Euroopa Liidu

Teataja

L 235

Eestikeelne väljaanne

Õigusaktid

58. aastakäik

9. september 2015

Sisukord

[1] EMPs kohaldatav tekst

ET

[1] EMPs kohaldatav tekst

II

(Muud kui seadusandlikud aktid)

MÄÄRUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) 2015/1501,

8. september 2015,

koostalitlusvõime raamistiku kohta vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 8

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, ([1]) eriti selle artikli 12 lõiget 8,

ning arvestades järgmist:

(1) Määruse (EL) nr 910/2014 artikli 12 lõikes 2 on sätestatud, et sama määruse artikli 9 lõike 1 kohaselt teatatud riiklike e-identimise süsteemide koostalitlusvõime jaoks tuleks luua koostalitlusvõime raamistik [termin on muutunud, endine termin oli „koosvõime raamistik"].

(2) Liikmesriikide e-identimise süsteemide omavahelises ühendamises on oluline koht võrgu sõlmedel. Nende funktsioone, kaasa arvatud eIDAS-sõlme funktsioone ja komponente, on selgitatud Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1316/2013 ([2]) loodud Euroopa ühendamise rahastuga seotud dokumentides.

(3) Kui liikmesriik või komisjon pakub teises liikmesriigis tegutsevas sõlmes autentimise võimaldamiseks tarkvara, võib autentimismehhanismi jaoks kasutatavat tarkvara tarniv ja uuendav pool leppida kokku tarkvara majutava poolega, kuidas autentimismehhanismi tööd hallatakse. Selline kokkulepe ei tohiks põhjustada hostivale poolele ebaproportsionaalseid tehnilisi nõudeid ega kulusid (sh tugi, vastutus, majutamis- ja muud kulud).

(4) Kui see on koostalitlusvõime raamistiku teostamise puhul õigustatud, võib komisjon koostöös liikmesriikidega töötada välja täiendavad tehnilised kirjeldused, mis sisaldavad üksikasju käesolevas määruses sätestatud tehniliste nõuete kohta, võttes eeskätt arvesse komisjoni rakendusotsuse (EL) 2015/296 ([3]) artikli 14 punktis d osutatud koostöövõrgu arvamusi. Selliste kirjelduste väljatöötamine peaks olema osa määruse (EL) nr 1316/2013 Euroopa digitaalteenuste taristust, millega nähakse ette vahendid e-identimise komponendi praktiliseks teostamiseks.

([1]) ELT L 257, 28.8.2014, lk 73.

([2]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 1316/2013, 11. detsember 2013, millega luuakse Euroopa ühendamise rahastu, muudetakse määrust (EL) nr 913/2010 ja tunnistatakse kehtetuks määrused (EÜ) nr 680/2007 ja (EÜ) nr 67/2010 (ELT L 348, 20.12.2013, lk 129).

([3]) Komisjoni rakendusotsus (EL) 2015/296, 24. veebruar 2015, millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 7 (ELT L 53, 25.2.2015, lk 14).

(5) Käesolevas määruses sätestatud tehnilised nõuded peaksid olema kohaldatavad olenemata võimalikest muutustest tehnilistes kirjeldustes, mis võidakse välja töötada vastavalt käesoleva määruse artiklile 12.

(6) Käesolevas määruses sätestatud koostalitlusvõime raamistiku korra kehtestamisel on täiel määral võetud arvesse suurprojekti STORK ja selle raames välja töötatud kirjeldusi ning Euroopa avalike teenuste koostalitusvõime raamistiku põhimõtteid ja kontseptsioone.

(7) Täies ulatuses on arvesse võetud liikmesriikidevahelise koostöö tulemusi.

(8) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisese

Käesolevas määruses sätestatakse kootalitlusvõime raamistiku tehnilised ja käitusnõuded, et tagada nende e-identimise süsteemide koostalitlusvõime, millest liikmesriigid komisjonile teatavad.

Eeskätt sisaldavad need nõuded järgmist:

a) määruse (EL) nr 910/2014 artikli 8 alusel teatatud e-identimise süsteemi alusel väljastatud teatatud e-identimise vahendite usaldusväärsuse tasemetega seotud minimaalsed tehnilised nõuded ja riigisiseste usaldusväärsuse tasemete vastavusseviimine vastavalt artiklitele 3 ja 4;

b) koostalitlusvõime minimaalsed tehnilised nõuded vastavalt artiklitele 5 ja 8;

c) füüsilist või juriidilist isikut kordumatult tähistavate identiteediandmete miinimumkogum vastavalt artiklile 11 ja lisale;

d) käitamise ühised turvastandardid vastavalt artiklitele 6, 7, 9 ja 10;

e) vaidluste lahendamise kord vastavalt artiklile 13.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „sõlm” – e-identimise koostalitlusvõimelise arhitektuuri osaks olev ja isikute piiriüleses autentimises osalev ühenduspunkt, mis suudab edastuse ära tunda ja seda töödelda või selle teistele sõlmedele edasi saata, pakkudes ühe liikmesriigi riigisisese e-identimise taristule liidest andmevahetuseks teiste liikmesriikide riigisiseste e-identimise taristutega;

2) „sõlme operaator” – üksus, kes vastutab selle eest, et sõlm täidab ühenduspunkti funktsioone korrektselt ja usaldusväärselt.

Artikkel 3

Usaldusväärsuse tasemetega seotud minimaalsed tehnilised nõuded

Usaldusväärsuse tasemetega seotud minimaalsed tehnilised nõuded on sätestatud komisjoni rakendusmääruses (EL) 2015/1502 ([1]).

Artikkel 4

Riigisiseste usaldusväärsuse tasemete vastavusseviimine

Teatatud e-identimise süsteemide riigisiseste usaldusväärsuse tasemete vastavusseviimisel järgitakse nõudeid, mis on sätestatud rakendusmääruses (EL) 2015/1502. Vastavusseviimise tulemustest teatatakse komisjonile, kasutades komisjoni rakendusotsuses (EL) 2015/1505 ([2]) sätestatud teatamisvormi.

Artikkel 5

Sõlmed

1. Ühes liikmesriigis asuva sõlme saab ühendada teiste liikmesriikide sõlmedega.

2. Sõlmed suudavad tehniliste vahendite abil eristada avaliku sektori asutusi ja muid tuginevaid isikuid.

3. See, kuidas liikmesriik teostab käesolevas määruses sätestatud tehnilised nõuded, ei tohi põhjustada ebaproportsionaalseid nõudeid ja kulusid teistele liikmesriikidele, kui need soovivad saavutada koostalitlusvõime kõnealuse liikmesriigi teostusega.

Artikkel 6

Andmete privaatsus ja konfidentsiaalsus

1. Vahetatavate andmete privaatsuse ja konfidentsiaalsuse kaitse ning andmete tervikluse säilimine sõlmede vahel tagatakse parimate kättesaadavate tehniliste lahenduste ja kaitsetavade kasutamisega.

2. Sõlmedes ei säilitata isikuandmeid, välja arvatud artikli 9 lõikes 3 sätestatud otstarbel.

Artikkel 7

Andmete terviklus ja autentsus side käigus

Sõlmedevahelise side käigus tagatakse andmete terviklus ja autentsus, et saaks olla kindel, et kõik päringud ja vastused on autentsed ning neid ei ole manipuleeritud. Selleks kasutatakse sõlmedes lahendusi, mida on piiriüleses käitamises edukalt kasutatud.

([1]) Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3 (vt käesoleva *Euroopa Liidu Teataja* lk 7).

([2]) Komisjoni rakendusotsus (EL) 2015/1505, 8. september 2015, millega kehtestatakse usaldusnimekirjade tehnilised kirjeldused ja vormingud vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 22 lõikele 5 (vt käesoleva *Euroopa Liidu Teataja* lk 26).

Artikkel 8

Sidesõnumite vorming

Sõlmed kasutavad edastuses levinud sõnumivorminguid, mis põhinevad standarditel, mida on liikmesriikide vahel juba kasutatud rohkem kui korra ning mis on osutunud käitamise seisukohast toimivaks. Süntaks peab võimaldama järgmist:

a) füüsilist või juriidilist isikut kordumatult tähistavate identiteediandmete miinimumkogumi nõuetekohast töötlemist;

b) e-identimise vahendite usaldusväärsuse tasemete nõuetekohast töötlemist;

c) avaliku sektori organite ja muude tuginevate isikute eristamist;

d) identimisega seotud täiendavate atribuutidega arvestamiseks vajalikku paindlikkust.

Artikkel 9

Turvalisusandmete ja metaandmete haldamine

1. Sõlme operaator edastab sõlme haldamise metaandmed standarditud masintöödeldaval kujul, turvaliselt ja usaldusväärselt.

2. Vähemalt turvalisuse seisukohast oluliste parameetrite väljavõtt toimub automaatselt.

3. Sõlme operaator talletab andmed, mille põhjal saab intsidendi korral taastada sõnumivahetuse järjekorra, et teha kindlaks intsidendi koht ja laad. Andmed salvestatakse riigisiseste nõuetega kohaseks ajavahemikuks ning need peavad sisaldama vähemalt järgmisi elemente:

a) sõlme tunnus;

b) sõnumi tunnus;

c) sõnumi kuupäev ja kellaaeg.

Artikkel 10

Teabetagatuse ja turbestandardid

1. Autentimist võimaldavate sõlmede operaatorid tõendavad, et koostalitlusvõime raamistikus osalevate sõlmede puhul on tagatud nende sõlmede vastavus standardi ISO/IEC 27001 nõuetele kas sertifikaadiga või samaväärse hindamismeetodiga või riigisiseste õigusaktide järgimisega.

2. Sõlmeoperaatorid juurutavad turvalisuse seisukohast olulised uuendused ilma põhjendamatute viivitusteta.

Artikkel 11

Isikute identiteediandmed

1. Kui füüsilist või juriidilist isikut kordumatult tähistavate identiteediandmete miinimumkogumit kasutatakse piiriüleselt, peab see vastama lisas esitatud nõuetele.

2. Juriidilist isikut esindava füüsilise isiku puhul peab andmete miinimumkogum sisaldama lisas füüsiliste ja juriidiliste isikute suhtes loetletud atribuutide kombinatsiooni, kui neid andmeid kasutatakse piiriüleselt.

3. Andmed edastatakse algupärases märgistikus ja vajaduse korral translitereeritakse need ladina kirjas.

Artikkel 12

Tehnilised kirjeldused

1. Kui see on koostalitlusvõime raamistiku elluviimise seisukohast õigustatud, võib rakendusotsusega (EL) 2015/296 loodud koostöövõrk võtta vastu tehniliste kirjelduste väljatöötamise vajadust käsitlevaid arvamusi vastavalt rakendusotsuse artikli 14 punktile d. Sellistes tehnilistes kirjeldustes esitatakse täpsemad üksikasjad käesolevas määruses sätestatud tehniliste nõuete kohta.

2. Komisjon töötab tehnilised kirjeldused välja määruse (EL) nr 1316/2013 digitaalteenuste taristu osana koostöös liikmesriikidega vastavalt lõikes 1 osutatud arvamusele.

3. Koostöövõrk võtab vastavalt rakendusotsuse (EL) 2015/296 artikli 14 punktile d vastu arvamuse, milles hinnatakse, kuivõrd vastavad lõike 2 kohaselt välja töötatud tehnilised kirjeldused lõikes 1 osutatud arvamuses esile toodud vajadustele või käesoleva määruse nõuetele. Koostöövõrk võib esitada liikmesriikidele soovituse võtta tehnilisi kirjeldusi arvesse koostalitlusvõime raamistiku elluviimisel.

4. Komisjon esitab tehniliste kirjelduste tõlgenduse näitena etalonrakenduse. Liikmesriigid võivad selle etalonrakenduse kasutusele võtta või kasutada seda tehniliste kirjelduste muude rakenduste testimisel näidisena.

Artikkel 13

Vaidluste lahendamine

1. Koostalitlusvõime raamistikku puudutavad vaidlused lahendatakse võimaluse korral asjaga seotud liikmesriikide läbirääkimiste käigus.

2. Kui lõike 1 kohaselt lahendust ei leita, on rakendusotsuse (EL) 2015/296 artikli 12 alusel loodud koostöövõrk pädev vaidluse lahendama kooskõlas oma töökorraga.

Artikkel 14

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel

president

Jean-Claude JUNCKER

LISA

Artiklis 11 osutatud nõuded füüsilist või juriidilist isikut kordumatult tähistavate identiteedi-andmete miinimumkogumile

1. **Andmete miinimumkogum füüsilise isiku puhul**

Füüsilise isiku puhul sisaldab andmete miinimumkogum kõiki järgmisi kohustuslikke atribuute:

a) praegune perekonnanimi/praegused perekonnanimed;

b) praegune eesnimi/praegused eesnimed;

c) sünniaeg;

d) kordumatu tunnus, mille saatev liikmesriik on loonud, järgides tehnilisi kirjeldusi piiriüleseks identimiseks, ja mis on ajas nii muutumatu kui võimalik.

Füüsilise isiku puhul võib andmete miinimumkogum sisaldada üht või mitut järgmistest atribuutidest:

a) sünnijärgsed eesnimed ja perekonnanimed;

b) sünnikoht;

c) praegune aadress;

d) sugu.

2. **Andmete miinimumkogum juriidilise isiku puhul**

Juriidilise isiku puhul sisaldab andmete miinimumkogum kõiki järgmisi kohustuslikke atribuute:

a) praegune ärinimi;

b) kordumatu tunnus, mille saatev liikmesriik on loonud, järgides tehnilisi kirjeldusi piiriüleseks identimiseks, ja mis on ajas nii muutumatu kui võimalik.

Juriidilise isiku puhul võib andmete miinimumkogum sisaldada üht või mitut järgmistest atribuutidest:

a) praegune aadress;

b) käibemaksukohustuslasena registreerimise number;

c) maksukohustuslasena registreerimise number;

d) Euroopa Parlamendi ja nõukogu direktiivi 2009/101/EÜ ([1]) artikli 3 lõikega 1 seotud tunnus;

e) komisjoni rakendusmääruses (EL) nr 1247/2012 ([2]) osutatud juriidilise isiku identifitseerimistunnus;

f) komisjoni rakendusmääruses (EL) nr 1352/2013 ([3]) osutatud ettevõtja registreerimis- ja identifitseerimisnumber (EORI nr);

g) nõukogu määruse (EL) nr 389/2012 ([4]) artikli 2 lõikes 12 sätestatud aktsiisinumber.

([1]) Euroopa Parlamendi ja nõukogu direktiiv 2009/101/EÜ, 16. september 2009, tagatiste kooskõlastamise kohta, mida liikmesriigid äriühingu liikmete ja kolmandate isikute huvide kaitseks asutamislepingu artikli 48 teises lõigus osutatud äriühingutelt nõuavad, et muuta sellised tagatised võrdväärseteks (ELT L 258, 1.10.2009, lk 11).

([2]) Komisjoni rakendusmäärus (EL) nr 1247/2012, 19. detsember 2012, milles sätestatakse rakenduslikud tehnilised standardid seoses kauplemisteabehoidlatele esitatava kauplemisteabe vormi ja teabe esitamise sagedusega vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 352, 21.12.2012, lk 20).

([3]) Komisjoni rakendusmäärus (EL) nr 1352/2013, 4. detsember 2013, millega kehtestatakse vormid, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) nr 608/2013, mis käsitleb intellektuaalomandi õiguskaitse tagamist tollis (ELT L 341, 18.12.2013, lk 10).

([4]) Nõukogu määrus (EL) nr 389/2012, 2. mai 2012, milles käsitletakse halduskoostööd aktsiisimaksude valdkonnas ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2073/2004 (ELT L 121, 8.5.2012, lk 1).

KOMISJONI RAKENDUSMÄÄRUS (EL) 2015/1502,

8. september 2015,

millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), [1] eriti selle artikli 8 lõiget 3,

ning arvestades järgmist:

(1) Määruse (EL) nr 910/2014 artiklis 8 on sätestatud, et e-identimise süsteemis, millest on teavitatud artikli 9 lõike 1 kohaselt, määratakse süsteemi raames väljastatud e-identimise vahendite madal, märkimisväärne ja/või kõrge usaldusväärsuse tase.

(2) Minimaalsete tehniliste kirjelduste, standardite ja menetluste kindlaksmääramine on hädavajalik, et tagada usaldusväärsuse tasemete üksikasjade ühene mõistmine ja kindlustada koostalitlusvõime teatatud e-identimise süsteemide riigisiseste usaldusväärsuse tasemete vastavusse viimisel artikli 8 kohaste usaldusväärsuse tasemetega, nagu on sätestatud määruse (EL) nr 910/2014 artikli 12 lõike 4 punktis b.

(3) Käesolevas rakendusaktis sätestatud kirjeldustes ja menetlustes on lähtutud rahvusvahelisest standardist ISO/IEC 29115, mis on peamine rahvusvaheline standard e-identimise vahendite usaldusväärsuse tasemete valdkonnas. Määruse (EL) nr 910/2014 sisu erineb siiski nimetatud rahvusvahelisest standardist eeskätt identiteedi tõestamise ja kontrollimise nõuete osas, aga ka selles osas, kuidas võetakse arvesse erinevusi liikmesriikide identiteedi-süsteemide ja ELis samal otstarbel kasutatavate vahendite vahel. Kuigi käesoleva dokumendi lisa toetub nimetatud rahvusvahelisele standardile, ei tuleks seal seetõttu konkreetselt viidata standardi ISO/IEC 29115 sisule.

(4) Käesoleva määruse koostamisel kasutati kõige otstarbekamaks peetud tulemuspõhist lähenemisviisi ning seda on näha ka terminite ja mõistete määratlustest. Neis võetakse arvesse määruse (EL) nr 910/2014 eesmärki e-identimise vahendite usaldusväärsuse tasemete puhul. Seepärast tuleks käesolevas rakendusaktis sätestatud kirjelduste ja menetluste juurutamisel võtta täiel määral arvesse nii suurprojekti STORK ja selle raames välja töötatud kirjeldusi kui ka standardi ISO/IEC 29115 määratlusi ja mõisteid.

(5) Olenevalt sellest, millises kontekstis tuleb identiteedi tõestamise mõnd aspekti kontrollida, võivad autoriteetsed allikad olla erinevad (nt registrid, dokumendid, organid jms). Eri liikmesriikides võivad autoriteetsed allikad olla erinevad isegi siis, kui kontekst on sarnane.

(6) Identiteedi tõestamise ja kontrollimise nõuetes tuleks arvestada erinevate süsteemide ja tavadega ning tagada samas vajaliku usalduse loomiseks piisavalt kõrge usaldusväärsuse tase. Seetõttu peaks varem muul otstarbel kui e-identimise vahendite väljastamiseks kasutatud menetluste heakskiitmise eeltingimuseks olema kinnitus, et nende menetluste puhul on täidetud vastava usaldusväärsuse taseme jaoks ette nähtud nõuded.

[1] ELT L 257, 28.8.2014, lk 73.

(7) Tavaliselt kasutatakse teatavaid autentimistegureid, milleks võib olla ühissaladus, füüsiline seade või füüsiline atribuut. Autentimisprotsessi turvalisuse suurendamiseks tuleks siiski soodustada rohkemate, eelistatavalt eri kategooriatesse kuuluvate autentimistegurite kasutamist.

(8) Käesolev määrus ei tohiks mõjutada juriidiliste isikute esindamise õigust. Lisas tuleks siiski ette näha nõuded füüsiliste ja juriidiliste isikute e-identimise vahendite sidumiseks.

(9) Tuleks tunnustada infoturbe ja teenuste juhtimise süsteemide olulisust ning tunnustatud metoodikate kasutamise ja standardites (nt ISO/IEC 27000 ja standardisari ISO/IEC 20000) esitatud põhimõtete rakendamise olulisust.

(10) Samuti tuleks arvesse võtta liikmesriikide häid tavasid usaldusväärsuse tasemete vallas.

(11) Rahvusvahelistel standarditel põhinev IT-turbe sertifitseerimine on oluline vahend, et kontrollida toote turvalisuse vastavust käesolevas rakendusaktis sätestatud nõuetele.

(12) Määruse (EL) nr 910/2014 artiklis 48 osutatud komitee ei esitanud arvamust oma esimehe kehtestatud tähtaja jooksul,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

1. Teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite madal, märkimisväärne või kõrge usaldusväärsuse tase määratakse kindlaks lisas sätestatud kirjelduste ja menetluste põhjal.

2. Lisas esitatud kirjeldusi ja menetlusi kasutatakse teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite usaldusväärsuse taseme täpsustamiseks, määrates selleks kindlaks järgmiste komponentide usaldatavuse ja kvaliteedi:

a) väljastamine käesoleva määruse lisa punktis 2.1 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktile a;

b) e-identimise vahendite haldamine käesoleva määruse lisa punktis 2.2 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktidele b ja f;

c) autentimine käesoleva määruse lisa punktis 2.3 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktile c;

d) haldamine ja korraldamine käesoleva määruse lisa punktis 2.4 sätestatud tähenduses vastavalt määruse (EL) nr 910/2014 artikli 8 lõike 3 punktidele d ja e.

3. Kui teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendid vastavad usaldusväärsuse kõrgema taseme nõudele, eeldatakse, et nad vastavad samale nõudele ka usaldusväärsuse madalama taseme puhul.

4. Kui lisa asjaomases osas ei ole sätestatud teisiti, peavad konkreetse usaldusväärsuse taseme saavutamiseks olema nõuded täidetud kõigi komponentide puhul, mis on lisas loetletud seoses e-identimise süsteemi alusel väljastatud e-identimise vahendi selle usaldusväärsuse tasemega.

Artikkel 2

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel
president
Jean-Claude JUNCKER

LISA

Teatatud e-identimise süsteemi alusel väljastatud e-identimise vahendite usaldusväärsuse madala, märkimisväärse ja kõrge taseme minimaalsed tehnilised kirjeldused ja menetlused

1. **Kasutatud mõisted**

Käesolevas lisas kasutatakse järgmisi mõisteid:

1) „autoriteetne allikas" – mis tahes allikas, ükskõik millises vormis, mille puhul võib kindel olla, et sealt saadavad andmed, teave ja/või tõendid on täpsed ja neid saab kasutada identiteedi tõendamiseks;

2) „autentimistegur" – tegur, mille puhul on kinnitatud tema seotus konkreetse isikuga ja mis kuulub ühte järgmistest kategooriatest:

   a) „millegi omamisel põhinev autentimistegur" – autentimistegur, mille puhul peab subjekt tõendama, et tal on see olemas;

   b) „teabel põhinev autentimistegur" – autentimistegur, mille puhul peab subjekt tõendama, et ta teab seda;

   c) „olemuslik autentimistegur" – autentimistegur, mis põhineb füüsilise isiku füüsilisel omadusel ja mille puhul peab subjekt tõendama, et tal on see füüsiline omadus;

3) „dünaamiline autentimine" – elektrooniline protsess, mille käigus kasutatakse krüpteerimist või muid meetodeid, mis võimaldavad nõudluspõhiselt luua elektroonilise tõendi, et subjekt valdab või omab identimisandmeid, ning mis muutub iga kord, kui subjekt autenditakse subjekti identiteeti kontrollivas süsteemis;

4) „infoturbe haldamise süsteem" – protsesside ja menetluste kogum, mille eesmärk on viia infoturbega seotud riskid vastuvõetavale tasemele.

2. **Tehnilised kirjeldused ja menetlused**

Käesolevas lisas kirjeldatud tehniliste kirjelduste ja menetluste komponente kasutatakse selleks, et teha kindlaks, kuidas kohaldatakse e-identimise süsteemi alusel väljastatud e-identimise vahendite suhtes määruse (EL) nr 910/2014 artikli 8 nõudeid ja kriteeriume.

2.1. *Väljastamine*

2.1.1. Taotluse esitamine ja registreerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Veendutakse, et taotluse esitaja on teadlik e-identimise vahendi kasutamise tingimustest. 2. Veendutakse, et taotluse esitaja on teadlik e-identimise vahendi kasutamisega seotud soovituslikest ettevaatusabinõudest. 3. Kogutakse identiteedi tõestamiseks ja kontrollimiseks vajalikud identiteediandmed.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.1.2. Identiteedi tõestamine ja kontrollimine (füüsilise isiku puhul)

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Võib eeldada, et isikul on väidetava identiteedi kohta tõendid, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse. 2. Võib eeldada, et tõendid on ehtsad või autoriteetse allika andmetel olemas ning tõendid tunduvad olevat kehtivad. 3. Autoriteetsele allikale tuginedes on teada, et väidetav identiteet on olemas, ning võib eeldada, et see identiteet on ka tegelikult isikul, kes väidab selle endal olevat.
Märkimisväärne	Lisaks madala taseme nõuetele peab olema täidetud üks punktides 1–4 loetletud tingimus: 1. on kontrollitud, et isikul on oma väidetava identiteedi kohta tõendid, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja tal on väidetav identiteet ka tegelikult, ning tõendeid on kontrollitud, et veenduda nende ehtsuses, või on tõendid autoriteetse allika andmetel olemas ja seotud reaalse isikuga ning võetud on meetmed minimeerimaks riski, et isiku väidetav identiteet ei ole tema tegelik identiteet; sealjuures võetakse arvesse näiteks tõendi kadumise, varastamise, selle kehtivuse peatamise, tühistamise või aegumise riski, või 2. liikmesriigis, kus dokument on väljastatud, esitatakse registreerimisprotsessi käigus identiteeti tõendav dokument, mis osutub olevat seotud isikuga, kes selle esitab, ning võetud on meetmed minimeerimaks riski, et isiku väidetav identiteet ei ole tema tegelik identiteet; sealjuures võetakse arvesse näiteks dokumentide kadumise, varastamise, nende kehtivuse peatamise, tühistamise või aegumise riski, või 3. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.2 sätestatud märkimisväärne usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008 ([1]) artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, või 4. kui e-identimise vahend väljastatakse märkimisväärse või kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal ning võttes arvesse isiku identimisandmete muutumise riske, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab märkimisväärset või kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ.

Usaldusväärsuse tase	Vajalikud komponendid
Kõrge	Täidetud peavad olema kas punkti 1 või 2 nõuded. 1. Lisaks märkimisväärse taseme nõuetele peab olema täidetud üks punktides a–c loetletud tingimus: a) kui on kontrollitud, et isikul on fotoga või biomeetriline identimist võimaldav tõend, mida tunnustab liikmesriik, kus esitatakse taotlus e-identimise vahendi saamiseks, ja see tõend vastab väidetavale identiteedile, veendutakse, et tõend on autoriteetse allika andmetel kehtiv, ning taotluse esitaja samasus väidetava identiteediga tuvastatakse, võrreldes isiku üht või mitut füüsilist omadust autoriteetse allikaga, või b) kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.2 sätestatud kõrge usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, ning võetakse meetmeid tõendamaks, et varasema menetluse tulemused kehtivad endiselt, või c) kui e-identimise vahend väljastatakse kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal ning võttes arvesse isiku identimisandmete muutumise riske, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ, ning võetakse meetmeid tõendamaks, et teatatud e-identimise vahendi väljastamise varasema menetluse tulemused kehtivad endiselt, või 2. kui taotluse esitaja ei esita fotoga või biomeetrilist identimist võimaldavat tunnustatud tõendit, kohaldatakse samasugust menetlust nagu kasutatakse sellise tunnustatud fotoga või biomeetrilist identimist võimaldava tõendi saamiseks riigisisesel tasemel registreerimise eest vastutava isiku liikmesriigis.

([1]) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, 9. juuli 2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

2.1.3. Identiteedi tõestamine ja kontrollimine (juriidiliste isikute puhul)

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendi alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse.

Usaldusväärsuse tase	Vajalikud komponendid
	2. Tõend tundub olevat kehtiv ning võib eeldada, et see on ehtne või autoriteetse allika andmetel olemas, kui juriidilise isiku lisamine autoriteetsesse allikasse on vabatahtlik ja seda reguleerib juriidilise isiku ja autoriteetse allika vaheline kokkulepe. 3. Autoriteetse allika andmetel ei ole juriidilise isiku seisund selline, mis takistaks teda kõnealuse juriidilise isikuna tegutsemast.
Märkimisväärne	Lisaks madala taseme nõuetele peab olema täidetud üks punktides 1–3 loetletud tingimus. 1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendite alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja milles on kirjas juriidilise isiku nimi, õiguslik vorm ja (vajaduse korral) registreerimisnumber, ning tõendit kontrollitakse, et veenduda, kas see on ehtne või autoriteetse allika andmetel olemas, kui juriidilise isiku lisamine autoriteetsesse allikasse on nõutav, et juriidiline isik saaks oma valdkonnas tegutseda, ning võetud on meetmed minimeerimaks riski, et väidetav identiteet ei ole juriidilise isiku tegelik identiteet; sealjuures võetakse arvesse näiteks dokumentide kadumise, varastamise, nende kehtivuse peatamise, tühistamise või aegumise riski, või 2. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.3 sätestatud märkimisväärne usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, või 3. kui e-identimise vahend väljastatakse märkimisväärse või kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab märkimisväärset või kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ.
Kõrge	Lisaks märkimisväärse taseme nõuetele peab olema täidetud üks punktides 1–3 loetletud tingimus. 1. Juriidilise isiku väidetavat identiteeti tõendatakse tõendite alusel, mida tunnustab liikmesriik, kus e-identimise vahendi saamise taotlus esitatakse, ja milles on kirjas juriidilise isiku nimi, õiguslik vorm ja vähemalt üks kordumatu tunnus, mida kasutatakse riigi sees juriidilise isiku tähistamiseks, ning tõendeid on kontrollitud veendumaks, et need on autoriteetse allika andmetel kehtivad, või

Usaldusväärsuse tase	Vajalikud komponendid
	2. kui menetlus, mida avalik-õiguslik või eraõiguslik isik on samas liikmesriigis varem kasutanud muul otstarbel kui e-identimise vahendite väljastamiseks, tagab samaväärse usaldusväärsuse taseme kui punktis 2.1.3 sätestatud kõrge usaldusväärsuse tase, ei pea registreerimise eest vastutav isik varasemaid menetlusi kordama, kui usaldusväärsuse samaväärsust kinnitab määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne asutus, ning võetakse meetmeid tõendamaks, et nimetatud eelmise menetluse tulemused kehtivad endiselt, või 3. kui e-identimise vahend väljastatakse kõrge usaldusväärsuse tasemega kehtiva teatatud e-identimise vahendi põhjal, ei ole identiteedi tõestamise ja kontrollimise protsessi vaja korrata. Kui aluseks võetavast e-identimise vahendist ei ole teavitatud, peab kõrget usaldusväärsuse taset kinnitama määruse (EÜ) nr 765/2008 artikli 2 lõikes 13 osutatud vastavushindamisasutus või samaväärne organ, ning võetakse meetmeid tõendamaks, et teatatud e-identimise vahendi väljastamise varasema menetluse tulemused kehtivad endiselt.

2.1.4. Füüsiliste ja juriidiliste isikute e-identimise vahendite seostamine

Vajaduse korral kehtivad füüsilise isiku e-identimise vahendi ja juriidilise isiku e-identimise vahendi omavahelise seostamise (edaspidi „seostamine") suhtes järgmised tingimused.

1) Seostamist peab olema võimalik peatada ja/või kehtetuks tunnistada. Seostamistsüklit (st aktiveerimist, peatamist, uuendamist, kehtetuks tunnistamist) hallatakse riiklikult tunnustatud menetluste kohaselt.

2) Füüsiline isik, kelle e-identimise vahend on seostatud juriidilise isiku e-identimise vahendiga, võib delegeerida seostamisest tulenevad toimingud riiklikult tunnustatud menetluse kohaselt teisele füüsilisele isikule. Vastutavaks jääb siiski füüsiline isik, kes toimingud delegeeris.

3) Seostamine toimub järgmiselt.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteet on tõestatud vähemalt madala usaldusväärsuse taseme nõuete kohaselt. 2. Seostamine on toimunud riiklikult tunnustatud menetluse kohaselt. 3. Autoriteetse allika andmetel ei ole füüsilise isiku seisund selline, mis takistaks teda juriidilise isiku nimel tegutsemast.
Märkimisväärne	Lisaks madala taseme punktile 3 peavad olema täidetud järgmised tingimused. 1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteedi tõestamine on toimunud märkimisväärse või kõrge usaldusväärsuse tasemega.

Usaldusväärsuse tase	Vajalikud komponendid
	2. Seostamine on toimunud riiklikult tunnustatud menetluse kohaselt, mille tulemusena registreeriti seostamine autoriteetses allikas. 3. Seostatust on kontrollitud autoriteetse allika teabe põhjal.
Kõrge	Lisaks madala taseme punktile 3 ja märkimisväärse taseme punktile 2 peavad olema täidetud järgmised tingimused. 1. Kontrollitakse, et juriidilise isiku nimel tegutseva füüsilise isiku identiteedi tõestamine on toimunud kõrge usaldusväärsuse tasemega. 2. Seostatust on kontrollitud kordumatu tunnuse põhjal, mida kasutatakse riigi sees juriidilise isiku tähistamiseks, ja füüsilist isikut tähistava autoriteetsest allikast pärit kordumatu teabe põhjal.

2.2. *E-identimise vahendite haldamine*

2.2.1. E-identimise vahendite tunnused ja disain

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. E-identimise vahend kasutab vähemalt üht autentimistegurit. 2. E-identimise vahend on kavandatud selliselt, et selle väljastaja võtab mõistlikke meetmeid veendumaks, et vahendit kasutatakse ainult selle isiku kontrolli all või selle isiku poolt, kelle oma see on.
Märkimisväärne	1. E-identimise vahend kasutab vähemalt kaht eri kategooriate autentimistegurit. 2. E-identimise vahend on kavandatud selliselt, et võib eeldada, et seda kasutatakse vaid selle isiku kontrolli all või selle isiku poolt, kelle oma see on.
Kõrge	Lisaks märkimisväärsele tasemele peavad olema täidetud järgmised tingimused. 1. E-identimise vahend on kaitstud kopeerimise ja manipuleerimise ning suure ründepotentsiaaliga ründajate vastu. 2. E-identimise vahend on kavandatud selliselt, et selle omanik saab seda kindlalt kaitsta teiste isikute poolse kasutamise eest.

2.2.2. Väljastamine, üleandmine ja aktiveerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Pärast väljastamist antakse e-identimise vahend üle sellise mehhanismi kaudu, mille puhul võib eeldada, et vahend jõuab vaid selle isikuni, kellele see on mõeldud.
Märkimisväärne	Pärast väljastamist antakse e-identimise vahend üle sellise mehhanismi kaudu, mille puhul võib eeldada, et vahend antakse üle vaid selle isiku kätte, kellele see kuulub.
Kõrge	Aktiveerimisprotsessi käigus kontrollitakse, et e-identimise vahend anti üle vaid selle isiku kätte, kellele ta kuulub.

2.2.3. Kehtivuse peatamine, kehtetuks tunnistamine ja taasaktiveerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. E-identimise vahendi kehtivust on võimalik kiiresti ja tõhusalt peatada ja/või see kehtetuks tunnistada. 2. Olemas on meetmed, mille abil takistatakse ilma loata kehtivuse peatamist, kehtetuks tunnistamist ja/või uuesti aktiveerimist. 3. Uuesti aktiveerimine toimub ainult siis, kui endiselt on täidetud samad usaldusväärsuse nõuded kui enne kehtivuse peatamist või kehtetuks tunnistamist.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.2.4. Uuendamine ja asendamine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Võttes arvesse isiku identiteediandmete muutumise riske, peavad uuendamine ja asendamine vastama samadele usaldusväärsuse nõuetele kui esialgne identiteedi tõestamine ja kontrollimine või põhinema sama või kõrgema usaldusväärsuse tasemega kehtival e-identimise vahendil.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Kui uuendamine või asendamine põhineb kehtival e-identimise vahendil, kontrollitakse identiteediandmeid autoriteetsest allikast.

2.3. *Autentimine*

Selles punktis keskendutakse autentimismehhanismi kasutamisega seotud ohtudele ning loetletakse iga usaldusväärsuse taseme nõuded. Käesoleva punkti tähenduses loetakse turvameetmed konkreetse taseme riskidega vastavuses olevaiks.

2.3.1. Autentimismehhanism

Järgmises tabelis on esitatud nõuded igale sellise autentimismehhanismi usaldusväärsuse tasemele, mille kaudu füüsiline või juriidiline isik kasutab e-identimise vahendit selleks, et kinnitada oma isikusamasust tuginevale isikule.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Enne isiku identiteediandmete loovutamist tuleb usaldusväärselt kontrollida e-identimise vahendit ja selle kehtivust. 2. Kui isiku identiteediandmed on salvestatud autentimismehhanismi osana, peab see teave olema turvatud, et kaitsta seda kadumise või rikkumise, sh väljaspool võrku analüüsimise eest. 3. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et baasoskustest suurema ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

Usaldusväärsuse tase	Vajalikud komponendid
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. 1. Enne isiku identiteediandmete loovutamist tuleb e-identimise vahendit ja selle kehtivust usaldusväärselt kontrollida dünaamilise autentimisega. 2. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et keskmise ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.
Kõrge	Lisaks märkimisväärsele tasemele peavad olema täidetud järgmised tingimused. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et suure ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

2.4. *Haldamine ja korraldamine*

Kõik osalised, kes osutavad piiriüleselt e-identimisega seotud teenust (edaspidi „teenuseosutajad"), peavad kasutama dokumenteeritud infoturbe haldamise tavasid, põhimõtteid, lähenemisviise riskihaldusele ja muid tunnustatud turvameetmeid, et asjaomaste liikmesriikide e-identimise süsteemide juhtimisega tegelevad asutused saaksid olla kindlad, et kasutatakse tõhusaid tegutsemisviise. Punktis 2.4 loetakse kõik nõuded/komponendid konkreetse taseme riskidega vastavuses olevaiks.

2.4.1. Üldsätted

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Käesoleva määrusega hõlmatud põhiteenuse osutajaks on liikmesriigi õigusega tunnustatud riigiasutus või juriidiline üksus, millel on kindlakskujunenud struktuur ja mis on täiesti tegev kõigis teenuse osutamise seisukohast asjakohastes aspektides. 2. Teenuseosutajad täidavad kõiki õigusaktidest tulenevaid nõudeid, mis nende suhtes kehtivad seoses teenuse käitamise ja osutamisega, kaasa arvatud teabe liigid, mille kohta võib päringuid esitada, kuidas toimub identiteedi tõestamine ning millist teavet ja kui kaua tuleb säilitada. 3. Teenuseosutajad peavad tõendama oma suutlikkust tulla toime kahjude eest vastutamise riskiga ning piisavate rahaliste vahendite olemasolu tegevuse jätkamiseks ja teenuste osutamiseks. 4. Teenuseosutajad vastutavad kõigi teistelt üksustelt tellitud kohustuste täitmise eest ja süsteemi põhimõtete järgmise eest, nagu oleksid nad ise neid ülesandeid täitnud. 5. E-identimise süsteemide puhul, mis ei ole loodud riigi seadusega, peab olemas olema tõhus tegevuse lõpetamise kava. Sellises kavas tuleb käsitleda teenuse osutamise korrakohast lõpetamist või teenuse osutamise üleminekut teisele teenuseosutajale, asjaomaste asutuste ja lõppkasutajate teavitamist ning seda, kuidas andmikke süsteemi põhimõtete kohaselt kaitstakse, säilitatakse ja hävitatakse.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.2. Avaldatud teatised ja kasutajatele mõeldud teave

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Avaldatud kujul on olemas teenuse määratlus, mis hõlmab kõiki tingimusi ja tasusid, kaasa arvatud teenuse kasutamise võimalikke piiranguid. Teenuse määratlus peab sisaldama privaatsuspõhimõtteid. 2. Kehtestada tuleb asjakohased tegevuspõhimõtted ja kord tagamaks, et teenuse kasutajaid teavitatakse õigeaegselt ja usaldusväärselt kõigist muudatustest teenuse määratluses ja kõigis kohaldatavates tingimustes ning konkreetse teenuse privaatsuspõhimõtetes. 3. Kehtestada tuleb asjakohased tegevuspõhimõtted ja kord, mis võimaldavad teabenõuetele täielikult ja korrektselt vastata.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.3. Infoturbe haldus

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Infoturvariskide haldamiseks ja juhtimiseks on olemas tõhus infoturbe halduse süsteem.
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Infoturbe halduse süsteem järgib infoturvariskide haldamise ja juhtimise juurdunud standardeid ja põhimõtteid.
Kõrge	Sama kui märkimisväärse taseme puhul.

2.4.4. Andmete säilitamine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Asjakohased andmed talletatakse ja neid säilitatakse, kasutades tõhusat teabehaldussüsteemi ning võttes arvesse andmekaitse ja andmete säilitamise suhtes kohaldatavaid õigusakte ja sellega seotud häid tavasid. 2. Andmeid säilitatakse, kuivõrd see on lubatud riigi õigusaktidega või muu riikliku halduskorraldusega, ja kaitstakse seni, kuni nad on vajalikud auditeerimiseks ja turvalisuse rikkumistega seotud uurimiste tarbeks ning säilitamiseks; pärast seda hävitatakse andmed turvaliselt.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.5. Ruumid ja personal

Järgmises tabelis on esitatud nõuded, millele peavad vastama ruumid ja personal ning vajaduse korral allhankijad, kes täidavad käesolevas määruses kirjeldatud ülesandeid. Iga nõude täitmine on proportsionaalne pakutava usaldusväärsuse tasemega seotud riski tasemega.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Olemas on menetlused, millega tagatakse, et personal ja allhankijad on oma ülesannete täitmiseks piisavalt koolitatud, kvalifitseeritud ja kogenud. 2. Teenuse nõuetekohaseks käigushoidmiseks ja ressursside tagamiseks vastavalt selle põhimõtetele ja menetlustele on piisavalt töötajaid ja allhankijaid. 3. Teenuse osutamiseks kasutatavaid ruume jälgitakse pidevalt ja neid kaitstakse keskkonnasündmuste tekitatavate kahjude, ilma loata juurdepääsu ja muude asjaolude eest, mis võiksid mõjutada teenuse turvalisust. 4. Teenuse osutamiseks kasutatavates ruumides on tagatud, et juurdepääs aladele, kus hoitakse või töödeldakse isikuandmeid, krüptograafilisi andmeid või muid delikaatseid andmeid, on lubatud vaid volitatud töötajatele või allhankijatele.
Märkimisväärne	Sama kui madala taseme puhul.
Kõrge	Sama kui madala taseme puhul.

2.4.6. Tehniline kontroll

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Teenuste turvalisusega seotud riskide haldamiseks on olemas proportsionaalsed tehnilise kontrolli meetmed, mis kaitsevad töödeldava teabe konfidentsiaalsust, terviklust ja käideldavust. 2. Isikuandmete või delikaatse teabe vahetamiseks kasutatavad elektroonilise side kanalid on kaitstud pealtkuulamise, manipuleerimise ja taasesituse vastu. 3. Kui e-identimise vahendite väljastamiseks ja autentimiseks kasutatakse krüptograafiat, on juurdepääs tundlikele krüptograafiamaterjalidele vaid neil rollidel ja rakendustel, mille jaoks on juurdepääs vältimatult vajalik. Tagatakse, et selliseid materjale ei salvestata kunagi püsivalt lihttekstina. 4. Kasutatakse menetlusi, mis tagavad, et turvalisus säilib aja jooksul ning et olemas on suutlikkus reageerida riskitaseme muutumisele, intsidentidele ja turvalisuse rikkumistele. 5. Kõiki andmekandjaid, mis sisaldavad isikuandmeid, krüptoandmeid või muud delikaatset teavet, hoitakse ja transporditakse ning need hävitatakse ohutult ja turvaliselt.
Märkimisväärne	Lisaks madalale tasemele peavad olema täidetud järgmised tingimused. Kui e-identimise vahendite väljastamiseks ja autentimiseks kasutatakse krüptograafiat, on delikaatsed krüptomaterjalid manipuleerimise vastu kaitstud.
Kõrge	Sama kui märkimisväärse taseme puhul.

2.4.7. Nõuete järgimine ja auditeerimine

Usaldusväärsuse tase	Vajalikud komponendid
Madal	Toimuvad korrapärased siseauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine.

Usaldusväärsuse tase	Vajalikud komponendid
Märkimisväärne	Toimuvad korrapärased sõltumatud sise- või välisauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine.
Kõrge	1. Toimuvad korrapärased sõltumatud välisauditid, mis hõlmavad kõiki pakutavate teenuste osutamise seisukohast olulisi osi, et tagada asjakohaste põhimõtete järgimine. 2. Kui süsteemi haldab otseselt valitsusasutus, auditeeritakse seda kooskõlas riigi õigusaktidega.

KOMISJONI RAKENDUSMÄÄRUS (EL) 2015/1503,

8. september 2015,

millega kehtestatakse kindlad impordiväärtused, et määrata kindlaks teatava puu- ja köögivilja hind piiril

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta määrust (EL) nr 1308/2013, millega kehtestatakse põllumajandustoodete ühine turukorraldus ning millega tunnistatakse kehtetuks nõukogu määrused (EMÜ) nr 922/72, (EMÜ) nr 234/79, (EÜ) nr 1037/2001 ja (EÜ) nr 1234/2007 ([1]),

võttes arvesse komisjoni 7. juuni 2011. aasta rakendusmäärust (EL) nr 543/2011, millega kehtestatakse nõukogu määruse (EÜ) nr 1234/2007 üksikasjalikud rakenduseeskirjad seoses puu- ja köögiviljasektori ning töödeldud puu- ja köögivilja sektoriga ([2]), eriti selle artikli 136 lõiget 1,

ning arvestades järgmist:

(1) Rakendusmääruses (EL) nr 543/2011 on sätestatud vastavalt mitmepoolsete kaubandusläbirääkimiste Uruguay vooru tulemustele kriteeriumid, mille alusel kehtestab komisjon kolmandatest riikidest importimisel kõnealuse määruse XVI lisa A osas sätestatud toodete ja ajavahemike kohta kindlad impordiväärtused.

(2) Iga turustuspäeva kindel impordiväärtus on arvutatud rakendusmääruse (EL) nr 543/2011 artikli 136 lõike 1 kohaselt, võttes arvesse päevaandmete erinevust. Seetõttu peaks käesolev määrus jõustuma selle *Euroopa Liidu Teatajas* avaldamise kuupäeval,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Käesoleva määruse lisas määratakse kindlaks rakendusmääruse (EL) nr 543/2011 artikliga 136 ette nähtud kindlad impordiväärtused.

Artikkel 2

Käesolev määrus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel

presidendi eest

põllumajanduse ja maaelu arengu peadirektor

Jerzy PLEWA

([1]) ELT L 347, 20.12.2013, lk 671.
([2]) ELT L 157, 15.6.2011, lk 1.

LISA

Kindlad impordiväärtused, et määrata kindlaks teatava puu- ja köögivilja hind piiril

(eurot 100 kg kohta)

CN-kood	Kolmanda riigi kood ([1])	Kindel impordiväärtus
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

(eurot 100 kg kohta)

CN-kood	Kolmanda riigi kood (1)	Kindel impordiväärtus
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Riikide nomenklatuur on sätestatud komisjoni 27. novembri 2012. aasta määruses (EL) nr 1106/2012, millega rakendatakse Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 471/2009 (mis käsitleb ühenduse statistikat väliskaubanduse kohta kolmandate riikidega) seoses riikide ja territooriumide nomenklatuuri ajakohastamisega (ELT L 328, 28.11.2012, lk 7). Kood „ZZ" tähistab „muud päritolu".

OTSUSED

KOMISJONI RAKENDUSOTSUS (EL) 2015/1504,

7. september 2015,

millega tehakse teatavatele liikmesriikidele erand Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1099/2008 (energiastatistika kohta) alusel statistika esitamise kohustusest

(teatavaks tehtud numbri C(2015) 6105 all)

(Ainult eesti-, hollandi-, kreeka-, prantsus- ja slovakikeelne tekst on autentsed)

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 22. oktoobri 2008. aasta määrust (EÜ) nr 1099/2008 energiastatistika kohta, ([1]) eriti selle artikli 5 lõiget 4 ja artikli 10 lõiget 2,

ning arvestades järgmist:

(1) Vastavalt määruse (EÜ) nr 1099/2008 artikli 5 lõikele 4 võib liikmesriigi nõuetekohaselt põhjendatud taotluse korral lubada erandeid riikliku statistika nende osade suhtes, mille kogumine võiks tekitada andmeesitajatele liigset koormust.

(2) Belgia, Eesti, Küpros ja Slovakkia on esitanud taotluse, et neile tehtaks erand kohustusest esitada teatud vaatlusaastate kohta üksikasjalik kodumajapidamiste energiatarbimise statistika lõppkasutuse liikide kaupa.

(3) Kõnealuste liikmesriikide esitatud teabest lähtudes tuleks erandid teha.

(4) Käesoleva otsusega ettenähtud meetmed on kooskõlas Euroopa statistikasüsteemi komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Käesolevaga tehakse määrusest (EÜ) nr 1099/2008 järgmised erandid:

1) Belgiale tehakse erand kohustusest esitada vaatlusaasta 2015 kohta B lisa punkti 1.2.3 alapunktide 4.2.1–4.2.5, punkti 2.2.3 alapunktide 4.2.1–4.2.5, punkti 3.2.3 alapunktide 3.1–3.6, punkti 4.2.3 alapunktide 7.2.1–7.2.5 ja punkti 5.2.4 alapunktide 4.2.1–4.2.5 kohane üksikasjalik kodumajapidamiste energiatarbimise statistika lõppkasutuse liikide kaupa, nagu on määratletud A lisa punktis 2.3 (26. mõiste „Muud sektorid – elamumajandus”).

([1]) ELT L 304, 14.11.2008, lk 1.

2) Eestile tehakse erand kohustusest esitada 2015., 2016. ja 2017. aasta kohta B lisa punkti 1.2.3 alapunktide 4.2.1–4.2.5, punkti 2.2.3 alapunktide 4.2.1–4.2.5, punkti 3.2.3 alapunktide 3.1–3.6, punkti 4.2.3 alapunktide 7.2.1–7.2.5 ja punkti 5.2.4 alapunktide 4.2.1–4.2.5 kohane üksikasjalik kodumajapidamiste energiatarbimise statistika lõppkasutuse liikide kaupa, nagu on määratletud A lisa punktis 2.3 (26. mõiste „Muud sektorid – elamumajandus").

3) Küprosele tehakse erand kohustusest esitada 2015., 2016. ja 2017. aasta kohta B lisa punkti 1.2.3 alapunktide 4.2.1–4.2.5, punkti 2.2.3 alapunktide 4.2.1–4.2.5, punkti 3.2.3 alapunktide 3.1–3.6 ja punkti 5.2.4 alapunktide 4.2.1–4.2.5 kohane üksikasjalik kodumajapidamiste energiatarbimise statistika lõppkasutuse liikide kaupa, nagu on määratletud A lisa punktis 2.3 (26. mõiste „Muud sektorid – elamumajandus").

4) Slovakkiale tehakse erand kohustusest esitada 2015. ja 2016. aasta kohta B lisa punkti 1.2.3 alapunktide 4.2.1–4.2.5, punkti 2.2.3 alapunktide 4.2.1–4.2.5, punkti 3.2.3 alapunktide 3.1–3.6, punkti 4.2.3 alapunktide 7.2.1–7.2.5 ja punkti 5.2.4 alapunktide 4.2.1–4.2.5 kohane üksikasjalik kodumajapidamiste energiatarbimise statistika lõppkasutuse liikide kaupa, nagu on määratletud A lisa punktis 2.3 (26. mõiste „Muud sektorid – elamumajandus").

Artikkel 2

Käesolev otsus on adresseeritud Belgia Kuningriigile, Eesti Vabariigile, Küprose Vabariigile ja Slovaki Vabariigile.

Brüssel, 7. september 2015

Komisjoni nimel

komisjoni liige

Marianne THYSSEN

KOMISJONI RAKENDUSOTSUS (EL) 2015/1505,

8. september 2015,

millega kehtestatakse usaldusnimekirjade tehnilised kirjeldused ja vormingud vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 22 lõikele 5

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), ([1]) eriti selle artikli 22 lõiget 5,

ning arvestades järgmist:

(1) Usaldusnimekirjad on turuosaliste vahelise usalduse loomisel väga olulised, sest need näitavad teenuseosutaja staatust järelevalve ajal.

(2) E-allkirjade piiriülesele kasutamisele aidati kaasa komisjoni otsusega 2009/767/EÜ, ([2]) milles sätestati liikmesriikide kohustus koostada, hallata ja avaldada usaldusnimekirju, mis sisaldavad teavet sertifitseerimisteenuse osutajate kohta, kes väljastavad üldsusele kvalifitseeritud sertifikaate vastavalt Euroopa Parlamendi ja nõukogu direktiivile 1999/93/EÜ ([3]) ning kelle üle teostavad järelevalvet ja kelle akrediteerimisega tegelevad liikmesriigid.

(3) Määruse (EL) nr 910/2014 artiklis 22 on sätestatud, et liikmesriigid on kohustatud koostama, haldama ja avaldama usaldusnimekirju turvalisel viisil, e-allkirja või e-templiga varustatult ja automaatseks töötlemiseks sobivas vormingus ning teatavad komisjonile nende asutuste nimed, kes vastutavad riigisiseste usaldusnimekirjade koostamise eest.

(4) Usaldusteenuse osutaja ja tema osutatavad usaldusteenused tuleks lugeda kvalifitseerituks, kui kvalifitseeritud staatus on seotud usaldusnimekirjas oleva osutajaga. Tagamaks, et teenuseosutajad saavad määrusest (EL) nr 910/2014 tulenevaid muid kohustusi, eeskätt artiklites 27 ja 37 sätestatud kohustusi hõlpsasti täita eemalt ja elektrooniliste vahendite abil, ning et täita selliste teiste sertifitseerimisteenuse osutajate õigustatud ootusi, kes ei väljasta kvalifitseeritud sertifikaate, kuid osutavad e-allkirjadega seotud teenuseid vastavalt direktiivile 1999/93/EÜ ja kes on nimekirja kantud 30. juuniks 2016, peaks liikmesriikidel olema võimalik lisada usaldusnimekirjadesse vabatahtlikkuse alusel muid usaldusteenuseid peale kvalifitseeritud usaldusteenuste, tingimusel et on selgelt märgitud, et need ei ole kvalifitseeritud teenused vastavalt määrusele (EL) nr 910/2014.

(5) Kooskõlas määruse (EL) nr 910/2014 põhjendusega 25 võivad liikmesriigid lisada nimekirja muud liiki riigisiseselt kindlaksmääratud usaldusteenuseid kui need, mis on määratletud määruse (EL) nr 910/2014 artikli 3 lõikes 16, kui on selgelt märgitud, et need ei ole kvalifitseeritud teenused vastavalt määrusele (EL) nr 910/2014.

(6) Käesoleva otsusega ettenähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Liikmesriigid koostavad, avaldavad ja haldavad usaldusnimekirju, mis sisaldavad teavet nende järelevalve all olevate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste kohta. Need nimekirjad vastavad I lisas sätestatud tehnilistele kirjeldustele.

([1]) ELT L 257, 28.8.2014, lk 73.
([2]) Komisjoni otsus 2009/767/EÜ, 16. oktoober 2009, millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul (ELT L 274, 20.10.2009, lk 36).
([3]) Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta (EÜT L 13, 19.1.2000, lk 12).

Artikkel 2

Liikmesriigid võivad lisada usaldusnimekirja teavet kvalifitseerimata usaldusteenuse osutajate ja nende osutatavate kvalifitseerimata usaldusteenuste kohta. Nimekirjas peab olema selgelt märgitud, millised usaldusteenuste osutajad ja nende osutatavad usaldusteenused ei ole kvalifitseeritud.

Artikkel 3

1. Vastavalt määruse (EL) nr 910/2014 artikli 22 lõikele 2 annavad liikmesriigid oma usaldusnimekirjale automaatseks töötlemiseks sobivas vormingus e-allkirja või e-templi vastavalt I lisas sätestatud tehnilistele kirjeldustele.

2. Kui liikmesriik avaldab usaldusnimekirja inimestele loetavas vormingus elektrooniliselt, tagab ta, et selles vormingus usaldusnimekiri sisaldab sama teavet kui automaatseks töötlemiseks sobiv nimekiri, ning annab sellele e-allkirja või e-templi vastavalt I lisas sätestatud tehnilistele kirjeldustele.

Artikkel 4

1. Liikmesriigid teatavad komisjonile määruse (EL) nr 910/2014 artikli 22 lõikes 3 osutatud teabe, kasutades selleks II lisas esitatud vormi.

2. Lõikes 1 osutatud teave sisaldab süsteemi käitaja vähemalt kahe avaliku võtme sertifikaate, mille kehtivusnihe on vähemalt kolm kuud ja mis vastavad privaatvõtmetele, mida saab kasutada e-allkirja või e-templi andmiseks usaldusnimekirjale automaatseks töötlemiseks sobivas vormingus ja inimestele loetavas vormingus, kui see avaldatakse.

3. Vastavalt määruse (EL) nr 910/2014 artikli 22 lõikele 4 teeb komisjon liikmesriikidelt saadud lõigetes 1 ja 2 osutatud teabe turvalise kanali kaudu autenditud veebiserveris avalikkusele kättesaadavaks e-allkirja või e-templiga varustatud vormingus, mis sobib automaatseks töötlemiseks.

4. Komisjon võib teha liikmesriikidelt saadud lõigetes 1 ja 2 osutatud teabe turvalise kanali kaudu autenditud veebiserveris avalikkusele kättesaadavaks e-allkirja või e-templiga varustatult ja inimestele loetavas vormingus.

Artikkel 5

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev otsus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel

president

Jean-Claude JUNCKER

I LISA

USALDUSNIMEKIRJADE ÜHTSE VORMI TEHNILISED NÕUDED

I PEATÜKK

ÜLDNÕUDED

Usaldusnimekirjad peavad sisaldama nimekirjas olevate usaldusteenuste staatuse kohta nii praegust kui ka kogu varasemat teavet alates usaldusteenuse osutaja usaldusnimekirja kandmisest.

Käesolevas kirjelduses hõlmavad terminid „heakskiidetud", „akrediteeritud" ja/või „järelevalvealune" ka riikide heakskiitmissüsteeme, kuid lisateabe selliste võimalike riiklike süsteemide kohta esitavad liikmesriigid oma usaldusnimekirjades, lisades selgitused võimalike erinevuste kohta, võrreldes kvalifitseeritud usaldusteenuste osutajate ja nende osutatavate usaldusteenuste suhtes kohaldatavate järelevalvesüsteemidega.

Usaldusnimekirjas esitatud teabe peamine eesmärk on toetada kvalifitseeritud usaldusteenuste märkide valideerimist. Nende märkide hulka kuuluvad füüsilised või binaarsed (loogilised) objektid, mis on loodud või väljastatud kvalifitseeritud usaldusteenuse kasutamise tulemusena, nt kvalifitseeritud e-allkirjad/e-templid, täiustatud e-allkirjad/e-templid, mida toetab kvalifitseeritud sertifikaat, kvalifitseeritud ajatemplid, kvalifitseeritud elektroonilise edastamise tõendid jms.

II PEATÜKK

USALDUSNIMEKIRJADE ÜHTSE VORMI ÜKSIKASJALIKUD NÕUDED

Käesolevad kirjeldused tuginevad standardis ETSI TS 119 612 v2.1.1 (edaspidi „ETSI TS 119 612") sätestatud kirjeldustele ja nõuetele.

Kui käesolevates nõuetes ei ole sätestatud erinõudeid, siis peab täielikult kohaldama ETSI TS 119 612 punktide 5 ja 6 nõudeid. Kui käesolevates nõuetes on sätestatud erinõuded, peab neid käsitama vastavate ETSI TS 119 612 nõuete suhtes ülimuslikena. Käesolevates nõuetes ja ETSI TS 119 612 nõuetes esinevate lahknevuste korral peab ülimuslikuks pidama käesolevaid nõudeid.

Scheme name (punkt 5.3.6)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.6 nõuetele, kusjuures süsteemi puhul peab kasutama järgmist nime:

„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 (punkt 5.3.7)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.7 nõuetele, kus „asjakohane teave süsteemi kohta" peab sisaldama vähemalt järgmist.

a) Kõigi liikmesriikide jaoks ühine tutvustav teave usaldusnimekirja ulatuse ja tausta, kasutatava järelevalvesüsteemi ja vajaduse korral riiklike heakskiitmissüsteemide (nt akrediteerimisüsteemide) kohta. Ühine tekst, mida tuleb kasutada, on järgmine, kusjuures märgistringi „[*asjaomase liikmesriigi nimi*]" peab asendama asjaomase liikmesriigi nimega:

> „Käesolev nimekiri on usaldusnimekiri, mis sisaldab teavet [*asjaomase liikmesriigi nimi*] järelevalve all olevate usaldusteenuse osutajate kohta ja usaldusteenuste kohta, mida nad osutavad, kooskõlas Euroopa Parlamendi ja nõukogu 23. juuli 2014 aasta määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ) asjaomaste sätetega.

E-allkirjade piiriülesele kasutamisele aidatakse kaasa komisjoni 16. oktoobri 2009. aasta otsusega 2009/767/EÜ, milles on sätestatud liikmesriikide kohustus koostada, hallata ja avaldada usaldusnimekirju, mis sisaldavad teavet sertifitseerimisteenuse osutajate kohta, kes väljastavad üldsusele kvalifitseeritud sertifikaate vastavalt Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiivile 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta ning kelle üle teostavad järelevalvet ja kelle akrediteerimisega tegelevad liikmesriigid. Käesolev usaldusnimekiri on jätkuks otsusega 2009/767/EÜ kehtestatud usaldusnimekirjale."

Usaldusnimekirjad on olulised komponendid, mis aitavad luua usaldust e-turul tegutsejate seas, võimaldades kasutajatel kindlaks teha, milline on usaldusteenuse osutajate ja nende teenuste kvalifitseeritud staatus praegu ja milline on see olnud varem.

Liikmesriikide usaldusnimekirjad peavad sisaldama vähemalt komisjoni rakendusotsuse (EL) 2015/1505 artiklites 1 ja 2 osutatud teavet.

Liikmesriigid võivad lisada usaldusnimekirja teavet kvalifitseerimata usaldusteenuse osutajate ja nende osutatavate kvalifitseerimata usaldusteenuste kohta. Sellisel juhul tuleb selgelt märkida, et need ei ole kvalifitseeritud vastavalt määrusele (EL) nr 910/2014.

Liikmesriigid võivad lisada usaldusnimekirja teavet muud liiki riigisiseselt kindlaksmääratud usaldusteenuste kohta kui need, mis on määratletud määruse (EL) nr 910/2014 artikli 3 lõike 16 alusel. Sellisel juhul tuleb selgelt märkida, et need ei ole kvalifitseeritud vastavalt määrusele (EL) nr 910/2014.

b) Konkreetne teave kasutatava järelevalvesüsteemi kohta ja vajaduse korral riiklike heakskiitmissüsteemide (st akrediteerimisüsteemide) kohta, eeskätt ([1]):

1) teave riigisisese järelevalve süsteemi kohta, mida kohaldatakse kvalifitseeritud ja kvalifitseerimata usaldusteenuste osutajate ning nende osutatavate kvalifitseeritud ja kvalifitseerimata usaldusteenuste suhtes vastavalt määrusele (EL) nr 910/2014;

2) vajaduse korral teave riigisiseste vabatahtlike akrediteerimissüsteemide koha, mida kohaldatakse sertifitseerimisteenuse osutajate suhtes, kes on väljastanud kvalifitseeritud sertifikaate vastavalt direktiivile 1999/93/EÜ.

See konkreetne teave peab sisaldama iga eespool loetletud süsteemi kohta vähemalt järgmist:

1) üldine kirjeldus;

2) teave protsessi kohta, mida järgitakse riigisisese järelevalve süsteemi ja vajaduse korral riigisisese heakskiitmissüsteemi alusel heakskiitmise jaoks;

3) teave kriteeriumide kohta, mille alusel toimub usaldusteenuse osutajate järelevalve või vajaduse korral heakskiitmine;

4) teave kriteeriumide ja õigusnormide kohta, mida kasutatakse järelevalve teostajate/audiitorite valikul ja selle kindlaksmääramisel, kuidas nad usaldusteenuse osutajaid ja nende osutatavaid usaldusteenuseid hindavad;

5) vajaduse korral muud kontaktandmed ja üldteave süsteemi toimimise kohta.

Scheme type/community/rules (punkt 5.3.9)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.9 nõuetele.

Väljal esitatakse URId ainul Briti inglise keeles.

([1]) Need teaberühmad on eriti olulised, et tuginevad isikud saaksid hinnata selliste süsteemide kvaliteedi ja turvalisuse taset. Need teaberühmad tuleb esitada usaldusnimekirja tasandil, kasutades käesolevat välja „Scheme information URI" (punkt 5.3.7 – liikmesriikide esitatav teave), välja „Scheme type/community/rules" (punkt 5.3.9 – kasutades kõigi liikmesriikide jaoks ühist teksti) ja välja „TSL policy/legal notice" (punkt 5.3.11 – kõigi liikmesriikide jaoks ühine tekst koos võimalusega, et iga liikmesriik võib lisada teksti/viiteid oma liikmesriigi kohta). Vajaduse korral ja kui see on nõutav (nt et eristada mitut kvaliteedi/turvalisuse taset), võib teenuse tasandil esitada lisateavet kvalifitseerimata usaldusteenuste ja riigisiseselt kindlaksmääratud (kvalifitseeritud) usaldusteenuste selliste süsteemide kohta, kasutades välja „Scheme service definition URI" (punkt 5.5.6).

Esitatakse vähemalt kaks URI:

1) kõigi liikmesriikide usaldusnimekirjade jaoks ühine URI, mis viitab kirjeldavale tekstile, mida peab kasutama kõigi usaldusnimekirjade puhul järgmiselt:

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

Kirjeldav tekst:

„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) iga liikmesriigi usaldusnimekirja URI, mis viitab kirjeldavale tekstile, mida peab kohaldama selle liikmesriigi usaldusnimekirja suhtes:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kus CC = standardile ISO 3166-1 ([1]) vastav kahetäheline riigikood, mida kasutatakse väljal „Scheme territory" (punkt 5.3.10)

— kus kasutajad pääsevad ligi asjaomase liikmesriigi põhimõtetele/õigusnormidele, mille põhjal nimekirja kantud usaldusteenuseid hinnatakse vastavalt liikmesriigi järelevalvesüsteemile ja vajaduse korral heakskiitmissüsteemile;

— kus kasutajad võivad leida asjaomase liikmesriigi konkreetse kirjelduse selle kohta, kuidas kasutada ja tõlgendada usaldusnimekirja sisu nimekirjas olevate kvalifitseerimata usaldusteenuste ja/või riigisiseselt kindlaksmääratud usaldusteenuste puhul. Seda võib kasutada selleks, et viidata QCsid mitteväljastavate CSPdega seotud riiklike heakskiitmissüsteemide võimalikule detailsusele ja sellele, kuidas kasutada välju „Scheme service definition URI" (punkt 5.5.6) ja „Service information extension" (punkt 5.5.9) sellel eesmärgil.

Liikmesriigid VÕIVAD määratleda ja kasutada täiendavaid URIsid laiendades eespool nimetatud liikmesriigi URI (st URId, mis on määratletud selle hierarhilise URI põhjal).

TSL policy/legal notice (punkt 5.3.11)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.11 nõuetele, kusjuures põhimõtted/õiguslik teade, mis käsitleb süsteemi juriidilist staatust või selles riigis süsteemi suhtes kohaldatavaid õigusnõudeid, kus süsteem on

([1]) ISO 3166-1:2006: „Maade ja nende jaotiste nimetuste tähised. Osa 1: Maatähised".

kehtestatud, ja/või mis tahes piiranguid ja tingimusi, mille alusel usaldusnimekirja hallatakse ja avaldatakse, peab olema mitmekeelsete märgistringide jada (vt punkt 5.1.4), milles esitatakse selliste põhimõtete või teate tekst järgmiselt (kohustuslik on need esitada Briti inglise keeles, võib esitada veel ühes või mitmes muus riigikeeles):

1) esimene osa on kohustuslik ja ühine kõigi liikmesriikide usaldusnimekirjade puhul; selles märgitakse kohaldatav õigusraamistik ning inglise keeles on tekst järgmine:

   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.

   Tekst liikmesriigi riigikeeles:

   Käesoleva usaldusnimekirja suhtes kohaldatav õigusraamistik on Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

2) Teine, vabatahtlik osa oleneb konkreetsest usaldusnimekirjast ja selles esitatakse viited konkreetsetele kohaldatavatele riiklikele õigusraamistikele.

Service current status (punkt 5.5.4)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.5.4 nõuetele.

ELi liikmesriigi usaldusnimekirjas olevate teenuste välja „Service current status" väärtused määruse (EL) nr 910/2014 kohaldamise kuupäeva eelse päeva seisuga (s.o 30. juuni 2016) viiakse üle päeval, mil määrust hakatakse kohaldama (s.o 1. juulil 2016) vastavalt ETSI TS 119 612 J lisa sätetele.

III PEATÜKK

USALDUSNIMEKIRJADE JÄRJEPIDEVUS

Sertifikaadid, millest tuleb komisjonile teatada vastavalt käesoleva otsuse artikli 4 lõikele 2, peavad vastama ETSI TS 119 612 punkti 5.7.1 nõuetele ning need tuleb väljastada selliselt, et:

— nende kehtivuse lõppkuupäevad erinevad vähemalt kolme kuu võrra (väli „Not After");

— nad luuakse uute võtmepaaridega. Varem kasutatud võtmepaare ei tohi uuesti sertifitseerida.

Kui aegub üks avaliku võtme sertifikaat, mida saaks kasutada sellise usaldusnimekirja allkirja või templi valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— juhul kui parajasti avaldatud usaldusnimekirjale on antud allkiri või tempel privaatvõtmega, mille avaliku võtme sertifikaat on aegunud, andma viivitamata uuesti välja uue usaldusnimekirja, millele on antud allkiri või tempel privaatvõtmega, mille teatatud avaliku võtme sertifikaat ei ole aegunud;

— vajaduse korral tekitama uued võtmepaarid, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

Kui rikutud või kasutuselt kõrvaldatud on üks privaatvõti, mis vastab ühele avaliku võtme sertifikaadile, mida saaks kasutada usaldusnimekirja allkirja või templi valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— viivitamata väljastama uue usaldusnimekirja, millele on antud allkiri või tempel rikkumata privaatvõtmega, kui avaldatud usaldusnimekirjale oli allkiri või tempel antud rikutud või kasutuselt kõrvaldatud privaatvõtmega;

— vajaduse korral tekitama uued võtmepaarid, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

Kui rikutud või kasutuselt kõrvaldatud on kõik privaatvõtmed, mis vastavad avaliku võtme sertifikaatidele, mida saaks kasutada usaldusnimekirja allkirja valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— tekitama uued võtmepaarid, mida võiks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— viivitamata väljastama uue usaldusnimekirja, millele on antud allkiri või tempel ühega nendest uutest privaatvõtmetest ja millele vastava avaliku võtme sertifikaat tuleb edastada;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

IV PEATÜKK

USALDUSNIMEKIRJA INIMLOETAVA VORMI NÕUDED

Inimloetava usaldusnimekirja koostamise ja avaldamise korral tuleb see esitada ISO 32000 ([1]) kohase PDF-dokumendina, mis tuleb vormindada PDF/A-profiili (ISO 19005) ([2]) kohaselt.

PDF/A-profiilil põhineva inimloetava usaldusnimekirja sisu peab vastama järgmistele nõuetele:

— inimloetava vormi struktuur peab kajastama tehnilistes nõuetes TS 119 612 kirjeldatud loogilist mudelit;

— igal olemasoleval väljal peab olema näidatud ja esitatud:

  — välja nimi (nt „*Service type identifier*”);

  — välja väärtus (nt „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}”);

  — vajaduse korral välja väärtuse tähendus (kirjeldus) (nt „*Sertifikaadi loomise teenus, mille raames luuakse ja allkirjastatakse kvalifitseeritud sertifikaadid, tuginedes identiteedile ja muudele asjaomase registreerimisteenuse kontrollitud atribuutidele.*”);

  — vajaduse korral mitu keeleversiooni loomulikes keeltes vastavalt usaldusnimekirjas esitatule;

— inimloetavas vormis peavad olema esitatud vähemalt järgmised väljal „Service digital identity” olevad digitaalsete sertifikaatide väljad ja vastavad väärtused ([3]):

  — versioon;

  — sertifikaadi seerianumber;

  — allkirja algoritm;

  — väljastaja – kõik asjaomased eristavad nimeväljad;

  — kehtivusaeg;

  — subjekt – kõik asjaomased eristavad nimeväljad;

([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]) ITU soovitus-T X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks (vt http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— avalik võti;

— väljaandja võtme identifikaator;

— subjekti võtme identifikaator;

— võtmekasutus;

— võtme laiendatud kasutus;

— sertifikaadipoliitika – kõik poliitika identifikaatorid ja täpsustid;

— poliitika kaardistamine;

— subjekti alternatiivne nimi;

— subjekti kataloogi atribuudid;

— põhipiirangud;

— poliitikapiirangud;

— CRLi jaotuspunktid ([1]);

— juurdepääs väljastaja teabele;

— juurdepääs subjekti teabele;

— kvalifitseeritud sertifikaadi määrang ([2]);

— räsialgoritm;

— sertifikaadi räsi väärtus;

— inimloetav vorm peab olema kergesti prinditav;

— süsteemi käitaja peab inimloetava vormi varustama allkirja või tempiga vastavalt komisjoni rakendusotsuse (EL) 2015/1505 artiklites 1 ja 3 sätestatud täiustatud PDF-allkirjale.

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

II LISA

LIIKMESRIIKIDE ESITATAVATE TEADETE VORM

Teave, mille liikmesriigid peavad esitama vastavalt käesoleva otsuse artikli 4 lõikele 1, peab sisaldama järgmisi andmeid ja nende võimalikke muudatusi:

1) Liikmesriik, kasutades standardile ISO 3166-1 ([1]) vastavalt kahetähelist riigikoodi, järgmiste eranditega:

   a) Ühendkuningriigi riigikood on „UK".

   b) Kreeka riigikood on „EL".

2) Asutus/asutused, kes vastutab/vastutavad automaatseks töötlemiseks sobivas vormingus ja inimestele loetavas vormingus usaldusnimekirjade koostamise, haldamise ja avaldamise eest.

   a) Süsteemi käitaja nimi: esitatav teave peab olema identne (tõstutundlik) väärtusega usaldusnimekirja väljal „Scheme operator name" kõigis usaldusnimekirjas kasutatud keeltes.

   b) Vabatahtlikult esitatav teave komisjonisiseseks kasutamiseks ainult juhtudel, kui asjaomase asutusega on vaja ühendust võtta (teavet ei avaldata komisjoni koostatavas usaldusnimekirjade nimekirjas):

      — süsteemi käitaja aadress;

      — vastutava(te) isiku(te) kontaktandmed (nimi, telefon, e-posti aadress).

3) Koht, kus avaldatakse usaldusnimekiri automaatseks töötlemiseks sobivas vormingus *(koht, kus on avaldatud kehtiv usaldusnimekiri)*.

4) Vajaduse korral koht, kus avaldatakse usaldusnimekiri inimestele loetavas vormingus *(koht, kus on avaldatud kehtiv usaldusnimekiri)*. Kui usaldusnimekirja inimestele loetavas vormingus enam ei avaldata, siis märge selle kohta.

5) Avalike võtmete sertifikaadid, mis vastavad privaatvõtmetele, mida saab kasutada e-allkirja või e-templi andmiseks automaatseks töötlemiseks sobivas vormingus usaldusnimekirjale ja inimestele loetavas vormingus usaldusnimekirjadele: need sertifikaadid esitatakse Privacy Enhanced Mail Base64 meetodiga kodeeritud DER-vormingus sertifikaatidena. Muutusest teatamise korral lisateave juhul, kui uus sertifikaat asendab konkreetse sertifikaadi komisjoni nimekirjas ja kui sertifikaat, millest teatatakse, tuleb olemasolevatele lisada ilma, et midagi asendataks.

6) Punktides 1–5 esitatud andmete esitamise kuupäev.

Andmed, mis esitatakse vastavalt punktidele 1, 2a, 3, 4 ja 5, lisatakse Euroopa Komisjoni koostatud usaldusnimekirjade nimekirja, kus need asendavad selles nimekirjas oleva varem esitatud teabe.

([1]) ISO 3166-1: „Maade ja nende jaotiste nimetuste tähised. Osa 1: Maatähised".

KOMISJONI RAKENDUSOTSUS (EL) 2015/1506,

8. september 2015,

millega kehtestatakse täiustatud e-allkirja ja täiustatud e-templi vormingu kirjeldus vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 27 lõikele 5 ja artikli 37 lõikele 5

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), ([1]) eriti selle artikli 27 lõiget 5 ja artikli 37 lõiget 5,

ning arvestades järgmist:

(1) Liikmesriigid peavad võtma kasutusele vajalikud tehnilised vahendid, mis võimaldavad neil töödelda avaliku sektori asutuse enda või tema nimel pakutava veebiteenuse kasutamisel nõutavaid elektrooniliselt allkirjastatud dokumente.

(2) Määrusega (EL) nr 910/2014 kohustatakse liikmesriike, kes nõuavad avaliku sektori asutuse enda või tema nimel pakutava veebiteenuse kasutamisel täiustatud e-allkirja või e-templit, tunnustama täiustatud e-allkirju ja e-templeid, kvalifitseeritud sertifikaadil põhinevaid e-allkirju ja e-templeid ning kvalifitseeritud e-allkirju ja e-templeid, mis on spetsiifilises vormingus või alternatiivsetes vormingutes, mis on valideeritud spetsiaalsete etalonmeetodite kohaselt.

(3) Spetsiifilise vormingu ja etalonmeetodite kindlaksmääramisel tuleks arvesse võtta seniseid tavasid, standardeid ja liidu õigusakte.

(4) Komisjoni rakendusotsuses 2014/148/EL ([2]) on nimetatud mitu kõige levinumat täiustatud e-allkirja vormingut, millele tuleks pakkuda tehnilist tuge liikmesriikides, kus nõutakse haldustoimingute teostamiseks veebis täiustatud e-allkirja. Etalonvormingute kehtestamisega püütakse hõlbustada e-allkirjade piiriülest valideerimist ja parandada e-toimingute piiriülest koostalitlusvõimet.

(5) Käesoleva otsuse lisas loetletud standardid on täiustatud e-allkirja vormingute kehtivad standardid. Standardiorganisatsioonid tegelevad pidevalt viidatud vormingute pikaajalise arhiveerimise vormide läbivaatamisega ja seetõttu ei kuulu pikaajalise arhiveerimise üksikasju käsitlevad standardid käesoleva otsuse kohaldamisalasse. Kui viidatud standardite uus versioon on kättesaadav, vaadatakse viited standarditele ja pikaajalist arhiveerimist käsitlevad tingimused uuesti läbi.

(6) Tehnilises mõttes on täiustatud e-allkirjad ja täiustatud e-templid sarnased. Seetõttu tuleks täiustatud e-allkirja vormingu standardeid kohaldada *mutatis mutandis* ka täiustatud e-templi vormingute suhtes.

(7) Kui allkirja või templi andmiseks kasutatakse teistsugust e-allkirja või e-templi vormingut kui need, millele üldiselt tehnilist tuge pakutakse, tuleks kättesaadavaks teha valideerimisvahendid, mis võimaldaksid e-allkirju ja e-templeid piiriüleselt kontrollida. Et vastuvõtvad liikmesriigid saaksid teiste liikmesriikide valideerimisvahendite peale kindlad olla, tuleb nende valideerimisvahendite kohta pakkuda lihtsalt kättesaadavat teavet, lisades selle näiteks elektroonilistesse dokumentidesse, e-allkirja või elektrooniliste dokumentide konteineritesse.

([1]) ELT L 257, 28.8.2014, lk 73.

([2]) Komisjoni rakendusotsus 2014/148/EL, 17. märts 2014, millega muudetakse otsust 2011/130/EL, millega kehtestatakse pädevate asutuste poolt elektrooniliselt allkirjastatud dokumentide piiriülese töötlemise miinimumnõuded vastavalt Euroopa Parlamendi ja nõukogu direktiivile 2006/123/EÜ teenuste kohta siseturul (ELT L 80, 19.3.2014, lk 7).

(8) Kui liikmesriigi avalikes teenustes saab kasutada automaatseks töötlemiseks sobivaid e-allkirja või e-templi valideerimise võimalusi, tuleks sellised valideerimisvõimalused teha kättesaadavaks ka vastuvõtvale liikmesriigile ja anda tema kasutusse. Käesolev otsus ei tohiks siiski takistada määruse (EL) nr 910/2014 artikli 27 lõigete 1 ja 2 ning artikli 37 lõigete 1 ja 2 kohaldamist, kui alternatiivsete meetodite puhul ei ole valideerimisvõimaluste automaatne töötlemine võimalik.

(9) Selleks, et kehtestada võrreldavad valideerimisnõuded ja suurendada usaldust valideerimisvõimaluste vastu, mida liikmesriigid pakuvad muude e-allkirja või e-templi vormingute puhul kui need, millele üldiselt tuge pakutakse, toetuvad käesolevas otsuses valideerimisvahenditele sätestatud nõuded kvalifitseeritud e-allkirjade ja e-templite valideerimise nõuetele, millele on viidatud määruse (EL) nr 910/2014 artiklites 32 ja 40.

(10) Käesoleva otsusega ettenähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Liikmesriigid, kes nõuavad täiustatud e-allkirja või kvalifitseeritud sertifikaadil põhinevat täiustatud e-allkirja vastavalt määruse (EL) nr 910/2014 artikli 27 lõikele 1 või 2, tunnustavad XMLi, CMSi või PDFi täiustatud e-allkirja vastavustasemel B, T või LT või seotud allkirjakonteineriga e-allkirja, kui need allkirjad vastavad lisas loetletud tehnilistele kirjeldustele.

Artikkel 2

1. Liikmesriigid, kes nõuavad täiustatud e-allkirja või kvalifitseeritud sertifikaadil põhinevat täiustatud e-allkirja vastavalt määruse (EL) nr 910/2014 artikli 27 lõikele 1 või 2, tunnustavad muid e-allkirja formaate peale käesoleva otsuse artiklis 1 nimetatute, tingimusel et liikmesriik, kus tegutseb allkirja andja kasutatud usaldusteenuse osutaja, pakub teistele liikmesriikidele allkirja valideerimise võimalusi, mis sobivad võimaluse korral automaatseks töötlemiseks.

2. Allkirja valideerimise võimalused peavad

a) võimaldama teistel liikmesriikidel saadud e-allkirju veebis valideerida tasuta ja ka teist keelt rääkivatele inimestele arusaadaval viisil;

b) olema märgitud allkirjastatud dokumendis, e-allkirjas või elektroonilise dokumendi konteineris ning

c) kinnitama täiustatud e-allkirja kehtivust, tingimusel et

1) täiustatud e-allkirja toetav sertifikaat oli allkirja andmise ajal kehtiv ja kui täiustatud e-allkirja toetab kvalifitseeritud sertifikaat, oli täiustatud e-allkirja toetav kvalifitseeritud sertifikaat allkirja andmise ajal e-allkirja kvalifitseeritud sertifikaat, mis vastas määruse (EL) nr 910/2014 I lisa nõuetele ja mille oli väljastanud kvalifitseeritud usaldusteenuse osutaja;

2) allkirja valideerimise andmed vastavad tuginevatele isikutele esitatud andmetele;

3) allkirja andjat tähistavate kordumatute andmete kogum esitatakse nõuetekohaselt tuginevatele isikutele;

4) kui allkirja andmise ajal kasutati pseudonüümi, on see tuginevale isikule selgesti märgitud;

5) kui täiustatud e-allkiri antakse kvalifitseeritud e-allkirja andmise vahendiga, tuleb sellise vahendi kasutamisest tuginevatele isikutele selgelt märku anda;

6) allkirjastatud andmete terviklust ei ole rikutud;

7) määruse (EL) nr 910/2014 artiklis 26 sätestatud nõuded olid allkirja andmise ajal täidetud;

8) täiustatud e-allkirja valideerimiseks kasutatav süsteem annab tuginevale isikule valideerimisprotsessi korrektse tulemuse ja võimaldab tugineval isikul tuvastada turvalisusega seotud probleeme.

Artikkel 3

Liikmesriigid, kes nõuavad täiustatud e-templit või kvalifitseeritud sertifikaadil põhinevat täiustatud e-templit vastavalt määruse (EL) nr 910/2014 artikli 37 lõikele 1 või 2, tunnustavad XMLi, CMSi või PDFi täiustatud e-templit vastavustasemel B, T või LT või seotud templikonteineriga e-templit, kui need vastavad lisas loetletud tehnilistele kirjeldustele.

Artikkel 4

1. Liikmesriigid, kes nõuavad täiustatud e-templit või kvalifitseeritud sertifikaadil põhinevat täiustatud e-templit vastavalt määruse (EL) nr 910/2014 artikli 37 lõikele 1 või 2, tunnustavad muid e-templi formaate peale käesoleva otsuse artiklis 3 nimetatute, tingimusel et liikmesriik, kus tegutseb templi andja kasutatud usaldusteenuse osutaja, pakub teistele liikmesriikidele templi valideerimise võimalusi, mis sobivad võimaluse korral automaatseks töötlemiseks.

2. Templi valideerimise võimalused peavad

a) võimaldama teistel liikmesriikidel saadud e-templeid veebis valideerida tasuta ja ka teist keelt rääkivatele inimestele arusaadaval viisil;

b) olema märgitud templiga dokumendis, e-templis või elektroonilise dokumendi konteineris;

c) kinnitama täiustatud e-templi kehtivust, tingimusel et

1) täiustatud e-templit toetav sertifikaat oli templi andmise ajal kehtiv ja kui täiustatud e-templit toetab kvalifitseeritud sertifikaat, oli täiustatud e-templit toetav kvalifitseeritud sertifikaat templi andmise ajal e-templi kvalifitseeritud sertifikaat, mis vastas määruse (EL) nr 910/2014 III lisa nõuetele ja mille oli väljastanud kvalifitseeritud usaldusteenuse osutaja;

2) templi valideerimise andmed vastavad tuginevatele isikutele esitatud andmetele;

3) templi andjat tähistavate kordumatute andmete kogum esitatakse nõuetekohaselt tuginevatele isikutele;

4) kui templi andmise ajal kasutati pseudonüümi, on see tuginevale isikule selgesti märgitud;

5) kui täiustatud e-tempel antakse kvalifitseeritud e-templi andmise vahendiga, tuleb sellise vahendi kasutamisest tuginevatele isikutele selgelt märku anda;

6) templiga andmete terviklust ei ole rikutud;

7) määruse (EL) nr 910/2014 artiklis 36 sätestatud nõuded olid templi andmise ajal täidetud;

8) täiustatud e-templi valideerimiseks kasutatav süsteem annab tuginevale isikule valideerimisprotsessi korrektse tulemuse ja võimaldab tugineval isikul tuvastada turvalisusega seotud probleeme.

Artikkel 5

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev otsus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel
president
Jean-Claude JUNCKER

LISA

XMLi, CMSi või PDFi täiustatud e-allkirjade ja seotud allkirja konteineri tehniliste kirjelduste nimekiri

Otsuse artiklis 1 nimetatud täiustatud e-allkirjad peavad vastama ühele järgmistest ETSI tehnilistest kirjeldustest, välja arvatud selle klausel 9:

XAdESi põhiprofiil	ETSI TS 103171 v.2.1.1 ([1]).
CAdESi põhiprofiil	ETSI TS 103173 v.2.2.1 ([2]).
PAdESi põhiprofiil	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

Otsuse artiklis 1 osutatud seotud allkirja konteiner peab vastama järgmistele ETSI tehnilistele kirjeldustele:

Seotud allkirja konteineri põhiprofiil	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

XMLi, CMSi või PDFi täiustatud e-templite ja seotud templikonteineri tehniliste kirjelduste nimekiri

Otsuse artiklis 3 nimetatud täiustatud e-templid peavad vastama ühele järgmistest ETSI tehnilistest kirjeldustest, välja arvatud selle klausel 9:

XAdESi põhiprofiil	ETSI TS 103171 v.2.1.1
CAdESi põhiprofiil	ETSI TS 103173 v.2.2.1
PAdESi põhiprofiil	ETSI TS 103172 v.2.2.2

Otsuse artiklis 3 osutatud seotud templikonteiner peab vastama järgmistele ETSI tehnilistele kirjeldustele:

Seotud templikonteineri põhiprofiil	ETSI TS 103174 v.2.2.1

ISSN 1977-0650 (elektrooniline väljaanne)
ISSN 1725-5082 (paberväljaanne)

Euroopa Liidu Väljaannete Talitus
2985 Luxembourg
LUKSEMBURG

ET