2025/1944

30.9.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1944,

29. september 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses kvalifitseeritud registreeritud e-andmevahetusteenustes andmete saatmise ja vastuvõtmise protsesside võrdlusstandarditega ja seoses nende teenuste koostalitlusvõimega

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 44 lõiget 2 ja artikli 44 lõiget 2b,

ning arvestades järgmist:

(1) Kvalifitseeritud registreeritud e-andmevahetusteenused pakuvad turvalist kanalit dokumentide edastamiseks koos andmete saatmise ja kättesaamise tõendamisega. Nende eesmärk on pakkuda kindlust adressaadi identifitseerimisel ja tagada kõrgel tasemel usaldus saatja identifitseerimise suhtes.

(2) Määruse (EL) nr 910/2014 artikli 44 lõikes 1a sätestatud eeldust tingimustele vastamise kohta tuleks kohaldada üksnes siis, kui kvalifitseeritud registreeritud e-andmevahetusteenuste pakkumiseks kvalifitseeritud usaldusteenused 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.

(3) Kui usaldusteenuse osutaja järgib käesoleva määruse I 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) Kui kvalifitseeritud usaldusteenuse osutajad lepivad kokku oma teenuste koostalitlusvõimeliseks muutmises vastavalt määruse (EL) nr 910/2014 artikli 44 lõikele 2a, on oluline, et nad järgivad käesoleva rakendusmääruse II lisas sätestatud asjakohaseid standardeid ja kirjeldusi, et registreeritud e-andmeid saaks kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel lihtsasti edastada ning siseturul õiglasi tavasid edendada.

(5) 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).

(6) Kõigi isikuandmete töötlemise toimingute 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]).

(7) 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.

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

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Kvalifitseeritud registreeritud e-andmevahetusteenuste võrdlusstandardid ja kirjeldused

Määruse (EL) nr 910/2014 artikli 44 lõikes 2 osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse I lisas.

Artikkel 2

Kvalifitseeritud registreeritud e-andmevahetusteenuste koostalitlusvõime võrdlusstandardid ja kirjeldused

Määruse (EL) nr 910/2014 artikli 44 lõikes 2b osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse II lisas.

Artikkel 3

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).

I LISA

Artiklis 1 osutatud võrdlusstandardite ja kirjelduste loetelu

Standardit ETSI EN 319 521 V1.1.1 (2019-02) (ETSI EN 319 521) kohaldatakse järgmiste kohandustega:

1. ETSI EN 319 521

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 EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“.

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture“.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content“.

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

— [6] ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.

— [7] Komisjoni rakendusmäärus (EL) 2024/482, ([2]) millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega.

— [8] Komisjoni rakendusmäärus (EL) 2024/3144, ([3]) millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

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

2) 3.1 Mõisted

— täiustatud e-tempel: vastavalt määrusele (EL) nr 910/2014 [i.1]

— täiustatud e-allkiri: vastavalt määrusele (EL) nr 910/2014 [i.1]

— kvalifitseeritud e-tempel: vastavalt määrusele (EL) nr 910/2014 [i.1]

— kvalifitseeritud e-allkiri: vastavalt määrusele (EL) nr 910/2014 [i.1]

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

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

3) 5.1.1 Ühissätted

— REQ-ERDS-5.1.1-01 Registreeritud e-andmevahetusteenus kindlustab, et sel ajal, kui registreeritud e-andmevahetusteenus käitleb kasutaja sisu, on selle käideldavus, terviklus ja konfidentsiaalsus piisavalt tagatud, ning valib sobivad tervikluse ja konfidentsiaalsuse krüptograafilised lahendused, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms"[5].

4) 5.2.1.1 Üldist

— REQ-QERDS-5.2.1.1-01 Kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja peab kontrollima vastuvõtja identiteeti väga kõrgel usaldusväärsuse tasemel kas otse või kolmandale isikule tuginedes ning kasutades üht järgmistest võimalustest või nende kombinatsiooni vastavalt vajadusele:

(a) füüsilise isiku või juriidilise isiku volitatud esindaja füüsiliselt kohal viibides ning vastavalt asjakohastele tõenditele ja menetlustele kooskõlas riigisisese õigusega;

(b) kaughindamise teel, kasutades e-identimise vahendeid, mis vastavad määruse (EL) nr 910/2014 [i.1] artiklis 8 sätestatud nõuetele seoses kõrge usaldusväärsuse tasemega, või kasutades Euroopa digiidentiteedikukrut;

(c) kvalifitseeritud e-allkirja või kvalifitseeritud e-templi sertifikaadi abil;

(d) kasutades muid identifitseerimismeetodeid, mis tagavad, et füüsiline isik või juriidilise isiku volitatud esindaja on võimalik identifitseerida väga kõrgel usaldusväärsuse tasemel. Tagatise, et selline identifitseerimine toimub väga kõrgel usaldusväärsuse tasemel, peab kinnitama vastavushindamisasutus.

— REQ-QERDS-5.2.1.1-01A Kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja peab kontrollima saatja identiteeti asjakohaste vahenditega kas otse või tuginedes kolmandale isikule, ühe järgmise meetodi või nende kombinatsiooni põhjal:

(a) füüsilise isiku või juriidilise isiku volitatud esindaja füüsiliselt kohal viibides ning vastavalt asjakohastele tõenditele ja menetlustele kooskõlas riigisisese õigusega;

(b) kaughindamise teel, kasutades Euroopa digiidentiteedikukrut või teavitatud e-identimise vahendit, mis vastab määruse (EL) nr 910/2014 [i.1] artiklis 8 sätestatud nõuetele seoses kõrge märkimisväärse usaldusväärsuse tasemega, eeldusel et see on välja antud füüsilise isiku või juriidilise isiku volitatud esindaja varasema füüsilise kohalviibimise põhjal;

(c) täiustatud e-allkirja või täiustatud e-templi sertifikaadi abil, eeldusel et sertifikaat on füüsilisele isikule või juriidilise isiku volitatud esindajale välja antud standardis ETSI EN 319 411-1 [2] määratletud normaliseeritud sertifitseerimispoliitika (NCP) alusel, või

(d) kasutades muid identifitseerimismeetodeid, mis tagavad, et füüsiline isik või juriidilise isiku volitatud esindaja on võimalik identifitseerida väga kõrgel usaldusväärsuse tasemel. Tagatise, et selline identifitseerimine toimub kõrgel usaldusväärsuse tasemel, peab kinnitama vastavushindamisasutus.

— MÄRKUS Saatja ja vastuvõtja identiteeti kontrollivaks kolmandaks isikuks võib olla mõni teine kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja, kui saatja ja vastuvõtja on erinevate kvalifitseeritud registreeritud e-andmevahetusteenuse osutajate abonendid.

5) 5.2.1.2 Vastuvõtja identifitseerimine ja kasutaja sisu üleandmine

— REQ-QERDS-5.2.1.2-03 Kui vastuvõtja identifitseerimine toimub kvalifitseeritud registreeritud e-andmevahetusteenus sisemise protsessi põhjal, sooritab kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja kogu protsessi turvalises ja kontrollitud keskkonnas.

6) 5.2.2 ELi kvalifitseeritud registreeritud e-andmevahetusteenuse autentimist käsitlevad sätted

— REQ-QERDS-5.2.2-03 [TINGIMUSLIK] Kui kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja seob autentimisvahendi saatja identiteediga, mida on kontrollitud vastavalt punktile 5.2.1, peab tegemist olema ühega järgmistest:

(a) kaksikautentimise mehhanismid;

(b) Euroopa digiidentiteedikukkur või teavitatud e-identimise vahend, mis vastab määruse (EL) nr 910/2014 [i.1] artiklis 8 sätestatud nõuetele seoses kõrge või märkimisväärse usaldusväärsuse tasemega;

(c) vastastikune TLS-autentimine, mis hõlmab standardis ETSI EN 319 411-1 [2] määratletud normaliseeritud sertifitseerimispoliitika alusel saatjale välja antud sertifikaati;

(d) digiallkiri, mida toetab standardis ETSI EN 319 411-1 [2] määratletud normaliseeritud sertifitseerimispoliitika alusel välja antud sertifikaat;

(e) muu vahend, mis tagab identifitseeritud saatja autentimise. Sidumise nõuetekohasust peab kinnitama vastavushindamisasutus. Näiteks võib see tähendada, et üht eespool punktis a, b või d nimetatud vahendit kasutatakse selleks, et registreerida transpordikihi turbe (TLS) kliendi sertifikaat automaatseks saatmiseks vastastikuse TLSi kaudu või registreerida digitempli sertifikaat, mida kasutatakse registreeritud e-andmevahetusteenusega autentimise avalduste templiga kinnitamiseks. Kohaldada võib ka muid mehhanisme, mille puhul identifitseeritud saatjad kasutavad delegeeritud kolmanda isiku teenuseid.

— REQ-QERDS-5.2.2-03A [TINGIMUSLIK] Kui kvalifitseeritud registreeritud e-andmevahetusteenuse osutaja seob autentimisvahendi vastuvõtja identiteediga, mida on kontrollitud vastavalt punktile 5.2.1, peab tegemist olema ühega järgmistest, eeldusel et vahend või vahendite kombinatsioon tagab seoses autenditud vastuvõtja identiteediga väga kõrge usaldusväärsuse taseme:

(a) mitmikautentimise mehhanism;

(b) Euroopa digiidentiteedikukkur või teavitatud e-identimise vahend, mis vastab määruse (EL) nr 910/2014 [i.1] artiklis 8 sätestatud nõuetele seoses kõrge või märkimisväärse usaldusväärsuse tasemega;

(c) kvalifitseeritud e-allkirja või kvalifitseeritud e-templi sertifikaat;

(d) muu vahend, mis tagab identifitseeritud vastuvõtja autentimise. Sidumise nõuetekohasust peab kinnitama vastavushindamisasutus. Näiteks võib see tähendada, et üht eespool punktides a–c nimetatud vahendit kasutatakse selleks, et registreerida transpordikihi turbe (TLS) kliendi sertifikaat automaatseks saatmiseks vastastikuse TLSi kaudu või registreerida digitempli sertifikaat, mida kasutatakse registreeritud e-andmevahetusteenusega autentimise avalduste templiga kinnitamiseks. Kohaldada võib ka muid mehhanisme, mille puhul identifitseeritud saatjad kasutavad delegeeritud kolmanda isiku teenuseid.

— REQ-QERDS-5.2.2-04 [TINGIMUSLIK] Kui saatja loob ühenduse kvalifitseeritud registreeritud e-andmevahetusteenusega turvalise ühenduse kaudu, mis eeldab masinatevahelist vastastikku autentimist saatja masina ja kvalifitseeritud registreeritud e-andmevahetusteenuse serveri vahel, tuginedes standardis ETSI EN 319 411-1 [2] määratletud normaliseeritud sertifitseerimispoliitika alusel välja antud sertifikaatidele, võib pärast kõnealuse turvalise ühenduse loomist võtta saatja autentimise teiseks etapiks kasutusele lihtautentimismehhanismid, kui organisatsioonis kehtestatud menetluste ja turbemeetmetega tagatakse saatja autentimise usaldusväärsus.

7) 5.4.1 Ühissätted

— REQ-ERDS-5.4.1-06 Registreeritud e-andmevahetusteenus genereerib ja teeb õigustatud huviga isikutele käideldavaks registreeritud e-andmevahetusteenuse tõendid registreeritud e-andmevahetuse sündmuste kohta, nagu on määratletud standardi ETSI EN 319 522-1 [3] punktis 6.

— REQ-ERDS-5.4.1-07 Registreeritud e-andmevahetusteenuse osutaja arhiveerib iga enda väljaantud tõendi kohta tõendi ja/või koondtõendid.

— REQ-ERDS-5.4.1-08 Registreeritud e-andmevahetusteenuse genereeritud tõendid registreeritud e-andmevahetusteenuse kohta peavad olema kooskõlas standardi ETSI EN 319 522-2 [4] punktis 8 määratletud tõendisemantikaga.

8) 7.2.1 Ühissätted

— REQ-ERDS-7.2.1-02 Registreeritud e-andmevahetusteenuse 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-ERDS-7.2,1-03 Nõude REQ-ERDS-7.2,1-02 täitmine hõlmab korrapärast ajakohastamist (vähemalt iga 12 kuu järel) uute ohtude ja praeguste turvatavade kohta.

9) 7.3.2 Kandjate käitlemine

— REQ-ERDS-7.3.1-02 Kohaldatakse kõiki standardi ETSI EN 319 401 [1] punkti 7.3.3 nõudeid.

10) 7.5 Krüptograafilised turvameetmed

— REQ-ERDS-7.5-01A Registreeritud e-andmevahetusteenus valib sobivad krüptomeetodid ja kasutab neid kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[5].

— REQ-ERDSP-7.5-03 Registreeritud e-andmevahetusteenuse privaatset signeerimisvõtit 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 [6] 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) [7][8] vähemalt EAL 4. tasemel või

(c) kuni 31.12.2030, FIPS PUB 140-3 [9] 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 [7][8] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt sellele sertifikaadile.

11) 7.8 Võrgu turvalisus

— REQ-ERDSP-7.8-04 Registreeritud e-andmevahetusteenuse osutaja kasutab transpordikihi tasandil krüpteerimiseks tehnika tipptasemel protokolle ja algoritme kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [5].

— REQ-ERDSP-7.8-06 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— REQ-ERDSP-7.8-07 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— REQ-ERDSP-7.8-08 Tulemüürid tuleb konfigureerida tõrjuma kõiki usaldusteenuse osutaja tegevuseks mittevajalikke protokolle ja juurdepääse.

12) 7.12 Registreeritud e-andmevahetusteenuse osutaja tegevuse lõpetamine ja registreeritud e-andmevahetusteenuse lõpetamise kavad

— REQ-ERDS-7.12-03 Registreeritud e-andmevahetusteenuse osutaja tegevuse lõpetamise kava peab vastama nõetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

13) 7.14 Tarneahel

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

II LISA

Artiklis 2 osutatud võrdlusstandardite ja kirjelduste loetelu

Kohaldatakse standardeid ETSI EN 319 522-1 V1.2.1 (2024-01) (ETSI EN 319 522-1), ETSI EN 319 522-2 V1.2.1 (2024-01) (ETSI EN 319 522-2), ETSI EN 319 522-3 V1.2.1 (2024-01) (ETSI EN 319 522-3), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (ETSI EN 319 522-4-1), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (ETSI EN 319 522-4-2) ja ETSI EN 319 522-4-3 V1.1.1 (2018-09) (ETSI EN 319 522-4-3).