2025/1929

30.9.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1929,

29. september 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses kuupäeva ja ajahetke andmetega sidumisega ning ajaallikate täpsuse kindlakstegemisega, et pakkuda kvalifitseeritud e-ajatempleid

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 42 lõiget 2,

ning arvestades järgmist:

(1) Kvalifitseeritud e-ajatemplitel on digikeskkonnas oluline roll, kuna need edendavad üleminekut traditsioonilistelt paberipõhistelt protsessidelt samaväärsetele elektroonilistele protsessidele. Kvalifitseeritud e-ajatempel seob kuupäeva ja ajahetke kohta käiva teabe elektrooniliste andmetega ning aitab seega tagada märgitud kuupäeva ja ajahetke täpsuse ja nende digitaalsete dokumentide tervikluse, millega kuupäev ja ajahetk on seotud.

(2) Määruse (EL) nr 910/2014 artikli 42 lõikes 1a sätestatud eeldust tingimustele vastamise kohta tuleks kohaldada üksnes siis, kui kvalifitseeritud ajatemplite väljastamiseks kvalifitseeritud usaldusteenused täidavad käesolevas määruses sätestatud standardite nõudeid. Need standardid peaksid kajastama väljakujunenud tavasid ja olema asjaomastes sektorites laialdaselt tunnustatud. Neid standardeid tuleks kohandada, et lisada täiendavad kontrollimeetmed, mis tagavad kvalifitseeritud usaldusteenuse ning kuupäeva ja ajahetke andmetega sidumise turvalisuse ja usaldusväärsuse ja ajaallika täpsuse.

(3) 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. Kvalifitseeritud usaldusteenuste osutaja võib siiski kasutada muid võimalusi, et tõendada vastavust määruse (EL) nr 910/2014 nõuetele.

(4) Komisjon hindab regulaarselt uusi tehnoloogialahendusi, tavasid, standardeid ja tehnilisi kirjeldusi. Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1183 ([2]) põhjenduse 75 kohaselt peaks komisjon käesoleva rakendusmääruse läbi vaatama ja seda vajaduse korral ajakohastama, et tagada selle kooskõla üleilmsete arengusuundumustega ja uute tehnoloogialahenduste, standardite või tehniliste kirjeldustega ning järgida siseturu parimaid tavasid.

(5) Isikuandmete selliste töötlemistoimingute suhtes, mis toimuvad käesoleva määruse alusel, kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679 ([3]) ning vajaduse korral Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([4]).

([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).

([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).

(6) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([5]) artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 6. juunil 2025.

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

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) nr 910/2014 artikli 42 lõikes 2 osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse lisas.

Artikkel 2

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 29. september 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

([5]) 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).

LISA

Kvalifitseeritud ajatempliteenuste võrdlusstandardite ja kirjelduste loetelu

Kohaldatakse standardeid ETSI EN 319 421 V1.3.1 ([1]) (ETSI EN 319 421) ja ETSI EN 319 422 V1.1.1 ([2]) (ETSI EN 319 422) järgmiste kohandustega:

1. ETSI EN 319 421

   1) 2.1 Viited normidele

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

      — [4] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“.

      — [5] ETSI EN 319 422 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles“.

      — [6] kehtetu.

      — [9] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“, avaldanud Euroopa Liidu Küberturvalisuse Amet (ENISA) ([3]).

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

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

   2) 3.1 Mõisted

      — sertifikaadi kehtivusaeg: ajavahemik parameetrist notBefore kuni parameetrini notAfter (kaasa arvatud) mille jooksul sertifitseerimisasutus tagab, et ta hoiab teavet sertifikaadi staatuse kohta.

   3) 3.3 Lühendid

      — EUCC – Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava

   4) 6.2 Usaldusteenuse tavade määrang

      — OVR-6.2–03 Ajatembeldusasutus lisab kinnituse oma ajatembeldusteenuse käideldavuse kohta oma avalikustamisavaldusse.

   5) 7.3 Personalialane turvalisus

      — OVR-7.3–02 Ajatembeldusasutuse usaldusrolle täitvad töötajad ja kui see on asjakohane, tema usaldusrolle täitvad alltöövõtjad peavad suutma täita erialaste teadmiste, kogemuste ja kvalifikatsiooni nõude ametliku koolituse ja tõendite või tegeliku töökogemuse või nende kahe kombinatsiooni kaudu.

      — OVR-7.3–03 Nõude OVR-7.3–02 täitmine hõlmab korrapärast ajakohastamist (vähemalt iga 12 kuu järel) uute ohtude ja praeguste turvatavade kohta.

([1]) EN 319 421 - Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time Stamps, V1.3.1.
([2]) EN 319 422 - Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles, V1.1.1 (2016-03). https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) ELT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Ajatembeldusüksuse võtme genereerimine

— TIS-7.6.2–03 Ajatembeldusüksuse võtme(te) genereerimine peab toimuma turvalises krüptoseadmes, mis on usaldusväärne süsteem, mis on sertifitseeritud kooskõlas järgmiste dokumentidega:

a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 [3] 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) EUCC [10][11] vähemalt EAL 4. tasemel või

c) kuni 31.12.2030, FIPS PUB 140–3 [7] 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 [10][11] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt sellele sertifikaadile.

— TIS-7.6.2–04 kehtetu.

— MÄRKUS 3 kehtetu

— TIS-7.6.2-05A Ajatembeldusüksuse võtme genereerimise algoritm, sellest tulenev signeerimisvõtme pikkus ja signeerimisalgoritm, mida kasutatakse vastavalt ajatemplite signeerimiseks ja ajatembeldusüksuse avaliku võtme sertifikaatide signeerimiseks, peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[9].

— MÄRKUS 4 kehtetu

— TIS-7.6.2–06 Ajatembeldusüksuse signeerimisvõtme võib teise turvalisse krüptoseadmesse eksportida ja importida ainult siis, kui selline eksportimine ja importimine toimub turvaliselt ja kooskõlas nende seadmete sertifikaatidega.

7) 7.6.3 Ajatembeldusüksuse privaatvõtme kaitsmine

— TIS-7.6.3–02 Ajatembeldusüksuse privaatvõtit tuleb hoida ja kasutada turvalises krüptoseadmes, mis on usaldusväärne süsteem, mis on sertifitseeritud kooskõlas järgmiste dokumentidega:

a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 [3] või infotehnoloogia turvalisuse hindamise ühiskriteeriumidega, versioon CC:2002, 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) [10][11] vähemalt EAL 4. tasemel või

c) kuni 31.12.2030, FIPS PUB 140–3 [7] 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 [10][11] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt sellele sertifikaadile.

— TIS-7.6.3–03 kehtetu.

— MÄRKUS 2 kehtetu

8) 7.6.7 Ajatembeldusüksuse võtme elutsükli lõpp

— TIS-7.6.7-03A Ajatembeldusüksuse privaatvõtmete aegumiskuupäev peab olema kooskõlas dokumendiga „Agreed Cryptographic Mechanisms“[9].

— MÄRKUS 1 kehtetu

9) 7.10 Võrgu turvalisus

— OVR-7.10–05 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8–13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— OVR-7.10–06 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— OVR-7.10–07 Tulemüürid tuleb konfigureerida tõrjuma kõiki ajatembeldusasutuse tegevuseks mittevajalikke protokolle ja juurdepääse.

10) 7.14 Ajatembeldusasutuse tegevuse lõpetamine ja tegevuse lõpetamise kavad

— OVR-7.14-01A Usaldusteenuse osutaja tegevuse lõpetamise kava peab vastama nõetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.4] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

2. ETSI EN 319 422

1) 2.1 Viited normidele

— [5] kehtetu.

— [6] kehtetu.

— [8] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: dokument „Agreed Cryptographic Mechanisms“.

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Kasutatavad räsialgoritmid

— Kohaldada tuleb järgmist tingimust:

Räsialgoritmid, mida kasutatakse ajatempliga varustatava teabe räsimiseks, ajatempli eeldatav kestus ja valitud räsifunktsioonid võrreldes ajaga peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[8].

— MÄRKUS kehtetu.

3) 4.2.3 Toetatavad algoritmid

— Kohaldada tuleb järgmist tingimust:

Toetatavad ajatemplitalongi signatuuri algoritmid peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[8].

— MÄRKUS kehtetu.

4) 4.2.4 Toetatavad võtmepikkused

— Kohaldada tuleb järgmist tingimust:

Valitud signatuurialgoritmi jaoks kasutatavad signatuurialgoritmi võtmepikkused peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“.

— MÄRKUS kehtetu.

5) 5.1.3 Toetatavad algoritmid

— Kohaldada tuleb järgmist tingimust:

Toetatavad ajatempliandmete räsialgoritmid, ajatempli eeldatav kestus ja valitud räsifunktsioonid võrreldes ajaga peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [8].

— MÄRKUS kehtetu.

6) 5.2.3 Kasutatavad algoritmid

— Kohaldada tuleb järgmist tingimust:

Räsialgoritmid, mida kasutatakse ajatempliga varustatava teabe räsimiseks, ja ajatemplitalongi signatuuri algoritmid peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [8].

— MÄRKUS kehtetu.

7) 6.3 Nõuded võtmepikkustele

— Kohaldada tuleb järgmist tingimust:

Ajatembeldusüksuse sertifikaadi valitud signatuurialgoritmi võtmepikkus peab olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [8].

— MÄRKUS kehtetu.

8) 6.5 Nõuded algoritmile

— Kohaldada tuleb järgmist tingimust:

Ajatembeldusüksuse avaliku võtme ja ajatembeldusüksuse sertifikaadi signatuuri jaoks tuleb kasutada algoritme, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [8].

— MÄRKUS kehtetu.

9) 7 Toetatavate transpordiprotokollide profiilid

— Ajatembeldusklient ja ajatembeldusserver peavad toetama ajatembeldusprotokolli HTTPSi [9] kaudu, nagu on kindlaks määratud IETF RFC 3161 [1] punktis 3.4.

10) 8 Krüptoalgoritmide objektiidentifikaatorid

— Kohaldada tuleb järgmist tingimust:

Ajatembeldusüksuse avaliku võtme ja ajatembeldusüksuse sertifikaadi signatuuri jaoks tuleb kasutada algoritme kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [8].

11) 9.1 Määrusele vastavuse avaldus

— Kui ajatembeldusasutus kinnitab, et ajatemplitalong on kvalifitseeritud e-ajatempel vastavalt määrusele (EL) nr 910/2014 [i.2], peab selle ajatemplitalongi laiendiväli sisaldama qcStatements-laiendi üht eksemplari vastavalt süntaksile, mis on määratletud dokumendi IETF RFC 3739 [i.3] punktis 3.2.6.

— qcStatements-laiend peab sisaldama B lisas määratletud lause „esi4-qtstStatement-1“ üht eksemplari.

— Laiendi qcStatements lauseid ei märgita kriitilise tähtsusega lauseteks.