Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1946

2025 9 30

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1946

2025 m. rugsėjo 29 d.

kuriuo dėl kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotų ilgalaikio išsaugojimo paslaugų nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 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 34 straipsnio 2 dalį ir 40 straipsnį,

kadangi:

(1) kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotos ilgalaikio išsaugojimo paslaugos užtikrina tokių elektroninių parašų ir elektroninių spaudų ilgalaikį vientisumą, autentiškumą, egzistavimo įrodomumą ir prieinamumą prie išsaugojimo įrodymų. Tokiu būdu įmanomą ilgą laikotarpį įrodyti jų teisinį galiojimą ir garantuojama, kad juos bus galima patvirtinti nepriklausomai nuo būsimų technologinių pokyčių. Šios paslaugos teikiamos nepriklausomai arba kartu su kitomis kvalifikuotomis patikimumo užtikrinimo paslaugomis, pavyzdžiui, su kvalifikuotomis elektroninio archyvavimo paslaugomis;

(2) Reglamento (ES) Nr. 910/2014 34 straipsnio 1a dalyje ir 40 straipsnyje numatyta atitikties užtikrinimo prezumpcija turėtų galioti tik jei kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotos ilgalaikio išsaugojimo paslaugos 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, taip pat galimybė ilgainiui patikrinti parašų ir spaudų kvalifikacijos statusą ir techninį galiojimą;

(3) 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;

(4) Komisija reguliariai vertina naujas technologijas, praktiką, standartus ar technines specifikacijas. Pagal Europos Parlamento ir Tarybos reglamento (ES) 2024/1183 ([2]) 75 konstatuojamąją dalį, Komisija turėtų šį reglamentą peržiūrėti ir prireikus atnaujinti, kad jis atitiktų pasaulinius pokyčius, naujas technologijas, standartus arba technines specifikacijas ir atitiktų geriausią vidaus rinkos praktiką;

([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).

(5) asmens duomenų tvarkymo pagal šį reglamentą veiklai taikomas Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ([3]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([4]);

(6) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([5]) 42 straipsnio 1 dalimi, konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2025 m. birželio 6 d.;

(7) šiame reglamente nustatytos 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 34 straipsnio 2 dalyje ir 40 straipsnyje nurodyti referenciniai standartai ir specifikacijos nustatyti 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. rugsėjo 29 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]) 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).

PRIEDAS

2 straipsnyje nurodytas referencinių standartų ir specifikacijų sąrašas

Standartai ETSI TS 119 511 V1.1.1 (2019-06) (ETSI TS 119 511) ir ETSI TS 119 172-4 V1.1.1 (2021-05) (ETSI TS 119 172-4) taikomi adaptuoti taip:

1. standartas ETSI TS 119 511:

1) 2.1. Norminės nuorodos:

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektroniniai parašai ir infrastruktūros (ESI). Bendrieji politikos reikalavimai patikimumo užtikrinimo paslaugų teikėjams“,

— [2] ETSI TS 119 612 (V2.3.1) „Elektroniniai parašai ir infrastruktūros (EPI). Patikimi sąrašai“,

— [5] FIPS PUB 140-3 (2019) „Šifravimo modulių saugumo reikalavimai“,

— [6] Komisijos įgyvendinimo reglamentas (ES) 2024/482 ([1]), kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo,

— [7] Komisijos įgyvendinimo reglamentas (ES) 2024/3144 ([2]), kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/482 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas,

— [8] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (*Agreed Cryptographic Mechanisms*) ([3]), paskelbė Europos Sąjungos kibernetinio saugumo agentūra (ENISA),

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Elektroniniai parašai ir infrastruktūros (ESI). parašų politika“, 4 dalis „Parašo taikomumo taisyklės (patvirtinimo politika), taikomos Europos kvalifikuotiems elektroniniams parašams arba spaudams, grindžiamiems patikimais parašais“,

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

2) 3.1. Terminai

— saugus šifravimo įrenginys – naudotojo privačiajam raktui laikyti ir saugoti nuo pažeidimo skirtas įrenginys, kuriuo naudotojo vardu atliekamos pasirašymo arba iššifravimo funkcijos;

3) 6.4. Apsaugos profiliai

— OVR-6.4-08A [WTS][WOS]. Numatytoji įrodymo galiojimo trukmė turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— 3 PASTABA negalioja;

4) 6.5. Apsaugos įrodymų politika

— OVR-6.5-04A. Naudojami šifravimo algoritmai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— 1 PASTABA negalioja;

([1]) OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) OL L, 2024/3144, 2024 12 19, 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. Žmogiškieji ištekliai

— OVR-7.2-02. Pasitikėjimo funkcijas vykdantys apsaugos paslaugų teikėjo darbuotojai ir, jei taikytina, pasitikėjimo funkcijas vykdantys samdomi rangovai turi būti pajėgūs įvykdyti reikalavimą turėti būtinas ekspertines žinias, patirtį ir kvalifikaciją, įgytą baigus oficialų mokymą ir patvirtintą pažymėjimais, ir (arba) praktinę patirtį,

— OVR-7.2-03. Kad būtų užtikrinta atitiktis OVR-7.2-02 punktui, reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinius saugumo užtikrinimo metodus;

6) 7.5. Šifravimo kontrolės priemonės

— OVR-7.5-05 [SU SĄLYGA]. Kai apsaugos paslaugų teikėjas pasirašo apsaugos įrodymą (jo dalį), apsaugos paslaugų teikėjo privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

a) standarte ISO/IEC 15408 [10] 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 [6][7] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

c) 3-čiojo lygio FIPS PUB 140-3 [5], 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) [6][7] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— OVR-7.5-06 [SU SĄLYGA] negalioja,

— OVR-7.5-07 [SU SĄLYGA]. Kai apsaugos paslaugų teikėjas pasirašo apsaugos įrodymą (jo dalį), visos atsarginės apsaugos paslaugų teikėjo privačiojo pasirašymo rakto kopijos turi būti apsaugotos naudojant saugų šifravimo įrenginį, kad tų kopijų vientisumas ir konfidencialumas būtų užtikrintas pirmiau nei jos bus laikomos už to įrenginio ribų;

— OVR-7.5-08. Apsaugos paslaugų teikėjo privatusis pasirašymo raktas į kitą saugų šifravimo įrenginį eksportuojamas arba importuojamas tik jei toks eksportas ir importas organizuotas saugiai ir suderintai su tokių įrenginių sertifikavimu;

7) 7.8. Tinklo saugumas

— OVR-7.8-03. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— OVR-7.8-04. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— OVR-7.8-05. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia apsaugos paslaugų teikėjo veikimui;

8) 7.14. Šifravimo stebėjimo priemonės

— OVR-7.14-03A. OVR-7.14.01 ir OVR-7.14.02 punktuose nurodytų šifravimo algoritmų vertinimas turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

9) 7.12. Patikimumo užtikrinimo paslaugų teikėjo veiklos nutraukimas ir veiklos nutraukimo planai

— OVR-7.12-01A. Laiko žymų tarnybos veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.2] 24 straipsnio 5 dalį, reikalavimus;

10) 7.17. Tiekimo grandinė

— OVR-7.17-01. Taikomi standarto ETSI EN 319 401 [1] 7.14 punkte nustatyti reikalavimai;

11) A priedas (norminis). Kvalifikuotų elektroninių parašų kvalifikuota ilgalaikės apsaugos paslauga, kaip nustatyta Reglamento (ES) Nr. 910/2014 34 straipsnyje

— OVR-A-02 [PDS][PDS+PGD]:

a) teikiant apsaugos paslaugą saugoma visa informacija, kurios reikia siekiant patikrinti elektroninio parašo arba spaudo kvalifikacijos statusą, jei tokia informacija nebūtų viešai prieinama, kol nepasibaigęs saugojimo laikotarpis,

b) apsaugos paslauga užtikrina, kad bet kada per saugojimo laikotarpį taip išsaugota informacija būtų tokia, kad ją kaip įvestį pateikus standarto ETSI TS 119 172-4 [9] 4.4 punkte nurodytam procesui, tokio proceso rezultatas aiškiai parodytų, ar skaitmeninis parašas arba spaudas jo saugojimo metu buvo (nebuvo) techniškai tinkamas ES kvalifikuotam elektroniniam parašui arba ES kvalifikuotam elektroniniam spaudui įgyvendinti;

— OVR-A-03 [PDS][PDS+PGD]. Apsaugos įrodyme naudojamos laiko žymos turi būti kvalifikuotos laiko žymos, kaip nustatyta Reglamente (ES) Nr. 910/2014 [i.2];

2. standartas ETSI TS 119 172-4:

1) 2.1. Norminės nuorodos:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). AdES skaitmeninių parašų kūrimo ir patvirtinimo procedūros“, 1 dalis „Kūrimas ir patvirtinimas“,

— visos nuorodos į standartą ETSI TS 119 102-1 [1] laikomos nuorodomis į standartą ETSI EN 319 102-1 [1],

— [2] ETSI TS 119 612 (V2.3.1) „Elektroniniai parašai ir infrastruktūros (EPI). Patikimi sąrašai“,

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Parašo kūrimo ir parašo patvirtinimo prietaikų politikos ir saugumo reikalavimai“;

2) 4.2. Patvirtinimo apribojimai ir patvirtinimo procedūros, REQ-4.2-03 reikalavimo X.509 skirsnio (*Validation constraints*) c punktas:

— i) jei galutinio subjekto sertifikatas yra patikimumo užtikrinimo priemonė, požymis *RevocationChecking-Constraints* nenaudojamas,

— ii) jei galutinio subjekto sertifikatas nėra patikimumo užtikrinimo priemonė, standarto ETSI TS 119 172-1 [3] A.4.2.1 punkto A.2 lentelės (m) eilutės 2.1 punkte apibrėžto požymio *RevocationChecking-Constraints* reikšmė turi būti *eitherCheck*,

— iii) jei galutinio subjekto sertifikatas yra patikimumo užtikrinimo priemonė, standarto ETSI TS 119 172-1 [3] A.4.2.1 punkto A.2 lentelės (m) eilutės 2.2 punkte apibrėžtas požymis *RevocationFreshness-Constraints* nenaudojamas,

— iv) jei galutinio subjekto sertifikatas nėra patikimumo užtikrinimo priemonė, standarto ETSI TS 119 172-1 [3] A.4.2.1 punkto A.2 lentelės (m) eilutės 2.2 punkte apibrėžto požymio *RevocationFreshness-Constraints*, skirto pasirašymo sertifikatui, didžiausioji reikšmė yra 0, užtikrinus, kad atšaukimo informacija būtų priimama tik jeigu ji pateikta po „patikimiausio laiko parašui patikrinti“. Požymio *RevocationFreshnessConstraints* vertė nustatoma tik pasirašymo sertifikatams ir jokiems kitiems sertifikatams, be kitų, laiko žymai pritaikytiems sertifikatams;

3) 4.3. Parašo patvirtinimo ir taikomumo taisyklių tikrinimo praktikos reikalavimai

— REQ-4.3-02. Parašo patvirtinimo prietaikos turi atitikti standartą ETSI TS 119 101 [13];

4) 4.4. Techninio taikomumo (taisyklių) tikrinimo procesas

— REQ-4.4.2-03. Jei bet kurio iš REQ-4.4.2-01 punkte nustatyto tikrinimo rezultatas neigiamas:

— procesas sustoja,

— parašas laikomas techniškai neapibrėžtu, t. y. nelaikomas nei ES kvalifikuotu elektroniniu parašu, nei ES kvalifikuotu elektroniniu spaudu,

— toks rezultatas ir visų tarpinių procesų rezultatai įrašomi į parašo taikomumo (taisyklių) tikrinimo ataskaitą.