На основу члана 43. 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 које морају да испуњавају квалификовани електронски сертификати

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим правилником прописују се услови које морају да испуњавају квалификовани електронски сертификати за електронски потпис, електронски печат и аутентикацију сајтова.

Члан 2.

Квалификовани електронски сертификати за електронски потпис, електронски печат и аутентикацију сајтова морају да буду у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на формат и садржај електронских сертификата.

Пружалац услуге издавања квалификованог електронског сертификата (у даљем тексту: издавалац сертификата), квалификоване електронске сертификате издаје у складу са препоруком ITU X.509 и документима ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures” и IETF RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Члан 3.

Квалификовани електронски сертификат обавезно садржи једну или више изјава да се сертификат користи као квалификовани електронски сертификат (поље „qcStatements”) према документу ETSI EN 319 412-5 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 5: QCStatements” засновано на документу IETF RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, у складу са политиком издавања сертификата коју примењује издавалац сертификата и условима прописаним овим правилником за појединачне врсте сертификата.

Члан 4.

Издавалац сертификата издаје квалификовани електронски сертификат у складу са политиком издавања сертификата коју примењује за издавање сертификата, тако што формира напредни електронски потпис или напредни електронски печат на основу свог асиметричног приватног кључа.

Избор алгоритма напредног електронског потписа треба да буде у складу са документом ETSI TS 119 312 „Electronic Signatures and Infrastructures (ESI) – Cryptographic Suites”.

Квалификовани електронски сертификат обавезно садржи ознаку политике пружаоца која је примењена за издавање сертификата.

Члан 5.

Квалификовани електронски сертификат обавезно садржи тачно време издавања сертификата.

II. КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ СЕРТИФИКАТИ ЗА ЕЛЕКТРОНСКИ ПОТПИС

Члан 6.

Квалификовани електронски сертификат за електронски потпис обавезно има садржај у складу са чланом 43. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17 – у даљем тексту: Закон) у делу који се односи на сертификат за електронски потпис и потписника.

Издавалац сертификата издаје квалификоване електронске сертификате за електронски потпис у складу документом ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 2: Certificate profile for certificates issued to natural persons”.

Члан 7.

Поље „Subject” квалификованог електронског сертификата за електронски потпис садржи скуп атрибута који јединствено идентификују потписника, а најмање:

1) Атрибут „countryName” који садржи двословну ознаку земље према стандарду EN ISO 3166-1:2013 „Codes for the representation of names of countries and their subdivisions – Part 1: Country codes”, са значењем које је дефинисано политиком пружаоца услуге издавања сертификата;

2) Оба атрибута „givenName” и „surname” који редом садрже пуно име и презиме потписника, уколико сертификат не садржи псеудоним, односно само атрибут „pseudonym”, који садржи псеудоним уколико је псеудоним употребљен у сертификату;

3) Атрибут „commonName” који почиње вредностима атрибута „givenName” и „surname” раздвојених размаком уколико сертификат не садржи псеудоним, односно вредношћу атрибута „pseudonym” уколико је псеудоним употребљен у сертификату;

4) Један или више атрибута „serialNumber” који садрже идентификацију потписника према формату из документа ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures”, одељак 5.1.3.

Атрибут „commonName” не сме да се завршава са 13 или више узастопних нумеричких карактера, нити да се завршава цртицом иза које следе два словна карактера и низ нумеричких карактера.

Атрибути „givenName”, „surname”, „pseudonym” и „commonName” обавезно се представљају у UTF8String кодирању тако да сва слова буду верно представљена одговарајућим карактерима.

Атрибут „serialNumber” представља се у PrintableString кодирању према ASN.1 спецификацији у складу са документом IETF RFC 5280.

Атрибут „serialNumber” из овог члана дефинисан према документу ITU-T X.520 представља део јединственог имена потписника у пољу „Subject” и разликује се од поља „serialNumber” сертификата. Поље „serialNumber” сертификата обавезно садржи серијски број квалификованог електронског сертификата, јединствен у оквиру издаваоца квалификованог електронског сертификата у складу са чланом 43. Закона, исказан као позитиван цео број представљен сагласно документу IETF RFC 5280.

Члан 8.

Уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ и када сертификат садржи ЈМБГ, издавалац сертификата уписује ЈМБГ у само један од атрибута „serialNumber” из поља „Subject” на начин одређен у документу ETSI EN 319 412-1, одељак 5.1.3, за референцу типа „PNO” и то у формату: трословна ознака PNO (према ASCII кодирању секвенца 80, 78, 79), затим двословна ознака земље RS (према ASCII кодирању секвенца 82, 83), цртица (45 према ASCII кодирању) и на крају ЈМБГ потписника.

Члан 9.

Уколико квалификовани електронски сертификат за електронски потпис садржи један или више бројева путне исправе потписника, сваки број путне исправе се уписује у један од атрибута „serialNumber” из поља „Subject” на начин одређен у документу ETSI EN 319 412-1 одељак 5.1.3 за референцу типа „PAS” и то у формату: трословна ознака PAS (према ASCII кодирању секвенца 80, 65, 83), двословна ознака земље издаваоца путне исправе према стандарду EN ISO 3166-1:2013 представљена ASCII карактерима, цртица (45 према ASCII кодирању) и на крају број путне исправе потписника.

Уколико се у квалификованом електронском сертификату за електронски потпис појављује више атрибута са бројем путне исправе, ознака земље издаваоца путне исправе мора бити јединствена у сваком од њих.

Уколико квалификовани електронски сертификат за електронски потпис садржи број путне исправе, издавалац сертификата је обавезан да политиком издавања сертификата обезбеди да сертификат неће бити валидан након датума истека било које путне исправе чији је број садржан у сертификату.

Члан 10.

Квалификоване електронске сертификате за електронски потпис који садрже ЈМБГ или број путне исправе потписника издавалац сертификата не сме да учини јавно доступним, осим ако за то нема сагласност потписника.

Члан 11.

Квалификовани електронски сертификат за електронски потпис у пољу „Subject” може да садржи и додатне атрибуте „serialNumber” према једној од шема из стандарда ETSI EN 319 412-1, одељак 5.1.3 укључујући и локално дефинисане шеме.

Употреба локалних шема „CA:” (према ASCII кодирању секвенца 67, 65, 58) и „SN:” (према ASCII кодирању секвенца 83, 78, 58) са двословном ознаком земље RS резервисана је за потребе издаваоца сертификата на начин и када је то предвиђено политиком издаваоца сертификата.

Члан 12.

Квалификовани електронски сертификат за електронски потпис у пољу „qcStatements” обавезно садржи предефинисану изјаву „qcStatement-2” према документу IETF RFC 3739 која укључује семантички идентификатор „id-etsi-qcs-semanticsId-Natural” који је одређен у стандарду ETSI EN 319 412-1, одељак 5.1.2.

Уколико се у квалификованом електронском сертификату за електронски потпис појављује један или више атрибута „serialNumber” према шеми резервисаној за потребе издаваоца, изјава „qcStatement-2” обавезно садржи листу „nameRegistrationAuthorities” и у тој листи референцу на политику издаваоца или други документ који дефинише семантику локалне шеме, у складу са стандардом ETSI EN 319 412-1, одељак 5.1.3.

Члан 13.

Поље „Subject” квалификованог електронског сертификата за електронски потпис може да садржи и друге атрибуте који, на пример, повезују потписника са правним лицем или другом организацијом, а у складу са овим правилником и политиком издаваоца.

У пољу „Subject” атрибути „countryName” и „commonName” појављују се само једном.

Члан 14.

Поље „Key Usage” квалификованог електронског сертификата за електронски потпис мора укључивати „Non-Repudiation” тј. „contentCommitment” бит.

Члан 15.

Квалификовани електронски сертификат за електронски потпис у пољу „Certificate Policies” обавезно садржи најмање идентификатор политике QCP-n-qscd у складу са документом ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates”, одељак 4.2.5.

Члан 16.

Квалификовани електронски сертификат за електронски потпис обавезно садржи у пољу „qcStatements” изјаве QcCompliance, QcSSCD и, изјаву QcType са идентификатором „id-etsi-qcs-esign”, а према документу ETSI EN 319 412-5.

III. КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ СЕРТИФИКАТИ ЗА ЕЛЕКТРОНСКИ ПЕЧАТ

Члан 17.

Квалификовани електронски сертификат за електронски печат обавезно има садржај у складу са чланом 43. Закона у делу који се односи на сертификат за електронски печат и печатиоца.

Уколико је печатилац правно лице или физичко лице у својству регистрованог субјекта, издавалац сертификата издаје квалификоване електронске сертификате за електронски печат у складу документом ETSI EN 319 412-3 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 3: Certificate profile for certificates issued to legal persons".

Уколико је печатилац физичко лице, назив из члана 43. став 1. тачка 3. подтачка 2. Закона укључује својство у коме се лице представља, а које се доказује јавном исправом издатом на основу закона.

У случају из става 3. овог члана сходно се примењују одредбе овог правилника које се односе на физичко лице у својству регистрованог субјекта.

Члан 18.

Поље „Subject" квалификованог електронског сертификата за електронски печат садржи скуп атрибута који јединствено идентификују печатиоца, а најмање:

1) Атрибут „countryName" који садржи двословну ознаку земље према стандарду EN ISO 3166-1:2013 у којој је печатилац регистрован;

2) Атрибут „organizationName" који садржи назив односно пуно пословно име печатиоца;

3) Атрибут „commonName" који почиње вредношћу атрибута „organizationName".

Квалифковани електронски сертификат за електронски печат не сме да у пољу „Subject" садржи атрибуте „givenName" и „surname".

Члан 19.

Поље „Subject" квалификованог електронског сертификата за електронски печат може да садржи један или више атрибута „organizationIdentifier" који садрже идентификацију печатиоца према формату из документа ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures", одељак 5.1.4.

Уколико печатилац има матични број који је печатиоцу доделио Републички завод за статистику (матични број) поље „Subject" обавезно садржи атрибут „organizationIdentifier" према документу ETSI EN 319 412-1 одељак 5.1.4 за референцу локалне шеме „MB:" и то у формату: ознака MB: (према ASCII кодирању секвенца 77, 66, 58), затим двословна ознака земље RS (према ASCII кодирању секвенца 82, 83), цртица (45 према ASCII кодирању) и на крају матични број.

Уколико печатилац има порески идентификациони број (ПИБ) који је печатиоцу доделио надлежан порески орган поље „Subject” обавезно садржи атрибут „organizationIdentifier” према документу ETSI EN 319 412-1 одељак 5.1.4 за референцу типа „VAT” и то у формату: трословна ознака VAT (према ASCII кодирању секвенца 86, 65, 84), затим двословна ознака земље RS (према ASCII кодирању секвенца 82, 83), цртица (45 према ASCII кодирању) и на крају ПИБ.

Члан 20.

Квалификовани електронски сертификат за електронски печат у пољу „qcStatements” обавезно садржи предефинисану изјаву „qcStatement-2” према документу IETF RFC 3739 која укључује семантички идентификатор „id-etsi-qcs-semanticsId-Legal” који је одређен у стандарду ETSI EN 319 412-1, одељак 5.1.2.

Уколико квалификовани електронски сертификат за електронски печат садржи матични број изјава „qcStatement-2” обавезно садржи листу „nameRegistrationAuthorities” и у тој листи референцу на политику издаваоца или други документ који упућује на овај правилник и семантику локалне шеме „MB:”, у складу са стандардом ETSI EN 319 412-1, одељак 5.1.4.

Члан 21.

Атрибути „commonName” и „organizationName” обавезно се представљају у UTF8String кодирању тако да сва слова буду верно представљена одговарајућим карактерима.

Члан 22.

Поље „Subject” квалификованог електронског сертификата за електронски печат може да садржи и друге атрибуте, а у складу са овим правилником и политиком издаваоца.

У пољу „Subject” атрибути „countryName” и „commonName” појављују се само једном.

Члан 23.

Поље „Key Usage” квалификованог електронског сертификата за електронски печат мора укључивати „Non-Repudiation” тј. „contentCommitment” бит.

Члан 24.

Квалификовани електронски сертификат за електронски печат у пољу „Certificate Policies” обавезно садржи најмање идентификатор политике QCP-l-qscd у складу са документом ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates” одељак 4.2.5.

Члан 25.

Квалификовани електронски сертификат за електронски печат обавезно садржи у пољу „qcStatements” изјаве QcCompliance, QcSSCD и, изјаву QcType са идентификатором „id-etsi-qcs-seal”, а према документу ETSI EN 319 412-5.

IV. КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ СЕРТИФИКАТИ ЗА АУТЕНТИКАЦИЈУ САЈТОВА

Члан 26.

Квалификовани електронски сертификат за аутентикацију сајтова обавезно има садржај у складу са чланом 59. Закона.

Издавалац сертификата издаје квалификоване електронске сертификате за аутентикацију сајтова у складу документом ETSI EN 319 412-4 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 4: Certificate profile for web site certificates".

Члан 27.

Садржај квалификованог електронског сертификата за аутентикацију сајтова које издавалац сертификата издаје правном лицу, физичком лицу или физичком лицу као регистрованом субјекту мора да буде у складу са документом CA/Browser Forum: „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

Садржај квалификованог електронског сертификата за аутентикацију сајтова са проширеном валидацијом које издавалац сертификата издаје правном лицу или физичком лицу као регистрованом субјекту мора да буде у складу са документом CA/Browser Forum: „Guidelines for The Issuance and Management of Extended Validation Certificates".

Члан 28.

Квалификовани електронски сертификат за аутентикацију сајтова у пољу „Certificate Policies" обавезно садржи најмање идентификатор политике QCP-w у складу са документом ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates" одељак 4.2.5.

Члан 29.

Квалификовани електронски сертификат за аутентикацију сајтова обавезно садржи у пољу „qcStatements" изјаве QcCompliance и QcType са идентификатором „id-etsi-qcs-web", а према документу ETSI EN 319 412-5.

V. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 30.

Сертификациона тела из члана 73. став 3. Закона могу да издају квалификоване електронске сертификате за електронски потпис у складу са Правилником о ближим условима за издавање квалификованих електронских сертификата („Службени гласник РС", број 26/08) до дана доношења акта Министарства о испуњености обавезе из члана 73. став 5. Закона.

Члан 31.

Даном ступања на снагу овог правилника престаје да важи Правилник о ближим условима за издавање квалификованих електронских сертификата („Службени гласник РС”, број 26/08).

Члан 32.

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

Број 110-00-17/2018-12

У Београду, 20. априла 2018. године

Министар,

др **Расим Љајић,** с.р.