Euroopa Liidu
Teataja

ET
L-seeria

2025/2531

17.12.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/2531,

16. detsember 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses kvalifitseeritud elektrooniliste arvestusraamatute võrdlusstandardite ja spetsifikatsioonidega

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, ([1]) eriti selle artikli 45l lõiget 3,

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu määrusega (EL) 2024/1183 ([2]) lisati määrusesse (EL) nr 910/2014 uute usaldusteenuste ja kvalifitseeritud usaldusteenuste loetelu, kuhu kuulus ka elektrooniliste andmete kandmine kvalifitseeritud elektroonilisse arvestusraamatusse. Komisjon peab koostama selliste teenuste võrdlusstandardite loetelu ja kehtestama vajaduse korral nende spetsifikatsioonid.

(2) Elektrooniline arvestusraamat on elektrooniliste andmekirjete jada, mille eesmärk on tagada selliste andmike terviklus ja nende kronoloogilise järjestuse täpsus. Selleks et tagada kvalifitseeritud elektroonilisse arvestusraamatusse salvestatavate andmete kronoloogiline järjestus, järjepidevus ja usaldusväärsus, on vaja kehtestada ühtsed spetsifikatsioonid elektrooniliste andmete kandmise kohta kvalifitseeritud elektroonilisse arvestusraamatusse.

(3) Määruse (EL) nr 910/2014 artikli 45l lõike 2 kohane eeldus, et nõuded on täidetud, peaks kehtima ainult juhul, kui kvalifitseeritud usaldusteenused elektrooniliste andmete kandmiseks kvalifitseeritud elektroonilisse arvestusraamatusse vastavad käesolevas määruses esitatud standarditele. Standardid peaksid kajastama väljakujunenud tavasid ja olema asjaomastes sektorites laialdaselt tunnustatud. Neid tuleks kohandada, et lisada täiendavad kontrollimeetmed, mis tagavad kvalifitseeritud usaldusteenuse turvalisuse ja usaldusväärsuse.

(4) Kui usaldusteenuse osutaja järgib käesoleva määruse lisas sätestatud nõudeid, peaksid järelevalveasutused eeldama, et määruse (EL) nr 910/2014 asjaomased nõuded on täidetud, ning võtma sellist eeldust usaldusteenuse osutajale kvalifitseeritud staatuse andmisel või selle staatuse kinnitamisel nõuetekohaselt arvesse. Samas võib kvalifitseeritud usaldusteenuse osutaja kasutada ka muid võimalusi tõendada vastavust määruse (EL) nr 910/2014 nõuetele.

(5) Komisjon hindab regulaarselt uusi tehnoloogialahendusi, tavasid, standardeid ja tehnilisi spetsifikatsioone. Kooskõlas määruse (EL) 2024/1183 põhjendusega 75 peaks komisjon käesoleva määruse läbi vaatama ja seda vajaduse korral ajakohastama, et viia see kooskõlla üleilmsete suundumuste, uute tehnoloogialahenduste, tavade, standardite või tehniliste spetsifikatsioonidega ning et järgida siseturu häid tavasid.

([1]) ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Euroopa Parlamendi ja nõukogu 11. aprilli 2024. aasta määrus (EL) 2024/1183, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega (ELT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Käesoleva määruse alusel toimuvate isikuandmete töötlemise toimingute suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679 ([3]) ning kui see on asjakohane, Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ, ([4]) võttes samuti arvesse Euroopa Andmekaitsenõukogu dokumenti „Guidelines 02/2025 on processing of personal data through blockchain technologies“ ([5]).

(7) Kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([6]) artikli 42 lõikega 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 21. oktoobril 2025 ([7]).

(8) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikli 48 alusel loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Võrdlusstandardid ja spetsifikatsioonid

Määruse (EL) nr 910/2014 artikli 45l lõikes 3 osutatud võrdlusstandardid ja spetsifikatsioonid kvalifitseeritud elektroonilistele arvestusraamatutele on esitatud käesoleva määruse lisas.

Artikkel 2

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 16. detsember 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

([3]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers.

LISA

Kvalifitseeritud elektrooniliste arvestusraamatute ja võrdlusstandardite loetelu

1. Käesolevas määruses kasutatakse järgmisi mõisteid:

   a) „lõplikkus“ – elektroonilises arvestusraamatus sisalduva andmiku olek, mille puhul see on muutunud tagasipööramatuks ja seda ei saa muuta ega kustutada;

   b) „hajusraamat“ – elektrooniline arvestusraamat, mis jaguneb ühele hajusraamatsolmede kogumile ja on nende hajusraamatsolmede vahel konsensusmehhanismiga sunkroniseeritud;

   c) „hajusraamatsõlm“ – hajusraamattehnoloogia vahend või protsess, mis osaleb võrgus ja talletab elektroonilise arvestusraamatu andmike täieliku või osalise duplikaadi;

   d) „hajusraamatvõrk“ – hajusraamatsolmede võrk, mis moodustab hajusraamatsüsteemi;

   e) „hajusraamatsüsteem“ – hajusraamatut teostav süsteem;

   f) „konsensus“ – hajusraamatsõlmede vaheline kokkulepe, mis puudutab tehingute valideeritust ning valideeritud tehingute kooskõlalise ja järjestatud kogumi hoidmist hajusraamatsüsteemis;

   g) „konsensusmehhanism“ – konsensuse saavutamise reeglid ja protseduurid;

   h) „juhtreeglid“ – protokollide, poliitika ja mehhanismide kogu, mis määrab ära selle, kuidas hajusraamatusüsteem toimub, kuidas andmeid valideeritakse ja elektroonilisse arvestusraamatusse lisatakse ning kuidas toimub süsteemi osaliste interaktsioon;

   i) „tehing“ – elektroonilise arvestusraamatu tööprotsessi vähim üksus;

   j) „tööprotsess“ – toimingujada(d), mis on vajalikud elektroonilise arvestusraamatu juhtreeglitele vastava tulemi saamiseks;

   k) „valideeritud tehing“ – tehing, mille nõutavat terviklust, autentsust ja vastavust protokollispetsiifilistele tingimustele on elektroonilise arvestusraamatu juhtreeglite kohaselt kontrollitud;

   l) „krüptolink“ – sobilike krüptomeetoditega loodud viide andmetele, et tagada viidatud andmete terviklus, autentsus või jälitatavus ning andmike õige järjestus;

   m) „arvestusraamatu aruanne“ – elektroonilise arvestusraamatu andmike kontrollitavate andmete struktureeritud väljavõte, mis annab ülevaate konkreetsetest toimingutest, olekutest või vastavusest eeldefineeritud reeglitele;

   n) „kvalifitseeritud elektroonilise arvestusraamatu pakkuja“ – kvalifitseeritud usaldusteenuse osutaja, kes osutab usaldusteenust, mis seisneb andmete jäädvustamises kvalifitseeritud elektroonilisse arvestusraamatusse;

   o) „kvalifitseeritud hajusraamat“ – hajusraamat, mis vastab kvalifitseeritud elektroonilisele arvestusraamatule esitatavale nõuetele.

2. Kui kvalifitseeritud usaldusteenuse osutaja peab koostama arvestusraamatu aruande, koostatakse see automaatselt.

3. Kvalifitseeritud elektroonilise arvestusraamatu pakkujad loovad elektroonilisi andmeid ja jäädvustavad neid elektroonilisse arvestusraamatusse ning ajakohastavad ja haldavad kvalifitseeritud elektroonilist arvestusraamatut järgmistes dokumentides esitatud spetsifikatsioonide kohaselt.

   a) Kõigi kvalifitseeritud elektrooniliste arvestusraamatute pakkujate puhul standard ETSI EN 319 401 v3.1.1 (2024-06) järgmiste kohandustega:

      — 2.1. Viited normidele

        [1] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“, avaldanud Euroopa Liidu Küberturvalisuse Amet (ENISA).

[2] IETF RFC 7515 (mai 2015): „JSON Web Signature (JWS)“.

[3] FIPS PUB 140-3 (2019) „Security Requirements for Cryptographic Modules“.

[4] Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega.

[5] Komisjoni 18. detsembri 2024. aasta rakendusmäärus (EL) 2024/3144, millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

[6] ISO/IEC 15408:2022 (1.–5. osa): „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security“.

— 6.1. Usaldusteenuse tavade määrang

  — REQ-6.1-12 Elektroonilise arvestusraamatu tavade määrang peab sisaldama vähemalt järgmist teavet:

    — elektroonilise arvestusraamatu platvormi funktsionaalsed ja tehnilised võimalused ning selle kasutamine andmete elektroonilisse arvestusraamatusse jäädvustamise kui kvalifitseeritud usaldusteenuse kestel;

    — teenuse osutamisel kasutatavad konkreetsed mehhanismid andmete päritolu autentimiseks;

    — teenuse osutamisel kasutatavad konkreetsed mehhanismid kronoloogiliseks järjestamiseks;

    — kui see on asjakohane, andmike järjestuse tagamiseks kasutatav krüptolink;

    — kui see on asjakohane, konsensusmehhanism, millega tagatakse arvestusraamatus talletatud andmike ja tehingute lõplikkus ja terviklus, sealhulgas võimalik ooteaeg enne lõplikkuse ja tervikluse saavutamist;

    — teenuse osutamisel kasutatavad konkreetsed mehhanismid andmete tervikluse tagamiseks.

— 6.2. Tingimused

  — REQ-6.2-03 Usaldusteenuse abonentidele ja selle kasutajatele teatatakse enne lepingulise suhte loomist selgel, arusaadaval ja hõlpsasti mõistetaval viisil avalikus keskkonnas ja eraldi täpsed tingimused, sealhulgas eespool loetletud punktid.

— 6.3. Infoturvapoliitika

  — REQ-6.3-04X Usaldusteenuse osutaja kehtestab menetlused, et teatada järelevalveasutusele kõigist muudatustest usaldusteenuse osutamises, järgides talitlusnõudeid ning vastavaid õigusakte. Usaldusteenuse osutaja esitab järelevalveasutusele teate vähemalt:

    — kuu aega enne mis tahes muudatuse tegemist;

    — kolm kuud enne usaldusteenuse osutamise kavandatud lõpetamist.

— 7.2. Personal

  — REQ-7.2-04X Usaldusteenuse osutaja usaldusrolle täitvad töötajad peavad suutma täita erialaste teadmiste, kogemuste ja kvalifikatsiooni nõude ametliku koolituse ja tõendite või tegeliku töökogemuse või nende kahe kombinatsiooni kaudu.

— REQ-7.2-05X See hõlmab uute ohtude ja käibivate turvatavade teemalist teadmiste korrapärast (vähemalt iga 12 kuu järel) ajakohastamist.

— 7.5. Krüptograafiline kontroll

— REQ-7.5-01X Krüptovõtmete, krüptoalgoritmide ja krüptoseadmete haldamiseks kogu nende elutsükli kestel peavad kehtima kohased turvameetmed, lähtudes vajaduse korral krüptograafilise kohandatavuse põhimõttest.

— REQ-7.5-02 Usaldusteenuse osutamiseks peab usaldusteenuse osutaja valima Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1] vastavad sobilikud krüptomeetodid ja neid kasutama.

Ennekõike:

— REQ-7.5-03 kvalifitseeritud elektrooniliste arvestusraamatute pakkujad teevad kindlaks elektroonilise arvestusraamatu andmike päritolu. Selleks kasutavad nad kvalifitseeritud sertifikaatidel põhinevaid täiustatud e-allkirju või kvalifitseeritud sertifikaatidel põhinevaid e-templeid, mille teenuse kasutajad on loonud kooskõlas järgmiste standardite ja spetsifikatsioonidega:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). „Electronic Signatures and Trust Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures“.

b) ETSI EN 319 132-1 V1.3.1 (2024-07). „Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures“.

c) ETSI TS 119 182-1 V1.2.1 (2024-07). „Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures“ järgmise kohandusega:

— 5.1.8 x5c (X.509 sertifikaatide ahel) päise parameeter

— JAdESi allkiri peab sisaldama standardi IETF RFC 7515 [2] punkti 4.1.6 määratletud x5c päise parameetrit kas päise signeeritud või signeerimata parameetri kujul.

— x5c päise parameetri semantika peab vastama standardi IETF RFC 7515 [2] punkti 4.1.6 määratlusele.

— x5c päise parameetri süntaks peab vastama standardi IETF RFC 7515 [2] punkti 4.1.6 määratlusele.

— REQ-7.5-04: kvalifitseeritud elektrooniliste arvestusraamatute pakkujad tagavad elektroonilise arvestusraamatu andmike kordumatu kronoloogilise järjestuse. Selleks kasutatakse krüptolinke, mille alus on räside loetelu või räsipuu, mille juures kasutatakse krüptograafilisi räsifunktsioone kooskõlas järgmiste spetsifikatsioonide ja standarditega:

a) SHA-256 või parem, mis vastab Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1].

b) SHA3-256 või parem, mis vastab Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1].

Teise võimalusena võivad kvalifitseeritud elektroonilise arvestusraamatu pakkujad, kes kasutavad elektroonilise arvestusraamatu andmestike kordumatu kronoloogilise järjestuse tagamiseks aja registreerimist, kasutada kvalifitseeritud ajatempleid.

— REQ-7.5-05 Kvalifitseeritud elektrooniliste arvestusraamatute pakkujad tagavad elektroonilisse arvestusraamatusse jäädvustatavate andmike tervikluse. Selleks kasutavad nad kvalifitseeritud sertifikaatidel põhinevat täiustatud e-allkirju või kvalifitseeritud sertifikaatidel põhinevaid e-templeid kooskõlas järgmiste standardite ja spetsifikatsioonidega:

  a) igasugune allkirja- või templivorming, mis vastab Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1];

  b) SHA-256 või parem, mis vastab Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1];

  c) SHA3-256 või parem, mis vastab Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“[1].

  d) Kvalifitseeritud elektrooniliste arvestusraamatute pakkujad tagavad, et kõik hilisemad muudatused elektroonilisse arvestusraamatusse jäädvustatud andmetes on võimalik viivitamatult avastada.

— REQ-7.5-06 Digiallkirjamehhanismide kasutamise korral tuleb kvalifitseeritud elektroonilise arvestusraamatu pakkuja privaatseid signeerimisvõtmeid hoida ja kasutada turvalises krüptoseadmes, mis kujutab enesest kooskõlas järgmiste dokumentidega sertifitseeritud usaldusväärset süsteemi:

  a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 ([1]) [6] või infotehnoloogia turvalisuse hindamise ühiskriteeriumidega, versioon CC:2022, 1.–5. osa, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised ning mis on sertifitseeritud vähemalt EAL 4. tasemel, või

  b) Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) ([2]) ([3]) [4][5] vähemalt EAL 4. tasemel või

  c) kuni 31.12.2030, FIPS PUB 140-3 ([4]) [3] 3. tase.

See sertifitseerimine peab käsitlema vastavust sellisele turvasihile või kaitseprofiilile või moodulprojektile ja turvadokumentatsioonile, mis vastab käesoleva dokumendi nõuetele, tuginedes riskianalüüsile ning võttes arvesse füüsilisi ja muid mittetehnilisi turbemeetmeid;

Kui turvalisel krüptoseadmel on EUCC [4][5] sertifikaat, siis seda seadet konfigureeritakse ja kasutatakse vastavalt kõnealusele sertifikaadile.

([1]) ISO/IEC 15408:2022 (1.–5. osa): „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security“.
([2]) Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).
([3]) Komisjoni 18. detsembri 2024. aasta rakendusmäärus (EL) 2024/3144, millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust (ELT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).
([4]) FIPS PUB 140-3 (2019): „Security Requirements for Cryptographic Modules“.

— 7.8. Võrguturve

— REQ-7.8-14X Nõude REQ-7.8-13 kohane nõrkuste skaneerimine tuleb teha vähemalt kord kvartalis.

— REQ-7.8-18X Nõude REQ-7.8-17X kohane läbistustest tuleb teha vähemalt kord aastas.

— REQ-7.8-21X: tulemüürid peavad olema konfigureeritud ka nii, et oleks välistatud kõik protokollid ja juurdepääsud, mis ei ole usaldusteenuse osutaja tööks vajalikud.

— 7.9.1. Seire ja logimine

— REQ-7.9.1-02X Seiretegevuse juures arvestatakse kõigi kogutud või analüüsitud andmete tundlikkusega.

— 7.12. Usaldusteenuse osutaja tegevuse lõpetamine ja tegevuse lõpetamise kavad

— REQ-7.12-02A Usaldusteenuse osutaja tegevuse lõpetamise kava peab vastama nõuetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

b) Lisaks sellele kõigi kvalifitseeritud elektroonilise arvestusraamatu selliste pakkujate puhul, kes kasutavad hajusraamatud tehnoloogiat:

1) ISO 23257:2022 „Blockchain and distributed ledger technologies – Reference architecture“ punkt 9, kus on esitatud täielik kirjeldus hajusraamatsüsteemi, sellele vastava hajusraamatvõrgu ja hajusraamatsõlmede kohta;

2) ISO/TS 23635:2022. „Blockchain and distributed ledger technologies – Guidelines for governance“ seoses kirjalike ja avalikult kättesaadavate tegevuspõhimõtete ja tavadega, mis puudutavad nende pakutavate elektroonilise arvestusraamatu teenuste juhtimisstruktuuri.