НАЦРТ

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 ДОКУМЕНАТА

Уводне одредбе

Члан 1.

Овим правилником прописују се услови за поступке и технолошка решења који се користе током поузданог електронског чувања докумената који у изворном облику садрже квалификовани електронски потпис односно печат и докумената којима 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.

Правно или физичко лице које обавља поуздано електронско чување докумената (у даљем тексту: руковалац чувања) дужно је да донесе интерна правила за поуздано електронско чување докумената (у даљем тексту: интерна правила), по којима ће поступати током поузданог електронског чувања, а којима се обезбеђује да поуздано електронско чување испуњава услове из Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (у даљем тексту: Закон), као и ближе услове из овог правилника.

Уколико су поједина питања која се односе на поуздано електронско чување докумената уређена другим актима руковаоца чувања, интерна правила треба да садрже упућујуће одредбе на та акта.

Циљеви поузданог чувања

Члан 3.

Како би се обезбедила могућност доказивања валидности квалификованог електронског потписа односно печата током целог периода чувања, поуздано електронско чување докумената 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);

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

4) одржавања поверења у интегритет и аутентичност свих података из тачке 3) 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.

Формат у коме се документи чувају

Члан 4.

Документа који у изворном облику садрже квалификовани електронски потпис односно печат, као и документа којима је квалификованим електронским потписом односно печатом из члана 61. став 1. тачка 4) Закона потврђена верност изворном документу и тачност додатно укључених података се поуздано електронски чувају у једном од формата:

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

2) врши се валидација 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, електронском потпису, односно печату се додаје недостајући прибављају 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 електронски потпис односно печат се додаје и тај временски жиг.

Формат у коме се документи примају на електронско чување

Члан 6.

Документ који у изворном облику садржи квалификовани електронски потпис односно печат се прима на поуздано електронско чување у формату из члана 4. став 1.

овог правилника, при чему формати електронског потписа, односно печата не морају да испуњавају нивое из става 2. тог члана, уколико након надоградње електронског потписа односно печата у складу са чланом 5. овог правилника буду постигнути нивои из члана 4. став 2. овог правилника.

Поновна надоградња електронског потписа односно печата

Члан 7.

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

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

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

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

Информациони систем за поуздано електронско чување

Члан 8.

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

Информациони системи, заједно са одговарајућим мерама одређеним интерним правилима, мора да обезбеди да се поновна надоградња 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.

Ступање на снагу

Члан 9.

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