Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1942

2025 9 30

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1942

2025 m. rugsėjo 29 d.

kuriuo dėl kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotų galiojimo patvirtinimo 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 33 straipsnio 2 dalį ir 40 straipsnį,

kadangi:

(1) kvalifikuotiems elektroniniams parašams ir kvalifikuotiems elektroniniams spaudams skirtos kvalifikuotos galiojimo patvirtinimo paslaugos užtikrina atitinkamai kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų procesų ir rezultatų vientisumą, autentiškumą, ir tikslumą. Tokių kvalifikuotų patikimumo užtikrinimo paslaugų funkcijos elektroninėje veiklos aplinkoje labai svarbios, nes jomis skatinama pereiti nuo įprastų popieriniais dokumentais grindžiamų procesų prie lygiaverčių elektroninių alternatyvų;

(2) Reglamento (ES) Nr. 910/2014 33 straipsnio 2 dalyje ir 40 straipsnyje numatyta atitikties užtikrinimo prezumpcija turėtų galioti tik jei kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotos galiojimo patvirtinimo paslaugos atitinka šiame reglamente nustatytus techninius standartus. Tie 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 saugumas ir patikimumas, taip pat galimybė patikrinti kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių 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 33 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

Kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotų galiojimo patvirtinimo paslaugų referencinių standartų ir specifikacijų sąrašas

Standartai ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (ETSI TS 119 441) ir ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (ETSI TS 119 172-4) yra taikomi adaptuoti taip:

1. standartas ETSI TS 119 441:

1) 2.1. Norminės nuorodos

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

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

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

— [4] ISO/IEC 15408-1:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. IT saugumo įvertinimo kriterijai“,

— [5] negalioja,

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

— [7] Komisijos įgyvendinimo reglamentas (ES) 2024/482 ([3]), kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2019/881 taikymo taisyklės dėl bendraisiais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EKSSS) priėmimo,

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

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Elektroniniai parašai ir infrastruktūros (EPI). AdES skaitmeninių parašų kūrimo ir patvirtinimo procedūros. 2 dalis. Parašo patvirtinimo ataskaita“,

— [10] Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Suderintieji šifravimo mechanizmai“ (*Agreed Cryptographic Mechanisms*) ([4]), paskelbė Europos Sąjungos kibernetinio saugumo agentūra (ENISA),

— [11] Komisijos įgyvendinimo reglamentas (ES) 2024/3144 ([5]), kuriuo iš dalies keičiamos Įgyvendinimo reglamento (ES) 2024/4822 nuostatos dėl taikytinų tarptautinių standartų ir tas reglamentas ištaisomas,

— [12] ETSI EN 319 411-1 „Elektroniniai parašai ir infrastruktūros (EPI). Politikos ir saugumo reikalavimai, keliami sertifikatus išduodantiems patikimumo užtikrinimo paslaugų teikėjams“, 1 dalis Bendrieji reikalavimai“;

([1]) ETSI TS 119 441 „Elektroniniai parašai ir infrastruktūros (ESI). Parašo patvirtinimo paslaugas teikiančiam patikimumo užtikrinimo paslaugų teikėjui keliami reikalavimai“, V1.2.1 (2023-10).

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

([3]) OL L, 2024/482, 2024 2 7, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([5]) OL L, 2024/3144, 2024 12 19, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2. Informacinės nuorodos

— [i.11] negalioja;

3) 3.3. Santrumpos

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

4) 4.3.3. Procesas

— 10 PASTABA. Daugiau patarimų apie ES kvalifikuoto parašo arba spaudo naudojimą pateikta standarte ETSI EN 319 102-1 [3] ir papildomai standarte ETSI TS 119 172-4 [8];

5) 6.1. Parašo patvirtinimo paslaugos praktikos pareiškimas

— OVR-6.1-02. Parašo patvirtinimo paslaugos praktikos pareiškimo sandara turi būti tokia, kaip nustatyta A priede,

— OVR-6.1-03. Parašo patvirtinimo paslaugos praktikos pareiškime turi būti išvardytos palaikomos parašo patvirtinimo paslaugos schemos (pvz., OID) arba daromos nuorodos į jas ir pateiktas trumas jų aprašymas;

6) 6.3. Informacijos saugumo politika

— OVR-6.3-02. Saugumo politikoje turi būti aprašytos asmens duomenims apsaugoti įdiegtos saugumo ir privatumo kontrolės priemonės;

7) 7.2. Žmogiškieji ištekliai

— OVR-7.2-02. Pasitikėjimo funkcijas vykdantys parašo patvirtinimo paslaugos 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;

8) 7.5. Šifravimo kontrolės priemonės

— OVR-7.5-02 [SU SĄLYGA]. Pasirašius patvirtinimo ataskaitas, patikima sertifikavimo institucija pagal normalizuotą sertifikatų politiką ir standarte ETSI EN 319 411-1 [12] nurodytą sertifikatų politiką išduoda parašo patvirtinimo paslaugos teikėjo viešąjį pasirašymo sertifikatą, atitinkantį parašo patvirtinimo paslaugos teikėjo privatųjį pasirašymo raktą. Jis turi būti išduodamas laikantis atitinkamos standarte ETSI EN 319 411-2 [i.17] nustatytos sertifikatų politikos,

— OVR-7.5-03 [SU SĄLYGA]. Pasirašius patvirtinimo ataskaitas, parašo patvirtinimo paslaugos teikėjo privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

a) standarte ISO/IEC 15408 [4] 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 [7][11] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

c) 3-čiojo lygio FIPS PUB 140-3 [6], 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) [7][11] sertifikatas, toks įrenginys turi būti sukonfigūruotas ir naudojamas pagal tą sertifikatą,

— OVR-7.5-04 negalioja,

— OVR-7.5-06. Parašo patvirtinimo paslaugos 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;

9) 7.7. Veiklos saugumas

— OVR-7.7-02. Siekiant užtikrinti, kad prietaikų kūrimo sistemose būtų taikomos tinkamos saugumo priemonės ir būtų prisitaikoma prie konkrečios prietaikos aplinkos, parašo patvirtinimo prietaikai naudojama taikomoji aplinka, prižiūrima įdiegiant naujausius saugumo spragų ištaisymus,

— OVR-7.7-03. Parašo patvirtinimo prietaikai keliami šie standarto ETSI TS 119 101 [1] 5.2 punkto reikalavimai: GSM 1.3;

10) 7.8. Tinklo saugumas

— OVR-7.8-02. Jei prie sistemų, kuriose saugomi arba apdorojami konfidencialūs duomenys, leidžiama nuotolinė prieiga, turi būti priimta oficiali politika ir ji turi būti aprašyta kaip OVR-6.3-02 punkte reikalaujamų elementų dalis,

— OVR-7.8-04. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— OVR-7.8-05. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— OVR-7.8-06. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia parašo patvirtinimo paslaugos teikėjo veiklai;

11) 7.12. Parašo patvirtinimo paslaugos teikimo nutraukimas ir veiklos nutraukimo planai

— OVR-7.12-02. 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;

12) 7.14. Tiekimo grandinė

— OVR-7.14-01. Taikomi standarto ETSI EN 319 401 [2] 7.14 punkte nustatyti reikalavimai.

13) 8.1. Parašo patvirtinimo procesas

— VPR-8.1-07. Parašo patvirtinimo prietaika turi atitikti standarto ETSI TS 119 101 [1] 7.4 punkto SIA 1–SIA 4 reikalavimus,

— VPR-8.1-11 [SU SĄLYGA]. Kai parašo patvirtinimo paslauga kvalifikuotus elektroninius parašus arba kvalifikuotus elektroninius spaudus turi patvirtinti pagal Reglamento (ES) Nr. 910/2014 [i.1] 32 straipsnio 1 dalį (arba atitinkamai pagal 40 straipsnį), patvirtinimo procesas turi atitikti standarto ETSI TS 119 172-4 [8] reikalavimus;

14) 8.2. Parašo patvirtinimo protokolas

— SVP-8.2-03. Atsake į parašo patvirtinimą turi būti parašo patvirtinimo paslaugos politikos organizacijos identifikacinis numeris (OID);

15) 8.4. Parašo patvirtinimo ataskaita

— SVR-8.4-02. Parašo patvirtinimo ataskaita turi atitikti standartą ETSI TS 119 102-2 [9],

— SVR-8.4-07 [SU SĄLYGA]. Jei parašo patvirtinimo paslauga apima ne visą parašo patvirtinimo politiką, į ataskaitą, be patvirtintų apribojimų, įtraukiami duomenys apie ignoruotus arba apeitus apribojimus,

— SVR-8.4-15. Parašo patvirtinimo ataskaitoje turi būti aiškiai nurodytas kiekvieno įrodymo (PoE) šaltinis (iš parašo, iš kliento, iš serverio),

— SVR-8.4-16. Parašo patvirtinimo ataskaitoje turi būti parašo patvirtinimo ataskaitos parašas – parašo patvirtinimo paslaugos teikėjo skaitmeninis parašas,

— SVR-8.4-17 [SU SĄLYGA]. Pasirašius parašo patvirtinimo ataskaitas, parašo formatas ir tikslas turi atitikti standartą ETSI TS 119 102-2 [9];

16) 9. Pagrindai, kuriais apibrėžiama parašo patvirtinimo paslaugos politika, parengta pagal šiame dokumente apibrėžtą patikimumo užtikrinimo paslaugų politiką

— OVR-9-05 [SU SĄLYGA]. Kuriant parašo patvirtinimo paslaugos politiką, grindžiamą šiame dokumente apibrėžta patikimumo užtikrinimo paslaugų politika, turi būti atliekamas rizikos vertinimas, kad būtų atsižvelgta į veiklos reikalavimus ir būtų nustatyti saugumo reikalavimai, kuriuos reikia įtraukti į minėtos bendruomenės ir taikomumo politiką,

— OVR-9-06 [SU SĄLYGA] Kuriant parašo patvirtinimo paslaugos politiką, grindžiamą šiame dokumente apibrėžta patikimumo užtikrinimo paslaugų politika, politika turi būti patvirtinama ir keičiama pagal nustatytą peržiūros procesą, įskaitant politikos administravimo pareigas,

— OVR-9-07 [SU SĄLYGA] Kuriant parašo patvirtinimo paslaugos politiką, grindžiamą šiame dokumente apibrėžta patikimumo užtikrinimo paslaugų politika, turi būti nustatytas peržiūros procesas siekiant užtikrinti, kad politika būtų grindžiama praktikos pareiškimais,

— OVR-9-08 [SU SĄLYGA] Kuriant parašo patvirtinimo paslaugos politiką, grindžiamą šiame dokumente apibrėžta patikimumo užtikrinimo paslaugų politika, patikimumo užtikrinimo paslaugų teikėjas turi savo naudotojų bendruomenę informuoti, kokią politiką palaiko,

— OVR-9-09 [SU SĄLYGA] Kuriant parašo patvirtinimo paslaugos politiką, grindžiamą šiame dokumente apibrėžta patikimumo užtikrinimo paslaugų politika, peržiūrėta politika, kurią palaiko patikimumo užtikrinimo paslaugų teikėjas, pateikiama paslaugų naudotojams;

17) B priedas (norminis). Kvalifikuotų elektroninių parašų kvalifikuota galiojimo patvirtinimo paslauga, kaip nustatyta Reglamento (ES) Nr. 910/2014 33 straipsnyje

— VPR-B-02 [SU SĄLYGA]. Jei parašo patvirtinimo paslaugos teikėjas yra kvalifikuotos parašo patvirtinimo paslaugos teikėjas, įgyvendinimas turi atitikti standartą ETSI TS 119 172-4 [8],

— 2 PASTABA negalioja,

— OVR-B-04 [SU SĄLYGA]. Jei parašo patvirtinimo paslaugos teikėjas yra kvalifikuotos parašo patvirtinimo paslaugos teikėjas, atliekant OVR-B-03 punkte nustatytus bandymus tikrinami įvairūs (tiek teigiami, tiek neigiami) naudojimo atvejai,

— VPR-B-11 [SU SĄLYGA]. Jei parašo patvirtinimo paslaugos teikėjas yra kvalifikuotos parašo patvirtinimo paslaugos teikėjas, tai parašo patvirtinimo paslaugos teikėjas turi kontroliuoti maišos skaičiavimą (arba atlikti skaičiavimą serveryje, arba kontroliuoti klientą, jei kontrolė įmanoma kliento pusėje),

— 5 PASTABA negalioja,

— 6 PASTABA negalioja,

— VPR-B-15 [SU SĄLYGA]. Jei parašo patvirtinimo paslaugos teikėjas yra kvalifikuotos parašo patvirtinimo paslaugos teikėjas, parašo patvirtinimo ataskaita turi atitikti standartą ETSI TS 119 102-2 [9], kad būtų patenkinti VPR-B-13–VPR-B-14 punktų reikalavimai,

— VPR-B-16 [SU SĄLYGA]. Jei parašo patvirtinimo paslaugos teikėjas yra kvalifikuotos parašo patvirtinimo paslaugos teikėjas, įgyvendinimas turi atitikti „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir paskelbė ENISA [8], kad teikiant kvalifikuoto elektroninio parašo kvalifikuotas patvirtinimo paslaugas būtų galima naudoti tinkamus šifravimo metodus;

18) C priedas (informacinis). Reikalavimų suderinimas su Reglamentu (ES) Nr. 910/2014, skirsnio „Patvirtinimas pagal 32 straipsnio 1 dalį“ 2 pastraipa:

— siekiant užtikrinti, kad būtų patikrintos visos Reglamento (ES) Nr. 910/2014 [i.1] 32 straipsnio 1 dalyje ir 40 straipsnyje nustatytos sąlygos, reikia tinkamo patvirtinimo algoritmo. Jis pateiktam tvirtinti parašui arba spaudui užtikrina tokį patį deterministinį rezultatą. Tam būtina parašo patvirtinimo politika. Todėl, remiantis standarte ETSI EN 319 102-1 [3] nurodytu patvirtinimo algoritmu, pateiktas standartas ETSI TS 119 172-4 [8];

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 (EPI). 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 (2024-11) „Elektroniniai parašai ir infrastruktūros (EPI). Patikimi sąrašai“,

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektroniniai parašai ir infrastruktūros (EPI). 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 24 valandos. Požymio *RevocationFreshnessConstraints* vertė nustatoma tik pasirašymo sertifikatams ir jokiems kitiems sertifikatams, be kitų, laiko žymai pritaikytiems sertifikatams;

3) 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:

a) procesas sustoja,

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

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