На основу члана 46. став 5. и члана 47. став 2. 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 које мора да испуњава квалификовано средство за креирање електронског потписа односно печата и условима које мора да испуњава именовано тело

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим правилником прописују се:

1) услови које мора да испуњава средство за креирање квалификованог електронског потписа односно печата, укључујући:

(1) техничка решења и критеријуме које мора да испуњава квалификовано средство за креирање електронског потписа односно печата,

(2) техничко-технолошке поступке за формирање електронског потписа односно печата које то средство примењује при креирању потписа односно печата,

(3) критеријуме који морају да буду испуњени када се средство користи путем услуге управљања квалификованим средством за креирање електронског потписа односно печата;

2) услови које мора да испуњава именовано тело за оцену усаглашености квалификованих средстава за креирање електронског потписа односно печата.

Члан 2.

Техничка решења и критеријуми које мора да испуњава квалификовано средство за креирање електронског потписа односно печата, техничко-технолошки поступци за формирање електронског потписа односно печата које то средство примењује и критеријуми који морају да буду испуњени када се средство користи путем услуге управљања квалификованим средством за креирање електронског потписа односно печата морају да буду у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на средства и поступке утврђеним овим правилником.

II. ТЕХНИЧКА РЕШЕЊА И КРИТЕРИЈУМИ

Члан 3.

Квалификовано средство за креирање електронског потписа односно печата, осим услова из члана 46. Закона о електронском документу, електронској идентификацији и

услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17 – у даљем тексту: Закон), мора да испуни и следеће критеријуме:

1) да се обезбеди коришћење средства за креирање квалификованог електронског потписа односно печата искључиво од стране потписника односно печатиоца уз претходно реализовану поуздану процедуру аутентикације;

2) да средство мора бити такво да је потписник односно печатилац у могућности да га користи у различитим апликацијама и информатичко-технолошким окружењима, додатно имајући у виду одредбу члана 6. Закона и потребу корисника да користи средство при коришћењу других услуга од поверења.

Члан 4.

Квалификовано средство за креирање електронског потписа односно печата мора да обезбеди да се подаци за креирање електронског потписа односно печата генеришу тако да могу постојати само у том средству.

Члан 5.

Квалификовано средство за формирање потписа односно печата мора да буде усаглашено са једним од следећих услова:

1) Услови профила заштите дефинисани стандардом SRPS EN 419211-2:2014 – Профили заштите средстава за формирање квалификованог електронског потписа – Део 2: Средство са генерисањем кључа испитивано по Common Criteria нивоу EAL4+;

2) Услови профила заштите дефинисани стандардом SRPS EN 419211-3:2014 – Профили заштите средстава за формирање квалификованог електронског потписа – Део 3: Средство са увођењем кључа испитивано по Common Criteria нивоу EAL4+, ако је испуњен и услов из члана 3. овог правилника;

3) FIPS 140-2 (Federal Information Processing Standard) нивоа 2 или виших.

Предмет испитивања усаглашености квалификованог средства за креирање потписа односно печата је само средство које обезбеђује податке за формирање електронског потписа односно печата. Веза средства са апликацијама за формирање електронског потписа односно печата, није обавезно предмет испитивања усаглашености.

III. ПОСТУПЦИ ЗА ФОРМИРАЊЕ ЕЛЕКТРОНСКОГ ПОТПИСА ОДНОСНО ПЕЧАТА

Члан 6.

Квалификовано средство за креирање електронског потписа односно печата при формирању електронског потписа односно печата користи један од стандардизованих асиметричних криптографских алгоритама, и то:

1) *RSA (Rivest Shamir Adleman)* применом стандарда PKCS#1 уз минималну дужину RSA модулуса n од 2048 бита;

2) *DSA (Digital Signature Algorithm)* са минималним дужинама параметара p и q од 2048 и 224 бита, респективно;

3) *ECDSA (Elliptic Curve Digital Signature Algorithm)* са минималним дужинама параметара p и q од 256 бита.

Члан 7.

При формирању квалификованог електронског потписа примењују се и хеш функције за добијање отисака поруке фиксне величине (најмање 160 бита). Хеш функције из става 1. овог члана реализују се применом неког од следећих стандардизованих хеш алгоритама:

1) SHA-224, SHA-256, SHA-384, SHA-512;

2) SHA3-256, SHA3-384, SHA3-512.

Члан 8.

Скуп стандардних алгоритама из чл. 5. и 6. овог правилника комбиновани са захтевима у вези избора параметара, као и листа стандардних комбинација примењених алгоритама у форми алгоритамских веза („signature suites”), морају бити у складу са документом ETSI TS 119 312 V1.2.1 „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.

IV. КВАЛИФИКОВАНО СРЕДСТВО КОЈЕ СЕ КОРИСТИ ПУТЕМ УСЛУГЕ УПРАВЉАЊА

Члан 9.

Квалификовано средство за креирање електронског потписа односно печата које се користи путем услуге управљања као квалификоване услуге поверења у складу са чланом 46. став 3. Закона (у даљем тексту: квалификовано средство на даљину) мора да обезбеди, уз високи ниво поузданости, да корисник има искључиву контролу над подацима за израду електронског потписа односно печата.

Члан 10.

Подаци за креирање електронског потписа односно печата, када се користе заједно са квалификованим средством на даљину, морају бити иницијално креирани унутар квалификованог средства за креирање електронског потписа и печата које испуњава услове Закона и овог правилника.

Члан 11.

Квалификовано средство на даљину мора да обезбеди да подаци за креирање електронског потписа односно печата могу да буду активирани искључиво од стране потписника уз претходно реализовану поуздану процедуру аутентикације.

Свака активација података за креирање електронског потписа односно печата, у квалификованом средству на даљину неопходно је да буде везана за важећу ауторизацију корисника и конкретан захтев за формирање електронског потписа односно печата.

Члан 12.

Квалификовано средство на даљину мора да обезбеди да се формирање електронског потписа односно печата може догодити само у квалификованом средству за формирање електронског потписа и печата.

Члан 13.

Квалификовано средство на даљину мора да буде усаглашено са условима који су прописани профилом дефинисаном стандардом CEN EN 419 241-2 Protection profile for QSCD for server signing (pending, Q1 2018) испитивано по Common Criteria нивоу EAL4 увећан AVA_VAN.4 анализом рањивости или вишем нивоу.

Члан 14.

Квалификовано средство на даљину у поступку формирања електронског потписа односно печата мора да обезбеђује исти ниво безбедности који је прописан за квалификована средства за креирање електронског потписа односно печата, посебно имајући у виду избор стандардизованих криптографских алгоритама, избор хеш функција за добијање отиска и минималне дужине параметара.

V. ТЕЛО ЗА ОЦЕНУ УСАГЛАШЕНОСТИ

Члан 15.

Именовано тело за оцену усаглашености квалификованих средстава за креирање електронског потписа односно печата (у даљем тексту: именовано тело) мора да буде компетентно, да обезбеђује неопходне људске ресурсе, експертско знање и опрему, те да буде оспособљено за поступак оцењивања усаглашености средства са техничким захтевима који су дефинисани Законом и овим правилником.

Као доказ о испуњености компетентности и наведених услова, именовано тело дужно је да буде акредитовано, у складу са законом којим се уређује акредитација, према стандарду SRPS ISO/IEC 17065:2016 – Оцењивање усаглашености – Захтеви за тела која сертификују производе, процесе и услуге, у обиму акредитације који обезбеђује проверу усаглашености квалификованог средства за креирање електронског потписа односно печата, према следећој листи стандарда:

1) SRPS ISO/IEC 15408-1:2014 – Информационе технологије – Технике безбедности – Критеријуми за вредновање безбедности у ИТ – Део 1: Увод и општи модел;

2) SRPS ISO/IEC 15408-1:2014 – Информационе технологије – Технике безбедности – Критеријуми за вредновање безбедности у ИТ – Део 2: Функционални захтеви за безбедност;

3) SRPS ISO/IEC 15408-1:2014 – Информационе технологије – Технике безбедности – Критеријуми за вредновање безбедности у ИТ – Део 3: Захтеви за осигурање безбедности;

4) ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation.

Члан 16.

Именовано тело мора да се води начелом независности и непристрасности при оцењивању усаглашености.

Посебно у поступку оцењивања, али и у поступку стицања акредитације, у раду именованог тела не могу да учествују лица повезана са средством које је предмет оцењивања усаглашености.

То не искључује могућност размене техничких информација између именованог тела и произвођача средстава.

Члан 17.

Именовано тело дужно је да уреди поступање и одлучивање по приговорима на рад и донете одлуке у вези са пословима оцењивања усаглашености.

Именовано тело дужно је да без одлагања, а најкасније у року од седам дана, обавести министарство надлежно за послове информационог друштва (у даљем тексту: Министарство) о постојању приговора на рад именованог тела и донете одлуке, а у вези са потврдама о усаглашености средстава које је издало то тело за средства која су уписана у Регистар квалификованих средстава за креирање електронског потписа односно печата из члана 47. Закона.

Члан 18.

При закључивању о оцени усаглашености средства именовано тело не може да се служи информацијама које су окарактерисане као пословна тајна.

Члан 19.

У складу са законом којим се уређују технички захтеви за производе и оцењивање усаглашености, именовано тело одговорно је за штету насталу употребом средства за које је тело издало потврду о усаглашености уколико се испостави да средство не испуњава техничке захтеве дефинисане Законом и овим правилником, уколико је штету проузрокована намером или непажњом именованог тела.

Именовано тело дужно је да обезбеди финансијске ресурсе за осигурање од ризика одговорности за штету из делатности тако да:

1) осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 евра у динарској противвредности, подразумевајући притом као штетни догађај појединачну штету насталу једном употребом оцењеног средства;

2) укупна осигурана сума на коју мора бити уговорено осигурање од одговорности именованог тела кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.000.000 евра у динарској противвредности.

VI. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 20.

Даном ступања на снагу овог правилника сматраће се да средство за формирање квалификованог електронског потписа које је за корисника обезбедило сертификационо тело из члана 73. став 3. Закона, а које испуњава услове из „Правилника о техничкотехнолошким поступцима за формирање квалификованог електронског потписа и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа“ („Службени гласник РС”, бр. 26/08, 13/10 и 23/15) испуњава услове из члана 5. овог правилника до истека рока важења квалификованог сертификата издатог према асиметричном пару кључева генерисаним у том средству, ако је квалификовани сертификат издат пре истека рока из члана 73. став 5. Закона.

Министарство ће у Регистар квалификованих средстава за креирање електронских потписа и електронских печата унети и средства из става 1. овог члана, са напоменом о начину испуњавања услова из члана 5. овог правилника и рока до ког ће се сматрати да средство испуњава те услове.

Члан 21.

Ступањем на снагу овог правилника престаје да важи Правилник о техничкотехнолошким поступцима за формирање квалификованог електронског потписа и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа („Службени гласник РС”, бр. 26/08, 13/10 и 23/15).

Члан 22.

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

Број 110-00-18/2018-12

У Београду, 20. априла 2018. године

Министар,

др **Расим Љајић,** с.р.