Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/2531

2025 12 17

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/2531

2025 m. gruodžio 16 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų, susijusių su kvalifikuotų elektroninių registrų referenciniais standartais ir specifikacijomis, taikymo taisyklės

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 45l straipsnio 3 dalį,

kadangi:

(1) naujų patikimumo užtikrinimo paslaugų ir kvalifikuotų patikimumo užtikrinimo paslaugų, įskaitant elektroninių duomenų įrašymą į kvalifikuotą elektroninį registrą, sąrašas į Reglamentą (ES) Nr. 910/2014 įtrauktas Europos Parlamento ir Tarybos reglamentu (ES) 2024/1183 ([2]); Komisija turi parengti tokioms paslaugoms taikomų referencinių standartų sąrašą ir, jei būtina, nustatyti tokių paslaugų specifikacijas;

(2) elektroninis registras – elektroninių duomenų įrašų seka, kuria turi būti užtikrinamas tų duomenų įrašų vientisumas ir chronologinės tų įrašų tvarkos tikslumas. Siekiant užtikrinti, kad duomenų įrašymas į kvalifikuotą elektroninį registrą vyktų chronologine tvarka, būtų nuoseklus ir patikimas, būtina sudaryti bendrą specifikacijų, taikomų elektroninių duomenų įrašymui į kvalifikuotą elektroninį registrą, rinkinį;

(3) Reglamento (ES) Nr. 910/2014 45l straipsnio 2 dalyje numatyta atitikties užtikrinimo prielaida turėtų būti daroma tik jei kvalifikuotos patikimumo užtikrinimo paslaugos, kurias teikiant vyksta elektroninių duomenų įrašymas į kvalifikuotą elektroninį registrą, atitinka šiame reglamente nustatytus standartus. Šie standartai turėtų atitikti nusistovėjusią praktiką ir būti plačiai pripažįstami atitinkamuose sektoriuose. Jie turėtų būti pritaikyti taip, kad apimtų papildomas kontrolės priemones, kuriomis garantuojamas kvalifikuotos patikimumo užtikrinimo paslaugos saugumas ir patikimumas;

(4) jei patikimumo užtikrinimo paslaugų teikėjas laikosi šio reglamento priede nustatytų reikalavimų, priežiūros įstaigos turėtų daryti prielaidą, kad jis laikosi ir aktualių Reglamento (ES) Nr. 910/2014 reikalavimų, ir tinkamai į tokią prielaidą atsižvelgti, kad suteiktų arba patvirtintų patikimumo užtikrinimo paslaugos kvalifikacijos statusą. Tačiau įrodyti, kad laikosi Reglamento (ES) Nr. 910/2014 reikalavimų, kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas gali ir kitais būdais;

(5) Komisija reguliariai vertina naujas technologijas, praktiką, standartus ar technines specifikacijas. Pagal Reglamento (ES) 2024/1183 75 konstatuojamąją dalį, Komisija šį reglamentą turėtų peržiūrėti ir prireikus atnaujinti, kad jis atitiktų pasaulinius pokyčius, naujas technologijas, praktiką, standartus arba technines specifikacijas ir atitiktų geriausius vidaus rinkos darbo metodus;

([1]) OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, (OL L, 2024/1183, 2024 4 30, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) asmens duomenų tvarkymo veikla pagal šį reglamentą vykdoma laikantis Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([3]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyvos 2002/58/EB ([4]), taip pat atsižvelgiant į Europos duomenų apsaugos valdybos gaires Nr. 02/2025 dėl asmens duomenų tvarkymo taikant blokų grandinės technologijas ([5]);

(7) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([6]) 42 straipsnio 1 dalimi, konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę ([7]) 2025 m. spalio 21 d.;

(8) šiame reglamente numatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Referenciniai standartai ir specifikacijos

Reglamento (ES) Nr. 910/2014 45l straipsnio 3 dalyje nurodyti kvalifikuotų elektroninių registrų referenciniai standartai ir specifikacijos nustatomi šio reglamento priede.

2 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2025 m. gruodžio 16 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

([3]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Europos duomenų apsaugos priežiūros pareigūno oficialios pastabos dėl įgyvendinimo reglamento, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų, susijusių su kvalifikuotų elektroninių registrų referenciniais standartais ir specifikacijomis, taikymo taisyklės, projekto.

PRIEDAS

Kvalifikuotų paskirstytųjų elektroninių registrų techninių specifikacijų ir referencinių standartų sąrašas

1. Šiame reglamente vartojamų terminų apibrėžtys:

   a) baigtumas – elektroninio registro duomenų įrašo būklė, kai tas įrašas yra galutinis ir jo neįmanoma pakeisti arba pašalinti;

   b) paskirstytasis elektroninis registras – paskirstytojo elektroninio registro mazgų grupei išdalytas elektroninis registras, kuris paskirstytojo elektroninio registro mazguose sinchronizuojamas sutarimo mechanizmu;

   c) paskirstytojo elektroninio registro mazgas – įrenginys arba procesas, kuris yra paskirstytojo elektroninio registro tinklo dalis ir kuriame saugoma visa elektroninio registro duomenų įrašų kopija arba jos dalis;

   d) paskirstytojo elektroninio registro tinklas – paskirstytojo elektroninio registro mazgų, iš kurių sudarytas paskirstytasis elektroninis registras, tinklas;

   e) paskirstytojo elektroninio registro sistema – sistema, kuria įgyvendinamas paskirstytasis elektroninis registras;

   f) sutarimas – paskirstytojo elektroninio registro mazgais užtikrinamas operacijų teisingumo pripažinimas ir teisingomis pripažintų operacijų nuoseklus ir tvarkingas išlaikymas visoje paskirstytojo elektroninio registro sistemoje;

   g) sutarimo mechanizmas – taisyklių ir procedūrų, kuriomis pasiekiamas sutarimas, rinkinys;

   h) galiojančios taisyklės – protokolų, politikos ir mechanizmų, nuo kurių priklauso elektroninio registro sistemos veikimas, duomenų teisingumo pripažinimas ir jų įrašymas į elektroninį registrą bei dalyvių sąveika, rinkinys;

   i) operacija – mažiausias darbo proceso elektroniniame registre vienetas;

   j) darbo procesas – viena arba kelios veiksmų sekos, būtinos tam, kad būtų gautas elektroninio registro galiojančias taisykles atitinkantis rezultatas;

   k) patvirtinta operacija – operacija, kurios būtinos vientisumo, autentiškumo ir specifinės protokolo sąlygos patikrintos pagal galiojančias paskirstytojo elektroninio registro sistemos taisykles;

   l) šifruotų duomenų saitas – nuoroda į duomenis, tinkamais šifravimo metodais sukurta sukurta tam, kad būtų užtikrintas nurodytųjų duomenų vientisumas, autentiškumas arba atsekamumas ir teisinga duomenų įrašų seka;

   m) registro ataskaita – iš elektroninio registro duomenų įrašų gauta struktūriškai pateikta patikrinama informacija, iš kurios galima suprasti konkrečią veiklą, būklę arba tai, kaip laikomasi iš anksto nustatytų taisyklių;

   n) kvalifikuoto elektroninio registro teikėjas – kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis kvalifikuotą patikimumo užtikrinimo paslaugą, kurios esmė – duomenų įrašymas į kvalifikuotą elektroninį registrą;

   o) kvalifikuotas paskirstytasis elektroninis registras – kvalifikuoto elektroninio registro reikalavimus atitinkantis paskirstytasis elektroninis registras.

2. Jei kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas turi parengti registro ataskaitą, tokia ataskaita parengiama automatizuotai.

3. Kvalifikuotų elektroninių registrų teikėjai sukuria kvalifikuotą elektroninį registrą, įrašo į jį elektroninius duomenis, jį atnaujina ir prižiūri pagal specifikacijas, nustatytas:

   a) visiems kvalifikuotų elektroninių registrų teikėjams – standarte ETSI EN 319 401 v3.1.1 (2024-06) su šiais pakeitimais:

      — 2.1. Norminės nuorodos:

      [1] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (*Agreed Cryptographic Mechanisms*), paskelbė Europos tinklų ir informacijos agentūra (ENISA),

[2] IETF RFC 7515 (2015 m. gegužės mėn.). „JSON internetinis parašas“ (*JSON Web Signature, JWS*),

[3] FIPS PUB 140-3 (2019) „Šifravimo modulių saugumo reikalavimai“ (*Security Requirements for Cryptographic Modules*),

[4] 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo,

[5] 2024 m. gruodžio 18 d. Komisijos įgyvendinimo reglamentas (ES) 2024/3144, kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/482 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas,

[6] ISO/IEC 15408:2022 (1–5 dalys). „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. IT saugumo įvertinimo kriterijai“;

— 6.1. Patikimumo užtikrinimo paslaugų praktikos pareiškimas:

  — REQ-6.1-12. Elektroninio registro praktikos pareiškime turi būti bent ši informacija:

    — elektroninio registro platformos funkcinės ir techninės galimybės ir jos naudojimas, kai duomenų įrašymas į kvalifikuotą elektroninį registrą teikiamas kaip kvalifikuota patikimumo užtikrinimo paslauga,

    — teikiant paslaugą naudojami konkretūs duomenų kilmės tikrumo patvirtinimo mechanizmai,

    — teikiant paslaugą naudojami konkretūs nuoseklios chronologinės eilės sudarymo mechanizmai,

    — kai taikytina, šifruotų duomenų saitas, naudojamas duomenų įrašų sekai užtikrinti,

    — kai taikytina, sutarimo mechanizmas, kuriuo užtikrinamas registre laikomų duomenų įrašų ir operacijų baigtumas ir vientisumas, įskaitant atsargumo laiką, kol pasiekiamas baigtumas ir vientisumas,

    — teikiant paslaugą naudojami konkretūs duomenų vientisumo mechanizmai;

  — 6.2. Sąlygos:

    — REQ-6.2-03. Abonentai ir šalys, pasikliaunantys patikimumo užtikrinimo paslauga, apie konkrečias sąlygas, įskaitant pirmiau išvardytus punktus, aiškiai, suprantamai ir lengvai prieinamu būdu viešoje erdvėje ir individualiai informuojami iki sutartinių santykių užmezgimo;

  — 6.3. Informacijos saugumo politika:

    — REQ-6.3-04X. Patikimumo užtikrinimo paslaugų teikėjas, laikydamasis verslo reikalavimų ir aktualių įstatymų ir kitų teisės aktų, nustato procedūras, pagal kurias apie visus patikimumo užtikrinimo paslaugos pakeitimus informuoja priežiūros įstaigą. Patikimumo užtikrinimo paslaugų teikėjas pranešimus priežiūros įstaigai pateikia bent prieš:

      — mėnesį iki pakeitimo įgyvendinimo,

      — tris mėnesius iki patikimumo užtikrinimo paslaugos teikimo planuoto nutraukimo;

  — 7.2. Žmogiškieji ištekliai:

    — REQ-7.2-04X. Pasitikėjimo funkciją vykdantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai turi būti pajėgūs įvykdyti reikalavimą turėti būtinų ekspertinių žinių, patirties ir kvalifikaciją, įgytą baigus oficialų mokymą ir patvirtintą pažymėjimais, ir (arba) praktinės patirties,

— REQ-7.2-05X. Tam reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinę saugumo užtikrinimo praktiką;

— 7.5. Šifravimo kontrolės priemonės:

— REQ-7.5-01X. Turi būti nustatytos reikiamos saugumo kontrolės priemonės, būtinos šifravimo raktams, šifravimo algoritmams ir šifravimo įrenginiams valdyti visą jų gyvavimo ciklą laikantis, kai tinkama, šifravimo lankstumo principo,

— REQ-7.5-02. Patikimumo užtikrinimo paslaugos teikimo tikslais patikimumo užtikrinimo paslaugų teikėjas pasirenka ir taiko tinkamus šifravimo metodus, atitinkančius Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA paskelbtus suderintuosius šifravimo mechanizmus [1],

Pirmiausia –

— REQ-7.5-03. Kvalifikuotų elektroninių registrų teikėjai nustato elektroniniame registre laikomų duomenų įrašų kilmę. Tam jie naudoja pažangiuosius elektroninius parašus, grindžiamus kvalifikuotais sertifikatais, arba pažangiuosius elektroninius parašus, grindžiamus kvalifikuotais sertifikatais, kuriuos paslaugos naudotojai sukūrė pagal šiuos standartus ir specifikacijas:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). Elektroniniai parašai ir infrastruktūros (ESI). CAdES skaitmeniniai parašai. 1 dalis. Komponentai ir CAdES baziniai parašai;

b) ETSI EN 319 132-1 V1.3.1 (2024-07). Elektroniniai parašai ir patikimumo infrastruktūros (ESI). XAdES skaitmeniniai parašai. 1 dalis. Komponentai ir XAdES baziniai parašai;

c) ETSI TS 119 182-1 V1.2.1 (2024-07). Elektroniniai parašai ir patikimumo infrastruktūros (ESI). JAdES skaitmeniniai parašai; 1 dalis. Komponentai ir JAdES baziniai parašai, su šiais pakeitimais:

— 5.1.8. x5c (X.509 sertifikatų seka) antraštės parametras:

— standarto IETF RFC 7515 [2] 4.1.6 punkte apibrėžtas x5c antraštės parametras turi būti JAdES paraše kaip pasirašytasis arba kaip nepasirašytasis antraštės parametras,

— x5c antraštės parametro semantika tokia, kokia nustatyta standarto IETF RFC 7515 [2] 4.1.6 punkte,

— x5c antraštės parametro sintaksė tokia, kokia nustatyta standarto IETF RFC 7515 [2] 4.1.6 punkte,

— REQ-7.5-04. Kvalifikuotų elektroninių registrų teikėjai užtikrina unikalią chronologinę duomenų įrašų tvarką elektroniniame registre. Tam jie naudoja maišos sąrašais arba maišos medžiais grindžiamus šifravimo maišos funkcijomis sukurtus šifruotų duomenų saitus, atitinkančius šias specifikacijas ir standartus:

a) SHA-256 arba didesnės išvesties maišos algoritmą, kaip nustatyta „Suderintuosiuose šifravimo mechanizmuose“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [1],

b) SHA3-256 arba didesnės išvesties maišos algoritmą, kaip nustatyta „Suderintuosiuose šifravimo mechanizmuose“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [1].

Kvalifikuotų elektroninių registrų teikėjai pasirinktinai naudoja kvalifikuotas laiko žymas, jeigu jie chronologinei unikaliai duomenų įrašų tvarkai elektroniniame registre užtikrinti naudoja laiko įrašus;

— REQ-7.5-05. Kvalifikuotų elektroninių registrų teikėjai užtikrina kvalifikuotame elektroniniame registre laikomų duomenų įrašų vientisumą. Tam jie naudoja pažangiuosius elektroninius parašus, grindžiamus kvalifikuotais sertifikatais, arba pažangiuosius elektroninius spaudus, grindžiamus kvalifikuotais sertifikatais, kaip nustatyta šiuose standartuose ir specifikacijose:

  a) bet kuris parašo arba spaudo formatas, atitinkantis „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [1];

  b) SHA-256 arba didesnės išvesties maišos algoritmą, kaip nustatyta „Suderintuosiuose šifravimo mechanizmuose“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [1],

  c) SHA3-256 arba didesnės išvesties maišos algoritmą, kaip nustatyta „Suderintuosiuose šifravimo mechanizmuose“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [1],

  d) kvalifikuotų elektroninių registrų teikėjai užtikrina, kad būtų galima iš karto pastebėti visus paskesnius į kvalifikuotą elektroninį registrą įrašytų duomenų pakeitimus,

— REQ-7.5-06. Kai naudojami skaitmeninio parašo mechanizmai, kvalifikuoto elektroninio registro teikėjo privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

  a) standarte ISO/IEC 15408 ([1]) [6] arba Bendrųjų IT saugumo srities kriterijų sertifikatų pripažinimo susitarimo dalyvių paskelbtuose Bendruosiuose informacinių technologijų saugumo vertinimo kriterijuose (redakcija CC:2022, 1–5 dalys) nustatytus bendruosius informacinių technologijų saugumo vertinimo kriterijus ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL) arba

  b) bendraisiais kriterijais grindžiamą Europos kibernetinio saugumo sertifikavimo schemą ([2]) ([3])[4][5] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

  c) 3-čiojo lygio FIPS PUB 140-3 ([4]) [3], iki 2030 m. gruodžio 31 d.

Remiantis rizikos analize ir atsižvelgiant į fizines ir kitas netechnines saugumo priemones, toks sertifikavimas turi atitikti saugumo tikslą arba apsaugos profilį, arba modulio sandarą ir saugumo dokumentus, kad atitiktų šio dokumento reikalavimus.

Jei saugiam šifravimo įrenginiui taikomas bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EUCC) sertifikatas [4][5], toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą;

([1]) ISO/IEC 15408:2022 (1–5 dalys). „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. IT saugumo įvertinimo kriterijai“.

([2]) 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo, (OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) 2024 m. gruodžio 18 d. Komisijos įgyvendinimo reglamentas (ES) 2024/3144, kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/482 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas, (OL L, 2024/3144, 2024 12 19, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019) „Šifravimo modulių saugumo reikalavimai“.

— 7.8. Tinklo saugumas:

— REQ-7.8-14X. Silpnųjų vietų paieška, kurios reikalaujama pagal REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— REQ-7.8-18X. Skverbimosi testas, kurio reikalaujama pagal REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— REQ-7.8-21X. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia patikimumo užtikrinimo paslaugų teikėjo veiklai,

— 7.9.1. Stebėjimas ir registravimas:

— REQ-7.9.1-02X. Vykdant stebėjimą atsižvelgiama į surinktos arba analizuojamos informacijos neskelbtinumą,

— 7.12. Patikimumo užtikrinimo paslaugų teikėjo veiklos nutraukimas ir veiklos nutraukimo planai:

— REQ-7.12-02A. Patikimumo užtikrinimo paslaugų teikėjo veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 5 dalį, reikalavimus;

b) be to, visiems kvalifikuotų elektroninių registrų teikėjams, besinaudojantiems paskirstytojo elektroninio registro technologijomis, taikomas:

1) standarto ISO 23257:2022 „Blokų grandinės ir paskirstytojo registro technologijos. Bazinė architektūra“ 9 punktas, kuriame išsamiai aprašyta paskirstytojo elektroninio registro technologijos sistema, atitinkamas paskirstytojo registro technologijos tinklas ir paskirstytojo registro technologijos mazgai;

2) standartas ISO/TS 23635:2022. „Blokų grandinės ir paskirstytojo registro technologijos. Valdymo gairės, taikomos rašytinei ir viešai prieinamai politikai ir praktikai, susijusioms su teikiamos elektroninio registro paslaugos valdymo struktūra“.