Euroopa Liidu
Teataja

ET
L-seeria

2025/1946

30.9.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1946,

29. september 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kvalifitseeritud säilitamisteenustega

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 34 lõiget 2 ja artiklit 40,

ning arvestades järgmist:

(1) Kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kvalifitseeritud säilitamisteenused tagavad nende e-allkirjade ja e-templite pikaajalise tervikluse, autentsuse, olemasolu tõendamise ja säilitamistõendite käideldavuse. See võimaldab tõendada nende õiguslikku kehtivust pika aja jooksul ja tagab, et neid saab valideerida sõltumata tehnoloogia arengust tulevikus. Neid teenuseid osutatakse sõltumatult või mõne muu kvalifitseeritud usaldusteenuse, näiteks kvalifitseeritud e-arhiveerimise teenuse osana.

(2) Määruse (EL) nr 910/2014 artikli 34 lõikes 1a ja artiklis 40 sätestatud eeldust tingimustele vastamise kohta tuleks kohaldada üksnes siis, kui kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite säilitamise kvalifitseeritud teenused täidavad käesolevas määruses sätestatud standardite nõudeid. Need 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 ja suutlikkuse kontrollida allkirjade ja templite kvalifitseeritud staatust ja tehnilist kehtivust aja jooksul.

(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 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 määruse 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.

([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).

(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]).

(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

Võrdlusstandardid ja kirjeldused

Määruse (EL) nr 910/2014 artikli 34 lõikes 2 ja artiklis 40 osutatud võrdlusstandardid ja kirjeldused 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, 29. september 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]) 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

Artiklis 2 osutatud võrdlusstandardite ja kirjelduste loetelu

Kohaldatakse standardeid ETSI TS 119 511 V1.1.1 (2019-06) (ETSI TS 119 511) ja ETSI TS 119 172-4 V1.1.1 (2021-05) (ETSI TS 119 172-4) järgmiste kohandustega:

1. ETSI TS 119 511

1) 2.1 Viited normidele

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

— [2] ETSI TS 119 612 (V2.3.1) „Electronic Signatures and Infrastructures (ESI); Trusted Lists“.

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

— [6] Komisjoni rakendusmäärus (EL) 2024/482, ([1]) millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega.

— [7] Komisjoni rakendusmäärus (EL) 2024/3144, millega muudetakse rakendusmäärust (EL) 2024/482 ([2]) kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

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

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists“.

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

2) 3.1 Mõisted

— turvaline krüptoseade: seade, mis sisaldab kasutaja privaatvõtit, kaitseb seda võtit rikkumise eest ja pakub kasutajale allkirja andmise ja dekrüpteerimisfunktsioone.

3) 6.4 Säilitamisprofiilid

— OVR-6.4-08A [WTS][WOS] Tõendi eeldatav kehtivus peab olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[8].

— MÄRKUS 3 kehtetu

4) 6.5 Säilitamistõendite poliitika

— OVR-6.5-04A Kasutatavad krüptoalgoritmid peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[8].

— MÄRKUS 1 kehtetu

([1]) ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) ELT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Personal

— OVR-7.2-02 Säilitusteenuse osutaja 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-7.2-03 Nõude OVR-7.2-02 täitmine hõlmab korrapärast ajakohastamist (vähemalt iga 12 kuu järel) uute ohtude ja praeguste turvatavade kohta.

6) 7.5 Krüptograafilised turvameetmed

— OVR-7.5-05 [TINGIMUSLIK] Kui säilitusteenuse osutaja signeerib säilitamistõendi (osa), tuleb säilitusteenuse osutaja privaatset signeerimisvõtit 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 [10] 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 [6][7] vähemalt EAL 4. tasemel või

(c) kuni 31.12.2030, FIPS PUB 140-3 [5] 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 [6][7] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt sellele sertifikaadile.

— OVR-7.5-06 [TINGIMUSLIK] kehtetu.

— OVR-7.5-07 [TINGIMUSLIK] Kui säilitusteenuse osutaja signeerib säilitamistõendi (osa), peavad säilitusteenuse osutaja privaatsete signeerimisvõtmete varukoopiad olema turvalise krüptoseadmega kaitstud, et tagada nende terviklus ja konfidentsiaalsus, enne kui neid võib talletada väljaspool seda seadet.

— OVR-7.5-08 Säilitusteenuse osutaja privaatse signeerimisvõtme võib teise turvalisse krüptoseadmesse eksportida ja importida ainult siis, kui selline eksportimine ja importimine toimub turvaliselt ja kooskõlas nende seadmete sertifikaatidega.

7) 7.8 Võrgu turvalisus

— OVR-7.8-03 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— OVR-7.8-04 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— OVR-7.8-05 Tulemüürid tuleb konfigureerida tõrjuma kõiki säilitusteenuse osutaja tegevuseks mittevajalikke protokolle ja juurdepääse.

8) 7.14 Krüptoseire

— OVR-7.14-03A Nõuetes OVR-7.14.01 ja OVR-7.14.02 osutatud krüptograafiliste algoritmide hindamine peab olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[8].

— MÄRKUS kehtetu.

9) 7.12 Usaldusteenuse osutaja tegevuse lõpetamine ja tegevuse lõpetamise kavad

— OVR-7.12-01A Usaldusteenuse osutaja tegevuse lõpetamise kava peab vastama nõuetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.2] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

10) 7.17 Tarneahel

— OVR-7.17-01 Kohaldatakse standardi ETSI EN 319 401 [1] punktis 7.14 nimetatud nõudeid.

11) A lisa (normatiivne): Määruse (EL) nr 910/2014 artiklis 34 määratletud kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenus

— OVR-A-02 [PDS][PDS+PGD]

(a) Säilitamisteenus peab säilitama kogu teabe, mis on vajalik, et kontrollida e-allkirja või e-templi kvalifitseeritud staatust, ja mis ei oleks enne säilitamisperioodi lõppu avalikult kättesaadav;

(b) säilitamisteenus peab tagama, et säilitatav teave on kogu säilitamisperioodi kestel selline, et kui see antakse sisendiks standardi ETSI TS 119 172-4 [9] punktis 4.4 sedastatud protsessile, määrab selle protsessi väljund selgelt ära, kas e-allkiri või e-tempel oli selle säilitamise ajal tehniliselt sobiv ELi kvalifitseeritud e-allkirja või ELi kvalifitseeritud e-templi rakendamiseks.

— OVR-A-03 [PDS][PDS+PGD] Säilitamistõendites kasutatavad ajatemplid peavad olema kvalifitseeritud ajatemplid määruse (EL) nr 910/2014 [i.2] tähenduses.

2. ETSI TS 119 172-4

1) 2.1 Viited normidele

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation“.

— Kõiki viiteid standardile ETSI TS 119 102-1 [1] käsitatakse viidetena standardile ETSI EN 319 102-1 [1].

— [2] ETSI TS 119 612 (V2.3.1) „Electronic Signatures and Infrastructures (ESI); Trusted Lists“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation“.

2) 4.2 Valideerimispiirangud ja valideerimisprotseduurid, nõue REQ-4.2-03, jaotis „X.509 valideerimispiirangud’, punkt c:

— i) Kui lõppolemi sertifikaat kujutab endast usaldusankrut, ei kasutata parameetrit RevocationChecking-Constraints.

— ii) Kui lõppolemi sertifikaat ei kujuta endast usaldusankrut, määratakse parameetri RevocationChecking-Constraints väärtuseks „eitherCheck“, mis on määratletud standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.1.

— iii) Kui lõppolemi sertifikaat kujutab endast usaldusankrut, ei kasutata parameetrit RevocationFreshness-Constraints, mis on määratletud standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.2.

— iv) Kui lõppolemi sertifikaat ei kujuta endast usaldusankrut, kasutatakse standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.2 määratletud parameetrit RevocationFreshnessConstraints, mille maksimumväärtus signeerimissertifikaadi kohta on 0, tagamaks, et tühistamisteavet aktsepteeritakse ainult juhul, kui see on välja antud pärast parimat signeerimisaega (*best signature time*). Parameetrile RevocationFreshnessConstraints ei määrata väärtust muude sertifikaatide puhul peale signeerimissertifikaadi, sealhulgas ajatempleid toetavate sertifikaatide puhul.

3) 4.3 Signatuuri valideerimise ja kohaldatavuseeskirjade kontrollimise tavade nõuded

— REQ-4.3-02 Signatuuri valideerimise rakendused peavad olema kooskõlas standardiga ETSI TS 119 101 [13].

4) 4.4 Tehnilise kohaldatavuse (eeskirjade) kontrollimise protsess

— REQ-4.4.2-03 Kui mõni nõudes REQ-4.4.2-01 nimetatud kontrollidest ebaõnnestub, siis:

— protsess seiskub;

— loetakse signatuur tehniliselt määramatuks, st seda ei peeta ei ELi kvalifitseeritud e-allkirjaks ega ELi kvalifitseeritud e-templiks;

— eespool nimetatud tulemus ja kõigi vaheprotsesside protsesside tulemusi kajastatakse signatuuri kohaldatavuseeskirjade kontrollimise aruandes.