2025/1944

30.9.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1944

(2025. gada 29. septembris),

ar ko paredz noteikumus Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz atsauces standartiem saistībā ar datu nosūtīšanas un saņemšanas procesiem kvalificētos elektroniski reģistrētos piegādes pakalpojumos un attiecībā uz šādu pakalpojumu sadarbspēju

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 44. panta 2. punktu un 44. panta 2.b punktu,

tā kā:

(1) Kvalificēti elektroniski reģistrēti piegādes pakalpojumi nodrošina drošu kanālu dokumentu nosūtīšanai, arī pierādījumu par datu nosūtīšanu un saņemšanu. To mērķis ir nodrošināt noteiktību, identificējot adresātu, un augstu uzticības līmeni sūtītāja identificēšanai.

(2) Regulas (ES) Nr. 910/2014 44. panta 1.a punktā noteiktais pieņēmums par atbilstību būtu jāpiemēro tikai tad, ja kvalificētu elektroniski reģistrēto piegādes pakalpojumu kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajiem standartiem. Šiem 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.

(3) Ja uzticamības pakalpojumu sniedzējs ievēro šīs regulas I pielikumā noteiktās prasības, uzraudzības iestādēm būtu jāpieņem, ka ir ievērotas Regulas (ES) Nr. 910/2014 attiecīgās prasības, un šāds pieņēmums pienācīgi jāņem vērā, piešķirot vai apstiprinot uzticamības pakalpojuma kvalificēto statusu. Tomēr atbilstības Regulas (ES) Nr. 910/2014 prasībām pierādīšanai kvalificēta uzticamības pakalpojuma sniedzējs joprojām var paļauties uz citu praksi.

(4) Saskaņā ar Regulas (ES) Nr. 910/2014 44. panta 2.a punktu gadījumā, ja kvalificēti uzticamības pakalpojumu sniedzēji vienojas padarīt savus pakalpojumus sadarbspējīgus, ir svarīgi, lai tie ievērotu attiecīgos standartus un specifikācijas, kas noteiktas šīs īstenošanas regulas II pielikumā, nolūkā atvieglot elektroniski reģistrētu datu nosūtīšanu starp diviem vai vairākiem kvalificētiem uzticamības pakalpojumu sniedzējiem un veicināt godprātīgu praksi iekšējā tirgū.

(5) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1183 ([2]) 75. apsvērumu Komisijai šī regula vajadzības gadījumā būtu jāpārskata un jāatjaunina, lai tā atbilstu globālajām norisēm, jaunām tehnoloģijām, standartiem un tehniskajām specifikācijām un lai ņemtu vērā 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) Visām šajā regulā noteiktajām 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]).

(7) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([5]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 6. jūnijā sniedza savu atzinumu.

(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

Kvalificētu elektroniski reģistrētu piegādes pakalpojumu atsauces standarti un specifikācijas

Regulas (ES) Nr. 910/2014 44. panta 2. punktā minētie atsauces standarti un specifikācijas ir izklāstītas šīs regulas I pielikumā.

2. pants

Atsauces standarti un specifikācijas kvalificētu elektroniski reģistrētu piegādes pakalpojumu sadarbspējai

Regulas (ES) Nr. 910/2014 44. panta 2.b punktā minētie atsauces standarti un specifikācijas ir noteiktas šīs regulas II pielikumā.

3. 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 29. septembrī

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]) 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).

I PIELIKUMS

Regulas 1. pantā norādīto atsauces standartu un specifikāciju saraksts

Standartu ETSI EN 319 521 V1.1.1 (2019-02) ("ETSI EN 319 521") piemēro ar šādiem pielāgojumiem.

1. Attiecībā uz ETSI EN 319 521

1) 2.1. Normatīvās atsauces

— [1] ETSI EN 319 401 V3.1.1 (2024-06) "Elektroniskie paraksti un infrastruktūras (*ESI*); vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem".

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Elektroniskie paraksti un infrastruktūras (*ESI*); politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus. 1. daļa: Vispārīgas prasības".

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) "Elektroniskie paraksti un infrastruktūras (*ESI*); elektroniski reģistrēti piegādes pakalpojumi. 1. daļa: Satvars un arhitektūra".

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) "Elektroniskie paraksti un infrastruktūras (*ESI*); elektroniski reģistrēti piegādes pakalpojumi. 2. daļa: Semantisks saturs".

— [5] Eiropas Kiberdrošības sertifikācijas grupas kriptogrāfijas jautājumu apakšgrupa: "Saskaņoti kriptogrāfijas mehānismi", ko publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ([1]).

— [6] ISO/IEC 15408-1:2022 "Informācijas drošība, kiberdrošība un privātuma aizsardzība – IT drošības vērtēšanas kritēriji".

— [7] Komisijas Īstenošanas regula (ES) 2024/482 ([2]) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881.

— [8] Komisijas Īstenošanas regula (ES) 2024/3144 ([3]) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

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

2) 3.1. Noteikumi

— "Uzlabots elektroniskais zīmogs": kā definēts Regulā (ES) Nr. 910/2014 [i.1].

— "Uzlabots elektroniskais paraksts": kā definēts Regulā (ES) Nr. 910/2014 [i.1].

— "Kvalificēts elektroniskais zīmogs": kā definēts Regulā (ES) Nr. 910/2014 [i.1].

— "Kvalificēts elektroniskais paraksts": kā definēts Regulā (ES) Nr. 910/2014 [i.1].

— "Drošas kriptogrāfijas ierīce": ierīce, kurā glabājas lietotāja privātā atslēga, kas aizsargā šo atslēgu pret apdraudējumu un veic parakstīšanas vai atšifrēšanas funkcijas lietotāja vārdā.

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

3) 5.1.1. Kopīgie noteikumi

— REQ-ERDS-5.1.1-01 *ERDS* nodrošina, ka lietotāja satura pieejamība, integritāte un konfidencialitāte tiek pienācīgi garantēta laikā, kad to apstrādā *ERDS*, izvēloties piemērotus integritātes un konfidencialitātes kriptogrāfijas paņēmienus, kas atbilst saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [5].

4) 5.2.1.1. Vispārīgi noteikumi

— REQ-QERDS-5.2.1.1-01 *QERDSP* ar ļoti augstu ticamības līmeni pārbauda saņēmēja identitāti vai nu tieši, vai paļaujoties uz trešo personu, un vajadzības gadījumā izmantojot vienu no šādiem līdzekļiem vai to kombināciju:

a) fiziskās personas vai juridiskās personas pilnvarotā pārstāvja fiziskā klātbūtnē, izmantojot atbilstīgus pierādījumus un procedūras, saskaņā ar valstu tiesību aktiem;

b) attālināti, izmantojot elektroniskās identifikācijas līdzekļus, kas atbilst Regulas (ES) Nr. 910/2014 [i.1] 8. pantā noteiktajām prasībām attiecībā uz uzticamības līmeni "augsts", vai izmantojot Eiropas digitālās identitātes maku;

c) izmantojot kvalificēta elektroniskā paraksta vai kvalificēta elektroniskā zīmoga sertifikātu;

d) izmantojot citas identifikācijas metodes, kas nodrošina, ka fizisko personu vai juridiskās personas pilnvaroto pārstāvi var identificēt ar ļoti augstu ticamības līmeni. Apliecinājumu, ka šī identifikācija tiek veikta ar ļoti augstu ticamības līmeni, apstiprina atbilstības novērtēšanas struktūra.

— REQ-QERDS-5.2.1.1-01A *QERDSP* pārbauda sūtītāja identitāti, izmantojot piemērotus līdzekļus vai nu tieši, vai paļaujoties uz trešo personu, pamatojoties uz vienu no šādām metodēm vai to kombināciju:

a) fiziskās personas vai juridiskās personas pilnvarotā pārstāvja fiziskā klātbūtnē, izmantojot atbilstīgus pierādījumus un procedūras, saskaņā ar valstu tiesību aktiem;

b) attālināti, izmantojot Eiropas digitālās identitātes maku vai paziņotus elektroniskās identifikācijas līdzekļus, kas atbilst Regulas (ES) Nr. 910/2014 [i.1] 8. pantā izklāstītajām prasībām attiecībā uz uzticamības līmeni "būtisks", ar noteikumu, ka tie ir izdoti, pamatojoties uz fiziskās personas vai juridiskās personas pilnvarotā pārstāvja iepriekšēju fizisku klātbūtni;

c) izmantojot uzlabotu elektronisko parakstu vai uzlabotu elektroniskā zīmoga sertifikātu ar noteikumu, ka sertifikāts ir izdots fiziskai personai vai juridiskās personas pilnvarotam pārstāvim saskaņā ar normalizēto sertifikātu politiku (*NCP*), kā definēts ETSI EN 319 411-1 [2]; vai

d) izmantojot citas identifikācijas metodes, kas nodrošina, ka fizisko personu vai juridiskās personas pilnvaroto pārstāvi var identificēt ar ļoti augstu ticamības līmeni. Apliecinājumu, ka šī identifikācija tiek veikta ar augstu ticamības līmeni, apstiprina atbilstības novērtēšanas struktūra.

— JĀŅEM VĒRĀ, ka trešā persona, kas pārbauda sūtītāja un saņēmēja identitāti, var būt cits *QERDSP*, ja sūtītājs un saņēmējs abonē dažādus *QERDSP*.

5) 5.2.1.2. Saņēmēja identifikācija un lietotāja satura nodošana

— REQ-QERDS-5.2.1.2-03 Ja saņēmēja identifikācijas pamatā ir *QERDS* iekšējais process, *QERDSP* veic visu procesu drošā un kontrolētā vidē.

6) 5.2.2. Noteikumi par *EU QERDS* autentifikāciju

— REQ-QERDS-5.2.2-03 [AR NOSACĪJUMIEM] Ja *QERDSP* saista autentifikācijas līdzekļus ar sūtītāja identitāti, kas verificēta saskaņā ar 5.2.1. punktu, autentifikācijas līdzeklis ir kāds no turpmāk uzskaitītajiem līdzekļiem:

a) divu faktoru autentifikācijas mehānismi;

b) Eiropas digitālās identitātes maks vai paziņots elektroniskās identifikācijas līdzeklis, kas atbilst Regulas (ES) Nr. 910/2014 [i.1] 8. pantā noteiktajām prasībām attiecībā uz uzticamības līmeni "augsts" vai "būtisks";

c) savstarpēja *TLS* autentifikācija, kas ietver sertifikātu, kurš sūtītājam izdots saskaņā ar *NCP*, kā definēts ETSI EN 319 411-1 [2];

d) digitālais paraksts, ko papildina sertifikāts, kurš izdots saskaņā ar *NCP*, kā definēts ETSI EN 319 411-1 [2];

e) citi līdzekļi, kas nodrošina identificētā nosūtītāja autentifikāciju. Saistošo nosacījumu atbilstību apstiprina atbilstības novērtēšanas struktūra. Piemērs. Tas var ietvert kāda no iepriekš a), b) un d) apakšpunktā minēto līdzekļu izmantošanu, lai reģistrētu *Transport Layer Security* (*TLS*) klienta sertifikātu automatizētai nosūtīšanai, izmantojot savstarpēju *TLS*, vai lai reģistrētu digitālā zīmoga sertifikātu, ko izmanto apliecinājumu apzīmogošanai ar mērķi nodrošināt autentifikāciju *ERDS*. Var piemērot arī citus mehānismus, ja identificētie sūtītāji izmanto deleģētu trešo personu pakalpojumus.

— REQ-QERDS-5.2.2-03A [AR NOSACĪJUMIEM] Ja *QERDSP* saista autentifikācijas līdzekļus ar saņēmēja identitāti, kas verificēta saskaņā ar 5.2.1. punktu, izmanto kādu no turpmāk minētajiem līdzekļiem ar noteikumu, ka līdzekļi vai jebkāda līdzekļu kombinācija nodrošina ļoti augstu ticamības līmeni attiecībā uz autentificētā saņēmēja identitāti:

a) daudzfaktoru autentifikācijas mehānisms;

b) Eiropas digitālās identitātes maks vai paziņots elektroniskās identifikācijas līdzeklis, kas atbilst Regulas (ES) Nr. 910/2014 [i.1] 8. pantā noteiktajām prasībām attiecībā uz uzticamības līmeni "augsts" vai "būtisks";

c) kvalificēta elektroniskā paraksta vai kvalificēta elektroniskā zīmoga sertifikāts;

d) citi līdzekļi, kas nodrošina identificētā saņēmēja autentifikāciju. Saistošo nosacījumu atbilstību apstiprina atbilstības novērtēšanas struktūra. Piemērs. Tas var ietvert viena no iepriekš a)–c) apakšpunktā minēto līdzekļu izmantošanu, lai reģistrētu *Transport Layer Security* (*TLS*) klienta sertifikātu automatizētai nosūtīšanai, izmantojot savstarpēju *TLS*, vai lai reģistrētu digitālā zīmoga sertifikātu apliecinājumu apzīmogošanai ar mērķi nodrošināt autentifikāciju *ERDS*. Var piemērot arī citus mehānismus, ja identificētie sūtītāji izmanto deleģētu trešo personu pakalpojumus.

— REQ-QERDS-5.2.2-04 [AR NOSACĪJUMIEM] Ja sūtītājs izveido drošu savienojumu ar *QERDS*, kam nepieciešama mašīnu savstarpēja autentifikācija starp sūtītāja iekārtu un *QERDS* serveri, pamatojoties uz sertifikātiem, kas izdoti saskaņā ar ETSI EN 319 411-1 [2] noteikto *NCP*, tad pēc šā drošā savienojuma izveidošanas nosūtītāja autentifikācijas otrajā posmā var piemērot viena faktora autentifikācijas mehānismus, ja ieviestās organizatoriskās procedūras un drošības pasākumi nodrošina uzticamību attiecībā uz nosūtītāja autentifikāciju.

7) 5.4.1. Kopīgie noteikumi

— REQ-ERDS-5.4.1-06 *ERDS* ģenerē un leģitīmām ieinteresētajām personām dara pieejamus *ERDS* pierādījumus par *ERD* notikumiem, kā noteikts ETSI EN 319 522-1 [3] 6. punktā.

— REQ-ERDS-5.4.1-07 *ERDSP* arhivē pierādījumus un/vai pierādījumu kopsavilkumu par katru tā izdoto pierādījumu.

— REQ-ERDS-5.4.1-08 *ERDS* ģenerētie pierādījumi atbilst ETSI EN 319 522-2 [4] 8. punktā definētajai pierādījumu semantikai.

8) 7.2.1. Kopīgie noteikumi

— REQ-ERDS-7.2.1-02 *ERDSP* darbinieki uzticamās lomās spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju.

— REQ-ERDS-7.2.1-03 Atbilstība REQ-ERDS-7.2.1-02 ietver regulārus (vismaz reizi 12 mēnešos) atjauninājumus par jauniem apdraudējumiem un pašreizējo drošības praksi.

9) 7.3.2. Mediju apstrāde

— REQ-ERDS-7.3.1-02 Piemēro visas ETSI EN 319 401 [1] 7.3.3. punkta prasības.

10) 7.5. Kriptogrāfijas kontroles

— REQ-ERDS-7.5-01A *ERDS* izvēlas un izmanto piemērotus kriptogrāfijas paņēmienus, kas atbilst saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [5].

— REQ-ERDSP-7.5-03 *ERDS* privāto parakstīšanas atslēgu glabā un izmanto drošas kriptogrāfijas ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotajiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kā izklāstīts ISO/IEC 15408 [6], vai vienoto informācijas tehnoloģiju drošības izvērtēšanas metodiku (versija CC:2002, 1.–5. daļa), ko publicējuši Vienošanos par kopējo kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki un kas sertificēti saskaņā ar *EAL* 4 vai augstāku standartu; vai

b) vienotos kritērijos balstīto Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*) [7][8], un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) līdz 31.12.2030. FIPS PUB 140-3 [9] 3. līmeni.

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* [7][8] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

11) 7.8. Tīkla drošība

— REQ-ERDSP-7.8-04 *ERDSP* izmanto mūsdienīgus protokolus un algoritmus šifrēšanai transporta slāņa līmenī saskaņā ar saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [5].

— REQ-ERDSP-7.8-06 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī.

— REQ-ERDSP-7.8-07 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā.

— REQ-ERDSP-7.8-08 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas *TSP* darbībai.

12) 7.12. *ERDSP* darbības izbeigšana un izbeigšanas plāni

— REQ-ERDS-7.12-03: *ERDSP* darbības izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kuri pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu [i.1].

13) 7.14. Piegādes ķēde

— REQ-ERDS-7.14-01 Piemēro ETSI EN 319 401 [1] 7.14. punktā noteiktās prasības.

II PIELIKUMS

Regulas 2. pantā norādīto atsauces standartu un specifikāciju saraksts

Piemēro standartus 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”) un ETSI EN 319 522-4-3 V1.1.1 (2018-09) (“ETSI EN 319 522-4-3”).