Europos Sąjungos
oficialusis leidinys

L 235

Leidimas
lietuvių kalba

Teisės aktai

58 tomas

2015 m. rugsėjo 9 d.

Turinys

[1] Tekstas svarbus EEE

LT

Aktai, kurių pavadinimai spausdinami paprastu šriftu, yra susiję su kasdieniu žemės ūkio reikalų valdymu ir paprastai galioja ribotą laikotarpį.

Visų kitų aktų pavadinimai spausdinami ryškesniu šriftu ir prieš juos dedama žvaigždutė.

[1] Tekstas svarbus EEE

II

(Ne teisėkūros procedūra priimami aktai)

REGLAMENTAI

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2015/1501

2015 m. rugsėjo 8 d.

dėl sąveikumo sistemos pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 12 straipsnio 8 dalį

(Tekstas svarbus EEE)

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 12 straipsnio 8 dalį,

kadangi:

(1) Reglamento (ES) Nr. 910/2014 12 straipsnio 2 dalyje numatyta, kad sąveikos sistema turėtų būti nustatyta nacionalinės elektroninės atpažinties schemų, apie kurias pranešta pagal to reglamento 9 straipsnio 1 dalį, sąveikos tikslais;

(2) mazgai atlieka pagrindinį vaidmenį sujungiant valstybių narių elektroninės atpažinties schemas. Jų indėlis, taip pat eIDAS mazgo funkcijos ir sudedamosios dalys yra paaiškinti dokumentuose, susijusiuose su Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1316/2013 ([2]) sukurta Europos infrastruktūros tinklų priemone;

(3) jeigu valstybė narė arba Komisija suteikia programinę įrangą kitoje valstybėje narėje eksploatuojamam mazgui, kad būtų galima nustatyti tapatumą, šalis, kuri teikia ir atnaujina programinę įrangą, naudojamą autentiškumo nustatymo mechanizmui, gali susitarti su programinę įrangą priimančia šalimi, kaip autentiškumo nustatymo mechanizmas bus valdomas. Tokiu susitarimu neturėtų būti priimančiajai šaliai keliama neproporcingų techninių reikalavimų ar sąnaudų (įskaitant paramos, atsakomybės, prieglobos ir kitas sąnaudas);

(4) jeigu pateisinama sąveikos sistemos įgyvendinimu, Komisija, bendradarbiaudama su valstybėmis narėmis, visų pirma atsižvelgdama į Komisijos įgyvendinimo sprendimo (ES) 2015/296 ([3]) 14 straipsnio d punkte nurodyto Bendradarbiavimo tinklo nuomones, gali parengti papildomas technines specifikacijas, kuriose pateikiama išsami techninių reikalavimų, kaip nurodyta šiame reglamente, informacija. Tokios specifikacijos turėtų būti rengiamos kaip Reglamento (ES) Nr. 1316/2013, kuriuo nustatomos priemonės praktiškai įgyvendinti elektroninės atpažinties modulį, skaitmeninių paslaugų infrastruktūros dalis;

([1]) OL L 257, 2014 8 28, p. 73.

([2]) 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1316/2013, kuriuo sukuriama Europos infrastruktūros tinklų priemonė ir iš dalies keičiamas Reglamentas (ES) Nr. 913/2010 bei panaikinami reglamentai (EB) Nr. 680/2007 ir (EB) Nr. 67/2010 (OL L 348, 2013 12 20, p. 129).

([3]) 2015 m. vasario 24 d. Komisijos įgyvendinimo sprendimas (ES) 2015/296, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 12 straipsnio 7 dalį nustatomos valstybių narių bendradarbiavimo procedūrinės sąlygos (OL L 53, 2015 2 25, p. 14).

(5) šiame reglamente nustatyti techniniai reikalavimai turėtų būti taikomi nepaisant techninių specifikacijų, kurios galėtų būti parengtos pagal šio reglamento 12 straipsnį, pakeitimų;

(6) nustatant tvarką, susijusią su šiame reglamente išdėstyta sąveikos sistema, su daugiausia dėmesio buvo atsižvelgta į didelio masto bandomąjį projektą STORK ir pagal jį parengtas specifikacijas, taip pat į Europos viešosioms paslaugoms skirtos Europos sąveikumo sistemos principus ir koncepcijas;

(7) su daugiausia dėmesio buvo atsižvelgta į valstybių narių bendradarbiavimo rezultatus;

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

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Dalykas

Šiame reglamente nustatomi sąveikumo sistemos techniniai ir veiklos reikalavimai, siekiant užtikrinti elektroninės atpažinties schemų, apie kurias valstybės narės praneša Komisijai, sąveikumą.

Tie reikalavimai visų pirma apima:

a) minimalius techninius reikalavimus, susijusius su saugumo užtikrinimo lygiais, ir nacionalinių saugumo užtikrinimo lygių nustatymą pagal elektroninės atpažinties schemas, apie kurias pranešta, išduotas elektroninės atpažinties priemones pagal Reglamento (ES) Nr. 910/2014 8 straipsnį, kaip nustatyta 3 ir 4 straipsniuose;

b) minimalius techninius sąveikumo reikalavimus, kaip nustatyta 5 ir 8 straipsniuose;

c) minimalų asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo, rinkinį, kaip nustatyta 11 straipsnyje ir priede;

d) bendrus veiklos saugumo standartus, kaip nustatyta 6, 7, 9 ir 10 straipsniuose;

e) ginčų sprendimo tvarką, kaip nustatyta 13 straipsnyje.

2 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) mazgas – tai jungties taškas, kuris yra elektroninės atpažinties sąveikumo struktūros dalis ir vykdo asmenų tapatumo nustatymą tarpvalstybiniu lygmeniu bei geba atpažinti, tvarkyti ar persiųsti duomenis kitiems mazgams, sudarydamas sąlygas vienos valstybės narės nacionalinei elektroninės atpažinties infrastruktūrai susisieti su kitų valstybių narių nacionalinėmis elektroninės atpažinties infrastruktūromis;

2) mazgo operatorius – subjektas, atsakingas už tai, kad mazgas tinkamai ir patikimai atliktų jungties taško funkcijas.

3 straipsnis

Minimalūs techniniai reikalavimai, susiję su saugumo užtikrinimo lygiais

Minimalūs techniniai reikalavimai, susiję su saugumo užtikrinimo lygiais, yra tokie, kokie nustatyti Komisijos įgyvendinimo reglamente (ES) 2015/1502 ([1]).

4 straipsnis

Nacionalinių saugumo užtikrinimo lygių nustatymas

Nustatant elektroninės atpažinties schemų, apie kurias pranešta, nacionalinius saugumo užtikrinimo lygius vadovaujamasi Įgyvendinimo reglamente (ES) 2015/1502 nustatytais reikalavimais. Nustatymo rezultatai pranešami Komisijai naudojant pranešimo formą, nustatytą Komisijos įgyvendinimo sprendime (ES) 2015/1505 ([2]).

5 straipsnis

Mazgai

1. Sudaromos sąlygos mazgui vienoje valstybėje susijungti su kitų valstybių narių mazgais.

2. Mazgai techninėmis priemonėmis turi gebėti atskirti viešojo sektoriaus įstaigas nuo kitų pasikliaujančiųjų šalių.

3. Valstybė narė, įgyvendindama šiame reglamente nustatytus techninius reikalavimus, nenustato neproporcingų techninių reikalavimų ir nesudaro neproporcingų sąnaudų kitoms valstybėms narėms, kad šios galėtų sąveikauti su minėtąja valstybe nare, atsižvelgiant į joje įgyvendintas priemones.

6 straipsnis

Duomenų privatumas ir konfidencialumas

1. Duomenų, kuriais keičiamasi, privatumo ir konfidencialumo apsauga bei duomenų vientisumo tarp mazgų išlaikymas užtikrinamas naudojant geriausius turimus techninius sprendimus ir apsaugos praktiką.

2. Mazguose nesaugomi jokie asmens duomenys, išskyrus 9 straipsnio 3 dalyje nurodytu tikslu.

7 straipsnis

Ryšių duomenų vientisumas ir tikrumas

Ryšiuose tarp mazgų užtikrinamas duomenų vientisumas ir tikrumas, siekiant užtikrinti, kad visi prašymai ir atsakymai yra tikri ir kad jie nebuvo suklastoti. Šiuo tikslu mazguose naudojami sprendimai, kurie sėkmingai buvo taikyti tarpvalstybinėje veikloje.

([1]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1502, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių (žr. šio Oficialiojo leidinio p. 7).

([2]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo sprendimas (ES) 2015/1505, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 22 straipsnio 5 dalį nustatomos patikimų sąrašų techninės specifikacijos ir formatai (žr. šio Oficialiojo leidinio p. 26).

8 straipsnis

Ryšių pranešimų formatas

Mazgai sintaksei naudoja įprastus pranešimų formatus, paremtus standartais, kurie jau buvo naudoti tarp valstybių narių daugiau nei kartą ir pasiteisino darbo aplinkoje. Sintaksė turi leisti:

a) tinkamai tvarkyti minimalų asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo, rinkinį;

b) tinkamai tvarkyti elektroninės atpažinties priemonių saugumo užtikrinimo lygį;

c) atskirti viešojo sektoriaus įstaigas nuo kitų pasikliaujančiųjų šalių;

d) suteikti lankstumo tenkinti su identifikavimu susijusius poreikius dėl papildomų požymių.

9 straipsnis

Saugumo informacijos ir metaduomenų valdymas

1. Mazgo operatorius pateikia mazgo valdymo metaduomenis standartizuota techninėmis priemonėmis apdorojama forma, saugiai ir patikimai.

2. Bent su saugumu susiję parametrai turi būti gaunami automatiškai.

3. Mazgo operatorius saugo duomenis, kurie, įvykus incidentui, leidžia atkurti keitimosi pranešimais seką, siekiant nustatyti incidento vietą ir pobūdį. Duomenys saugomi tam tikrą pagal nacionalinius reikalavimus nustatytą laikotarpį ir juos sudaro bent šie elementai:

a) mazgo identifikaciniai duomenys;

b) pranešimo identifikaciniai duomenys;

c) pranešimo data ir laikas.

10 straipsnis

Informacijos saugumo užtikrinimas ir saugumo standartai

1. Tapatumą nustatančių mazgų operatoriai turi įrodyti, kad mazgai, dalyvaujantys sąveikumo sistemoje, atitinka standarto ISO/IEC 27001 reikalavimus, pateikdami sertifikatą arba lygiaverčiais vertinimo metodais arba laikydamiesi nacionalinių teisės aktų.

2. Mazgų operatoriai nedelsdami atlieka saugumui svarbius atnaujinimus.

11 straipsnis

Asmens tapatybės duomenys

1. Kai minimalus asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo, rinkinys naudojamas tarpvalstybiniu mastu, jis turi atitikti priede nustatytus reikalavimus.

2. Kai juridiniam asmeniui atstovaujančio fizinio asmens minimalus duomenų rinkinys naudojamas tarpvalstybiniu mastu, jame turi būti pateiktas priede išvardytų fiziniams asmenims ir juridiniams asmenims taikomų požymių derinys.

3. Duomenys perduodami originaliais rašmenimis ir, jeigu tinkama, taip pat perrašomi lotynų kalbos rašmenimis.

12 straipsnis

Techninės specifikacijos

1. Jei tai pagrįsta sąveikumo sistemos įgyvendinimo procesu, bendradarbiavimo tinklas, įsteigtas Įgyvendinimo sprendimu (ES) 2015/296, gali parengti nuomones pagal jo 14 straipsnio d punktą dėl poreikio parengti technines specifikacijas. Tokiose techninėse specifikacijose turi būti suteikta daugiau informacijos apie techninius reikalavimus, kaip nustatyta šiame reglamente.

2. Pagal 1 dalyje nurodytą nuomonę Komisija, bendradarbiaudama su valstybėmis narėmis, parengia technines specifikacijas kaip Reglamento (ES) Nr. 1316/2013 skaitmeninių paslaugų infrastruktūros dalį.

3. Bendradarbiavimo tinklas pagal Įgyvendinimo sprendimo (ES) 2015/296 14 straipsnio d punktą priima nuomonę, kurioje įvertinama, ar ir kokiu mastu pagal 2 dalį parengtos techninės specifikacijos atitinka poreikį, nustatytą 1 dalyje nurodytoje nuomonėje, arba šiame reglamente nustatytus reikalavimus. Jis gali rekomenduoti, kad valstybės narės, įgyvendindamos sąveikumo sistemą, atsižvelgtų į technines specifikacijas.

4. Komisija pateikia įgyvendinimo modelį kaip techninių specifikacijų aiškinimo pavyzdį. Valstybės narės gali taikyti šį įgyvendinimo modelį arba, bandydamos kitus techninių specifikacijų įgyvendinimo būdus, jį naudoti kaip pavyzdį.

13 straipsnis

Ginčų sprendimas

1. Jei įmanoma, bet koks ginčas dėl sąveikumo sistemos sprendžiamas susijusių valstybių narių derybomis.

2. Jeigu pagal 1 dalį nepriimamas joks sprendimas, bendradarbiavimo tinklas, įsteigtas pagal Įgyvendinimo sprendimo (ES) 2015/296 12 straipsnį, turi kompetenciją spręsti ginčą pagal savo darbo tvarkos taisykles.

14 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 2015 m. rugsėjo 8 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

PRIEDAS

Reikalavimai dėl 11 straipsnyje nurodyto minimalaus asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo, rinkinio

1. **Minimalus fizinio asmens duomenų rinkinys**

Minimalų fizinio asmens duomenų rinkinį turi sudaryti visi šie privalomi požymiai:

a) dabartinė (-ės) pavardė (-ės);

b) dabartinis (-iai) vardas (-ai);

c) gimimo data;

d) pagal technines specifikacijas tarpvalstybinės atpažinties tikslu siunčiančiosios valstybės narės sukurtas unikalus identifikatorius, kuris turi būti kuo pastovesnis.

Minimalų fizinio asmens duomenų rinkinį gali sudaryti vienas ar daugiau šių papildomų požymių:

a) vardas (-ai) ir pavardė (-ės) gimimo metu;

b) gimimo vieta;

c) dabartinis adresas;

d) lytis.

2. **Minimalus juridinio asmens duomenų rinkinys**

Minimalų juridinio asmens duomenų rinkinį turi sudaryti visi šie privalomi požymiai:

a) dabartinis teisinis pavadinimas;

b) pagal technines specifikacijas tarpvalstybinės atpažinties tikslu siunčiančiosios valstybės narės sukurtas unikalus identifikatorius, kuris turi būti kuo pastovesnis.

Minimalų juridinio asmens duomenų rinkinį gali sudaryti vienas ar daugiau šių papildomų požymių:

a) dabartinis adresas;

b) PVM mokėtojo kodas;

c) mokesčių mokėtojo registracijos kodas;

d) identifikacinis kodas, susijęs su Europos Parlamento ir Tarybos direktyvos 2009/101/EB 3 straipsnio 1 dalimi ([1]);

e) Komisijos įgyvendinimo reglamente (ES) Nr. 1247/2012 ([2]) nurodytas juridinio asmens identifikatorius;

f) Komisijos įgyvendinimo reglamente (ES) Nr. 1352/2013 ([3]) nurodytas Ekonominių operacijų vykdytojų registracijos ir identifikavimo kodas (EORI kodas);

g) Tarybos reglamento (ES) Nr. 389/2012 2 straipsnio 12 dalyje nurodytas akcizo numeris ([4]).

([1]) 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos direktyva 2009/101/EB dėl apsaugos priemonių, kurių valstybės narės reikalauja iš Sutarties 48 straipsnio antroje pastraipoje apibrėžtų bendrovių siekiant apsaugoti narių ir trečiųjų asmenų interesus, koordinavimo, siekiant suvienodinti tokias apsaugos priemones (OL L 258, 2009 10 1, p. 11).

([2]) 2012 m. gruodžio 19 d. Komisijos įgyvendinimo reglamentas (ES) Nr. 1247/2012, kuriuo nustatomi pranešimų apie sandorius, teikiamų sandorių duomenų saugykloms pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų, formato ir dažnumo techniniai įgyvendinimo standartai (OL L 352, 2012 12 21, p. 20).

([3]) 2013 m. gruodžio 4 d. Komisijos įgyvendinimo reglamentas (ES) Nr. 1352/2013, kuriuo nustatomos Europos Parlamento ir Tarybos reglamente (ES) Nr. 608/2013 dėl muitinės atliekamo intelektinės nuosavybės teisių vykdymo užtikrinimo numatytos formos (OL L 341, 2013 12 18, p. 10).

([4]) 2012 m. gegužės 2 d. Tarybos reglamentas (ES) Nr. 389/2012 dėl administracinio bendradarbiavimo akcizų srityje ir panaikinantis Reglamentą (EB) Nr. 2073/2004 (OL L 121, 2012 5 8, p. 1).

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2015/1502

2015 m. rugsėjo 8 d.

kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių

(Tekstas svarbus EEE)

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 8 straipsnio 3 dalį,

kadangi:

(1) Reglamento (ES) Nr. 910/2014 8 straipsnyje numatyta, kad elektroninės atpažinties schemoje, apie kurią pranešta pagal 9 straipsnio 1 dalį, turi būti apibrėžti elektroninės atpažinties priemonių, išduodamų pagal tą schemą, žemas, pakankamas ir (arba) aukštas saugumo užtikrinimo lygiai;

(2) būtina nustatyti minimalias technines specifikacijas, standartus ir procedūras, siekiant užtikrinti saugumo užtikrinimo lygių informacijos bendrą aiškinimą ir užtikrinti sąveikumą derinant elektroninės atpažinties schemų, apie kurias pranešta, nacionalinius saugumo užtikrinimo lygius su 8 straipsnyje numatytais saugumo užtikrinimo lygiais, kaip numatyta Reglamento (ES) Nr. 910/2014 12 straipsnio 4 dalies b punkte;

(3) nustatant šiame įgyvendinimo akte pateiktas specifikacijas ir procedūras buvo atsižvelgta į tarptautinį standartą ISO/IEC 29115 kaip į pagrindinį elektroninės atpažinties priemonių saugumo užtikrinimo lygiams taikomą tarptautinį standartą. Tačiau Reglamento (ES) Nr. 910/2014 turinys skiriasi nuo to tarptautinio standarto, visų pirma kiek tai susiję su tapatybės įrodymo ir tikrinimo reikalavimais, taip pat su tuo, kaip atsižvelgiama į valstybių narių tapatybės nustatymo tvarkos ir tapatybės nustatymo tvarkos esamose ES priemonėse skirtumus. Todėl nors priede ir remiamasi šiuo tarptautiniu standartu, jame neturėtų būti daroma nuoroda į jokį konkretų standarto ISO/IEC 29115 turinį;

(4) šis reglamentas parengtas remiantis rezultatais pagrįstu metodu, kuris laikomas tinkamiausiu – tai taip pat matyti iš apibrėžčių, vartojamų terminams ir sąvokoms apibrėžti. Juose atsižvelgiama į Reglamento (ES) Nr. 910/2014 tikslą, susijusį su elektroninės atpažinties priemonių saugumo užtikrinimo lygiais. Todėl nustatant šiame įgyvendinimo akte nustatytas specifikacijas ir procedūras turėtų būti kuo labiau atsižvelgiama į didelio masto bandomąjį projektą STORK, įskaitant pagal jį parengtas specifikacijas, ir į standarto ISO/IEC 29115 apibrėžtis ir sąvokas;

(5) priklausomai nuo aplinkybių, pagal kurias turi būti patikrintas tapatybės įrodymo aspektas, autoritetingų šaltinių forma gali būti įvairi, pavyzdžiui, be kita ko, registrai, dokumentai ar įstaigos. NET ir panašiomis aplinkybėmis autoritetingi šaltiniai skirtingose valstybėse narėse gali būti skirtingi;

(6) reikalavimuose dėl tapatybės įrodymo ir tikrinimo turėtų būti atsižvelgiama į skirtingas sistemas ir praktiką, kartu užtikrinant pakankamai aukštą saugumo lygį, būtiną reikiamam pasitikėjimui garantuoti. Todėl priimti procedūras, anksčiau naudotas kitu nei elektroninės atpažinties priemonių išdavimo tikslu, turėtų būti galima tik patvirtinus, kad šios procedūros atitinka reikalavimus, numatytus atitinkamam užtikrinimo lygiui;

([1]) OL L 257, 2014 8 28, p. 73.

(7) paprastai naudojami tam tikri tapatumo nustatymo veiksniai, tokie kaip bendros paslaptys, fiziniai įtaisai ir fizinės savybės. Vis dėlto siekiant padidinti tapatumo nustatymo proceso saugumą reikėtų skatinti naudoti daugiau tapatumo nustatymo veiksnių, ypač priklausančių įvairioms veiksnių kategorijoms;

(8) šiuo reglamentu neturėtų būti daromas poveikis juridinių asmenų atstovavimo teisėms. Vis dėlto priede turėtų būti numatyti reikalavimai dėl fizinių ir juridinių asmenų elektroninės atpažinties priemonių susiejimo;

(9) turėtų būti pripažįstama informacijos saugumo ir paslaugų valdymo sistemų svarba, taip pat pripažintos metodikos naudojimo bei principų, nustatytų standartuose, tokiuose kaip ISO/IEC 27000 ir EN ISO/IEC 20000 serijos, taikymo svarba;

(10) taip pat turėtų būti atsižvelgiama į gerąją praktiką, susijusią su saugumo užtikrinimo lygiais valstybėse narėse;

(11) tarptautiniais standartais grindžiamas IT saugumo sertifikavimas yra svarbi priemonė siekiant patikrinti, ar produktai atitinka šiame įgyvendinimo akte nustatytus saugumo reikalavimus;

(12) Reglamento (ES) Nr. 910/2014 48 straipsnyje nurodytas komitetas nepareiškė nuomonės per jo pirmininko nustatytą laikotarpį,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

1. Elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, žemas, pakankamas ir aukštas saugumo užtikrinimo lygiai nustatomi remiantis priede pateiktomis specifikacijomis ir procedūromis.

2. Elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, saugumo užtikrinimo lygiui apibrėžti naudojamos priede pateiktos specifikacijos ir procedūros, nustatant šių elementų patikimumą ir kokybę:

a) registracijos, kaip nustatyta šio reglamento priedo 2.1 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies a punktą;

b) elektroninės atpažinties priemonių valdymo, kaip nustatyta šio reglamento priedo 2.2 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies b ir f punktus;

c) tapatumo nustatymo, kaip nustatyta šio reglamento priedo 2.3 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies c punktą;

d) valdymo ir organizavimo, kaip nustatyta šio reglamento priedo 2.4 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies d ir e punktus.

3. Jeigu elektroninės atpažinties priemonė, išduota pagal elektroninės atpažinties schemą, apie kurią pranešta, atitinka aukštesnio saugumo užtikrinimo lygio reikalavimą, laikoma, kad ji atitinka lygiavertį žemesnio saugumo užtikrinimo lygio reikalavimą.

4. Jeigu atitinkamoje priedo dalyje nenurodyta kitaip, elektroninės atpažinties priemonė, išduota pagal elektroninės atpažinties schemą, apie kurią pranešta, turi atitikti visus priede išvardytus tam tikro saugumo užtikrinimo lygio elementus, kad atitiktų tą lygį.

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 2015 m. rugsėjo 8 d.

Komisijos vardu
Pirmininkas
Jean-Claude JUNCKER

PRIEDAS

Techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, žemo, pakankamo ir aukšto saugumo užtikrinimo lygių

1. **Terminų apibrėžtys**

Šiame priede vartojamų terminų apibrėžtys:

1) autoritetingas šaltinis – bet kokios formos šaltinis, kurio tikslūs duomenys, informacija ir (arba) įrodymai yra patikimi ir jus galima naudoti tapatybei įrodyti;

2) tapatumo nustatymo veiksnys – veiksnys, patvirtintas kaip esantis susijęs su asmeniu ir priklausantis prie vienos iš šių kategorijų:

   a) turėjimu grindžiamas tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kai subjektas turi įrodyti jį turįs;

   b) žiniomis grindžiamas tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kai subjektas turi įrodyti apie jį žinąs;

   c) būdingasis tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kuris grindžiamas fizinio asmens fizinėmis savybėmis ir subjektas turi įrodyti turįs tas fizines savybes;

3) dinaminis tapatumo nustatymas – elektroninis procesas, kuriuo naudojant kriptografijos ar kitus metodus suteikiama priemonė sukurti reikalaujamam elektroniniam įrodymui, kad subjektas kontroliuoja arba turi identifikavimo duomenis, ir kuris, priklausomai nuo subjekto ir subjekto tapatybę tikrinančios sistemos, kinta kiekvieną kartą nustatant tapatybę;

4) informacijos saugumo valdymo sistema – visuma procesų ir procedūrų, skirtų priimtinu lygiu valdyti rizikai, susijusiai su informacijos saugumu.

2. **Techninės specifikacijos ir procedūros**

Šiame priede nurodyti techninių specifikacijų ir procedūrų elementai naudotini siekiant nustatyti, kaip Reglamento (ES) Nr. 910/2014 8 straipsnyje pateikti reikalavimai ir kriterijai turi būti taikomi elektroninėms atpažinties priemonėms, išduotoms pagal elektroninės atpažinties schemą.

2.1. *Registracija*

2.1.1. Prašymo teikimas ir užregistravimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Užtikrinti, kad prašytojas būtų susipažinęs su elektroninės atpažinties priemonių naudojimo sąlygomis. 2. Užtikrinti, kad prašytojas būtų susipažinęs su rekomenduojamomis saugumo priemonėmis, susijusiomis su elektroninės atpažinties priemonėmis. 3. Rinkti reikiamus tapatybės duomenis, reikalingus tapatybei įrodyti ir patikrinti.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.1.2. Tapatybės įrodymas ir tikrinimas (fizinio asmens)

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Gali būti laikoma, kad asmuo turi įrodymų, kuriuos yra pripažinusi valstybė narė, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir kurie nurodo pareikštą tapatybę. 2. Gali būti laikoma, kad įrodymas yra tikras arba egzistuoja remiantis autoritetingu šaltiniu, ir atrodo, kad įrodymas yra galiojantis. 3. Autoritetingam šaltiniui žinoma, kad tvirtinama tapatybė egzistuoja, ir gali būti laikoma, kad asmuo, kuris pareiškia turintis tam tikrą tapatybę, yra tas pats.
Pakankamas	Be žemo lygio elementų, turi būti atitinkama viena iš 1–4 punktuose nurodytų sąlygų: 1. buvo patikrinta ir patvirtinta, kad asmuo turi įrodymų, pripažintų valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir kurie nurodo pareikštą tapatybę, ir įrodymai patikrinti siekiant nustatyti, ar jie yra tikri; arba, remiantis autoritetingu šaltiniu, žinoma, kad jie egzistuoja ir yra susiję su realiu asmeniu, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad asmens tapatybė nėra tvirtinama tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad įrodymai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 2. asmens tapatybės dokumentas pateiktas per registracijos procesą jo išdavimo valstybėje narėje ir atrodo, kad dokumentas yra susijęs su jį pateikusiu asmeniu, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad asmens tapatybė nėra pareikšta tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad dokumentai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 3. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.2 skirsnyje nustatytam pakankamo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Europos Parlamento ir Tarybos reglamento (EB) Nr. 765/2008 [1] 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga, arba lygiavertė įstaiga; arba 4. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis pakankamo arba aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, ir atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų; jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, pakankamą arba aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga.

Saugumo užtikrinimo lygis	Būtini elementai
Aukštas	Turi būti laikomasi 1 arba 2 punkto reikalavimų: 1. Be pakankamo lygio elementų, turi būti atitinkama viena iš a–c punktuose nurodytų sąlygų: a) jeigu buvo patikrinta ir patvirtinta, kad asmuo turi fotografinių arba biometrinių atpažinties įrodymų, pripažintų valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir tie įrodymai nurodo pareikštą tapatybę, tie įrodymai tikrinami siekiant nustatyti, ar jie galioja, remiantis autoritetingu šaltiniu, ir prašytojo tapatybė nustatoma kaip tvirtinama tapatybė, lyginant vieną ar kelias asmens fizines savybes su autoritetingu šaltiniu, arba b) jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.2 skirsnyje nustatytam aukšto saugumo užtikrinimo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga arba lygiavertė įstaiga, ir imtasi veiksmų siekiant įrodyti, kad šių ankstesnių procedūrų rezultatai tebegalioja; arba c) jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, ir atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. Jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga, ir imtasi veiksmų, siekiant įrodyti, kad elektroninių atpažinties priemonių, apie kurias pranešta, ankstesnės išdavimo procedūros rezultatai tebegalioja. ARBA 2. Jeigu prašytojas nepateikia jokių pripažintų fotografinių ar biometrinių tapatybės atpažinties įrodymų, taikomos tos pačios procedūros, kurios nacionaliniu lygiu naudojamos įstaigos, atsakingos už registraciją, valstybėje narėje, siekiant gauti tokius pripažintus fotografinius arba biometrinius tapatybės nustatymo įrodymus.

([1]) 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

2.1.3. Tapatybės įrodymas ir tikrinimas (juridinio asmens)

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Juridinio asmens tvirtinama tapatybė įrodoma remiantis valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais.

Saugumo užtikrinimo lygis	Būtini elementai
	2. Atrodo, kad įrodymai yra galiojantys, ir gali būti laikoma, kad jie yra tikri arba egzistuoja, remiantis autoritetingu šaltiniu, jeigu juridinio asmens įtraukimas į autoritetingą šaltinį yra savanoriškas ir reglamentuojamas juridinio asmens ir autoritetingo šaltinio susitarimu. 3. Autoritetingam šaltiniui nežinoma, ar juridinis asmuo yra būklėje, kuri neleistų jam veikti kaip tam juridiniam asmeniui.
Pakankamas	Be žemo lygio elementų, turi būti atitinkama viena iš 1–3 punktuose nurodytų sąlygų: 1. juridinio asmens pareikšta tapatybė įrodoma remiantis valstybės narės, kurioje pateiktas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais, be kita ko, juridinio asmens pavadinimu, teisine forma ir (jei taikoma) registracijos numeriu ir įrodymai tikrinami siekiant nustatyti, ar jie tikri, arba žinoma, kad jie egzistuoja, remiantis autoritetingu šaltiniu, jeigu juridinio asmens įtraukimas į autoritetingą šaltinį yra reikalingas tam, kad juridinis asmuo galėtų veikti savo sektoriuje, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad juridinio asmens tapatybė nėra pareikšta tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad dokumentai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 2. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.3 skirsnyje nustatytam pakankamo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga, arba lygiavertė įstaiga; arba 3. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis pakankamo arba aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. jeigu apie elektroninės atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, pakankamą arba aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga.
Aukštas	Be pakankamo lygio elementų, turi būti atitinkama viena iš 1–3 punktuose nurodytų sąlygų: 1. juridinio asmens tvirtinama tapatybė įrodoma remiantis valstybės narės, kurioje pateiktas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais, be kita ko, juridinio asmens pavadinimu, teisine forma ir bent vienu nacionalinėje aplinkoje naudojamu unikaliu identifikatoriumi, susijusiu su juridiniu asmeniu, ir įrodymai tikrinami siekiant nustatyti, ar jie yra tikri, remiantis autoritetingu šaltiniu; arba

Saugumo užtikrinimo lygis	Būtini elementai
	2. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo, nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.3 skirsnyje nustatytam aukšto lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga arba lygiavertė įstaiga, ir imtasi veiksmų siekiant įrodyti, kad šių ankstesnių procedūrų rezultatai tebegalioja; arba 3. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. Jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga, ir imtasi veiksmų, siekiant įrodyti, kad elektroninių atpažinties priemonių, apie kurias pranešta, ankstesnės išdavimo procedūros rezultatai tebegalioja.

2.1.4. Fizinių ir juridinių asmenų elektroninės atpažinties priemonių susiejimas

Atitinkamais atvejais fizinio asmens elektroninės atpažinties priemonių ir juridinio asmens elektroninės atpažinties priemonių susiejimui (toliau – susiejimas) taikomos šios sąlygos:

1) turi būti įmanoma sustabdyti ir (arba) atšaukti susiejimą. Susiejimo gyvavimo ciklas (pvz., aktyvavimas, sustabdymas, atnaujinimas, atšaukimas) tvarkomas laikantis nacionaliniu lygiu pripažintų procedūrų.

2) Fizinis asmuo, kurio elektroninės atpažinties priemonės yra susietos su juridinio asmens elektroninės atpažinties priemonėmis, pagal nacionaliniu lygiu pripažintas procedūras susiejimą gali įgalioti kitam fiziniam asmeniui. Vis dėlto atsakomybė išlieka įgaliojančiojo fizinio asmens.

3) Susiejimas atliekamas taip:

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas žemu arba aukštesniu lygiu. 2. Susiejimas nustatytas remiantis nacionaliniu lygiu pripažintomis procedūromis. 3. Autoritetingam šaltiniui nežinoma, kad fizinis asmuo yra būklėje, dėl kurios jis negalėtų veikti juridinio asmens vardu.
Pakankamas	Žemo lygio 3 punkto, be to: 1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas pakankamu arba aukštu lygiu.

Saugumo užtikrinimo lygis	Būtini elementai
	2. Susiejimas nustatytas remiantis nacionaliniu lygiu pripažintomis procedūromis, kurį atlikus susiejimas įregistruotas autoritetingame šaltinyje. 3. Susiejimas buvo patikrintas remiantis autoritetingo šaltinio informacija.
Aukštas	Žemo lygio 3 punkto ir pakankamo lygio 2 punkto, be to: 1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas aukštu lygiu. 2. Susiejimas patikrintas remiantis nacionalinėje aplinkoje naudojamu unikaliu identifikatoriumi, susijusiu su juridiniu asmeniu, taip pat remiantis autoritetingo šaltinio informacija, kuria nurodomas konkretus fizinis asmuo.

2.2. *Elektroninės atpažinties priemonių valdymas*

2.2.1. Elektroninės atpažinties priemonių savybės ir struktūra

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Elektroninės atpažinties priemonėje naudojamas bent vienas tapatumo nustatymo veiksnys. 2. Elektroninės atpažinties priemonė sukurta taip, kad išdavėjas imtųsi pagrįstų veiksmų patikrinti, kad tik asmuo, kuriam ji priklauso, galėtų ją kontroliuoti arba turėti.
Pakankamas	1. Elektroninės atpažinties priemonėje naudojami bent du skirtingų kategorijų tapatumo nustatymo veiksniai. 2. Elektroninės atpažinties priemonė sukurta taip, kad galima būtų laikyti, kad ją gali naudoti tik asmuo, kuriam ji priklauso, ir kuris ją kontroliuoja arba turi.
Aukštas	Pakankamo lygio, be to: 1. Elektroninės atpažinties priemonė apsaugo nuo kopijavimo ir klastojimo, taip pat nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu. 2. Elektroninės atpažinties priemonė sukurta taip, kad asmuo, kuriam ji priklauso, ją galėtų patikimai apsaugoti nuo kitų asmenų naudojimo.

2.2.2. Išdavimas, pristatymas ir aktyvavimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Išduota elektroninės atpažinties priemonė pristatoma naudojant mechanizmą, kuriuo galima laikyti, kad ji pasiekė tik tą asmenį, kuriam ji numatyta.
Pakankamas	Išduota elektroninės atpažinties priemonė pristatoma naudojant mechanizmą, kuriuo galima laikyti, kad ji pristatyta tik tam asmeniui, kuriam ji priklauso.
Aukštas	Aktyvavimo procesu patvirtinama, kad elektroninės atpažinties priemonė buvo pristatyta tik tam asmeniui, kuriam ji priklauso.

2.2.3. Sustabdymas, atšaukimas ir pakartotinis aktyvavimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Elektroninės atpažinties priemonių galiojimą galima laiku ir veiksmingai sustabdyti ir (arba) jas atšaukti. 2. Imtasi priemonių siekiant užkirsti kelią neteisėtam galiojimo sustabdymui, atšaukimui ir (arba) pakartotinam aktyvavimui. 3. Pakartotinis aktyvavimas galimas tik jeigu toliau atitinkami tie patys iki galiojimo sustabdymo arba atšaukimo nustatyti patikimumo užtikrinimo reikalavimai.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.2.4. Atnaujinimas ir pakeitimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, atnaujinimui arba pakeitimui turi būti keliami tokie patys saugumo užtikrinimo reikalavimai kaip pradiniam tapatybės įrodymo nustatymui ir tikrinimui, arba atnaujinimas ar pakeitimas turi būti pagrįstas tokio paties arba aukštesnio patikimumo lygio galiojančiomis elektroninės atpažinties priemonėmis.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Žemo lygio, be to: kai atnaujinimas ar pakeitimas pagrįstas galiojančiomis elektroninės atpažinties priemonėmis, tapatybės duomenys tikrinami su autoritetingu šaltiniu.

2.3. *Tapatumo nustatymas*

Šiame skirsnyje daugiausia dėmesio skiriama grėsmėms, susijusioms su tapatumo nustatymo mechanizmu, ir išvardijami kiekvieno saugumo užtikrinimo lygio reikalavimai. Šiame skirsnyje laikoma, kad kontrolės priemonės atitinka tam tikro lygio riziką.

2.3.1. Tapatumo nustatymo mechanizmas

Šioje lentelėje pateikti tapatumo nustatymo mechanizmo, pagal kurį fizinis arba juridinis asmuo naudojasi elektroninės atpažinties priemone, kad patvirtintų savo tapatybę pasikliaujančiajai šaliai, kiekvieno saugumo užtikrinimo lygio reikalavimai.

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Prieš pateikiant asmens tapatybės duomenis patikimai tikrinama elektroninės atpažinties priemonė ir jos galiojimas. 2. Jeigu pagal tapatumo nustatymo mechanizmą turi būti saugomi asmens tapatybės duomenys, ta informacija apsaugoma, siekiant ją apsaugoti nuo praradimo ir pažeidimo, įskaitant analizavimą neprisijungus prie interneto. 3. Tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su baziniu sustiprintu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.

Saugumo užtikrinimo lygis	Būtini elementai
Pakankamas	Žemo lygio, be to: 1. prieš pateikiant asmens tapatybės duomenis, vykdant dinaminį tapatumo nustatymą patikimai tikrinama elektroninės atpažinties priemonė ir jos galiojimas. 2. Tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su vidutiniu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.
Aukštas	Pakankamo lygio, be to: tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su dideliu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.

2.4. *Valdymas ir organizavimas*

Visi dalyviai, teikiantys paslaugą, susijusią su tarpvalstybinio lygmens elektronine atpažintimi (toliau – teikėjai), turi būti nustatę dokumentais patvirtintą informacijos saugumo valdymo praktiką, politikos priemones, rizikos valdymo metodus ir kitas pripažintas kontrolės priemones, kad atitinkamų valstybių narių elektroninės atpažinties schemų valdymo organams galėtų garantuoti, jog įdiegta veiksminga praktika. 2.4 skirsnyje laikoma, kad visi reikalavimai/elementai atitinka tam tikro lygio riziką.

2.4.1. Bendrosios nuostatos

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Paslaugų teikėjai, teikiantys bet kokią paslaugą, kuriai taikomas šis reglamentas, yra valdžios institucija ar juridinis subjektas, tokiu pripažįstamas pagal valstybės narės nacionalinę teisę; jie turi nustatytą struktūrą ir visapusiškai veikia visose su paslaugų teikimu susijusiose srityse. 2. Paslaugų teikėjai laikosi visų jiems tenkančių teisinių reikalavimų, susijusių su paslaugos valdymu ir teikimu, įskaitant reikalavimus, susijusius su informacija, kurios gali būti prašoma, tapatybės įrodymo nustatymu, su tuo, kokia informacija gali būti saugoma ir kiek laiko. 3. Paslaugų teikėjai gali įrodyti savo gebėjimą prisiimti atsakomybės už žalą riziką, taip pat turėt pakankamų finansinių išteklių tęsti veiklą ir teikti paslaugas. 4. Paslaugų teikėjai yra atsakingi už bet kokių kitam subjektui perduotų savo įsipareigojimų vykdymą ir turi laikytis schemos politikos nuostatų taip, tarsi tas pareigas būtų įvykdę patys paslaugų teikėjai. 5. Elektroninės atpažinties schemose, kurios nesukurtos pagal nacionalinę teisę, turi būti numatytas veiksmingas nutraukimo planas. Tokiame plane turi būti numatyta, kokia tvarka nutraukti paslaugą arba jos tęsimą paskirti kitam paslaugų teikėjui, kaip atitinkamos valdžios institucijos ir galutiniai naudotojai turi būti informuojami ir kaip pagal schemos politiką įrašai turi būti saugomi, laikomi ir sunaikinami.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.2. Paskelbti pranešimai ir informacija naudotojams

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Paskelbta paslaugos apibrėžtis, kurioje pateikti visi taikomi terminai, sąlygos ir mokesčiai, įskaitant bet kokius naudojimosi ja apribojimus. Paslaugos apibrėžtyje turi būti nustatytos privatumo taisyklės. 2. Turi būti nustatytos tinkamos politikos nuostatos ir procedūros siekiant užtikrinti, kad paslaugos naudotojams būtų laiku ir patikimu būdu pranešta apie bet kokius paslaugos apibrėžties ir taikomų terminų, sąlygų ir privatumo taisyklių pasikeitimus. 3. Turi būti nustatytos tinkamos politikos nuostatos ir procedūros, pagal kurias būtų visapusiškai ir deramai atsakoma į prašymus pateikti informacijos.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.3. Informacijos saugumo valdymas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Veikia veiksminga informacijos saugumo valdymo sistema, skirta informacijos saugumo rizikai valdyti ir kontroliuoti.
Pakankamas	Žemo lygio, be to: informacijos saugumo valdymo sistemoje laikomasi pasiteisinusių standartų arba principų, skirtų informacijos saugumo rizikai valdyti ir kontroliuoti.
Aukštas	Tokie patys, kaip pakankamo lygio.

2.4.4. Įrašų saugojimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Registruoti ir išlaikyti atitinkamą informaciją naudojant veiksmingą įrašų valdymo sistemą, atsižvelgiant į taikomus teisės aktus ir gerąją praktiką, susijusius su duomenų apsauga ir saugojimu. 2. Laikyti informaciją, kiek tai leidžiama pagal nacionalinę teisę arba kitą nacionalinę administracinę tvarką, ir apsaugoti bei išsaugoti duomenis tiek, kiek būtina siekiant atlikti auditą ir saugumo pažeidimų tyrimus; po to duomenys turi būti saugiai sunaikinti.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.5. Įrenginiai ir darbuotojai

Šioje lentelėje pateikiami reikalavimai įrenginiams, darbuotojams ir (jei taikytina) subrangovams, kurie vykdo pareigas pagal šį reglamentą. Atitiktis kiekvienam reikalavimui turi būti proporcinga rizikos laipsniui, susijusiam su nustatytu saugumo užtikrinimo lygiu.

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Įdiegtos procedūros, kuriomis užtikrinama, kad darbuotojai ir subrangovai būtų pakankamai išmokyti, būtų kvalifikuoti ir turėtų patirties, reikalingos vykdant atitinkamas funkcijas. 2. Yra pakankamai darbuotojų ir subrangovų, galinčių tinkamai vykdyti paslaugą ir suteikti išteklių pagal jos politiką ir procedūras. 3. Įrenginiai, naudojami teikiant paslaugą, yra nuolat stebimi ir apsaugo nuo aplinkos įvykių daromos žalos, neleistinos prieigos ir kitų veiksnių, kurie gali paveikti paslaugos saugumą. 4. Įrenginiai, naudojami teikiant paslaugą, užtikrina, kad patekti į zonas, kuriose laikoma arba tvarkoma asmens, kriptografinė ar kita neskelbtina informacija, galėtų tik įgalioti darbuotojai ar subrangovai.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.6. Techninė kontrolė

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Veikia proporcingos techninės kontrolės priemonės, skirtos paslaugų saugumui kylančiai rizikai valdyti ir tvarkomos informacijos konfidencialumui, vientisumui ir prieinamumui apsaugoti. 2. Elektroninių ryšių kanalai, naudojami keistis asmens arba neskelbtina informacija, yra apsaugoti nuo pasiklausymo, keitimo ir pakartotino išklausymo. 3. Prieiga prie neskelbtinos kriptografinės medžiagos, jeigu ji naudojama elektroninės atpažinties priemonėms išduoti ir tapatumui nustatyti, suteikiama tik toms funkcijoms ir taikomosioms programoms, kurioms prieiga yra būtina. Turi būti užtikrinta, kad tokia medžiaga niekada nebūtų nuolat saugoma paprasto teksto pavidalu. 4. Veikia procedūros, kuriomis užtikrinama, kad saugumas būtų nuolat išlaikytas ir kad būtų sugebama reaguoti į rizikos lygių pokyčius, incidentus ir saugumo pažeidimus. 5. Visos laikmenos, kuriose laikoma asmens, kriptografinė ar kita neskelbtina informacija, saugomos, transportuojamos ir šalinamos saugiai ir patikimai.
Pakankamas	Tokie patys, kaip žemo lygio, be to: neskelbtina kriptografinė medžiaga, jeigu ji naudojama elektroninės atpažinties priemonėms išduoti ir tapatumui nustatyti, yra apsaugota nuo klastojimo.
Aukštas	Tokie patys, kaip pakankamo lygio.

2.4.7. Atitiktis ir auditas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Periodiškai vykdomas vidaus auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų.

Saugumo užtikrinimo lygis	Būtini elementai
Pakankamas	Periodiškai vykdomas nepriklausomas vidaus arba išorės auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų.
Aukštas	1. Periodiškai vykdomas nepriklausomas išorės auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų. 2. Tais atvejais, kai schemą tiesiogiai valdo valdžios institucija, ji tikrinama pagal nacionalinę teisę.

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2015/1503

2015 m. rugsėjo 8 d.

kuriuo nustatomos standartinės importo vertės, skirtos tam tikrų vaisių ir daržovių įvežimo kainai nustatyti

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1308//2013, kuriuo nustatomas bendras žemės ūkio produktų rinkų organizavimas ir panaikinami Tarybos reglamentai (EEB) Nr. 922/72, (EEB) Nr. 234/79, (EB) Nr. 1037/2001 ir (EB) Nr. 1234/2007 ([1]),

atsižvelgdama į 2011 m. birželio 7 d. Komisijos įgyvendinimo reglamentą (ES) Nr. 543/2011, kuriuo nustatomos išsamios Tarybos reglamento (EB) Nr. 1234/2007 taikymo vaisių bei daržovių ir perdirbtų vaisių bei daržovių sektoriuose taisyklės ([2]), ypač į jo 136 straipsnio 1 dalį,

kadangi:

(1) Įgyvendinimo reglamentu (ES) Nr. 543/2011, atsižvelgiant į daugiašalių derybų dėl prekybos Urugvajaus raunde rezultatus, nustatomi kriterijai, pagal kuriuos Komisija nustato standartines importo iš trečiųjų šalių vertes produktams ir laikotarpiams, nurodytiems jo XVI priedo A dalyje;

(2) remiantis Įgyvendinimo reglamento (ES) Nr. 543/2011 136 straipsnio 1 dalimi, standartinė importo vertė apskaičiuojama kiekvieną darbo dieną atsižvelgiant į kintančius kasdienius duomenis. Todėl šis reglamentas turėtų įsigalioti jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Įgyvendinimo reglamento (ES) Nr. 543/2011 136 straipsnyje minimos standartinės importo vertės yra nustatytos šio reglamento priede.

2 straipsnis

Šis reglamentas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

Šis reglamentas yra privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2015 m. rugsėjo 8 d.

Komisijos vardu

Pirmininko pavedimu

Jerzy PLEWA

Žemės ūkio ir kaimo plėtros generalinis direktorius

([1]) OL L 347, 2013 12 20, p. 671.
([2]) OL L 157, 2011 6 15, p. 1.

PRIEDAS

Standartinės importo vertės, skirtos kai kurių vaisių ir daržovių įvežimo kainai nustatyti

(EUR/100 kg)

KN kodas	Trečiosios šalies kodas ([1])	Standartinė importo vertė
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

KN kodas	Trečiosios šalies kodas (1)	Standartinė importo vertė
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Šalių nomenklatūra nustatyta 2012 m. lapkričio 27 d. Komisijos reglamentu (ES) Nr. 1106/2012, kuriuo dėl šalių ir teritorijų nomenklatūros atnaujinimo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 471/2009 dėl Bendrijos statistikos, susijusios su išorės prekyba su ES nepriklausančiomis šalimis (OL L 328, 2012 11 28, p. 7). Kodas „ZZ“ atitinka „kitas šalis“.

SPRENDIMAI

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2015/1504

2015 m. rugsėjo 7 d.

kuriuo tam tikroms valstybėms narėms leidžiama taikyti nukrypti leidžiančias nuostatas dėl statistinių duomenų perdavimo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 1099/2008 dėl energetikos statistikos

(pranešta dokumentu Nr. C(2015) 6105)

(Tekstas autentiškas tik estų, graikų, prancūzų, nyderlandų ir slovakų kalbomis)

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2008 m. spalio 22 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 1099/2008 dėl energetikos statistikos ([1]), ypač į jo 5 straipsnio 4 dalį ir 10 straipsnio 2 dalį,

kadangi:

(1) pagal Reglamento (EB) Nr. 1099/2008 5 straipsnio 4 dalį gavus tinkamai pagrįstą valstybės narės prašymą jai gali būti leista taikyti leidžiančias nukrypti nuostatas dėl tų nacionalinių statistinių duomenų, kuriuos renkant respondentams tektų pernelyg didelė našta;

(2) Belgija, Estija, Kipras ir Slovakija pateikė prašymus, kad joms būtų leista taikyti nukrypti leidžiančias nuostatas dėl namų ūkių išsamaus energijos suvartojimo pagal galutinio vartojimo rūšį statistinių duomenų teikimo tam tikrais ataskaitiniais metais;

(3) pagal tų valstybių narių pateiktą informaciją leidimas taikyti tokias nukrypti leidžiančias nuostatas pateisinamas ir turėtų būti suteiktas;

(4) šiame sprendime nustatytos priemonės atitinka Europos statistikos sistemos komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Leidžiama taikyti toliau nurodytas nuo Reglamento (EB) Nr. 1099/2008 leidžiančias nukrypti nuostatas:

1. Belgijai leidžiama taikyti nukrypti leidžiančią nuostatą ir neteikti 2015 ataskaitinių metų rezultatų, susijusių su B priedo 1.2.3 punkto 4.2.1–4.2.5 papunkčiais, 2.2.3 punkto 4.2.1–4.2.5 papunkčiais, 3.2.3 punkto 3.1–3.6 papunkčiais, 4.2.3 punkto 7.2.1–7.2.5 papunkčiais ir 5.2.4 punkto 4.2.1–4.2.5 papunkčiais, kiek tai susiję su namų ūkių išsamaus energijos suvartojimo pagal galutinio vartojimo rūšį (kaip apibrėžta A priedo 2.3 punkto 26 papunktyje „Kiti sektoriai – gyvenamųjų būstų“) statistiniais duomenimis.

([1]) OL L 304, 2008 11 14, p. 1.

2. Estijai leidžiama taikyti nukrypti leidžiančią nuostatą ir neteikti 2015, 2016 ir 2017 ataskaitinių metų rezultatų, susijusių su B priedo 1.2.3 punkto 4.2.1–4.2.5 papunkčiais, 2.2.3 punkto 4.2.1–4.2.5 papunkčiais, 3.2.3 punkto 3.1–3.6 papunkčiais, 4.2.3 punkto 7.2.1–7.2.5 papunkčiais ir 5.2.4 punkto 4.2.1–4.2.5 papunkčiais, kiek tai susiję su namų ūkių išsamaus energijos suvartojimo pagal galutinio vartojimo rūšį (kaip apibrėžta A priedo 2.3 punkto 26 papunktyje „Kiti sektoriai – gyvenamųjų būstų“) statistiniais duomenimis.

3. Kiprui leidžiama taikyti nukrypti leidžiančią nuostatą ir neteikti 2015, 2016 ir 2017 ataskaitinių metų rezultatų, susijusių su B priedo 1.2.3 punkto 4.2.1–4.2.5 papunkčiais, 2.2.3 punkto 4.2.1–4.2.5 papunkčiais, 3.2.3 punkto 3.1–3.6 papunkčiais ir 5.2.4 punkto 4.2.1–4.2.5 papunkčiais, kiek tai susiję su namų ūkių išsamaus energijos suvartojimo pagal galutinio vartojimo rūšį (kaip apibrėžta A priedo 2.3 punkto 26 papunktyje „Kiti sektoriai – gyvenamųjų būstų“) statistiniais duomenimis.

4. Slovakijai leidžiama taikyti nukrypti leidžiančią nuostatą ir neteikti 2015 ir 2016 ataskaitinių metų rezultatų, susijusių su B priedo 1.2.3 punkto 4.2.1–4.2.5 papunkčiais, 2.2.3 punkto 4.2.1–4.2.5 papunkčiais, 3.2.3 punkto 3.1–3.6 papunkčiais, 4.2.3 punkto 7.2.1–7.2.5 papunkčiais ir 5.2.4 punkto 4.2.1–4.2.5 papunkčiais, kiek tai susiję su namų ūkių išsamaus energijos suvartojimo pagal galutinio vartojimo rūšį (kaip apibrėžta A priedo 2.3 punkto 26 papunktyje „Kiti sektoriai – gyvenamųjų būstų“) statistiniais duomenimis.

2 straipsnis

Šis sprendimas skirtas Belgijos Karalystei, Estijos Respublikai, Kipro Respublikai ir Slovakijos Respublikai.

Priimta Briuselyje 2015 m. rugsėjo 7 d.

Komisijos vardu

Marianne THYSSEN

Komisijos narė

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2015/1505

2015 m. rugsėjo 8 d.

kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 22 straipsnio 5 dalį nustatomos patikimų sąrašų techninės specifikacijos ir formatai

(Tekstas svarbus EEE)

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 22 straipsnio 5 dalį,

kadangi:

(1) patikimi sąrašai yra labai svarbūs tam, kad rinkos dalyviai įgytų tarpusavio pasitikėjimą, nes juose, atliekant priežiūrą, nurodomas paslaugos teikėjo statusas;

(2) tarpvalstybinis elektroninių parašų naudojimas buvo palengvintas Komisijos sprendimu 2009/767/EB ([2]), kuriuo nustatyta valstybių narių pareiga sudaryti, tvarkyti ir skelbti patikimus sąrašus, kuriuose pateikta informacija apie valstybių narių prižiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, pagal Europos Parlamento ir Tarybos direktyvą 1999/93/EB ([3]) visuomenei išduodančius kvalifikuotus sertifikatus;

(3) Reglamento (ES) Nr. 910/2014/ES 22 straipsnyje nustatyta valstybių narių pareiga sudaryti, tvarkyti ir saugiai skelbti elektroniniu būdu pasirašytus arba užantspauduotus patikimus sąrašus tokia forma, kad juos būtų galima tvarkyti automatizuotomis priemonėmis, ir pranešti Komisijai apie įstaigas, atsakingas už nacionalinių patikimų sąrašų sudarymą;

(4) patikimumo užtikrinimo paslaugų teikėjas ir jo teikiamos patikimumo užtikrinimo paslaugos turėtų būti laikomi kvalifikuotais, jei kvalifikacijos statusas yra susijęs su į patikimą sąrašą įrašytu paslaugų teikėju. Siekiant užtikrinti, kad paslaugų teikėjai galėtų lengvai nuotoliniu būdu ir elektroninėmis priemonėmis įvykdyti kitus įsipareigojimus, nustatytus Reglamente (ES) Nr. 910/2014, visų pirma jo 27 ir 37 straipsniuose, ir siekiant patenkinti teisėtus sertifikavimo paslaugų teikėjų, kurie neišduoda kvalifikuotų sertifikatų, bet teikia paslaugas, susijusias su elektroniniais parašais, pagal Direktyvą 1999/93/EB ir yra įtraukti į sąrašą iki 2016 m. birželio 30 d., lūkesčius, valstybėms narėms turėtų būti suteikta galimybė savanoriškai nacionaliniu lygiu į patikimus sąrašus įtraukti kitas nei kvalifikuotas patikimumo užtikrinimo paslaugas, su sąlyga, kad aiškiai nurodoma, jog jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;

(5) pagal Reglamento (ES) Nr. 910/2014 25 konstatuojamąją dalį valstybės narės gali įtraukti kitų rūšių nacionaliniu lygiu nustatytas patikimumo užtikrinimo paslaugas, nei nustatytas Reglamento (ES) Nr. 910/2014 3 straipsnio 16 dalyje, su sąlyga, kad aiškiai nurodoma, jog jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;

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

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Valstybės narės sudaro, skelbia ir tvarko patikimus sąrašus, į kuriuos įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos jos prižiūri, ir informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas. Tie sąrašai turi atitikti I priede nustatytas technines specifikacijas.

([1]) OL L 257, 2014 8 28, p. 73.

([2]) 2009 m. spalio 16 d. Komisijos sprendimas 2009/767/EB, kuriuo pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje nustatomos priemonės procedūroms, atliekamoms naudojantis elektroninėmis priemonėmis ir kontaktinių centrų paslaugomis, palengvinti (OL L 274, 2009 10 20, p. 36).

([3]) 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (OL L 13, 2000 1 19, p. 12).

2 straipsnis

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nekvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, taip pat informaciją apie jų teikiamas nekvalifikuotas patikimumo užtikrinimo paslaugas. Sąraše turi būti aiškiai nurodyta, kurie patikimumo užtikrinimo paslaugų teikėjai yra nekvalifikuoti ir kurios jų teikiamos patikimumo užtikrinimo paslaugos yra nekvalifikuotos.

3 straipsnis

1. Pagal Reglamento (ES) Nr. 910/2014 22 straipsnio 2 dalį valstybės narės elektroniniu būdu pasirašo arba užantspauduoja patikimus sąrašus tokia forma, kad juos būtų galima tvarkyti automatizuotomis priemonėmis, remiantis I priede nustatytomis techninėmis specifikacijomis.

2. Jei valstybė narė elektroniniu būdu skelbia žmonėms suprantamos formos patikimą sąrašą, ji užtikrina, kad šios formos patikimame sąraše būtų pateikti tie patys duomenys kaip ir formos, kurią galima tvarkyti automatizuotomis priemonėmis, ir pasirašo arba užantspauduoja ją elektroniniu būdu, remdamasi I priede nustatytomis techninėmis specifikacijomis.

4 straipsnis

1. Valstybės narės pateikia Komisijai Reglamento (ES) Nr. 910/2014 22 straipsnio 3 dalyje nurodytą informaciją, naudodamos II priede pateiktą formą.

2. 1 dalyje nurodyta informacija apima du ar daugiau schemos operatoriaus viešojo rakto sertifikatų, kurių perkeltas galiojimo laikotarpis ne trumpesnis nei trys mėnesiai, atitinkančių privačius raktus, kurie gali būti naudojami siekiant elektroniniu būdu pasirašyti arba užantspauduoti patikimo sąrašo formą, kurią galima tvarkyti automatizuotomis priemonėmis, o kai jis paskelbtas – žmonėms suprantamą formą.

3. Pagal Reglamento (ES) Nr. 910/2014 22 straipsnio 4 dalį Komisija saugiu prieigos prie patvirtinto žiniatinklio serverio kanalu visuomenei pateikia 1 ir 2 dalyse numatytą, kaip pranešta valstybių narių, pasirašytą arba užantspauduotą informaciją tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.

4. Komisija saugiu prieigos prie patvirtinto žiniatinklio serverio kanalu visuomenei gali pateikti 1 ir 2 dalyse numatytą, kaip pranešta valstybių narių, pasirašytą arba užantspauduotą informaciją žmonėms suprantama forma.

5 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis sprendimas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2015 m. rugsėjo 8 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

I PRIEDAS

PATIKIMŲ SĄRAŠŲ BENDROSIOS FORMOS TECHNINĖS SPECIFIKACIJOS

I SKYRIUS

BENDRIEJI REIKALAVIMAI

Patikimuose sąrašuose pateikiama tiek dabartinė, tiek visa ankstesnė informacija apie į sąrašą įtrauktų patikimumo užtikrinimo paslaugų statusą nuo patikimumo užtikrinimo paslaugų teikėjo įtraukimo į patikimus sąrašus.

Sąvokos „patvirtinti“, „akredituoti“ ir (arba) „prižiūrimi“ šiose specifikacijose taip pat apima nacionalines patvirtinimo schemas, tačiau valstybės narės savo patikimame sąraše teiks papildomą informaciją apie bet kokių tokių nacionalinių schemų pobūdį, įskaitant galimų skirtumų nuo priežiūros schemų, taikomų kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms, paaiškinimą.

Informacija, pateikta patikimame sąraše, visų pirma skirta padėti tvirtinti kvalifikuotų patikimumo užtikrinimo paslaugų ženklus, t. y. fizinius arba dvejetainius (loginius) objektus, sukurtus arba išduotus teikiant kvalifikuotą patikimumo užtikrinimo paslaugą, pvz., kvalifikuotus elektroninius parašus/spaudus; pažangiuosius elektroninius parašus/spaudus, patvirtintus kvalifikuotu sertifikatu; kvalifikuotas laiko žymas; kvalifikuotus elektroninio pristatymo įrodymus ir kt.

II SKYRIUS

PATIKIMŲ SĄRAŠŲ BENDROSIOS FORMOS IŠSAMIOS SPECIFIKACIJOS

Šios specifikacijos pagrįstos specifikacijomis ir reikalavimais, nustatytais ETSI TS 119 612 v2.1.1 (toliau – ETSI TS 119 612).

Jeigu šiose specifikacijose konkretus reikalavimas nenurodytas, taikomi visi ETSI TS 119 612 5 ir 6 punktuose nustatyti reikalavimai. Jeigu šiose specifikacijose pateikti konkretūs reikalavimai, jiems teikiama pirmenybė prieš atitinkamus ETSI TS 119 612 nustatytus reikalavimus. Jei šios specifikacijos prieštarauja ETSI TS 119 612 specifikacijoms, pirmenybė teikiama šioms specifikacijoms.

Schemos pavadinimas (5.3.6 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.6 punkte nustatytas specifikacijas, pagal kurias schemai pavadinti turi būti naudojamas toks pavadinimas:

„EN_name_value“ = „Patikimas sąrašas, į kurį įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos prižiūri išduodančioji valstybė narė, taip pat informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas, laikantis atitinkamų nuostatų, nustatytų 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB“.

Schemos informacijos UII (5.3.7 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.7 punkte nustatytas specifikacijas, pagal kurias į tinkamą schemos informaciją turi būti įtraukta bent ši informacija:

a) visoms valstybėms narėms vienoda įvadinė informacija apie patikimo sąrašo taikymo sritį ir aplinkybes, pamatinę priežiūros schemą ir, kai taikytina, nacionalinę (-es) patvirtinimo (pvz., akreditacijos) schemą (-as). Bendras naudotinas tekstas – jame rašmenų eilutė „[*atitinkamos valstybės narės pavadinimas*]“ turi būti pakeista atitinkamos valstybės narės pavadinimu – yra toks:

> „Šis sąrašas – tai patikimas sąrašas, į kurį įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos prižiūri *[atitinkamos valstybės narės pavadinimas]*, taip pat informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas, laikantis atitinkamų nuostatų, nustatytų 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

Tarpvalstybinis elektroninių parašų naudojimas palengvintas 2009 m. spalio 16 d. Komisijos sprendimu 2009/767/EB, kuriuo nustatyta valstybių narių pareiga sudaryti, tvarkyti ir skelbti patikimus sąrašus, kuriuose būtų pateikta informacija apie valstybių narių prižiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, išduodančius kvalifikuotus sertifikatus pagal 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos visuomenei. Šis patikimas sąrašas – tai Sprendimu 2009/767/EB nustatyto patikimo sąrašo tęsinys."

Patikimi sąrašai yra labai svarbūs didinant pasitikėjimą tarp elektroninės rinkos operatorių, nes leidžia vartotojams nustatyti patikimumo užtikrinimo paslaugų teikėjų ir jų teikiamų paslaugų kvalifikacijos statusą ir statuso istoriją.

Valstybių narių patikimuose sąrašuose pateikiama bent jau informacija, nurodyta Komisijos įgyvendinimo sprendimo (ES) 2015/1505 1 ir 2 straipsniuose.

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nekvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, taip pat informaciją apie jų teikiamas nekvalifikuotas patikimumo užtikrinimo paslaugas. Turi būti aiškiai nurodyta, kad teikėjai ir paslaugos yra nekvalifikuoti pagal Reglamentą (ES) Nr. 910/2014.

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nacionaliniu lygiu apibrėžtas kitų rūšių, nei nustatytos Reglamento (ES) Nr. 910/2014 3 straipsnio 16 dalyje, patikimumo užtikrinimo paslaugas. Turi būti aiškiai nurodyta, kad jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;

b) specifinė informacija apie pamatinę priežiūros schemą ir, kai taikoma, nacionalinę (-es) patvirtinimo (pvz., akreditacijos) schemą (-as), visų pirma ([1]):

1) informacija apie nacionalinę priežiūros sistemą, taikomą kvalifikuotų ir nekvalifikuotų patikimumo užtikrinimo paslaugų teikėjams ir kvalifikuotoms ir nekvalifikuotoms patikimumo užtikrinimo paslaugoms, kaip numatyta Reglamente (ES) Nr. 910/2014;

2) atitinkamais atvejais informacija apie nacionalines savanoriškos akreditacijos schemas, taikomas sertifikavimo paslaugų teikėjams, kurie išdavė kvalifikuotus sertifikatus pagal Direktyvą 1999/93/EB.

Teikiant šią specifinę informaciją apie kiekvieną nurodytą pamatinę schemą turi būti pateikta bent tokia informacija:

1) bendras aprašas;

2) informacija apie nacionalinės priežiūros sistemos procesą ir atitinkamais atvejais patvirtinimo pagal nacionalinę patvirtinimo schemą procesą;

3) informacija apie kriterijus, pagal kuriuos vykdoma patikimumo užtikrinimo paslaugų teikėjų priežiūra arba atitinkamais atvejais jie yra patvirtinami;

4) informacija apie kriterijus ir taisykles, taikomus prižiūrėtojams ir (arba) auditoriams atrinkti ir nustatyti, kaip jie turi vertinti patikimumo užtikrinimo paslaugų teikėjus ir jų teikiamas patikimumo užtikrinimo paslaugas;

5) atitinkamais atvejais kita informacija ryšiams ir bendra informacija apie schemos veikimą.

Schemos tipas, naudotojai ir (arba) taisyklės (5.3.9 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.9 punkte nustatytas specifikacijas.

Jame turi būti pateikti tik UII Jungtinės Karalystės anglų kalba.

([1]) Šie informacijos rinkiniai yra ypač svarbūs, kad susijusios šalys galėtų įvertinti tokių sistemų kokybę ir saugumą. Tie informacijos rinkiniai teikiami patikimo sąrašo lygmeniu naudojant šį lauką „Schemos informacijos UII" (5.3.7 punktas – informaciją teikia valstybės narės), „Schemos tipas, naudotojai ir (arba) taisyklės" (5.3.9 punktas – naudojamas visoms valstybėms narėms bendras tekstas) ir „PUPSS politika ir (arba) teisinė informacija" (5.3.11 punktas – visoms valstybėms narėms bendras tekstas; be to, kiekviena valstybė narė gali pateikti papildomą jai svarbų tekstą ir (arba) nuorodų). Kai reikia ir reikalaujama, paslaugos lygmeniu naudojant lauką „Pagal schemą teikiamos paslaugos apibrėžties UII" (5.5.6 punktas) gali būti teikiama papildoma informacija apie tokias nekvalifikuotų patikimumo užtikrinimo paslaugų irnacionaliniu mastu nustatytų (kvalifikuotų) patikimumo užtikrinimo paslaugų sistemas (pvz., norint išskirti keletą kokybės ir (arba) saugumo lygmenų).

Jame turi būti pateikti bent du UII:

1) visų valstybių narių patikimiems sąrašams bendras UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas visiems patikimiems sąrašams:

UII: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Aprašomasis tekstas:

„Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (ES) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (ES) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (ES) No 910/2014 are as follows:

The „qualified" status of a trust service is indicated by the combination of the „Service type identifier" („Sti") value in a service entry and the status according to the „Service current status" field value as from the date indicated in the „Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A „CA/QC" „Service type identifier" („Sti") entry (possibly further qualified as being a „RootCA-QC" through the use of the appropriate „Service information extension" („Sie") additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the „Service digital identifier" („Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. „undersupervision", „supervisionincessation", „accredited" or „granted") for that entry.

— **and IF**„Sie" „Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of „Sie" „Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the „SSCD support" and/or „Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific „Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, ir t. t.). These qualifiers are part of the following set of „Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — „QCStatement" meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

    — „QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

    — „QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

    — „QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — „NotQualified" meaning the identified certificate(s) is(are) not to be considered as qualified; And/or

  — to indicate the nature of the SSCD support:

    — „QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — „QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — „QCSSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — „QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — „QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — „QCQSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — „QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; And/or

— to indicate issuance to Legal Person:

— „QCForLegalPerson“ meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no „Sie“ „Qualifications Extension“ information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a „QCStatement“ qualifier, or

— an „Sie“ „Qualifications Extension“ information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a „NotQualified“ qualifier,

then the certificate is not to be considered as qualified.

„Service digital identifiers“ are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other „Sti“ type entry is that, for that „Sti“ identified service type, the listed service named according to the „Service name“ field value and uniquely identified by the „Service digital identity“ field value has the current qualified or approval status according to the „Service current status“ field value as from the date indicated in the „Current status starting date and time“.

Specific interpretation rules for any additional information with regard to a listed service (e.g. „Service information extensions“ field) may be found, when applicable, in the Member State specific URI as part of the present „Scheme type/community/rules“ field.

Please refer to the applicable secondary legislation pursuant to Regulation (ES) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.“

2) specifinis kiekvienos valstybės narės patikimo sąrašo UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas šios valstybės narės patikimam sąrašui:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, CC – ISO 3166-1 ([1]) dviejų raidžių šalies kodas, nurodytas lauke „Schemos teritorija“ (5.3.10 punktas).

— šiame tekste naudotojai gali rasti informacijos apie specifinę nurodytos valstybės narės politiką ir (arba) taisykles, pagal kurias, laikantis tos valstybės narės priežiūros režimo ir, kai taikytina, patvirtinimo schemos, vertinamos į sąrašą įtrauktos patikimos paslaugos,

— šiame tekste naudotojai gali rasti specifinį nurodytos valstybės narės aprašą, kaip naudoti ir aiškinti patikimo sąrašo turinį, susijusį su į sąrašą įtrauktomis nekvalifikuotomis patikimumo užtikrinimo paslaugomis ir (arba) nacionaliniu lygiu nustatytomis patikimumo užtikrinimo paslaugomis. Šis tekstas gali būti naudojamas galimam nacionalinių patvirtinimo sistemų, susijusių su kvalifikuotų sertifikatų neišduodančiais sertifikavimo paslaugų teikėjais, hierarchijos lygiui nurodyti, taip pat nurodyti, kaip šiuo tikslu naudojami laukai „Pagal schemą teikiamos paslaugos apibrėžties UII“ (5.5.6 punktas) ir „Informacijos apie paslaugą plėtinys“ (5.5.9 punktas).

Valstybės narės, praplėsdamos minėtą specifinį valstybės narės UII, GALI nustatyti ir naudoti papildomus UII (t. y. UII, nustatomus remiantis šiuo specifiniu hierarchiniu UII).

Informacija apie PUPSS politiką ir (arba) teisinė informacija (5.3.11 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.11 punkte nustatytas specifikacijas, pagal kurias informacija apie politiką ir (arba) teisinė informacija apie teisinį schemos statusą arba teisinius reikalavimus, kuriuos schema turi atitikti atsižvelgiant į jurisdikciją, pagal kurią taikoma ši schema, ir (arba) visus apribojimus ir sąlygas, pagal kuriuos

([1]) ISO 3166-1:2006: „Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių kodai“

patikimas sąrašas yra tvarkomas ir skelbiamas, turi būti įvairiakalbių rašmenų eilučių seka (žr. 5.1.4 punktą), pateikiant (privaloma kalba – Jungtinės Karalystės anglų kalba ir pasirinktinai viena arba daugiau nacionalinių kalbų) bet kokios tokios informacijos apie politiką ar teisinės informacijos faktinį tekstą, sudarytą iš:

1) visų valstybių narių patikimiems sąrašams bendros pirmosios privalomosios dalies, kurioje nurodomas taikomas teisinis pagrindas ir kurios tekstas anglų kalba yra toks:

> The applicable legal framework for the present trusted list is Regulation (ES) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Tekstas valstybės narės nacionaline (-ėmis) kalba (-omis):

> Taikomas esamo patikimo sąrašo teisinis pagrindas yra 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

2) antrosios neprivalomos specifinės kiekvienam patikimam sąrašui dalies, kurioje pateikiamos nuorodos į konkretų taikomą nacionalinį teisinį pagrindą.

Dabartinis paslaugos statusas (5.5.4 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.5.4 punkte nustatytas specifikacijas.

Į ES valstybės narės patikimą sąrašą prieš įsigaliojant Reglamentui (ES) Nr. 910/2014 (t. y. 2016 m. birželio 30 d.) įtrauktų paslaugų „dabartinio paslaugos statuso“ vertė perkeliama reglamento taikymo pradžios dieną (t. y. 2016 m. liepos 1 d.), kaip nurodyta ETSI TS 119 612 J priede.

III SKYRIUS

PATIKIMŲ SĄRAŠŲ TĘSTINUMAS

Sertifikatai, apie kuriuos Komisijai turi būti pranešta pagal šio sprendimo 4 straipsnio 2 dalį, turi atitikti ETSI TS 119 612 5.7.1 punkto reikalavimus ir turi būti išduodami taip, kad:

— jų galiojimo pabaigos data („ne vėliau kaip“) skirtųsi bent trim mėnesiais,

— jie būtų sukurti naudojant naujas raktų poras. Anksčiau naudotos raktų poros neturi būti pakartotinai sertifikuotos.

Jeigu pasibaigia vieno iš viešųjų raktų sertifikatų, kuris galėtų būti naudojamas patikimo sąrašo parašui ar spaudui tvirtinti, apie kurį buvo pranešta Komisijai ir kuris yra paskelbtas pagrindiniame Komisijos nuorodų sąraše, galiojimas, valstybės narės turi:

— jeigu šiuo metu paskelbtas patikimas sąrašas buvo pasirašytas arba užantspauduotas privačiuoju raktu, kurio viešojo rakto sertifikato galiojimas pasibaigęs, nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą privačiuoju raktu, kurio viešojo rakto sertifikatas, apie kurį pranešta, nepasibaigęs,

— prireikus parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar užantspauduoti, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,

— skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

Jeigu vienas iš privačiųjų raktų, atitinkančių viešojo rakto sertifikatą, kuris galėtų būti naudojamas patikimo sąrašo parašui ar spaudui tvirtinti, apie kurį buvo pranešta Komisijai ir kuris yra paskelbtas pagrindiniame Komisijos nuorodų sąraše, yra pažeidžiamas arba nutraukiamas jo naudojimas, valstybės narės turi:

— nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą nepažeistu privačiuoju raktu, jeigu paskelbtas patikimas sąrašas buvo pasirašytas arba užantspauduotas privačiuoju raktu, kuris buvo pažeistas ar kurio naudojimas buvo nutrauktas,

— prireikus parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar patvirtinti spaudu, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,

— skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

Jeigu visi privatieji raktai, atitinkantys viešųjų raktų sertifikatus, kurie galėtų būti naudojami patikimo sąrašo parašui tvirtinti, apie kuriuos buvo pranešta Komisijai ir kurie yra paskelbti pagrindiniame Komisijos nuorodų sąraše, yra pažeidžiami arba nutraukiamas jų naudojimas, valstybės narės turi:

— parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar patvirtinti spaudu, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,

— nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą vienu iš tų naujų privačiųjų raktų, apie kurių atitinkamą viešojo rakto sertifikatą turi būti pranešta,

— skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

IV SKYRIUS

ŽMONĖMS SUPRANTAMOS PATIKIMO SĄRAŠO FORMOS SPECIFIKACIJOS

Jeigu sudaromas ir skelbiamas žmonėms suprantamos formos patikimas sąrašas, jis teikiamas kaip portatyvaus formato (PDF) dokumentas, parengtas pagal ISO 32000 ([1]), ir jo formatas atitinka PDF/A aprašą (ISO 19005 ([2])).

PDF/A aprašu pagrįsto žmonėms suprantamos formos patikimo sąrašo turinys turi atitikti šiuos reikalavimus:

— žmonėms suprantamos formos struktūra turi atitikti loginį modelį, aprašytą TS 119612,

— kiekvienas esamas laukas turi būti rodomas ir jame turi būti nurodyta:

  — lauko pavadinimas (pvz., „*Paslaugos rūšies identifikatorius*“),

  — lauko reikšmė (pvz., „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}“),

  — kai taikoma, lauko vertės reikšmė (aprašymas) (pvz., „*sertifikatų sudarymo tarnyba, rengianti ir pasirašanti kvalifikuotus sertifikatus remdamasi tapatybe ir kitais požymiais, patikrintais atitinkamų registracijos tarnybų*“),

  — jeigu reikia, įvairios žmonių kalbų versijos, numatytos patikimame sąraše,

— žmonėms suprantama forma turi būti pateikti bent toliau nurodyti laukai ir atitinkamos skaitmeninių sertifikatų ([3]), jeigu jos nurodytos lauke „Paslaugos skaitmeninis identifikatorius“, reikšmės:

  — versija,

  — sertifikato serijos numeris,

  — parašo algoritmas,

  — išdavėjas – visi atitinkami išskirtiniai pavadinimo laukai,

  — galiojimo laikotarpis,

  — subjektas – visi atitinkami išskirtiniai pavadinimo laukai,

([1]) ISO 32000-1:2008: „Dokumentų tvarkyba. Portatyvus dokumento formatas. 1 dalis. PDF 1.7“.
([2]) ISO 19005-2:2011: „Dokumentų tvarkyba. Ilgalaikio saugojimo elektroninio dokumento rinkmenos formatas. 2 dalis. ISO 32000-1 (PDF/A-2) naudojimas“.
([3]) Rekomendacija ITU-T X.509 | ISO/IEC 9594-8: Informacinė technologija. Atvirųjų sistemų jungtis. Rodyklė: Viešojo rakto ir požymių sertifikato sistemos (žr. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— viešasis raktas,

— institucijos rakto identifikatorius,

— subjekto rakto identifikatorius,

— rakto naudojimas,

— pratęstas rakto naudojimas,

— sertifikavimo politika – visi politikos identifikatoriai ir kvalifikatoriai,

— politikos nustatymas,

— subjekto alternatyvus pavadinimas,

— subjekto rodyklės požymiai,

— pagrindiniai apribojimai,

— politikos apribojimai,

— CRL paskirstymo taškai ([1]),

— institucijos informacijos prieiga,

— subjekto informacijos prieiga,

— kvalifikuoto sertifikato patvirtinimai ([2]),

— maišos algoritmas,

— sertifikato maišos vertė,

— žmonėms suprantama forma turi būti lengvai išspausdinama,

— žmonėms suprantama forma turi būti pasirašyta arba patvirtinta spaudu schemos operatoriaus, remiantis PDF pažangiojo parašo reikalavimais, nurodytais Komisijos įgyvendinimo sprendimo (ES) 2015/1505 1 ir 3 straipsniuose.

([1]) RFC 5280: interneto X.509 PKI sertifikatas ir CRL profilis.
([2]) RFC 3739: interneto X.509 PKI: kvalifikuoto sertifikato profilis.

II PRIEDAS

VALSTYBIŲ NARIŲ PRANEŠIMŲ FORMA

Informacija, kurią valstybės narės turi pranešti pagal šio sprendimo 4 straipsnio 1 dalį, apima šiuos duomenis ir visus jų pakeitimus:

1) Valstybė narė, naudojant ISO 3166-1 ([1]) dviejų raidžių kodą, išskyrus šias išimtis:

   a) Jungtinės Karalystės šalies kodas yra „UK“.

   b) Graikijos šalies kodas yra „EL“.

2) Įstaiga (-os), atsakinga (-os) už patikimų sąrašų formos, kurią galima tvarkyti automatizuotomis priemonėmis, ir žmonėms suprantamos formos sudarymą, tvarkymą ir skelbimą:

   a) Schemos operatoriaus pavadinimas: pateikta informacija turi būti identiška (skirti didžiąsias ir mažąsias raides) patikimame sąraše pateiktam schemos operatoriaus pavadinimui visomis kalbomis, naudojamomis patikimame sąraše.

   b) Neprivaloma informacija, skirta Komisijos vidaus naudojimui tik tuo atveju, jei reikėtų susisiekti su atitinkama įstaiga (ši informacija nebus skelbiama EK sudarytame patikimų sąrašų suvestiniame sąraše):

      — schemos operatoriaus adresas,

      — atsakingo (-ų) asmens (-ų) kontaktiniai duomenys (vardas, pavardė, telefonas, e. pašto adresas).

3) Vieta, kur paskelbta forma, tinkama patikimam sąrašui tvarkyti automatizuotomis priemonėmis *(esamo patikimo sąrašo skelbimo vieta)*.

4) Vieta, kur patikimas sąrašas atitinkamais atvejais paskelbtas žmonėms suprantama forma *(esamo patikimo sąrašo skelbimo vieta)*. Jei patikimas sąrašas žmonėms suprantama forma nebeskelbiamas, tai turi būti nurodyta.

5) Viešųjų raktų sertifikatai, atitinkantys privačius raktus, kurie gali būti naudojami siekiant elektroniniu būdu pasirašyti arba užantspauduoti formą, tinkamą patikimam sąrašui automatizuotomis priemonėmis tvarkyti, ir patikimų sąrašų žmonėms suprantamą formą: šie sertifikatai turi būti pateikti kaip slaptojo pašto protokolo Base64 pagrindu šifruoti DER sertifikatai. Pranešant apie pasikeitusius duomenis papildoma informacija pridedama atvejais, kai naujas sertifikatas pakeičia konkretų Komisijos sąraše esantį sertifikatą, ir atvejais, kai pranešamas sertifikatas pridedamas prie esamo (-ų) sertifikato (-ų) jo (jų) nepakeisdamas.

6) Pagal 1–5 punktus praneštų duomenų pateikimo data.

Pagal 1, 2 (a papunktį), 3, 4 ir 5 punktus pranešti duomenys turi būti įtraukti į Europos Komisijos sudarytą patikimų sąrašų suvestinį sąrašą, pakeičiant anksčiau praneštą informaciją, įtrauktą į suvestinį sąrašą.

([1]) ISO 3166-1: „Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių kodai“.

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2015/1506

2015 m. rugsėjo 8 d.

kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 27 straipsnio 5 dalį ir 37 straipsnio 5 dalį nustatomos pažangiųjų elektroninių parašų ir pažangiųjų spaudų formatų, kuriuos turi pripažinti viešojo sektoriaus įstaigos, specifikacijos

(Tekstas svarbus EEE)

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 27 straipsnio 5 dalį ir 37 straipsnio 5 dalį,

kadangi:

(1) valstybės narės turi įdiegti reikiamas technines priemones, leidžiančias joms tvarkyti elektroniniu būdu pasirašytus dokumentus, kurių reikalaujama naudojant viešojo sektoriaus įstaigos arba jos vardu teikiamą internetinę paslaugą;

(2) Reglamentu (ES) Nr. 910/2014 valstybės narės, pažangiojo elektroninio parašo arba spaudo reikalaujančios tam, kad būtų galima pasinaudoti viešojo sektoriaus įstaigos arba jos vardu teikiama internetine paslauga, įpareigojamos pripažinti pažangiuosius elektroninius parašus ir spaudus, kvalifikuotais sertifikatais patvirtintus pažangiuosius elektroninius parašus ir spaudus ir konkrečių formatų arba alternatyvių formatų, patvirtintų pagal konkrečius bazinius metodus, kvalifikuotus elektroninius parašus ir spaudus;

(3) siekiant apibrėžti konkrečius formatus ir bazinius metodus reikėtų atsižvelgti į esamą praktiką, standartus ir Sąjungos teisės aktus;

(4) Komisijos įgyvendinimo sprendime 2014/148/ES ([2]) buvo nustatytas keletas įprasčiausių pažangiojo elektroninio parašo formatų, kuriuos turi techniškai palaikyti tos valstybės narės, kuriose pažangieji elektroniniai parašai reikalingi vykdant internetines administracines procedūras. Nustatant bazinius formatus siekiama palengvinti tarpvalstybinį elektroninių parašų patvirtinimą ir pagerinti tarpvalstybinį elektroninių procedūrų sąveikumą;

(5) šio sprendimo priede išvardyti standartai yra galiojantys pažangiųjų elektroninių parašų formatų standartai. Atsižvelgiant į tai, kad šiuo metu standartizacijos įstaigos peržiūri bazinių formatų ilgalaikio archyvavimo formas, ilgalaikio archyvavimo standartai į šio sprendimo taikymo sritį neįtraukti. Kai bus paskelbta nauja bazinių standartų redakcija, bus peržiūrėtos nuorodos į ilgalaikio archyvavimo standartus ir nuostatas;

(6) techniniu požiūriu pažangieji elektroniniai parašai ir pažangieji elektroniniai spaudai yra panašūs. Todėl pažangiųjų elektroninių parašų formatų standartai turėtų *mutatis mutandis* būti taikomi pažangiųjų elektroninių spaudų formatams;

(7) jeigu pasirašymui ar antspaudavimui naudojami kiti elektroninio parašo ar spaudo formatai, nei įprastai techniškai palaikomi, turėtų būti pateikta patvirtinimo priemonių, kurios leistų elektroninius parašus arba spaudus patikrinti tarpvalstybiniu mastu. Tam, kad priimančiosios valstybės narės galėtų pasitikėti tomis kitos valstybės narės patvirtinimo priemonėmis, būtina pateikti lengvai prieinamą informaciją apie tas patvirtinimo priemones, įtraukiant informaciją į elektroninius dokumentus, elektroninius parašus arba į elektroninių dokumentų sudėtinį rodinį;

([1]) OL L 257, 2014 8 28, p. 73.

([2]) 2014 m. kovo 17 d. Komisijos įgyvendinimo sprendimas 2014/148/ES, kuriuo iš dalies keičiamas Sprendimas 2011/130/ES, kuriuo nustatomi būtinieji dokumentų, kompetentingų institucijų pasirašomų elektroniniu būdu pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje, tarptautinio tvarkymo reikalavimai (OL L 80, 2014 3 19, p. 7).

(8) jeigu valstybės narės viešosios tarnybos turi elektroninio parašo arba spaudo patvirtinimo galimybių, tinkamų tvarkymui automatizuotomis priemonėmis, tokios patvirtinimo galimybės turėtų būti suteiktos priimančiai valstybei narei. Vis dėlto šis sprendimas neturėtų trukdyti taikyti Reglamento (ES) Nr. 910/2014 27 straipsnio 1 ir 2 dalių bei 37 straipsnio 1 ir 2 dalių, kai alternatyvių metodų patvirtinimo galimybių tvarkymas automatizuotomis priemonėmis nėra įmanomas;

(9) siekiant nustatyti panašius patvirtinimo reikalavimus ir padidinti pasitikėjimą valstybių narių teikiamomis patvirtinimo galimybėmis, susijusiomis su kitais elektroninio parašo arba spaudo formatais nei visuotinai palaikomais, šiame sprendime nustatyti reikalavimai dėl patvirtinimo priemonių grindžiami kvalifikuotiems elektroniniams parašams ir spaudams keliamais patvirtinimo reikalavimais, nurodytais Reglamento (ES) Nr. 910/2014 32 ir 40 straipsniuose;

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

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Valstybės narės, reikalaujančios pažangiojo elektroninio parašo arba kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio parašo, kaip numatyta Reglamento (ES) Nr. 910/2014 27 straipsnio 1 ir 2 dalyse, pripažįsta B, T arba LT atitikties lygmens XML, CMS arba PDF pažangųjį elektroninį parašą arba parašą su susietojo parašo sudėtiniu rodiniu, jeigu tie parašai atitinka priede išvardytas technines specifikacijas.arba parašą su susietojo parašo sudėtiniu rodiniu

2 straipsnis

1. Valstybės narės, reikalaujančios pažangiojo elektroninio parašo arba kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio parašo, kaip numatyta Reglamento (ES) Nr. 910/2014 27 straipsnio 1 ir 2 dalyse, pripažįsta kito formato elektroninius parašus, nei nurodytus šio sprendimo 1 straipsnyje, su sąlyga, kad valstybė narė, kurioje įsisteigęs pasirašančiojo asmens naudojamas patikimumo užtikrinimo paslaugų teikėjas, siūlo kitoms valstybėms narėms parašo patvirtinimo galimybių, kurios tinka, jei įmanoma, tvarkymui automatizuotomis priemonėmis.

2. Parašo patvirtinimo galimybės:

a) leidžia nemokamai kitoms valstybėms narėms internetu patvirtinti gautus elektroninius parašus taip, kad, kaip tą padaryti, suprastų ir asmenys, kuriems tos šalies kalba nėra gimtoji;

b) nurodomos pasirašytame dokumente, elektroniniame paraše arba elektroninio dokumento sudėtiniame rodinyje; ir

c) patvirtina pažangiojo elektroninio parašo galiojimą su sąlyga, kad:

1) sertifikatas, kuriuo tvirtinamas pažangusis elektroninis parašas, galiojo pasirašymo metu, ir, kai pažangusis elektroninis parašas yra tvirtinamas kvalifikuotu sertifikatu, kvalifikuotas sertifikatas, kuriuo tvirtinamas pažangusis elektroninis parašas, pasirašymo metu buvo kvalifikuotas elektroninio parašo sertifikatas, atitinkantis Reglamento (ES) Nr. 910/2014 I priedą, ir kad jį išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas;

2) parašo patvirtinimo duomenys atitinka pasikliaujančiajai šaliai pateiktus duomenis;

3) duomenų, kuriais nurodomas konkretus pasirašantis asmuo, rinkinys tinkamai pateikiamas pasikliaujančiajai šaliai;

4) jei pasirašymo metu buvo naudojamas slapyvardis, tai aiškiai nurodoma pasikliaujančiajai šaliai;

5) kai pažangusis elektroninis parašas yra sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą, tai, kad naudotas toks įtaisas, aiškiai nurodoma pasikliaujančiajai šaliai;

6) nebuvo pažeistas pasirašytų duomenų vientisumas;

7) pasirašymo metu buvo laikomasi Reglamento (ES) Nr. 910/2014 26 straipsnyje nurodytų reikalavimų;

8) sistema, naudojama pažangiajam elektroniniam parašui patvirtinti, duoda pasikliaujančiajai šaliai teisingą patvirtinimo procedūros rezultatą ir leidžia pasikliaujančiai šaliai nustatyti bet kokias su saugumu susijusias problemas.

3 straipsnis

Valstybės narės, reikalaujančios pažangiojo elektroninio spaudo arba kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio spaudo, kaip numatyta Reglamento (ES) Nr. 910/2014 37 straipsnio 1 ir 2 dalyse, pripažįsta B, T arba LT atitikties lygmens XML, CMS arba PDF pažangųjį elektroninį spaudą arba parašą su susietojo parašo sudėtiniu rodiniu, jeigu jie atitinka priede išvardytas technines specifikacijas.

4 straipsnis

1. Valstybės narės, reikalaujančios pažangiojo elektroninio spaudo arba kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio spaudo, kaip numatyta Reglamento (ES) Nr. 910/2014 37 straipsnio 1 ir 2 dalyse, pripažįsta kito formato elektroninius parašus, nei nurodytus šio sprendimo 3 straipsnyje, su sąlyga, kad valstybė narė, kurioje įsisteigęs spaudo kūrėjo naudojamas patikimumo užtikrinimo paslaugų teikėjas, siūlo kitoms valstybėms narėms spaudo patvirtinimo galimybių, kurios tinka, jei įmanoma, tvarkymui automatizuotomis priemonėmis.

2. Spaudo patvirtinimo galimybės:

a) leidžia nemokamai kitoms valstybėms narėms internetu patvirtinti gautus elektroninius spaudus taip, kad, kaip tą padaryti, suprastų ir asmenys, kuriems tos šalies kalba nėra gimtoji;

b) nurodomos užantspauduotame dokumente, elektroniniame spaude arba elektroninio dokumento sudėtiniame rodinyje;

c) patvirtina pažangiojo elektroninio spaudo galiojimą su sąlyga, kad:

1) sertifikatas, kuriuo tvirtinamas pažangusis elektroninis spaudas, galiojo antspaudavimo metu, ir, kai pažangusis elektroninis spaudas yra tvirtinamas kvalifikuotu sertifikatu, kvalifikuotas sertifikatas, kuriuo tvirtinamas pažangusis elektroninis spaudas, antspaudavimo metu buvo kvalifikuotas elektroninio spaudo sertifikatas, atitinkantis Reglamento (ES) Nr. 910/2014 III priedą, ir kad jį išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas;

2) spaudo patvirtinimo duomenys atitinka pasikliaujančiajai šaliai pateiktus duomenis;

3) duomenų, kuriais nurodomas konkretus spaudo kūrėjas, rinkinys tinkamai pateikiamas pasikliaujančiajai šaliai;

4) jei antspaudavimo metu buvo naudojamas slapyvardis, tai aiškiai nurodoma pasikliaujančiajai šaliai;

5) kai pažangusis elektroninis spaudas yra sukurtas naudojant kvalifikuotą elektroninio spaudo kūrimo įtaisą, tai, kad naudotas toks įtaisas, aiškiai nurodoma pasikliaujančiajai šaliai;

6) nebuvo pažeistas antspauduotų duomenų vientisumas;

7) antspaudavimo metu buvo laikomasi Reglamento (ES) Nr. 910/2014 36 straipsnyje nurodytų reikalavimų;

8) sistema, naudojama pažangiajam elektroniniam spaudui patvirtinti, duoda pasikliaujančiajai šaliai teisingą patvirtinimo procedūros rezultatą ir leidžia pasikliaujančiajai šaliai nustatyti bet kokias su saugumu susijusias problemas.

5 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis sprendimas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2015 m. rugsėjo 8 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

PRIEDAS

XML, CMS arba PDF pažangiojo elektroninio parašo ir susietojo parašo sudėtinio rodinio techninių specifikacijų sąrašas

Sprendimo 1 straipsnyje minimi pažangieji elektroniniai parašai turi atitikti vieną iš šių ETSI techninių specifikacijų, išskyrus jo 9 sąlygą:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1 ([1]).
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1 ([2]).
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2 ([3]).

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Sprendimo 1 straipsnyje minimas susietojo parašo sudėtinis rodinys turi atitikti šią ETSI techninę specifikaciją:

Associated Signature Container Baseline Profile	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

XML, CMS arba PDF pažangiojo elektroninio spaudo ir susietojo spaudo sudėtinio rodinio techninių specifikacijų sąrašas

Sprendimo 3 straipsnyje minimi pažangieji elektroniniai spaudai turi atitikti vieną iš šių ETSI techninių specifikacijų, išskyrus jo 9 sąlygą:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Sprendimo 3 straipsnyje minimas susietojo spaudo sudėtinis rodinys turi atitikti šią ETSI techninę specifikaciją:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

ISSN 1977-0723 (elektroninis leidimas)
ISSN 1725-5120 (popierinis leidimas)

Europos Sąjungos leidinių biuras
2985 Liuksemburgas
LIUKSEMBURGAS

LT