Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1929

2025 9 30

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1929

2025 m. rugsėjo 29 d.

kuriuo dėl datos ir laiko susiejimo su duomenimis ir dėl laiko šaltinių tikslumo suderinimo, būtinų kvalifikuotai elektroninei laiko žymai suteikti, 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 42 straipsnio 2 dalį,

kadangi:

(1) kvalifikuotų elektroninių laiko žymų funkcijos elektroninėje erdvėje labai svarbios, nes jomis skatinama pereiti nuo įprastų popieriniais dokumentais grindžiamų procesų prie lygiaverčių elektroninių alternatyvų. Elektroninius duomenis su data ir laiku susiejančios kvalifikuotos elektroninės laiko žymos padeda garantuoti jose įrašytos datos ir laiko tikslumą ir skaitmeninių dokumentų, su kuriais susieta data ir laikas, vientisumą;

(2) Reglamento (ES) Nr. 910/2014 42 straipsnio 1a dalyje numatyta atitikties užtikrinimo prezumpcija turėtų galioti tik jei kvalifikuotos patikimumo užtikrinimo paslaugos, kurias teikiant išduodamos kvalifikuotos elektroninės laiko žymos, atitinka šiame reglamente nustatytus standartus. Šie standartai turėtų atitikti nusistovėjusią praktiką ir būti plačiai pripažįstami atitinkamuose sektoriuose. Šie standartai turėtų būti pritaikyti taip, kad apimtų papildomas kontrolės priemones, kuriomis garantuojamas kvalifikuotos patikimumo užtikrinimo paslaugos, taip pat datos ir laiko susiejimo su duomenimis saugumas ir patikimumas ir laiko šaltinio tikslumas;

(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 įgyvendinimo reglamentą peržiūrėti ir prireikus atnaujinti, kad jis atitiktų pasaulinius pokyčius, naujas technologijas, standartus arba technines specifikacijas ir atitiktų geriausią vidaus rinkos praktiką;

(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]);

([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).

([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.

(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

Reglamento (ES) Nr. 910/2014 42 straipsnio 2 dalyje nurodyti referenciniai standartai ir specifikacijos nustatyti šio reglamento priede.

2 straipsnis

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

([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

Kvalifikuotos laiko žymos paslaugoms taikomų referencinių standartų sąrašas

Standartai ETSI EN 319 421 V1.3.1 ([1]) (ETSI EN 319 421) ir ETSI EN 319 422 V1.1.1 ([2]) (ETSI EN 319 422) taikomi adaptuoti taip:

1. standartas ETSI EN 319 421:

1) 2.1. Norminės nuorodos

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) „Elektroniniai parašai ir infrastruktūros (ESI). Laiko žymos įterpimo protokolas ir laiko žymos atpažinties ženklo profiliai“,

— [6] negalioja,

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

— [10] 2024 m. sausio 31 d. Komisijos įgyvendinimo reglamentas (ES) 2024/482, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo ([4]),

— [11] 2024 m. gruodžio 18 d. Komisijos įgyvendinimo reglamentas (ES) 2024/3144, kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/482 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas ([5]);

2) 3.1. Terminai

— sertifikato galiojimo laikotarpis – laikotarpis imtinai nuo *notBefore* iki *notAfter*, kuriuo sertifikavimo institucija garantuoja laikysianti informaciją apie sertifikato statusą;

3) 3.3. Santrumpos

— EKSSS – bendraisiais kriterijais grindžiama Europos kibernetinio saugumo sertifikavimo schema;

4) 6.2. Patikimumo užtikrinimo paslaugų praktikos pareiškimas

— OVR-6.2-03. Į savo pareiškimą dėl laiko žymų tarnybos informacijos atskleidimo laiko žymų tarnyba įtraukia teiginius apie savo laiko žymėjimo paslaugos prieinamumą;

5) 7.3. Personalo patikimumas

— OVR-7.3-02. Pasitikėjimo funkcijas vykdantys laiko žymų tarnybos 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-7.3-03. Kad būtų užtikrinta atitiktis OVR-7.3-02 punktui, reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinius saugumo užtikrinimo metodus;

([1]) EN 319 421„Elektroniniai parašai ir infrastruktūros (ESI). Politikos ir saugumo reikalavimai, keliami laiko žymas išduodantiems patikimumo užtikrinimo paslaugų teikėjams“, V1.3.1.
([2]) EN 319 422 „Elektroniniai parašai ir infrastruktūros (ESI). Laiko žymos įterpimo protokolas ir laiko žymos atpažinties ženklo profiliai“, 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]) OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) OL L, 2024/3144, 2024 12 19, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2. Laiko žymos padalinio rakto generavimas

— TIS-7.6.2-03. Laiko žymos padalinio raktas (-ai) generuojamas (-i) saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

a) standarte ISO/IEC 15408 [3] 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 [10][11] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

c) 3-čiojo lygio FIPS PUB 140-3 [7], 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 [10][11] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— TIS-7.6.2-04 negalioja,

— 3 PASTABA negalioja,

— TIS-7.6.2-05A. Laiko žymos padalinio rakto generavimo algoritmas, gautas pasirašymo rakto ilgis ir parašo algoritmas, naudojami atitinkamai laiko žymoms pasirašyti ir laiko žymos padalinio viešojo rakto sertifikatams pasirašyti, turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė [9] ir paskelbė ENISA,

— 4 PASTABA negalioja,

— TIS-7.6.2-06. Laiko žymos padalinio 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) 7.6.3. Laiko žymos padalinio privačiojo rakto apsauga

— TIS-7.6.3-02. Laiko žymos padalinio privatusis raktas laikomas ir naudojamas saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

a) standarte ISO/IEC 15408 [3] arba Bendrųjų IT saugumo srities kriterijų sertifikatų pripažinimo susitarimo dalyvių paskelbtuose Bendruosiuose informacinių technologijų saugumo vertinimo kriterijuose (redakcija CC:2002, 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 [10][11] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

c) 3-čiojo lygio FIPS PUB 140-3 [7], 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 [10][11] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— TIS-7.6.3-03 negalioja,

— 2 PASTABA negalioja;

8) 7.6.7. Laiko žymos padalinio rakto gyvavimo ciklo pabaiga

— TIS-7.6.7-03A. Laiko žymos padalinio privačiųjų raktų galiojimo pabaigos data turi atitikti „Suderintuosius šifravimo mechanizmus“ [9],

— 1 PASTABA negalioja;

9) 7.10. Tinklo saugumas

— OVR-7.10-05. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— OVR-7.10-06. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— OVR-7.10-07. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia laiko žymų tarnybos veikimui;

10) 7.14. Laiko žymų tarnybos veiklos nutraukimas ir veiklos nutraukimo planai

— OVR-7.14-01A. Laiko žymų tarnybos veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.4] 24 straipsnio 5 dalį, reikalavimus;

2. standartas ETSI EN 319 422:

1) 2.1. Norminės nuorodos

— [5] negalioja,

— [6] negalioja,

— [8] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“,

— [9] RFC 9110 HTTP semantika;

2) 4.1.3. Naudotini maišos algoritmai

— Taikoma ši nuostata:

informacijai, kuriai turi būti priskirta laiko žyma, maišyti naudojami maišos algoritmai, numatoma laiko žymos galiojimo trukmė ir pasirinktos maišos funkcijos laikui bėgant turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

3) 4.2.3. Tinkami algoritmai

— Taikoma ši nuostata:

tinkami laiko žymos atpažinties ženklo parašo algoritmai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

4) 4.2.4. Tinkami rakto ilgiai

— Taikoma ši nuostata:

pasirinktojo parašo algoritmo parašo algoritmo rakto ilgiai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriuos patvirtino Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA,

— PASTABA negalioja;

5) 5.1.3. Tinkami algoritmai

— Taikoma ši nuostata:

tinkami laiko žymai naudojami maišos algoritmai, numatoma laiko žymos galiojimo trukmė ir pasirinktos maišos laiko atžvilgiu funkcijos turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

6) 5.2.3. Naudotini algoritmai

— Taikoma ši nuostata:

informacijai, kuriai turi būti priskirta laiko žyma, maišyti naudojami maišos algoritmai ir laiko žymos atpažinties ženklo parašo algoritmai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

7) 6.3. Rakto ilgio reikalavimai

— Taikoma ši nuostata:

laiko žymos padalinio pasirinktajam parašo algoritmui taikomas rakto ilgis turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

8) 6.5. Algoritmų reikalavimai

— Taikoma ši nuostata:

laiko žymos padalinio viešajam raktui ir laiko žymos padalinio sertifikato parašui naudojami algoritmai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8],

— PASTABA negalioja;

9) 7. Tinkamų persiuntimo protokolų profiliai

— Laiko žymos įterpimo klientas ir laiko žymos įterpimo serveris turi būti pajėgūs veikti laiko žymos įterpimo protokolu per HTTPS [9], kaip nustatyta standarto IETF RFC 3161 [1] 3.4 punkte;

10) 8. Objekto identifikatorius ir šifravimo algoritmai

— Taikoma ši nuostata:

laiko žymos padalinio viešajam raktui ir laiko žymos padalinio sertifikato parašui naudojami algoritmai turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8];

11) 9.1. Atitikties reglamentui deklaracija

— Jei laiko žymų tarnyba deklaruoja laiko žymos atpažinties ženklą kaip kvalifikuotą elektroninę laiko žymą, atitinkančią Reglamentą (ES) Nr. 910/2014 [i.2], jos laiko žymos plėtinio lauke, kurio sintaksė tokia, kaip nustatyta standarto ETF RFC 3739 [i.3] 3.2.6 punkte, turi būti vienas plėtinio *qcStatements* egzempliorius,

— plėtinyje *qcStatements* turi būti vienas B priede apibrėžto sakinio *esi4-qtstStatement-1* egzempliorius,

— plėtinys *qcStatements* neturi būti žymimas kaip kritinis.