2025/1929

30.9.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1929

(2025. gada 29. septembris),

kas nosaka Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu datuma un laika sasaistei ar datiem un precīzus laika avotus kvalificētu elektronisko laika zīmogu nodrošināšanai

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 42. panta 2. punktu,

tā kā:

(1) Kvalificētiem elektroniskajiem laika zīmogiem ir izšķiroša nozīme digitālajā vidē, jo tie veicina pāreju no tradicionāliem procesiem papīra formātā uz elektroniskiem ekvivalentiem. Sasaistot datuma un laika informāciju ar elektroniskajiem datiem, kvalificēti elektroniskie laika zīmogi palīdz nodrošināt tajos norādītā datuma un laika precizitāti un to digitālo dokumentu integritāti, uz kuriem attiecas datums un laiks.

(2) Regulas (ES) Nr. 910/2014 42. panta 1.a punktā noteiktais pieņēmums par atbilstību būtu jāpiemēro tikai tad, ja kvalificētu elektronisko zīmogu izsniegšanas kvalificēti uzticamības pakalpojumi atbilst šajā regulā noteiktajiem standartiem. Šiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Šie standarti būtu jāpielāgo nolūkā iekļaut papildu kontroles, kas nodrošina kvalificētā uzticamības pakalpojuma un datuma un laika sasaistes ar datiem, kā arī laika avota precizitātes drošību un uzticamību.

(3) Ja uzticamības pakalpojumu sniedzējs ievēro šīs regulas pielikumā izklāstītās prasības, uzraudzības iestādēm būtu jāpieņem, ka attiecīgās Regulas (ES) Nr. 910/2014 prasības ir ievērotas un pienācīgi jāņem vērā šis pieņēmums uzticamības pakalpojuma kvalificētā statusa piešķiršanai vai apstiprināšanai. Tomēr atbilstības Regulas (ES) Nr. 910/2014 prasībām pierādīšanai kvalificēts uzticamības pakalpojumu sniedzējs joprojām var paļauties uz citu praksi.

(4) 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 īstenošanas regula vajadzības gadījumā būtu jāpārskata un jāatjaunina nolūkā nodrošināt tās atbilstību globālajām norisēm, jaunajām tehnoloģijām, standartiem un tehniskajām specifikācijām un ievērot paraugpraksi iekšējā tirgū.

(5) 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]).

([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).

([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.

(6) 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.

(7) Šajā regulā noteiktie pasākumi atbilst ar Regulas (ES) Nr. 910/2014 48. pantu izveidotās komitejas atzinumam,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Regulas (ES) Nr. 910/2014 42. panta 2. punktā minētie atsauces standarti un specifikācijas ir izklāstītas šīs regulas pielikumā.

2. pants

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

([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).

PIELIKUMS

Kvalificētu laika zīmogu pakalpojumu atsauces standartu un specifikāciju saraksts

Standartus ETSI EN 319 421 V1.3.1 ([1]) ("ETSI EN 319 421") un ETSI EN 319 422 V1.1.1 ([2]) ("ETSI EN 319 422") piemēro ar šādiem pielāgojumiem:

1. ETSI EN 319 421:

   1) 2.1. Normatīvās atsauces:

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

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

      — [5] ETSI EN 319 422 V1.1.1 (2016-03) "Elektroniskie paraksti un infrastruktūras (*ESI*); Laika zīmogošanas protokols un laika zīmoga marķieru profili",

      — [6] nav spēkā,

      — [9] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos: "Saskaņoti kriptogrāfijas mehānismi", ko publicējusi Eiropas Savienības Kiberdrošības aģentūra ("*ENISA*") ([3]),

      — [10] 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 ([4]),

      — [11] 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 ([5]);

   2) 3.1. Definīcijas

      — sertifikāta derīguma termiņš: laika intervāls no "ne pirms" [*notBefore*] līdz "ne pēc" [*notAfter*] (ieskaitot), kurā sertifikācijas iestāde ("SI") garantē, ka saglabās informāciju par sertifikāta statusu;

   3) 3.3. Saīsinājumi

      — *EUCC*: vienotos kritērijos balstītā Eiropas kiberdrošības sertifikācijas shēma;

   4) 6.2. Uzticamības pakalpojumu prakses paziņojums

      — OVR-6.2-03 *TSA* savā *TSA* paziņojumā par informācijas atklāšanu iekļauj paziņojumus par sava laika zīmogošanas pakalpojuma pieejamību;

   5) 7.3. Personāla drošība

      — OVR-7.3-02 *TSA* darbinieki, kas pilda uzticamības funkcijas, un attiecīgā gadījumā apakšuzņēmēji, kas pilda uzticamības funkcijas, spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju,

      — OVR-7.3-03 Atbilstība OVR-7.3-02 ietver regulārus atjauninājumus (vismaz reizi 12 mēnešos) par jauniem apdraudējumiem un pašreizējo drošības praksi;

([1]) EN 319 421 – Elektroniskie paraksti un infrastruktūras (*ESI*). Politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izsniedz laika zīmogus, V1.3.1.
([2]) EN 319 422 – Elektroniskie paraksti un infrastruktūras (*ESI*) – Laika zīmogošanas protokols un laika zīmoga marķieru profili, V1.1.1 (2016-03). https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) OV L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2. *TSU* atslēgas ģenerēšana

— TIS-7.6.2-03 *TSU* atslēgas(-u) ģenerēšanu veic drošā kriptogrāfiskā ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kas noteikti *ISO/IEC* 15408 [3] vai Vienotajos informācijas tehnoloģiju drošības izvērtēšanas kritērijos, CC:2022. redakcija, 1.–5. daļa, ko publicējuši Vienošanās par vienotu kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki, un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

b) *EUCC* [10][11] un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) *FIPS PUB* 140-3 [7] 3. līmeni (līdz 31.12.2030.).

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

Ja drošas kriptogrāfijas ierīcei piemēro *EUCC* [10][11] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju;

— TIS-7.6.2-04 nav spēkā,

— 3. PIEZĪME nav spēkā,

— TIS-7.6.2-05A *TSU* atslēgas ģenerēšanas algoritms, rezultātā iegūtās parakstīšanas atslēgas garums un paraksta algoritms, ko izmanto attiecīgi laika zīmogu parakstīšanai un *TSU* publiskās atslēgas sertifikātu parakstīšanai, atbilst saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa [9] un publicējusi *ENISA*,

— 4. PIEZĪME nav spēkā,

— TIS-7.6.2-06 *TSU* parakstīšanas atslēgu eksportē un importē citā drošas kriptogrāfijas ierīcē tikai tad, ja šo eksportu un importu veic droši un saskaņā ar minēto ierīču sertifikāciju;

7) 7.6.3. *TSU* privātās atslēgas aizsardzība

— TIS-7.6.3-02 *TSU* privāto atslēgu glabā un izmanto drošas kriptogrāfijas ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kas noteikti *ISO/IEC* 15408 [3] vai Vienotajos informācijas tehnoloģiju drošības izvērtēšanas kritērijos, CC:2002. redakcija, 1.–5. daļa, ko publicējuši Vienošanās par vienotu kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki, un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

b) vienotos kritērijos balstīto Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*) [10][11], un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) *FIPS PUB* 140-3 [7] 3. līmeni (līdz 31.12.2030.).

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

Ja drošas kriptogrāfijas ierīcei piemēro *EUCC* [10][11] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju,

— TIS-7.6.3-03 nav spēkā,

— 2. PIEZĪME nav spēkā;

8) 7.6.7. *TSU* atslēgas aprites cikla beigas

— TIS-7.6.7-03A *TSU* privāto atslēgu derīguma termiņš atbilst saskaņotajiem kriptogrāfijas mehānismiem [9],

— 1. PIEZĪME nav spēkā;

9) 7.10. Tīkla drošība

— OVR-7.10-05 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī,

— OVR-7.10-06 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā,

— OVR-7.10-07 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas uzticamības pakalpojuma sniedzēja darbībai;

10) 7.14. *TSA* darbības izbeigšana un izbeigšanas plāni

— OVR-7.14-01A *TSP* darbības izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu [i.4].

2. ETSI EN 319 422:

1) 2.1. Normatīvās atsauces

— [5] nav spēkā,

— [6] nav spēkā,

— [8] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos: "Saskaņoti kriptogrāfijas mehānismi",

— [9] RFC 9110 *HTTP Semantics*;

2) 4.1.3. Izmantojamie jaucējalgoritmi

— Piemēro šādu klauzulu:

Jaucējalgoritmi, ko izmanto ar laika zīmogu apzīmogotas informācijas jaukšanai, paredzamais laika zīmoga ilgums un izvēlētās jaucējfunkcijas atkarībā no laika atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

3) 4.2.3. Atbalstāmie algoritmi

— Piemēro šādu klauzulu:

Atbalstāmie laika zīmoga marķiera algoritmi atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

4) 4.2.4. Atbalstāmie atslēgu garumi

— Piemēro šādu klauzulu:

Paraksta algoritma atslēgas garumi izvēlētajam paraksta algoritmam atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA*,

— PIEZĪME nav spēkā;

5) 5.1.3. Atbalstāmie algoritmi

— Piemēro šādu klauzulu:

Jaucējalgoritmi atbalstāmajiem laika zīmoga datiem, paredzamais laika zīmoga ilgums un izvēlētās jaucējfunkcijas atkarībā no laika atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

6) 5.2.3. Izmantojamie algoritmi

— Piemēro šādu klauzulu:

Jaucējalgoritmi, ko izmanto ar laika zīmogu apzīmogotas informācijas jaukšanai, un laika zīmoga marķiera paraksta algoritms atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

7) 6.3. Prasības attiecībā uz atslēgas garumu

— Piemēro šādu klauzulu:

Atslēgas garums izvēlētajam *TSU* sertifikāta paraksta algoritmam atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

8) 6.5. Prasības attiecībā uz algoritmiem

— Piemēro šādu klauzulu:

TSU publiskajā atslēgā un *TSU* sertifikāta parakstā izmanto algoritmus, kas atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8],

— PIEZĪME nav spēkā;

9) 7. Atbalstāmo transporta protokolu profili

— Laika zīmogošanas klients un laika zīmogošanas serveris atbalsta laika zīmogošanas protokolu, izmantojot *HTTPS* [9], kā noteikts *IETF RFC* 3161 [1] 3.4. punktā;

10) 8. Kriptogrāfijas algoritmu objekta identifikatori

— Piemēro šādu klauzulu:

TSU publiskajā atslēgā un *TSU* sertifikātā izmanto algoritmus saskaņā ar saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8];

11) 9.1. Paziņojums par atbilstību regulai

— Ja *TSA* norāda, ka laika zīmoga marķieris ir kvalificēts elektroniskais laika zīmogs saskaņā ar Regulu (ES) Nr. 910/2014 [i.2], laika zīmoga marķiera paplašinājuma laukā ietver vienu *qcStatements* paplašinājumu ar tādu sintaksi, kā definēts *IETF RFC* 3739 [i.3.] 3.2.6. punktā,

— *QcStatements* paplašinājumā ietver vienu piebildi "*esi4-qtstStatement*-1", kā noteikts B pielikumā,

— paplašinājumu *QcStatements* neatzīmē kā kritisku.