Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2531

17.12.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2531

(2025. gada 16. decembris),

ar ko nosaka noteikumus Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz kvalificētu elektronisko virsgrāmatu atsauces standartiem un specifikācijām

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 45.l panta 3. punktu,

tā kā:

(1) Ar Eiropas Parlamenta un Padomes Regulu (ES) 2024/1183 ([2]) Regulā (ES) Nr. 910/2014 tika ieviests saraksts ar jauniem uzticamības pakalpojumiem un kvalificētiem uzticamības pakalpojumiem, citastarp elektronisku datu reģistrēšana kvalificētā elektroniskā virsgrāmatā. Komisijai ir jāizveido šādu pakalpojumu atsauces standartu saraksts un vajadzības gadījumā jānosaka šādu pakalpojumu specifikācijas.

(2) Elektroniska virsgrāmata ir elektronisko datu ierakstu sekvence, kuras uzdevums ir nodrošināt minēto datu ierakstu integritāti un minēto ierakstu hronoloģiskās secības precizitāti. Lai nodrošinātu, ka datu reģistrēšana kvalificētā elektroniskā virsgrāmatā notiek hronoloģiskā secībā, ir konsekventa un uzticama, ir nepieciešams noteikt vienotu specifikāciju kopumu elektronisko datu reģistrēšanai kvalificētā elektroniskā virsgrāmatā.

(3) Regulas (ES) Nr. 910/2014 45.l panta 2. punktā izklāstītais pieņēmums par atbilstību būtu piemērojams tikai tad, ja kvalificēti uzticamības pakalpojumi elektronisko datu reģistrēšanai kvalificētā elektroniskā virsgrāmatā atbilst šajā regulā noteiktajiem standartiem. Šādiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Tie būtu jāpielāgo, lai iekļautu papildu kontroles, kas nodrošina kvalificētā uzticamības pakalpojuma drošību un uzticamību.

(4) Ja uzticamības pakalpojumu sniedzējs ievēro šīs regulas pielikumā noteiktās prasības, uzraudzības iestādēm būtu jāpieņem, ka Regulas (ES) Nr. 910/2014 attiecīgās prasības ir ievērotas, un šāds pieņēmums pienācīgi jāņem vērā, piešķirot vai apstiprinot uzticamības pakalpojuma kvalifikācijas statusu. Tomēr, lai pierādītu atbilstību Regulas (ES) Nr. 910/2014 prasībām, kvalificēts uzticamības pakalpojumu sniedzējs joprojām drīkst izmantot citu praksi.

(5) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Saskaņā ar Regulas (ES) 2024/1183 75. apsvērumu Komisijai šī regula būtu jāpārskata un vajadzības gadījumā jāatjaunina nolūkā nodrošināt tās atbilstību globālajām norisēm, jaunām tehnoloģijām, praksei, standartiem un tehniskajām specifikācijām un nolūkā ievērot paraugpraksi iekšējā tirgū.

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([3]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([4]), ņemot vērā arī Eiropas Datu aizsardzības kolēģijas "Vadlīnijas par personas datu apstrādi, izmantojot blokķēdes tehnoloģijas, 2025. gada februāris" ([5]).

(7) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([6]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 21. oktobrī sniedza savu atzinumu ([7]).

(8) Šajā regulā noteiktie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Atsauces standarti un specifikācijas

Regulas (ES) Nr. 910/2014 45.l panta 3. punktā minētie kvalificētu elektronisko virsgrāmatu atsauces standarti un specifikācijas ir noteiktas šīs regulas pielikumā.

2. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2025. gada 16. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) EDAU oficiālās piezīmes par projektu īstenošanas regulai, ar ko nosaka noteikumus Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz kvalificētu elektronisko virsgrāmatu atsauces standartiem un specifikācijām.

PIELIKUMS

Kvalificētu sadalīto elektronisko virsgrāmatu tehnisko specifikāciju un atsauces standartu saraksts

1. Šajā regulā piemēro šādas definīcijas:

   a) "galīgums" ir elektroniskas virsgrāmatas datu ieraksta stāvoklis, kurā tas ir kļuvis neatgriezenisks un to nevar grozīt vai noņemt;

   b) "sadalīta elektroniska virsgrāmata" ir elektroniska virsgrāmata, ko kopīgo sadalītas elektroniskās virsgrāmatas mezglu kopumā un ko starp sadalītas elektroniskās virsgrāmatas mezgliem sinhronizē, izmantojot konsensa mehānismu;

   c) "sadalītas elektroniskas virsgrāmatas mezgls" ir ierīce vai process, kas ir daļa no sadalītas elektroniskas virsgrāmatas tīkla un kurā glabājas pilnīga vai daļēja elektroniskas virsgrāmatas datu ierakstu kopija;

   d) "sadalītas elektroniskas virsgrāmatas tīkls" ir sadalītas elektroniskas virsgrāmatas mezglu tīkls, kas veido sadalītas elektroniskas virsgrāmatas sistēmu;

   e) "sadalītas elektroniskas virsgrāmatas sistēma" ir sistēma, kas īsteno sadalītu elektronisko virsgrāmatu;

   f) "konsenss" ir vienošanās starp sadalītas elektroniskas virsgrāmatas mezgliem par darījumu derīgumu un konsekventa un sakārtota validētu darījumu kopuma uzturēšana sadalītas elektroniskās virsgrāmatas sistēmā;

   g) "konsensa mehānisms" ir noteikumu un procedūru kopums, ar kuru tiek panākts konsenss;

   h) "pārvaldības noteikumi" ir protokolu, politikas un mehānismu kopums, kas nosaka, kā darbojas sadalītās elektroniskās virsgrāmatas sistēma, kā dati tiek validēti un pievienoti elektroniskai virsgrāmatai un kā dalībnieki mijiedarbojas;

   i) "darījums" ir elektroniskas virsgrāmatas darba procesa mazākā vienība;

   j) "darba process" ir viena vai vairākas darbību secības, kas vajadzīgas, lai iegūtu iznākumu, kurš atbilst elektroniskas virsgrāmatas pārvaldības noteikumiem;

   k) "validēts darījums" ir darījums, kura integritāte, autentiskums un protokola īpašie nosacījumi ir pārbaudīti saskaņā ar sadalītās elektroniskās virsgrāmatas sistēmas pārvaldības noteikumiem;

   l) "kriptogrāfijas saite" ir atsauce uz datiem, kas radīti, izmantojot piemērotus kriptogrāfiskus paņēmienus, lai nodrošinātu atsauces datu integritāti, autentiskumu vai izsekojamību un datu ierakstu pareizu secību;

   m) "virsgrāmatas ziņojums" ir no elektroniskas virsgrāmatas datu ierakstiem izgūtas verificējamas informācijas strukturēts izklāsts, kas sniedz ieskatu par konkrētām darbībām, stāvokļiem vai atbilstību iepriekš definētiem noteikumiem;

   n) "kvalificētas elektroniskas virsgrāmatas nodrošinātājs" ir kvalificēts uzticamības pakalpojumu sniedzējs, kas sniedz kvalificētu uzticamības pakalpojumu, ko veido datu reģistrēšana kvalificētā elektroniskā virsgrāmatā;

   o) "kvalificēta sadalīta elektroniska virsgrāmata" ir sadalīta elektroniska virsgrāmata, kas atbilst kvalificētas elektroniskas virsgrāmatas prasībām.

2. Ja kvalificētajam uzticamības pakalpojumu sniedzējam ir jāsagatavo virsgrāmatas ziņojums, to sagatavo automatizēti.

3. Kvalificētu elektronisku virsgrāmatu nodrošinātāji izveido un reģistrē elektroniskus datus kvalificētā elektroniskā virsgrāmatā un atjaunina un uztur kvalificētu elektronisko virsgrāmatu saskaņā ar specifikācijām, kas noteiktas turpmāk uzskaitītajos dokumentos.

   a) Visiem kvalificētu elektronisku virsgrāmatu nodrošinātājiem – ETSI EN 319 401 v3.1.1 (2024-06) ar šādiem pielāgojumiem:

      — 2.1. Normatīvās atsauces:

         [1] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos – "Saskaņoti kriptogrāfijas mehānismi", ko publicējusi Eiropas Savienības Kiberdrošības aģentūra ("*ENISA*").

[2] IETF RFC 7515 (2015. gada maijs) – "*JSON* tīmekļa paraksts (*JWS*)".

[3] FIPS PUB 140-3 (2019) "Drošības prasības kriptogrāfijas moduļiem".

[4] Komisijas Īstenošanas regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881.

[5] Komisijas Īstenošanas regula (ES) 2024/3144 (2024. gada 18. decembris) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

[6] SO/IEC 15408:2022 (1.–5. daļa) – "Informācijas drošība, kiberdrošība un privātuma aizsardzība – IT drošības vērtēšanas kritēriji".

— 6.1. Uzticamības pakalpojumu prakses paziņojums:

  — REQ-6.1-12. Elektroniskas virsgrāmatas prakses paziņojumā iekļauj vismaz šādu informāciju:

    — elektroniskās virsgrāmatas platformas funkcionālās un tehniskās spējas un tās kā kvalificēta uzticamības pakalpojuma izmantošana visā tajā laikā, kad tiek nodrošināta datu reģistrēšana kvalificētā elektroniskā virsgrāmatā,

    — konkrētie datu izcelsmes autentifikācijas mehānismi, ko izmanto, sniedzot pakalpojumu,

    — konkrētie secīgas hronoloģiskas kārtošanas mehānismi, ko izmanto, sniedzot pakalpojumu,

    — attiecīgā gadījumā – kriptogrāfijas saite, ko izmanto, lai nodrošinātu datu ierakstu secību,

    — attiecīgā gadījumā – konsensa mehānisms, kas nodrošina virsgrāmatā glabāto datu ierakstu un darījumu galīgumu un integritāti, citastarp laika pielaide līdz galīguma un integritātes sasniegšanai,

    — konkrētie datu integritātes mehānismi, ko izmanto, sniedzot pakalpojumu.

  — 6.2. Noteikumi:

    — REQ-6.2-03. Abonentus un puses, kas izmanto uzticamības pakalpojumu, pirms līgumattiecību uzsākšanas skaidrā, visaptverošā un viegli pieejamā veidā publiski pieejamā telpā un individuāli informē par precīziem noteikumiem, ietverot iepriekšējos punktos uzskaitīto.

  — 6.3. Informācijas drošības politika:

    — REQ-6.3-04X. Uzticamības pakalpojumu sniedzējs izveido procedūras, ar kurām saskaņā ar uzņēmējdarbības prasībām un attiecīgajiem normatīvajiem aktiem uzraudzības iestādei paziņo par visām izmaiņām uzticamības pakalpojuma sniegšanā. Uzticamības pakalpojumu sniedzējs uzraudzības iestādi informē vismaz:

      — vienu mēnesi pirms jebkādu izmaiņu ieviešanas,

      — trīs mēnešus pirms plānotās uzticamības pakalpojuma sniegšanas izbeigšanas.

  — 7.2. Cilvēkresursi:

    — REQ-7.2-04X. Uzticamības pakalpojumu sniedzēja darbinieki uzticamības lomā spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju.

— REQ-7.2-05X. Tas ietver regulārus (vismaz reizi 12 mēnešos) atjauninājumus par jauniem apdraudējumiem un pašreizējo drošības praksi.

— 7.5. Kriptogrāfijas kontroles:

— REQ-7.5-01X. Ir ieviestas pienācīgas drošības kontroles visu kriptogrāfijas atslēgu, kriptogrāfijas algoritmu un kriptogrāfijas ierīču pārvaldībai visā to dzīves ciklā, attiecīgā gadījumā ievērojot kriptogrāfiskās elastības pieeju.

— REQ-7.5-02. Nolūkā nodrošināt savus uzticamības pakalpojumus uzticamības pakalpojumu sniedzējs izvēlas un izmanto piemērotus kriptogrāfijas paņēmienus, kas atbilst saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [1].

Konkrētāk:

— REQ-7.5-03. Kvalificētu elektronisku virsgrāmatu nodrošinātāji apliecina datu ierakstu izcelsmi elektroniskajā virsgrāmatā. Šajā nolūkā tie izmanto uzlabotus elektroniskos parakstus, kuru pamatā ir kvalificēti sertifikāti, vai uzlabotus elektroniskos zīmogus, kuru pamatā ir kvalificēti sertifikāti, ko radījuši pakalpojuma lietotāji saskaņā ar šādiem standartiem un specifikācijām:

a) ETSI EN 319 122-1 V1.3.1 (2023-06) – Elektroniskie paraksti un infrastruktūras (*ESI*), *CAdES* elektroniskie paraksti, 1. daļa – Pamatelementi un *CAdES* pamata paraksti;

b) ETSI EN 319 132-1 V1.3.1 (2024-07) – Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*), *XAdES* elektroniskie paraksti, 1. daļa – Pamatelementi un *XAdES* pamata paraksti;

c) ETSI TS 119 182-1 V1.2.1 (2024-07) – Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*), *JAdES* elektroniskie paraksti, 1. daļa – Pamatelementi un *JAdES* pamata paraksti ar šādu pielāgojumu:

— 5.1.8. Galvenes parametrs x5c (X.509 Sertifikāta ķēde)

— IETF RFC 7515 [2] 4.1.6. punktā definētais x5c galvenes parametrs ir klātesošs *JAdES* parakstā vai nu kā parakstīts, vai neparakstīts galvenes parametrs,

— x5c galvenes parametra semantika ir, kā norādīts IETF RFC 7515 [2] 4.1.6. punktā,

— x5c galvenes parametra sintakse ir, kā norādīts IETF RFC 7515 [2] 4.1.6. punktā.

— REQ-7.5-04. Kvalificētu elektronisku virsgrāmatu nodrošinātāji nodrošina datu ierakstu unikālo secīgo kārtošanu elektroniskajā virsgrāmatā. Šajā nolūkā tie izmanto kriptogrāfijas saites, kuru pamatā ir jaucējkodu saraksti vai jaucējkodu koki, izmantojot kriptogrāfiskās jaucējfunkcijas, saskaņā ar šādām specifikācijām un standartiem:

a) SHA-256 vai augstāks jaucējkoda lielums saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [1];

b) SHA3-256 vai augstāks jaucējkoda lielums saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [1].

Alternatīvs variants – izmantojot laika reģistrēšanu, lai nodrošinātu datu ierakstu unikālo secīgo hronoloģisko kārtību elektroniskajā virsgrāmatā, kvalificētu elektronisko virsgrāmatu nodrošinātāji lieto kvalificētus laika zīmogus.

— REQ-7.5-05. Kvalificētu elektronisku virsgrāmatu nodrošinātāji nodrošina kvalificētā elektroniskā virsgrāmatā reģistrētu datu ierakstu integritāti. Šajā nolūkā tie izmanto uzlabotus elektroniskos parakstus, kuru pamatā ir kvalificēti sertifikāti, vai uzlabotus elektroniskos zīmogus, kuru pamatā ir kvalificēti sertifikāti, saskaņā ar šādiem standartiem un specifikācijām:

a) jebkādi paraksta vai zīmoga formāti, kas atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [1];

b) SHA-256 vai augstāks jaucējkoda lielums saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [1];

c) SHA3-256 vai augstāks jaucējkoda lielums saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [1];

d) kvalificētu elektronisku virsgrāmatu nodrošinātāji nodrošina kvalificētā elektroniskā virsgrāmatā reģistrētu datu jebkādu sekojošu izmaiņu tūlītēju atklājamību.

— REQ-7.5-06. Ja izmanto digitālā paraksta mehānismus, kvalificētas elektroniskas virsgrāmatas nodrošinātāja parakstīšanas privātās atslēgas glabā un izmanto drošas kriptogrāfijas ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotajiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kā noteikts ISO/IEC 15408 ([1]) [6], vai vienoto informācijas tehnoloģiju drošības izvērtēšanas vienotajiem kritērijiem (versija CC:2022, 1.–5. daļa), ko publicējuši Vienošanās par kopējo kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki un kas sertificēti saskaņā ar *EAL 4* vai augstāka līmeņa *EAL*; vai

b) vienotos kritērijos balstīto Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*) ([2]) ([3]) [4][5], un sertificēta saskaņā ar *EAL 4* vai augstāka līmeņa *EAL*; vai

c) FIPS PUB 140-3 ([4]) [3] 3. līmeni (līdz 31.12.2030.).

Šī sertifikācija attiecas uz drošības mērķi vai aizsardzības profilu, vai moduļa dizainu un drošības dokumentāciju, kas atbilst šā dokumenta prasībām, pamatojoties uz riska analīzi un ņemot vērā fiziskos un citus netehniskos drošības pasākumus.

Ja drošajai kriptogrāfiskajai ierīcei piemēro *EUCC* sertifikāciju [4] [5], šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

([1]) ISO/IEC 15408:2022 (1.–5. daļa) – "Informācijas drošība, kiberdrošība un privātuma aizsardzība – IT drošības vērtēšanas kritēriji".

([2]) Komisijas Īstenošanas Regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Komisijas Īstenošanas regula (ES) 2024/3144 (2024. gada 18. decembris) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem (OV L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019) – "Drošības prasības kriptogrāfijas moduļiem".

— 7.8. Tīkla drošība:

— REQ-7.8-14X. Ievainojamības skenēšanu, kas prasīta REQ-7.8-13, veic vismaz reizi ceturksnī.

— REQ-7.8-18X. Ielaušanās testu, kas prasīts REQ-7.8-17X, veic vismaz reizi gadā.

— REQ-7.8-21X. Ugunsmūri arī ir konfigurēti tā, lai novērstu visus protokolus un piekļuvi, kas nav vajadzīga uzticamības pakalpojumu sniedzēja darbībai.

— 7.9.1. Uzraudzība un reģistrēšana:

— REQ-7.9.1-02X. Uzraudzības darbībās ņem vērā visas savāktās vai analizētās informācijas sensitivitāti.

— 7.12. Uzticamības pakalpojumu sniedzēja darbības izbeigšana un izbeigšanas plāni:

— REQ-7.12-02A Uzticamības pakalpojumu sniedzēja darbības izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu [i.1].

b) Turklāt visiem kvalificētu elektronisku virsgrāmatu nodrošinātājiem, kas izmanto sadalītas elektroniskās virsgrāmatas tehnoloģijas:

1) ISO 23257:2022. Blokķēdes un sadalītās virsgrāmatas tehnoloģijas. Atsauces arhitektūra, 9. punkts, kurā sniegts pilnīgs apraksts par sadalītās elektroniskās virsgrāmatas tehnoloģiju sistēmu, atbilstošo sadalītās elektroniskās virsgrāmatas tehnoloģiju tīklu un sadalītajiem elektroniskās virsgrāmatas tehnoloģiju mezgliem;

2) ISO/TS 23635:2022. Blokķēdes un sadalītās virsgrāmatas tehnoloģijas. Pārvaldības vadlīnijas attiecībā uz rakstisku un publiski pieejamu politiku un praksi, kas saistīta ar to nodrošināto elektroniskās virsgrāmatas pakalpojumu pārvaldības struktūru.