EUROOPA KOMISJON

Brüssel, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS

e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul

(EMPs kohaldatav tekst)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

Käesolevas seletuskirjas selgitatakse kavandatavat õigusraamistikku, mis on loodud elektrooniliste tehingute usaldusväärsuse suurendamiseks siseturul.

Usalduse loomine internetikeskkonnas on majandusarengu alus. Usalduse puudumise tõttu kahtlevad tarbijad, ettevõtjad ja ametiasutused elektrooniliste tehingute tegemises ja uute teenuste kasutuselevõtus.

Euroopa digitaalarengu tegevuskavas[1] on sõnastatud Euroopa digitaalse arengu praegused takistused ning esitatud ettepanekud e-allkirja käsitleva õigusakti (3. põhimeede) ja e-identimise ja e-autentimise vastastikuse tunnustamise kohta (16. põhimeede), millega luuakse selge õigusraamistik killustatuse ja koostalitlusvõime puudumise kõrvaldamiseks, digitaalse kodakondsuse edendamiseks ja küberkuritegevuse ennetamiseks. Kogu ELi piires e-identimise ja e-autentimise vastastikuse tunnustamise tagavad õigusaktid ja e-allkirja käsitleva direktiivi läbivaatamine on ka *ühtse turu akti*[2] põhimeede digitaalse ühtse turu teostamiseks. *Stabiilsus- ja majanduskasvu tegevuskavas*[3] rõhutatakse, kui oluline on digitaalse majanduse arengus tulevane ühine õigusraamistik piiriülese e-identimise ja e-autentimise vastastikuseks tunnustamiseks ja aktsepteerimiseks.

Kavandatava õigusraamistiku – *„Euroopa Parlamendi ja nõukogu määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul”* – eesmärk on ettevõtjate, kodanike ja avaliku sektori asutuste vahelise turvalise ja tõrgeteta elektroonilise suhtluse võimaldamine, millega suurendatakse avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust ELis.

Kehtiv ELi õigusakt, direktiiv 1999/93/EÜ *elektroonilisi allkirju käsitleva ühenduse raamistiku kohta*[4] käsitleb üksnes e-allkirja. Puudub turvalisi, usaldusväärseid ja kasutajasõbralikke e-tehinguid käsitlev kõikehõlmav piiri- ja sektoriülene ELi raamistik, mis hõlmaks nii e-identimist, e-autentimist kui ka e-allkirja.

Eesmärk on parandada ja täiendada olemasolevaid õigusakte, et need hõlmaksid teavitatud e-identimise süsteemide ja muude oluliste elektrooniliste usaldusteenuste vastastikust tunnustamist ja aktsepteerimist ELis.

2. HUVITATUD ISIKUTEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

Käesolev algatus põhineb praeguse e-allkirja käsitleva õigusraamistiku läbivaatamiseks peetud ulatuslikel konsultatsioonidel, mille käigus kogus komisjon tagasisidet liikmesriikidelt, Euroopa Parlamendilt ja teistelt sidusrühmadelt[5]. Lisaks internetipõhisele avalikule arutelule kasutati VKE Testpaneeli, et teha kindlaks VKEde eriseisukohad ja -vajadused, ning muid

1 KOM(2010) 245, 19.5.2010.
2 KOM(2011) 206 (lõplik), 13.4.2011.
3 KOM(2011) 669, 12.10.2011.
4 EÜT L 13, 19.1.2000, lk 12.
5 Konsultatsioonide kohta vt täpsemalt http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

konkreetset teemat käsitlevaid konsultatsioone sidusrühmadega[6,7]. Komisjon algatas ka mitu uuringut e-identimise, e-autentimise, e-allkirja ja nendega seotud usaldusteenuste kohta (eIAS).

Konsulteerimisel sai selgeks, et enamik sidusrühmi nõustus vajadusega praegune raamistik e-allkirja direktiivi jäetud lünkade täitmiseks läbi vaadata. Oldi arvamusel, et see aitaks paremini lahendada probleeme, mis on tekkinud seoses uute tehnoloogiate (eelkõige interneti- ja mobiiliühenduse) kiire arengu ja kasvava globaliseerumisega, ning samas säiliks õigusraamistiku neutraalsus tehnoloogiaküsimustes.

Komisjon korraldas kooskõlas parema õigusloome poliitikaga eri poliitikavalikute mõju hindamise. Hinnati kolme poliitikasuunda, mis olid seotud 1) uue raamistiku reguleerimisalaga, 2) õigusaktiga ja 3) nõutava järelevalvetasemega[8]. Eelistati poliitikasuunda, mis seisneb õiguskindluse suurendamises, riikliku järelevalve koordineerimise edendamises, e-identimise süsteemide vastastikuse tunnustamise ja aktsepteerimise tagamises ning oluliste asjaomaste usaldusteenuste kaasamises. Mõjuhinnangu kohaselt suurendaks see märkimisväärselt õiguskindlust, piiriüleste e-tehingute turvalisust ja usaldusväärsust ning aitaks vähendada turu killustatust.

3. ETTEPANEKU ÕIGUSLIK KÜLG

3.1 Õiguslik alus

Käesolev ettepanek põhineb Euroopa Liidu toimimise lepingu artiklil 114, milles käsitletakse selliste normide vastuvõtmist, millega kõrvaldada takistused siseturu toimimisele. E-identimise, e-autentimise, e-allkirja ja muude piiriüleste usaldusteenuste vastastikusest tunnustamisest ja aktsepteerimisest saavad elektroonilistele toimingutele või tehingutele juurdepääsul või nende tegemisel kasu kodanikud, ettevõtjad ja ametiasutused.

Määrus on selleks kõige kohasem õiguslik vahend. ELi toimimise lepingu artikli 288 kohane määruse vahetu kohaldatavus vähendab õiguslikku killustatust ja tagab suurema õiguskindluse, kehtestades ühtlustatud põhieeskirjad, mis aitavad kaasa siseturu toimimisele.

---

6 10.3.2011 toimus sidusrühmade seminar, kus osalesid avaliku ja erasektori ning akadeemiliste ringkondade esindajad, et arutada eesseisvate probleemide lahendamiseks vajalikke seadusandlikke meetmeid. Tegemist oli interaktiivse foorumiga, kus vahetati arvamusi ja toodi välja eri seisukohad avaliku konsultatsiooni käigus tõstatatud küsimustes. Mitu organisatsiooni saatis omal algatusel seisukohavõtu.

7 Konkreetsemalt korraldas ELi eesistujariik Poola 9.11.2011 Varssavis e-allkirja teemalise ja 17.11.2011 Poznanis e-identimise teemalise liikmesriikide kohtumise. 25.1.2012 korraldas komisjon liikmesriikide seminari, kus arutati muid e-identimise, e-autentimise ja e-allkirjaga seotud küsimusi.

8 Seoses esimese suunaga analüüsiti nelja võimalust: e-allkirja direktiiv tunnistatakse kehtetuks; poliitikat ei muudeta; suurendatakse õiguskindlust, parandatakse riikliku järelevalve koordineerimist ning tagatakse e-identimise vastastikune tunnustamine ja aktsepteerimine kogu ELis; õigusakti täiendatakse teatavate asjaomaste usaldusteenuste lisamisega. Teise suuna puhul hinnati suhtelisi eeliseid, mis on valdkonna reguleerimisel kas ühe või kahe õigusaktiga ning kas direktiivi või määrusega. Seoses kolmanda suunaga analüüsiti võimalusi, mida pakub ühelt poolt ühistel olulistel järelevalvenõuetel põhinevate riiklike järelevalvesüsteemide rakendamine ja teiselt poolt ELi-põhine järelevalvesüsteem. Igat poliitikavõimalust aitas hinnata rühm, mis koondas komisjoni kõik huvitatud peadirektoraadid, lähtuvalt poliitikaeesmärkide saavutamise tõhususest, majanduslikust mõjust sidusrühmadele (sealhulgas ELi institutsioonide eelarvele), sotsiaalsest ja keskkonnamõjust ning mõjust halduskoormusele.

3.2 Subsidiaarsus ja proportsionaalsus

Selleks et meetmete võtmine ELi tasandil oleks põhjendatud, tuleb järgida subsidiaarsuse põhimõtet.

a) Probleemi piiriülene olemus (vajalikkuse hindamine)

eIAS-i piiriülene olemus eeldab ELi meetmeid. Üksnes riigisisesed (s.t riiklikud) meetmed ei oleks *Euroopa 2020. aasta strateegias*[9] püstitatud eesmärkide saavutamiseks piisavad. Vastupidi, kogemus on näidanud, et riiklikud meetmed on e-allkirjade koostalitlusel kogu ELis tegelikult takistuseks ning et neil on praegu samasugune toime ka e-identimisele, e-autentimisele ja nendega seotud usaldusteenustele. Seepärast on vajalik, et EL looks raamistiku, mis võimaldab lahendada piiriülese koostalitlusvõime probleemi ja parandada riiklike järelevalvesüsteemide koordineerimist. E-identimist aga ei saa kavandatavas määruses käsitleda sama üldiselt nagu muid elektroonilisi usaldusteenuseid, sest identimisvahendite väljastamine kuulub liikmesriikide pädevusse. Seepärast keskendutakse ettepanekus üksnes e-identimise piiriülestele aspektidele.

Kavandatava määrusega luuakse usaldusteenuseid osutavatele ettevõtjatele võrdsed võimalused valdkondades, kus praegused riiklike õigusaktide vahelised erinevused põhjustavad sageli õiguslikku ebakindlust ja lisakoormust. Õiguskindlust suurendatakse märkimisväärselt liikmesriikidele seatava selge kohustusega aktsepteerida kvalifitseeritud usaldusteenuse osutajaid ja sellega luuakse ettevõtjatele lisaajend välismaal tegutsemiseks. Näiteks saavad ettevõtjad elektroonilisel teel osaleda avalikus pakkumismenetluses, mille on välja kuulutanud teise liikmesriigi haldusasutus, ilma et nende e-allkirja blokeeritaks riigisiseste erinõuete ja koostalitlusprobleemide tõttu. Samamoodi saavad ettevõtjad elektrooniliselt allkirjastada teises liikmesriigis asuva osapoolega sõlmitud lepinguid, kartmata erinevate õiguslike nõuete esitamist sellistele usaldusteenustele nagu e-templid, e-dokumendid või ajatemplid. Nii saab üks liikmesriik teisele teatada rikkumishoiatusest, olles kindel, et see on õiguslikult kehtiv mõlemas liikmesriigis. Kui ostjatel on vahendid kontrollimaks, et nad sisenevad tõepoolest enda valitud kaupmehe veebisaidile ja mitte veebisaidile, mis võib olla võltsitud, muutub internetikaubandus lõpuks usaldusväärsemaks.

Vastastikku tunnustatavad e-identimise vahendid ja üldiselt aktsepteeritavad e-allkirjad lihtsustavad paljude teenuste piiriülest osutamist siseturul ja võimaldavad ettevõtjatel piiriüleselt tegutseda, ilma et neil oleks takistusi avaliku sektori asutustega suhtlemisel. Praktikas tähendab see, et ettevõtjate ja kodanike jaoks muutub haldusformaalsuste täitmine märkimisväärselt tõhusamaks. Näiteks üliõpilastel avaneb võimalus registreeruda elektrooniliselt välismaa ülikoolidesse, kodanikud saavad esitada teisele liikmesriigile maksudeklaratsiooni interneti teel ja patsiendid pääsevad internetis ligi oma terviseandmetele. Kui sellised vastastikku tunnustatavad e-identimise vahendid puuduvad, ei pääse arstid ligi patsientide raviks vajalikele meditsiinilistele andmetele ning patsiendile juba tehtud meditsiinilised ja laborianalüüsid tuleb uuesti teha.

b) Lisandväärtus (tõhususe hindamine)

Eespool nimetatud eesmärke ei ole liikmesriikidevahelise vabatahtliku koordineerimise abil seni saavutatud ning on vähe tõenäoline, et see ka tulevikus juhtuks. See põhjustab kattuvat tegevust, erinevate standardite seadmist, info- ja kommunikatsioonitehnoloogia mõjude

[9] Komisjoni teatis „Euroopa 2020. aastal. Aruka, jätkusuutliku ja kaasava majanduskasvu strateegia” (KOM(2010) 2020), 3.3.2010.

piiriülesust ning loob olukorra, kus koordineerimist on kahe- ja mitmepoolsete lepingute kaudu halduslikult keeruline korraldada.

Pealegi nõuab ELi liikmesriikide vahelist koordineerimist, mida saab tõhusamalt teha ELi tasandil, selliste probleemide lahendamine nagu a) õiguskindluse puudumine elektroonilise allkirja direktiivi lahknevatest tõlgendustest tulenevate erinevate riigisiseste õigusnormide tõttu ja b) riiklikul tasandil loodud e-allkirjasüsteemide koostalitlusvõime puudumine tehniliste standardite ebaühtlase kohaldamise tõttu.

3.3 Ettepaneku üksikasjalik selgitus

3.3.1 I PEATÜKK. ÜLDSÄTTED

Artiklis 1 on kindlaks määratud määruse sisu.

Artiklis 2 on kindlaks määratud määruse reguleerimisala.

Artikkel 3 sisaldab määruses kasutatud mõistete seletusi. Osa mõisteid on võetud üle direktiivist 1999/93/EÜ, osa selgitatud või täiendatud lisaelementidega, osa täiesti uued.

Artiklis 4 on kindlaks määratud siseturu põhimõtted seoses määruse territoriaalse kohaldatavusega. Sõnaselgelt on nimetatud kohustust mitte piirata teenuste osutamise vabadust ja toodete vaba liikumist.

3.3.2 II PEATÜKK. E-IDENTIMINE

Artiklis 5 on sätestatud selliste e-identimise vahendite vastastikune tunnustamine ja aktsepteerimine, mis kuuluvad süsteemi, millest teavitatakse komisjoni vastavalt määruses sätestatud tingimustele. Enamik ELi liikmesriike on võtnud kasutusele teatavat liiki e-identimise süsteemi. Süsteemide vahel on aga suuri erinevusi. Asjaolu, et puudub ühine õiguslik alus, millega nõutaks igalt liikmesriigilt teises liikmesriigis väljastatud e-identimise vahendite tunnustamist ja aktsepteerimist internetipõhiste teenuste kasutamisel, ning riigisiseste e-identimise vahendite puudulik piiriülene koostalitlusvõime loovad takistused, mis ei lase kodanikel ja ettevõtjatel digitaalsest ühtsest turust täielikku kasu saada. Kõikide käesoleva määruse kohaselt teavitatud süsteemi kuuluvate e-identimise vahendite vastastikune tunnustamine ja aktsepteerimine kõrvaldab need õiguslikud takistused.

Määrus ei kohusta liikmesriike e-identimise süsteeme kasutusele võtma või nendest teavitama, vaid tunnustama ja aktsepteerima teavitatud e-identimise vahendeid nende internetipõhiste teenuste puhul, kus e-identimist nõutakse teenuse kasutamiseks liikmesriigis. Võimalik mastaabisäästu kasv, mis tuleneb teavitatud e-identimise vahendite ja autentimissüsteemide piiriülesest kasutamisest, võib ergutada liikmesriike oma e-identimise süsteemidest teavitama. Artiklis 6 on sätestatud e-identimise süsteemidest teavitamise viis tingimust.

Liikmesriigid võivad teavitada oma pädevuse raames aktsepteeritavatest e-identimise süsteemidest, kui e-identimist nõutakse avalike teenuste puhul. Lisaks sellele peab asjaomane e-identimise vahend olema väljastatud süsteemist teavitava liikmesriigi nimel või vähemalt vastutusel.

Liikmesriigid peavad tagama üheselt mõistetava seose elektrooniliste identimisandmete ja asjaomase isiku vahel. See kohustus ei tähenda, et isikul ei tohi olla mitut e-identimise vahendit, vaid et need kõik peavad olema seotud sama isikuga.

E-identimise usaldusväärsus sõltub autentimisvahendite kättesaadavusest (s.t võimalusest kontrollida elektrooniliste identimisandmete kehtivust). Määrusega kohustatakse teavitavaid liikmesriike tagama tasuta internetipõhine autentimine kolmandatele isikutele. Autentimisvõimalus peab olema pidevalt kättesaadav. Autentimisest sõltuvatele osalistele ei tohi seada tehnilisi erinõudmisi näiteks riist- või tarkvara osas. Kõnealust sätet ei kohaldata e-identimise vahendite kasutajatele (omanikele) esitatavate tehniliste nõuete, näiteks kaardilugejate suhtes, mis on vajalikud e-identimise vahendite kasutamiseks.

Liikmesriigid peavad võtma vastutuse seose üheselt mõistetavuse (s.t asjaolu, et isikule omistatavad identimisandmed ei ole seotud ühegi teise isikuga) ja autentimisvõimaluse (s.t võimalus kontrollida elektrooniliste identimisandmete kehtivust) eest. Liikmesriikide vastutus ei hõlma identimisprotsessi muid aspekte või identimist eeldavaid tehinguid.

Artikkel 7 hõlmab eeskirju, mis käsitlevad komisjoni teavitamist e-identimise süsteemidest.

Artikli 8 eesmärk on tagada teavitatud identimissüsteemide tehniline koostalitlus koordineerimise, sealhulgas delegeeritud õigusaktide kaudu.

3.3.3 III PEATÜKK. USALDUSTEENUSED

3.3.3.1 1. jagu. Üldsätted

Artiklis 9 on sätestatud nii kvalifitseerimata kui ka kvalifitseeritud usaldusteenuse osutajate vastutusega seotud põhimõtted. See põhineb direktiivi 1999/93/EÜ artiklil 6 ja laiendab õigust saada hüvitist kahju eest, mille on põhjustanud ettevaatamatu usaldusteenuse osutaja sellega, et ei ole täitnud häid turvatavasid, mille tulemuseks on teenusele märkimisväärset mõju avaldav turvarikkumine.

Artiklis 10 on kirjeldatud mehhanismi kolmandates riikides asuvate teenuseosutajate pakutavate kvalifitseeritud usaldusteenuste tunnustamiseks ja aktsepteerimiseks. See põhineb direktiivi 1999/93/EÜ artiklil 7, kuid selles on säilinud vaid ainuke praktikas teostatav võimalus, s.t kõnealuse tunnustamise võimaldamine Euroopa Liidu ja kolmandate riikide või rahvusvaheliste organisatsioonide vaheliste rahvusvaheliste kokkulepete alusel.

Artiklis 11 on sätestatud andmekaitse ja minimaalse andmehulga põhimõtted. See põhineb direktiivi 1999/93/EÜ artiklil 8.

Artikliga 12 muudetakse usaldusteenused kättesaadavaks puuetega inimestele.

3.3.3.2 2. jagu. Järelevalve

Artikliga 13 kohustatakse liikmesriike asutama direktiivi 1999/93/EÜ artikli 3 lõikel 3 põhinevad järelevalveasutused ning täpsustama ja laiendama nende pädevust nii usaldusteenuse osutajate kui ka kvalifitseeritud usaldusteenuse osutajate suhtes.

Artiklis 14 on sõnastatud liikmesriikide järelevalveasutuste vahelise vastastikuse abi üksikasjalik mehhanism, mille eesmärk on lihtsustada usaldusteenuse osutajate piiriülest

järelevalvet. Artikliga kehtestatakse ühistegevuse eeskirjad ja järelevalveasutuste õigus sellises tegevuses osaleda.

Artiklis 15 on sõnastatud kvalifitseeritud ja kvalifitseerimata usaldusteenuse osutajate kohustus rakendada oma tegevuse turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. Lisaks sellele tuleb pädevaid järelevalveasutusi ja teisi asjaomaseid asutusi teavitada kõikidest turvarikkumistest. Need asutused teavitavad vajaduse korral omakorda teiste liikmesriikide järelevalveasutusi ja otse või asjaomase usaldusteenuse osutaja kaudu ka üldsust.

Artiklis 16 on sätestatud tingimused kvalifitseeritud usaldusteenuse osutajate järelevalve ja nende osutatavate kvalifitseeritud usaldusteenuste kohta. Artikliga seatakse kohustus kvalifitseeritud usaldusteenuse osutajate iga-aastaseks kontrollimiseks tunnustatud sõltumatu asutuse poolt, kinnitamaks järelevalveasutusele, et teenuseosutajad täidavad määruses sätestatud kohustusi. Lisaks sellele antakse järelevalveasutustele artikli 16 lõikega 2 õigus kvalifitseeritud usaldusteenuse osutajaid igal ajal kohapeal kontrollida. Samuti on järelevalveasutustel õigus esitada kvalifitseeritud usaldusteenuse osutajatele siduvaid suuniseid, et need heastaksid proportsionaalselt kõik kohustuste täitmatajätmised, mis ilmnesid turvakontrolli käigus.

Artiklis 17 käsitletakse järelevalveasutuse tegutsemist juhul, kui usaldusteenuse osutaja soovib alustada kvalifitseeritud usaldusteenuse osutamist.

Artikliga 18 nähakse ette selliste usaldusnimekirjade[10] koostamine, mis sisaldavad teavet järelevalve alla kuuluvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate teenuste kohta. Kõnealune teave tuleb teha avalikult kättesaadavaks ühtse vormi kaudu, et lihtsustada selle automaatset kasutust ja tagada piisav detailsus.

Artiklis 19 on sätestatud nõuded, mida kvalifitseeritud usaldusteenuste osutajad peavad täitma, et neid sellistena tunnustataks. Artikkel põhineb direktiivi 1999/93/EÜ II lisal.

3.3.3.3 3. jagu. E-allkiri

Artiklis 20 on esitatud füüsiliste isikute e-allkirja õigusliku toimega seotud eeskirjad. Selles selgitatakse ja laiendatakse direktiivi 1999/93/EÜ artiklit 5 ning sõnastatakse selgelt kohustus anda kvalifitseeritud e-allkirjale käsitsi kirjutatud allkirjaga samaväärne õiguslik toime. Lisaks sellele peavad liikmesriigid tagama kvalifitseeritud e-allkirja piiriülese aktsepteerimise avalike teenuste osutamise kontekstis ja nad ei tohi kehtestada mingeid lisanõudeid, mis võiksid kõnealuse allkirja kasutamisel takistuseks osutuda.

Artiklis 21 on sätestatud nõuded allkirja kvalifitseeritud sertifikaatidele. Selles selgitatakse direktiivi 1999/93/EÜ I lisa ja jäetakse kõrvale sätted, mis ei ole praktikas toiminud (nt piirangud tehingute väärtusele).

Artiklis 22 on sätestatud nõuded kvalifitseeritud e-allkirja moodustamise vahenditele. Selles selgitatakse direktiivi 1999/93/EÜ artikli 3 lõikes 5 sätestatud nõudeid turvalistele allkirja moodustamise vahenditele, mida tuleb vastavalt käesolevale määrusele edaspidi käsitada kvalifitseeritud allkirja moodustamise vahenditena. Artikliga selgitatakse ka seda, et allkirja

[10] Komisjoni uue, käesolevas määruses sätestatud usaldusnimekirju käsitleva otsuse aluseks saavad usaldusnimekirjad, mis on sätestatud komisjoni otsuses 2009/767/EÜ, mida on muudetud komisjoni otsusega 2010/425/EL.

moodustamise vahendi võimalused võivad olla palju laiemad kui vaid allkirja moodustamiseks vajalike andmete sisaldamine. Komisjon võib koostada ka nimekirja vahenditele esitatavate turvanõuete standardite viitenumbritest.

Artiklis 23, mis põhineb direktiivi 1999/93/EÜ artikli 3 lõikel 4, on sätestatud kvalifitseeritud e-allkirja moodustamise vahendite sertifitseerimine eesmärgiga teha kindlaks vahendite vastavus II lisas sätestatud turvanõuetele. Kui liikmesriigi määratud sertifitseerimisasutus on vahendid sertifitseerinud, peavad kõik liikmesriigid kõnealuseid vahendeid nõuetele vastavana tunnustama. Komisjon avaldab vastavalt artiklile 24 sertifitseeritud vahendite nimekirja. Samuti võib komisjon koostada artikli 23 lõikes 1 osutatud nimekirja infotehnoloogiatoodete turvalisuse hindamise standardite viitenumbritest.

Artiklis 24 käsitletakse kvalifitseeritud e-allkirja moodustamise vahendite nimekirja avaldamist komisjoni poolt pärast seda, kui liikmesriigid on teatanud vahendite nõuetele vastavusest.

Artikkel 25 põhineb direktiivi 1999/93/EÜ IV lisa soovitustel sätestada siduvad nõuded kvalifitseeritud e-allkirjade valideerimisele, et suurendada nimetatud valideerimise õiguskindlust.

Artiklis 26 on sätestatud tingimused kvalifitseeritud valideerimisteenustele.

Artiklis 27 on sätestatud kvalifitseeritud e-allkirjade pikaajalise säilitamise tingimus. See on võimalik tänu selliste menetluste ja sellise tehnoloogia kasutamisele, mis võimaldavad pikendada kvalifitseeritud e-allkirja valideerimisandmete usaldusväärsust üle nende tehnoloogilise kehtivusaja, mil võltsimine võib muutuda küberkurjategijatele lihtsaks.

3.3.3.4 4. jagu. E-tempel

Artiklis 28 käsitletakse juriidiliste isikute e-templi õiguslikku toimet. Kvalifitseeritud e-templile antakse õiguslik erieeldus tagada sellega seotud e-dokumentide päritolu ja terviklikkus.

Artiklis 29 on sätestatud nõuded e-templi kvalifitseeritud sertifikaatidele.

Artiklis 30 on sätestatud nõuded kvalifitseeritud e-templi moodustamise vahenditele ja nende sertifitseerimisele ning nende nimekirjade avaldamisele.

Artiklis 31 on sätestatud kvalifitseeritud e-templite valideerimise ja säilitamise tingimus.

3.3.3.5 5. jagu. E-ajatempel

Artiklis 32 käsitletakse e-ajatempli õiguslikku toimet. Kvalifitseeritud e-ajatemplile antakse õiguslik erieeldus aja kindlaksmääramiseks.

Artiklis 33 on sätestatud nõuded kvalifitseeritud e-ajatemplile.

3.3.3.6 6. jagu. E-dokumendid

Artikkel 34 on seotud e-dokumentide õigusliku toime ja aktsepteerimise tingimustega. Kehtib õiguslik erieeldus, et kõik e-dokumendid, mis on allkirjastatud kvalifitseeritud e-allkirjaga või millel on kvalifitseeritud e-tempel, on ehtsad ja terviklikud. Seoses e-dokumentide

aktsepteerimisega tunnustatakse juhul, kui avaliku teenuse osutamiseks nõutakse originaaldokumenti või kinnitatud koopiat, teistes liikmesriikides ilma täiendavate nõueteta vähemalt selliseid e-dokumente, mille on väljastanud asjaomaste dokumentide väljastamiseks pädevad isikud ja mida käsitatakse päritoluliikmesriigi õigusaktide kohaselt originaalidokumentide või kinnitatud koopiatena.

3.3.3.7 7. jagu. E-andmevahetusteenused

Artiklis 35 käsitletakse e-andmevahetusteenuse abil saadetavate või saadavate andmete õiguslikku toimet. Kvalifitseeritud e-andmevahetusteenuste puhul on tagatud õiguslik erieeldus, et saadetavad või saadavad andmed on terviklikud ja andmete saatmise aeg on täpne. Samuti tagatakse artikliga kvalifitseeritud e-andmevahetusteenuste vastastikune tunnustamine kogu ELis.

Artiklis 36 on sätestatud nõuded kvalifitseeritud e-andmevahetusteenustele.

3.3.3.8 8. jagu. Veebisaidi autentimine

Kõnealuse jao eesmärk on tagada, et garanteeritakse veebisaidi kuuluvus selle omanikule.

Artiklis 37 on sätestatud nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele, mida võib kasutada veebisaidi ehtsuse tagamiseks. Veebisaidi autentimise kvalifitseeritud sertifikaadist leiab veebisaidi ja selle omaniku juriidilise staatusega seotud usaldusväärse miinimumteabe.

3.3.4 IV PEATÜKK. DELEGEERITUD ÕIGUSAKTID

Artikkel 38 sisaldab kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 delegeeritud volituste kasutamise standardsätteid (delegeeritud õigusaktid). See võimaldab seadusandjal delegeerida komisjonile õiguse võtta vastu muid kui seadusandlikke akte, mis on üldkohaldatavad ja mis täiendavad või muudavad seadusandliku akti teatavaid mitteolemuslikke osi.

3.3.5 V PEATÜKK. RAKENDUSAKTID

Artikkel 39 sisaldab sätet komiteemenetluse kasutamise kohta rakendusvolituste delegeerimisel komisjonile juhtudel, kui kooskõlas Euroopa Liidu toimimise lepingu artikliga 291 on liidu õiguslikult siduvate aktide rakendamiseks vaja ühetaolisi tingimusi. Kohaldatakse kontrollimenetlust.

3.3.6 VI PEATÜKK. LÕPPSÄTTED

Artikliga 40 seatakse komisjonile kohustus määrust hinnata ja esitada tähelepanekute kohta aruandeid.

Artiklis 41 tunnistatakse direktiiv 1999/93/EÜ kehtetuks ning sätestatakse praeguse e-allkirja taristu sujuv vastavusseviimine määruse uute nõuetega.

Artiklis 42 on sätestatud määruse jõustumise kuupäev.

4. MÕJU EELARVELE

Ettepaneku konkreetne mõju eelarvele on seotud Euroopa Komisjonile pandud ülesannetega ja seda on täpsustatud käesolevale ettepanekule lisatud finantsselgituses.

Ettepanek ei mõjuta tegevuskulusid.

Käesolevale määruse ettepanekule lisatud finantsselgituses käsitletakse määruse enda mõju eelarvele.

2012/0146 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS

e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse komisjoni ettepanekut,

pärast õigusakti eelnõu esitamist riikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[11],

olles konsulteerinud Euroopa andmekaitseinspektoriga[12],

tegutsedes tavapärase seadusandliku menetluse kohaselt

ning arvestades järgmist:

(1) Usalduse loomine internetikeskkonnas on majandusarengu alus. Usalduse puudumise tõttu kahtlevad tarbijad, ettevõtjad ja ametiasutused elektrooniliste tehingute tegemises ja uute teenuste kasutuselevõtus.

(2) Käesoleva määruse eesmärk on suurendada elektrooniliste tehingute usaldusväärsust siseturul, võimaldades turvalist ja terviklikku elektroonilist suhtlust ettevõtjate, kodanike ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust ELis.

(3) Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiivis 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta[13] on käsitletud üksnes e-allkirju, kuid seal ei ole esitatud kõikehõlmavat piiri- ja sektoriülest raamistikku turvaliste, usaldusväärsete ja kasutajasõbralike e-tehingute kohta. Käesoleva määrusega täiendatakse ja avardatakse direktiivi *acquis*'d.

(4) Komisjoni Euroopa digitaalarengu tegevuskavas[14] on digitaalse majanduse mõjuringi peamiste takistustena nimetatud digitaalse turu killustatust, koostalitlusvõime

[11] ELT C, , lk.
[12] ELT C, , lk.
[13] EÜT L 13, 19.1.2000, lk 12.
[14] KOM(2010) 245 (lõplik/2).

puudumist ja küberkuritegevuse kasvu. 2010. aasta aruandes ELi kodakondsuse kohta rõhutas komisjon veelgi vajadust lahendada peamised probleemid, mis takistavad Euroopa kodanikel digitaalsest ühtsest turust ja piiriülestest digitaalteenustest kasu saamast[15].

(5) Euroopa Ülemkogu soovitas komisjonil luua 2015. aastaks digitaalne ühtne turg[16] kiirete edusammude tegemiseks digitaalmajanduse võtmetähtsusega valdkondades ja täielikult integreeritud digitaalse ühtse turu edendamiseks[17], lihtsustades internetipõhiste teenuste piiriülest kasutamist ja pöörates erilist tähelepanu turvalise e-identimise ja e-autentimise hõlbustamisele.

(6) Nõukogu palus komisjonil edendada digitaalset ühtset turgu sobivate tingimuste loomisega piiriüleste põhieelduste, näiteks e-identimise, e-dokumentide, e-allkirjade ja e-andmevahetusteenuste vastastikuseks tunnustamiseks ning koostalitlust võimaldavateks e-valitsuse teenusteks kogu Euroopa Liidus[18].

(7) Euroopa Parlament rõhutas elektrooniliste teenuste, eelkõige e-allkirja turvalisuse tähtsust ja vajadust luua avaliku võtme infrastruktuur (PKI) üleeuroopalisel tasandil ning palus komisjonil asutada Euroopa valideerimisasutuste portaal eesmärgiga tagada elektroonilise allkirja kasutamise võimalus piiriülestes tehingutes ja suurendada internetis tehtavate tehingute turvalisust[19].

(8) Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiivis 2006/123/EÜ teenuste kohta siseturul[20] nõutakse liikmesriikidelt ühtsete kontaktpunktide loomist, tagamaks, et kõiki teenuste osutamise valdkonnale juurdepääsuga ja selles valdkonnas tegutsemisega seotud toiminguid ja formaalsusi oleks lihtne teostada vahemaa tagant, elektrooniliste vahendite abil, sobiva ühtse kontaktpunkti kaudu ja asjaomaste ametiasutustega. Paljud ühtsete kontaktpunktide kaudu kättesaadavad internetipõhised teenused eeldavad e-identimist, e-autentimist ja e-allkirja.

(9) Enamasti ei saa teise liikmesriigi teenuseosutajad kasutada nimetatud teenustele juurdepääsuks oma e-identimist, sest asjaomase riigi elektroonilisi autentimissüsteeme ei tunnustata ega aktsepteerita teistes liikmesriikides. Selline elektrooniline takistus ei lase teenuseosutajatel siseturust täielikku kasu saada. Vastastikku tunnustatavad ja aktsepteeritavad e-identimise vahendid lihtsustavad paljude teenuste piiriülest osutamist siseturul ja võimaldavad ettevõtjatel piiriüleselt tegutseda, ilma et neil oleks palju takistusi avaliku sektori asutustega suhtlemisel.

(10) Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiivis 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius[21] on ette nähtud e-tervise eest vastutavate riiklike asutuste võrgustik. Võrgustik peab piiriüleste

---

15 2010. aasta aruanne ELi kodakondsuse kohta: ELi kodanike õigusi piiravate takistuste kõrvaldamine. KOM(2010) 603 (lõplik), punkt 2.2.2, lk 13.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Nõukogu järeldused Euroopa e-valitsuse tegevuskava kohta aastateks 2011–2015, transpordi, telekommunikatsiooni ja energeetika nõukogu 3093. kohtumine, Brüssel, 27. mai 2011.

19 Euroopa Parlamendi resolutsioon, 21. september 2010, e-kaubanduse siseturu väljakujundamise kohta, 21.9.10, P7_TA(2010)0320, ja Euroopa Parlamendi resolutsioon, 15. juuni 2010, interneti haldamise järgmiste sammude kohta, P7_TA(2010)0208.

20 ELT L 376, 27.12.2006, lk 36.

21 ELT L 88, 4.4.2011, lk 45.

tervishoiuteenuste turvalisuse ja järjepidevuse suurendamiseks koostama suunised piiriüleseks juurdepääsuks elektroonilistele tervishoiuandmetele ja -teenustele, toetades liikmesriike sealjuures *„ühiste identifitseerimis- ja autentimismeetmete väljatöötamisel, et hõlbustada piiriüleste tervishoiuteenuste osutamisel andmete edastamist”*. E-identimise ja e-autentimise vastastikune tunnustamine ja aktsepteerimine on põhitegur, et muuta piiriülesed tervishoiuteenused Euroopa kodanike jaoks tegelikkuseks. Kui inimesed reisivad ravi eesmärgil, peavad nende meditsiinilised andmed olema ravi osutavas riigis kättesaadavad. See eeldab ühtset, turvalist ja usaldusväärset e-identimise raamistikku.

(11) Üks käesoleva määruse eesmärke on kõrvaldada praegused takistused liikmesriikides vähemalt avalikele teenustele juurdepääsuks kasutatavate e-identimise vahendite piiriülesel kasutamisel. Määruse eesmärk ei ole sekkuda liikmesriikides loodud e-identiteedi haldamissüsteemide ja nendega seotud taristute küsimuses. Määruse eesmärk on tagada, et juurdepääsul liikmesriikide pakutavatele piiriülestele internetipõhistele teenustele oleks võimalik turvaline e-identimine ja e-autentimine.

(12) Liikmesriikidel peaks olema vabadus kasutada või juurutada e-identimise vahendeid juurdepääsuks internetipõhistele teenustele. Samuti peaks neil olema võimalus otsustada, kas erasektor saab neid vahendeid pakkuda. Liikmesriikidel ei peaks olema e-identimise süsteemidest teavitamise kohustust. Neil on võimalus valida, kas teavitada kõikidest riigisiseselt vähemalt avalikele internetipõhistele teenustele juurdepääsuks kasutatavatest e-identimise süsteemidest, teha seda mõne süsteemi puhul või üldse mitte.

(13) Määruses tuleb sätestada mõned tingimused e-identimise vahendite aktsepteerimise ja süsteemidest teavitamise kohta. Need tingimused peaksid aitama liikmesriikidel luua vajalikku usaldust üksteise e-identimise süsteemide vastu ning vastastikku tunnustada ja aktsepteerida e-identimise vahendeid, mis kuuluvad nende teavitatud süsteemidesse. Vastastikuse tunnustamise ja aktsepteerimise põhimõtet peaks rakendama juhul, kui teavitav liikmesriik täidab teavitamise tingimusi ja teavitamine on avaldatud Euroopa Liidu Teatajas. Juurdepääs kõnealustele internetipõhistele teenustele ja nende lõplik osutamine taotlejale peaksid siiski olema tihedalt seotud õigusega selliseid teenuseid riigisisestes õigusaktides sätestatud tingimustel tarbida.

(14) Liikmesriikidel peaks olema võimalus otsustada, kas kaasata erasektor e-identimise vahendite väljastamisse ja kas lubada erasektoril vajaduse korral kasutada teavitatud süsteemi kuuluvaid e-identimise vahendeid identimiseks internetipõhiste teenuste või e-tehingute puhul. Võimalus kasutada kõnealuseid e-identimise vahendeid võimaldaks luua erasektoris usalduse paljudes liikmesriikides juba vähemalt avalike teenuste puhul laialdaselt kasutatava e-identimise ja e-autentimise vastu ning muuta piiriülene juurdepääs erasektori internetipõhistele teenustele ettevõtjate ja kodanike jaoks lihtsamaks. Selleks et e-identimise vahendite piiriülest kasutamist erasektori jaoks lihtsamaks muuta, peaks liikmesriikide pakutav autentimisvõimalus olema asjaomastele osalistele kättesaadav selliselt, et ei diskrimineeritaks ei avalikku ega erasektorit.

(15) Teavitatud süsteemi kuuluvate e-identimise vahendite piiriülene kasutamine eeldab liikmesriikide koostööd tehnilise koostalitluse tagamisel. See välistab igasugused riigisisesed tehnilised eeskirjad, millega nõutaks riigivälistelt osalistelt näiteks spetsiaalse riist- või tarkvara soetamist, et teavitatud e-identimist kontrollida ja

valideerida. Teisalt on vältimatud kasutajatele esitatavad tehnilised tingimused, mis tulenevad mis tahes kasutatavale lubakaardile (nt kiipkaardid) omastest tehnilistest tingimustest.

(16) Liikmesriikide koostöö peaks olema suunatud teavitatud e-identimise süsteemide tehnilisele koostalitlusele, et soodustada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele. Liikmesriikidevaheline teabevahetus ja parimate tavade jagamine nende vastastikuse tunnustamise eesmärgil peaks nimetatud koostööle kaasa aitama.

(17) Käesolevas määrusega tuleb luua üldine õigusraamistik elektrooniliste usaldusteenuste kasutamiseks. Sellega ei peaks siiski looma üldist kohustust teenuseid kasutada. Konkreetsemalt ei tohiks määrus hõlmata vabatahtlikel eraõiguslikel kokkulepetel põhinevate teenuste osutamist. Samuti ei peaks määrus hõlmama selliseid lepingute või muude juriidiliste kohustuste sõlmimise ja kehtivusega seotud aspekte, kus on tegemist riiklikes või ELi õigusaktides sätestatud vormiliste nõuetega.

(18) Selleks et soodustada elektrooniliste usaldusteenuste üldist piiriülest kasutamist, peaks neid kõikides liikmesriikides olema võimalik kasutada tõendina kohtumenetlustes.

(19) Liikmesriikidel peaks olema vabadus lisaks käesolevas määruses sätestatud usaldusteenuste suletud nimekirja kuuluvatele usaldusteenustele kindlaks määrata muud liiki usaldusteenuseid, et neid tunnustataks riiklikul tasandil kvalifitseeritud usaldusteenustena.

(20) Arvestades tehnoloogiliste muutuste kiirust, tuleks käesolevas määruses kasutada uuendustele avatud lähenemisviisi.

(21) Määrus peaks olema tehnoloogiaküsimustes neutraalne. Määruse õiguslik mõju peaks olema saavutatav mis tahes tehniliste vahenditega eeldusel, et täidetakse käesoleva määruse tingimusi.

(22) Selleks et suurendada inimeste usaldust siseturu vastu ning edendada usaldusteenuste ja -toodete kasutamist, tuleks nõuetele ja kohustustele viitamiseks võtta kasutusele kvalifitseeritud usaldusteenuste ja kvalifitseeritud usaldusteenuse osutaja mõiste, et tagada mis tahes kasutatavate või osutatavate kvalifitseeritud usaldusteenuste ja -toodete turvalisuse kõrge tase.

(23) Vastavalt ka ELis jõustunud ÜRO puuetega inimeste õiguste konventsioonist tulenevatele kohustustele peaksid puuetega inimesed saama kasutada usaldusteenuseid ja nende teenuste osutamisel kasutatavaid lõpptarbijale suunatud tooteid teiste tarbijatega võrdsetel alustel.

(24) Usaldusteenuse osutaja haldab isikuandmeid ja peab seetõttu täitma tingimusi, mis on sätestatud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivis 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[22]. Eelkõige peaks võimaluste piires miinimumini viima andmete kogumise, võttes arvesse osutatava teenuse eesmärki.

(25) Järelevalveasutused peaksid tegema koostööd ja vahetama teavet andmekaitseasutustega, et tagada andmekaitsealaste õigusaktide nõuetekohane

[22] EÜT L 281, 23.11.1995, lk 31.

rakendamine teenuseosutajate poolt. Teabevahetus peaks hõlmama eelkõige turvaintsidente ja isikuandmetega seotud rikkumisi.

(26) Kõik usaldusteenuse osutajad on kohustatud kohaldama oma tegevusega seotud ohte arvestavaid häid turvatavasid, et suurendada kasutajate usaldust ühtse turu vastu.

(27) Sätted, mis käsitlevad varjunimede kasutamist sertifikaatidel, ei tohiks takistada liikmesriike nõudmast isikute tuvastamist liidu või riikliku õiguse kohaselt.

(28) Kõik liikmesriigid peaksid täitma olulisi ühiseid järelevalvenõudeid, et tagada kvalifitseeritud usaldusteenuste võrreldav turvatase. Selleks et hõlbustada nimetatud nõuete järjekindlat kohaldamist kogu ELis, peaksid liikmesriigid võtma kasutusele võrreldavad meetmed ning vahetama teavet oma järelevalvetegevuse ja parimate tavade kohta kõnealuses valdkonnas.

(29) Turvarikkumistest teatamine ja turvaohtude hindamine on väga oluline asjaomastele pooltele adekvaatse teabe andmisel turvarikkumise või tervikluse kao korral.

(30) Selleks et võimaldada komisjonil ja liikmesriikidel hinnata käesolevas määruses sätestatud rikkumistest teatamise mehhanismi tõhusust, tuleks järelevalveasutustelt nõuda kokkuvõtliku teabe esitamist komisjonile ning Euroopa Võrgu- ja Infoturbeametile (ENISA).

(31) Selleks et võimaldada komisjonil ja liikmesriikidel hinnata käesoleva määruse mõju, tuleks järelevalveasutustelt nõuda statistika esitamist kvalifitseeritud usaldusteenuste ja nende kasutamise kohta.

(32) Selleks et võimaldada komisjonil ja liikmesriikidel hinnata käesoleva määrusega kehtestatud täiustatud järelevalvemehhanismi tõhusust, tuleks järelevalveasutustelt nõuda aruandeid nende tegevuse kohta. See aitaks oluliselt lihtsustada heade tavade vahetamist järelevalveasutuste vahel ja tagaks, et kõikides liikmesriikides kontrollitakse oluliste järelevalvenõuete järjekindlat ja tõhusat rakendamist.

(33) Selleks et tagada kvalifitseeritud usaldusteenuste jätkusuutlikkus ja püsivus ning suurendada kasutajate usaldust kvalifitseeritud usaldusteenuste järjepidevuse vastu, peaksid järelevalveasutused tagama, et kvalifitseeritud usaldusteenuse osutajate andmeid säilitatakse ja hoitakse piisava aja jooksul kättesaadavana isegi juhul, kui kvalifitseeritud usaldusteenuse osutaja lõpetab tegevuse.

(34) Kvalifitseeritud usaldusteenuse osutajate üle järelevalve teostamise lihtsustamiseks näiteks juhul, kui teenuseosutaja pakub oma teenuseid teise liikmesriigi territooriumil ja ei ole seal järelevalve all, või juhul, kui teenuseosutaja arvutid asuvad mõne muu liikmesriigi territooriumil kui teenuseosutaja asukohaliikmesriik, tuleks luua liikmesriikide järelevalveasutuste vahelise vastastikuse abistamise süsteem.

(35) Usaldusteenuse pakkujad vastutavad käesolevas määruses sätestatud usaldusteenuste ja eelkõige kvalifitseeritud usaldusteenuste osutamisega seotud nõuete täitmise eest. Järelevalveasutused vastutavad selle jälgimise eest, kuidas usaldusteenuse osutajad nimetatud nõudeid täidavad.

(36) Selleks et võimaldada tõhusat algatusprotsessi, mis viiks kvalifitseeritud usaldusteenuse osutajate ja nende pakutavate kvalifitseeritud usaldusteenuste

usaldusnimekirja kandmiseni, tuleks ergutada eelsuhtlust tulevaste kvalifitseeritud usaldusteenuse osutajate ja pädevate järelevalveasutuste vahel, et lihtsustada hoolsuskohustuse täitmist, mis viib kvalifitseeritud usaldusteenuste osutamiseni.

(37) Usaldusnimekirjad on turu korraldajate vahelise usalduse loomisel väga olulised, sest need näitavad teenuseosutaja kvalifitseeritud staatust järelevalve ajal; samas ei ole nimekirjad kvalifitseeritud staatuse saamise ja käesoleva määruse nõuete kohaste kvalifitseeritud usaldusteenuste osutamise eeltingimus.

(38) Kui kvalifitseeritud usaldusteenusest on juba teavitatud, ei saa asjaomane avaliku sektori asutus sellest haldustoimingu või formaalsuse täitmisel keelduda põhjendusega, et teenus ei kuulu liikmesriikide koostatud usaldusnimekirja. Sel eesmärgil viitab avaliku sektori asutus ametiasutusele või muule üksusele, mis osutab selliseid e-valitsuse teenuseid nagu internetipõhine maksude deklareerimine, sünnitunnistuste taotlemine, elektroonilistes riigihankemenetlustes osalemine jne.

(39) Kuigi e-allkirjade vastastikuse tunnustamise tagamiseks on vaja kõrget turvataset, tuleks teatavatel juhtudel, näiteks kontekstis, mis on seotud komisjoni 16. oktoobri 2009. aasta otsusega 2009/767/EÜ, millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul[23], tunnustada ka madalama turvatasemega e-allkirju.

(40) Allakirjutaja peaks saama usaldada kvalifitseeritud e-allkirja moodustamise vahendeid kolmanda isiku hooleks eeldusel, et rakendatakse asjakohaseid mehhanisme ja menetlusi tagamaks, et üksnes allakirjutajal on kontroll oma e-allkirja moodustamiseks vajalike andmete üle, ning eeldusel, et vahendi kasutamisel täidetakse kvalifitseeritud allkirjaga seotud nõudeid.

(41) Allkirja kehtivusega seotud õiguskindluse tagamiseks on väga oluline täpsustada, milliseid kvalifitseeritud e-allkirja osi peab asjaomane valideeriv osaline hindama. Lisaks sellele peaks selliste nõuete täpsustamine, mida esitatakse kvalifitseeritud usaldusteenuse osutajatele, kes võivad osutada kvalifitseeritud valideerimisteenust asjaomastele osalistele, kes ei soovi või ei saa ise kvalifitseeritud e-allkirju valideerida, innustama era- või avalikku sektorit sellistesse teenustesse investeerima. Need asjaolud peaksid muutma kvalifitseeritud e-allkirjade valideerimise lihtsaks ja mugavaks kõigile osalistele kogu ELis.

(42) Kui tehingu tegemine eeldab juriidilise isiku kvalifitseeritud e-templit, peaks samavõrra aktsepteeritav olema ka juriidilise isiku volitatud esindaja kvalifitseeritud e-allkiri.

(43) E-tempel peaks olema tõend selle kohta, et e-dokumendi on väljastanud juriidiline isik ning et dokumendi päritolu ja terviklikkus on kindlalt tagatud.

(44) Käesoleva määrusega tuleks tagada teabe pikaajaline säilitamine, s.t e-allkirjade ja e-templite juriidiline kehtivus pika aja jooksul, ning garanteerida võimalus neid valideerida sõltumata tehnoloogia arengust tulevikus.

---

[23] ELT L 274, 20.10.2009, lk 36.

(45) E-dokumentide piiriülese kasutuse soodustamiseks tuleks käesoleva määrusega ette näha e-dokumentide õiguslik toime, mida tuleks pidada samaväärseks paberdokumentidega, sõltuvalt riskihindamisest ja tingimusel, et tagatakse dokumentide ehtsus ja terviklikkus. Samuti on piiriüleste e-tehingute edasiarendamiseks siseturul oluline, et ühe liikmesriigi asjaomase pädeva asutuse poolt vastavalt riiklikele õigusaktidele väljastatud e-dokumentide originaale või kinnitatud koopiaid aktsepteeritaks sellistena ka teistes liikmesriikides. Käesolev määrus ei tohiks mõjutada liikmesriikide õigust otsustada, mida mõeldakse originaali või koopia all riigisiseselt, vaid see peaks tagama võimaluse kasutada neid sellistena ka piiriüleselt.

(46) Kuna praegu kasutavad liikmesriikide pädevad ametiasutused oma dokumentide elektrooniliseks allkirjastamiseks täiustatud e-allkirja erinevaid vorminguid, on vaja tagada, et liikmesriikidel on võimalik elektrooniliselt allkirjastatud dokumentide saamise korral tehniliselt toetada vähemalt teatavat hulka täiustatud e-allkirja vorminguid. Samamoodi tuleks tagada, et kui liikmesriikide pädevad asutused kasutavad täiustatud e-templit, toetaksid nad vähemalt teatavat hulka täiustatud e-templi vorminguid.

(47) E-templit võib lisaks juriidilise isiku väljastatud dokumendi autentimisele kasutada ka kõikide juriidilise isiku digitaalvarade, näiteks tarkvarakoodide ja serverite autentimiseks.

(48) Võimalus autentida veebisaite ja nende omanikke muudaks keerulisemaks veebisaitide võltsimise ja seega väheneks pettuste arv.

(49) Käesoleva määruse teatavate tehniliste üksikasjade paindlikuks ja kiireks täiendamiseks tuleks komisjonile anda volitus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud õigusakte seoses e-identimise koostalitlusega; usaldusteenuse pakkujatelt nõutavate turvameetmetega; tunnustatud sõltumatute asutustega, kes vastutavad teenuseosutajate kontrollimise eest; usaldusnimekirjadega; e-allkirja turvatasemetega seotud nõuetega; kvalifitseeritud sertifikaatidele esitatavate nõuetega, sertifikaatide valideerimise ja säilitamisega; kvalifitseeritud e-allkirja moodustamise vahendite sertifitseerimise eest vastutavate asutustega; e-templi turvatasemete ja e-templi kvalifitseeritud sertifikaatidega seotud nõuetega; andmevahetusteenuste vahelise koostalitlusvõimega. Eriti oluline on, et komisjon korraldaks ettevalmistustöö käigus asjakohaseid konsultatsioone, sealhulgas eksperditasandil.

(50) Komisjon peaks delegeeritud õigusaktide ettevalmistamise ja koostamise ajal tagama asjaomaste dokumentide sama- ja õigeaegse ning nõuetekohase edastamise Euroopa Parlamendile ja nõukogule.

(51) Selleks et tagada ühtsed tingimused käesoleva määruse rakendamiseks, tuleks komisjonile anda rakendamisvolitused eelkõige selliste standardite viitenumbrite täpsustamiseks, mille kasutamine eeldaks vastavust teatavatele käesolevas määruses sätestatud või delegeeritud õigusaktides sõnastatud nõuetele. Neid volitusi tuleks kasutada vastavalt Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrusele (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis

käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes[24].

(52) Õiguskindluse ja selguse huvides tuleks direktiiv 1999/93/EÜ tunnistada kehtetuks.

(53) Selleks et tagada õiguskindlus turu korraldajatele, kes juba kasutavad vastavalt direktiivile 1999/93/EÜ väljastatud kvalifitseeritud sertifikaate, tuleb ette näha piisav üleminekuaeg. Samuti tuleb anda komisjoni käsutusse vahendid rakendusaktide ja delegeeritud õigusaktide vastuvõtmiseks enne nimetatud tähtaega.

(54) Kuna käesoleva määruse eesmärki ei suuda liikmesriigid piisaval määral saavutada ning meetme ulatuse tõttu on seda parem saavutada liidu tasandil, võib liit võtta vastu meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale, eelkõige komisjoni rolli osas riikide tegevuse koordinaatorina,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

1. Käesolevas määruses sätestatakse e-identimise ja e-tehingute tegemiseks vajalike elektrooniliste usaldusteenuste eeskirjad eesmärgiga tagada siseturu nõuetekohane toimimine.

2. Käesolevas määruses sätestatakse tingimused, mille alusel peavad liikmesriigid tunnustama ja aktsepteerima füüsiliste ja juriidiliste isikute e-identimise vahendeid, mis kuuluvad teise liikmesriigi teavitatud e-identimise süsteemi.

3. Käesolevas määruses sätestatakse õigusraamistik e-allkirja, e-templi, e-ajatempli, e-dokumentide, e-andmevahetusteenuste ja veebisaitide autentimise kohta.

4. Käesoleva määrusega tagatakse, et määrusega kooskõlas olevatel usaldusteenustel ja -toodetel lubatakse siseturul vabalt ringelda.

Artikkel 2

Reguleerimisala

1. Käesolevat määrust kohaldatakse liikmesriikide poolt, nimel või vastutusel pakutava e-identimise ja ELis asuvate usaldusteenuse osutajate suhtes.

2. Käesolevat määrust ei kohaldata vabatahtlikul kokkuleppel põhinevate eraõiguslike elektrooniliste usaldusteenuste osutamise suhtes.

[24] ELT L 55, 28.2.2011, lk 13.

3. Käesolevat määrust ei kohaldata selliste lepingute või muude juriidiliste kohustuste sõlmimise ja kehtivusega seotud aspektide suhtes, kus on tegemist riiklikes või ELi õigusaktides sätestatud vormiliste nõuetega.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „e-identimine” – protsess, mille käigus kasutatakse elektroonilisi isikutuvastamisandmeid, mis esindavad üheselt mõistetavalt üht füüsilist või juriidilist isikut;

2) „e-identimise vahend” – materiaalne või mittemateriaalne üksus, mis sisaldab käesoleva artikli punktis 1 osutatud andmeid ja mida kasutatakse juurdepääsuks artiklis 5 osutatud internetipõhistele teenustele;

3) „e-identimise süsteem” – e-identimiseks vajalik süsteem, mille raames väljastatakse e-identimise vahendeid käesoleva artikli punktis 1 osutatud isikutele;

4) „autentimine” – elektrooniline protsess, mis võimaldab valideerida füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja terviklust;

5) „allakirjutaja” – e-allkirja andnud füüsiline isik;

6) „e-allkiri” – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida allakirjutaja kasutab allkirja andmiseks;

7) „täiustatud e-allkiri” – e-allkiri, mis vastab järgmistele nõuetele:

(a) see on seotud ainuüksi allakirjutajaga;

(b) selle abil on võimalik allakirjutajat tuvastada;

(c) see antakse e-allkirja moodustamiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allakirjutaja, ning

(d) see on seotud nende andmetega, millele see viitab, nii et kõik hilisemad andmete muudatused on tuvastatavad;

8) „kvalifitseeritud e-allkiri” – täiustatud e-allkiri, mis moodustatakse kvalifitseeritud e-allkirja moodustamise vahendi abil ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil;

9) „e-allkirja moodustamiseks vajalikud andmed” – ainulaadsed andmed, mida allakirjutaja kasutab e-allkirja andmiseks;

10) „sertifikaat” – elektrooniline tõend, mis seob füüsilise isiku e-allkirja või juriidilise isiku e-templi valideerimise andmed sertifikaadiga ja kinnitab selle isiku kõnealused andmed;

11) „e-allkirja kvalifitseeritud sertifikaat” – tõend, mida kasutatakse e-allkirja toetamiseks, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab I lisas sätestatud nõuetele;

12) „usaldusteenus” – elektrooniline teenus, mis seisneb e-allkirjade, e-templite, e-ajatemplite, e-dokumentide, e-andmevahetusteenuste, veebisaitide autentimise ja e-tõendite, sealhulgas e-allkirja ja e-templi jaoks vajalike sertifikaatide loomises, kontrollimises, valideerimises, käitamises ja säilitamises;

13) „kvalifitseeritud usaldusteenus” – usaldusteenus, mis vastab käesolevas määruses sätestatud kohaldatavatele nõuetele;

14) „usaldusteenuse osutaja” – füüsiline või juriidiline isik, kes osutab üht või mitut usaldusteenust;

15) „kvalifitseeritud usaldusteenuse osutaja” – usaldusteenuse osutaja, kes vastab käesolevas määruses sätestatud nõuetele;

16) „toode” – riist- või tarkvara või selle juurde kuuluvad osad, mis on ette nähtud usaldusteenuste osutamiseks;

17) „e-allkirja moodustamise vahend” – seadistatud tark- või riistvara, mida kasutatakse e-allkirja moodustamiseks;

18) „kvalifitseeritud e-allkirja moodustamise vahend” – e-allkirja moodustamise vahend, mis vastab II lisas sätestatud nõuetele;

19) „templi andja” – e-templi andnud juriidiline isik;

20) „e-tempel” – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mis tagavad seotud andmete päritolu ja tervikluse;

21) „täiustatud e-tempel” – elektrooniline tempel, mis vastab järgmistele nõuetele:

(a) see on seotud ainuüksi templi andjaga;

(b) selle abil on võimalik templi andjat tuvastada;

(c) see antakse e-templi moodustamiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures e-templi andmiseks kasutada üksnes templi andja; ning

(d) see on seotud nende andmetega, millele see viitab, nii et kõik hilisemad andmete muudatused on tuvastatavad;

22) „kvalifitseeritud e-tempel” – täiustatud e-tempel, mis moodustatakse kvalifitseeritud e-templi moodustamise vahendi abil ja mis põhineb e-templi kvalifitseeritud sertifikaadil;

23) „e-templi moodustamiseks vajalikud andmed” – ainulaadsed andmed, mida e-templi andja kasutab e-templi moodustamiseks;

24) „e-templi kvalifitseeritud sertifikaat” – tõend, mida kasutatakse e-templi toetamiseks, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab III lisas sätestatud nõuetele;

25) „e-ajatempel” – elektroonilised andmed, mis seovad muud elektroonilised andmed kindla ajahetkega ja tõendavad, et nimetatud andmed olid sel ajahetkel olemas;

26) „kvalifitseeritud e-ajatempel” – e-ajatempel, mis vastab artiklis 33 sätestatud nõuetele;

27) „e-dokument” – mis tahes elektroonilises vormingus dokument;

28) „e-andmevahetusteenus” – teenus, mis võimaldab edastada andmeid elektrooniliselt, tõendab edastatud andmete käitamist, sealhulgas andmete saatmist või kättesaamist, ja kaitseb edastatud andmeid kadumise, varastamise, kahjustamise või lubamatu muutmise eest;

29) „kvalifitseeritud e-andmevahetusteenus” – elektrooniline andmevahetusteenus, mis vastab artiklis 36 sätestatud nõuetele;

30) „kvalifitseeritud sertifikaat veebisaidi autentimiseks” – tõend, mis võimaldab autentida veebisaiti ja seob selle isikuga, kellele sertifikaat on väljastatud, ning mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab IV lisas sätestatud nõuetele;

31) „valideerimisandmed” – andmed, mida kasutatakse e-allkirja või e-templi valideerimiseks.

Artikkel 4

Siseturu põhimõtted

1. Ühe liikmesriigi territooriumil ei tohi piirata teises liikmesriigis asuva usaldusteenuse osutaja usaldusteenuste osutamist põhjustel, mis kuuluvad käesoleva määrusega hõlmatud valdkondadesse.

2. Käesoleva määrusega kooskõlas olevatel toodetel lubatakse siseturul vabalt ringelda.

II PEATÜKK

E-IDENTIMINE

Artikkel 5

Vastastikune tunnustamine ja aktsepteerimine

Kui vastavalt riigisisestele õigusaktidele või haldustavadele nõutakse internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja e-autentimist, peab nimetatud teenusele juurdepääsuks tunnustama ja aktsepteerima igat teises liikmesriigis väljastatud e-identimise vahendit, mis kuulub komisjoni poolt vastavalt artiklis 7 esitatud menetlusele avaldatud nimekirjas olevasse süsteemi.

Artikkel 6

E-identimise süsteemidest teavitamise tingimused

1. E-identimise süsteemidest saab vastavalt artiklile 7 teavitada juhul, kui täidetud on kõik järgmised tingimused:

(a) e-identimise vahend on väljastatud teavitava liikmesriigi poolt, nimel või vastutusel;

(b) e-identimise vahendit saab kasutada vähemalt e-identimist eeldavatele avalikele teenustele juurdepääsuks teavitavas liikmesriigis;

(c) teavitav liikmesriik tagab, et isikutuvastamisandmeid saab üheselt mõistetavalt omistada artikli 3 punktis 1 osutatud füüsilisele või juriidilisele isikule;

(d) teavitav liikmesriik tagab igal ajal tasuta internetipõhise autentimise võimaluse olemasolu, nii et iga asjaomane osapool saab valideerida elektrooniliselt saadud isikutuvastusandmed; liikmesriigid ei tohi asjaomastele osalistele kehtestada mingeid tehnilisi eritingimusi autentimiseks väljaspool oma territooriumi; kui teavitatud identimissüsteemi või autentimisvõimalust rikutakse või see on osaliselt ohustatud, peavad liikmesriigid teavitatud identimissüsteemi, autentimisvõimaluse või

asjaomased ohustatud osad viivitamata peatama või tühistama ning teavitama teisi liikmesriike ja komisjoni vastavalt artiklile 7;

(e) teavitav liikmesriik on vastutav

– i) punktis c osutatud isikutuvastamisandmete üheselt mõistetava omistamise ja

– ii) punktis d osutatud autentimisvõimaluse eest.

2. Lõike 1 punkt e ei piira osaliste vastutust tehingute eest, milles kasutatakse teavitatud süsteemi kuuluvaid e-identimise vahendeid.

Artikkel 7

Teavitamine

1. Liikmesriigid, kes teatavad e-identimise süsteemist, peavad komisjonile edastama järgmise teabe ja põhjendamatu viivituseta selle iga hilisema muudatuse:

(a) teavitatud e-identimise süsteemi kirjeldus;

(b) e-identimise süsteemi eest vastutavad asutused;

(c) teave selle kohta, kes haldab üheselt mõistetavate isikutuvastamisandmete registreerimist;

(d) autentimisvõimaluse kirjeldus;

(e) teavitatud identimissüsteemi, autentimisvõimaluse või asjaomase ohustatud osa peatamise või tühistamise kord.

2. Kuus kuud pärast määruse jõustumist avaldab komisjon *Euroopa Liidu Teatajas* nimekirja e-identimise süsteemidest, millest on teavitatud vastavalt lõikele 1, ja nendega seotud põhiteabe.

3. Kui komisjoni teavitatakse pärast lõikes 2 osutatud ajavahemiku möödumist, muudab ta nimekirja kolme kuu jooksul.

4. Komisjon võib rakendusaktidega kindlaks määrata lõigetes 1 ja 3 osutatud teavitamise asjaolud, vormingud ja menetlused. Need rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 8

Koordineerimine

1. Liikmesriigid teevad koostööd, et tagada teavitatud süsteemi kuuluvate e-identimise vahendite koostalitlus ja suurendada nende turvalisust.

2. Komisjon kehtestab rakendusaktide abil vajaliku korra lõikes 1 osutatud liikmesriikidevahelise koostöö hõlbustamiseks eesmärgiga edendada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele. Nimetatud rakendusaktid hõlmavad eelkõige teabevahetust, e-identimise süsteemide alaseid kogemusi ja häid tavasid, teavitatud e-

identimise süsteemide vastastikust hindamist ja e-identimise valdkonnas toimuva arengu analüüsimist liikmesriikide pädevate asutuste poolt. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

3. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte e-identimise vahendite piiriülese koostalitluse lihtsustamiseks tehniliste miinimumnõuete kehtestamise abil.

III PEATÜKK

USALDUSTEENUSED

1. jagu

Üldsätted

Artikkel 9

Vastutus

1. Usaldusteenuse osutaja vastutab füüsilisele või juriidilisele isikule põhjustatud mis tahes otsese kahju eest, mis tuleneb artikli 15 lõikes 1 sätestatud kohustuste täitmatajätmisest, välja arvatud juhul, kui usaldusteenuse osutaja suudab tõestada, et ta ei ole tegutsenud ettevaatamatult.

2. Kvalifitseeritud usaldusteenuse osutaja vastutab füüsilisele või juriidilisele isikule põhjustatud mis tahes otsese kahju eest, mis tuleneb käesolevas määruses, eelkõige artiklis 19, sätestatud kohustuste mittetäitmisest, välja arvatud juhul, kui kvalifitseeritud usaldusteenuse osutaja suudab tõestada, et ta ei ole tegutsenud ettevaatamatult.

Artikkel 10

Kolmandatest riikidest pärit usaldusteenuste osutajad

1. Kolmandas riigis asuvate kvalifitseeritud usaldusteenuse osutajate pakutavaid kvalifitseeritud usaldusteenuseid ja kvalifitseeritud sertifikaate käsitatakse liidu territooriumil asuvate kvalifitseeritud usaldusteenuse osutajate pakutavate kvalifitseeritud usaldusteenuste ja kvalifitseeritud sertifikaatidena juhul, kui kolmandast riigist pärit kvalifitseeritud usaldusteenuseid ja kvalifitseeritud sertifikaate tunnustatakse liidu ja kolmandate riikide või rahvusvaheliste organisatsioonide vahelise kokkuleppe alusel kooskõlas ELi toimimise lepingu artikliga 218.

2. Lõike 1 osas tagatakse selliste kokkulepetega, et kolmandate riikide usaldusteenuse osutajad või rahvusvahelised organisatsioonid täidavad liidu territooriumil asuvate kvalifitseeritud usaldusteenuse osutajate pakutavate kvalifitseeritud usaldusteenuste ja kvalifitseeritud sertifikaatide suhtes kohaldatavaid nõudeid, eelkõige seoses isikuandmete kaitse, turvalisuse ja järelevalvega.

Artikkel 11

Andmetöötlus ja -kaitse

1. Usaldusteenuse osutajad ja järelevalveasutused tagavad isikuandmete õiglase ja seadusliku töötlemise kooskõlas direktiiviga 95/46/EÜ.

2. Usaldusteenuse osutajad töötlevad isikuandmeid direktiivi 95/46/EÜ kohaselt. Kõnealusel töötlemisel piirdutakse rangelt minimaalse andmehulgaga, mis on vajalik sertifikaadi väljaandmiseks ja haldamiseks või usaldusteenuse osutamiseks.

3. Usaldusteenuse osutajad tagavad selle isiku andmete konfidentsiaalsuse ja tervikluse, kellele usaldusteenust osutatakse.

4. Ilma et see piiraks riikliku õiguse kohast varjunimede õiguslikku toimet, ei takista liikmesriigid usaldusteenuse osutajaid märkimast e-allkirja sertifikaadile allakirjutaja nime asemel varjunime.

Artikkel 12

Puuetega inimeste takistusteta juurdepääs

Osutatavad usaldusteenused ja kõnealuste teenuste osutamisel kasutatavad lõpptarbijale suunatud tooted tehakse võimaluse korral puuetega inimestele juurdepääsetavaks.

2. jagu

Järelevalve

Artikkel 13

Järelevalveasutus

1. Liikmesriigid määravad oma territooriumil või, vastastikusel kokkuleppel, teises liikmesriigis asuva asjakohase asutuse määrava liikmesriigi vastutusel. Järelevalveasutustele antakse kõik nende ülesannete täitmiseks vajalikud järelevalve- ja uurimisvolitused.

2. Järelevalveasutus vastutab järgmiste ülesannete täitmise eest:

(a) teostada järelevalvet määrava liikmesriigi territooriumil asuvate usaldusteenuse osutajate üle tagamaks, et nad täidavad artiklis 15 sätestatud nõudeid;

(b) teostada järelevalvet määrava liikmesriigi territooriumil asuvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste üle tagamaks, et nemad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses sätestatud kohaldatavatele nõuetele;

(c) tagada, et artikli 19 lõike 2 punktis g osutatud ja kvalifitseeritud usaldusteenuse osutajate poolt salvestatud asjaomane teave ja andmed säilitatakse ning hoitakse kättesaadavana piisava aja jooksul pärast kvalifitseeritud usaldusteenuste osutaja tegevuse lõpetamist, et tagada teenuse järjepidevus.

3. Iga järelevalveasutus esitab komisjonile ja liikmesriikidele järgmise aasta esimese kvartali lõpuks aastaaruande viimase kalendriaasta järelevalvetegevuse kohta. Aruanne peab sisaldama vähemalt järgmist:

(a) teave asutuse järelevalvetegevuse kohta;

(b) kokkuvõte usaldusteenuse osutajatelt artikli 15 lõike 2 kohaselt saadud rikkumisteadetest;

(c) statistika kvalifitseeritud usaldusteenuste turu ja kasutuse kohta, sealhulgas teave kvalifitseeritud usaldusteenuse osutajate, nende osutatavate kvalifitseeritud usaldusteenuste ja kasutatavate toodete kohta ning nende klientide üldkirjeldus.

4. Liikmesriigid teatavad komisjonile ja teistele liikmesriikidele oma vastavate määratud järelevalveasutuste nimed ja aadressid.

5. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse lõikes 2 osutatud ülesannete suhtes kohaldatavate menetluste määratlemist.

6. Komisjon võib rakendusaktide abil kindlaks määrata lõikes 3 osutatud aruande asjaolusid, vorminguid ja menetlusi. Need rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 14

Vastastikune abi

1. Selleks et tegevus saaks toimuda järjepidevalt, teevad järelevalveasutused koostööd heade tavade vahetamiseks ja üksteisele võimalikult kiiresti asjaomase teabe ja vastastikuse abi andmiseks. Vastastikune abi hõlmab eelkõige teabenõudeid ja järelevalvemeetmeid, näiteks taotlusi turvakontrollide läbiviimiseks, nagu on osutatud artiklites 15, 16 ja 17.

2. Järelevalveasutus, kellele abitaotlus on adresseeritud, ei või taotluse täitmisest keelduda, välja arvatud juhul, kui:

(a) asutus ei ole taotlusega tegelemiseks pädev või

(b) taotluse täitmine oleks vastuolus käesoleva määrusega.

3. Kui see on asjakohane, võivad järelevalveasutused korraldada ühiseid uurimisi, millesse on kaasatud teiste liikmesriikide järelevalveasutuste töötajad.

Selle liikmesriigi järelevalveasutus, kus uurimine toimub, võib kooskõlas oma riigisiseste õigusaktidega anda uurimisülesanded üle abistatava järelevalveasutuse töötajatele. Kõnealuseid volitusi võib kasutada ainult vastuvõtva järelevalveasutuse töötajate juhendamisel ja juuresolekul. Abistatava järelevalveasutuse töötajate suhtes kohaldatakse vastuvõtva järelevalveasutuse riigisisest õigust. Vastuvõttev järelevalveasutus vastutab abistatava järelevalveasutuse töötajate tegevuse eest.

4. Komisjon võib rakendusaktide abil täpsustada käesolevas artiklis sätestatud vastastikuse abi vorminguid ja menetlusi. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 15

Usaldusteenuse osutajate suhtes kohaldatavad turvanõuded

1. Liidu territooriumil asuvad usaldusteenuse osutajad võtavad asjakohased tehnilised ja korralduslikud meetmed, et ohjata nende osutatavate usaldusteenuste turvalisusega seotud riske. Tehnika taset arvesse võttes tagatakse nende meetmetega riski astmele vastav turvalisuse tase. Eelkõige võetakse meetmeid turvaintsidentide vältimiseks ja nende mõju minimeerimiseks ning sidusrühmade teavitamiseks võimalike intsidentide kahjulikust mõjust.

Ilma et see piiraks artikli 16 lõike 1 kohaldamist, võib iga usaldusteenuse osutaja esitada järelevalveasutusele aruande tunnustatud sõltumatu asutuse teostatud turvakontrolli kohta, et kinnitada asjakohaste turvameetmete võtmist.

2. Usaldusteenuse osutajad peavad põhjendamatu viivituseta teavitama pädevat järelevalveasutust, infoturbe eest vastutavat pädevat riiklikku asutust ja muid asjaomaseid kolmandaid isikuid, nagu andmekaitseasutused, igast turvarikkumisest või tervikluse kaost, millel on märkimisväärne mõju osutatavale usaldusteenusele ja selles sisalduvatele isikuandmetele, tehes seda võimaluse korral 24 tunni jooksul pärast sellest teadasaamist.

Kui see on asjakohane ja eelkõige juhul, kui turvarikkumine või tervikluse kadu hõlmab kahte või enamat liikmesriiki, teavitab asjaomane järelevalveasutus teiste liikmesriikide järelevalveasutusi ning Euroopa Võrgu- ja Infoturbeametit (ENISA).

Kui asjaomane järelevalveasutus leiab, et avalik huvi nõuab rikkumise avalikustamist, võib ta teavitada ka üldsust või nõuda üldsuse teavitamist asjaomaselt usaldusteenuse osutajalt.

3. Järelevalveasutus esitab ENISAle ja komisjonile kord aastas kokkuvõtte usaldusteenuse osutajatelt saadud rikkumisteadetest.

4. Lõigete 1 ja 2 rakendamiseks on pädeval järelevalveasutusel õigus anda usaldusteenuse osutajatele siduvaid suuniseid.

5. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse lõikes 1 osutatud meetmete edasist täpsustamist.

6. Komisjon võib rakendusaktidega kindlaks määrata lõigete 1 ja 3 kohaldamisega seotud asjaolud, vormingud ja menetlused, sealhulgas tähtajad. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 16

Kvalifitseeritud usaldusteenuse osutajate järelevalve

1. Tunnustatud sõltumatu asutus kontrollib kvalifitseeritud usaldusteenuse osutajaid kord aastas tagamaks, et kõnealused teenuseosutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses sätestatud nõuetele, ning esitavad turvakontrolli aruande järelevalveasutusele.

2. Ilma et see piiraks lõike 1 kohaldamist, võib järelevalveasutus kvalifitseeritud usaldusteenuse osutajaid igal ajal kas oma algatusel või komisjoni taotluse alusel kontrollida

tagamaks, et kõnealused teenuseosutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad jätkuvalt käesolevas määruses sätestatud tingimustele. Kui isikuandmete kaitse eeskirju on ilmselt rikutud, teavitab järelevalveasutus oma kontrollide tulemustest andmekaitseasutusi.

3. Järelevalveasutusel on õigus anda kvalifitseeritud usaldusteenuse osutajatele siduvaid suuniseid, et nad heastaksid kõik turvakontrolli aruandes osutatud nõuete täitmatajätmised.

4. Kui kvalifitseeritud usaldusteenuse osutaja ei heasta lõikes 3 osutatu kohaselt kõnealust nõuete täitmatajätmist järelevalveasutuse seatud ajavahemiku jooksul, kaotab ta oma kvalifitseeritud staatuse ja järelevalveasutus teatab talle tema staatuse vastavast muutmisest artiklis 18 osutatud usaldusnimekirjades.

5. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse selliste tingimuste täpsustamist, mille alusel tunnustatakse käesoleva artikli lõikes 1, artikli 15 lõikes 1 ja artikli 17 lõikes 1 osutatud turvakontrolli teostavat sõltumatut asutust.

6. Komisjon võib rakendusaktidega kindlaks määrata lõigete 1, 2 ja 4 kohaldamisega seotud asjaolud, menetlused ja vormingud. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 17

Kvalifitseeritud usaldusteenuse osutamise alustamine

1. Kvalifitseeritud usaldusteenuse osutajad teavitavad järelevalveasutust oma kavatsusest alustada kvalifitseeritud usaldusteenuse osutamist ja esitavad järelevalveasutusele artikli 16 lõikes 1 sätestatud, tunnustatud sõltumatu asutuse teostatud turvakontrolli aruande. Kvalifitseeritud usaldusteenuse osutajad võivad alustada kvalifitseeritud usaldusteenuse osutamist pärast seda, kui nad on esitanud teate ja turvakontrolli aruande järelevalveasutusele.

2. Kui asjaomased dokumendid on lõike 1 kohaselt järelevalveasutusele esitatud, kantakse kvalifitseeritud teenuseosutajad artiklis 18 osutatud usaldusnimekirjadesse, mis näitab, et teade on esitatud.

3. Järelevalveasutus kontrollib kvalifitseeritud usaldusteenuse osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste vastavust käesoleva määruse nõuetele.

Pärast kontrolli positiivse tulemuse saamist näitab järelevalveasutus kvalifitseeritud usaldusteenuse osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste kvalifitseeritud staatust usaldusnimekirjades hiljemalt üks kuu pärast teate esitamist vastavalt lõikele 1.

Kui kontrolli ei ole ühe kuu jooksul lõpule viidud, teavitab järelevalveasutus kvalifitseeritud usaldusteenuse osutajat viivituse põhjustest ja ajavahemikust, mille vältel kontroll lõpule viiakse.

4. Kui kvalifitseeritud usaldusteenuse kohta on esitatud lõike 1 kohane teade, ei saa asjaomane avaliku sektori asutus teenusest haldusmenetluse või formaalsuse täitmiseks keelduda põhjendusega, et seda ei ole kantud lõikes 3 osutatud nimekirjadesse.

5. Komisjon võib rakendusaktidega kindlaks määrata lõigete 1, 2 ja 3 kohaldamisega seotud asjaolud, vormingud ja menetlused. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 18

Usaldusnimekirjad

1. Iga liikmesriik koostab, haldab ja avaldab usaldusnimekirjad, mis sisaldavad teavet tema vastutusalasse kuuluvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste kohta.

2. Liikmesriigid koostavad, haldavad ja avaldavad elektrooniliselt allkirjastatud või e-templiga varustatud, lõikes 1 sätestatud usaldusnimekirjad turvalisel viisil ja automaatseks töötlemiseks sobivas vormingus.

3. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta teabe, mis hõlmab riigisiseste usaldusnimekirjade koostamise, haldamise ja avaldamise eest vastutavat asutust, kõnealuste nimekirjade avaldamise koha üksikasju, nimekirjade allkirjastamiseks või templiga varustamiseks kasutatavat sertifikaati ning nimekirjade mis tahes muudatusi.

4. Komisjon teeb lõikes 3 osutatud teabe turvalise kanali kaudu avalikkusele kättesaadavaks automaatseks töötlemiseks sobivas, elektrooniliselt allkirjastatud või e-templiga varustatud vormingus.

5. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse lõikes 1 osutatud teabe määratlemist.

6. Komisjon võib rakendusaktidega kindlaks määrata lõigete 1–4 kohaldamisega seotud usaldusnimekirjade tehnilised kirjeldused ja vormingud. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 19

Nõuded kvalifitseeritud usaldusteenuse osutajatele

1. Kvalifitseeritud sertifikaati väljastades kontrollib kvalifitseeritud usaldusteenuse osutaja asjakohaste vahenditega ja riiklike õigusaktide kohaselt selle füüsilise või juriidilise isiku identiteeti, kellele kvalifitseeritud sertifikaat väljastatakse, ja vajaduse korral tema eritunnuseid.

Kvalifitseeritud teenuseosutaja või kvalifitseeritud teenuseosutaja vastutusel tegutsev volitatud kolmas isik kontrollib kõnealust teavet järgmiselt:

(a) füüsilise isiku või juriidilise isiku volitatud esindaja füüsilise välimuse alusel või

(b) kaughindamise teel, kasutades kooskõlas punktiga a väljastatud teavitatud süsteemi kuuluvaid e-identimise vahendeid.

2. Kvalifitseeritud usaldusteenuseid osutavad kvalifitseeritud usaldusteenuse osutajad:

(a) võtavad tööle personali, kellel on vajalik pädevus, kogemus ja kvalifikatsioon, kes rakendavad Euroopa või rahvusvahelistele standarditele vastavaid haldus- ja juhtimismenetlusi ning kes on saanud turva- ja isikuandmete kaitse eeskirjade alal asjakohase koolituse;

(b) kannavad vastutust võimalike kahjude eest, hallates piisavat hulka rahalisi vahendeid või omades asjakohast vastutuskindlustust;

(c) teavitavad enne lepingu sõlmimist kõiki kvalifitseeritud usaldusteenust kasutada soovivaid isikuid kõnealuse teenuse kasutamise täpsetest tingimustest;

(d) kasutavad usaldusväärseid süsteeme ja tooteid, mis on kaitstud muutmise eest, ja tagavad nende toetatavate toimingute tehnilise turvalisuse ja usaldusväärsuse;

(e) kasutavad neile esitatud andmete säilitamiseks ehtsuse tõendamist võimaldavas vormingus usaldusväärseid süsteeme nii, et:

– need on otsingutes üldkättesaadavad üksnes siis, kui isik, kellele andmed on väljastatud, on andnud selleks nõusoleku,

– andmeid saavad sisestada ja muuta üksnes selleks volitatud isikud,

– on võimalik kindlaks teha, kas andmed on ehtsad;

(f) võtavad meetmeid andmete võltsimise ja varguse vastu;

(g) salvestavad sobivaks tähtajaks kogu asjakohase teabe kvalifitseeritud usaldusteenuse osutaja väljastatud ja saadud andmete kohta, eelkõige tõendamiseks kohtumenetlustes. Sellised andmed võib salvestada elektrooniliselt;

(h) omavad ajakohast tegevuse lõpetamiskava, et tagada teenuse järjepidevus kooskõlas järelevalveasutuse artikli 13 lõike 2 punkti c kohaselt kehtestatud korraga;

(i) tagavad isikuandmete seadusliku töötlemise kooskõlas artikliga 11.

3. Kvalifitseeritud sertifikaate väljastavad kvalifitseeritud usaldusteenuse osutajad registreerivad sertifikaadi tühistamise oma sertifikaatide andmebaasis 10 minuti jooksul pärast kõnealust tühistamist.

4. Seoses lõikega 3 annavad kvalifitseeritud sertifikaate väljastavad kvalifitseeritud usaldusteenuse osutajad asjaomastele osalistele teavet nende väljastatud kvalifitseeritud sertifikaatide kehtivuse või tühistamise kohta. Kõnealune teave tehakse igal ajal vähemalt iga sertifikaadi kohta kättesaadavaks automaatsel viisil, mis on usaldusväärne, tasuta ja tõhus.

5. Komisjon võib rakendusaktidega kehtestada usaldusväärsete süsteemide ja toodete standardite viitenumbrid. Kui usaldusväärsed süsteemid ja tooted vastavad kõnealustele standarditele, loetakse artiklis 19 sätestatud nõuded täidetuks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

3. jagu

E-allkiri

Artikkel 20

E-allkirjade õiguslik toime ja tunnustamine

1. E-allkirja ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul.

2. Kvalifitseeritud e-allkirjal on käsitsi kirjutatud allkirjaga samaväärne õiguslik toime.

3. Kvalifitseeritud e-allkirju tunnustatakse ja aktsepteeritakse kõikides liikmesriikides.

4. Kui nõutakse kvalifitseeritud e-allkirjast madalama turvagarantii tasemega e-allkirja, eriti siis, kui seda nõuab liikmesriik avaliku sektori asutuse osutatava internetipõhise teenuse kasutamiseks sellise teenusega seotud riskide asjakohase hindamise alusel, tunnustatakse ja aktsepteeritakse kõiki e-allkirju, millel on vähemalt sama turvagarantii tase.

5. Liikmesriigid ei nõua avaliku sektori asutuse osutatava internetipõhise teenuse piiriüleseks kasutamiseks e-allkirja, mille turvagarantii tase on kõrgem kui kvalifitseeritud e-allkirjal.

6. Komisjonile antakse volitused võtta artiklis 38 sätestatud korras vastu delegeeritud õigusakte, milles käsitletakse lõikes 4 osutatud e-allkirja eri turvatasemete määratlemist.

7. Komisjon võib rakendusaktidega kehtestada e-allkirja turvatasemete standardite viitenumbrid. Kui e-allkiri vastab kõnealustele standarditele, loetakse see lõike 6 kohaselt vastuvõetud delegeeritud aktis määratletud turvatasemele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 21

E-allkirja kvalifitseeritud sertifikaadid

1. E-allkirja kvalifitseeritud sertifikaadid peavad vastama I lisas sätestatud nõuetele.

2. E-allkirja kvalifitseeritud sertifikaatide suhtes ei kohaldata ühtegi kohustuslikku nõuet, mis ületab I lisas sätestatud nõudeid.

3. Kui e-allkirja kvalifitseeritud sertifikaat tühistatakse pärast esialgset aktiveerimist, kaotab see kehtivuse ega saa oma staatust mingil juhul kehtivuse uuendamisega tagasi.

4. Komisjonile antakse volitused võtta vastavalt artiklile 38 vastu delegeeritud õigusakte I lisas sätestatud nõuete edasise täpsustamise kohta.

5. Komisjon võib rakendusaktidega kehtestada e-allkirja kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui e-allkirja kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see I lisas sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 22

Nõuded kvalifitseeritud e-allkirja moodustamise vahenditele

1. Kvalifitseeritud e-allkirja moodustamise vahendid peavad vastama II lisas sätestatud nõuetele.

2. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirja moodustamise vahendite standardite viitenumbrid. Kui kvalifitseeritud e-allkirja moodustamise vahend vastab kõnealustele standarditele, loetakse see II lisas sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 23

Kvalifitseeritud e-allkirja moodustamise vahendite sertifitseerimine

1. Kvalifitseeritud e-allkirja moodustamise vahendeid võivad sertifitseerida liikmesriikide määratud asjakohased avalik-õiguslikud või eraõiguslikud asutused, tingimusel et nad on läbinud turvalisuse hindamise protsessi, mis on teostatud kooskõlas ühega standarditest selliste infotehnoloogiatoodete turvalisuse hindamiseks, mis on kantud komisjoni poolt rakendusaktidega koostatavasse nimekirja. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

2. Liikmesriigid teatavad komisjonile ja teistele liikmesriikidele selliste avalik-õiguslike või eraõiguslike asutuste nimed ja aadressid, kelle nad on lõike 1 kohaselt määranud.

3. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse lõikes 1 osutatud selliste konkreetsete kriteeriumide kehtestamist, millele määratud asutused peavad vastama.

Artikkel 24

Sertifitseeritud kvalifitseeritud e-allkirja moodustamise vahendite nimekirja avaldamine

1. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta teabe selliste kvalifitseeritud e-allkirja moodustamise vahendite kohta, mille on sertifitseerinud artiklis 23 osutatud asutused. Samuti edastavad nad komisjonile põhjendamatu viivituseta teabe selliste kvalifitseeritud e-allkirja moodustamise vahendite kohta, mis ei ole enam sertifitseeritud.

2. Saadud teabe põhjal koostab komisjon sertifitseeritud kvalifitseeritud e-allkirja moodustamise vahendite nimekirja, haldab seda ja avaldab selle.

3. Komisjon võib rakendusaktidega kindlaks määrata lõike 1 kohaldamisega seotud asjaolud, vormingud ja menetlused. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 25

Nõuded kvalifitseeritud e-allkirjade valideerimisele

1. Kvalifitseeritud e-allkiri loetakse kehtivaks, kui on võimalik väga kindlalt tagada, et allkirja andmise ajal olid täidetud järgmised tingimused:

(a) allkirja sertifikaat on kvalifitseeritud e-allkirja sertifikaat, mis vastab I lisa sätetele;

(b) nõutav kvalifitseeritud sertifikaat on ehtne ja kehtiv;

(c) allkirja valideerimise andmed vastavad asjaomastele osalistele esitatud andmetele;

(d) allakirjutajat üheselt mõistetavalt esindavad andmed on esitatud nõuetekohaselt asjaomasele osalisele;

(e) kui kasutatakse varjunime, on varjunime kasutus asjaomasele osalisele selgesti näidatud;

(f) e-allkiri on antud kvalifitseeritud e-allkirja moodustamise vahendiga;

(g) allkirjastatud andmete terviklust ei ole rikutud;

(h) artikli 3 punktis 7 sätestatud nõuded on täidetud;

(i) allkirja valideerimiseks kasutatav süsteem annab asjaomasele osalisele valideerimisprotsessi korrektse tulemuse ja võimaldab asjaomasel osalisel tuvastada turvalisusega seotud probleeme.

2. Komisjonile antakse volitused võtta vastavalt artiklile 38 vastu delegeeritud õigusakte lõikes 1 sätestatud nõuete edasise täpsustamise kohta.

3. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirjade valideerimise standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade valideerimine vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 26

Kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenus

1. Kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenust osutab kvalifitseeritud usaldusteenuse osutaja, kes:

(a) osutab valideerimisteenust kooskõlas artikli 25 lõikega 1 ja

(b) võimaldab asjaomastel osalistel saada valideerimisprotsessi tulemused automaatsel viisil, mis on usaldusväärne, tõhus ja millel on kvalifitseeritud valideerimisteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel.

2. Komisjon võib rakendusaktidega kehtestada lõikes 1 osutatud kvalifitseeritud valideerimisteenuse standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade valideerimisteenus vastab kõnealustele standarditele, loetakse see lõike 1 punktis b sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 27

Kvalifitseeritud e-allkirjade säilitamine

1. Kvalifitseeritud e-allkirjade säilitamise teenust osutab kvalifitseeritud usaldusteenuse osutaja, kes kasutab menetlusi ja tehnoloogiat, millega on võimalik pikendada kvalifitseeritud e-allkirja valideerimise andmete usaldusväärsust üle nende tehnoloogilise kehtivusaja.

2. Komisjonile antakse volitused võtta vastavalt artiklile 38 vastu delegeeritud õigusakte lõikes 1 sätestatud nõuete edasise täpsustamise kohta.

3. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirjade säilitamise standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade säilitamise kord vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

4. jagu

E-tempel

Artikkel 28

E-templi õiguslik toime

1. E-templit ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul.

2. Kvalifitseeritud e-templil on õiguslik eeldus tagada sellega seotud andmete päritolu ja terviklus.

3. Kvalifitseeritud e-templit tunnustatakse ja aktsepteeritakse kõikides liikmesriikides.

4. Kui nõutakse kvalifitseeritud e-templist madalama turvagarantii tasemega e-templit, eriti siis, kui seda nõuab liikmesriik avaliku sektori asutuse osutatava internetipõhise teenuse kasutamiseks sellise teenusega seotud riskide asjakohase hindamise alusel, aktsepteeritakse kõiki e-templeid, millel on vähemalt sama turvagarantii tase.

5. Liikmesriigid ei nõua avaliku sektori asutuse osutatavate internetipõhiste teenuste kasutamiseks e-templit, mille turvagarantii tase on kõrgem kui kvalifitseeritud e-templil.

6. Komisjonile antakse volitused võtta artiklis 38 sätestatud korras vastu delegeeritud õigusakte, milles käsitletakse lõikes 4 osutatud e-templi eri turvatasemete määratlemist.

7. Komisjon võib rakendusaktidega kehtestada e-templi turvagarantii tasemete standardite viitenumbrid. Kui e-tempel vastab kõnealustele standarditele, loetakse see lõike 6 kohaselt vastuvõetud delegeeritud õigusaktis määratletud turvagarantii tasemele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 29

Nõuded e-templi kvalifitseeritud sertifikaatidele

1. E-templi kvalifitseeritud sertifikaadid peavad vastama III lisas sätestatud nõuetele.

2. E-templi kvalifitseeritud sertifikaatide suhtes ei kohaldata ühtegi kohustuslikku nõuet, mis ületab III lisas sätestatud nõudeid.

3. Kui e-templi kvalifitseeritud sertifikaat tühistatakse pärast esialgset aktiveerimist, kaotab see kehtivuse ega saa oma staatust mingil juhul kehtivuse uuendamisega tagasi.

4. Komisjonile antakse volitused võtta vastavalt artiklile 38 vastu delegeeritud õigusakte III lisas sätestatud nõuete edasise täpsustamise kohta.

5. Komisjon võib rakendusaktidega kehtestada e-templi kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui e-templi kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see III lisas sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

Artikkel 30

Kvalifitseeritud e-templi moodustamise vahendid

1. Kvalifitseeritud e-templi moodustamise vahendeid käsitlevate nõuete suhtes kohaldatakse *mutatis mutandis* artiklit 22.

2. Kvalifitseeritud e-templi moodustamise vahendite sertifitseerimise suhtes kohaldatakse *mutatis mutandis* artiklit 23.

3. Sertifitseeritud kvalifitseeritud e-templi moodustamise vahendite nimekirja avaldamise suhtes kohaldatakse *mutatis mutandis* artiklit 24.

Artikkel 31

Kvalifitseeritud e-templite valideerimine ja säilitamine

Kvalifitseeritud e-templite valideerimise ja säilitamise suhtes kohaldatakse *mutatis mutandis* artikleid 25, 26 ja 27.

5. jagu

E-ajatempel

Artikkel 32

E-ajatempli õiguslik toime

1. E-ajatemplit ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul.

2. Kvalifitseeritud e-ajatemplil on õiguslik eeldus tõendada sellega osutatavat ajahetke ja tagada kõnealuse ajahetkega seotud andmete terviklus.

3. Kvalifitseeritud e-ajatemplit tunnustatakse ja aktsepteeritakse kõikides liikmesriikides.

Artikkel 33

Nõuded kvalifitseeritud e-ajatemplitele

1. Kvalifitseeritud e-ajatempel peab vastama järgmistele nõuetele:

(a) see on täpselt seotud koordineeritud maailmaajaga (UTC), et välistada andmete tuvastamatu muutmise võimalus;

(b) see põhineb täpsel ajaallikal;

(c) selle väljastab kvalifitseeritud usaldusteenuse osutaja;

(d) selle allkirjastamiseks kasutatakse kvalifitseeritud usaldusteenuse osutaja pakutavat täiustatud e-allkirja või täiustatud e-templit või muud samaväärset meetodit.

2. Komisjon võib rakendusaktidega kehtestada viitenumbrid standarditele, mis hõlmavad andmete sidumist täpse ajahetkega ja täpset ajaallikat. Kui andmete sidumine täpse ajahetkega ja täpne ajaallikas vastavad kõnealustele standarditele, loetakse need lõikes 1 sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

6. jagu

E-dokumendid

Artikkel 34

E-dokumentide õiguslik toime ja tunnustamine

1. E-dokumenti loetakse paberdokumendiga samaväärseks ja see on kohtumenetlustes tõenduskõlblik, kui on võetud arvesse selle ehtsuse ja tervikluse tagamise taset.

2. Dokumendil, millel on asjaomase dokumendi väljastamiseks pädeva isiku kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel, on õiguslik eeldus ehtsusele ja terviklusele tingimusel, et dokument ei sisalda dünaamilisi elemente, mis võivad dokumenti automaatselt muuta.

3. Kui avaliku sektori asutuse pakutava internetipõhise teenuse osutamiseks nõutakse originaaldokumenti või kinnitatud koopiat, aktsepteeritakse teistes liikmesriikides ilma täiendavate nõueteta vähemalt selliseid e-dokumente, mille on väljastanud asjaomaste

dokumentide väljastamiseks pädevad isikud ja mida käsitatakse päritoluliikmesriigi õigusaktide kohaselt originaalidokumentide või kinnitatud koopiatena.

4. Komisjon võib rakendusaktidega kindlaks määrata selliste e-allkirjade ja e-templite vormingud, mida aktsepteeritakse siis, kui liikmesriik nõuab lõikes 2 osutatud avaliku sektori asutuse pakutava internetipõhise teenuse osutamiseks allkirjastatud või templiga dokumenti. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega.

7. jagu

Kvalifitseeritud e-andmevahetusteenus

Artikkel 35

E-andmevahetusteenuse õiguslik toime

1. E-andmevahetusteenust kasutades saadetud või kättesaadud andmed on kohtumenetlustes tõenduskõlblikud, kui on vaja tõendada andmete terviklust ning kuupäeva ja ajahetke, millal andmed saadeti või millal asjaomane adressaat need kätte sai.

2. Kvalifitseeritud e-andmevahetusteenust kasutades saadetud või kättesaadud andmetel on õiguslik eeldus andmete terviklusele ning kvalifitseeritud e-andmevahetusteenuse süsteemis osutatud andmete saatmise või kättesaamise kuupäeva ja ajahetke täpsusele.

3. Komisjonile antakse volitused võtta artikli 38 kohaselt vastu delegeeritud õigusakte, milles käsitletakse selliste e-andmevahetusteenuse kaudu andmete saatmiseks ja kättesaamiseks rakendatavate mehhanismide tehnilisi kirjeldusi, mida kasutatakse e-andmevahetusteenuste vahelise koostalitlusvõime edendamiseks.

Artikkel 36

Nõuded kvalifitseeritud e-andmevahetusteenustele

1. Kvalifitseeritud e-andmevahetusteenused peavad vastama järgmistele nõuetele:

(a) neid peab osutama üks või mitu kvalifitseeritud usaldusteenuse osutajat;

(b) need peavad võimaldama saatja ja vajaduse korral adressaadi üheselt mõistetavat identimist;

(c) andmete saatmine ja kättesaamine peavad olema kaitstud kvalifitseeritud usaldusteenuse osutaja pakutava täiustatud e-allkirja või täiustatud e-templiga viisil, mis välistab andmete tuvastamatu muutmise võimaluse;

(d) mis tahes muudatusi andmete saatmiseks või kättesaamiseks vajalikes andmetes tuleb andmete saatjale ja adressaadile selgelt näidata;

(e) andmete saatmise, kättesaamise ja mis tahes muudatuste kuupäeva tuleb näidata kvalifitseeritud e-ajatempliga;

(f) kui andmeid saadetakse kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel, kohaldatakse punktides a–e osutatud nõudeid kõikide kvalifitseeritud usaldusteenuse osutajate suhtes.

2. Komisjon võib rakendusaktidega kehtestada andmete saatmise ja kättesaamise protsesse käsitlevate standardite viitenumbrid. Kui andmete saatmise ja kättesaamise protsess vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

8. jagu

Veebisaidi autentimine

Artikkel 37

Nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele

1. Veebisaidi autentimise kvalifitseeritud sertifikaadid peavad vastama IV lisas sätestatud nõuetele.

2. Veebisaidi autentimise kvalifitseeritud sertifikaate tunnustatakse ja aktsepteeritakse kõikides liikmesriikides.

3. Komisjonile antakse volitused võtta vastavalt artiklile 38 vastu delegeeritud õigusakte IV lisas sätestatud nõuete edasise täpsustamise kohta.

4. Komisjon võib rakendusaktidega kehtestada veebisaidi autentimise kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui veebisaidi autentimise kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see IV lisas sätestatud nõuetele vastavaks. Rakendusaktid võetakse vastu kooskõlas artikli 39 lõikes 2 osutatud kontrollimenetlusega. Komisjon avaldab kõnealused aktid *Euroopa Liidu Teatajas*.

IV PEATÜKK

DELEGEERITUD ÕIGUSAKTID

Artikkel 38

Delegeeritud volituste rakendamine

1. Komisjonile antakse käesolevas artiklis sätestatud tingimustel õigus võtta vastu delegeeritud õigusakte.

2. Volitused võtta vastu artikli 8 lõikes 3, artikli 13 lõikes 5, artikli 15 lõikes 5, artikli 16 lõikes 5, artikli 18 lõikes 5, artikli 20 lõikes 6, artikli 21 lõikes 4, artikli 23 lõikes 3, artikli 25 lõikes 2, artikli 27 lõikes 2, artikli 28 lõikes 6, artikli 29 lõikes 4, artikli 30 lõikes 2, artiklis 31, artikli 35 lõikes 3 ja artikli 37 lõikes 3 osutatud delegeeritud õigusakte antakse komisjonile kindlaksmääramata ajaks alates käesoleva määruse jõustumisest.

3. Euroopa Parlament või nõukogu võivad artikli 8 lõikes 3, artikli 13 lõikes 5, artikli 15 lõikes 5, artikli 16 lõikes 5, artikli 18 lõikes 5, artikli 20 lõikes 6, artikli 21 lõikes 4, artikli 23 lõikes 3, artikli 25 lõikes 2, artikli 27 lõikes 2, artikli 28 lõikes 6, artikli 29 lõikes 4, artikli 30 lõikes 2, artiklis 31, artikli 35 lõikes 3 ja artikli 37 lõikes 3 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. Otsus ei mõjuta juba kehtivate delegeeritud õigusaktide kehtivust.

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

5. Delegeeritud õigusakt, mis on vastu võetud kooskõlas artikli 8 lõikega 3, artikli 13 lõikega 5, artikli 15 lõikega 5, artikli 16 lõikega 5, artikli 18 lõikega 5, artikli 20 lõikega 6, artikli 21 lõikega 4, artikli 23 lõikega 3, artikli 25 lõikega 2, artikli 27 lõikega 2, artikli 28 lõikega 6, artikli 29 lõikega 4, artikli 30 lõikega 2, artikliga 31, artikli 35 lõikega 3 ja artikli 37 lõikega 3, jõustub ainult juhul, kui Euroopa Parlament ega nõukogu ei ole esitanud vastuväiteid kahe kuu jooksul pärast kõnealusest õigusaktist teatamist Euroopa Parlamendile ja nõukogule või kui Euroopa Parlament ja nõukogu on mõlemad enne nimetatud ajavahemiku lõppemist komisjonile teatanud, et nad ei kavatse vastuväiteid esitada. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

V PEATÜKK

RAKENDUSAKTID

Artikkel 39

Komiteemenetlus

1. Komisjoni abistab komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

VI PEATÜKK

LÕPPSÄTTED

Artikkel 40

Aruandlus

Komisjon annab Euroopa Parlamendile ja nõukogule aru käesoleva määruse kohaldamise kohta. Esimene aruanne esitatakse hiljemalt neli aastat pärast käesoleva määruse jõustumist. Järgmised aruanded esitatakse iga nelja aasta järel.

Artikkel 41

Kehtetuks tunnistamine

1. Direktiiv 1999/93/EÜ tunnistatakse kehtetuks.

2. Viiteid kehtetukstunnistatud direktiivile käsitatakse viidetena käesolevale määrusele.

3. Selliseid turvalisi allkirja andmise vahendeid, mille vastavus on direktiivi 1999/93/EÜ artikli 3 lõike 4 kohaselt kindlaks määratud, käsitatakse käesoleva määruse kohaselt kvalifitseeritud e-allkirja moodustamise vahenditena.

4. Direktiivi 1999/93/EÜ alusel väljastatud kvalifitseeritud sertifikaate käsitatakse käesoleva määruse kohaselt e-allkirja kvalifitseeritud sertifikaatidena kuni nende kehtivuse lõpuni, kuid mitte kauem kui viis aastat alates käesoleva määruse jõustumisest.

Artikkel 42

Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

Nõuded e-allkirja kvalifitseeritud sertifikaatidele

E-allkirja kvalifitseeritud sertifikaadid peavad sisaldama järgmist:

(a) vähemalt automaatseks töötlemiseks sobivas vormingus märge selle kohta, et sertifikaat on väljastatud e-allkirja kvalifitseeritud sertifikaadina;

(b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus kõnealune teenuseosutaja asub, ning

– kui tegemist on juriidilise isikuga: nimi ja registrinumber, nagu need on esitatud ametlikes dokumentides,

– kui tegemist on füüsilise isikuga: isiku nimi;

(c) allakirjutajat, kellele sertifikaat väljastatakse, üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt allakirjutaja nime või varjunime, mille puhul märgitakse, et see on varjunimi;

(d) e-allkirja valideerimisandmed, mis vastavad e-allkirja moodustamiseks vajalikele andmetele;

(e) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

(f) kvalifitseeritud usaldusteenuse osutajale omistatud ainulaadne sertifikaadi tunnuskood;

(g) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

(h) koht, kus punktis g osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

(i) nende sertifikaadi kehtivusega seotud teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust;

(j) kui e-allkirja valideerimisandmetega seotud e-allkirja moodustamiseks vajalikud andmed asuvad kvalifitseeritud e-allkirja moodustamise vahendis, siis vähemalt automaatseks töötlemiseks sobivas vormingus asjakohane viide kõnealusele kohale.

II LISA

Nõuded kvalifitseeritud e-allkirja moodustamise vahenditele

1. Kvalifitseeritud e-allkirja moodustamise vahendid tagavad asjakohaste tehnikavõtete ja menetluste abil vähemalt selle, et:

(a) on tagatud selliste e-allkirja moodustamiseks vajalike andmete salajasus, mida kasutatakse e-allkirja loomiseks;

(b) e-allkirja moodustamiseks vajalikud andmed, mida kasutatakse e-allkirja loomiseks, võivad esineda ainult ühe korra;

(c) on piisavalt kindel, et e-allkirja moodustamiseks vajalikke andmeid, mida kasutatakse e-allkirja loomiseks, ei saa tuletada ja e-allkirja ei saa praegu kasutatava tehnoloogia abil võltsida;

(d) e-allkirja moodustamiseks vajalikke andmeid, mida kasutatakse e-allkirja loomiseks, saab õiguspärane allakirjutaja piisavalt kaitsta, et teised isikud ei saaks neid kasutada.

2. Kvalifitseeritud e-allkirja moodustamise vahendid ei tohi muuta allkirjastatavaid andmeid ega takistada selliste andmete esitamist allakirjutajale enne allkirjastamist.

3. E-allkirja moodustamiseks vajalikke andmeid loob või haldab allakirjutaja nimel kvalifitseeritud usaldusteenuse osutaja.

4. Kvalifitseeritud usaldusteenuse osutaja, kes haldab e-allkirja moodustamiseks vajalikke andmeid allakirjutaja nimel, võib dubleerida e-allkirja moodustamiseks vajalikud andmed varukoopiate omamiseks eeldusel, et on täidetud järgmised tingimused:

(a) dubleeritud andmekogumi turvatase peab olema sama mis algsel andmekogumil;

(b) dubleeritud andmekogumite arv ei ületa teenuse järjepidevuse tagamiseks vajalikku miinimumi.

III LISA

Nõuded e-templi kvalifitseeritud sertifikaatidele

E-templi kvalifitseeritud sertifikaadid peavad sisaldama järgmist:

(a) vähemalt automaatseks töötlemiseks sobivas vormingus märge selle kohta, et sertifikaat on väljastatud e-templi kvalifitseeritud sertifikaadina;

(b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus teenuseosutaja asub, ning

– kui tegemist on juriidilise isikuga: nimi ja registrinumber, nagu need on esitatud ametlikes dokumentides,

– kui tegemist on füüsilise isikuga: isiku nimi;

(c) juriidilist isikut, kellele sertifikaat väljastatakse, üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt nime ja registrinumbrit, nagu need on esitatud ametlikes dokumentides;

(d) e-templi valideerimisandmed, mis vastavad e-templi moodustamiseks vajalikele andmetele;

(e) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

(f) kvalifitseeritud usaldusteenuse osutajale omistatud ainulaadne sertifikaadi tunnuskood;

(g) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

(h) koht, kus punktis g osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

(i) nende sertifikaadi kehtivusega seotud teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust;

(j) kui e-templi valideerimisandmetega seotud e-templi moodustamiseks vajalikud andmed asuvad kvalifitseeritud e-templi moodustamise vahendis, siis vähemalt automaatseks töötlemiseks sobivas vormingus asjakohane viide kõnealusele kohale.

IV LISA

Nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele

Kvalifitseeritud sertifikaadid veebisaidi autentimiseks peavad sisaldama järgmist:

(a) vähemalt automaatseks töötlemiseks sobivas vormingus märge selle kohta, et sertifikaat on väljastatud kvalifitseeritud sertifikaadina veebisaidi autentimiseks;

(b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus teenuseosutaja asub, ning

– kui tegemist on juriidilise isikuga: nimi ja registrinumber, nagu need on esitatud ametlikes dokumentides,

– kui tegemist on füüsilise isikuga: isiku nimi;

(c) juriidilist isikut, kellele sertifikaat väljastatakse, üheselt mõistetavalt esindavad andmed, mis sisaldavad vähemalt nime ja registrinumbrit, nagu need on esitatud ametlikes dokumentides;

(d) selle juriidilise isiku aadressi elemendid, kellele sertifikaat väljastatakse, sealhulgas vähemalt linn ja liikmesriik, nagu need on esitatud ametlikes dokumentides;

(e) selle domeeni nimi / nende domeenide nimed, mida haldab juriidiline isik, kellele sertifikaat väljastatakse;

(f) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

(g) kvalifitseeritud usaldusteenuse osutajale omistatud ainulaadne sertifikaadi tunnuskood;

(h) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

(i) koht, kus punktis h osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

(j) nende sertifikaadi kehtivusega seotud teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust.

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

Käesolevas finantsselgituses esitatakse üksikasjalikult nõuded halduskuludele, mis on vajalikud kavandatava määruse *e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul* rakendamiseks.

Pärast seadusandlikku menetlust ja läbirääkimisi, mille käigus arutati kavandatava määruse vastuvõtmist Euroopa Parlamendi ja nõukogu poolt, vajab komisjon 12 täistööajaga töötajat, et koostada määrusega seotud delegeeritud ja rakendusaktid, tagada korralduslike ja tehniliste standardite kättesaadavus, käsitleda liikmesriikide edastatud teavet, eelkõige hallata usaldusnimekirjadega seotud teavet, kindlustada sidusrühmade, eelkõige kodanike ja VKEde teadlikkus e-identimise, e-autentimise, e-allkirja ja seotud usaldusteenuste (eIAS) kasutamise eelistest ning pidada läbirääkimisi kolmandate riikidega, et saavutada eIAS-teenuste üleilmne koostalitlusvõime.

1.1. Ettepaneku/algatuse nimetus

Komisjoni ettepanek määruse kohta, milles käsitletakse e-identimist ja e-tehingute jaoks vajalikke usaldusteenuseid siseturul

1.2. Asjaomased poliitikavaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise struktuurile[25]

09 INFOÜHISKOND

1.3. Ettepaneku/algatuse liik

☐ Ettepanek/algatus käsitleb **uut meedet**

☐ Ettepanek/algatus käsitleb **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[26]

☐ Ettepanek/algatus käsitleb **olemasoleva meetme pikendamist**

☑ Ettepanek/algatus käsitleb **ümbersuunatud meedet**

1.4. Eesmärgid

1.4.1. Komisjoni mitmeaastased strateegilised eesmärgid, mida ettepaneku/algatuse kaudu täidetakse

Ettepaneku üldeesmärgid on samad mis ELi üldistel poliitikasuundadel, nt ELi 2020. aasta strateegial, mille alla kõnealune ettepanek asetub. Selle eesmärk on tagada, et „EL muutub aruka, jätkusuutliku ja kaasava majandusega liiduks, kus on kõrge tööhõive, tootlikkuse ja sotsiaalse ühtekuuluvuse tase”.

[25] ABM – tegevuspõhine juhtimine; ABB – tegevuspõhine eelarvestamine.

[26] Vastavalt finantsmääruse artikli 49 lõike 6 punktile a või b.

1.4.2. Erieesmärgid ning asjaomased tegevusvaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise süsteemile

Suurendada üleeuroopaliste e-tehingute usaldusväärsust ja tagada e-identimise, e-autentimise, e-allkirja ja seotud usaldusteenuste piiriülene õiguslik tunnustamine ning andmekaitse kõrge tase ja kasutajate võimekustamine ühtsel turul (vt Euroopa digitaalarengu tegevuskava 3. ja 16. põhimeede).

Asjaomased tegevusalad vastavalt tegevuspõhise juhtimise ja eelarvestamise süsteemile

09 02 – Euroopa digitaalarengu tegevuskava õigusraamistik

1.4.3. Oodatavad tulemused ja mõju

Täpsustage, milline peaks olema ettepaneku/algatuse oodatav mõju abisaajatele/sihtrühmale.

Luua eIAS-teenustele selge õigusraamistik, mis suurendaks kasutajate mugavust, usaldust ja kindlustunnet digitaalmaailma suhtes.

1.4.4. Tulemus- ja mõjunäitajad

Täpsustage, milliste näitajate alusel hinnatakse ettepaneku/algatuse elluviimist.

1. Paljudes ELi liikmesriikides tegutsevate eIAS-teenuste osutajate olemasolu;

2. millisel määral muutuvad seadmed (nt kiipkaardilugejad) sektorite ja riikide vahel koostalitlusvõimeliseks;

3. eIAS-teenuste kasutamine kõikides elanikkonnarühmades;

4. millisel määral kasutavad lõppkasutajad eIAS-teenuseid riigisiseste ja rahvusvaheliste (piiriüleste) tehingute sooritamiseks;

5. millisel määral on eIAS-teenustega seotud õigusaktid eri liikmesriikides ühtlustatud;

6. komisjonile teatatud e-identimise süsteemid;

7. teenused, mis on avalikus sektoris kättesaadavad teavitatud e-identimise vahendite abil (nt e-valitsus, e-tervis, e-õigus, e-hange);

8. teenused, mis on erasektoris kättesaadavad teavitatud e-identimise vahendite abil (nt internetipangateenused, e-kaubandus, e-hasartmängud, veebisaitidele sisselogimine, turvalisemad internetipõhised teenused).

1.5. Ettepaneku/algatuse põhjendus

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused

Liikmesriikide erinevatest tõlgendustest tulenev e-allkirja direktiivi lahknev rakendamine riikide tasandil toob kaasa piiriüleseid koostalitlusprobleeme ning seoses sellega ELi killustunud tegevuskeskkonna ja siseturu moonutused. Sellele lisandub vähene usaldus elektrooniliste süsteemide vastu, mis ei lase Euroopa kodanikel saada digitaalkeskkonnas samaväärseid teenuseid kui füüsilises maailmas.

1.5.2. Euroopa Liidu meetme lisaväärtus

ELi tasandi meetmetel oleks üksikute liikmesriikide meetmetega võrreldes selgeid eeliseid. Kogemustest nähtub, et riigisisestest meetmetest mitte ainult ei piisa elektrooniliste tehingute piiriülesuse võimaldamiseks, vaid need on loonud lausa takistusi e-allkirja koostalitlusvõimele kogu ELis ning avaldavad praegu sarnast mõju e-identimisele, e-autentimisele ja seotud usaldusteenustele.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Ettepanek tugineb e-allkirja direktiiviga saadud kogemustele ja kõnealuse direktiivi killustatud ülevõtmisest ja rakendamisest põhjustatud probleemidele, mis on takistanud direktiivis sätestatud eesmärkide saavutamist.

1.5.4. Kooskõla ja võimalik koostoime muude asjaomaste meetmetega

E-allkirja direktiivile viidatakse paljudes muudes ELi õigusaktides, mis on koostatud selleks, et kõrvaldada teatavat tüüpi elektrooniliste tehingutega seotud koostalitlusvõime ning piiriülese tunnustamise ja aktsepteerimise probleemid. Kõnealused õigusaktid on näiteks teenuste direktiiv, riigihankedirektiivid, läbivaadatud käibemaksudirektiiv (e-arved) ja Euroopa kodanikualgatuse määrus. Lisaks nähakse kavandatava määrusega ette õigusraamistik, millest saavad kasu suuremahulised katseprojektid, mis on käivitatud ELi tasandil koostalitlusvõimeliste ja usaldusväärsete elektroonilise side vahendite toetamiseks (sealhulgas SPOCS, mis toetab teenuste direktiivi rakendamist; STORK, mis toetab koostalitlusvõimelise e-identimise väljatöötamist ja kasutamist; PEPPOL, mis toetab e-hangete koostalitlusvõimeliste lahenduste väljatöötamist ja kasutamist; epSOS, mis toetab e-tervise koostalitlusvõimeliste lahenduste väljatöötamist ja kasutamist; eCodex, mis toetab e-õiguse koostalitlusvõimeliste lahenduste väljatöötamist ja kasutamist).

1.6. Meetme kestus ja finantsmõju

☐ **Piiratud kestusega** ettepanek/algatus

– ☐ Ettepanek/algatus hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ Finantsmõju avaldub ajavahemikul AAAA – AAAA

☑ **Piiramatu kestusega** ettepanek/algatus

1.7. Ettenähtud eelarve täitmise viisid[27]

☑ **Otsene tsentraliseeritud eelarve täitmine** komisjoni poolt

☐ **Kaudne tsentraliseeritud eelarve täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ rakendusametitele

[27] Eelarve täitmise viise selgitatakse koos viidetega finantsmäärusele veebisaidil BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

– ☐ ühenduste asutatud asutustele[28]

– ☐ riigi avalik-õiguslikele asutustele või avalikke teenuseid osutavatele asutustele

– ☐ isikutele, kellele on delegeeritud konkreetsete meetmete rakendamine Euroopa Liidu lepingu V jaotise kohaselt ja kes on kindlaks määratud asjaomases alusaktis finantsmääruse artikli 49 tähenduses

☐ **Eelarve täitmine** koostöös liikmesriikidega

☐ **Detsentraliseeritud eelarve täitmine** koostöös kolmandate riikidega

☐ **Eelarve täitmine ühiselt** rahvusvaheliste organisatsioonidega (***täpsustage***)

Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused”.

Märkused:

[//]

[28] Määratletud finantsmääruse artiklis 185.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Täpsustage tingimused ja sagedus.

Esimene hindamine toimub nelja aasta möödumisel määruse jõustumisest. Määrus sisaldab selgesõnalist klauslit aruande kohta, millega komisjon annab määruse kohaldamise kohta aru Euroopa Parlamendile ja nõukogule. Järgmised aruanded esitatakse iga nelja aasta järel. Kohaldatakse komisjoni hindamismetoodikat. Kõnealused hindamised tehakse õigusaktide rakendamist käsitlevate sihtotstarbeliste uuringute, riikide ametiasutustele esitatavate küsimustike, ekspertide arutelude, õpikodade, Eurobaromeetri uuringute jne abil.

2.2. Haldus- ja kontrollisüsteemid

2.2.1. Tuvastatud ohud

Määruse ettepanekuga on kaasas sellele tehtud mõjuhinnang. Uue õigusaktiga nähakse ette piiriülese e-identimise vastastikune tunnustamine ja aktsepteerimine, täiustatakse olemasolevat e-allkirja raamistikku, tugevdatakse usaldusteenuse osutajate riigisisest järelevalvet ning antakse õiguslik mõju ja tunnustus seotud usaldusteenustele. Määrusega võetakse ühtlasi kasutusele delegeeritud ja rakendusaktid tehnoloogia arenguga seotud paindlikkuse tagamise mehhanismina.

2.2.2. Ettenähtud kontrollimeetod(id)

Komisjoni kohaldatavad olemasolevad kontrollimeetodid hõlmavad täiendavaid assigneeringuid.

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Täpsustage rakendatavad või kavandatud ennetus- ja kaitsemeetmed

Komisjoni kohaldatavad olemasolevad pettuse ärahoidmise meetmed hõlmavad täiendavaid assigneeringuid.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriikide ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr [Nimetus…...….]	Liigendatud/ liigendamata (29)	EFTA[30] riigid	Kandidaatriigid[31]	Kolmandad riigid	Rahaline osalus finantsmääruse artikli 18 lõike 1 punkti aa tähenduses
5	09. 01 01 01 Infoühiskonna ja meedia peadirektoraadis alaliselt töötava personaliga seotud kulud	Liigendamata	EI	EI	EI	EI
5	09. 01 02 01 Koosseisuvälised töötajad	Liigendamata	EI	EI	EI	EI

29 Liigendatud assigneeringud / liigendamata assigneeringud.
30 EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
31 Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

Mitmeaastase finantsraamistiku rubriik	**Nr**	[Rubriik 1 **Arukas ja kaasav majanduskasv** ……...……]

Infoühiskonna ja meedia peadirektoraat			Aasta **2014**	Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta 2018	**Aasta 2019**	**Aasta 2020**	**KOKKU**
• Tegevusassigneeringud										
Eelarverida nr – ei kohaldata	Kulukohustused	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksed	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Eelarverida nr – ei kohaldata	Kulukohustused	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksed	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Eelarverida nr		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Infoühiskonna ja meedia peadirektoraadi assigneeringud KOKKU	Kulukohustused	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksed	=2+2a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

[32] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised B.A read), otsene teadustegevus, kaudne teadustegevus.

Mitmeaastase finantsraamistiku rubriik	**5**	Halduskulud

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2014**	Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Aasta **2019**	Aasta **2020**	**KOKKU**
Infoühiskonna ja meedia peadirektoraat									
• Personalikulud		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Muud halduskulud									
Infoühiskonna ja meedia peadirektoraat KOKKU	Assigneeringud	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Mitmeaastase finantsraamistiku RUBRIIGI 5 assigneeringud KOKKU	(Kulukohustuste kogusumma = maksete kogusumma)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2014**	Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Aasta **2019**	Aasta **2020**	**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIKIDE 1– 5 assigneeringud KOKKU	Kulukohustused	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Maksed	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Hinnanguline mõju tegevusassigneeringutele

– ☑ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– ☐ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

3.2.3. Hinnanguline mõju haldusassigneeringutele

3.2.3.1. Ülevaade

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta **N 2014**	Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Aasta **2019**	Aasta **2020**	**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIK 5								
Personalikulud	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Muud halduskulud								
Mitmeaastase finantsraamistiku RUBRIIK 5 kokku	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Mitmeaastase finantsraamistiku RUBRIIGIST 5 välja jäävad kulud[33]								
Personalikulud								
Muud halduskulud								
Mitmeaastase finantsraamistiku RUBRIIGIST 5 välja jäävad kulud kokku								

KOKKU	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised B.A read), otsene teadustegevus, kaudne teadustegevus.

3.2.3.2. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist
– ☑ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

hinnanguline väärtus täisarvuna (või maksimaalselt ühe kohaga pärast koma)

	Aasta **2014**	Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Aasta **2019**	Aasta **2020**
• Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)							
09 01 01 01 (komisjoni peakorteris ja esindustes)	9	9	9	9	9	9	9
XX 01 01 02 (delegatsioonides)							
XX 01 05 01 (kaudne teadustegevus)							
10 01 05 01 (otsene teadustegevus)							
• Koosseisuväline personal (täistööajale taandatud töötajad)[34]							
09 01 02 01 (üldvahenditest rahastatavad lepingulised töötajad, renditööjõud ja riikide lähetatud eksperdid)	3	3	3	3	3	3	3
XX 01 02 02 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)							
XX 01 04 ***yy***[35] - peakorteris[36]							
XX 01 04 ***yy***[35] - delegatsioonides							
XX 01 05 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)							
10 01 05 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)							
Muud eelarveread (täpsustage)							
KOKKU	**12**	**12**	**12**	**12**	**12**	**12**	**12**

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate ümberpaigutamise teel peadirektoraadi siseselt. Vajaduse korral võidakse personali täiendada meedet haldavale peadirektoraadile iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	Selliste seadusandlike menetluste haldamine, mis on vajalikud selleks, et Euroopa Parlament ja nõukogu võtaksid vastu kavandatud määruse ja sellega seotud delegeeritud aktid / rakendusaktid.

[34] Lepingulised töötajad, renditööjõud, noored eksperdid delegatsioonides, kohalikud töötajad, riikide lähetatud eksperdid.

[35] Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised B.A read).

[36] Peamiselt struktuurifondid, Euroopa Maaelu Arengu Põllumajandusfond (EAFRD) ja Euroopa Kalandusfond (EKF).

	Prioriteetsed valdkonnad: 1. elektroonilisi usaldusteenuseid hõlmava uue õigusraamistiku kehtestamine; 2. elektrooniliste usaldusteenuste kasutuselevõtu soodustamine, suurendades VKEde ja kodanike teadlikkust nimetatud teenustega seotud võimalustest; 3. direktiiviga 1999/93/EÜ seotud järelmeetmed, sealhulgas rahvusvahelised aspektid; 4. suuremahuliste katseprojektide tõhustamine, et kiirendada uue seadusandliku raamistiku eesmärkide saavutamist.
Koosseisuvälised töötajad	Sama mis ülal.

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

– ☑ Ettepanek/algatus on kooskõlas kehtiva mitmeaastase finantsraamistikuga

– ☐ Ettepanekuga/algatusega kaasneb mitmeaastase finantsraamistiku asjakohase rubriigi ümberplaneerimine

Selgitage ümberplaneerimist, osutades asjaomastele rubriikidele, eelarveridadele ja summadele.

– ☐ Ettepanekuga/algatusega seoses on vajalik paindlikkusinstrumendi kohaldamine või mitmeaastase finantsraamistiku läbivaatamine[37]

Selgitage vajalikku toimingut, osutades asjaomastele rubriikidele, eelarveridadele ja summadele.

3.2.5. Kolmandate isikute rahaline osalus

– ☑ Ettepanek/algatus ei hõlma kolmandate isikute poolset kaasrahastamist

– ☐ Ettepanek/algatus hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

3.3. Hinnanguline mõju tuludele

– ☑ Ettepanekul/algatusel puudub finantsmõju tuludele.

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

- ☐ omavahenditele
- ☐ mitmesugustele tuludele

[37] Vt institutsioonidevahelise kokkuleppe punktid 19 ja 24.