцу и примаоцу, који од података о личности могу да садрже податке из члана 43. став 1. тачка 3) овог закона као и адресу за електронску доставу;
- 3) податке који повезују потврду са садржајем електронске поруке;
- 4) датум и време пријема и прослеђивања електронске поруке од стране пружаоца услуге, односно датум и време преузимања достављене електронске поруке од стране примаоца.

Потврда из става 1. тачка 2) овог члана сматра се доставницом у електронском облику у смислу закона којим се уређује управни поступак, при чему се датум и време преузимања из става 3. тачка 4) овог члана сматрају датумом и временом уручења.

Датум и време пријема поднеска који је странка у управном поступку упутила органу путем квалификоване електронске доставе сматра се да је датум и време преузимања из става 3. тачка 4) овог члана.

Ако дође до техничких проблема приликом електронског достављања односно пријема података, пружалац услуге квалификоване електронске доставе дужан је да о томе обавести пошиљаоца и примаоца.

Министарство прописује ближе услове, стандарде, спецификације и процедуре за пружање услуге квалификоване електронске доставе из члана 64. овог закона и садржај потврда из става 3. овог члана.

Размена електронских порука између пружалаца услуге квалификоване електронске доставе

Члан 66.

Пружаоци услуге квалификоване електронске доставе у обавези су да приликом пружања услуге квалификоване електронске доставе омогуће пријем и слање порука и када је пошиљалац или прималац поруке корисник другог пружаоца услуге квалификоване електронске доставе.

Размена електронских порука из става 1. овог члана врши се на начин уређен прописом из члана 55. овог закона који ближе уређује услове за услуге квалификоване електронске доставе.

Правно дејство услуге електронске доставе

Члан 67.

Подацима послатим или примљеним путем услуге електронске доставе не може се оспорити правна снага и допуштеноост као доказ у правном промету само из разлога што су у електронској форми или из разлога што не испуњавају све услове услуге квалификоване електронске доставе.

За податке из електронске поруке послате или примљене путем услуге квалификоване електронске доставе важи правна претпоставка интегритета података, слања података од назначеног пошиљаоца, пријем од стране назначеног примаоца, поузданости датума и времена слања или примања.

4. Аутентификација веб сајтова

Квалификовани сертификати за аутентификацију веб сајтова

Члан 68.

Аутентификација веб сајта користи се за потврду идентитета веб сајта од стране корисника квалификоване услуге од поверења, којом се гарантује његова поузданост коришћења.

За аутентификацију веб сајта користи се квалификовани сертификат који издаје пружалац квалификованих услуга од поверења, у складу са законом.

Квалификовани сертификат за аутентификацију веб сајта мора да испуњава услове из члана 69. овог закона.

Садржај квалификованих сертификата за аутентификацију веб сајтова

Члан 69.

Квалификовани сертификати за аутентификацију веб сајтова садрже:

1) ознаку, која се може препознати при аутоматској обради, да је сертификат издат као квалификовани сертификат за аутентификацију веб сајтова;

2) скуп података који недвосмислено представљају пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова, што обавезно укључује државу седишта, пословно име и матични број тог пружаоца услуге;

3) име и презиме или псеудоним физичког лица коме је издат сертификат, односно пословно име и матични број правног лица коме је издат сертификат;

4) адресу, односно седиште физичког или правног лица коме је издат сертификат;

5) назив интернет домена физичког или правног лица коме је издат сертификат;

6) податке о почетку и крају рока важења сертификата;

7) идентификациону ознаку сертификата која мора да буде јединствена за пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова;

8) напредан електронски потпис, или напредан електронски печат пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова;

9) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа, односно напредног електронског печата из тачке 8) овог става;

10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата.

Квалификовани сертификати за аутентификацију веб сајтова треба да испуне искључиво захтеве утврђене ставом 1. овог члана.

Министарство прописује ближе услове, стандарде, спецификације и процедуре за пружање услуге издавања квалификованог сертификата за аутентификацију веб сајтова.

Информациона безбедност веб сајтова

Члан 70.

Пружалац услуга претраге веб сајтова путем интернет претраживача дужан је да обезбеди подршку, односно интероперабилност квалификованих сертификата за аутентификацију веб сајтова, као и да се атрибути потврђени у сертификату приказују на начин прилагођен корисницима.

Пружалац услуга из става 1. овог члана може предузети додатне мере предострожности ако посумња у рањивост једног или више квалификованих сертификата за аутентификацију веб сајтова, о чему, без одлагања, обавештава Министарство, Регистар националног интернет домена Србије и пружаоца квалификоване услуге од поверења који је издао сертификат.

По пријему обавештења из става 2. овог члана Министарство спроводи инспекцијски надзор и одлучује да ли је потребно опозвати сертификат који је предмет надзора.

5. Електронска потврда атрибута

Квалификована електронска потврда атрибута

Члан 71.

Квалификовану електронску потврду атрибута издаје пружалац квалификоване услуге од поверења регистрован за пружање те услуге.

Квалификована електронска потврда атрибута садржи:

- 1) ознаку, која се може препознати при аутоматској обради, да је потврда издата као квалификована електронска потврда атрибута;
- 2) скуп података који недвосмислено идентификују пружаоца услуге од поверења који издаје квалификовану електронску потврду атрибута, укључујући податке о држави седишта, пословном имену и матичном броју;
- 3) скуп података који недвосмислено идентификују лице на које се односе потврђени атрибути, односно његов псеудоним ако га користи;
- 4) потврђен атрибут, односно атрибуте, и по потреби додатне информације о атрибуту;
- 5) податке о почетку и крају рока важења потврде;
- 6) идентификациону ознаку потврде јединствену за пружаоца квалификоване услуге од поверења и, по потреби, идентификациону ознаку, односно назнаку шеме аутентичног извора атрибута као и назив тог извора, односно назив евиденције, односно регистра у коме се води атрибут;
- 7) квалификован електронски потпис, односно квалификован електронски печат пружаоца квалификоване услуге од поверења који издаје потврду;
- 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става;
- 9) информације или локација услуге где се проверава валидност квалификоване електронске потврде.

Квалификована електронска потврда атрибута која је опозвана након почетног издавања трајно губи валидност од тренутка опозива.

Министарство ближе прописује стандарде, спецификације и процедуре за пружање услуге издавања квалификоване електронске потврде атрибута.

Провера атрибута упоређивањем са изворним евиденцијама

Члан 72.

Пружалац квалификоване услуге од поверења који издаје електронске потврде атрибута, на захтев корисника, може вршити проверу аутентичности атрибута из изворних евиденција за следеће атрибуте о кориснику:

- 1) адресу пребивалишта, односно боравишта;

- 2) године;
- 3) пол;
- 4) брачно стање;
- 5) сродство;
- 6) чланове домаћинства;
- 7) држављанство;
- 8) ниво образовања и титуле;
- 9) занимање;
- 10) стручне лиценце;
- 11) овлашћења за заступање физичких и правних лица;
- 12) податке о адвокатима, јавним извршитељима, односно бележницима;
- 13) пословно име, адресу седишта као и финансијске податке правног лица, односно физичког лица у својству регистрованог субјекта.

Министарство ближе прописује стандарде, спецификације и процедуре за оцену усаглашености пружаоца услуге издавања електронске потврде атрибута.

Електронска потврда атрибута коју издаје орган јавне власти

Члан 73.

Орган јавне власти који води изворну евиденцију одређеног атрибута издаје, сам или преко овлашћеног лица, електронску потврду атрибута која садржи:

- 1) ознаку, која се може препознати при аутоматској обради, да је потврда издата као електронска потврда атрибута коју издаје орган јавне власти;
- 2) скуп података који недвосмислено идентификују орган јавне власти који издаје електронску потврду атрибута, пословно име и матични број;
- 3) скуп података који недвосмислено идентификују лице на које се односи потврђени атрибут а ако се користи псеудоним, то мора бити јасно назначено;
- 4) потврђен атрибут, односно атрибуте, и по потреби додатне информације о атрибуту;
- 5) податке о почетку и крају рока важења потврде;
- 6) јединствена идентификациона ознака и назив евиденције, односно регистра у којем се атрибут води;
- 7) квалификован електронски потпис овлашћеног лица, односно квалификован електронски печат органа који издаје потврду;
- 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става;
- 9) локацију на којој се може проверити валидност квалификоване електронске потврде.

Електронска потврда атрибута која је опозвана након издавања трајно губи валидност од тренутка опозива.

Орган јавне власти који издаје електронску потврду атрибута из става 1. овог члана дужан је да испуни услове из члана 36. овог закона који се односе на пружаоца квалификоване услуге од поверења.

Министарство ближе прописује стандарде, спецификације и процедуре за оцену усаглашености пружаоца услуге издавања електронске потврде атрибута коју издаје орган јавне власти.

Електронске потврде атрибута у оквиру дигиталног идентификационог новчаника

Члан 74.

Пружалац услуге од поверења који издаје електронске потврде атрибута дужан је да на захтев корисника дигиталног идентификационог новчаника изда електронску потврду атрибута коју корисник може сачувати и користити у свом дигиталном идентификационом новчанику.

Пружалац услуге од поверења издавања квалификоване електронске потврде атрибута мора испуњавати услове за дигитални идентификациони новчаник из чл. 15. и 16. овог закона.

Правно дејство електронске потврде атрибута

Члан 75.

Електронској потврди атрибута не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику, односно због тога што не испуњава услове за квалификовану електронску потврду атрибута.

Квалификована електронска потврда атрибута и потврда атрибута коју издаје орган јавне власти имају пуноважност и доказну снагу као и издате потврде, односно исправе у папирном облику.

Потврда атрибута коју издаје орган јавне власти може бити призната у другој држави или међународној организацији ако је то предвиђено међународним споразумом који закључи република Србија са другом државом или међународном организацијом.

Заштита података о личности при издавању електронских потврда атрибута

Члан 76.

Подаци о личности који се обрађују приликом издавања електронске потврде атрибута као и квалификоване електронске потврде атрибута не смеју се комбиновати са другим подацима о личности који се обрађују приликом пружања других услуга од поверења.

Подаци о личности који се обрађују приликом издавања електронске потврде атрибута чувају се логички одвојено од других података које чува пружалац услуге од поверења.

Пружалац квалификоване услуге од поверења дужан је да функционално раздвоји услугу издавања квалификоване електронске потврде атрибута од других услуга које пружа.

6. Електронско архивирање документа

Квалификована услуга електронског архивирања

Члан 77.

Пружалац квалификоване услуге од поверења електронског архивирања дужан је да:

- 1) се региструје као пружалац квалификоване услуге од поверења у складу са законом;
- 2) примењује поступке и користи технологије којима се обезбеђује трајност и читљивост података и електронских докумената најмање током законом прописаног рока, односно рока утврђеног листом категорија архивске грађе и документарног материјала са роковима чувања, уз очување интегритета података;
- 3) обезбеди да се подаци и електронска документа заштите од губитка и промена, осим података које се односе на медиј или електронски облик;
- 4) поуздајућој страни омогући аутоматско преузимање потврде потписане, односно печатране квалификованим електронским потписом, односно печатом, којом се гарантује интегритет података и електронских докумената преузетих из електронског архива у периоду чувања.

Министарство ближе прописује услове, стандарде, спецификације и процедуре које је потребно да испуни пружалац квалификоване услуге од поверења електронског архивирања.

Правно дејство електронског архивирања

Члан 78.

Подацима и електронским документима који су електронски архивирани не може се оспорити пуноважност или доказна снага само због тога што су у електронском облику, односно због тога што нису чувани коришћењем квалификоване услуге електронског архивирања.

Пружалац квалификоване услуге од поверења електронског архивирања гарантује интегритет и порекло података и електронских докумената који су чувани у електронском архиву за период чувања.

7. Електронска евиденција

Квалификована услуга вођења електронске евиденције

Члан 79.

Пружалац квалификоване услуге од поверења вођења електронске евиденције дужан је да:

- 1) успоставља и води самостално, односно са другим пружаоцима услуге, електронску евиденцију;
- 2) утврђује порекло записа података у евиденцији;
- 3) обезбеди јединствен секвенцијални хронолошки редослед уписа података у евиденцију;
- 4) бележи податке тако да је свака накнадна промена података одмах уочљива, чиме се обезбеђује њихова целовитост, односно интегритет током времена.

Евиденција коју води орган јавне власти сматра се квалификованом услугом вођења електронске евиденције ако испуњава услове из става 1. овог члана и ако се води у складу са законом којим се уређује електронска управа.

Министарство ближе прописује услове, стандарде, спецификације и процедуре за пружање квалификоване услуге од поверења вођења електронске евиденције.

Правно дејство електронских евиденција

Члан 80.

Подацима из електронских евиденција не може се оспорити пуноважност или доказна снага само због тога што су у електронском облику, односно због тога што не испуњавају захтеве квалификоване услуге вођења електронске евиденције.

Пружалац квалификоване услуге од поверења вођења електронске евиденције гарантује јединствен и тачан хронолошки редослед, као и целовитост, односно интегритет података које евидентира.

У циљу ефикасније размене и ажурирања података, органи могу користити механизам за аутоматско обавештавање о променама у подацима, како би се подаци у електронским евиденцијама, односно регистрима аутоматизовано ажурирали без потребе за појединачним интервенцијама, у складу са законом којим се уређује метарегистар.

VI. ИНСПЕКЦИЈСКИ НАДЗОР

Послови инспекције за електронску идентификацију и услуге од поверења у електронском пословању

Члан 81.

Инспекција за електронску идентификацију и услуге од поверења у електронском пословању врши инспекцијски надзор над применом овог закона и радом пружалаца услуга електронске идентификације и пружалаца услуга од поверења (у даљем тексту: пружаоци услуга) преко инспектора за електронску идентификацију и услуге од поверења (у даљем тексту: инспектор).

У оквиру инспекцијског надзора пружалаца услуга инспектор утврђује да ли су испуњени услови прописани овим законом и прописима донетим за спровођење овог закона.

Овлашћења инспектора

Члан 82.

Инспектор је овлашћен да у поступку инспекцијског надзора:

- 1) налаже отклањање утврђених неправилности и за то остави рок;
- 2) забрањује употребу неадекватних поступака и инфраструктуре, и даје рок пружаоцу услуга у којем је дужан да обезбеди адекватне поступке и инфраструктуру;
- 3) привремено забрањује вршење услуге пружаоца услуга до отклањања неадекватности поступака и инфраструктуре;
- 4) наређује привремени опозив неког или свих сертификата издатих од стране пружаоца услуге, ако постоји основана сумња да се ради о неадекватном поступку или фалсификату.

VII. КАЗНЕНЕ, ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

1. Казнене одредбе

Члан 83.

Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај пружалац квалификоване услуге од поверења – правно лице ако:

- 1) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга од поверења (члан 32. став 1);
- 2) без одлагања, а најкасније у року од 24 сата од сазнања, не обавести Министарство о сваком нарушавању безбедности или губитку интегритета услуге који имају значајан утицај на пружање услуга од поверења (члан 32. став 3);
- 3) о повреди безбедности или губитку интегритета услуге, без одлагања, не обавести корисника услуге од поверења, ако би угрожавање безбедности или губитак интегритета услуге од поверења могло неповољно утицати на кориснике услуга од поверења (члан 32. став 4);
- 4) пре закључења уговора из члана 35. став 1. овог закона не обавести лице које је поднело захтев за пружање квалификоване услуге од поверења о свим важним околностима коришћења услуге из члана 35. став 2. тач. 1)–3) овог закона (члан 35. став 2);
- 5) не испуњава услове из члана 36. овог закона;
- 6) при издавању квалификованог сертификата за услуге од поверења не провери податке о идентитету физичког односно правног лица који су садржани у квалификованом сертификату, у складу са чланом 38. став 1. овог закона (члан 38. ст. 1. и 2);
- 7) не изврши проверу испуњености услова пре почетка пружања квалификованих услуга од поверења, односно најмање једном у 24 месеца (члан 40. став 3);
- 8) не изврши налог за ванредно оцењивање испуњености услова (члан 40. став 5);
- 9) пре отпочињања пружања квалификованих услуга од поверења не буде уписан у Регистар пружаоца квалификованих услуга од поверења (члан 41. став 3);
- 10) издавалац квалификованих електронских сертификата, који намерава да престане са обављањем делатности, о намери раскида уговора не обавести сваког корисника квалификоване услуге од поверења и Министарство најмање три месеца пре настанка о намераваном престанку обављања делатности (члан 42. став 1);
- 11) у случају престанка са обављањем послова не обезбеди код другог пружаоца услуга од поверења наставак обављања услуге за кориснике којима је издао сертификат, или не опозове све издате сертификате и о предузетим мерама одмах не обавести Министарство (члан 42. став 2);
- 12) не достави сву документацију у вези са обављањем услуга од поверења другом издаваоцу на кога преноси обавезе обављања једне или више услуга од поверења, односно Министарству (члан 42. ст. 3. и 4);
- 13) квалификовани електронски сертификат не садржи све податке из члана 50. став 1. овог закона (члан 50. став 1);

14) издавалац квалификованих сертификата не изврши опозив издатих сертификата, у случајевима из члана 51. став 1. (члан 51. став 1) овог закона;

15) издавалац квалификованих сертификата не обавести корисника квалификоване услуге од поверења о опозиву сертификата у року од 24 часа од примљеног обавештења, односно настанка околности због којих се сертификат опозива (члан 51. став 2);

16) издавалац квалификованих сертификата не чува комплетну документацију о издатим и опозваним квалификованим сертификатима као средство за доказивање и верификацију у управним, судским и другим поступцима најмање десет година по престанку важења сертификата (члан 52.);

17) не обезбеди пријем и слање порука и када је пошиљалац или прималац поруке корисник другог пружаоца услуге квалификоване електронске доставе (члан 66. став 1);

18) пружалац услуга који омогућава претрагу веб сајтова путем интернет претраживача не обезбеди подршку, односно интероперабилност квалификованих сертификата за аутентификацију веб сајтова, као и да се подаци о идентитету и додатни атрибути потврђени у сертификату приказују на начин прилагођен корисницима у складу са чланом 70. овог закона;

19) не издаје квалификовану електронску потврду атрибута са садржајем из члана 71. став 2. овог закона;

20) не пружа квалификовану услугу електронског архивирања у складу са чланом 77. овог закона;

21) не пружа квалификовану услугу од поверења вођења електронске евиденције у складу са чланом 79. овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге од поверења новчаном казном од 5.000 до 100.000 динара.

За прекршај из става 1. овог члана казниће се пружалац услуге од поверења – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара.

Члан 84.

Новчаном казном од 50.000 до 200.000 динара казниће се за прекршај корисник квалификоване услуге од поверења – правно лице ако, у случају промене података из става 1. члана 38. овог закона не обавести без одлагања пружаоца квалификоване услуге од поверења.

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу новчаном казном од 5.000 до 50.000 динара.

За прекршај из става 1. овог члана казниће се корисник услуге од поверења – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 100.000 динара.

За прекршај из става 1. овог члана казниће се корисник услуге од поверења – физичко лице новчаном казном од 5.000 до 50.000 динара.

Члан 85.

Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај регистрован пружалац услуге електронске идентификације – правно лице ако:

1) дигитални идентификациони новчаник не испуњава услове из члана 15. и 16. овог закона;

2) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно коришћење дигиталног идентификационог новчаника из члана 15. ст. 1. и 2., члана 16. став 7. и члана 19. овог закона;

3) пре отпочињања коришћења дигиталног идентификационог новчаника не буде уписан у регистар поуздајуће стране за коришћење дигиталног идентификационог новчаника у складу са чланом 17. овог закона;

4) шема електронске идентификације не испуњава услове из члана 21. овог закона;

5) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга из члана 26. став 2. овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге електронске идентификације новчаном казном од 5.000 до 100.000 динара.

За прекршај из става 1. овог члана казниће се пружалац услуге електронске идентификације – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара.

Члан 86.

Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај пружалац услуге из члана 64. овог закона ако не поступи по налогу инспектора у остављеном року из члана 82. став 1. овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге новчаном казном од 5.000 до 100.000 динара.

За прекршај из става 1. овог члана казниће се пружалац услуге – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара.

Члан 87.

Новчаном казном од 5.000 до 100.000 динара казниће се за прекршај одговорно лице у државном органу, као и органу аутономне покрајине или јединице локалне самоуправе ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност, односно оспори доказну снагу електронском документу сачињеном у складу са овим законом, односно дигитализованог акта овереног у складу са чланом 11. овог закона, само због тога што је достављен у таквом формату (члан 7).

Новчаном казном од 20.000 до 150.000 динара казниће се за прекршај одговорно лице у државном органу, као и органу аутономне покрајине или јединице локалне самоуправе, ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност електронском документу, укључујући и акте органа јавних власти, потписаном квалификованим електронским потписом или квалификованим електронским печатом, ако је за пуноважност тог документа прописана обавеза својеручног потписивања, односно стављања печата (чл. 60. и 61).

Новчаном казном од 20.000 до 150.000 динара казниће се за прекршај одговорно лице у органу јавне власти ако не испуњава услове из члана 73. овог закона за издавање електронске потврде атрибута у чијим се евиденцијама изворно води потврђен атрибут, односно која се издаје у његово име из члана 73. овог закона.

Новчаном казном од 20.000 до 150.000 динара казниће се за прекршај одговорно лице у органу јавне власти ако не издаје електронске потврде атрибута у чијим се евиденцијама изворно води потврђен атрибут, односно која се издаје у његово име у складу са чланом 73. овог закона.

Новчаном казном од 5.000 до 100.000 динара казниће се за прекршај одговорно лице у органу јавне власти ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност, односно оспори доказну снагу електронској потврди атрибута сачињеној у складу са овим законом, (члан 73).

Члан 88.

Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај правно лице које је орган јавне власти у смислу овог закона ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност, односно оспори доказну снагу електронском документу сачињеном у складу са овим законом, односно дигитализованог акта овереног у складу са чланом 11. овог закона, само због тога што је достављен у таквом формату (члан 7).

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу из става 1. овог члана новчаном казном од 5.000 до 100.000 динара.

За прекршај из става 1. овог члана казниће се орган јавне власти ако је физичко лице новчаном казном од 5.000 до 100.000 динара.

Новчаном казном од 100.000 до 2.000.000 динара казниће се за прекршај правно лице које је орган јавне власти у смислу овог закона ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност електронском документу, укључујући и акте органа јавних власти, потписаном квалификованим електронским потписом или квалификованим електронским печатом, ако је за

пуноважност тог документа прописана обавеза својеручног потписивања, односно стављања печата (чл. 60. и 61).

За прекршај из става 4. овог члана казниће се и одговорно лице у правном лицу из става 4. овог члана новчаном казном од 20.000 до 150.000 динара.

За прекршај из става 4. овог члана казниће се орган јавне власти ако је физичко лице новчаном казном од 20.000 до 150.000 динара.

Новчаном казном од 100.000 до 2.000.000 динара казниће се за прекршај правно лице које је орган јавне власти ако у поступку који спроводи у вршењу јавних овлашћења не призна пуноважност, односно оспори доказну снагу електронској потврди атрибута сачињеној у складу са овим законом, (члан 73).

2. Прелазне и завршне одредбе

Спровођење закона

Члан 89.

Подзаконска акта из члана 16. став 10, члана 17. став 9, члана 18. став 6, члана 19. став 6, члана 21. став 2, члана 22. став 5, члана 23. став 11, члана 32. став 6, члана 36. став 6, члана 41. став 10, члана 45. став 6, члана 46. став 4, члана 47. став 4, члана 50. став 3, члана 53. став 6, члана 54. став 2, члана 55. став 10, члана 56. став 4, члана 57. став 4, члана 58. став 2, члана 59. став 2, члана 62. став 2, члана 65. став 7, члана 71. став 4, члана 72. став 2, члана 73. став 4, члана 77. став 2, члана 79. став 3. овог закона донеће се у року од 12 месеци од дана ступања на снагу овог закона.

Успостављање дигиталног идентификационог новчаника

Члан 90.

Канцеларија ће успоставити дигитални идентификациони новчаник из члана 15. овог закона у року од 12 месеци од дана ступања на снагу овог закона.

Престанак важења досадашњих прописа, наставак примене подзаконских аката и наставак рада на основу претходне регистрације

Члан 91.

Даном ступања на снагу овог закона престаје да важи Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021).

Подзаконски акти донети на основу закона из става 1. овог члана примењиваће се и после престанка важења наведених закона, све до доношења одговарајућих прописа сагласно овом закону, осим ако су у супротности са одредбама овог закона.

Даном ступања на снагу овог закона пружаоци услуга електронске идентификације и шема електронске идентификације који су регистровани на основу Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као регистровани пружаоци услуга електронске идентификације за шеме електронске идентификације које су регистроване у складу са тим законом.

Даном ступања на снагу овог закона пружаоци квалификованих услуга од поверења који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге за коју су били регистровани.

Даном ступања на снагу овог закона пружаоци услуга од поверења дуготрајног чувања који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге електронског архивирања и квалификовани пружаоци услуге чувања квалификованог електронског потписа, односно печата.

Пружаоци услуга из става 3. овог члана дужни су да у року од 24 месеци од дана ступања на снагу овог закона ускладе своје пословање са одредбама овог закона и доставе Министарству сертификат о усаглашености из члана 23. овог закона.

Пружаоци услуга од поверења из ст. 4. и 5. овог члана дужни су да у року од 24 месеци од дана ступања на снагу овог закона ускладе своје пословање са одредбама овог закона и доставе Министарству извештај о оцењивању усаглашености из члана 40. овог закона.

Министарство врши оцењивање усаглашености из члана 40. овог закона до акредитације првог тела за оцењивање усаглашености, у складу са прописима.

Даном ступања на снагу овог закона средства за креирање електронског потписа односно печата уписана у регистар квалификованих средстава за креирање електронских потписа и електронских печата на основу Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) уписују се у регистар из члана 55. овог закона.

Ступање на снагу закона

Члан 92.

Овај закон ступа на снагу осам дана од дана објављивања у „Службеном гласнику Републике Србије”.

ОБРАЗЛОЖЕЊЕ

I. УСТАВНИ ОСНОВ

Уставни основ за доношење Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању садржан је у члану 97. тачка 6. и 17. Устава Републике Србије, којим је прописано да Република Србија уређује и обезбеђује систем у области електронских комуникација, информационог друштва и заштите података, као и правни положај привредних субјеката и друге односе од општег интереса за Републику.

II. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА

Свеобухватна дигитална трансформација јавне управе, привреде и друштва у целини захтева правни оквир који обезбеђује поузданост, сигурност и правну извесност у електронском пословању. Важећи Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, бр. 94/2017 и 52/2021) примењивао се више од шест година, током којих је дошло до значајних технолошких и регулаторних промена у области дигиталних услуга, што је створило потребу за доношењем новог закона.

Постојећи законски оквир више не обезбеђује довољно флексибилности и обухватности у домену електронске идентификације, електронског потписа и других услуга од поверења, посебно у контексту развоја дигиталног идентитета и увођења дигиталног идентификационог новчаника као кључног механизма за једноставно и сигурно електронско пословање.

Унапређење европског регулаторног оквира, посебно увођење Уредбе (ЕУ) бр. 150/2024 – eIDAS 2, донело је нове концепте у области електронске идентификације и дигиталних услуга од поверења. Као држава кандидат за чланство у Европској унији, Република Србија има обавезу да своје прописе усклади са овом уредбом, ради обезбеђивања интероперабилности система и признавања електронских докумената и идентификационих шема у прекограничном промету.

Нови закон уводи и низ нових института, као што су:

- дигитални идентификациони новчаник као средство за безбедно управљање дигиталним идентитетом и атрибутима,
- електронске потврде атрибута,
- квалификоване услуге електронског архивирања,
- услуге дуготрајног чувања електронских потписа и печата,
- вођење електронских евиденција као услуге од поверења,
- чиме се заокружује правни оквир за потпуно дигитално пословање.

Доношење новог закона има за циљ да:

- повећа правну сигурност у електронској комуникацији,

- унапреди услове за коришћење електронских докумената у јавним и пословним процесима,
- ојача поверење грађана и привреде у електронске услуге,
- усклади домаће прописе са правом ЕУ, посебно eIDAS 2,
- омогући ефикасно функционисање дигиталне јавне управе и дигиталног тржишта Србије.

1. Проблеми које закон треба да реши

- Унапређење законских решења и отклањање уочених недостатака важећег Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, који су се појавили током његове примене у пракси;
- Потреба за успостављањем правног основа за дигитални идентитет и дигитални идентификациони новчаник, у складу са новом Уредбом (ЕУ) бр. 150/2024 (eIDAS 2), ради обезбеђивања јединственог и безбедног система електронске идентификације;
- Обезбеђивање интероперабилности електронских шема идентификације и признавања електронских докумената и услуга од поверења у прекограничном промету;
- Јачање поверења у електронско пословање кроз увођење нових квалификованих услуга од поверења, као што су електронско архивирање, дуготрајно чување квалификованих електронских потписа и печата, као и издавање електронских потврда атрибута;
- Унапређење безбедности и заштите података у процесима електронске идентификације и пружању услуга од поверења, уз јасно прописане рокове чувања и начела поступања са подацима;
- Обезбеђивање услова за развој тржишта услуга од поверења и дигиталних производа, подстицањем конкуренције, технолошких иновација и улагања у безбедну дигиталну инфраструктуру;
- Усаглашавање домаћег правног оквира са прописима Европске уније, ради остваривања прекограничног поверења и пуне интеграције Републике Србије у јединствено европско дигитално тржиште.

2. Циљеви који се законом постижу

Овим законом постиже се унапређење правног и институционалног оквира у области електронског пословања, усклађивањем са новим регулаторним решењима Европске уније, нарочито са Уредбом (ЕУ) бр. 150/2024 (eIDAS 2).

Циљ је да се обезбеди јединствен, поуздан и сигуран систем електронске идентификације и електронских услуга од поверења, који ће омогућити пуну интероперабилност у прекограничном промету електронских докумената, као и правну сигурност у њиховој употреби у домаћем правном систему.

Законом се постиже:

- стварање услова за успостављање и примену дигиталног идентитета и дигиталног идентификационог новчаника, као основних инструмената за сигурну електронску комуникацију и пружање јавних и пословних услуга;
- унапређење поверења у електронске трансакције кроз јачање безбедности, интегритета и заштите података у електронском пословању;
- јачање институционалних капацитета и надзорног механизма у области електронске идентификације и услуга од поверења, ради ефикасне примене прописа и заштите права корисника;
- унапређење конкурентности и развој тржишта услуга од поверења, подстицањем иновација, нових дигиталних решења и инвестирања у безбедну ИКТ инфраструктуру;
- успостављање правног оквира за прекогранично признавање електронских докумената, потписа и печата, чиме се омогућава пуно учешће Републике Србије у јединственом дигиталном тржишту ЕУ.

Овим законом се ствара модеран, стабилан и технолошки неутралан систем електронског пословања, који омогућава да Република Србија активно учествује у европском дигиталном простору и убрза процес дигиталне трансформације јавне управе, привреде и друштва у целини.

3. Разматране могућности да се проблем реши и без доношења закона

Имајући у виду да је Република Србија, у поступку придруживања Европској унији, преузела обавезу да своје законодавство усклади са прописима Европске уније, посебно са новом Уредбом (ЕУ) бр. 150/2024 (eIDAS 2), у области електронске идентификације и услуга од поверења, није било могуће постићи потребно усклађивање без доношења новог закона.

Постојећи законски оквир више не омогућава примену нових технолошких и регулаторних решења, нити успоставља институционалне и техничке услове за функционисање дигиталног идентитета, дигиталног идентификационог новчаника и нових квалификованих услуга од поверења.

Како се ради о свеобухватној области која захтева увођење нових института, техничких стандарда, надлежности и механизма надзора, као и успостављање прекограничне интероперабилности у складу са правом Европске уније, ниједан други инструмент осим доношења новог закона није адекватан за постизање ових циљева.

4. Зашто је доношење закона најбољи начин за решавање проблема

Закони, а нарочито системски, представљају основ за развој области електронског пословања и дигиталне трансформације друштва.

Доношењем овог закона обезбеђује се јединствен и стабилан правни оквир за електронски документ, електронску идентификацију и услуге од поверења, који ће омогућити потпуно дигитално пословање у јавном и приватном сектору, уз поуздану правну заштиту и једнакост електронског и папирног облика документа.

Нови закон треба да омогући адекватан одговор на технолошке изазове и ризике у вези са употребом електронских докумената, потписа и идентификационих средстава, као и да подстакне развој безбедног и поверења вредног дигиталног окружења.

Такође, изражена је потреба да законска решења буду флексибилна и технолошки неутрална, како би могла да прате брзи развој дигиталних технологија, као и да се заснивају на међународним прописима и стандардима Европске уније, посебно на Уредби (ЕУ) бр. 150/2024 (eIDAS 2) и пратећим актима.

Доношење овог закона није само најбољи, већ и једини одговарајући начин за успостављање правног оквира који обезбеђује пуно усклађивање са правом Европске уније, као и за даље унапређење дигиталног пословања, правне сигурности и поверења у електронску комуникацију у Републици Србији.

III. ОБЈАШЊЕЊЕ ПОЈЕДИНИХ РЕШЕЊА

I. УВОДНЕ ОДРЕДБЕ

Члан 1. (Предмет закона)

Овим чланом се утврђује предмет уређивања електронски документ, електронска идентификација и услуге од поверења у електронском пословању.

Члан 2. (Значење појединих израза)

Успостављају се дефиниције (електронски документ, електронско пословање, електронска трансакција, производ, итд.), чиме се обезбеђује правна извесност у примени и тумачењу појмова у наставку закона.

Члан 3. (Примена)

Прецизира се да пружаоци услуга од поверења поступају по овом закону, док се изузимају затворени системи без утицаја на трећа лица (интерни/ограничени круг), чиме се одржава пропорционалност и технолошка неутралност.

Члан 4. (Обрада и заштита података)

Наглашава се усклађеност са прописима о заштити података о личности и истиче начело минимизације и рокови чувања, ради јасног правног основа за обраду у услугама е-идентификације и од поверења.

Члан 5. (Пристанак на идентификацију и аутентификацију)

Поступци е-идентификације/аутентификације покрећу се на захтев лица, осим ако је другачије прописано.

Члан 6. (Доступност и приступ особама са инвалидитетом)

Услуге од поверења, услуге електронске идентификације и производи који се користе за пружање тих услуга једнако су доступни и особама с инвалидитетом.

II. ЕЛЕКТРОНСКИ ДОКУМЕНТ

Члан 7. (Пуноважност и доказна снага)

Електронском документу не може се оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику.

Члан 8. (Израда електронског документа)

Документ се израђује применом доступних ИКТ технологија. Уколико је у питању документ који представља архивску грађу, мора задовољити услове за поуздану припрему за електронско чување.

Члан 9. (Форма приказа)

Разликују се унутрашња (техничко-програмска) и спољна (визуелно разумљиви приказ) форма, ако постоји потпис/печат, то мора бити јасно исказано.

Члан 10. (Оригинал и копија)

Оригиналом се сматра изворно електронски настали документ и његов истоветни дигитални запис, дигитализацијом папирног настаје електронска копија.

Члан 11. (Овера дигитализованог акта)

Уводе се кумулативни услови да дигитализовани акт има доказну снагу оригинала (надзор овлашћених лица/органа; потврда истоветности квалификованим електронским потписом/печатом), укључујући надлежност органа јавне власти.

Члан 12. (Овера одштампаног примерка електронског документа)

Одштампани примерак има исту доказну снагу ако је штампан под прописаним надзором и ако је потврђена истоветност на један од кумулативног наведених начина, уређен је и посебан режим за органе јавне власти.

Члан 13. (Потврда о пријему)

Утврђује се да је потврда доказ о пријему и да је издаје прималац или пружалац услуге електронске доставе.

Члан 14. (Дуплирање електронских докумената)

Утврђује се да се примљени електронски документ сматра се посебним документом, осим ако је више пута примљен истоветан документ и прималац је знао или је морао знати да је реч о истоветном документу.

III. ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА И ДИГИТАЛНИ ИДЕНТИТЕТ

Члан 15. – 19. (Дигитални идентификациони новчаник)

Чланови од 15. до 19. уређују дигитални идентификациони новчаник (ДИН): његове функције за безбедно и селективно управљање идентитетом/атрибутима, стандардизоване протоколе, псеудониме, потписивање/печат и увид у евиденције. ДИН издаје Канцеларија у оквиру шеме високог нивоа поузданости, уз интероперабилност, одвојено чување података и бесплатност за физичка лица:

поуздајуће стране се обавезно региструју и смеју тражити само пријављене податке, а посредници имају исте обавезе. Сертификацију ДИН спроводи акредитовано тело (важност 5 година, процена рањивости на 2 године), а у случају безбедносних инцидената Канцеларија привремено обуставља или повлачи ДИН/механизме, уз обавештавање корисника, поуздајућих страна и министарства.

Члан 20. – 29. (Шеме електронске идентификације)

Чланови 20. до 29. уређују шеме електронске идентификације, њихове нивое поузданости, регистрацију, сертификацију, употребу, одговорност, безбедност и прекограничну интероперабилност. Прописују се услови које шема мора испуњавати, од основног до високог нивоа поузданости, као и поступак уписа у регистар који води Министарство. Акредитована тела врше сертификацију техничких, организационих и безбедносних аспеката шема, а потврда важи пет година. Утврђује се да се регистроване шеме могу користити у електронском пословању и пред органима јавне власти, где високи ниво поузданости замењује потпис. Закон дефинише одговорност издаваоца и других учесника у поступку електронске идентификације, као и обавезу пружалаца услуга да примењују адекватне безбедносне мере и спроводе редовне процене ризика. Прописује се прекогранична сарадња, техничка и правна интероперабилност, заштита података и обавеза Канцеларије за информационе технологије и електронску управу да омогући бесплатан и недискриминаторан приступ релевантним хардверским и софтверским функцијама, као и признавање страних сертификата у складу са међународним стандардима и Уредбом eIDAS.

IV УСЛУГЕ ОД ПОВЕРЕЊА

Члан 30. – 34. (Одговорност пружаоца услуга од поверења и терет доказивања)

Чланови 30. до 34. уређују основне одредбе које се односе на услуге од поверења, одговорност њихових пружалаца и корисника, услове рада, као и надлежности Министарства.

Члан 35. – 47. (Квалификоване услуге од поверења)

Чланови 35. до 47. уређује се уговорни однос пружаоца и корисника уз обавезу претходног јасног информисања; посебни услови за квалификоване пружаоце (стручност, осигурање, безбедни системи, чување/обрада података, план прекида, локализација података, акта и пријаве промена); обавезна поуздана идентификација и верификација атрибута при издавању; периодично и ванредно оцењивање усаглашености, мера надзора и последице неиспуњавања услова; упис у регистар и услови за почетак/престанак пружања услуге, укључујући обавезе при гашењу издаваоца сертификата; обавеза органа јавне власти да подрже квалификоване сертификате и временске жигове свих регистрованих пружалаца; могућност да државни орган буде пружалац уз посебну проверу и упис; јавна листа квалификованих услуга са статусним догађајима и техничким условима објаве; знак поузданости и његов изглед/употреба до чланства у ЕУ; прекогранично признавање

услуга на основу међународног споразума/акта Владе и принципа реципроцитета (без електронског архивирања).

V ПОЈЕДИНЕ ВРСТЕ УСЛУГА ОД ПОВЕРЕЊА

Члан 48. (Врсте услуга од поверења)

Члан 49. - 61. (Напредни електронски потпис и напредни електронски печат)

Чланови 49–61 уређују целокупан правни и технички оквир за електронски потпис и електронски печат у Републици Србији. Они дефинишу шта је напредни и квалификовани електронски потпис/печат, које услове морају да испуне (повезаност са потписником, идентификација, искључива контрола и интегритет података), као и садржај квалификованог електронског сертификата. Такође се прописују правила за издавање, важење, опозив и суспензију сертификата, обавезе пружалаца услуга од поверења, чување документације и технички захтеви за квалификована средства за креирање електронских потписа и печата, укључујући и услуге на даљину и њихову сертификацију и упис у регистре.

Ови чланови даље уређују поступке валидације електронских потписа и печата, као и квалификоване услуге валидације и чувања, како би се обезбедила поузданост и доказна вредност потписаних података и након истека важења сертификата. На крају, прописује се правно дејство електронског потписа и печата: квалификовани електронски потпис има исто правно дејство као својеручни потпис, а квалификовани електронски печат ужива претпоставку интегритета и тачности порекла података, уз изузетке за правне послове за које закон изричито захтева посебну форму.

Члан 62. – 63. (Електронски временски жиг)

Чланови 62. до 63. уређују услове за квалификоване електронске временске жигове и правно дејство електронског временског жига.

Члан 64. – 67. (Електронска достава)

Чланови 64. до 67. уређују услове за услуге квалификоване електронске доставе, издавање и садржину потврде о електронској достави, размену електронских порука између пружалаца и правно дејство електронске доставе.

Члан 68. – 70. (Аутентификација веб сајтова)

Уређује да се за аутентификацију користи квалификовани сертификат који издаје пружалац квалификованих услуга од поверења, садржај квалификованих сертификата за аутентификацију и информациона безбедност веб сајтова.

Члан 71.- 76. (Електронска потврда атрибута)

Чланови 61–76 уређују квалификовану електронску потврду атрибута: ко је издаје, обавезни садржај и начин провере валидности, као и поступак верификације атрибута упоређивањем са изворним евиденцијама. Прописују издавање потврда од стране органа јавне власти, њихову употребу и чување у дигиталном идентификационом новчанику, као и пуно важење и доказну снагу (укљ. могућност

међународног признавања). Посебно се утврђују правила заштите података: логичка и функционална одвојеност обраде и забрана комбиновања са другим услугама од поверења.

Члан 77. – 78. (Квалификована услуга електронског архивирања)

Чланови 77–78 уређују квалификовану услугу електронског архивирања, односно услове које мора да испуни пружалац услуге: регистрацију, примену технологија које обезбеђују трајност, читљивост и интегритет електронских података и докумената током прописаног рока, као и заштиту од губитка или измена. Такође, прописују да се електронски архивираним документима не може оспорити пуноважност само зато што су у електронском облику, док пружалац услуге гарантује њихов интегритет и порекло током целог периода чувања.

Члан 79. – 80. (Електронска евиденција)

Чланови 79. до 80. прописују услове за квалификовану услугу вођења електронске евиденције, укључујући обавезу пружаоца да обезбеди утврђивање порекла података, јединствен хронолошки редослед уписа и уочљивост сваке измене ради очувања интегритета записа. Евиденције органа јавне власти сматрају се квалификованим ако испуњавају исте техничке и безбедносне стандарде. Утврђује се и да електронским евиденцијама не може бити оспорена пуноважност због њиховог електронског облика, док пружалац услуге гарантује тачност, редослед и целокупност података, уз могућност аутоматизованог ажурирања преко метареистра.

VI. ИНСПЕКЦИЈСКИ НАДЗОР

Члан 81. – 82. (Инспекцијски надзор)

Члановима 81. до 82. уређују се послови и овлашћења инспекције за електронску идентификацију и услуге од поверења у електронском пословању.

VII. КАЗНЕНЕ, ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 83.- 88.

Члановима 83. до 88. прописују се износи новчане казне за прекршај који учине: правно лице, одговорно лице у правном лицу, као и физичко лице у својству регистрованог субјекта и оне су подељене у више распона зависно од учињеног прекршаја.

Члан 89. – 92. (Прелазне и завршне одредбе)

Прелазне и завршне одредбе (чланови 89–92) уређују начин и рокове за примену новог закона. Оне прописују да се у року од 12 месеци донесу сва неопходна подзаконска акта, као и да се у истом року успостави дигитални идентификациони новчаник. Истовремено се утврђује дан престанка важења претходног закона из 2017. године, уз правило да се постојећи подзаконски акти настављају примењивати док се не донесу нови, ако нису у супротности са новим законом.

IV. ПРОЦЕНА ФИНАНСИЈСКИХ СРЕДСТАВА ПОТРЕБНИХ ЗА СПРОВОЂЕЊЕ ЗАКОНА

За спровођење овог закона у 2026. години обезбеђена су средства у Закону о буџету Републике Србије за 2026. годину („Службени гласник РС”, број 108/25) у износу од 2.000.000 динара на Разделу 38 – Министарство информисања и телекомуникација, Програм 0703 – Телекомуникације и информационо друштво, Програмска активност 0008 – Развој информационог друштва, економска класификација 423 – Услуге по уговору.

За спровођење закона у 2027. години пројектована су средства у износу од 2.000.000 динара на разделу Министарства информисања и телекомуникација.

Ради примене закона у 2028. години пројектована су средства у износу од 2.500.000 динара на разделу Министарства информисања и телекомуникација.

За спровођење овог закона обезбеђена су средства Чланом 5. Закона о буџету Републике Србије за 2026. годину („Службени гласник РС”, број 108/25) на Разделу 51 - Канцеларија за информационе технологије и електронку управу, Програм 0614 – Информационе технологије и електронска управа, Функција 140 – Основно истраживање, Пројекат 5003 - Имплементација електронских регистара органа и организација, јавне управе и запослених у систем јавне управе, економска класификација 515 – нематеријална имовина, и то:

- за 2026. годину у износу од 150.000.000,00 динара
- за 2027. годину у износу од 150.000.000,00 динара.