Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1944

2025 9 30

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1944

2025 m. rugsėjo 29 d.

kuriuo dėl duomenų siuntimo ir gavimo procesų, atliekamų teikiant kvalifikuotas elektroninio registruoto pristatymo paslaugas, referencinių standartų ir dėl tokių paslaugų sąveikumo 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 44 straipsnio 2 dalį ir 44 straipsnio 2b dalį,

kadangi:

(1) kvalifikuotomis elektroninio registruoto pristatymo paslaugomis sudaroma galimybė saugiu kanalu perduoti dokumentus, įskaitant duomenų išsiuntimo ir gavimo įrodymą. Teikiant tokias paslaugas tiksliai nustatoma adresato tapatybė ir labai patikimai užtikrinama siuntėjo tapatybė;

(2) Reglamento (ES) Nr. 910/2014 44 straipsnio 1a dalyje numatyta atitikties užtikrinimo prezumpcija turėtų galioti tik jei kvalifikuotoms elektroninio registruoto pristatymo paslaugoms teikti būtinos kvalifikuotos patikimumo užtikrinimo 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;

(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 paslaugos teikėjas gali ir kitais būdais;

(4) jei kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai pagal Reglamento (ES) Nr. 910/2014 44 straipsnio 2a dalį susitaria dėl savo paslaugų sąveikumo, svarbu, kad jie laikytųsi šio įgyvendinimo reglamento II priede nustatytų atitinkamų standartų ir specifikacijų, kad elektroninio registruoto pristatymo duomenis lengvai perduotų dviem arba keliems kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir kad visoje vidaus rinkoje būtų laikomasi sąžiningos veiklos praktikos;

(5) 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).

(6) visai 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]);

(7) 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.;

(8) šiame reglamente nustatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Kvalifikuotų elektroninio registruoto pristatymo paslaugų referenciniai standartai ir specifikacijos

Reglamento (ES) Nr. 910/2014 44 straipsnio 2 dalyje nurodyti referenciniai standartai ir specifikacijos nustatyti šio reglamento I priede.

2 straipsnis

Kvalifikuotų elektroninio registruoto pristatymo paslaugų sąveikumo referenciniai standartai ir specifikacijos

Reglamento (ES) Nr. 910/2014 44 straipsnio 2b dalyje nurodyti referenciniai standartai ir specifikacijos nustatyti šio reglamento II priede.

3 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).

I PRIEDAS

1 straipsnyje nurodytas referencinių standartų ir specifikacijų sąrašas

Standartas ETSI EN 319 521 V1.1.1 (2019-02) (ETSI EN 319 521) taikomas adaptuotas taip:

1. standartas ETSI EN 319 521:

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 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“,

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Elektroniniai parašai ir infrastruktūros (ESI). Elektroninio registruoto pristatymo paslaugos“, 1 dalis „Pagrindai ir architektūra“,

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Elektroniniai parašai ir infrastruktūros (ESI). Elektroninio registruoto pristatymo paslaugos“, 2 dalis „Semantinis turinys“,

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

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

— [7] 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,

— [8] 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,

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

2) 3.1. Terminai

— pažangusis elektroninis spaudas – kaip apibrėžta Reglamente (ES) Nr. 910/2014 [i.1],

— pažangusis elektroninis parašas – kaip apibrėžta Reglamente (ES) Nr. 910/2014 [i.1],

— kvalifikuotas elektroninis spaudas – kaip apibrėžta Reglamente (ES) Nr. 910/2014 [i.1],

— kvalifikuotas elektroninis parašas – kaip apibrėžta Reglamente (ES) Nr. 910/2014 [i.1],

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

([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.

3) 5.1.1. Bendrosios nuostatos

— REQ-ERDS-5.1.1-01. Elektroninio registruoto pristatymo paslaugos užtikrina, kad siekiant tinkamai garantuoti vartotojo turinio prieinamumą, vientisumą ir konfidencialumą, kol jis naudojamas tokioms paslaugoms teikti, būtų pasirenkami tinkami vientisumo ir konfidencialumo šifravimo metodai, atitinkantys „Suderintuosius šifravimo mechanizmus“, kuriems pritarė Europos kibernetinio saugumo sertifikavimo grupė ir kuriuos paskelbė ENISA [5];

4) 5.2.1.1. Bendrieji reikalavimai

— REQ-QERDS-5.2.1.1-01. Kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas aukštą gavėjo tapatybės patikimumo lygį užtikrina pats arba pasitelkęs trečiąją šalį ir prireikus naudoja vieną iš šių priemonių arba jų derinį:

a) fiziškai dalyvaujant fiziniam asmeniui arba juridinio asmens įgaliotajam atstovui, pateikiant įrodymus ir vykdant tinkamas procedūras laikantis nacionalinės teisės,

b) nuotoliniu būdu elektroninės atpažinties priemone, atitinkančia Reglamento (ES) Nr. 910/2014 [i.1] 8 straipsnyje nustatytus aukšto saugumo lygio reikalavimus, arba naudojant europinę skaitmeninės tapatybės dėklę,

c) naudodamas kvalifikuotą elektroninio parašo arba elektroninio spaudo sertifikatą,

d) kitais identifikavimo metodais, kuriais užtikrinama, kad fizinį asmenį arba juridinio asmens įgaliotąjį atstovą būtų galima identifikuoti labai aukštu patikimumo lygiu. Labai aukštą patikimumo lygį, kuriuo atliekamas toks identifikavimas, turi patvirtinti atitikties vertinimo įstaiga;

— REQ-QERDS-5.2.1.1-01A. Kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas siuntėjo tapatybę patikrina tinkamomis priemonėmis tiesiogiai arba pasitelkęs trečiąją šalį ir tam taiko vieną iš šių metodų arba jų derinį:

a) fiziškai dalyvaujant fiziniam asmeniui arba juridinio asmens įgaliotajam atstovui, pateikiant įrodymus ir vykdant tinkamas procedūras laikantis nacionalinės teisės,

b) nuotoliniu būdu, naudodamas europinę skaitmeninės tapatybės dėklę arba elektroninę tapatybės nustatymo priemonę, apie kurią pranešta, atitinkančią Reglamento (ES) Nr. 910/2014 [i.1] 8 straipsnyje nustatytus pakankamo saugumo lygio reikalavimus, jeigu ji išduota remiantis tuo, kad anksčiau fizinis asmuo arba juridinio asmens įgaliotasis atstovas dalyvavo fiziškai,

c) pažangiuoju elektroninio parašo arba pažangiojo elektroninio spaudo sertifikatu, jei sertifikatas fiziniams asmeniui arba juridinio asmens įgaliotajam atstovui išduotas pagal standarte ETSI EN 319 411-1 [2] apibrėžtą normalizuotą sertifikatų politiką, arba

d) kitais identifikavimo metodais, kuriais užtikrinama, kad fizinį asmenį arba juridinio asmens įgaliotąjį atstovą būtų galima identifikuoti labai aukštu patikimumo lygiu. Aukštą patikimumo lygį, kuriuo atliekamas toks identifikavimas, turi patvirtinti atitikties vertinimo įstaiga,

— PASATABA. Siuntėjo ir gavėjo tapatybę tikrinanti trečioji šalis gali būti kitas kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas, jei siuntėjas ir gavėjas naudojasi skirtingų kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjų paslaugomis;

5) 5.2.1.2. Gavėjo identifikavimas ir naudotojo turinio perdavimas

— REQ-QERDS-5.2.1.2-03. Jei gavėjo identifikavimas grindžiamas kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjo vidaus procesu, kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas visą procesą vykdo saugioje ir kontroliuojamoje aplinkoje;

6) 5.2.2. ES kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjo tapatumo nustatymo nuostatos

— REQ-QERDS-5.2.2-03 [SU SĄLYGA]. Jei kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas tapatumo nustatymo priemonę susieja su siuntėjo tapatybe, patikrinta pagal 5.2.1 punktą, tokia priemonė turi būti viena iš šių priemonių:

a) dviejų veiksnių tapatumo nustatymo mechanizmai,

b) europinė skaitmeninės tapatybės dėklė arba elektroninės atpažinties priemonė, apie kurią pranešta, atitinkanti Reglamento (ES) Nr. 910/2014 [i.1] 8 straipsnyje nustatytus reikalavimus dėl aukšto arba pakankamo saugumo užtikrinimo lygio,

c) abipusis TLS tapatumo nustatymas, apimantis siuntėjui pagal standarte ETSI EN 319 411-1 [2] apibrėžtą normalizuotą sertifikatų politiką išduodamą sertifikatą,

d) skaitmeninis parašas, kurį palaiko siuntėjui pagal standarte ETSI EN 319 411-1 [2] apibrėžtą normalizuotą sertifikatų politiką išduodamas sertifikatas,

e) kitos priemonės, kuriomis užtikrinamas identifikuotojo siuntėjo tapatumo nustatymas. Susiejimo atitiktį reikalavimams turi patvirtinti atitikties vertinimo įstaiga. Pavyzdžiui, a, b ir d punktuose nurodytos priemonės naudojamos užregistruoti transporto lygmens saugumo (TLS) kliento sertifikatą, skirtą automatiniam perdavimui su abipusiu TLS, arba užregistruoti skaitmeninio spaudo sertifikatą, naudojamą spaudo tvirtinimui siekiant nustatyti tapatumą elektroninio registruoto pristatymo paslaugai. Gali būti taikomi ir kiti mechanizmai, kai identifikuotieji siuntėjai naudojasi trečiosioms šalims deleguotosiomis paslaugomis;

— REQ-QERDS-5.2.2-03A [SU SĄLYGA]. Jei kvalifikuotos elektroninio registruoto pristatymo paslaugos teikėjas tapatumo nustatymo priemonę susieja su gavėjo tapatybe, patikrinta pagal 5.2.1 punktą, tokia priemonė turi būti viena iš šių priemonių, jei priemone arba tokių priemonių deriniu užtikrinamas labai aukštas gavėjo, kurio tapatybė nustatyta, tapatybės patikimumo lygis:

a) daugiaveiksnio tapatumo nustatymo mechanizmai,

b) europinė skaitmeninės tapatybės dėklė arba elektroninės atpažinties priemonė, apie kurią pranešta, atitinkanti Reglamento (ES) Nr. 910/2014 [i.1] 8 straipsnyje nustatytus reikalavimus dėl aukšto arba pakankamo saugumo užtikrinimo lygio,

c) kvalifikuoto elektroninio parašo arba elektroninio spaudo sertifikatas,

d) kitos priemonės, kuriomis užtikrinamas identifikuotojo gavėjo tapatumo nustatymas. Susiejimo atitiktį reikalavimams turi patvirtinti atitikties vertinimo įstaiga. Pavyzdžiui, a–c punktuose nurodytos priemonės naudojamos užregistruoti transporto lygmens saugumo (TLS) kliento sertifikatą, skirtą automatiniam perdavimui su abipusiu TLS, arba užregistruoti skaitmeninio spaudo sertifikatą, naudojamą spaudo tvirtinimui siekiant nustatyti tapatumą elektroninio registruoto pristatymo paslaugai. Gali būti taikomi ir kiti mechanizmai, kai identifikuotieji siuntėjai naudojasi trečiosioms šalims deleguotosiomis paslaugomis;

— REQ-QERDS-5.2.2-04 [SU SĄLYGA]. Jei prie kvalifikuotos elektroninio registruoto pristatymo paslaugos siuntėjas jungiasi saugiu ryšiu, kuriam būtinas įrenginių tarpusavio tapatumo nustatymas tarp siuntėjo įrenginio ir kvalifikuotos elektroninio registruoto pristatymo paslaugos serverio, remiantis pagal standarte ETSI EN 319 411-1 [2] apibrėžtą normalizuotą sertifikatų politiką išduotais sertifikatais, tai, užmezgus tokį saugų ryšį, antrajam siuntėjo tapatumo nustatymo etapui gali būti naudojami vieno veiksnio tapatumo nustatymo mechanizmai, jei siuntėjo tapatumo nustatymo patikimumas užtikrinamas įdiegtomis organizacinėmis procedūromis ir nustatytomis saugumo priemonėmis;

7) 5.4.1. Bendrosios nuostatos

— REQ-ERDS-5.4.1-06. Elektroninio registruoto pristatymo paslauga sugeneruoja ir teisėtą interesą turinčioms šalims pateikia elektroninio registruoto pristatymo paslaugos įrodymus, susijusius su elektroninio registruoto pristatymo įvykiais, kaip nustatyta standarto ETSI EN 319 522-1 [3] 6 punkte,

— REQ-ERDS-5.4.1-07. Elektroninio registruoto pristatymo paslaugos teikėjas archyvuoja kiekvieno savo pateikto įrodymo įrodymą ir (arba) įrodymų santraukas,

— REQ-ERDS-5.4.1-08. Elektroninio registruoto pristatymo paslaugos teikėjo sugeneruoti įrodymai turi atitikti standarto ETSI EN 319 522-2 [4] 8 punkte apibrėžtą semantiką;

8) 7.2.1. Bendrosios nuostatos

— REQ-ERDS-7.2.1-02. Pasitikėjimo funkcijas vykdantys elektroninio registruoto pristatymo paslaugos teikėjo darbuotojai turi būti pajėgūs įvykdyti reikalavimą turėti būtinas ekspertines žinias, patirtį ir kvalifikaciją, įgytą baigus oficialų mokymą ir patvirtintą pažymėjimais, ir (arba) praktinę patirtį,

— REQ-ERDS-7.2.1-03. Kad būtų užtikrinta atitiktis REQ-ERDS-7.2.1-02 punktui, reikia reguliariai (bent kas 12 mėnesių) atnaujinti žinias apie naujausias grėsmes ir šiuolaikinius saugumo užtikrinimo metodus;

9) 7.3.2. Laikmenų tvarkymas

— REQ-ERDS-7.3.1-02. Taikomi visi standarto ETSI EN 319 401 [1] 7.3.3 punkto reikalavimai;

10) 7.5. Šifravimo kontrolės priemonės

— REQ-ERDS-7.5-01A. Elektroninio registruoto pristatymo paslaugos teikėjas turi pasirinkti ir taikyti tinkamus šifravimo metodus, atitinkančius Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA paskelbtus suderintuosius šifravimo mechanizmus [5],

— REQ-ERDSP-7.5-03. Elektroninio registruoto pristatymo paslaugos teikėjo privatusis pasirašymo raktas laikomas ir naudojamas saugiame šifravimo įrenginyje – patikimoje sistemoje, sertifikuotoje pagal:

a) standarte ISO/IEC 15408 [6] 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 [7][8] ir sertifikuotoje ne žemesniu kaip 4-uoju vertinimo užtikrinimo lygiu (EAL), arba

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

11) 7.8. Tinklo saugumas

— REQ-ERDSP-7.8-04. Elektroninio registruoto pristatymo paslaugos teikėjas šifravimui transporto lygmeniu naudoja naujausius protokolus ir algoritmus, atitinkančius Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir ENISA paskelbtus suderintuosius šifravimo mechanizmus [5],

— REQ-ERDSP-7.8-06. Silpnųjų vietų paieška, kurios reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-13 punktą, atliekama bent kartą per ketvirtį,

— REQ-ERDSP-7.8-07. Įsiskverbimo bandymas, kurio reikalaujama pagal standarto ETSI EN 319 401 [1] REQ-7.8-17X punktą, atliekamas bent kartą per metus,

— REQ-ERDSP-7.8-08. Užkardos sureguliuojamos taip, kad nepraleistų jokių protokolų ir neleistų jokios prieigos, kurių nereikia patikimumo užtikrinimo paslaugų teikėjo veiklai;

12) 7.12. Elektroninio registruoto pristatymo paslaugos teikėjo veiklos nutraukimas ir veiklos nutraukimo planai

— REQ-ERDS-7.12-03. Elektroninio registruoto pristatymo paslaugos teikėjo veiklos nutraukimo planas turi atitikti įgyvendinimo aktų, priimtų pagal Reglamento (ES) Nr. 910/2014 [i.1] 24 straipsnio 5 dalį, reikalavimus;

13) 7.14. Tiekimo grandinė

— REQ-ERDS-7.14-01. Taikomi standarto ETSI EN 319 401 [1] 7.14 punkte nustatyti reikalavimai.

II PRIEDAS

2 straipsnyje nurodytas pamatinių standartų ir specifikacijų sąrašas

Taikomi standartai: ETSI EN 319 522-1 V1.2.1 (2024-01) (ETSI EN 319 522-1), ETSI EN 319 522-2 V1.2.1 (2024-01) (ETSI EN 319 522-2), ETSI EN 319 522-3 V1.2.1 (2024-01) (ETSI EN 319 522-3), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (ETSI EN 319 522-4-1), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (ETSI EN 319 522-4-2) ir ETSI EN 319 522-4-3 V1.1.1 (2018-09) (ETSI EN 319 522-4-3).