Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1943

2025 9 30

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1943

2025 m. rugsėjo 29 d.

kuriuo dėl referencinių standartų, taikomų kvalifikuotiems elektroninių parašų sertifikatams ir kvalifikuotiems elektroninių spaudų sertifikatams, 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 28 straipsnio 6 dalį ir 38 straipsnio 6 dalį,

kadangi:

(1) kvalifikuotų elektroninių parašų sertifikatų ir kvalifikuotų elektroninių spaudų sertifikatų funkcijos elektroninėje verslo erdvėje labai svarbios, nes jais skatinama pereiti nuo įprastų popieriniais dokumentais grindžiamų procesų prie lygiaverčių elektroninių alternatyvų. Elektroninio parašo patvirtinimo duomenis arba elektroninio spaudo patvirtinimo duomenis kvalifikuotais sertifikatais susiejus su atitinkamai fiziniu arba juridiniu asmeniu ir patvirtinus tokių asmenų vardus ir pavardes arba pavadinimus, atsiranda daugiau tikrumo dėl pasirašančio asmens arba spaudo kūrėjo tapatybės;

(2) Reglamento (ES) Nr. 910/2014 28 straipsnio 6 dalyje ir 38 straipsnio 6 dalyje numatyta atitikties užtikrinimo prezumpcija turėtų galioti tik jei kvalifikuotos patikimumo užtikrinimo paslaugos, skirtos kvalifikuotiems elektroninių parašų sertifikatams išduoti, ir kvalifikuotos patikimumo užtikrinimo paslaugos, skirtos kvalifikuotiems elektroninių parašų sertifikatams išduoti, 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 kvalifikuotų patikimumo užtikrinimo paslaugų, taip pat kvalifikuotų sertifikatų turinio saugumas ir patikimumas;

(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;

(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

Referenciniai standartai ir specifikacijos, taikomi kvalifikuotiems elektroninių parašų ir elektroninių spaudų sertifikatams

1. Reglamento (ES) Nr. 910/2014 28 straipsnio 6 dalyje nurodyti referenciniai standartai ir specifikacijos nustatyti šio reglamento I priede.

2. Reglamento (ES) Nr. 910/2014 38 straipsnio 6 dalyje nurodyti referenciniai standartai ir specifikacijos nustatyti šio reglamento II 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

([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).

I PRIEDAS

Kvalifikuotiems elektroninių parašų sertifikatams taikomų referencinių standartų sąrašas

Standartai ETSI EN 319 411-2 V2.6.1 (ETSI EN 319 411-2), ETSI EN 319 412-1 V1.6.1 (ETSI EN 319 412-1), ETSI EN 319 412-2 V2.4.1 (ETSI EN 319 412-2) ir ETSI EN 319 412-5 V2.5.1 (ETSI EN 319 412-5) taikomi adaptuoti taip:

1. Standartas ETSI EN 319 411-2:

1) 2.1. Norminės nuorodos

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Politikos ir saugumo reikalavimai, keliami sertifikatus išduodantiems patikimumo užtikrinimo paslaugų teikėjams“, 1 dalis „Bendrieji reikalavimai“, adaptuotas taip:

standarto ETSI EN 319 411-1 V1.5.1 2.1 punktas „Norminės nuorodos“ su šiais pakeitimais:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 2 dalis „Sertifikatų profiliai fiziniams asmenims išduodamiems sertifikatams“,

— [14] ETSI EN 319 412-1 V1.6.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 1 dalis „Apžvalga ir bendros duomenų struktūros“,

— [3] ETSI EN 319 412-5 V2.5.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 5 dalis „Kvalifikuoto sertifikato plėtinys *QCStatements*“,

— [5] ETSI EN 319 412-1 V1.6.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 1 dalis „Apžvalga ir bendros duomenų struktūros“,

— [6] CEN/TS 419261:2015 „Saugumo reikalavimai, keliami patikimoms sertifikatų ir laiko žymų valdymo sistemoms“,

— [7] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (*Agreed Cryptographic Mechanisms*) [1], paskelbė Europos Sąjungos kibernetinio saugumo agentūra (ENISA),

— [8] Komisijos įgyvendinimo reglamentas (ES) 2024/482 [2], kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo,

— [9] Komisijos įgyvendinimo reglamentas (ES) 2024/3144 [3], kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/482 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas,

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

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

[1] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
[2] OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
[3] OL L, 2024/3144, 2024 12 19, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 5.2. Sertifikavimo praktikos pareiškimo reikalavimai

— OVR-5.2-02. Patikimumo užtikrinimo paslaugų teikėjo dokumentuose nurodytoje sertifikatų politikoje turi būti paaiškinta, kokie reikalavimai keliami naudotiniems sertifikato profiliams;

3) 5.3. Sertifikatų politikos pavadinimas ir identifikavimas

— OVR-5.3-01. Sertifikatų politikos identifikatorius turi būti pakeistas, jei 4.2.2 punkte aprašytoje sertifikatų politikoje padaroma pakeitimų, nuo kurių priklauso taikymas;

4) 6.1. Paskelbimo ir saugyklos pareigos

— OVR-6.1-02. Prie numerio [2] nurodyto standarto ETSI EN 319 411-1 punkte DIS-6.1-04 nustatyta informacija skelbiama viešai ir tarptautiniu mastu;

5) 6.2.2. Pirminis tapatybės patvirtinimas

— REG-6.2.2-01A. Subjekto tapatybės požymių ir įrodymų rinkimas, taip pat jų patvirtinimas vykdomi taip, kaip nustatyta pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 1c dalį priimtuose įgyvendinimo aktuose,

— REG-6.2.2-02. [QCP-n] ir [QCP-n-qscd]. Fizinio asmens tapatybė ir, kai taikytina, visi konkretūs asmens požymiai tikrinami taip, kaip nustatyta pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 1c dalį priimtuose įgyvendinimo aktuose,

— 1 PASTABA negalioja;

6) 6.3.3. Sertifikatų išdavimas

— GEN-6.3.3-01. Taikomi standarto ETSI EN 319 411-1 [2] punkte 6.3.3 nustatyti reikalavimai GEN-6.3.3-01–GEN-6.3.3-10,

— GEN-6.3.3-02 [SU SĄLYGA]. Jei pažymėjimas išduodamas fiziniam asmeniui, identifikuotam drauge su juridiniu asmeniu, į sertifikatą įtraukti organizaciją identifikuojantys subjekto požymiai reiškia juridinį asmenį arba to juridinio asmens padalinį, o į sertifikatą įtrauktas subjekto identifikatorius – fizinį asmenį,

— GEN-6.3.3-03. Sertifikatų politikos identifikatorius yra [PASIRINKTI]:

a) [QCP-n]

— kaip nustatyta 5.3 punkto a papunktyje ir (arba)

— organizacijos identifikacinis numeris (OID), kurį paskyrė patikimumo užtikrinimo paslaugų teikėjas arba kitas susijęs suinteresuotasis subjektas, arba tolesnis sertifikatų politikos standartizavimas, kuriuo tobulinami šiame dokumente apibrėžti atitinkami taikytini politikos reikalavimai;

b) [QCP-n-qscd]

— kaip nustatyta 5.3 punkto c papunktyje ir (arba)

— organizacijos identifikacinis numeris (OID), kurį paskyrė patikimumo užtikrinimo paslaugų teikėjas arba kitas susijęs suinteresuotasis subjektas, arba tolesnis sertifikatų politikos standartizavimas, kuriuo tobulinami šiame dokumente apibrėžti atitinkami taikytini politikos reikalavimai;

7) 6.3.5. Raktų pora ir sertifikatų naudojimas

— SDP-6.3.5-02A [SU SĄLYGA]. Jei subjekto kvalifikuoto elektroninio parašo kūrimo įtaisą (QSCD) valdo patikimumo užtikrinimo paslaugų teikėjas, pagal Reglamentą (ES) Nr. 910/2014 [i.1] toks teikėjas turi būti kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis kvalifikuotą patikimumo užtikrinimo paslaugą nuotoliniam kvalifikuotam parašo kūrimo įtaisui valdyti,

— SDP-6.3.5-11A. Jei naudotojo raktus sugeneruoja naudotojas arba subjektas, naudotojo pareigos (žr. 6.3.4 punktą) turi apimti:

a) pareigą subjekto raktus sugeneruoti naudojantis algoritmu, atitinkančiu Europos kibernetinio saugumo sertifikavimo grupės patvirtintus [7] ir ENISA paskelbtus suderintuosius šifravimo mechanizmus, kad sertifikuotas raktas būtų naudojamas pagal sertifikatų politiką;

b) pareigą naudoti rakto ilgį ir algoritmą, atitinkančius Europos kibernetinio saugumo sertifikavimo grupės patvirtintus [7] ir ENISA paskelbtus suderintuosius šifravimo mechanizmus, kad sertifikuotas raktas, kol galioja sertifikatas, būtų naudojamas pagal sertifikatų politiką;

8) 6.3.10 Sertifikato būsenos paslaugos

— CSS-6.3.10-08 [SU SĄLYGA]. Jei pateikiami sertifikatų atšaukimo sąrašai, patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti naujausio sertifikatų atšaukimo sąrašo vientisumą ir prieinamumą bent laikotarpį, nustatytą sertifikavimo praktikos pareiškime, kaip to reikalaujama CSS-6.3.10-12;

9) 6.4.4. Darbuotojų kontrolės priemonės

— OVR-6.4.4-02. Pasitikėjimo funkcijas vykdantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai ir, jei taikytina, pasitikėjimo funkcijas vykdantys samdomi rangovai turi būti pajėgūs įvykdyti reikalavimą turėti būtinas ekspertines žinias, patirtį ir kvalifikaciją, įgytas baigus oficialų mokymą ir patvirtintas pažymėjimais, ir (arba) praktinę patirtį,

— OVR-6.4.4-03. Kad būtų užtikrinta atitiktis OVR-6.4.4-02 punktui, reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinius saugumo užtikrinimo metodus,

— OVR-6.4.4-04. Be pasitikėjimo funkcijų, nustatytų standarte ETSI EN 319 401 [1] (7.2-15 punkte), turi būti palaikomos ir registravimo ir atšaukimo tarnautojų, vykdančių standarte TS 419261 [6] apibrėžtas pareigas, pasitikėjimo funkcijos. Jei kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas yra tiesiogiai administruojamas arba valdomas valstybės narės arba viešojo sektoriaus institucijos vardu, tokias papildomas pasitikėjimo funkcijas gali atlikti vienas arba keli oficialūs atstovai, dirbantys vietos arba regiono administracijos registravimo arba atšaukimo tarnautojams arba tokių tarnautojų vardu;

10) 6.4.9. Veiklos nutraukimas, kurį vykdo sertifikavimo institucija arba registravimo institucija

— OVR-6.4.9-02. Patikimumo užtikrinimo paslaugų teikėjo veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 5 dalį, reikalavimus;

11) 6.5.1. Raktų poros generavimas ir įdiegimas

— OVR-6.5.1-01A. Sertifikavimo institucijos raktų pora sertifikavimo institucijos parašui sugeneruojama naudojantis algoritmu, atitinkančiu Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus,

— OVR-6.5.1-01B. Pasirinktas rakto ilgis ir sertifikavimo institucijos pasirašymo rakto, naudojamo sertifikavimo institucijos parašui, algoritmas turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus,

— OVR-6.5.1-01C [SU SĄLYGA]. Jei subjekto raktus generuoja sertifikavimo institucija, jos sugeneruoti raktai, naudojami sertifikatų politikoje nurodytais tikslais, kol galioja sertifikatas, turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus;

12) 6.5.2. Privačiojo rakto apsauga ir šifravimo modulio inžinerinė kontrolė

— GEN-6.5.2-01. Taikomi visi standarto ETSI EN 319 411-1 [2] 6.5.2 punkte nurodyti reikalavimai, išskyrus OVR-6.5.2-01, OVR-6.5.2-03 ir OVR-6.5.2-04 reikalavimus,

— GEN-6.5.2-02. Patikimumo užtikrinimo paslaugų teikėjo raktų pora, įskaitant atšaukimo ir registravimo paslaugoms naudojamus raktus, generuojama saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

— standarte ISO/IEC 15408 [10] 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

— bendraisiais kriterijais grindžiamą Europos kibernetinio saugumo sertifikavimo schemą [8][9] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

— 3-čiojo lygio FIPS PUB 140-3 [11], 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) [8][9] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— GEN-6.5.2-03. Sertifikavimo institucijos privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje, atitinkančiame GEN-6.5.2-01 ir GEN-6.5.2-02 reikalavimus;

13) 6.5.7. Tinklo saugumo kontrolės priemonės

— OVR-6.5.7-02. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— OVR-6.5.7-03. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— OVR-6.5.7-04. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia patikimumo užtikrinimo paslaugų teikėjo veiklai;

14) 6.6.1. Sertifikato profilis

— GEN-6.6.1-05. Sertifikate turi būti vienas iš politikos identifikatorių, nustatytų GEN-6.3.3-03 [PASIRINKTI]. Sertifikate gali būti kiti organizacijos identifikaciniai numeriai (OID), kuriuos priskyrė patikimumo užtikrinimo paslaugų teikėjas.

2. Standartas ETSI EN 319 412-2:

1) 2.1. Norminės nuorodos

— [2] ETSI EN 319 412-5 V2.5.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 5 dalis „Kvalifikuoto sertifikato plėtinys *QCStatements*“,

— [9] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis „Suderintieji šifravimo mechanizmai“, kuriuos paskelbė ENISA;

2) 4.2.2. Parašas

— GEN-4.2.2-2. Parašo algoritmas pasirenkamas pagal „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [9],

— PASTABA negalioja;

3) 4.2.3.1. Išdavėjai, kurie yra juridiniai asmenys

— GEN-4.2.3.1-3. Jei žinoma, kad yra atitinkamas registracijos numeris, į išdavėjo tapatybę turi būti įtrauktas požymis *organizationIdentifier*, kuriam priskirta vertė yra tas registracijos numeris, koks įrašytas į oficialų dokumentą, kuriuo nustatomas tas registracijos numeris;

4) 4.2.5. Informacija apie subjekto viešąjį raktą

— GEN-4.2.5-2. Subjekto viešasis raktas pasirenkamas pagal „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [9],

— PASTABA negalioja;

5) 4.2.6. Serijos numeris

— GEN-4.2.6-01. Sertifikato požymio *serialNumber* vertė (kaip nustatyta standarto IETF RFC 5280 [1] 4.1.2.2 punkte) turi būti unikali kiekviename patikimumo užtikrinimo paslaugų teikėjo išduotame sertifikate.

II PRIEDAS

Kvalifikuotiems elektroninių spaudų sertifikatams taikomų referencinių standartų sąrašas

Standartai ETSI EN 319 411-2 V2.6.1 (ETSI EN 319 411-2), ETSI EN 319 412-1 V1.6.1 (ETSI EN 319 412-1), ETSI EN 319 412-3 V1.3.1 (ETSI EN 319 412-3), ETSI EN 319 412-2 V2.4.1 (ETSI EN 319 412-2) ir ETSI EN 319 412-5 V2.5.1 (ETSI EN 319 412-5) taikomi adaptuoti taip:

1. Standartas ETSI EN 319 411-2:

1) 2.1. Norminės nuorodos

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Politikos ir saugumo reikalavimai, keliami sertifikatus išduodantiems patikimumo užtikrinimo paslaugų teikėjams“, 1 dalis „Bendrieji reikalavimai“, adaptuotas taip:

standarto ETSI EN 319 411-1 V1.5.1 2.1 punktas „Norminės nuorodos“ su šiais pakeitimais:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 2 dalis „Sertifikatų profiliai fiziniams asmenims išduodamiems sertifikatams“,

— [14] ETSI EN 319 412-1 V1.6.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 1 dalis „Apžvalga ir bendros duomenų struktūros“,

— [3] ETSI EN 319 412-5 V2.5.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 5 dalis „Kvalifikuoto sertifikato plėtinys *QCStatements*“,

— [5] ETSI EN 319 412-1 V1.6.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 1 dalis „Apžvalga ir bendros duomenų struktūros“,

— [6] CEN/TS 419261:2015 „Saugumo reikalavimai, keliami patikimoms sertifikatų ir laiko žymų valdymo sistemoms“ (parengė CEN),

— [7] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (parengė ENISA),

— [8] 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,

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

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

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

2) 5.2. Sertifikavimo praktikos pareiškimo reikalavimai

— OVR-5.2-02. Patikimumo užtikrinimo paslaugų teikėjo dokumentuose nurodytoje sertifikatų politikoje turi būti paaiškinta, kokie reikalavimai keliami naudotiniems sertifikato profiliams;

3) 5.3. Sertifikatų politikos pavadinimas ir identifikavimas

— OVR-5.3-01. Sertifikatų politikos identifikatorius turi būti pakeistas, jei 4.2.2 punkte aprašytoje sertifikatų politikoje padaroma pakeitimų, nuo kurių priklauso taikymas;

4) 6.1. Paskelbimo ir saugyklos pareigos

— OVR-6.1-02. Prie numerio [2] nurodyto standarto ETSI EN 319 411-1 punkte DIS-6.1-04 nustatyta informacija skelbiama viešai ir tarptautiniu mastu;

5) 6.2.2. Pirminis tapatybės patvirtinimas

— REG-6.2.2-01A. Subjekto tapatybės požymių ir įrodymų rinkimas, taip pat jų patvirtinimas vykdomi taip, kaip nustatyta pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 1c dalį priimtuose įgyvendinimo aktuose,

— REG-6.2.2-03 [QCP-l] ir [QCP-l-qscd]. Juridinio asmens tapatybė ir, kai taikytina, visi konkretūs asmens požymiai tikrinami taip, kaip nustatyta pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 1c dalį priimtuose įgyvendinimo aktuose,

— 3 PASTABA. Žr. 2 pastabą;

6) 6.3.3. Sertifikatų išdavimas

— GEN-6.3.3-01. Taikomi standarto ETSI EN 319 411-1 [2] punkte 6.3.3 nustatyti reikalavimai GEN-6.3.3-01–GEN-6.3.3-10,

— GEN-6.3.3-02. Sertifikatų politikos identifikatorius yra [PASIRINKTI]:

a) [QCP-l]

— kaip nustatyta 5.3 punkto b papunktyje ir (arba)

— organizacijos identifikacinis numeris (OID), kurį paskyrė patikimumo užtikrinimo paslaugų teikėjas arba kitas susijęs suinteresuotasis subjektas, arba tolesnis sertifikatų politikos standartizavimas, kuriuo tobulinami šiame dokumente apibrėžti atitinkami taikytini politikos reikalavimai;

b) [QCP-l-qscd]

— kaip nustatyta 5.3 punkto d papunktyje ir (arba)

— organizacijos identifikacinis numeris (OID), kurį paskyrė patikimumo užtikrinimo paslaugų teikėjas arba kitas susijęs suinteresuotasis subjektas, arba tolesnis sertifikatų politikos standartizavimas, kuriuo tobulinami šiame dokumente apibrėžti taikytini politikos reikalavimai;

7) 6.3.5. Raktų pora ir sertifikatų naudojimas

— SDP-6.3.5-02A [SU SĄLYGA]. Jei subjekto kvalifikuoto elektroninio parašo kūrimo įtaisą (QSCD) valdo patikimumo užtikrinimo paslaugų teikėjas, pagal Reglamentą (ES) Nr. 910/2014 [i.1] toks teikėjas turi būti kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis kvalifikuotą patikimumo užtikrinimo paslaugą nuotoliniam kvalifikuotam spaudo kūrimo įtaisui valdyti,

— SDP-6.3.5-11A. Jei naudotojo raktus sugeneruoja naudotojas arba subjektas, naudotojo pareigos (žr. 6.3.4 punktą) turi apimti:

a) pareigą subjekto raktus sugeneruoti naudojantis algoritmu, atitinkančiu Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus, kad sertifikuotas raktas būtų naudojamas pagal sertifikatų politiką, ir

b) pareigą naudoti rakto ilgį ir algoritmą, atitinkančius Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus, kad sertifikuotas raktas, kol galioja sertifikatas, būtų naudojamas pagal sertifikatų politiką;

8) 6.3.10 Sertifikato būsenos paslaugos

— CSS-6.3.10-08 [SU SĄLYGA]. Jei pateikiami sertifikatų atšaukimo sąrašai, patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti naujausio sertifikatų atšaukimo sąrašo vientisumą ir prieinamumą bent laikotarpį, nustatytą sertifikavimo praktikos pareiškime, kaip to reikalaujama CSS-6.3.10-12;

9) 6.4.4. Darbuotojų kontrolės priemonės

— OVR-6.4.4-02. Pasitikėjimo funkcijas vykdantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai ir, jei taikytina, pasitikėjimo funkcijas vykdantys samdomi rangovai turi būti pajėgūs įvykdyti reikalavimą turėti būtinas ekspertines žinias, patirtį ir kvalifikaciją, įgytas baigus oficialų mokymą ir patvirtintas pažymėjimais, ir (arba) praktinę patirtį,

— OVR-6.4.4-03. Kad būtų užtikrinta atitiktis OVR-6.4.4-02 punktui, reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinius saugumo užtikrinimo metodus,

— OVR-6.4.4-04. Be pasitikėjimo funkcijų, nustatytų standarte ETSI EN 319 401 [1] (7.2-15 punkte), turi būti palaikomos ir registravimo ir atšaukimo tarnautojų, vykdančių standarte TS 419261 [6] apibrėžtas pareigas, pasitikėjimo funkcijos. Jei kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas yra tiesiogiai administruojamas arba valdomas valstybės narės arba viešojo sektoriaus institucijos vardu, tokias papildomas pasitikėjimo funkcijas gali atlikti vienas arba keli oficialūs atstovai, dirbantys vietos arba regiono administracijos registravimo arba atšaukimo tarnautojams arba tokių tarnautojų vardu;

10) 6.4.9. Veiklos nutraukimas, kurį vykdo sertifikavimo institucija arba registravimo institucija

— OVR-6.4.9-02. Patikimumo užtikrinimo paslaugų teikėjo veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 5 dalį, reikalavimus;

11) 6.5.1. Raktų poros generavimas ir įdiegimas

— OVR-6.5.1-01A. Sertifikavimo institucijos raktų pora sertifikavimo institucijos parašui sugeneruojama naudojantis algoritmu, atitinkančiu Europos kibernetinio saugumo sertifikavimo grupės patvirtintus, ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus,

— OVR-6.5.1-01B. Pasirinktas rakto ilgis ir sertifikavimo institucijos pasirašymo rakto, naudojamo sertifikavimo institucijos parašui, algoritmas turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus, ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus,

— OVR-6.5.1-01C [SU SĄLYGA]. Jei subjekto raktus generuoja sertifikavimo institucija, jos sugeneruoti raktai, naudojami sertifikatų politikoje nurodytais tikslais, kol galioja sertifikatas, turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA [7] paskelbtus suderintuosius šifravimo mechanizmus;

12) 6.5.2. Privačiojo rakto apsauga ir šifravimo modulio inžinerinė kontrolė

— GEN-6.5.2-01. Taikomi visi standarto ETSI EN 319 411-1 [2] 6.5.2 punkte nurodyti reikalavimai, išskyrus OVR-6.5.2-01, OVR-6.5.2-03 ir OVR-6.5.2-04 reikalavimus,

— GEN-6.5.2-02. Patikimumo užtikrinimo paslaugų teikėjo raktų pora, įskaitant atšaukimo ir registravimo paslaugoms naudojamus raktus, generuojama saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

  — standarte ISO/IEC 15408 [10] 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

  — bendraisiais kriterijais grindžiamą Europos kibernetinio saugumo sertifikavimo schemą [8][9] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

  — 3-čiojo lygio FIPS PUB 140-3 [11], 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) [8][9] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— GEN-6.5.2-03. Sertifikavimo institucijos privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje, atitinkančiame GEN-6.5.2-01 ir GEN-6.5.2-02 reikalavimus;

13) 6.5.7. Tinklo saugumo kontrolės priemonės

— OVR-6.5.7-02. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— OVR-6.5.7-03. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— OVR-6.5.7-04. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia patikimumo užtikrinimo paslaugų teikėjo veiklai;

14) 6.6.1. Sertifikato profilis

— GEN-6.6.1-05. Sertifikate turi būti vienas iš politikos identifikatorių, nustatytų GEN-6.3.3-02 [PASIRINKTI].

2. Standartas ETSI EN 319 412-3:

1) 2.1. Norminės nuorodos

— [2] ETSI EN 319 412-2 V2.4.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 2 dalis „Sertifikatų profiliai fiziniams asmenims išduodamiems sertifikatams“;

2) 4.2.1. Subjektas

— LEG-4.2.1-6. Į požymį *organizationIdentifier* turi būti įtraukta subjekto identifikacija, kuri skiriasi nuo organizacijos pavadinimo. Jei žinoma, kad yra atitinkamas registracijos numeris, į požymį *organizationIdentifier* turi būti įtraukta registracijos numerio, koks įrašytas į oficialų dokumentą, kuriuo nustatomas tas registracijos numeris, vertė;

3. Standartas ETSI EN 319 412-2:

1) 2.1. Norminės nuorodos

— [2] ETSI EN 319 412-5 V2.5.1 „Elektroniniai parašai ir patikimumo infrastruktūros (ESI). Sertifikato profiliai“, 5 dalis „Kvalifikuoto sertifikato plėtinys *QCStatements*“,

— [9] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (parengė ENISA);

2) 2.2. Informacinės nuorodos

— [i.7] negalioja;

3) 4.2.2. Parašas

— GEN-4.2.2-2. Parašo algoritmas pasirenkamas pagal „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [9],

— PASTABA negalioja;

4) 4.2.3.1. Išdavėjai, kurie yra juridiniai asmenys

— GEN-4.2.3.1-3. Jei žinoma, kad yra atitinkamas registracijos numeris, į išdavėjo tapatybę turi būti įtrauktas požymis *organizationIdentifier*, kuriam priskirta vertė yra tas registracijos numeris, koks įrašytas į oficialų dokumentą, kuriuo nustatomas tas registracijos numeris;

5) 4.2.5. Informacija apie subjekto viešąjį raktą

— GEN-4.2.5-2. Subjekto viešasis raktas pasirenkamas pagal „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [9],

— PASTABA negalioja;

6) 4.2.6. Serijos numeris

— GEN-4.2.6-01. Sertifikato požymio *serialNumber* vertė (kaip nustatyta standarto IETF RFC 5280 [1] 4.1.2.2 punkte) turi būti unikali kiekviename patikimumo užtikrinimo paslaugų teikėjo išduotame sertifikate.