

ЗАКОН О ЕЛЕКТРОНСКОМ ПОТПИСУ РЕПУБЛИКЕ СРПСКЕ

ГЛАВА I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим законом уређује се право физичких и правних лица на употребу електронског потписа у управним, судским и другим поступцима, пословним и другим радњама, те права, обавезе и одговорности физичких и правних лица која пружају услуге израде, верификације и валидације електронског потписа, временског жига, електронског печата и сертификата за аутентификацију мрежних страница на територији Републике Српске (у даљем тексту: Република), ако посебним законом није другачије одређено.

Члан 2.

Поједини изрази који се користе у овом закону имају сљедеће значење:

1) електронски документ – једнообразно повезан цјеловит скуп података који су електронски обликовани (израђени помоћу рачунара и других електронских уређаја), послани, примљени или сачувани на електронском, магнетном, оптичком или другом медију, и који садржи особине којима се утврђује аутор, утврђује вјеродостојност садржаја, те доказује вријеме када је документ сачињен,

2) корисник – правно лице, односно самостални предузетник или физичко лице које користи услуге сертификационог тијела,

3) потписник – лице које посједује средство за израду електронског потписа, а које потписује у своје име или у име правног лица, односно самосталног предузетника,

4) подаци за израду електронског потписа – јединствени подаци, као што су кодови или приватни криптографски кључеви које потписник користи за израду електронског потписа,

5) средство за израду електронског потписа – одговарајућа рачунарска опрема и рачунарски програм које потписник користи при изради електронског потписа,

6) средство за израду квалификованог електронског потписа – одговарајућа рачунарска опрема и рачунарски програм које потписник користи при изради електронског потписа и који испуњавају услове утврђене овим законом,

7) подаци за верификацију електронског потписа – подаци, као што су кодови или јавни криптографски кључеви, који се користе ради провјере валидности електронског потписа,

8) средство за верификацију електронског потписа – одговарајућа рачунарска опрема и рачунарски програм који се користе за провјеру података за верификацију потписа,

9) сертификационо тијело – правно лице, односно самостални предузетник који је регистрован и који обавља послове у складу са Законом о занатско-предузетничкој дјелатности, које издаје електронске сертификате или пружа друге услуге које су у вези са електронским потписима,

10) временски жиг – званично вријеме придружено електронском документу или групи електронских докумената којим се потврђује садржај електронског документа у то вријеме, односно садржај сваког документа у групи,

11) електронски печат – скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику ради осигурања изворности и цјеловитости тих података,

12) квалификовани електронски печат – електронски печат који је креиран помоћу средства за израду квалификованог електронског печата и који се заснива на квалификованом сертификату за електронски печат,

13) аутор електронског печата – правно лице, односно самостални предузетник који креира електронски печат,

14) сертификат за аутентификацију мрежних страница – потврда помоћу које је могуће извршити аутентификацију мрежних страница, те којом се мрежне странице повезују са физичким или правним лицем којем је издат сертификат и

15) квалификовани сертификат за аутентификацију мрежних страница – потврда коју је издало сертификационо тијело и која испуњава услове из члана 18. овог закона.

ГЛАВА II

ЕЛЕКТРОНСКИ ПОТПИС И КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ПОТПИС

Члан 3.

Електронски потпис је скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику и који служе за идентификацију потписника и аутентичност потписаног електронског документа.

Члан 4.

Квалификовани електронски потпис је електронски потпис који:

- 1) је повезан искључиво са потписником,
- 2) поуздано идентификује потписника,
- 3) настаје кориштењем средстава којима потписник може самостално да управља и која су искључиво под надзором потписника и
- 4) је директно повезан са подацима на које се односи и то на начин који недвосмислено омогућава увид у било коју измјену изворних података.

Члан 5.

Квалификовани електронски потпис у односу на податке у електронском облику има исту правну снагу као и својеручни потпис, односно својеручни потпис и печат, у односу на податке у папирном облику.

Члан 6.

(1) Електронски потпис сматра се правно ваљаним и допуштено га је користи у судским и другим поступцима ако испуњава услове прописане овим законом.

(2) Електронски потпис се не може оспоравати у судским и другим поступцима искључиво на основу тога што је у електронском облику или због тога што не испуњава све захтјеве за квалификовани електронски потпис.

Члан 7.

- (1) Електронски потпис израђује се средствима за израду електронског потписа.

(2) Квалификован електронски потпис израђује се средствима за израду квалификованог електронског потписа која морају да испуњавају услове из члана 8. овог закона.

Члан 8.

(1) Средство за израду квалификованог електронског потписа мора испуњавати слjedeће услове:

1) да осигура да се подаци за израду квалификованог електронског потписа могу појавити само једном, те да је обезбијеђена њихова тајност у разумној мјери,

2) да осигура да се подаци за израду квалификованог електронског потписа не могу, уз разумне сигурносне мјере, поновити, те да је потпис заштићен од фалсификовања кориштењем постојеће расположиве технологије и

3) да осигура да подаци за израду квалификованог електронског потписа буду поуздано заштићени од неовлаштеност кориштења од стране трећих лица.

(2) Средство за израду квалификованог електронског потписа не може приликом израде квалификованог електронског потписа промијенити податке који се потписују или онемогућити потписнику увид у те податке прије процеса потписивања.

(3) Изузетно од одредбе става 1. овог члана, сертификационо тијело које издаје квалификоване електронске сертификате и које управља подацима за израду електронског потписа у име потписника може копирати податке за израду електронског потписа искључиво у сврху израде резервних копија, под условом да су испуњени слjedeћи услови:

1) сигурност копираних скупова података мора бити на једнаком нивоу сигурности изворних скупова података и

2) број копираних скупова података не прелази број неопходан за осигуравање континуитета услуге.

(4) Министар науке и технологије (у даљем тексту: министар) правилником прописује које се мјере заштите електронског потписа и квалификованог електронског потписа морају предузети, техничко-технолошке поступке за израду квалификованог електронског потписа и услове које треба да испуне средства за израду електронског потписа и квалификованог електронског потписа.

Члан 9.

Средство за верификацију квалификованог електронског потписа мора испуњавати слjedeће услове:

1) мора се осигурати да подаци који се користе за верификацију електронског потписа одговарају подацима приказаним лицу које обавља верификацију,

2) потпис мора бити поуздано верификован, а резултат те верификације на исправан начин приказан,

3) лице које обавља верификацију мора имати могућност увида у садржај потписаних података,

4) мора се осигурати поуздана провјера аутентичности и ваљаности сертификата који се захтијева у вријеме провјере потписа,

5) идентитет потписника мора бити приказан на исправан начин,

6) употреба псеудонима, ако је псеудоним био кориштен у тренутку потписивања, мора бити јасно назначена и

7) мора се осигурати да се поуздано открију било какве промјене у потписаним подацима.

ГЛАВА III ВРЕМЕНСКИ ЖИГ

Члан 10.

Временски жиг је скуп података у електронском облику који повезује друге податке у електронском облику са одређеним временом и на тај начин доказује да су ти подаци постојали у то вријеме.

Члан 11.

Квалификовани временски жиг мора испуњавати сљедеће услове:

- 1) мора повезивати датум и вријеме са подацима на такав начин да се може, у разумној мјери, искључити могућност неовлаштене промјене података,
- 2) мора се заснивати на извору тачног времена који је повезан са координисаним универзалним временом (UTC енгл. Coordinated Universal Time) и
- 3) мора бити потписан помоћу квалификованог електронског потписа или печатаћен помоћу квалификованог електронског печата или на неки други одговарајући начин који обезбјеђује једнак ниво сигурности.

Члан 12.

(1) Цертификационо тијело које издаје временски жиг дужно је да, на основу захтјева за формирање временског жига, обезбиједи формирање прописане структуре података временског жига, као и поуздано утврђивање времена његовог настанка и електронско потписивање структуре података временског жига.

(2) Цертификационо тијело које издаје временски жиг дужно је да обезбиједи поуздан систем складиштења релевантних информација које се односе на временски жиг у прописаном периоду, посебно у сврху доказивања за потребе одређених поступака.

(3) На временски жиг и с њим повезане услуге примјењују се одредбе овог закона које се односе на сертификат.

(4) Министар правилником прописује услове које мора да испуњава систем за формирање временског жига, садржај захтјева за формирање временског жига, садржај структуре података временског жига и поступак означавања времена које је садржано у временском жигу.

ГЛАВА IV ЕЛЕКТРОНСКИ ПЕЧАТ

Члан 13.

(1) Електронски печат је скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику и који обезбјеђују аутентичност и цјеловитост тих података.

(2) Квалификовани електронски печат мора испуњавати сљедеће услове:

- 1) мора бити повезан искључиво са аутором печата,
- 2) мора поуздано идентификовати аутора печата,
- 3) настаје кориштењем средстава којима потписник може самостално да управља и која су искључиво под надзором потписника и

4) мора бити директно повезан са подацима на које се односи и то на начин који недвосмислено омогућава увид у било коју измјену изворних података.

Члан 14.

(1) Електронски печат сматра се правно ваљаним и допуштено га је користи у судским и другим поступцима ако испуњава услове прописане овим законом.

(2) У погледу средства за израду квалификованог електронског печата и средства за верификацију квалификованог електронског печата примјењују се одредбе чл. 8. и 9. овог закона које се односе на квалификовани електронски потпис.

ГЛАВА V ЕЛЕКТРОНСКИ ЦЕРТИФИКАТИ И ЦЕРТИФИКАЦИОНА ТИЈЕЛА

Члан 15.

(1) Електронски сертификат за електронски потпис је потврда у електронском облику која повезује податке за верификацију електронског потписа са неким лицем и потврђује идентитет тог лица.

(2) Електронски сертификат за електронски печат је потврда у електронском облику која повезује податке за верификацију електронског печата са правним лицем, односно самосталним предузетником и потврђује назив тог правног лица, односно самосталног предузетника.

(3) Електронски сертификат за аутентификацију мрежних страница је електронска потврда помоћу које је могуће извршити аутентификацију мрежних страница и којом се те мрежне странице повезују са физичким или правним лицем, односно самосталним предузетником којима је издат сертификат.

Члан 16.

(1) Квалификовани електронски сертификат за електронски потпис је потврда у електронском облику којом сертификационо тијело потврђује квалификовани електронски потпис.

(2) Квалификовани електронски сертификат из става 1. овог члана мора садржавати:

1) ознаку о томе да је ријеч о квалификованом електронском сертификату,
2) идентификациони скуп података о сертификационом тијелу које издаје квалификовани електронски сертификат, укључујући и назив државе у којој има сједиште, и:

1. назив правног лица и број судског регистра, када је то примјенљиво, ако електронски сертификат издаје правно лице,

2. назив самосталног предузетника ако електронски сертификат издаје предузетник,

3) име потписника или псеудоним, ако се потписник користи псеудонимом,

4) податке за верификацију електронског потписа који одговарају подацима за израду електронског потписа,

5) податке о почетку и крају важења електронског сертификата,

6) идентификациону ознаку издатог електронског сертификата,

7) квалификовани електронски потпис или квалификовани електронски печат сертификационог тијела,

8) локацију на којој је бесплатно доступан сертификат који подржава квалификовани електронски потпис или квалификовани електронски печат из тачке 7) овог члана,

9) локацију услуга које се могу користити за провјеру статуса квалификованог сертификата,

10) информацију о томе ако су подаци за израду електронског потписа који су повезани са подацима за верификацију електронског потписа смјештени у средству за израду квалификованог електронског потписа.

Члан 17.

Квалификовани електронски сертификат за електронски печат мора садржавати:

1) ознаку о томе да је сертификат издат као квалификовани електронски сертификат за електронске печате,

2) идентификациони скуп података о сертификационом тијелу које издаје квалификовани електронски сертификат, укључујући и назив државе у којој има сједиште, и:

1. назив правног лица и број судског регистра, када је то примјенљиво, ако електронски сертификат издаје правно лице,

2. назив самосталног предузетника, ако електронски сертификат издаје предузетник,

3) назив аутора печата и, када је то примјенљиво, регистарски број,

4) податке за верификацију електронског печата који одговарају подацима за израду електронског печата,

5) податке о почетку и крају рока важења сертификата,

6) идентификациону ознаку издатог електронског сертификата,

7) квалификовани електронски потпис или квалификовани електронски печат сертификационог тијела,

8) локацију на којој је бесплатно доступан сертификат који подржава квалификовани електронски потпис или квалификовани електронски печат из тачке 7) овог члана,

9) локацију услуга које се могу користити за провјеру статуса квалификованог сертификата,

10) информацију о томе ако су подаци за израду електронског печата који су повезани са подацима за верификацију електронског печата смјештени у средству за израду квалификованог електронског печата.

Члан 18.

Квалификовани електронски сертификат за аутентификацију мрежних страница мора садржавати:

1) ознаку о томе да је сертификат издат као квалификовани електронски сертификат за аутентификацију мрежних страница,

2) идентификациони скуп података о сертификационом тијелу које издаје квалификоване електронске сертификате за аутентификацију мрежних страница, укључујући и назив државе у којој сертификационо тијело има сједиште, и:

1. назив правног лица и број судског регистра, када је то примјенљиво, ако електронски сертификат издаје правно лице,

2. назив самосталног предузетника, ако електронски сертификат издаје самостални предузетник,

3) идентификациони скуп података о кориснику сертификата:

1. најмање име лица којем је издат сертификат или псеудоним, ако га користи, уколико је ријеч о самосталном предузетнику или физичком лицу,

2. назив правног лица и број судског регистра, када је то примјенљиво, уколико се ради о правном лицу,
- 4) адресу, укључујући најмање ознаку града и државе, корисника коме је издат сертификат,
- 5) назив(-е) домене(-а) којом(-има) управља корисник сертификата,
- 6) податке о почетку и крају рока важења сертификата,
- 7) идентификациону ознаку издатог електронског сертификата,
- 8) квалификовани електронски потпис или квалификовани електронски печат сертификационог тијела,
- 9) локацију на којој је бесплатно доступан сертификат који подржава квалификовани електронски потпис или квалификовани електронски печат из тачке 8) овог члана и
- 10) локацију услуга које се могу користити за провјеру статуса квалификованог сертификата.

Члан 19.

- (1) Сертификационо тијело које издаје неквалификоване електронске сертификате не треба посебну дозволу за обављање услуга.
- (2) Сертификационо тијело може обављати услуге електронске сертификације ако има:
 - 1) организацију рада која обезбјеђује квалитет издавања електронских сертификата,
 - 2) финансијска и материјална средства која су довољна за трајније издавање електронских сертификата и покривање могуће штете, накнаде на име осигурања и слично,
 - 3) запослено лице које је квалификовано за извршавање одговарајућих стручно-техничких послова услуга издавања електронских сертификата, вођење регистра сертификата и заштите личних података,
 - 4) техничку и програмску основу која осигурава међународне стандарде за спровођење услуга електронске сертификације,
 - 5) систем физичке заштите уређаја, опреме и података и
 - 6) рјешења за заштиту од неовлаштеног приступа, као и сигурносна рјешења за чување информација.

Члан 20.

- (1) Министарство науке и технологије (у даљем тексту: Министарство) води евиденцију о сертификационим тијелима у Републици (у даљем тексту: евиденција) која је јавно доступна.
- (2) Сертификациона тијела која издају сертификате на комерцијалној основи дужна су да пријаве Министарству почетак обављања услуга електронске сертификације најмање 14 дана прије почетка рада.
- (3) Министарство уписује сертификационо тијело у евиденцију, одмах након што сертификационо тијело поднесе пријаву којом обавјештава Министарство о почетку обављања услуга.
- (4) Министар правилником прописује садржај евиденције, начин вођења евиденције, обрасце пријаве за упис у евиденцију, обрасце пријаве за упис промјена, као и врсту, садржај и начин достављања документације неопходне за упис у евиденцију.

Члан 21.

(1) Поред услова из члана 19. овог закона, сертификационо тијело које издаје квалификоване електронске сертификате мора да испуњава и сљедеће услове:

1) приказује поузданост неопходну за пружање услуга електронске сертификације,
2) обезбјеђује сигурно и ажурно вођење регистра сертификата, те спровођење безбједног и тренутног прекида, односно опозива услуге електронске сертификације на захтјев корисника,

3) омогућава тачно утврђивање датума и времена (сат и минута) издавања или опозива електронског сертификата,

4) провјерава на одговарајући начин и у складу са прописима идентитет и, ако је потребно, друга обиљежја корисника којима се издаје електронски сертификат,

5) има запослена лица са специјалистичким знањима, искуством и стручним квалификацијама потребним за вршење услуге издавања електронских сертификата, а нарочито у односу на: управљачке способности, стручност у примјени технологија електронског потписа и одговарајућих безбједносних процедура и безбједну примјену одговарајућих административних и управљачких поступака који су усаглашени са признатим стандардима,

6) има поуздане системе и производе који су заштићени од промјена и осигуравају техничку и криптографску сигурност процеса,

7) предузима мјере против фалсификовања и крађе података,

8) има обезбијеђена потребна финансијска средства за рад, посебно за сношење ризика од одговорности за штету,

9) има обезбијеђен поуздан систем складиштења релевантних информација које се односе на квалификоване електронске сертификате у прописаном периоду/року, посебно у сврху доказивања за потребе одређених поступака,

10) не чува и не копира податке из сертификата за кориснике којима се пружа услуга електронске сертификације,

11) информисе кориснике који траже услугу електронске сертификације о тачним условима кориштења услуга, укључујући било која ограничења у кориштењу, као и поступке за рјешавање притужби и жалби, с тим да те информације морају:

1. бити написане и припремљене на једном од језика конститутивних народа у Републици Српској, на ћирилици или латиници и могу се доставити електронским путем,
2. релевантни дијелови тих информација бити на располагању на захтјев трећих лица која користе електронски сертификат,

12) има обезбијеђен поуздан систем чувања електронских сертификата у облику који омогућава њихову провјеру како би:

1. унос и промјене радила само овлаштена лица,
2. могла бити утврђена провјера аутентичности информација из сертификата,
3. електронски сертификат био јавно расположив за претраживање само у оним случајевима за које је власник сертификата, односно корисник дао сагласност и
4. било која техничка промјена која би могла да наруши безбједносне захтјеве била позната сертификационом тијелу.

(2) Министар правилником детаљније прописује услове које морају испуњавати сертификациона тијела из овог члана и члана 19. овог закона, као и најнижи износ обавезног осигурања из става 1. тачка 8) овог члана којим је сертификационо тијело обавезно да осигура ризик од одговорности за штету која настане обављањем услуга електронске сертификације.

Члан 22.

(1) Сертификационо тијело из члана 21. овог закона, које издаје квалификоване електронске сертификате, може да обавља услуге на основу дозволе коју издаје Министарство.

(2) На основу захтјева сертификационог тијела за издавање дозволе, министар именује Комисију за провјеру испуњености услова за обављање услуга издавања квалификованих електронских сертификата (у даљем тексту: Комисија), која има три члана.

(3) У Комисију се именују стручњаци из области информационих технологија, који имају искуство у области примјене електронског потписа и који познају систем инфраструктуре јавног кључа.

(4) Чланови Комисије имају право на накнаду за свој рад, која се утврђује рјешењем министра.

(5) На основу препоруке Комисије, министар доноси рјешење којим се рјешава по захтјеву за издавање дозволе.

(6) Дозвола за издавање квалификованих електронских сертификата (у даљем тексту: дозвола) има значење рјешења издатог у управном поступку.

(7) Дозвола се издаје у року од 30 дана од дана подношења уредног захтјева.

(8) У поступку за издавање дозволе, у питањима која нису уређена овим законом примјењују се одредбе Закона о општем управном поступку.

Члан 23.

(1) Заједно са издавањем дозволе из члана 22. став 5. овог закона, сертификационо тијело се уписује се у Регистар сертификационих тијела у Републици Српској (у даљем тексту: Регистар), који води Министарство и који је јавно доступан.

(2) Сертификационо тијело може почети да обавља услуге даном уписа у Регистар.

(3) Сертификациона тијела која су уписана у Регистар могу то да назначе у издатим квалификованим електронским сертификатима.

(4) Министар правилником прописује садржај и начин вођења Регистра, обрасце захтјева за издавање дозволе и потребних прилога уз захтјев, обрасце захтјева за упис промјена и потребних прилога, као и поступак издавања дозволе и уписа у Регистар.

Члан 24.

(1) Електронске сертификате може издавати и орган управе, ако испуњава све услове прописане овим законом и прописима донесеним на основу овог закона.

(2) Дјелокруг, садржај и носиоци послова електронске сертификације у органима управе и за органе управе утврђују се уредбом Владе Републике Српске.

ГЛАВА VI ПРАВА, ОБАВЕЗЕ И ОДГОВОРНОСТИ КОРИСНИКА И ЦЕРТИФИКАЦИОНИХ ТИЈЕЛА

Члан 25.

(1) Корисници су слободни у избору сертификационог тијела.

(2) Корисник може користити услуге сертификације од једног сертификационог тијела или више њих.

(3) Корисници могу користити и услуге сертификационог тијела у иностранству.

(4) Корисници користе услуге сертификације на основу уговора са одабраним сертификационим тијелом.

Члан 26.

(1) Електронски сертификат може се издати сваком кориснику на његов захтјев, на основу несумњиво утврђеног идентитета и осталих података о кориснику који је поднио захтјев.

(2) Идентитет корисника се утврђује на основу личне карте, путне исправе или другог идентификационог документа корисника или овлаштеног представника корисника, који садржи фотографију лица и који је важећи у тренутку подношења захтјева.

(3) Сертификационо тијело издаје електронски сертификат за сваког појединачног корисника на основу уговора потписаног са корисником.

Члан 27.

(1) Сваки корисник обавезан је да предузме све потребне организационе и техничке мјере заштите од губитака и штете које може узроковати другим корисницима, сертификационом тијелу или трећим лицима.

(2) Обавеза корисника је да средства и податке за израду електронског потписа и електронског печата користи пажљиво и у складу са одредбама овог закона, те да их заштити и чува од неовлаштеног приступа и употребе.

Члан 28.

(1) Све потребне податке и информације о промјенама које утичу или могу утицати на тачност сертификата корисник је обавезан да одмах пријави, односно достави сертификационом тијелу.

(2) Корисник је обавезан да одмах затражи опозив свог сертификата у свим случајевима губитка или оштећења средстава или података за израду електронског потписа и електронског печата.

Члан 29.

Корисник је одговоран за неправилности које су настале због неиспуњавања обавеза утврђених одредбама чл. 27. и 28. овог закона.

Члан 30.

Сертификационо тијело које издаје квалификоване електронске сертификате има обавезу да:

1) осигура да сваки квалификовани електронски сертификат садржи све потребне податке у складу са чл. 16, 17. и 18. овог закона,

2) утврди идентитет корисника за којег спроводи услуге сертификације,

3) осигура тачност и цјеловитост података које уноси у евиденцију издатих сертификата,

4) у сваки сертификат унесе основне податке о свом идентитету,

5) омогући сваком заинтересованом лицу увид у идентификационе податке сертификационог тијела и увид у дозволу за издавање квалификованих електронских сертификата,

- 6) води тачну и заштићену евиденцију електронских сертификата,
- 7) води тачну и заштићену евиденцију опозваних електронских сертификата,
- 8) осигура видљив податак о тачном датуму и времену (сат и минута) издавања, односно опозива електронских сертификата у евиденцији издатих електронских сертификата,
- 9) чува све податке и документацију о издатим и опозваним електронским сертификатима, у складу са важећим прописима, као средство доказивања у судским, управним и другим поступцима, при чему подаци и пратећа документација могу бити и у електронском облику и
- 10) примјењује одредбе закона и других прописа којима је уређена заштита личних података.

Члан 31.

(1) Сертификационо тијело обавезно је да изврши опозив сертификата, најкасније у року од 24 часа, корисницима:

- 1) који су то изричито затражили,
- 2) за које је утврђена нетачност или непотпуност података у евиденцији сертификата,
- 3) за које је примљена службена обавијест о губитку пословне способности и
- 4) за које је примљена службена обавијест о смрти.

(2) Опозив ступа на снагу одмах након његовог објављивања у евиденцији опозваних сертификата.

(3) Сертификационо тијело обавезно је да ажурно води евиденцију свих опозваних електронских сертификата.

(4) Обавеза сертификационог тијела је да обавијести корисника о опозиву сертификата у року од 24 часа од примљеног обавјештења, односно настанка околности због којих се електронски сертификат опозива.

(5) Од тренутка када је опозван, сертификат губи правно дејство и његов статус се не може поново активирати.

Члан 32.

(1) Сертификационо тијело обавезно је да, у случају престанка пословања, о намјери раскида уговора обавијести сваког корисника, као и да престанак пословања пријави Министарству.

(2) Обавеза сертификационог тијела је да осигура код другог сертификационог тијела наставак обављања услуга сертификације за кориснике којима је издало сертификате најмање за период важења оригиналног сертификата, а уколико за то нема могућности, дужно је да опозове све издате сертификате.

(3) Сертификационо тијело које престаје да пружа услуге електронске сертификације обавезно је да достави сву документацију у вези са обављеним услугама сертификације другом сертификационом тијелу на кога преноси обавезе обављања услуга сертификације.

Члан 33.

(1) Квалификовани сертификати које су издала сертификациона тијела са сједиштем у једној од земаља чланица Европске уније имају исту правну снагу као и квалификовани сертификати издати у Републици Српској.

(2) Квалификовани сертификати које су издала сертификациона тијела са сједиштем у иностранству изван Европске уније имају исту правну снагу као и квалификовани

сертификати издати у Републици Српској, у случају да је испуњен најмање један од сљедећих услова:

1) сертификационо тијело испуњава услове прописане овим законом за издавање квалификованих сертификата и регистровано је у Републици Српској,

2) домаће сертификационо тијело које је уписано у Регистар гарантује за такав квалификовани сертификат,

3) билатералним или мултилатералним споразумом између Републике Српске или Босне и Херцеговине и других земаља или међународних организација одређено је да се признаје и

4) квалификовани сертификат или сертификационо тијело признато је на основу билатералног или мултилатералног споразума између Европске уније и трећих земаља или међународних организација.

ГЛАВА VII НАДЗОР

Члан 34.

(1) Надзор над примјеном овог закона и радом сертификационих тијела врши Републичка управа за инспекцијске послове посредством надлежних инспектора.

(2) Надзор над радом сертификационих тијела на пословима прикупљања, употребе и заштите личних података врше органи одређени прописима којима се уређује заштита личних података.

Члан 35.

У оквиру инспекцијског надзора сертификационих тијела инспектор:

1) утврђује да ли су испуњени услови прописани овим законом и прописима донесеним на основу овог закона,

2) контролише правилност примјене прописаних поступака и организационо-техничких мјера, примјену интерних правила која су у вези са условима прописаним овим законом и прописима донесеним на основу овог закона,

3) врши контролу поступка издавања, чувања и опозива електронских сертификата и

4) врши контролу законитости обављања других услуга сертификационих тијела.

Члан 36.

(1) У вршењу инспекцијског надзора инспектор има право и дужност да:

1) прегледа акте и документацију која је повезана са дјелатношћу издавања сертификата,

2) провјерава пословне просторије сертификационог тијела, информациони систем, рачунарску мрежу, осталу опрему, техничку документацију, као и безбједносне мјере које се предузимају и

3) изврши увид у цјелокупну документацију ради обезбјеђивања доказа или тачног утврђивања евентуалне нерегуларности.

(2) Инспектор је дужан да чува као службену тајну све податке о сертификатима и личне податке о кориснику сертификата.

(3) Сертификационо тијело је дужно да у циљу спровођења инспекцијског надзора омогући инспектору приступ у своје пословне просторије и омогући увид у податке о

пословању, увид у пословну документацију, приступ регистру корисника и рачунарској опреми и уређајима који се примјењују у поступку издавања сертификата.

Члан 37.

(1) Надлежни инспектор рјешењем:

1) забрањује примјену неадекватних поступака и инфраструктуре и даје рок сертификационом тијелу у којем је оно дужно да обезбиједи адекватне поступке и инфраструктуру,

2) забрањује лицима која не посједују специјалистичка знања, искуство и стручне квалификације потребне за вршење услуге издавања електронских сертификата, рад на пословима издавања сертификата и даје рок за обезбјеђење адекватног кадра,

3) привремено забрањује пословање сертификационог тијела до отклањања неадекватности поступака и инфраструктуре,

4) налаже опозив једног или више сертификата издатих од сертификационог тијела, ако постоји основана сумња да је ријеч о неадекватном поступку или фалсификату и

5) налаже опозив свих сертификата издатих од сертификационог тијела, што доводи до престанка рада сертификационог тијела, ако постоји основана сумња да је ријеч о неадекватном поступку или фалсификату.

(2) У случају привремене забране пословања сертификационог тијела из става 1. тачка 3) овог члана, сертификати издати до дана настанка узрока због којих је изречена мјера забране и даље важе.

(3) У случају опозива свих сертификата, односно престанка рада сертификационог тијела из става 1. тачка 5) овог члана, инспектор ће одмах обавијестити Министарство и затражити брисање из евиденције, односно Регистра.

(4) Уколико се током инспекцијске контроле утврди да сертификационо тијело које издаје квалификоване електронске сертификате и које је уписано у Регистар више не испуњава услове прописане овим законом, надлежни инспектор о томе одмах обавјештава Министарство.

(5) Министарство је дужно да сертификационо тијело, одмах по добијању обавјештења од стране надлежног инспектора, брише из Регистра.

ГЛАВА VIII КАЗНЕНЕ ОДРЕДБЕ

Члан 38.

Новчаном казном од 500 КМ до 1.500 КМ казниће се за прекршај физичко лице које неовлаштено приступи и употрежи податке и средства за израду електронског потписа и квалификованог електронског потписа.

Члан 39.

(1) Новчаном казном од 500 КМ до 1.500 КМ казниће се за прекршај корисник – физичко лице или самостални предузетник који:

1) непажљиво и неодговорно користи средства и податке за израду електронског потписа и електронског печата (члан 27. став 2),

2) сертификационом тијелу не достави потребне податке и информације о промјенама које утичу или могу утицати на тачност електронског сертификата (члан 28. став 1) и

3) одмах не достави сертификационом тијелу захтјев за опозив сертификата (члан 28. став 2).

(2) За прекршај из става 1. овог члана корисник – правно лице ће се казнити новчаном казном од 1.000 КМ до 3.000 КМ.

(3) Одговорно лице у правном лицу казниће се за прекршај из става 1. овог члана новчаном казном од 500 КМ до 1.000 КМ.

Члан 40.

(1) Новчаном казном од 1.000 КМ до 15.000 КМ казниће се за прекршај сертификационо тијело које:

- 1) издаје квалификовани електронски сертификат који не садржи све потребне податке (члан 16. став 2, чл. 17. и 18),
- 2) не пријави Министарству почетак обављања услуга електронске сертификације (члан 20. став 2),
- 3) чува и копира податке из сертификата (члан 21. став 1. тачка 10),
- 4) не обавијести корисника којем издаје електронски сертификат о свим битним условима употребе издатог сертификата (члан 21. став 1. тачка 11),
- 5) не утврди идентитет корисника којем издаје квалификовани електронски сертификат (члан 30. тачка 2),
- 6) не води ажурно и безбједносним мјерама заштићену евиденцију сертификата (члан 30. тачка 6),
- 7) не прекине услуге сертификације, односно не изврши опозив издатих сертификата у прописаним случајевима (члан 31. став 1),
- 8) не води ажурно евиденцију свих опозваних сертификата (члан 31. став 2),
- 9) не обавијести у прописаном року корисника о извршеном опозиву електронског сертификата (члан 31. став 3),
- 10) не чува комплетну документацију о издатим и опозваним сертификатима у предвиђеном року (члан 30. тачка 9),
- 11) благовремено не обавијести кориснике којима је издао електронске сертификате и Министарство о престанку пословања (члан 32. став 1) и
- 12) не омогући надлежним инспекцијским органима приступ у своје пословне просторије и увид у податке о пословању, увид у пословну документацију, приступ регистру корисника, рачунарској опреми и уређајима (члан 36. став 3).

(2) Одговорно лице у сертификационом тијелу казниће се за прекршај из става 1. овог члана новчаном казном од 500 КМ до 1.000 КМ.

Члан 41.

(1) Новчаном казном од 1.000 КМ до 15.000 КМ казниће се за прекршај сертификационо тијело – издавалац временског жига који:

1) формира временски жиг који не садржи све податке прописане законом и подзаконским актима донесеним на основу овог закона (члан 11. став 2),

2) не чува на безбједан начин и у прописаним роковима податке о издатим временским жиговима (члан 12. став 2) и

3) не омогући надлежним инспекцијским органима приступ у своје пословне просторије и не омогући увид у податке о пословању, увид у пословну документацију, приступ регистру корисника, рачунарској опреми и уређајима (члан 36. став 3).

(2) Одговорно лице у сертификационом тијелу казниће се за прекршај из става 1. овог члана новчаном казном од 500 КМ до 1.000 КМ.

ГЛАВА IX ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 42.

Влада Републике Српске донијеће уредбу из члана 24. став 2. овог закона у року од три мјесеца од дана ступања на снагу овог закона.

Члан 43.

Министар ће у року од шест мјесеци од дана ступања на снагу овог закона донијети:

- 1) Правилник о техничко-технолошким поступцима за израду квалификованог електронског потписа и других услуга повјерења и мјерама заштите електронског потписа и других услуга повјерења (члан. 8. став 4),
- 2) Правилник о издавању временског жига (члан 12. став 4),
- 3) Правилник о евиденцији сертификационих тијела (члан 20. став 4),
- 4) Правилник о посебним условима које морају да испуњавају сертификациона тијела (члан 21. став 2) и
- 5) Правилник о поступку издавања дозволе и уписа у регистар сертификационих тијела за издавање квалификованих електронских сертификата (члан 23. став 4).

Члан 44.

До доношења подзаконских аката из чл. 42. и 43. овог закона примјењиваће се подзаконски акти донесени на основу раније важећег Закона, ако нису у супротности са одредбама овог закона.

Члан 45.

Ступањем на снагу овог закона престаје да важи Закон о електронском потпису Републике Српске („Службени гласник Републике Српске“, бр. 59/08 и 68/13).

Члан 46.

Овај закон ступа на снагу осмога дана од дана објављивања у „Службеном гласнику Републике Српске“.

Број: 02/1-021-1563/15
Датум: 10. децембар 2015. године

По овлаштењу
Предсједника Народне скупштине

Ненад Стевандић