Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1946

30.9.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1946

(2025. gada 29. septembris),

kas nosaka Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu kvalificētu elektronisko parakstu un kvalificētu elektronisko zīmogu saglabāšanas pakalpojumiem

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]), jo īpaši tās 34. panta 2. punktu un 40. pantu,

tā kā:

(1) kvalificētu elektronisko parakstu un kvalificētu elektronisko zīmogu kvalificēti saglabāšanas pakalpojumi nodrošina minēto elektronisko parakstu un elektronisko zīmogu saglabāšanas pierādījumu ilgtermiņa integritāti, autentiskumu, pastāvēšanas pierādījumus un pieejamību. Tas ļauj pierādīt to juridisko derīgumu ilgākos laikposmos un garantē, ka tos var validēt neatkarīgi no turpmākās tehnoloģiju attīstības. Šie pakalpojumi tiek sniegti neatkarīgi vai kā daļa no cita kvalificēta uzticamības pakalpojuma, piemēram, kvalificētiem elektroniskās arhivēšanas pakalpojumiem;

(2) Regulas (ES) Nr. 910/2014 34. panta 1.a punktā un 40. pantā noteiktais pieņēmums par atbilstību būtu jāpiemēro tikai tad, ja kvalificētu elektronisko parakstu un kvalificētu elektronisko zīmogu kvalificētas saglabāšanas pakalpojumi atbilst šajā regulā noteiktajiem standartiem. Šiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Tie būtu jāpielāgo nolūkā iekļaut papildu kontroles, kas nodrošina kvalificētā uzticamības pakalpojuma drošību un uzticamību, kā arī spēju laika gaitā pārbaudīt parakstu un zīmogu kvalificēto statusu un tehnisko derīgumu;

(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 šī regula Komisijai vajadzības gadījumā būtu jāpārskata un jāatjaunina nolūkā nodrošināt tās atbilstību globālajām norisēm, jaunajām tehnoloģijām, standartiem un tehniskajām specifikācijām un 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).

(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]);

(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 atzinumu;

(7) šajā regulā paredzētie pasākumi ir atbilstoši ar Regulas (ES) Nr. 910/2014 48. pantu izveidotās komitejas atzinumam,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Atsauces standarti un specifikācijas

Regulas (ES) Nr. 910/2014 34. panta 2. punktā un 40. pantā minētie atsauces standarti un specifikācijas ir izklāstītas 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 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).

PIELIKUMS

2. pantā minēto atsauces standartu un specifikāciju saraksts

Standartus ETSI TS 119 511 V1.1.1 (2019-06) ("ETSI TS 119 511") un ETSI TS 119 172-4 V1.1.1 (2021-05) ("ETSI TS 119 172-4") piemēro ar šādiem pielāgojumiem:

1. ETSI TS 119 511

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 TS 119 612 (V2.3.1) "Elektroniskie paraksti un infrastruktūras (*ESI*)"; Uzticamības saraksti".

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

— [6] Komisijas Īstenošanas regula (ES) 2024/482 ([1]) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881.

— [7] Komisijas Īstenošanas regula (ES) 2024/3144 ([2]) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

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

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) "Elektroniskie paraksti un infrastruktūras (*ESI*); Parakstīšanas politikas. 4. daļa: Noteikumi par paraksta piemērojamību (validācijas politika) kvalificētiem Eiropas elektroniskajiem parakstiem/zīmogiem, kas izmanto uzticamības sarakstus".

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

2) 3.1. Definīcijas

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

3) 6.4. Saglabāšanas profili

— OVR-6.4-08A [WTS][WOS] Paredzamais pierādījumu ilgums atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA*[8].

— 3. PIEZĪME nav spēkā.

4) 6.5. Pierādījumu saglabāšanas politika

— OVR-6.5-04A Izmantotie kriptogrāfijas algoritmi atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA*[8].

— 1. PIEZĪME nav spēkā.

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

5) 7.2. Cilvēkresursi

— OVR-7.2-02 *PSP* 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-7.2-03 Atbilstība OVR-7.2-02 ietver regulārus atjauninājumus (vismaz reizi 12 mēnešos) par jauniem apdraudējumiem un pašreizējo drošības praksi.

6) 7.5. Kriptogrāfijas kontroles

— OVR-7.5-05 [AR NOSACĪJUMIEM] Ja *PSP* paraksta saglabāšanas pierādījumus (vai to daļu), *PSP* privāto parakstīšanas 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 [10] 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* [6][7] un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) *FIPS PUB* 140-3 [5] 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* [6][7] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

— OVR-7.5-06 [AR NOSACĪJUMIEM] nav spēkā.

— OVR-7.5-07 [AR NOSACĪJUMIEM] Ja *PSP* paraksta saglabāšanas pierādījumus (vai to daļu), visas *PSP* privāto parakstīšanas atslēgu rezerves kopijas aizsargā ar drošas kriptogrāfijas ierīces palīdzību pirms to uzglabāšanas ārpus šīs ierīces, lai nodrošinātu to integritāti un konfidencialitāti.

— OVR-7.5-08 *PSP* privāto 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) 7.8. Tīkla drošība

— OVR-7.8-03 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī.

— OVR-7.8-04 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā.

— OVR-7.8-05 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas *PSP* darbībai.

8) 7.14. Kriptogrāfijas uzraudzība

— OVR-7.14-03A OVR-7.14.01 un OVR-7.14.02 kriptogrāfijas algoritmu izvērtēšana atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [8].

— PIEZĪME nav spēkā.

9) 7.12. *TSP* darbības izbeigšana un izbeigšanas plāni

— OVR-7.12-01A *TSP* darbības izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu [i.2].

10) 7.17. Piegādes ķēde

— OVR-7.17-01 Piemēro ETSI EN 319 401 [1] 7.14. punktā noteiktās prasības.

11) A pielikums (normatīvais): *QES* kvalificēts saglabāšanas pakalpojums, kā definēts Regulas (ES) Nr. 910/2014 34. pantā

— OVR-A-02 [PDS][PDS+PGD]

a) saglabāšanas pakalpojums saglabā visu informāciju, kas vajadzīga, lai pārbaudītu elektroniskā paraksta vai zīmoga kvalificēto statusu, un kas nebūtu publiski pieejama līdz saglabāšanas perioda beigām,

b) saglabāšanas pakalpojums nodrošina, ka jebkurā saglabāšanas perioda brīdī saglabātā informācija ir tāda, ka, ievadot to ETSI TS 119 172-4 [9] 4.4. punktā minētajā procesā, šā procesa iznākums skaidri nosaka, vai digitālais paraksts vai zīmogs tā saglabāšanas laikā bijis tehniski piemērots ES kvalificēta elektroniskā paraksta vai ES kvalificēta elektroniskā zīmoga ieviešanai.

— OVR-A-03 [PDS][PDS+PGD] Saglabāšanas pierādījumos izmantotie laika zīmogi ir kvalificēti laika zīmogi saskaņā ar Regulu (ES) Nr. 910/2014 [i.2].

2. ETSI TS 119 172-4:

1) 2.1. Normatīvās atsauces:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) "Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)"; Procedūras *AdES* digitālo parakstu izveidei un validēšanai. 1. daļa: Izveide un validācija".

— Visas atsauces uz "*ETSI TS* 119 102-1 [1]" saprot kā atsauces uz "*ETSI EN* 319 102-1 [1]".

— [2] ETSI TS 119 612 (V2.3.1) "Elektroniskie paraksti un infrastruktūras (*ESI*)"; Uzticamības saraksti".

— [13] ETSI TS 119 101 V1.1.1 (2016-03) "Elektroniskie paraksti un infrastruktūras (*ESI*); Politikas un drošības prasības attiecībā uz paraksta radīšanas un paraksta validācijas pieteikumiem".

2) 4.2. Validācijas ierobežojumi un validācijas procedūras, *REQ*-4.2-03 prasība, iedaļa "X.509 validācijas ierobežojumi", c) punkts:

— i) ja gala subjekta sertifikāts ir uzticamības enkurs, *RevocationCheckingConstraints* neizmanto;

— ii) ja gala subjekta sertifikāts nav uzticamības enkurs, *RevocationCheckingConstraints* iestata uz "*eitherCheck*", kā definēts *ETSI TS* 119 172-1 [3] A.4.2.1. punkta A.2. tabulas m)2.1. rindā;

— iii) ja gala subjekta sertifikāts ir uzticamības enkurs, *ETSI TS* 119 172-1 [3] A.4.2.1. punkta A.2. tabulas m)2.2. rindā definēto *RevocationFreshnessConstraints* neizmanto;

— iv) ja gala subjekta sertifikāts nav uzticamības enkurs, *ETSI TS* 119 172-1 [3] A.4.2.1. punkta A.2. tabulas (m)2.2. rindā definēto *RevocationFreshnessConstraints* izmanto ar parakstīšanas sertifikāta maksimālo vērtību 0, nodrošinot, ka atsaukšanas informācija tiek pieņemta tikai tad, ja tā izdota pēc vislabākā parakstīšanas laika. *RevocationFreshnessConstraints* vērtību nenosaka sertifikātiem, kas nav parakstīšanas sertifikāts, ieskaitot sertifikātiem, kas apliecina laika zīmogus.

3) 4.3. Prasības paraksta validēšanai un piemērojamības noteikumu pārbaudes praksei

— REQ-4.3-02 Paraksta validācijas pieteikumi atbilst ETSI TS 119 101 [13].

4) 4.4. Tehniskās piemērojamības (noteikumu) pārbaudes process

— REQ-4.4.2-03 Ja kāda no REQ-4.4.2-01. punktā norādītajām pārbaudēm ir nesekmīga, tad:

— procesu aptur,

— parakstu tehniski nosaka kā nenoteiktu, t. i., ne kā ES kvalificētu elektronisko parakstu, ne kā kvalificētu ES elektronisko zīmogu,

— iepriekš minēto rezultātu un visu starpprocesu procesu rezultātus atspoguļo paraksta piemērojamības noteikumu pārbaudes ziņojumā.