Eiropas Savienības

Oficiālais Vēstnesis

L 235

Izdevums latviešu valodā

Tiesību akti

58. sējums

2015. gada 9. septembris

Saturs

[1] Dokuments attiecas uz EEZ

[1] Dokuments attiecas uz EEZ

II

(Neleģislatīvi akti)

REGULAS

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2015/1501

(2015. gada 8. septembris)

par sadarbspējas sistēmu saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 12. panta 8. punktu

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 12. panta 8. punktu,

tā kā:

(1) Regulas (ES) Nr. 910/2014 12. panta 2. punktā noteikts, ka jāizveido sadarbspējas sistēma, lai panāktu saskaņā ar minētās regulas 9. panta 1. punktu izziņoto valsts elektroniskās identifikācijas shēmu sadarbspēju.

(2) Dalībvalstu elektroniskās identifikācijas shēmu savstarpējā savienošanā galvenā nozīme ir mezgliem. To nozīme ir izskaidrota dokumentos par Eiropas Infrastruktūras savienošanas instrumentu, kas izveidots ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1316/2013 ([2]), ieskaitot "eIDAS mezgla" funkcijas un komponentus.

(3) Ja dalībvalsts vai Komisija nodrošina programmatūru, kas ļauj autentifikāciju veikt mezglam, kurš darbojas citā dalībvalstī, persona, kura piegādā un atjaunina autentificēšanas mehānismā izmantojamo programmatūru, var ar personu, kura mitina attiecīgo programmatūru, vienoties par to, kā tiks pārvaldīta autentifikācijas mehānisma darbība. Tāda vienošanās nedrīkstētu radīt mitinātājam nesamērīgas tehniskas prasības vai izmaksas (kā atbalsta, pienākumu izpildes, mitināšanas un citas izmaksas).

(4) Cik vajadzīgs sadarbspējas sistēmas īstenošanai, Komisija varētu sadarbībā ar dalībvalstīm izstrādāt papildu tehniskās specifikācijas ar sīkāku informāciju par tehniskajām prasībām, kā noteikts šajā regulā, it īpaši, ņemot vērā Komisijas Īstenošanas lēmuma (ES) 2015/296 ([3]) 14. panta d) punktā minētā Sadarbības tīkla atzinumus. Tādas specifikācijas būtu jāizstrādā kā daļa no digitālo pakalpojumu infrastruktūras, ko nosaka Regula (ES) Nr. 1316/2013, kurā paredzēti elektroniskās identifikācijas elementa praktiskās īstenošanas līdzekļi.

([1]) OV L 257, 28.8.2014., 73. lpp.

([2]) Eiropas Parlamenta un Padomes 2013. gada 11. decembra Regula (ES) Nr. 1316/2013, ar ko izveido Eiropas infrastruktūras savienošanas instrumentu, groza Regulu (ES) Nr. 913/2010 un atceļ Regulu (EK) Nr. 680/2007 un Regulu (EK) Nr. 67/2010 (OV L 348, 20.12.2013., 129. lpp.).

([3]) Komisijas 2015. gada 24. februāra Īstenošanas lēmums (ES) 2015/296, ar ko nosaka procesuālo kārtību dalībvalstu sadarbībai elektroniskās identifikācijas jomā, kā paredzēts 12. panta 7. punktā Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū (OV L 53, 25.2.2015., 14. lpp.).

(5) Šajā regulā izklāstītās tehniskās prasības būtu jāpiemēro arī tad, ja mainītos tehniskās specifikācijas, ko izstrādā saskaņā ar šās regulas 12. pantu.

(6) Nosakot sadarbspējas sistēmas darbības kārtību, kas izklāstīta šajā regulā, vislielākajā mērā ir ņemti vērā lielapjoma eksperimentālais projekts *STORK* un tā izstrādātās specifikācijas un Eiropas publisko pakalpojumu Eiropas sadarbspējas satvara principi un jēdzieni.

(7) Vislielākajā mērā ir ņemti vērā dalībvalstu sadarbības rezultāti.

(8) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Priekšmets

Šī regula nosaka sadarbspējas sistēmas tehniskās un darbības prasības, lai nodrošinātu to elektroniskās identifikācijas shēmu sadarbspēju, par kurām dalībvalstis paziņo Komisijai.

Minētajās prasībās galvenokārt ietilpst:

a) minimālās tehniskās prasības, kas attiecas uz saskaņā ar Regulas (ES) Nr. 910/2014 8. pantu elektroniskās identifikācijas shēmu ietvaros izziņoto elektroniskās identifikācijas līdzekļu uzticamības līmeņiem un valstu uzticamības līmeņu attiecināšanu, kā izklāstīts 3. un 4. pantā;

b) sadarbspējas minimālās tehniskās prasības, kā izklāstīts 5. un 8. pantā;

c) personas identifikācijas datu minimālais kopums, kas unikāli apzīmē fizisku vai juridisku personu, kā izklāstīts 11. pantā un pielikumā;

d) kopīgi darbības drošības standarti, kā noteikts 6., 7., 9. un 10. pantā;

e) strīdu izšķiršanas kārtība, kā noteikts 13. pantā.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "mezgls" ir savienojuma punkts, kas ir elektroniskās identifikācijas sadarbspējas arhitektūras sastāvdaļa un ir iesaistīts personu pārrobežu autentifikācijā, un spēj pazīt un apstrādāt vai pārsūtīt sūtījumus citiem mezgliem, ļaujot vienas dalībvalsts elektroniskās identifikācijas infrastruktūrai saskarnēt ar citu dalībvalstu elektroniskās identifikācijas infrastruktūrām;

2) "mezgla operators" ir vienība, kam ir pienākums nodrošināt mezgla pareizu un drošu darbošanos savienojuma punkta funkcijā.

3. pants

Minimālās tehniskās prasības, kas attiecas uz uzticamības līmeņiem

Minimālās tehniskās prasības, kas attiecas uz uzticamības līmeņiem, ir noteiktas Komisijas Īstenošanas regulā (ES) 2015/1502 ([1]).

4. pants

Valstu uzticamības līmeņu attiecināšana

Izziņoto elektroniskās identifikācijas shēmu valsts uzticamības līmeņu attiecināšanā ievēro prasības, kas noteiktas Komisijas Īstenošanas regulā (ES) 2015/1502. Attiecināšanas rezultātus paziņo Komisijai, izmantojot paziņojuma veidni, kas dota Komisijas Īstenošanas lēmumā (ES) 2015/1505 ([2]).

5. pants

Mezgli

1. Mezglam vienā dalībvalstī jāspēj savienoties ar citu dalībvalstu mezgliem.

2. Mezgliem jāspēj ar tehniskiem līdzekļiem atšķirt publiskā sektora iestādes no citām atkarīgajām pusēm.

3. Dalībvalsts pieņemts šajā regulā noteikto tehnisko prasību īstenojums neuzliek nesamērīgas tehniskas prasības un izmaksas citām dalībvalstīm, lai tās spētu sadarboties ar pirmās dalībvalsts īstenojumu.

6. pants

Datu privātums un konfidencialitāte

1. Apmaiņas datu privātuma aizsardzību un konfidencialitāti un datu integritātes saglabāšanu starp mezgliem nodrošina, izmantojot labākos pieejamos tehniskos risinājumus un aizsardzības praksi.

2. Mezgli neglabā personas datus, izņemot 9. panta 3. punktā noteiktajam mērķim.

7. pants

Datu integritāte un autentiskums sakariem

Sakariem starp mezgliem jānodrošina datu integritāte un autentiskums, lai būtu drošība, ka visi pieprasījumi un atbildes ir autentiski un nav viltoti. Šim nolūkam mezgli izmanto risinājumus, kas ir sekmīgi izmantoti pārrobežu operatīvās sadarbības vajadzībām.

([1]) Komisijas 2015. gada 8. septembra Īstenošanas regula (ES) 2015/1502, kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras (skatīt šā *Oficiālā Vēstneša* 7. lappusi).

([2]) Komisijas 2015. gada 8. septembra Īstenošanas lēmums (ES) 2015/1505, kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 22. panta 5. punktu izklāstītas tehniskās specifikācijas un formāti, kas attiecas uz uzticamības sarakstiem (skatīt šā *Oficiālā Vēstneša* 26. lappusi).

8. pants

Ziņojuma formāts sūtīšanai

Sintaksei mezgli izmanto parastus ziņojumu formātus, kas balstīti uz standartiem, kuri jau vairākas reizes ir izmantoti dalībvalstu saziņā un izrādījušies noderīgi operatīvās sadarbības vidē. Sintakse ļauj:

a) pienācīgi apstrādāt personas identifikācijas datu minimālo kopumu, kas unikāli apzīmē fizisku vai juridisku personu;

b) pienācīgi apstrādāt elektroniskās identifikācijas līdzekļa uzticamības līmeni;

c) atšķirt publiskā sektora struktūras no citām atkarīgajām pusēm;

d) elastīgi apmierināt papildu atribūtu vajadzības, kas attiecas uz identifikāciju.

9. pants

Drošības informācijas un metadatu pārvaldība

1. Mezgla operators mezgla pārvaldības metadatus sūta standartizētā mašīnapstrādājamā veidā, aizsargātus un uzticamus.

2. Automātiski izgūst vismaz drošībai svarīgos parametrus.

3. Mezgla operators glabā datus, kas incidenta gadījumā ļauj rekonstruēt ziņojumu apmaiņas secību, lai noteiktu incidenta vietu un raksturu. Datus uzglabā valsts prasībām atbilstošu laiku, un tie sastāv no vismaz šādiem elementiem:

a) mezgla identifikācija;

b) ziņojuma identifikācija;

c) ziņojuma datums un laiks.

10. pants

Informācijas uzticamība un drošības standarti

1. To mezglu mezgla operatori, kuros nodrošina autentificēšanu, pierāda, ka attiecībā uz mezgliem, kuri piedalās sadarbspējas sistēmā, mezgls atbilst standarta ISO/IEC 27001 prasībām ar sertifikāciju vai līdzvērtīgu novērtēšanas metodi, vai saskanību ar valsts tiesību aktiem.

2. Drošības kritiskos atjauninājumus mezgla operatori palaiž bez nepamatotas kavēšanās.

11. pants

Personas identifikācijas dati

1. Personas identifikācijas datu minimālais kopums, kas unikāli apzīmē fizisku vai juridisku personu, izmantošanā pārrobežu sadarbībai atbilst pielikumā izklāstītajām prasībām.

2. Fiziskas personas, kura pārstāv juridisku personu, minimālais datu kopums izmantošanā pārrobežu sadarbībai ietver pielikumā uzskaitīto fizisko un juridisko personu atribūtu kombināciju.

3. Datus nosūta ar oriģināla rakstzīmēm un attiecīgos gadījumos transliterē latīņu alfabētā.

12. pants

Tehniskās specifikācijas

1. Cik vajadzīgs sadarbspējas sistēmas īstenošanai, Sadarbības tīkls, kas izveidots ar Īstenošanas lēmumu (ES) 2015/296, var saskaņā ar tā 14. panta d) punktu pieņemt atzinumus par nepieciešamību izstrādāt tehniskās specifikācijas. Tādās tehniskajās specifikācijās sniedz sīkākas ziņas par tehniskajām prasībām, kas noteiktas šajā regulā.

2. Saskaņā ar 1. punktā minēto atzinumu Komisija sadarbībā ar dalībvalstīm izstrādā tehniskās specifikācijas kā daļu no Regulas (ES) Nr. 1316/2013 digitālo pakalpojumu infrastruktūras.

3. Sadarbības tīkls saskaņā ar Īstenošanas lēmuma (ES) 2015/296 14. panta d) punktu sniedz atzinumu, kurā izvērtē, vai un kādā mērā tehniskās specifikācijas, kas izstrādātas saskaņā ar 2. punktu, atbilst 1. punktā minētajā atzinumā apzinātajai vajadzībai vai šajā regulā izklāstītajām prasībām. Tas var ieteikt dalībvalstīm tehniskās specifikācijas ņemt vērā sadarbspējas sistēmas īstenošanā.

4. Komisija nodrošina īstenošanas etalonu kā paraugu tehnisko specifikāciju interpretācijai. Dalībvalstis var piemērot šo īstenošanas etalonu vai izmantot to par paraugu, izmēģinot citus tehnisko specifikāciju īstenošanas veidus.

13. pants

Strīdu izšķiršana

1. Ja iespējams, visus strīdus, kas saistīti ar sadarbspējas sistēmu, attiecīgās dalībvalstis atrisina sarunās.

2. Ja nav panākts risinājums saskaņā ar 1. punktu, strīdu piekrīt izšķirt ar Īstenošanas lēmuma (ES) 2015/296 12. pantu izveidotajam Sadarbības tīklam saskaņā ar tā reglamentu.

14. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

Prasības personas identifikācijas datu minimālajam kopumam, kas unikāli apzīmē fizisku vai juridisku personu (minētas 11. pantā)

1. **Fiziskas personas minimālais datu kopums**

Fiziskas personas minimālais datu kopums ietver visus šos obligātos atribūtus:

a) pašreizējie uzvārdi;

b) pašreizējie vārdi;

c) dzimšanas datums;

d) unikāls identifikators, ko sūtītāja dalībvalsts sastādījusi saskaņā ar tehniskajām specifikācijām pārrobežu identifikācijas vajadzībām un kas saglabājas pēc iespējas ilgāk.

Fiziskas personas minimālais datu kopums var ietvert vienu vai vairākus no šiem papildu atribūtiem:

a) dzimtie vārdi un uzvārdi;

b) dzimšanas vieta;

c) pašreizējā adrese;

d) dzimums.

2. **Juridiskas personas minimālais datu kopums**

Juridiskas personas minimālais datu kopums ietver visus šos obligātos atribūtus:

a) pašreizējais juridiskais nosaukums;

b) unikāls identifikators, ko sūtītāja dalībvalsts sastādījusi saskaņā ar tehniskajām specifikācijām pārrobežu identifikācijas vajadzībām un kas saglabājas pēc iespējas ilgāk.

Juridiskas personas minimālais datu kopums var ietvert vienu vai vairākus no šiem papildu atribūtiem:

a) pašreizējā adrese;

b) PVN maksātāja reģistrācijas numurs;

c) nodokļu maksātāja numurs;

d) identifikators, kas saistīts ar Eiropas Parlamenta un Padomes Direktīvas 2009/101/EK ([1]) 3. panta 1. punktu;

e) juridiskās personas identifikators (*LEI*), kas minēts Komisijas Īstenošanas regulā (ES) Nr. 1247/2012 ([2]);

f) ekonomikas dalībnieku reģistrācija un identifikācija (*EORI*), kas minēta Komisijas Īstenošanas regulā (ES) Nr. 1352/2013 ([3]);

g) akcīzes numurs, kas paredzēts Padomes Regulas (ES) Nr. 389/2012 ([4]) 2. panta 12. punktā.

([1]) Eiropas Parlamenta un Padomes 2009. gada 16. septembra Direktīva 2009/101/EK par to, kā vienādošanas nolūkā koordinēt nodrošinājumus, ko dalībvalstis prasa no sabiedrībām Līguma 48. panta otrās daļas nozīmē, lai aizsargātu sabiedrību dalībnieku un trešo personu intereses (OV L 258, 1.10.2009., 11. lpp.).

([2]) Komisijas 2012. gada 19. decembra Īstenošanas regula (ES) Nr. 1247/2012, ar ko nosaka īstenošanas tehniskos standartus attiecībā uz tirdzniecības ziņojumu formātu un to sniegšanas biežumu darījumu reģistriem saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (OV L 352, 21.12.2012., 20. lpp.).

([3]) Komisijas 2013. gada 4. decembra Īstenošanas regula (ES) Nr. 1352/2013, ar ko izveido veidlapas, kuras paredzētas Eiropas Parlamenta un Padomes Regulā (ES) Nr. 608/2013 par muitas darbu intelektuālā īpašuma tiesību īstenošanā (OV L 341, 18.12.2013., 10. lpp.).

([4]) Padomes 2012. gada 2. maija Regula (ES) Nr. 389/2012 par administratīvu sadarbību akcīzes nodokļu jomā un ar ko atceļ Regulu (EK) Nr. 2073/2004 (OV L 121, 8.5.2012., 1. lpp.).

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2015/1502

(2015. gada 8. septembris),

kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK [1], un jo īpaši tās 8. panta 3. punktu,

tā kā:

(1) Regulas (ES) Nr. 910/2014 8. pants nosaka, ka elektroniskās identifikācijas shēmai, par ko paziņots atbilstoši 9. panta 1. punktam, ir jāprecizē atbilstīgi minētajai shēmai izsniegto elektroniskās identifikācijas līdzekļu uzticamības līmenis (proti, zems, būtisks vai augsts).

(2) Noteikt minimālās tehniskās specifikācijas, standartus un procedūras ir būtiski, lai panāktu vienotu izpratni par uzticamības līmeņu detaļām un nodrošinātu sadarbspēju, valstu noteiktos izziņoto elektroniskās identifikācijas shēmu uzticamības līmeņus attiecinot uz 8. pantā minētajiem uzticamības līmeņiem, kā noteikts Regulas (ES) Nr. 910/2014 12. panta 4. punkta b) apakšpunktā.

(3) Šā īstenošanas akta specifikācijās un procedūrās ir ņemts vērā starptautiskais standarts ISO/IEC 29115, jo tas ir galvenais elektroniskās identifikācijas līdzekļu uzticamības līmeņa jomā pieejamais starptautiskais standarts. Tomēr Regulas (ES) Nr. 910/2014 saturs atšķiras no minētā starptautiskā standarta, it īpaši identitātes pārbaudes un verifikācijas prasību ziņā, kā arī pēc tā, kā tiek ņemtas vērā dalībvalstu identitātes noteikšanas kārtības un attiecīgo Eiropas Savienībā esošo instrumentu atšķirības. Tādēļ pielikumā, gan balstoties uz ISO/IEC 29115, nebūtu jāatsaucas uz specifisku minētā starptautiskā standarta saturu.

(4) Šī regula ir izstrādāta kā uz iznākumu balstīta pieeja, kas ir vispiemērotākā, un tas atspoguļojas arī terminu un jēdzienu precizēšanai izmantotajās definīcijās. Tajās ir ņemts vērā Regulas (ES) Nr. 910/2014 mērķis, kas attiecas uz elektroniskās identifikācijas līdzekļu uzticamības līmeņiem. Tādēļ, nosakot specifikācijas un procedūras šajā īstenošanas aktā, vislielākajā mērā būtu jāņem vērā eksperimentālais lielapjoma projekts *STORK*, ieskaitot tajā izstrādātās specifikācijas, un ISO/IEC 29115 definīcijas un jēdzieni.

(5) Atkarā no konteksta, kādā jāverificē identitātes pierādījumu aspekts, autoritatīvi avoti var būt dažādi, piemēram, reģistri, dokumenti, apkopojumi. Dažādu dalībvalstu autoritatīvie avoti var atšķirties pat līdzīgos apstākļos.

(6) Identitātes pierādīšanas un verifikācijas prasībās būtu jāņem vērā dažādas sistēmas un prakse, vienlaikus nodrošinot pietiekami lielu uzticamību, lai panāktu nepieciešamo uzticēšanos. Tādēļ, akceptējot procedūras, ko agrāk izmantoja citiem mērķiem, nevis elektroniskās identifikācijas līdzekļu izdošanai, ir jāizvirza nosacījums, ka apstiprināšanas brīdī šīs procedūras atbilst prasībām, kas paredzētas attiecīgajam uzticamības līmenim.

[1] OV L 257, 28.8.2014., 73. lpp.

(7) Parasti izmanto tādus autentifikācijas faktorus kā kopīgs noslēpums, fiziskas ierīces un fiziski atribūti. Tomēr, lai paaugstinātu autentifikācijas procesa drošību, ir jāmudina izmantot daudzveidīgākus autentifikācijas faktorus, it īpaši no dažādām faktoru kategorijām.

(8) Šai regulai nebūtu jāietekmē juridisko personu pārstāvības tiesības. Tomēr pielikumā būtu jānosaka fizisko un juridisko personu elektroniskās identifikācijas līdzekļu saistījuma prasības.

(9) Būtu jāatzīst, cik liela nozīme ir informācijas drošības un pakalpojumu vadības sistēmām, kā arī atzītas metodikas izmantošanai un standartos (piemēram, ISO/IEC 27000 un ISO/IEC 20000 sērija) iestrādāto principu piemērošanai.

(10) Jāņem vērā arī dalībvalstu labas prakses piemēri darbā ar uzticamības līmeņiem.

(11) Svarīgs instruments, ar ko pārbaudīt produktu atbilstību šā īstenošanas akta drošības prasībām, ir IT drošības sertifikācija uz starptautisku standartu pamata.

(12) Regulas (ES) Nr. 910/2014 48. pantā minētā komiteja nav sniegusi atzinumu tās priekšsēdētāja noteiktajā termiņā,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

1. Izziņotas elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu zemo, būtisko un augsto uzticamības līmeni nosaka ar atsauci uz pielikumā izklāstītajām specifikācijām un procedūrām.

2. Pielikumā izklāstītās specifikācijas un procedūras izmanto, lai izraudzītos elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu uzticamības līmeni, nosakot šādu elementu drošu izmantojamību un kvalitāti:

a) uzņemšana – kā izklāstīts šīs regulas pielikuma 2.1. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta a) apakšpunktu;

b) elektroniskās identifikācijas līdzekļu pārvaldība – kā izklāstīts šīs regulas pielikuma 2.2. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta b) un f) apakšpunktu;

c) autentifikācija – kā izklāstīts šīs regulas pielikuma 2.3. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta c) apakšpunktu;

d) pārvaldība un organizācija – kā izklāstīts šīs regulas pielikuma 2.4. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta d) un e) apakšpunktu.

3. Ja izziņotas elektroniskās identifikācijas shēmas ietvaros izdotais elektroniskās identifikācijas līdzeklis atbilst prasībai, kas minēta pie augstāka uzticamības līmeņa, uzskatāms, ka tas apmierina līdzvērtīgu zemāka uzticamības līmeņa prasību.

4. Ja attiecīgajā pielikuma daļā nav noteikts citādi, tad, lai panāktu pieprasīto uzticamības līmeni, ir jāapmierina visi elementi, kas pielikumā norādīti pie elektroniskās identifikācijas shēmas ietvaros izdota elektroniskās identifikācijas līdzekļa konkrēta uzticamības līmeņa.

2. pants

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

Izziņotas elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu zema, būtiska un augsta uzticamības līmeņa tehniskās specifikācijas un procedūras

1. **Piemērojamās definīcijas**

Šajā pielikumā piemēro šādas definīcijas:

1) "autoritatīvs avots" – jebkura veida avots, uz kuru var paļauties, ka tas sniedz precīzus datus, informāciju un/vai pierādījumu, ko var izmantot identitātes pierādīšanai;

2) "autentifikācijas faktors" – faktors, kas apstiprināts par saistītu ar personu un ietilpst kādā no šīm kategorijām:

   a) "turējumā balstīts autentifikācijas faktors" – autentifikācijas faktors, kurā subjektam ir jāpierāda, ka tas ir viņa turējumā;

   b) "zināšanā balstīts autentifikācijas faktors" – autentifikācijas faktors, kurā subjektam ir jāpierāda, ka viņš to zina;

   c) "piemitīgs autentifikācijas faktors" – autentifikācijas faktors, kas balstās uz fiziskas personas fizisku īpašību un par kuru subjektam ir jāpierāda, ka viņam piemīt šī fiziskā īpašība;

3) "dinamiskā autentifikācija" – elektronisks process, kurā izmanto kriptogrāfiju vai citas metodes, kas dod iespēju pēc pieprasījuma izveidot elektronisku pierādījumu tam, ka subjekta pārziņā vai turējumā ir identifikācijas dati, un kas mainās līdzi katrai autentifikācijai starp subjektu un sistēmu, kura verificē subjekta identitāti;

4) "informācijas drošības pārvaldības sistēma" – procesu un procedūru kopums, kura uzdevums ir informācijas drošības apdraudējumu noturēt pieņemamā līmenī.

2. **Tehniskās specifikācijas un procedūras**

Šajā pielikumā izklāstīto tehnisko specifikāciju un procedūru elementus izmanto, lai noteiktu, kā Regulas (ES) Nr. 910/2014 8. panta prasības un kritērijus piemērot elektroniskās identifikācijas shēmas ietvaros izsniegtiem elektroniskās identifikācijas līdzekļiem.

2.1. *Uzņemšana*

2.1.1. Pieteikšanās un reģistrēšanās

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Nodrošina, ka pieteikuma iesniedzējs zina noteikumus, kas saistīti ar elektroniskās identifikācijas līdzekļu lietošanu. 2. Nodrošina, ka pieteikuma iesniedzējs zina ieteiktos piesardzības pasākumus, kas saistīti ar elektroniskās identifikācijas līdzekļiem. 3. Vāc attiecīgos personas datus, kas vajadzīgi identitātes pierādīšanai un verificēšanai.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.1.2. Identitātes pierādīšana un verificēšana (fiziskai personai)

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Var pieņemt, ka personai ir pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un tas atspoguļo uzdoto identitāti. 2. Pierādījumus var uzskatīt par patiesiem vai tādiem, kas pastāv pēc autoritatīva avota ziņām, un pierādījumi šķiet derīgi. 3. Autoritatīvais avots zina, ka uzdotā identitāte pastāv, un var tikt uzskatīts, ka persona, kura uzdod identitāti, ir tā pati.
Būtisks	Jāizpilda zemais līmenis plus viena no alternatīvām 1.–4. punktā: 1. Ir verificēts, ka personai ir pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un tā atbilst uzdotajai identitātei, un ir pārbaudīts pierādījuma patiesums; vai pēc autoritatīva avota ziņām tas pastāv un attiecas uz īstu personu, un ir veikti pasākumi, lai minimalizētu risku, ka personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēts, nozagts, apturēts, anulēts vai notecējis pierādījums. vai 2. Reģistrēšanās laikā tiek iesniegts personas dokuments dalībvalstī, kurā šis dokuments izdots, un šķiet, ka dokuments attiecas uz tā uzrādītāju, un ir veikti pasākumi, lai minimalizētu risku, ka personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēti, nozagti, apturēti, anulēti vai notecējuši dokumenti. vai 3. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.2. punktā attiecībā uz būtisku uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Eiropas Parlamenta un Padomes Regulas (EK) Nr. 765/2008 ([1]) 2. panta 13. punktā, vai līdzvērtīga struktūra. vai 4. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir būtisks vai augsts, un ņem vērā personas identifikācijas datu maiņas riskus, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, būtiskais vai augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai.

Uzticamības līmenis	Nepieciešamie elementi
Augsts	Jāizpilda 1. vai 2. punkta prasības: 1. Jāizpilda būtiskais līmenis plus viena no alternatīvām a)–c) apakšpunktā: a) ja ir verificēts, ka personai ir fotogrāfiskās vai biometriskās identifikācijas pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un minētais pierādījums atspoguļo uzdoto identitāti, pierādījumu pārbauda, lai noteiktu, vai tas ir derīgs pēc autoritatīva avota ziņām, un pieteikuma iesniedzējs tiek identificēts ar uzdoto identitāti, salīdzinot vienu vai vairākas personas fiziskās īpašības ar autoritatīvu avotu; vai b) ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.2. punktā attiecībā uz augstu uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra, un tiek veikti pasākumi, kas pierāda, ka agrākās procedūras rezultāti vēl ir derīgi, vai c) ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir augsts, un ņem vērā personas identifikācijas datu maiņas riskus, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai, un tiek veikti pasākumi, kas pierāda, ka iepriekšējās šā izziņotā elektroniskās identifikācijas līdzekļa izdošanas procedūras rezultāti vēl ir derīgi. VAI 2. Ja pieteikuma iesniedzējs neuzrāda atzītu fotogrāfiskās vai biometriskās identifikācijas pierādījumu, piemēro tieši tās pašas procedūras, ko tāda atzīta fotogrāfiskās vai biometriskās identifikācijas pierādījuma iegūšanai valsts līmenī izmanto par reģistrāciju atbildīgās dalībvalsts vienība.

([1]) Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regula (EK) Nr. 765/2008, ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

2.1.3. Identitātes pierādīšana un verificēšana (juridiskai personai)

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli.

Uzticamības līmenis	Nepieciešamie elementi
	2. Pierādījumi šķietami ir derīgi un tos var uzskatīt par patiesiem vai pastāvošiem pēc autoritatīvu avota ziņām, ja juridiskas personas iekļāvums autoritatīvajā avotā ir brīvprātīgs un to reglamentē juridiskās personas un autoritatīvā avota vienošanās. 3. Autoritatīvam avotam nav zināms, ka juridiskā persona būtu statusā, kas tai neļauj rīkoties kā šai juridiskajai personai.
Būtisks	Jāizpilda zemais līmenis plus viena no alternatīvām 1.–3. punktā: 1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, ieskaitot juridiskās personas nosaukumu, juridisko formu un (attiecīgā gadījumā) reģistrācijas numuru, un pierādījumus pārbauda, lai noteiktu, vai tie ir patiesi vai pastāv pēc autoritatīva avota ziņām, ja juridiskajai personai ir jābūt iekļautai autoritatīvajā informācijas avotā, lai darbotos savā nozarē, un ir veikti pasākumi, lai minimalizētu risku, ka juridiskās personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēti, nozagti, apturēti, anulēti vai notecējuši dokumenti. vai 2. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.3. punktā attiecībā uz būtisku uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra. vai 3. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir būtisks vai augsts, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, būtiskais vai augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai.
Augsts	Jāizpilda būtiskais līmenis plus viena no alternatīvām 1.–3. punktā: 1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, ieskaitot juridiskās personas nosaukumu, juridisko formu un vismaz vienu unikālu identifikatoru, kas atspoguļo juridisko personu un ko lieto valsts vajadzībām, un ir pārbaudīts pierādījuma derīgums pēc autoritatīva avota ziņām. vai

Uzticamības līmenis	Nepieciešamie elementi
	2. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.3. punktā attiecībā uz augstu uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra, un tiek veikti pasākumi, kas pierāda, ka agrākās procedūras rezultāti vēl ir derīgi. vai 3. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir augsts, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai, un tiek veikti pasākumi, kas pierāda, ka iepriekšējās šā izziņotā elektroniskās identifikācijas līdzekļa izdošanas procedūras rezultāti vēl ir derīgi.

2.1.4. Fizisku un juridisku personu elektroniskās identifikācijas līdzekļu saistījums

Attiecīgos gadījumos uz starp fiziskas personas elektroniskās identifikācijas līdzekļa un juridiskas personas elektroniskās identifikācijas līdzekļa saistījumu ("saistījumu") attiecas šādi nosacījumi:

1. Jābūt iespējai saistījumu apturēt un/vai anulēt. Saistījuma darbības ciklu (piemēram, aktivizēšanu, apturēšanu, atjaunošanu, anulēšanu) pārvalda saskaņā ar valsts atzītām procedūrām.

2. Fiziska persona, kuras elektroniskās identifikācijas līdzeklis ir saistīts ar juridiskās personas elektroniskās identifikācijas līdzekli, var deleģēt saistījuma īstenošanu citai fiziskai personai, pamatojoties uz valsts atzītām procedūrām. Tomēr atbildība paliek deleģējošajai fiziskajai personai.

3. Saistījums veidojams šādi:

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu zemajā līmenī vai augstākā. 2. Saistījums ir izveidots, pamatojoties uz valsts atzītām procedūrām. 3. Autoritatīvam avotam nav zināms, ka fiziskā persona būtu statusā, kas tai neļauj rīkoties juridiskās personas vārdā.
Būtisks	Zemā līmeņa 3. punkts plus: 1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu būtiskajā vai augstajā līmenī.

Uzticamības līmenis	Nepieciešamie elementi
	2. Saistījums ir izveidots, pamatojoties uz valsts atzītām procedūrām, kuru rezultātā saistījums reģistrēts autoritatīvā avotā. 3. Saistījums ir verificēts, pamatojoties uz informāciju no autoritatīva avota.
Augsts	Zemā līmeņa 3. punkts un būtiskā līmeņa 2. punkts plus: 1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu augstajā līmenī. 2. Saistījums ir verificēts, pamatojoties uz unikālu identifikatoru, kas apzīmē juridisko personu un ko lieto valsts vajadzībām, un pamatojoties uz autoritatīva avota informāciju, kas unikāli apzīmē fizisko personu.

2.2. *Elektroniskās identifikācijas līdzekļu pārvaldība*

2.2.1. Elektroniskās identifikācijas līdzekļu īpašības un izveids

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Elektroniskās identifikācijas līdzeklis izmanto vismaz vienu autentifikācijas faktoru. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, ka izdevējs veic piemērotus pasākumus, lai pārliecinātos, ka to izmanto tikai tās personas kontrolē vai turējumā, kurai tas pieder.
Būtisks	1. Elektroniskās identifikācijas līdzeklis izmanto vismaz divus dažādu kategoriju autentifikācijas faktorus. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, lai var pieņemt, ka to izmanto tikai tad, ja tas ir tās personas kontrolē vai turējumā, kurai tas pieder.
Augsts	Būtiskais līmenis plus: 1. Elektroniskās identifikācijas līdzeklis sargā no dublēšanas un viltošanas, kā arī no uzbrucējiem ar augstu uzbrukuma potenciālu. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, lai persona, kurai tas pieder, to varētu droši aizsargāt tā, ka to neizmanto citi.

2.2.2. Izdošana, piegāde un aktivizācija

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pēc izdošanas elektroniskās identifikācijas līdzekli piegādā ar mehānismu, kura izmantošana ļauj pieņemt, ka tas nonāk tikai pie personas, kam tas paredzēts.
Būtisks	Pēc izdošanas elektroniskās identifikācijas līdzekli piegādā ar mehānismu, kura izmantošana ļauj pieņemt, ka tas nonāk tikai tās personas turējumā, kam tas pieder.
Augsts	Aktivizēšanas process verificē, vai elektroniskās identifikācijas līdzeklis ir nonācis tikai tās personas turējumā, kurai tas pieder.

2.2.3. Apturēšana, anulēšana un reaktivizācija

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Elektroniskās identifikācijas līdzekli ir iespējams laicīgi un efektīvi apturēt un/vai anulēt. 2. Ir veikti pasākumi, kas novērš neautorizētu apturēšanu, anulēšanu un/vai reaktivizāciju. 3. Reaktivizācija notiek tikai tad, ja joprojām tiek apmierinātas tādas pašas uzticamības prasības, kādas izvirzītas pirms apturēšanas vai anulēšanas.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.2.4. Atjaunošana un aizstāšana

Uzticamības līmenis	Nepieciešamie elementi
Zems	Ņemot vērā risku, ka var mainīties personas identifikācijas dati, atjaunošanai vai aizstāšanai jāizpilda tādas pašas uzticamības prasības kā sākotnējā identitātes pierādīšanā un verifikācijā vai ir jābūt balstītai uz derīgu tāda paša vai augstāka uzticamības līmeņa elektroniskās identifikācijas līdzekli.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Zemais līmenis plus: ja atjaunošana vai aizstāšana ir balstīta uz elektroniskās identifikācijas līdzekli, identitātes datus verificē pēc autoritatīva avota.

2.3. *Autentifikācija*

Šajā punktā uzmanība veltīta briesmām, kas saistās ar autentifikācijas mehānisma lietošanu, un uzskaitītas prasības katrā uzticamības līmenī. Šajā punktā tiek uzskatīts, ka kontrole ir samērīga ar riskiem dotajā līmenī.

2.3.1. Autentifikācijas mehānisms

Tabulā ir izklāstītas prasības katrā uzticamības līmenī attiecībā uz autentifikācijas mehānismu, kurā fiziskā vai juridiskā persona izmanto elektroniskās identifikācijas līdzekli, lai apstiprinātu savu identitāti pārbaudītājam.

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pirms personas identifikācijas datu izlaišanas tiek droši verificēts elektroniskās identifikācijas līdzeklis un tā derīgums. 2. Ja personas identifikācijas dati tiek glabāti kā daļa no autentifikācijas mehānisma, minētā informācija ir aizsargāta, lai nodrošinātos pret nozaudēšanu un drošības politikas pārkāpumiem, ieskaitot analīzi bezsaistē. 3. Autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar vairāk nekā parastu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.

Uzticamības līmenis	Nepieciešamie elementi
Būtisks	Zemais līmenis plus: 1. Pirms personas identifikācijas datu izlaišanas ar dinamisko autentifikāciju tiek droši verificēts elektroniskās identifikācijas līdzeklis un tā derīgums. 2. Autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar vidēji augstu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.
Augsts	Būtiskais līmenis plus: autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar augstu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.

2.4. *Pārvaldība un organizācija*

Visiem dalībniekiem, kas ar elektronisko identifikāciju saistītu pakalpojumu sniedz pārrobežu kontekstā ("pakalpojuma sniedzēji"), ir jābūt dokumentētai informācijas drošības pārvaldības praksei, rīcības politikai, riska pārvaldības pieejām un citiem atzītiem kontroles līdzekļiem, lai attiecīgām elektroniskās identifikācijas shēmu vadības struktūrām attiecīgajās dalībvalstīs sniegtu pārliecību, ka pastāv efektīva prakse. Visā 2.4. punktā visas prasības/elementus uzskata par samērīgiem ar dotā līmeņa riskiem.

2.4.1. Vispārīgi noteikumi

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pakalpojuma sniedzēji, kas nodrošina darbības pakalpojumus, uz ko attiecas šī regula, ir publiska iestāde vai juridiska vienība, ko par tādu atzīst kādas dalībvalsts tiesību akti un kam ir izveidota organizatoriskā struktūra un pilnībā darbojas visas daļas, kas vajadzīgas pakalpojumu sniegšanai. 2. Pakalpojumu sniedzēji ievēro juridiskās prasības, kas tiem izvirzītas sakarā ar darbību un pakalpojuma sniegšanu, ieskaitot jautājumos par pieprasāmās informācijas veidiem, identitātes pierādīšanas veidu, par to, kāda informāciju drīkst paturēt un cik ilgi. 3. Pakalpojumu sniedzēji spēj pierādīt spēju uzņemties risku sakarā ar atbildību par zaudējumiem, kā arī to, ka viņiem pietiek finanšu resursu nepārtrauktai darbībai un pakalpojumu sniegšanai. 4. Pakalpojumu sniedzēji atbild par citām vienībām ārpakalpojumu veidā nodoto saistību izpildi un par to, lai shēmas politika būtu ievērota tā, it kā pienākumus būtu pildījuši paši pakalpojumu sniedzēji. 5. Elektroniskās identifikācijas shēmām, kas nav izveidotas ar valsts tiesību aktiem, ir jābūt efektīvam darbības izbeigšanas plānam. Plānā jābūt noteiktai kārtībai, kā pakalpojums tiek izbeigts vai kā to turpina cits pakalpojumu sniedzējs, kā informējamas attiecīgās iestādes un galalietotāji, kā arī ziņas par to, kā uzskaites dati ir jāaizsargā, jāsaglabā un jāiznīcina saskaņā ar shēmas politiku.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.2. Publicētie paziņojumi un informācija lietotājiem

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Ir publicēta pakalpojuma definīcija, kas aptver visus piemērojamos noteikumus un maksas, ieskaitot tā izmantošanas ierobežojumus (ja tādi ir). Pakalpojuma definīcijā ietilpst privātuma politika. 2. Ir jāievieš atbilstoša politika un procedūras, lai nodrošinātu, ka pakalpojuma lietotāji laicīgi un droši tiek informēti par izmaiņām pakalpojuma definīcijā un piemērojamajos noteikumos un privātuma politikā. 3. Ir jāievieš atbilstoša rīcības politika un procedūras, kas nodrošina pilnīgas un pareizas atbildes uz informācijas pieprasījumiem.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.3. Informācijas drošības pārvaldība

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pastāv efektīva informācijas drošības pārvaldības sistēma informācijas drošības risku pārvaldībai un kontrolei.
Būtisks	Zemais līmenis plus: informācijas drošības pārvaldības sistēma ievēro pārbaudītus informācijas drošības risku pārvaldības un kontroles standartus vai principus.
Augsts	Tāpat kā būtiskajā līmenī.

2.4.4. Uzskaite

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Reģistrē un uztur attiecīgu informāciju, izmantojot efektīvu uzskaitvedības sistēmu, ņemot vērā piemērojamos tiesību aktus un labu praksi, kas attiecas uz datu aizsardzību un datu saglabāšanu. 2. Saglabā, cik to ļauj valsts tiesību akti vai citi valsts administratīvi noteikumi, un aizsargā uzskaites datus tik ilgi, kamēr tie ir nepieciešami revīzijai un drošības pārkāpumu izmeklēšanai, un saglabāšanai, pēc kuras uzskaites datus drošā veidā iznīcina.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.5. Iekārtas un personāls

Tabulā ir norādītas prasības iekārtām un darbiniekiem un – attiecīgā gadījumā – apakšuzņēmējiem, kas uzņemas pienākumus, uz kuriem attiecas šī regula. Katras prasības izpilde ir proporcionāla riskam, kas saistās ar uzticamības līmeni.

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pastāv procedūras, kas nodrošina, ka darbinieki un apakšuzņēmēji ir pietiekami apmācīti, kvalificēti un pieredzējuši prasmēs, kas nepieciešamas viņu funkciju pildīšanai. 2. Pietiek personāla un apakšuzņēmēju pakalpojuma pienācīgai sniegšanai un apgādei ar resursiem saskaņā ar tā politiku un procedūrām. 3. Iekārtas, ko izmanto pakalpojuma sniegšanai, pastāvīgi uzrauga un aizsargā pret dabas untumu nodarīto kaitējumu, neatļautu piekļuvi un citiem faktoriem, kas var ietekmēt pakalpojuma drošību. 4. Pakalpojuma sniegšanai izmantojamās iekārtas nodrošina piekļūšanu personas datu un kriptogrāfiskas vai citādas sensitīvas informācijas apstrādes zonām tikai pilnvarotiem darbiniekiem vai apakšuzņēmējiem.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.6. Tehniskā kontrole

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Samērīga tehniskā kontrole, aizsargādama apstrādātās informācijas konfidencialitāti, integritāti un pieejamību, pārvalda riskus, kas apdraud pakalpojumu drošību. 2. Elektronisko sakaru kanāli, ko izmanto personas datu vai sensitīvas informācijas apmaiņai, ir aizsargāti no pārtveršanas, manipulēšanas un pārspēlēšanas. 3. Piekļuve sensitīviem kriptogrāfiskiem materiāliem, ko izmanto elektroniskās identifikācijas līdzekļu izdošanai un autentifikācijai, tiek dota tikai funkcijām un lietojumiem, kam piekļuve noteikti nepieciešama. Ir jānodrošina, ka šādus materiālus nekad pastāvīgi neuzglabā kā vienkāršu tekstu. 4. Pastāv procedūras, kas nodrošina, ka drošība tiek uzturēta pastāvīgi un ka ir spēja reaģēt uz riska līmeņa maiņu, incidentiem un drošības pārkāpumiem. 5. Visus informācijas nesējus ar personas datiem, kriptogrāfisku vai citādu sensitīvu informāciju uzglabā, pārvadā un likvidē drošā un aizsargātā veidā.
Būtisks	Tāpat kā zemajā līmenī plus: sensitīvi kriptogrāfiskie materiāli, ko izmanto elektroniskās identifikācijas līdzekļu izdošanai un autentifikācijai, ir aizsargāti no viltošanas.
Augsts	Tāpat kā būtiskajā līmenī.

2.4.7. Atbilstība un revīzija

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pastāv regulāra iekšējā revīzija, kas aptver visas daļas, kuras attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai.

Uzticamības līmenis	Nepieciešamie elementi
Būtisks	Pastāv regulāra neatkarīga iekšējā revīzija vai ārējā revīzija, kas aptver visas daļas, kuras attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai.
Augsts	1. Pastāv regulāra neatkarīga ārējā revīzija, kas aptver visas daļas, kas attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai. 2. Ja shēmu tieši pārvalda valsts pārvaldes struktūra, shēmas revīziju veic saskaņā ar attiecīgās valsts tiesību aktiem.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2015/1503

(2015. gada 8. septembris),

ar kuru nosaka standarta importa vērtības atsevišķu veidu augļu un dārzeņu ievešanas cenas noteikšanai

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2013. gada 17. decembra Regulu (ES) Nr. 1308/2013, ar ko izveido lauksaimniecības produktu tirgu kopīgu organizāciju un atceļ Padomes Regulas (EEK) Nr. 922/72, (EEK) Nr. 234/79, (EK) Nr. 1037/2001 un (EK) Nr. 1234/2007 ([1]),

ņemot vērā Komisijas 2011. gada 7. jūnija Īstenošanas regulu (ES) Nr. 543/2011, ar ko nosaka sīki izstrādātus noteikumus Padomes Regulas (EK) Nr. 1234/2007 piemērošanai attiecībā uz augļu un dārzeņu un pārstrādātu augļu un dārzeņu nozari ([2]), un jo īpaši tās 136. panta 1. punktu,

tā kā:

(1) Īstenošanas regulā (ES) Nr. 543/2011, piemērojot Urugvajas kārtas daudzpusējo tirdzniecības sarunu iznākumu, paredzēti kritēriji, pēc kuriem Komisija nosaka standarta importa vērtības minētās regulas XVI pielikuma A daļā norādītajiem produktiem no trešām valstīm un laika periodiem.

(2) Standarta importa vērtību aprēķina katru darbdienu saskaņā ar Īstenošanas regulas (ES) Nr. 543/2011 136. panta 1. punktu, ņemot vērā mainīgos dienas datus. Tāpēc šai regulai būtu jāstājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Standarta importa vērtības, kas paredzētas Īstenošanas regulas (ES) Nr. 543/2011 136. pantā, ir tādas, kā norādīts šīs regulas pielikumā.

2. pants

Šī regula stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas

un tās priekšsēdētāja vārdā –

lauksaimniecības un lauku attīstības ģenerāldirektors

Jerzy PLEWA

([1]) OV L 347, 20.12.2013., 671. lpp.
([2]) OV L 157, 15.6.2011., 1. lpp.

PIELIKUMS

Standarta importa vērtības atsevišķu veidu augļu un dārzeņu ievešanas cenas noteikšanai

(EUR/100 kg)

KN kods	Trešās valsts kods (1)	Standarta importa vērtība
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 kods	Trešās valsts kods (1)	Standarta importa vērtība
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Valstu nomenklatūra, kas paredzēta Komisijas 2012. gada 27. novembra Regulā (ES) Nr. 1106/2012, ar ko attiecībā uz valstu un teritoriju nomenklatūras atjaunināšanu īsteno Eiropas Parlamenta un Padomes Regulu (EK) Nr. 471/2009 par Kopienas statistiku attiecībā uz ārējo tirdzniecību ar ārpuskopienas valstīm (OV L 328, 28.11.2012., 7. lpp.). Kods "ZZ" nozīmē "cita izcelsme".

LĒMUMI

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2015/1504

(2015. gada 7. septembris),

ar kuru dažām dalībvalstīm piešķir atkāpes attiecībā uz statistikas datu sniegšanu saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1099/2008 par enerģētikas statistiku

(izziņots ar dokumenta numuru C(2015) 6105)

(Autentisks ir tikai teksts franču, grieķu, igauņu, nīderlandiešu un slovāku valodā)

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2008. gada 22. oktobra Regulu (EK) Nr. 1099/2008 par enerģētikas statistiku ([1]) un jo īpaši tās 5. panta 4. punktu un 10. panta 2. punktu,

tā kā:

(1) Saskaņā ar Regulas (EK) Nr. 1099/2008 5. panta 4. punktu pēc pienācīgi pamatota dalībvalsts pieprasījuma var piešķirt atkāpes no tādu valsts statistikas datu apkopošanas, kuru vākšana radītu pārmērīgu slogu respondentiem.

(2) Beļģija, Igaunija, Kipra un Slovākija iesniedza pieteikumus atkāpju saņemšanai attiecībā uz statistikas datu sniegšanu par detalizētu enerģijas patēriņu mājsaimniecībās pa galaizlietojuma veidiem par atsevišķiem pārskata gadiem.

(3) Šo dalībvalstu sniegtā informācija pamato to, ka atkāpes būtu jāpiešķir.

(4) Šajā lēmumā paredzētie pasākumi ir saskaņā ar Eiropas Statistikas sistēmas komitejas atzinumu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Ar šo piešķir šādas atkāpes no Regulas (EK) Nr. 1099/2008 noteikumiem:

1) Beļģijai piešķir atkāpi no rezultātu sniegšanas par 2015. pārskata gadu attiecībā uz 1.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 2.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 3.2.3. punkta posteņiem 3.1. līdz 3.6., 4.2.3. punkta posteņiem 7.2.1. līdz 7.2.5. un 5.2.4. punkta posteņiem 4.2.1. līdz 4.2.5. B pielikumā par detalizētiem statistikas datiem par enerģijas patēriņu mājsaimniecībās pa galaizlietojuma veidiem (kā noteikts A pielikuma 2.3. punkta 26. postenī "Citi sektori – dzīvojamais sektors");

([1]) OV L 304, 14.11.2008., 1. lpp.

2) Igaunijai piešķir atkāpi no rezultātu sniegšanas par 2015., 2016. un 2017. pārskata gadu attiecībā uz 1.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 2.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 3.2.3. punkta posteņiem 3.1. līdz 3.6., 4.2.3. punkta posteņiem 7.2.1. līdz 7.2.5. un 5.2.4. punkta posteņiem 4.2.1. līdz 4.2.5. B pielikumā par detalizētiem statistikas datiem par enerģijas patēriņu mājsaimniecībās pa galaizlietojuma veidiem (kā noteikts A pielikuma 2.3. punkta 26. postenī "Citi sektori – dzīvojamais sektors");

3) Kiprai piešķir atkāpi no rezultātu sniegšanas par 2015., 2016. un 2017. pārskata gadu attiecībā uz 1.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 2.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 3.2.3. punkta posteņiem 3.1. līdz 3.6. un 5.2.4. punkta posteņiem 4.2.1. līdz 4.2.5. B pielikumā par detalizētiem statistikas datiem par enerģijas patēriņu mājsaimniecībās pa galaizlietojuma veidiem (kā noteikts A pielikuma 2.3. punkta 26. postenī "Citi sektori – dzīvojamais sektors");

4) Slovākijai piešķir atkāpi no rezultātu sniegšanas par 2015. un 2016. pārskata gadu attiecībā uz 1.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 2.2.3. punkta posteņiem 4.2.1. līdz 4.2.5., 3.2.3. punkta posteņiem 3.1. līdz 3.6., 4.2.3. punkta posteņiem 7.2.1. līdz 7.2.5. un 5.2.4. punkta posteņiem 4.2.1. līdz 4.2.5. B pielikumā par detalizētiem statistikas datiem par enerģijas patēriņu mājsaimniecībās pa galaizlietojuma veidiem (kā noteikts A pielikuma 2.3. punkta 26. postenī "Citi sektori – dzīvojamais sektors").

2. pants

Šis lēmums ir adresēts Beļģijas Karalistei, Igaunijas Republikai, Kipras Republikai un Slovākijas Republikai.

Briselē, 2015. gada 7. septembrī

Komisijas vārdā –
Komisijas locekle
Marianne THYSSEN

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2015/1505

(2015. gada 8. septembris),

kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 22. panta 5. punktu izklāstītas tehniskās specifikācijas un formāti, kas attiecas uz uzticamības sarakstiem

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 22. panta 5. punktu,

tā kā:

(1) Uzticamības sarakstiem ir būtiska nozīme uzticēšanās veidošanā tirgus operatoru starpā, jo tajos norādīts pakalpojumu sniedzēja statuss pārraudzības brīdī.

(2) Elektronisko parakstu pārrobežu izmantošanu veicināja Komisijas Lēmums 2009/767/EK ([2]), kas noteica pienākumu dalībvalstīm izveidot, uzturēt un publicēt uzticamības sarakstus, kuros ir informācija, kas attiecas uz sertifikācijas pakalpojumu sniedzējiem, kuri izdod kvalificētus sertifikātus sabiedrībai saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 1999/93/EK ([3]) un kurus pārrauga un akreditē dalībvalstis.

(3) Regulas (ES) Nr. 910/2014 22. pantā dalībvalstīm uzlikts par pienākumu izveidot, uzturēt un publicēt uzticamības sarakstus aizsargātā veidā, elektroniski parakstītus vai apzīmogotus, automatizētai apstrādei piemērotā formā un paziņot Komisijai, kuras struktūras atbild par valsts uzticamības sarakstu izveidi.

(4) Uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi būtu jāuzskata par kvalificētiem, ja kvalifikācijas statuss tiek saistīts ar pakalpojumu sniedzēju uzticamības sarakstā. Lai nodrošinātu, ka citus Regulas (ES) Nr. 910/2014 uzliktos pienākumus, it īpaši 27. un 37. pantā noteiktos, pakalpojumu sniedzēji var viegli izpildīt no attāluma ar elektroniskiem līdzekļiem, un nekaitētu to citu sertifikācijas pakalpojumu sniedzēju tiesiskajai paļāvībai, kuri neizdod kvalificētus sertifikātus, bet sniedz ar elektroniskajiem parakstiem saistītus pakalpojumus saskaņā ar Direktīvu 1999/93/EK un ir uzskaitē līdz 2016. gada 30. jūnijam, būtu jāparedz iespēja dalībvalstīm brīvprātīgi valsts līmenī pievienot sarakstam uzticamības pakalpojumus, kas nav kvalificēti uzticamības pakalpojumi, ar noteikumu, ka tiek skaidri norādīts, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

(5) Saskaņā ar Regulas (ES) Nr. 910/2014 25. apsvērumu dalībvalstis var pievienot sarakstam arī tādus valsts noteiktus uzticamības pakalpojumu veidus, kas nav definēti Regulas (ES) Nr. 910/2014 3. panta 16. punktā, ar noteikumu, ka tiek skaidri norādīts, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

(6) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) Nr. 910/2014 48. pantu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Dalībvalstis izveido, publicē un uztur uzticamības sarakstus, kuros ir informācija par kvalificētu uzticamības pakalpojumu sniedzējiem, ko tās pārrauga, kā arī informācija par to sniegtajiem kvalificētajiem uzticamības pakalpojumiem. Minētie saraksti atbilst I pielikumā izklāstītajām tehniskajām specifikācijām.

([1]) OV L 257, 28.8.2014., 73. lpp.
([2]) Komisijas 2009. gada 16. oktobra Lēmums 2009/767/EK par pasākumiem, lai veicinātu procedūru veikšanu elektroniski, izmantojot vienotos kontaktpunktus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2006/123/EK par pakalpojumiem iekšējā tirgū (OV L 274, 20.10.2009., 36. lpp.).
([3]) Eiropas Parlamenta un Padomes 1999. gada 13. decembra Direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu (OV L 13, 19.1.2000., 12. lpp.).

2. pants

Uzticamības sarakstos dalībvalstis drīkst iekļaut informāciju par nekvalificētu uzticamības pakalpojumu sniedzējiem kopā ar informāciju par nekvalificētajiem uzticamības pakalpojumiem, ko tie sniedz. Sarakstā skaidri norāda, kuri uzticamības pakalpojumu sniedzēji un to sniegtie uzticamības pakalpojumi nav kvalificēti.

3. pants

1. Saskaņā ar Regulas (ES) Nr. 910/2014 22. panta 2. punktu dalībvalstis elektroniski paraksta vai apzīmogo sava uzticamības saraksta automatizētai apstrādei piemēroto formu saskaņā ar I pielikumā izklāstītajām tehniskajām specifikācijām.

2. Ja dalībvalsts elektroniski publicē cilvēklasāmu uzticamības saraksta formu, tā nodrošina, ka šajā uzticamības saraksta formā ir tie paši dati, kas automatizēti apstrādājamā formā, un to paraksta vai apzīmogo elektroniski saskaņā ar I pielikumā izklāstītajām tehniskajām specifikācijām.

4. pants

1. Regulas (ES) Nr. 910/2014 22. panta 3. punktā minēto informāciju dalībvalstis dara zināmu Komisijai, izmantojot II pielikuma veidni.

2. 1. punktā minētajā informācijā ietilpst divi vai vairāki shēmas operatora publiskās atslēgas sertifikāti ar vismaz trīs mēnešu derīguma termiņa nobīdi, kuri atbilst privātajām atslēgām, ko var izmantot, lai elektroniski parakstītu vai apzīmogotu automatizētai apstrādei piemēroto uzticamā saraksta formu un cilvēklasāmo formu, kad tā publicēta.

3. Saskaņā ar Regulas (ES) Nr. 910/2014 22. panta 4. punktu Komisija pa aizsargātu kanālu autentificētā tīmekļa serverī publisko dalībvalstu piegādāto 1. un 2. punktā minēto informāciju parakstītā vai apzīmogotā automatizētai apstrādei piemērotā formā.

4. Komisija var dalībvalstu piegādāto 1. un 2. punktā minēto informāciju parakstītā vai apzīmogotā cilvēklasāmā formā pa aizsargātu kanālu publiskot autentificētā tīmekļa serverī.

5. pants

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šis lēmums uzliek saistības kopumā un ir tieši piemērojams visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas vārdā –

priekšsēdētājs

Jean-Claude JUNCKER

I PIELIKUMS

VIENOTĀS UZTICAMĪBAS SARAKSTU VEIDNES TEHNISKĀS SPECIFIKĀCIJAS

I NODAĻA

VISPĀRĪGAS PRASĪBAS

Uzticamības sarakstā iekļauj gan kārtējo, gan visu senāko informāciju par sarakstā minēto uzticamības pakalpojumu statusu no brīža, kad uzticamības pakalpojuma sniedzējs iekļauts uzticamības sarakstos.

Jēdzieni "apstiprināt", "akreditēt" un/vai "pārraudzīt" šajās specifikācijās aptver arī valsts apstiprināšanas shēmas, taču papildinformāciju par tādu valsts shēmu īpatnībām dalībvalstis sniegs savos uzticamības sarakstos līdz ar skaidrojumu par iespējamām atšķirībām no pārraudzības shēmām, ko piemēro uzticamības pakalpojuma sniedzējiem un kvalificētajiem uzticamības pakalpojumiem, kurus tie sniedz.

Uzticamības sarakstā sniegtās informācijas galvenais mērķis ir atbalstīt kvalificētu uzticamības pakalpojumu marķieru validēšanu; marķieri ir kvalificētu uzticamības pakalpojumu rezultātā ģenerēti vai izdoti fiziski vai bināri (loģiskie) objekti, kā kvalificēti elektroniskie paraksti/zīmogi, uzlaboti elektroniskie paraksti/zīmogi, kurus balsta kvalificēts sertifikāts, kvalificēti laika zīmogi, kvalificēti elektroniskie piegādes pierādījumi utt.

II NODAĻA

VIENOTĀS UZTICAMĪBAS SARAKSTU VEIDNES DETALIZĒTAS SPECIFIKĀCIJAS

Šīs specifikācijas ir balstītas uz specifikācijām un prasībām, kas noteiktas ETSI TS 119 612 v2.1.1 (turpmāk "ETSI TS 119 612").

Ja šajās specifikācijās nav izvirzītas īpašas prasības, pilnībā piemēro ETSI TS 119 612 5. un 6. punkta prasības. Ja šajās specifikācijās ir izvirzītas īpašas prasības, tās ir pārākas par attiecīgajām ETSI TS 119 612 prasībām. Ja ir neatbilstības starp šīm specifikācijām un ETSI TS 119 612 specifikācijām, pārākas ir šīs specifikācijas.

Scheme name (5.3.6. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.6. punktā, un shēmai izmanto šādu nosaukumu:

"*EN_name_value*" = "*Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) 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.*"

Scheme information URI (5.3.7. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.7. punktā, un "pienācīgajā informācijā par shēmu" tiek iekļauti vismaz šādi dati:

a) visām dalībvalstīm kopīga ievada informācija par uzticamības saraksta darbības jomu un kontekstu, pamatā esošo pārraudzības shēmu un – attiecīgā gadījumā – valsts apstiprināšanas (piem., akreditācijas) shēmām. Izmantojamais kopīgais teksts ir tālākais teksts, kurā rakstzīmju virkni "[*attiecīgās dalībvalsts nosaukums*]" aizstāj ar attiecīgās dalībvalsts nosaukumu:

> "Šis saraksts ir uzticamības saraksts, kurā iekļauta informācija par kvalificēta uzticamības pakalpojuma sniedzējiem, kurus pārrauga [*attiecīgās dalībvalsts nosaukums*], kā arī informācija par kvalificētajiem uzticamības pakalpojumiem, ko tie sniedz, saskaņā ar attiecīgajiem noteikumiem Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulā (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK.

Elektronisko parakstu pārrobežu izmantošanu veicinājis Komisijas 2009. gada 16. oktobra Lēmums 2009/767/EK, kas uzliek dalībvalstīm par pienākumu izveidot, uzturēt un publicēt uzticamības sarakstus ar informāciju par sertifikācijas pakalpojumu sniedzējiem, kuri izsniedz kvalificētus sertifikātus sabiedrībai saskaņā ar Eiropas Parlamenta un Padomes 1999. gada 13. decembra Direktīvu 1999/93/EK par Kopienas elektronisko parakstu sistēmu un kuru pārraudzību/akreditāciju veic dalībvalstis. Šis uzticamības saraksts ir ar Lēmumu 2009/767/EK izveidotā uzticamības saraksta turpinājums."

Uzticamības sarakstiem ir būtiska nozīme, veidojot uzticēšanos starp elektronisko sakaru tirgus operatoriem, jo tie ļauj lietotājiem noskaidrot uzticamības pakalpojumu sniedzēju un to pakalpojumu kvalifikācijas statusu un tā vēsturi.

Dalībvalstu uzticamības sarakstos tiek iekļauta vismaz Komisijas Īstenošanas lēmuma (ES) 2015/1505 1. un 2. pantā noteiktā informācija.

Dalībvalstis var uzticamības sarakstos iekļaut informāciju par nekvalificētiem uzticamības pakalpojumu sniedzējiem un informāciju par nekvalificētajiem uzticamības pakalpojumiem, ko tie sniedz. Ir skaidri jānorāda, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

Dalībvalstis var uzticamajā sarakstā iekļaut informāciju par valsts līmenī definētiem tādu veidu uzticamības pakalpojumiem, kas nav definēti Regulas (ES) Nr. 910/2014 3. panta 16. punktā. Ir skaidri jānorāda, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014;

b) īpaša informācija par pamatā esošo pārraudzības shēmu un – vajadzības gadījumā – valsts apstiprināšanas (piemēram, akreditācijas) shēmām, it īpaši ([1]):

1) informācija par valsts pārraudzības shēmu, kas piemērojama kvalificētiem un nekvalificētiem uzticamības pakalpojumu sniedzējiem un kvalificētajiem un nekvalificētajiem uzticamības pakalpojumiem, ko reglamentē Regula (ES) Nr. 910/2014;

2) attiecīgā gadījumā – informācija par valsts brīvprātīgās akreditācijas shēmām, ko piemēro sertifikācijas pakalpojumu sniedzējiem, kuri izdevuši kvalificētus sertifikātus saskaņā ar Direktīvu 1999/93/EK.

Šajā īpašajā informācijā par katru iepriekš uzskaitīto pamatā esošo shēmu iekļauj vismaz šādus datus:

1) vispārīgu aprakstu;

2) informāciju par procesu, kas jāievēro valstu uzraudzības sistēmā un – vajadzības gadījumā – apstiprināšanā saskaņā ar valsts apstiprināšanas shēmu;

3) informāciju par kritērijiem, pēc kuriem uzticamības pakalpojumu sniedzējus pārrauga vai attiecīgā gadījumā apstiprina;

4) informāciju par kritērijiem un noteikumiem, ko izmanto, lai izraudzītu pārraugus/revidentus, un par to, kā tie novērtē uzticamības pakalpojumu sniedzējus un to sniegtos uzticamības pakalpojumus;

5) attiecīgā gadījumā – citu kontaktinformāciju un vispārīgu informāciju, kas attiecas uz shēmas darbību.

Scheme type/community/rules (5.3.9. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.9. punktā.

Tas ietver *URI* tikai AK angļu valodā.

([1]) Šiem informācijas kopumiem ir izšķiroša nozīme, lai atkarīgās puses varētu novērtēt šādu sistēmu kvalitātes un drošības līmeni. Šos informācijas kopumus nodrošina uzticamības saraksta līmenī, izmantojot pašreizējos laukus "Scheme information URI" (5.3.7. punkts – dalībvalsts sniegtā informācija), "Scheme type/community/rules" (5.3.9. punkts – izmantojot visām dalībvalstīm kopīgu tekstu) un "TSL policy/legal notice" (5.3.11. punkts – visām dalībvalstīm kopīgs teksts, kā arī iespēja katrai dalībvalstij pievienot specifisku tekstu/atsauces). Attiecīgā gadījumā un pēc vajadzības pakalpojuma līmenī var sniegt papildinformāciju par šādām sistēmām, kas attiecas uz nekvalificētiem uzticamības pakalpojumiem un valsts līmenī definētiem (kvalificētiem) uzticamības pakalpojumiem (piemēram, lai nošķirtu vairākus kvalitātes/drošības līmeņus), izmantojot lauku "Scheme service definition URI" (5.5.6. punkts).

Tas ietver vismaz divus *URI*:

1) vienu šādu *URI*, kas kopīgs visu dalībvalstu uzticamības sarakstiem un norāda uz aprakstošu tekstu, kurš piemērojams visiem uzticamības sarakstiem:

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

Aprakstošais teksts:

"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 (EU) 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 (EU) 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 (EU) 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 (EU) 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, etc.). 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 (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.";

2) vienu *URI*, kas specifisks katras dalībvalsts uzticamības sarakstam un norāda uz aprakstošo tekstu, kurš piemērojams šās dalībvalsts uzticamības sarakstam:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kur CC ir ISO 3166-1 ([1]) valsts divburtu kods, kas lietots laukā "Scheme territory" (5.3.10. punkts),

— kur lietotāji var iegūt ziņas par attiecīgās dalībvalsts īpašo politiku/noteikumiem, pēc kuriem tiek novērtēti sarakstā iekļautie uzticamības pakalpojumi atbilstoši dalībvalsts attiecīgajai pārraudzības sistēmai un – attiecīgos gadījumos – apstiprināšanas shēmai,

— kur lietotāji var iegūt attiecīgās dalībvalsts norādīto īpašo aprakstu par to, kā izmantot un interpretēt uzticamības saraksta saturu, kas attiecas uz sarakstā iekļautajiem nekvalificētajiem uzticamības pakalpojumiem un/vai valsts līmenī definētajiem uzticamības pakalpojumiem. To var izmantot, lai norādītu potenciālo granularitāti valsts apstiprināšanas sistēmās, kas saistītas ar *CSP*, kuri neizsniedz *QC*, un to, kā šim nolūkam izmanto laukus "Scheme service definition URI" (5.5.6. punkts) un "Service information extension" (5.5.9. punkts).

Dalībvalstis var definēt un izmantot papildu *URI*, kas paplašina iepriekš norādīto dalībvalstij specifisko *URI* (t. i., *URI*, kas definēti no šā hierarhiskā specifiskā *URI*).

TSL policy/legal notice (5.3.11. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.11. punktā, un tajā politikas/juridiskais paziņojums par shēmas juridisko statusu vai juridiskajām prasībām, kuras shēma ievēro saskaņā ar jurisdikciju, kurā tā ir reģistrēta,

([1]) ISO 3166-1:2006: "Valstu un to administratīvi teritoriālā iedalījuma vienību nosaukumu kodi. 1. daļa: Valstu kodi"

un/vai jebkuri ierobežojumi un nosacījumi, ar kuriem uzticamības saraksts tiek uzturēts un publicēts, ir daudzvalodu rakstzīmju virkne (sk. 5.1.4. punktu), kas obligāti AK angļu valodā un fakultatīvi vienā vai vairākās valstu valodās sniedz faktisko politikas/juridiskā paziņojuma tekstu ar šādu uzbūvi:

1. Pirmā, obligātā, visu dalībvalstu uzticamajiem sarakstiem kopīgā daļa, kas norāda uz piemērojamo tiesisko regulējumu un kuras teksts angļu valodā ir šāds:

   "*The applicable legal framework for the present trusted list is Regulation (EU) 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.*"

   Teksts dalībvalsts valodā:

   "Šim uzticamības sarakstam piemērojamais tiesiskais regulējums ir Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK."

2. Otra, fakultatīva, katram uzticamības sarakstam specifiska daļa, ar atsaucēm uz īpašu piemērojamo valsts tiesisko regulējumu.

Service current status (5.5.4. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.5.4. punktā.

ES dalībvalstu uzticamības sarakstā uzskaitīto pakalpojumu "Service current status" vērtības dienā pirms Regulas (ES) Nr. 910/2014 piemērošanas sākuma (t. i., 2016. gada 30. jūnija) migrēšanu veic regulas piemērošanas sākuma dienā (t. i., 2016. gada 1. jūlijā), kā norādīts ETSI TS 119 612 J pielikumā.

III NODAĻA

UZTICAMĪBAS SARAKSTU NEPĀRTRAUKTĪBA

Sertifikāti, par kuriem jāpaziņo Komisijai saskaņā ar šā lēmuma 4. panta 2. punktu, atbilst 5.7.1. punkta prasībām no ETSI TS 119 612, un tos izdod tādā veidā, ka:

— to derīguma termiņš atšķiras vismaz par trim mēnešiem ("Not After")

— un tos rada ar jauniem atslēgu pāriem. Agrāk izmantotus atslēgu pārus nedrīkst pārsertificēt.

Ja ir notecējis viens no publiskās atslēgas sertifikātiem, ko var izmantot uzticamības saraksta paraksta vai zīmoga validēšanai, par kuru ir paziņots Komisijai un kas ir publicēts Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— gadījumā, ja publicētais uzticamības saraksts bijis parakstīts vai apzīmogots ar privāto atslēgu, kuras publiskās atslēgas sertifikāts ir notecējis, nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar privāto atslēgu, kuras izziņotais publiskās atslēgas sertifikāts nav notecējis,

— pēc vajadzības ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

Ja ir kompromitēta vai norakstīta viena no privātajām atslēgām, kas atbilst publiskās atslēgas sertifikātam, kuru var izmantot uzticamības saraksta paraksta validēšanai un kurš ir paziņots Komisijai un publicēts Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar nekompromitētu privāto atslēgu, gadījumā, ja publicētais uzticamības saraksts ticis parakstīts ar kompromitētu vai norakstītu privātu atslēgu,

— pēc vajadzības ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

Ja ir kompromitētas vai norakstītas visas privātās atslēgas, kas atbilst publiskās atslēgas sertifikātiem, kurus var izmantot uzticamības saraksta paraksta validēšanai un kuri ir paziņoti Komisijai un publicēti Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar vienu no šīm jaunajām privātajām atslēgām un par kura atbilstošo publiskās atslēgas sertifikātu ir jāpaziņo,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

IV NODAĻA

UZTICAMĪBAS SARAKSTA CILVĒKLASĀMĀS FORMAS SPECIFIKĀCIJAS

Ja izveido un publicē uzticamības saraksta cilvēklasāmo formu, tā sniedzama ISO 32000 ([1]) atbilstoša pārnesama dokumentu formāta (*PDF*) veidā, kas formatēts saskaņā ar profilu *PDF/A* (ISO 19005 ([2])).

Uz *PDF/A* balstītās uzticamības saraksta cilvēklasāmās formas saturam jāatbilst šādām prasībām:

— cilvēklasāmās formas struktūrai jāatspoguļo loģiskais modelis, kas aprakstīts TS 119 612,

— jāattēlo katrs ietvertais lauks, un tajā jānorāda:

  — lauka nosaukums (piemēram, *Service type identifier*),

  — lauka vērtība (piemēram, "http://uri.etsi.org/TrstSvc/Svctype/CA/QC"),

  — attiecīgā gadījumā – lauka vērtības nozīme (apraksts) (piemēram, "*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*");

  — attiecīgā gadījumā – vairākas versijas dabiskajās valodās, kas paredzētas uzticamības sarakstā;

— cilvēklasāmajā formā norāda vismaz šādus laukus un atbilstošās laukā "Service digital identity" norādīto digitālo sertifikātu vērtības ([3]):

  — versija,

  — sertifikāta sērijas numurs,

  — paraksta algoritms,

  — izdevējs – visi attiecīgie atšķiramu nosaukumu lauki,

  — derīguma termiņš,

  — subjekts – visi attiecīgie atšķiramu nosaukumu lauki,

([1]) ISO 32000-1:2008: *Document management – Portable document format – Part 1: PDF 1.7*.
([2]) ISO 19005-2:2011: *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)*.
([3]) Ieteikums *ITU-T X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks* (sk. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— publiskā atslēga,

— iestādes atslēgas identifikators,

— subjekta atslēgas identifikators,

— atslēgas lietošana,

— atslēgas lietošanas paplašinājums,

— sertifikātu politika – visi politikas identifikatori un politikas kvalifikatori,

— politikas attiecinājumi,

— subjekta alternatīvais nosaukums,

— subjekta direktorija atribūti,

— pamatierobežojumi,

— politikas ierobežojumi,

— *CRL* izplatīšanas vietas ([1]),

— piekļuve iestādes informācijai,

— piekļuve subjekta informācijai,

— kvalificēta sertifikāta definējums ([2]),

— jaucējalgoritms,

— sertifikāta jaucējvērtība.

— Cilvēklasāmajai formai jābūt viegli drukājamai.

— Cilvēklasāmo formu shēmas operators paraksta un apzīmogo saskaņā ar Komisijas Īstenošanas lēmuma (ES) 2015/1505 1. un 3. punktā noteikto *PDF* uzlaboto parakstu.

([1]) *RFC 5280: Internet X.509 PKI Certificate and CRL Profile.*
([2]) *RFC 3739: Internet X.509 PKI: Qualified Certificates Profile.*

II PIELIKUMS

VEIDNE DALĪBVALSTU PAZIŅOJUMIEM

Informācijā, ko dalībvalstis sniedz saskaņā ar šā lēmuma 4. panta 1. punktu, iekļaujami šādi dati un to izmaiņas:

1. Dalībvalsts, izmantojot ISO 3166-1 ([1]) divburtu kodus, ar šādiem izņēmumiem:

   a) Apvienotās Karalistes valsts kods ir "UK";

   b) Grieķijas valsts kods ir "EL".

2. Struktūra/struktūras, kas atbild par uzticamības sarakstu izveidi, uzturēšanu un publicēšanu automatizētai apstrādei piemērotā formā un cilvēklasāmā formā:

   a) shēmas operatora nosaukums: sniegtajai informācijai ir jābūt identiskai – reģistrjutīgi – ar vērtību "Shēmas operatora nosaukums", kas ir uzticamības sarakstā, tik valodās, cik izmantotas uzticamības sarakstā;

   b) fakultatīva informācija Komisijas iekšējai lietošanai tikai tādos gadījumos, ja ir vajadzīgs sazināties ar attiecīgo struktūru (informācija netiks publicēta EK uzticamības sarakstu apkopotajā sarakstā):

      — shēmas operatora adrese,

      — atbildīgo personu kontaktinformācija (vārds, uzvārds, tālruņa numurs, e-pasta adrese).

3. Vieta, kur tiek publicēta uzticamības saraksta automatizētai apstrādei piemērotā forma *(vieta, kur ir publicēts pašreizējais uzticamības saraksts)*.

4. Attiecīgā gadījumā – vieta, kur tiek publicēts cilvēklasāmais uzticamības saraksts *(vieta, kur ir publicēts pašreizējais uzticamības saraksts)*. Ja cilvēklasāmais uzticamības saraksts vairs netiek publicēts, uz šo faktu jānorāda.

5. Publiskās atslēgas sertifikāti, kuri atbilst privātajām atslēgām, ko var izmantot, lai elektroniski parakstītu vai apzīmogotu automatizētai apstrādei piemēroto uzticamības saraksta formu un uzticamības sarakstu cilvēklasāmo formu: šos sertifikātus nodrošina paaugstināta privātuma pasta *Base64* šifrētu *DER* sertifikātu veidā. Paziņošanai par izmaiņu – papildu informācija gadījumā, kad jaunam sertifikātam ir jāaizstāj konkrēts sertifikāts Komisijas sarakstā, un gadījumā, kad paziņotais sertifikāts ir jāpievieno esošajiem bez aizstāšanas.

6. 1.–5. punktā paziņoto datu iesniegšanas datums.

Datus, ko paziņo saskaņā ar 1. punktu, 2. punkta a) apakšpunktu, 3., 4. un 5. punktu, iekļauj EK uzticamības sarakstu apkopotajā sarakstā, nomainot agrāk paziņoto informāciju, kas iekļauta minētajā apkopotajā sarakstā.

([1]) ISO 3166-1: "Valstu un to administratīvi teritoriālā iedalījuma vienību nosaukumu kodi. 1. daļa. Valstu kodi".

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2015/1506

(2015. gada 8. septembris),

kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 27. panta 5. punktu un 37. pantu 5. punktu izklāstītas specifikācijas, kas attiecas uz uzlabotu elektronisko parakstu formātiem un uzlabotiem zīmogiem, kas jāatzīst publiskā sektora struktūrām

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 27. panta 5. punktu un 37. panta 5. punktu,

tā kā:

(1) Dalībvalstīm jāievieš nepieciešamie tehniskie līdzekļi, kas tām ļauj apstrādāt elektroniski parakstītus dokumentus, kuri tiek prasīti tiešsaistes pakalpojumos, ko piedāvā publiskā sektora struktūras vai ko piedāvā to vārdā.

(2) Regula (ES) Nr. 910/2014 dalībvalstīm, kuras pieprasa uzlabotu elektronisko parakstu vai zīmogu izmantošanai tiešsaistes pakalpojumā, ko piedāvā publiskā sektora struktūra vai ko piedāvā tās vārdā, uzliek par pienākumu atzīt uzlabotus elektroniskos parakstus un zīmogus, uzlabotus elektroniskos parakstus un zīmogus, kuru pamatā ir kvalificēts sertifikāts, un kvalificētus elektroniskos parakstus un zīmogus īpašos formātos vai alternatīvus formātus, kas validēti saskaņā ar īpašām atsauces metodēm.

(3) Īpašo formātu un atsauces metožu definēšanā būtu jāņem vērā pastāvošā prakse, standarti un Savienības tiesību akti.

(4) Komisijas Īstenošanas lēmumā 2014/148/ES ([2]) ir noteikti parastākie uzlabota elektroniskā paraksta formāti, ko dalībvalstīm jāspēj tehniski uzturēt gadījumos, kad kādai tiešsaistes administratīvajai procedūrai ir vajadzīgi uzlaboti elektroniskie paraksti. Atsauces formātu izveides mērķis ir veicināt elektronisko parakstu pārrobežu validēšanu un uzlabot elektronisko procedūru pārrobežu sadarbspēju.

(5) Šā lēmuma pielikumā uzskaitītie standarti ir spēkā esošie uzlabota elektroniskā paraksta formātu standarti. Tā kā patlaban standartizācijas iestādes pārskata atsaucēs minēto formātu ilgtermiņa arhivēšanas formas, tad sīkāki ilgtermiņa arhivēšanas standarti šā lēmuma darbības jomā nav iekļauti. Kad būs pieejama atsaucēs minēto standartu jaunā redakcija, atsauces uz standartiem un punkti par ilgtermiņa arhivēšanu tiks pārskatīti.

(6) Uzlaboti elektroniskie paraksti un uzlaboti elektroniskie zīmogi no tehniskā viedokļa ir līdzīgi. Tādēļ uzlabotu elektronisko parakstu formātu standarti būtu pēc analoģijas jāattiecina uz uzlabotu elektronisko zīmogu formātu standartiem.

(7) Ja parakstīšanai vai apzīmogošanai tiek izmantoti elektroniskā paraksta vai zīmoga formāti, kurus parasti tehniski neatbalsta, ir jānodrošina validēšanas līdzekļi, kas ļauj elektronisko parakstu vai zīmogu verificēt pāri robežām. Lai saņēmējas dalībvalstis varētu paļauties uz šiem citas dalībvalsts validācijas rīkiem, ir nepieciešams sniegt viegli pieejamu informāciju par šiem validācijas rīkiem, iekļaujot informāciju elektroniskajos dokumentos, elektroniskajos parakstos vai elektronisko dokumentu konteineros.

([1]) OV L 257, 28.8.2014., 73. lpp.

([2]) Komisijas 2014. gada 17. marta Īstenošanas lēmums 2014/148/ES, ar ko groza Lēmumu 2011/130/ES, ar kuru nosaka minimālās prasības kompetento iestāžu elektroniski parakstītu dokumentu pārrobežu apstrādei saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2006/123/EK par pakalpojumiem iekšējā tirgū (OV L 80, 19.3.2014., 7. lpp.).

(8) Ja dalībvalsts publiskajos pakalpojumos ir pieejamas automatizētai apstrādei piemērotas elektroniskā paraksta vai zīmoga validācijas iespējas, šādas validācijas iespējas būtu jādara pieejamas un izmantojamas saņēmējai dalībvalstij. Tomēr šim lēmumam nevajadzētu kavēt Regulas (ES) Nr. 910/2014 27. panta 1. un 2. punkta un 37. panta 1. un 2. punkta piemērošanu gadījumos, kad alternatīvu metožu validācijas iespēju automatizēta apstrāde nav iespējama.

(9) Lai nodrošinātu salīdzināmas validācijas prasības un vairotu uzticēšanos dalībvalstu sniegtajām iespējām validēt elektroniskā paraksta vai zīmoga formātus, kas parasti netiek atbalstīti, šajā lēmumā izklāstītajās prasībās validācijas rīkiem izmantotas prasības kvalificētu elektronisko parakstu validācijai, kas minētas Regulas (ES) Nr. 910/2014 32. un 40. pantā.

(10) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) Nr. 910/2014 48. pantu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Dalībvalstis, kuras prasa uzlabotu elektronisko parakstu vai uzlabotu elektronisko parakstu, kas balstīts uz kvalificētu sertifikātu, kā noteikts Regulas (ES) Nr. 910/2014 27. panta 1. un 2. punktā, atzīst uzlabotu elektronisko parakstu *XML*, *CMS* vai *PDF* formātā ar atbilstības līmeni B, T vai LT vai saistīto paraksta konteineru, ja minētie paraksti atbilst tehniskajām specifikācijām, kas uzskaitītas pielikumā.

2. pants

1. Dalībvalstis, kuras prasa uzlabotu elektronisko parakstu vai uzlabotu elektronisko parakstu, kas balstīts uz kvalificētu sertifikātu, kā noteikts Regulas (ES) Nr. 910/2014 27. panta 1. un 2. punktā, atzīst elektroniskā paraksta formātus, kas nav minēti šā lēmuma 1. pantā, ar nosacījumu, ka dalībvalsts, kurā ir iedibināts uzticamības pakalpojuma sniedzējs, kuru izmanto parakstītājs, piedāvā citām dalībvalstīm paraksta validācijas iespējas, kas, ja iespējams, ir piemērotas automatizētai apstrādei.

2. Paraksta validācijas iespējas:

a) ļauj citām dalībvalstīm saņemto elektronisko parakstu validēt tiešsaistē, par brīvu un tā, ka tas ir saprotams personām, kam attiecīgā valoda nav dzimtā valoda;

b) ir norādītas parakstītajā dokumentā, elektroniskajā parakstā vai elektroniskā dokumenta konteinerā; un

c) apstiprina uzlabota elektroniskā paraksta derīgumu ar noteikumu, ka:

1) sertifikāts, kas atbalsta uzlaboto elektronisko parakstu, bijis derīgs parakstīšanas brīdī, un, ja uzlaboto elektronisko parakstu atbalsta kvalificēts sertifikāts, kvalificētais sertifikāts, kas atbalsta uzlaboto elektronisko parakstu, parakstīšanas brīdī bijis kvalificēts elektroniskā paraksta sertifikāts, kurš atbilst Regulas (ES) Nr. 910/2014 III pielikumam, un to ir izdevis kvalificēts uzticamības pakalpojumu sniedzējs;

2) paraksta validācijas dati atbilst datiem, kas sniegti atkarīgajai pusei;

3) unikālais datu kopums, kas apzīmē parakstītāju, ir pareizi nosūtīts atkarīgajai pusei;

4) ja parakstīšanas brīdī izmantots pseidonīms, uz šo faktu tiek skaidri norādīts atkarīgajai pusei;

5) ja uzlaboto elektronisko parakstu ir radījusi kvalificēta elektroniskā paraksta radīšanas ierīce, tādas ierīces izmantojums tiek skaidri norādīts atkarīgajai pusei;

6) parakstīto datu integritāte nav tikusi apdraudēta;

7) parakstīšanas brīdī bija izpildītas Regulas (ES) Nr. 910/2014 26. pantā paredzētās prasības;

8) uzlabota elektroniskā paraksta validēšanai izmantotā sistēma nosūta atkarīgajai pusei pareizus validēšanas rezultātus un ļauj atkarīgajai pusei atklāt iespējamas ar drošību saistītas problēmas.

3. pants

Dalībvalstis, kuras prasa uzlabotu elektronisko zīmogu vai uzlabotu elektronisko zīmogu, kas balstīts uz kvalificētu sertifikātu, kā noteikts Regulas (ES) Nr. 910/2014 37. panta 1. un 2. punktā, atzīst uzlabotu elektronisko zīmogu *XML*, *CMS* vai *PDF* formātā ar atbilstības līmeni B, T vai LT vai saistītu zīmoga konteineru, ja tie atbilst tehniskajām specifikācijām, kas uzskaitītas pielikumā.

4. pants

1. Dalībvalstis, kuras prasa uzlabotu elektronisko zīmogu vai uzlabotu elektronisko zīmogu, kas balstīts uz kvalificētu sertifikātu, kā noteikts Regulas (ES) Nr. 910/2014 37. panta 1. un 2. punktā, atzīst elektroniskā zīmoga formātus, kas nav minēti šā lēmuma 3. pantā, ar nosacījumu, ka dalībvalsts, kurā ir iedibināts uzticamības pakalpojuma sniedzējs, kuru izmanto zīmoga radītājs, piedāvā citām dalībvalstīm zīmoga validācijas iespējas, kas, ja iespējams, ir piemērotas automatizētai apstrādei.

2. Zīmoga validācijas iespējas:

a) ļauj citām dalībvalstīm saņemtos elektroniskos zīmogus validēt tiešsaistē, par brīvu un tā, ka tas ir saprotams personām, kam attiecīgā valoda nav dzimtā valoda;

b) ir norādītas apzīmogotajā dokumentā, elektroniskajā zīmogā vai elektroniskā dokumenta konteinerā;

c) apstiprina uzlabota elektroniskā zīmoga derīgumu ar noteikumu, ka:

1) sertifikāts, kas atbalsta uzlaboto elektronisko zīmogu, bijis derīgs apzīmogošanas brīdī, un, ja uzlaboto elektronisko zīmogu atbalsta kvalificēts sertifikāts, kvalificētais sertifikāts, kas atbalsta uzlaboto elektronisko zīmogu, apzīmogšanas brīdī bijis kvalificēts elektroniskā zīmoga sertifikāts, kas atbilst Regulas (ES) Nr. 910/2014 III pielikumam, un to ir izdevis kvalificēts uzticamības pakalpojumu sniedzējs;

2) zīmoga validācijas dati atbilst datiem, kurus sniedz atkarīgajai pusei;

3) unikālo datu kopums, kas apzīmē zīmoga radītāju, tiek pareizi nosūtīts atkarīgajai pusei;

4) ja apzīmogošanas brīdī izmantots pseidonīms, par šo faktu tiek skaidri norādīts atkarīgajai pusei;

5) ja uzlaboto elektronisko zīmogu ir radījusi kvalificēta elektroniskā zīmoga radīšanas ierīce, tādas ierīces izmantojums tiek skaidri norādīts atkarīgajai pusei;

6) apzīmogoto datu integritāte nav tikusi apdraudēta;

7) parakstīšanas brīdī bijušas izpildītas Regulas (ES) Nr. 910/2014 36. pantā noteiktās prasības;

8) zīmoga validēšanai izmantotā sistēma nosūta atkarīgajai pusei pareizus validēšanas rezultātus un ļauj atkarīgajai pusei atklāt iespējamas ar drošību saistītas problēmas.

5. pants

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šis lēmums uzliek saistības kopumā un ir tieši piemērojams visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

Uzlabotu *XML*, *CMS* vai *PDF* formāta elektronisko parakstu un saistītā paraksta konteinera tehnisko specifikāciju saraksts

Lēmuma 1. pantā minētajiem uzlabotajiem elektroniskajiem parakstiem jāatbilst vienām no šādām ETSI tehniskajām specifikācijām, izņemot to 9. punktu:

XAdES bāzes profils	ETSI TS 103171 v.2.1.1. ([1])
CAdES bāzes profils	ETSI TS 103173 v.2.2.1. ([2])
PAdES bāzes profils	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

Lēmuma 1. pantā minētajam saistītajam paraksta konteineram jāatbilst šādām ETSI tehniskajām specifikācijām:

Saistītā paraksta konteinera bāzes profils	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

Uzlabotu *XML*, *CMS* vai *PDF* formāta elektronisko zīmogu un saistīto zīmoga konteineru tehnisko specifikāciju saraksts

Lēmuma 3. pantā minētajiem uzlabotajiem elektroniskajiem zīmogiem jāatbilst vienām no šādām ETSI tehniskajām specifikācijām, izņemot to 9. punktu:

XAdES bāzes profils	ETSI TS 103171 v.2.1.1
CAdES bāzes profils	ETSI TS 103173 v.2.2.1
PAdES bāzes profils	ETSI TS 103172 v.2.2.2

Lēmuma 3. pantā minētajam saistītajam zīmoga konteineram jāatbilst šādām ETSI tehniskajām specifikācijām:

Saistītā zīmoga konteinera bāzes profils	ETSI TS 103174 v.2.2.1

ISSN 1977-0715 (elektroniskais izdevums)
ISSN 1725-5112 (papīra izdevums)

Eiropas Savienības Publikāciju birojs
2985 Luksemburga
LUKSEMBURGA

LV