Euroopa Liidu
Teataja

ET
L-seeria

2026/1735

22.7.2026

KOMISJONI RAKENDUSMÄÄRUS (EL) 2026/1735,

15. juuli 2026,

millega muudetakse rakendusmäärust (EL) 2025/1569 kohaldatavate standardite ja spetsifikatsioonide osas

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 45d lõiget 5, artikli 45e lõiget 2, artikli 45f lõiget 6 ja artikli 45f lõiget 7,

ning arvestades järgmist:

(1) Et tagada Euroopa digiidentiteedikukrute arendamise jaoks kõrgeimal tasemel ühtlustamine liikmesriikide vahel, tuginevad kukrute tehnilised spetsifikatsioonid tööle, mida on tehtud komisjoni soovituse (EL) 2021/946 ([2]) põhjal, ja eeskätt selle osaks olevale arhitektuurile ja võrdlusraamistikule. Kuna arhitektuur ja võrdlusraamistik on pärast komisjoni rakendusmääruse (EL) 2025/1569 ([3]) vastuvõtmist märkimisväärselt muutunud, tuleks rakendusmäärust (EL) 2025/1569 nüüd muuta, et viia see uute standardite ja spetsifikatsioonidega kooskõlla.

(2) Kooskõlas määruse (EL) nr 910/2014 eesmärkidega on elektrooniliste tõendite väljastamisele, haldamisele ja kontrollimisele esitatavate nõuete täitmiseks välja valitud mitu standardit. Standardid peaksid kajastama väljakujunenud tavasid ja olema asjaomastes sektorites laialdaselt tunnustatud. Vajaduse korral tuleks neid standardeid kohandada või täiendada, et tagada elektrooniliste tõendite kõrgetasemeline turvalisus ja terviklus ning soodustada samal ajal piiriülest koostalitlusvõimet ja siseturu tõrgeteta toimimist. Selle eesmärgiga kooskõlas ajakohastatakse käesoleva määrusega nõudeid, mida kohaldatakse kvalifitseeritud elektrooniliste tõendite ja autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite väljastamisel ja kehtetuks tunnistamisel, ning kehtestatakse nõuded autentsete allikate alusel tehtud kontrolli tulemuste allkirjastamiseks ja nende tempiga varustamiseks.

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

([1]) ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Komisjoni 3. juuni 2021. aasta soovitus (EL) 2021/946, mis käsitleb ühiseid liidu tööriistu Euroopa digiidentiteedi raamistiku koordineeritud käsitlusviisi jaoks (ELT L 210, 14.6.2021, lk 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Komisjoni 29. juuli 2025. aasta rakendusmäärus (EL) 2025/1569, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate kvalifitseeritud elektrooniliste tõendite ja elektrooniliste tõenditega (ELT L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([6]) artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 17. aprillil 2026 ([7]).

(5) 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

Rakendusmääruse (EL) 2025/1569 muudatused

Rakendusmäärust (EL) 2025/1569 muudetakse järgmiselt:

1) artikli 3 lõige 2 asendatakse järgmisega:

„2. Kui kvalifitseeritud elektrooniliste tõendite pakkujad ja autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite pakkujad väljastavad elektroonilisi tõendeid, mis kuuluvad atribuutide tõendamise kavade kataloogis registreeritud kavadesse, peavad nad täitma vastava atribuutide tõendamise kava nõudeid. Põhimõtted ja menetlused, mille tõendite väljastajad on kehtestanud, et täita atribuutide tõendamise kavade nõudeid, on osa määrusega (EL) nr 910/2014 kehtestatud vastavushindamisest.“

2) Artiklit 4 muudetakse järgmiselt:

a) lõige 1 jäetakse välja;

b) lõige 3 asendatakse järgmisega:

„3. Kvalifitseeritud elektrooniliste tõendite pakkujad ja autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite pakkujad tunnistavad juhul, kui kõnealused tõendid on väljastatud kehtivusajaga üle 24 tunni, need kehtetuks vähemalt järgmistel asjaoludel:

a) kui seda taotleb isik, kellele elektrooniline tõend väljastati, või kui see on asjakohane, tõendi subjekt;

b) kui pakkuja saab teada, et kvalifitseeritud elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite turvalisust või usaldusväärsust on kahjustatud;

c) muudes olukordades, kui see on nõutav liidu või liikmesriigi õigusega.“

c) lõige 4 asendatakse järgmisega:

„4. Kvalifitseeritud elektrooniliste tõendite pakkujad ja autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite pakkujad peavad kehtestama kehtetuks tunnistamise metoodika ja haldusmeetodid, mis võimaldavad säilitada privaatsust ning takistada seostatavust ja jälgitavust. Kehtetuks tunnistamise metoodikad peavad vastama II lisas esitatud nõuetele.“

([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 Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | European Data Protection Supervisor.

3) Artiklit 9 muudetakse järgmiselt:

a) lõike 2 järele lisatakse lõige 2a:

„2a. Kontrollimehhanism peab vastama IV lisas esitatud spetsifikatsioonidele.“;

b) lõige 4 asendatakse järgmisega:

„4. Kontrolli tulemuses märgitakse, kas atribuuti on kontrollitud või mitte, ning nimetatakse autentse allika eest vastutav avaliku sektori asutus või vajaduse korral avaliku sektori asutus, kes on määratud tegutsema selle autentse allika nimel, mille alusel atribuuti on kontrollitud.

Kontrolli tulemuse allkirjastab või varustab templiga autentse allika eest vastutav avaliku sektori asutus või riiklikul tasandil tunnustatud määratud vahendaja, kasutades vähemalt kas e-allkirja kvalifitseeritud sertifikaadil põhinevat täiustatud e-allkirja või e-templi kvalifitseeritud sertifikaadil põhinevat täiustatud e-templit.“

4) I lisa asendatakse käesoleva määruse I lisas esitatud tekstiga.

5) II lisa asendatakse käesoleva määruse II lisas esitatud tekstiga.

6) Käesoleva määruse III lisas esitatud tekst lisatakse IV lisana.

Artikkel 2

Jõustumine

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

Artikli 1 lõiget 3 kohaldatakse alates 1. jaanuarist 2027.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 15. juuli 2026

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

„*I LISA*

Artiklis 3 osutatud võrdlusstandardite ja spetsifikatsioonide loetelu

Standardit ETSI TS 119 471 V1.1.1 (2025-05) kohaldatakse järgmiste kohandustega:

1) 2.1 Viited normidele

[1] ETSI EN 319 401 V3.2.1 (2026-01): „Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers“;

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

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

[4] 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;

[5] Komisjoni rakendusmäärus (EL) 2024/3144, ([2]) 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“.

2) 3.1 Mõisted

Lisatakse järgmine mõiste:

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

3) 4. Elektrooniliste tõendite usaldusteenused

— Punkt 4.2.2.2 „Verification of attributes against authentic sources“ ei kehti.

— REQ-EAASP-4.2.2.3-02: elektrooniliste tõendite teenuse osutaja rakendab enese autentimisel Euroopa digiidentiteedikukru eksemplari jaoks kehtivat pääsusertifikaati kasutavaid autentimismehhanisme.

— REQ-EAASP-4.2.2.3-03: elektrooniliste tõendite teenuse osutaja valideerib Euroopa digiidentiteedikukru ja kontrollib, *kas Euroopa digiidentiteedikukru eksemplar on kehtetuks tunnistatud*.

— Punkt *4.3.2 „EUDIW Specific“ ei kehti.*

4) 6.1 Atribuutide elektroonilise tõendamise teenuse tavade määrang

— REQ-EAASP-6.1-02: Elektrooniliste tõendite teenuse osutaja dokumenteerib kehtetuks tunnistamise mehhanismi elektrooniliste tõendite teenuse tavade määrangus.

5) 6.3. Infoturvapoliitika

— REQ-EAASP-6.3-02: Elektrooniliste tõendite teenuse osutaja kehtestab menetlused, mille kohaselt teatada järelevalveasutusele kõigist muudatustest elektrooniliste tõendite pakkumise usaldusteenuse osutamises ja kavatsusest see tegevus lõpetada, järgides talitlusnõudeid ning vastavaid õigusakte, sealhulgas määruse (EL) nr 910/2014 artikli 24 lõike 5 kohaselt vastu võetud rakendusaktides esitatud nõudeid. Elektrooniliste tõendite teenuse osutaja esitab järelevalveasutusele teate vähemalt:

— kuu aega enne mis tahes muudatuse tegemist;

— kolm kuud enne usaldusteenuse osutamise kavandatud lõpetamist.

([1]) 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/oj).

([2]) 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).

6) 7.5. Krüptograafiline kontroll

— REQ-EAASP-7.5.2-05: ei kehti.

— REQ-EAASP-7.5.2-06: ei kehti.

— REQ-EAASP-7.5.3-01A: krüptovõtmete, krüptoalgoritmide ja krüptoseadmete haldamiseks kogu nende elutsükli kestel peavad kehtima kohased turvameetmed, lähtudes vajaduse korral krüptograafilise kohandatavuse põhimõttest.

— REQ-EAASP-7.5.3-01B: usaldusteenuse osutamiseks peab elektrooniliste tõendite teenuse osutaja valima Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendile „Agreed Cryptographic Mechanisms“ [2] vastavad sobilikud krüptomeetodid ja neid kasutama.

— REQ-EAASP-7.5.3-02: elektrooniliste tõendite teenuse osutaja peab tagama, et tema poolt elektroonilise tõendi digiallkirjastamiseks või templiga varustamiseks kasutatav turvaline krüptoseade on seade kvalifitseeritud allkirja andmiseks või templi loomiseks ja et kõik muud digiallkirjad või templid, mida kasutades osutatakse vastavat elektroonilise tõendi pakkumise usaldusteenust või selle osa, antakse sellist turvalist krüptoseadet kasutades, mis kujutab enesest usaldusväärset süsteemi ja on sertifitseeritud vastavalt järgmisele:

  a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on esitatud standardi „Common Criteria for Information Technology Security Evaluation“ versioonis 2027 3.1 (CC3.1) (kuni 31. augustini 2027) või versiooni CC:2022 1.–5. osas, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised, või standardis ISO/IEC 15408 [6], saavutades vähemalt EAL 4. tasemel sertifitseerimise, või

  b) Euroopa ühiskriteeriumidel põhinev küberturvalisuse sertifitseerimise kava (EUCC) [4][5], saavutades vähemalt EAL 4. tasemel sertifitseerimise, või

  c) standard FIPS-140-2, 3. tase (kasutatakse olemasolevate sertifitseeritud süsteemide jaoks kuni 31. augustini 2027) või standard FIPS PUB 140-3 [3], 3. tase (kuni 31. detsembrini 2030).

  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.

— REQ-EAASP-7.5.5-01: ei kehti.

— REQ-EAASP-7.5.5-02: ei kehti.

— REQ-EAASP-7.5.5-04: ei kehti.

7) 7.9 Haavatavused ja intsidendihaldus

— REQ-EAASP-7.9-02: seiretegevuse juures arvestatakse kõigi kogutud või analüüsitud andmete tundlikkusega.

8) 7.12 Elektrooniliste tõendite teenuse osutaja tegevuse ja elektrooniliste tõendite teenuse osutamise lõpetamine ja lõpetamiskavad

— REQ-EAASP-7.12-04: elektrooniliste tõendite teenuse osutaja tegevuse lõpetamise kava peab vastama nõuetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.“

II LISA

„*II LISA*

Artiklis 3 ja artiklis 4 osutatud tehnilised spetsifikatsioonid

Kvalifitseeritud elektrooniliste tõendite pakkujad ja autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel väljastatud elektrooniliste tõendite pakkujad peavad neid tõendeid väljastama kooskõlas vähemalt ühega komisjoni rakendusmääruse (EL) 2024/2979 ([1]) II lisas loetletud standarditest ja kohaldama vastavaid kehtetuks tunnistamise metoodikaid, mis on esitatud ka komisjoni rakendusmääruse (EL) 2024/2979 II lisas.“

([1]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2979, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses Euroopa digiidentiteedikukrute tervikluse ja tuumikfunktsioonidega (ELT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

III LISA

„IV LISA

Artiklis 9 osutatud standardite ja tehniliste spetsifikatsioonide loetelu

Artiklis 9 osutatud kontrollimehhanismid peavad vastama kas ühele või mõlemale järgmistest spetsifikatsioonidest järgmiste kohandustega.

a) Standardi ETSI TS 119 478 V1.1.1 (2026-01) „Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources“ punktis 6.1.1 esitatud tehnilised spetsifikatsioonid

— REQ-ASIP-6.1.1.2-04-01 [TINGIMUSLIK]: kui attributeVerificationResult on kas http://uri.etsi.org/19478/VerificationResult/Match või http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, võib attributeVerificationResult sisaldada elementi attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [TINGIMUSLIK]: juhul kui tagastatud attributeVerificationResult on http://uri.etsi.org/19478/VerificationResult/Match ja attributeVerificationResult sisaldab elementi attributeValue, peab element attributeValue sisaldama taotluses esitatud väärtust.

— REQ-ASIP-6.1.1.2-04-03 [TINGIMUSLIK]: juhul kui tagastatud attributeVerificationResult on http://uri.etsi.org/19478/VerificationResult/MatchWithVariation ja attributeVerificationResult sisaldab elementi attributeValue, peab element attributeValue sisaldama atribuudi väärtust, mis on salvestatud autentses allikas.

— REQ-ASIP-6.1.1.2-06-04-01 [TINGIMUSLIK]: kui element fragmentVerificationResult on kas http://uri.etsi.org/19478/VerificationResult/Match või http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, võib attributeVerificationResult sisaldada elementi fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [TINGIMUSLIK]: juhul kui tagastatud fragmentVerificationResult on http://uri.etsi.org/19478/VerificationResult/Match ja attributeVerificationResult sisaldab elementi fragmentValue, peab element fragmentValue sisaldama taotluses esitatud väärtust.

— REQ-ASIP-6.1.1.2-06-04-03 [TINGIMUSLIK]: juhul kui tagastatud fragmentVerificationResult on http://uri.etsi.org/19478/VerificationResult/MatchWithVariation ja attributeVerificationResult sisaldab elementi fragmentValue, peab element fragmentValue sisaldama atribuudi fragmendi väärtust, mis on salvestatud autentses allikas.

b) Standardi ETSI TS 119 478 V1.1.1 (2026-01) „Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources“ punktis 6.2.3 esitatud tehnilised spetsifikatsioonid

— REQ-ASIP-6.2.3.2.1-08-04: Element AttributeVerificationResponse võib sisaldada täpselt üht järgmistest tütarelementidest: TextValue, XMLValue või AttributeProperties.“