На основу члана 62. став 3. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17),

Министар трговине, туризма и телекомуникација доноси

ПРАВИЛНИК

о условима за поступке и технолошка решења који се користе током поузданог електронског чувања документа

„Службени гласник РС“, бр. 94 од 7. децембра 2018, 87 од 19. јуна 2020.

Уводна одредба

Члан 1.

Овим правилником прописују се услови за поступке и технолошка решења који се користе током поузданог електронског чувања документа који у изворном облику садржи квалификовани електронски потпис односно печат и документа којем је квалификованим електронским потписом односно печатом потврђена верност изворном документу и тачност додатно укључених података у складу са чланом 61. став 1. тачка 4) Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (у даљем тексту: Закон).

Интерна правила

Члан 2.

Поуздано електронско чување документа врши се у складу са интерним правилима за поуздано електронско чување документа (у даљем тексту: интерна правила), на основу којих се поступа током поузданог електронског чувања, а којима се обезбеђује да поуздано електронско чување испуњава услове из Закона.

Циљеви поузданог чувања

Члан 3.

Како би се обезбедила могућност доказивања валидности квалификованог електронског потписа односно печата током целог периода чувања, поуздано електронско чување документа подразумева обезбеђење:

1) доказа да је документ постојао у тачно одређеном тренутку, засновано на квалификованом временском жигу;

2) одржавање статуса валидности квалификованог електронског потписа или печата у односу на временски тренутак из тачке 1) овог члана;

3) доступности изворно чуваног електронског документа и свих додатних података којима се потврђује испуњеност услова из тач. 1) и 2) овог члана;

4) одржавања поверења у интегритет и аутентичност свих података из тачке 3) овог члана под претпоставком да током периода чувања може да се појави сумња у претходно коришћене криптографске алгоритме, хеш функције и поступке или да се догоди опозив сертификата корисника или сертификата пружаоца услуге од поверења.

Примена стандарда

Члан 3а.

Услуга квалификованог електронског чувања докумената обавља се сагласно захтевима следећих стандарда:

1) ETSI TS 119 511 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques”;

2) ETSI TS 119 512 „Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services”.

Услуга квалификованог електронског чувања документа обавља се и сагласно захтевима из других стандарда на које се из стандарда из става 1. овог члана директно и индиректно упућује, одговарајућим међународним стандардима и препорукама.

Квалификовани електронски потпис, односно печат на документу који се поуздано електронски чува

Члан 4.

Документ који се поуздано електронски чува обавезно мора да има придружен квалификовани електронски потпис односно печат, без обзира да ли је у питању документ који у изворном облику садржи квалификовани електронски потпис, односно печат или документ којем је квалификованим електронским потписом односно печатом из члана 61. став 1. тачка 4) Закона потврђена верност изворном документу и тачност додатно укључених података.

Формат квалификованог електронског потписа односно печата из става 1. овог члана мора да испуњава један од услова:

1) PDF у складу са ISO 32000 „Document management Portable document format” и PAdES форматом електронског потписа односно печата у складу са ETSI EN 319 142 „Electronic Signatures and Infrastructures (ESI); PAdES digital signatures”;

2) ASiC-S контејнер који у себи садржи документ и електронски потпис односно печат тог документа у XAdES или CAdES формату у складу са ETSI EN 319 162 „Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)”;

3) XAdES формат електронског потписа односно печата који у себи садржи потписан односно печатиран документ у складу са ETSI EN 319 132 „Electronic Signatures and Infrastructures (ESI); XAdES digital signatures”;

4) CAdES формат електронског потписа односно печата који у себи садржи потписан односно печатиран документ у складу са ETSI EN 319 122 „Electronic Signatures and Infrastructures (ESI); CAdES digital signatures”.

Нивои XAdES, CAdES и PAdES формата електронског потписа односно печата из става 1. овог члана морају редом бити XAdES-B-LTA или XAdES-E-A, CAdES-B-LTA или CAdES-E-A и PAdES-B-LTA или PAdES-E-LTV.

Надоградња квалификованог електронског потписа, односно печата

Члан 5.

Приликом отпочињања поузданог електронског чувања, врши се поступак надоградње квалификованог електронског потписа, односно печата у XAdES, CAdES или PAdES формату на документу који се чува, што укључује:

1) уколико је квалификовани електронски потпис односно печат на основном XAdES, CAdES односно PAdES нивоу, квалификованом електронском потпису односно печату додаје се квалификовани временски жиг;

2) врши се валидација квалификованог електронског потписа односно печата и том приликом се прибављају подаци за проверу валидности као што су сертификати и статуси опозваности;

3) у складу са форматом, квалификованом електронском потпису, односно печату се додају недостајући подаци за проверу валидности, рачуна се хеш оригинално потписаног односно печатираног документа заједно са самим потписом односно печатом, креира се квалификовани временски жиг на основу тог хеша и у квалификовани електронски потпис односно печат се додаје и тај временски жиг.

Квалификовани електронски потпис односно печат на документу који се прима на поуздано електронско чување

Члан 6.

Документ који се прима на поуздано електронско чување мора да испуни услове из члана 4. ст. 1. и 2. овог правилника, као и услов да је након надоградње квалификованог електронског потписа односно печата у складу са чланом 5. овог правилника могуће обезбедити нивое из члана 4. став 3. овог правилника.

Поновна надоградња квалификованог електронског потписа односно печата

Члан 7.

Поновна надоградња квалификованог електронског потписа односно печата на електронском документу који се чува врши се обавезно пре него што:

1) истекне сертификат последњег временског жига у квалификованом електронском потпису односно печату;

2) из техничких или формалних разлога криптографски алгоритам или хеш алгоритам који је употребљен у последњем временском жигу у квалификованом електронском потпису односно печату може постати основ оспоравања валидности квалификованог електронског потписа односно печата.

Поновна надоградња квалификованог електронског потписа односно печата обавља се по поступку из члана 5. овог правилника.

Информациони систем за поуздано електронско чување

Члан 8.

Поуздано електронско чување документа врши се у оквиру за то намењеног информационог система (у даљем тексту: информациони систем) којим управља и о којем се стара руковалац чувања.

Информациони системи, заједно са одговарајућим мерама одређеним интерним правилима, мора да обезбеди да се поновна надоградња квалификованог електронског потписа, односно печата врши благовремено, како би се обезбедила могућност доказивања валидности квалификованог електронског потписа, односно печата током целог периода чувања.

Информациони систем мора да обезбеди висок ниво заштите од губитака података који се чувају, нарушавања интегритета тих података и неовлашћеног приступа тим подацима.

Руковалац чувања управља информационим системом сагласно стандарду ISO/IEC 27001 „Information security management” на начин да се сматрају високоризичним инциденти који доводе до губитака података који се чувају, нарушавања интегритета тих података, неовлашћеног приступа тим подацима или губитка могућности доказивања валидности квалификованог електронског потписа односно печата током целог периода чувања.

Мере заштите захтеване стандардом из става 4. овог члана документују се у оквиру интерних правила.

Члан 9.

У циљу обезбеђивања токова приступа, размене и обраде података, у складу са потврђеним међународним споразумима, Министарство унутрашњих послова може да, поред примене овог правилника, примењује и друге услове који се односе на поуздано

електронско чување документа, а који се примењују услед специфичности информационих система и техничко-технолошких поступака у Министарству унутрашњих послова.

Ступање на снагу

Члан 10.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

Број 110-00-53/2018-12

У Београду, 21. новембра 2018. године

Министар,

др **Расим Љајић,** с.р.