EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 910/2014,

annettu 23 päivänä heinäkuuta 2014,

sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 114 artiklan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen, kun esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon ([1]),

noudattavat tavallista lainsäätämisjärjestystä ([2]),

sekä katsovat seuraavaa:

(1) Verkkoympäristöön kohdistuvan luottamuksen lujittaminen on talouden ja yhteiskunnan kehityksen kannalta olennaisen tärkeää. Luottamuksen puute, joka johtuu erityisesti koetusta oikeusvarmuuden puutteesta, saa aikaan sen, että kuluttajat, yritykset ja viranomaiset vierastavat sähköisten transaktioiden ja uusien palvelujen käyttöä.

(2) Tällä asetuksella pyritään lisäämään luottamusta sähköisiin transaktioihin sisämarkkinoilla tarjoamalla yhteinen perusta turvalliselle sähköiselle vuorovaikutukselle kansalaisten, yritysten ja viranomaisten välillä sekä parantamalla näin julkisten ja yksityisten verkkopalvelujen, sähköisen liiketoiminnan ja sähköisen kaupankäynnin toimivuutta unionissa.

(3) Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY ([3]) koski sähköisiä allekirjoituksia tarjoamatta kokonaisvaltaisia rajat ylittäviä ja eri alat kattavia puitteita turvallisia, luotettavia ja helppokäyttöisiä sähköisiä transaktioita varten. Tämä asetus parantaa ja laajentaa mainittuun direktiiviin liittyvää säännöstöä.

(4) Komission 26 päivänä elokuuta 2010 antamassa tiedonannossa ”Euroopan digitaalistrategia” digitaalimarkkinoiden hajanaisuus, yhteentoimivuuden puutteet ja verkkorikollisuuden lisääntyminen todettiin vakaviksi esteiksi digitaalitalouden hyvän kierteen syntymiselle. Kertomuksessaan ”Katsaus Euroopan unionin kansalaisuuteen vuonna 2010 – Unionin kansalaisoikeuksien esteiden poistaminen” komissio nosti edelleen esiin tarpeen ratkaista vaikeimmat ongelmat, jotka estävät unionin kansalaisia hyötymästä digitaalisista sisämarkkinoista ja rajat ylittävistä digitaalisista palveluista.

(5) Eurooppa-neuvosto kehotti 4 päivänä helmikuuta 2011 ja 23 päivänä lokakuuta 2011 antamissaan päätelmissä komissiota luomaan digitaaliset sisämarkkinat vuoteen 2015 mennessä, pyrkimään nopeaan edistymiseen digitaalitalouden keskeisillä osa-alueilla ja edistämään digitaalisten sisämarkkinoiden täyttä yhdentymistä helpottamalla verkkopalvelujen käyttöä yli rajojen kiinnittäen erityistä huomiota turvallisen sähköisen tunnistamisen ja todentamisen helpottamiseen.

([1]) EUVL C 351, 15.11.2012, s. 73.
([2]) Euroopan parlamentin kanta, vahvistettu 3. huhtikuuta 2014 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 23. heinäkuuta 2014.
([3]) Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista (EYVL L 13, 19.1.2000, s. 12).

(6) Neuvosto kehotti 27 päivänä toukokuuta 2011 antamissaan päätelmissä komissiota edistämään digitaalisten sisämarkkinoiden kehittymistä luomalla tarvittavat edellytykset tärkeimpien rajat ylittävien mahdollistavien tekijöiden, kuten sähköisen tunnistamisen, sähköisten asiakirjojen, sähköisten allekirjoitusten ja sähköisten jakelupalvelujen, vastavuoroista tunnustamista varten sekä yhteentoimivia sähköisen hallinnon palveluja varten koko Euroopan unionissa.

(7) Euroopan parlamentti korosti sisämarkkinoiden täydentämisestä sähköistä kaupankäyntiä ajatellen 21 päivänä syyskuuta 2010 antamassaan päätöslauselmassa ([1]) turvallisuuden merkitystä sähköisten palvelujen, erityisesti sähköisten allekirjoitusten, yhteydessä sekä sitä, että on tarpeen luoda yleiseurooppalaisella tasolla julkisen avaimen infrastruktuuri, ja kehotti komissiota perustamaan validointiviranomaisten eurooppalaisen portaalin, jolla varmistetaan sähköisten allekirjoitusten rajat ylittävä yhteentoimivuus ja parannetaan internetissä suoritettujen maksujen turvallisuutta.

(8) Euroopan parlamentin ja neuvoston direktiivissä 2006/123/EY ([2]) jäsenvaltioita edellytetään perustamaan ”keskitettyjä asiointipisteitä” sen varmistamiseksi, että kaikki palvelutoiminnan aloittamiseen ja harjoittamiseen liittyvät menettelyt ja muodollisuudet voidaan hoitaa vaivatta etäältä ja sähköisesti asianomaisen keskitetyn asiointipisteen kautta ja asianomaisten toimivaltaisten viranomaisten kanssa. Monet keskitettyjen asiointipisteiden kautta käytettävissä olevat verkkopalvelut edellyttävät sähköistä tunnistamista, todentamista ja allekirjoittamista.

(9) Useimmissa tapauksissa kansalaiset eivät voi käyttää sähköistä tunnistettaan todentaakseen itsensä toisessa jäsenvaltiossa, koska niiden kotimaan kansallisia sähköisen tunnistamisen järjestelmiä ei tunnusteta muissa jäsenvaltioissa. Tämän sähköisen esteen vuoksi palveluntarjoajat eivät voi hyödyntää kaikkia sisämarkkinoiden suomia etuja. Vastavuoroisesti tunnustetut sähköisen tunnistamisen menetelmät helpottavat lukuisten palvelujen rajat ylittävää tarjoamista sisämarkkinoilla ja antavat yrityksille mahdollisuuden toimia rajojen yli ilman, että ne kohtaavat monia esteitä viranomaisasioinnissa.

(10) Euroopan parlamentin ja neuvoston direktiivillä 2011/24/EU ([3]) perustetaan sähköisestä terveydenhuollosta vastaavien kansallisten viranomaisten verkosto. Rajat ylittävän terveydenhuollon turvallisuuden ja jatkuvuuden parantamiseksi verkoston on määrä tuottaa ohjeistoja rajat ylittävästä pääsystä sähköisiin terveystietoihin ja -palveluihin muun muassa tukemalla ”yhteisiä tunnistamismenetelmiä ja alkuperäisyyden toteamismenetelmiä, jotta voidaan helpottaa tietojen siirrettävyyttä rajatylittävässä terveydenhoidossa”. Sähköisen tunnistamisen ja todentamisen vastavuoroinen tunnustaminen on olennaisen tärkeää tuotaessa rajat ylittävää terveydenhuoltoa Euroopan kansalaisten ulottuville. Kun ihmiset matkustavat ulkomaille saamaan hoitoa, heidän potilastietojensa on oltava saatavilla hoitomaassa. Tämä edellyttää vankkoja, turvallisia ja luotettuja sähköisen tunnistamisen puitteita.

(11) Tätä asetusta sovellettaessa olisi noudatettava täysin henkilötietojen suojaan liittyviä periaatteita, joista säädetään Euroopan parlamentin ja neuvoston direktiivissä 95/46/EY ([4]). Kun otetaan huomioon tällä asetuksella vahvistettu vastavuoroisen tunnustamisen periaate, verkkopalveluun liittyvän todentamisen olisi tältä osin koskettava ainoastaan niiden tunnistetietojen käsittelyä, jotka ovat riittäviä ja asiaankuuluvia eivätkä aiheettoman runsaita kyseisen verkkopalvelun käytön sallimiseksi. Lisäksi luottamuspalvelun tarjoajien ja valvontaelinten olisi noudatettava luottamuksellisuutta ja käsittelyn turvallisuutta koskevia direktiivin 95/46/EY vaatimuksia.

(12) Yksi tämän asetuksen tavoitteista on poistaa nykyiset esteet, jotka haittaavat jäsenvaltioiden ainakin julkisissa palveluissa todentamiseen käyttämien sähköisen tunnistamisen menetelmien käyttöä yli rajojen. Tällä asetuksella ei pyritä puuttumaan jäsenvaltioissa käytettäviin sähköisen identiteetin hallintajärjestelmiin ja niihin liittyviin infrastruktuureihin. Tämän asetuksen tarkoituksena on varmistaa, että jäsenvaltioiden tarjoamia rajat ylittäviä verkkopalveluja varten on käytössä turvallisia sähköisen tunnistamisen ja todentamisen menetelmiä.

([1]) EUVL C 50 E, 21.2.2012, s. 1.
([2]) Euroopan parlamentin ja neuvoston direktiivi 2006/123/EY, annettu 12 päivänä joulukuuta 2006, palveluista sisämarkkinoilla (EUVL L 376, 27.12.2006, s. 36).
([3]) Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU, annettu 9 päivänä maaliskuuta 2011, potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa (EUVL L 88, 4.4.2011, s. 45).
([4]) Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, 23.11.1995, s. 31).

(13) Jäsenvaltioiden olisi edelleen voitava vapaasti käyttää ja ottaa käyttöön verkkopalvelujen edellyttämiä sähköisen tunnistamisen menetelmiä. Niiden olisi myös voitava päättää, ottavatko ne yksityisen sektorin mukaan näiden menetelmien tarjoamiseen. Jäsenvaltioita ei olisi velvoitettava ilmoittamaan sähköisen tunnistamisen järjestelmiään komissiolle. Jäsenvaltiot voivat päättää, ilmoittavatko ne komissiolle kaikki kansallisella tasolla käytetyt sähköisen tunnistamisen järjestelmät, joita tarvitaan ainakin julkisten verkkopalvelujen tai tiettyjen palvelujen käyttöön, vai ilmoittavatko ne vain jotkin tällaiset järjestelmät tai ei mitään niistä.

(14) Tässä asetuksessa on säädettävä joitakin ehtoja sille, mitkä sähköisen tunnistamisen menetelmät on tunnustettava ja miten sähköisen tunnistamisen järjestelmät olisi ilmoitettava. Näiden ehtojen avulla jäsenvaltioiden olisi helpompi rakentaa tarvittavaa luottamusta toistensa sähköisen tunnistamisen järjestelmiin ja tunnustaa vastavuoroisesti sähköisen tunnistamisen menetelmät, jotka kuuluvat ilmoitettujen järjestelmien piiriin. Vastavuoroisen tunnustamisen periaatetta olisi sovellettava, jos ilmoittavan jäsenvaltion sähköisen tunnistamisen järjestelmä täyttää ilmoittamiselle asetetut ehdot ja ilmoitus on julkaistu *Euroopan unionin virallisessa lehdessä*. Vastavuoroisen tunnustamisen periaatteen tulisi kuitenkin koskea ainoastaan verkkopalveluun liittyvää todentamista. Näihin verkkopalveluihin pääsyn ja niiden lopputarjonnan käyttäjälle olisi kuitenkin oltava tiiviisti sidoksissa kansallisessa lainsäädännössä säädettyihin ehtoihin, jotka koskevat oikeutta saada hyödyntää kyseisiä palveluja.

(15) Velvoitteen tunnustaa sähköisen tunnistamisen menetelmät olisi koskettava ainoastaan niitä menetelmiä, joiden tunnistamisen varmuustaso on yhtä korkea tai korkeampi kuin kyseiseltä verkkopalvelulta edellytettävä taso. Lisäksi tätä velvoitetta olisi sovellettava vain, kun kyseessä oleva julkisen sektorin elin käyttää varmuustasoa ”korotettu” tai ”korkea” kyseisen verkkopalvelun käytön osalta. Jäsenvaltioiden olisi unionin oikeuden mukaisesti voitava vapaasti tunnustaa sähköisen tunnistamisen menetelmät, joiden tunnistamisen varmuustasot ovat matalammat.

(16) Varmuustasojen olisi luonnehdittava sähköisen tunnistamisen menetelmän luotettavuuden astetta henkilön henkilöllisyyden toteamisessa ja siten tarjota varmuus siitä, että henkilö, joka väittää omaavansa tietyn henkilöllisyyden, on tosiasiassa henkilö, jolle kyseinen henkilöllisyys on osoitettu. Varmuustaso riippuu kyseisen sähköisen tunnistamisen menetelmän tarjoamasta luottamustasosta henkilön väitetyn tai esitetyn henkilöllisyyden suhteen ottaen huomioon toteutetut prosessit (esimerkiksi henkilöllisyyden todistaminen ja varmentaminen sekä todentaminen), hallinnolliset toimet (esimerkiksi sähköisen tunnistamisen menetelmän myöntävä toimija ja menettely tällaisen menetelmän myöntämiseksi) ja tekniset tarkastukset. Unionin rahoittamien suuren mittakaavan pilottihankkeiden, standardisoinnin ja kansainvälisen toiminnan seurauksena on laadittu lukuisia teknisiä eritelmiä ja varmuustasojen kuvauksia. Erityisesti suuren mittakaavan pilottihanke STORK ja ISO 29115 viittaavat muun muassa tasoihin 2, 3 ja 4, jotka olisi otettava mahdollisimman tarkkaan huomioon vahvistettaessa teknisten vaatimusten, standardien ja menettelyjen vähimmäistaso tässä asetuksessa tarkoitetuille matalalle, korotetulle ja korkealle varmuustasolle, ja samalla on huolehdittava tämän asetuksen johdonmukaisesta soveltamisesta erityisesti hyväksyttyjen varmenteiden myöntämiseen liittyvän henkilöllisyyden todistamisen edellyttämän korkean varmuustason osalta. Vahvistettujen vaatimusten olisi oltava teknologianeutraaleja. Tarvittavat turvallisuusvaatimukset olisi oltava mahdollista saavuttaa erilaisilla teknologioilla.

(17) Jäsenvaltioiden olisi kannustettava yksityistä sektoria käyttämään vapaaehtoisesti ilmoitetun järjestelmän piiriin kuuluvia sähköisen tunnistamisen menetelmiä tunnistamistarkoituksiin, kun se on tarpeen verkkopalveluissa tai sähköisissä transaktioissa. Tällaisten sähköisen tunnistamisen menetelmien käyttömahdollisuuden ansiosta yksityinen sektori voisi luottaa monissa jäsenvaltioissa ainakin julkisissa palveluissa jo laajasti käytettyihin sähköisen tunnistamisen ja todentamisen tapoihin, jolloin yritysten ja kansalaisten olisi helpompi käyttää niiden verkkopalveluja rajojen yli. Jotta yksityisen sektorin olisi helpompi käyttää tällaisia sähköisen tunnistamisen menetelmiä rajojen yli, minkä tahansa jäsenvaltion tarjoaman todentamismahdollisuuden olisi oltava kyseisen jäsenvaltion alueen ulkopuolelle sijoittautuneiden yksityisen sektorin luottavien osapuolten käytettävissä samoin edellytyksin, joita sovelletaan kyseisen jäsenvaltion alueelle sijoittautuneisiin yksityisen sektorin luottaviin osapuoliin. Näin ollen ilmoittava jäsenvaltio voi määritellä yksityisen sektorin luottavien osapuolten osalta todentamismenetelmän käyttöehdot. Tällaisiin käyttöehtoihin voi sisältyä tieto siitä, onko ilmoitettuun järjestelmään liittyvä todentamismenetelmä parhaillaan yksityisen sektorin luottavien osapuolten käytettävissä.

(18) Tässä asetuksessa olisi säädettävä ilmoittavan jäsenvaltion, sähköisen tunnistamisen menetelmän myöntävän osapuolen ja todentamismenettelyä operoivan osapuolen vastuusta siinä tapauksessa, etteivät ne noudata tässä asetuksessa säädettyjä asianmukaisia velvoitteita. Tätä asetusta olisi kuitenkin sovellettava kansallisten vastuusääntöjen mukaisesti. Se ei näin ollen vaikuta näihin kansallisiin sääntöihin, jotka koskevat esimerkiksi vahinkojen määrittelyä, tai asiaan liittyviin sovellettaviin menettelysääntöihin, todistustaakka mukaan lukien.

(19) Sähköisen tunnistamisen järjestelmien tietoturva on olennainen seikka sähköisen tunnistamisen menetelmien luotettavan rajat ylittävän vastavuoroisen tunnustamisen kannalta. Tässä yhteydessä jäsenvaltioiden olisi tehtävä yhteistyötä sähköisen tunnistamisen järjestelmien tietoturvan ja yhteentoimivuuden osalta unionin tasolla. Kun sähköisen tunnistamisen järjestelmät edellyttävät, että luottavat osapuolet käyttävät erityisiä laitteistoja tai ohjelmistoja kansallisella tasolla, rajat ylittävä yhteentoimivuus taas edellyttää, että nämä jäsenvaltiot eivät määrää tällaisia vaatimuksia ja niihin liittyviä kustannuksia niiden alueen ulkopuolelle sijoittautuneille luottaville osapuolille. Tässä tapauksessa olisi käsiteltävä ja kehitettävä asianmukaisia ratkaisuja yhteentoimivuusjärjestelmän puitteissa. Kansallisten sähköisen tunnistamisen menetelmien ominaispiirteistä johtuvilta teknisiltä vaatimuksilta, jotka todennäköisesti vaikuttavat tällaisten sähköisten menetelmien (esimerkiksi älykorttien) haltijoihin, ei silti voida välttyä.

(20) Jäsenvaltioiden yhteistyön olisi edistettävä ilmoitettujen sähköisen tunnistamisen järjestelmien teknistä yhteentoimivuutta, ja siinä olisi pyrittävä vaalimaan luottamuksen ja tietoturvan korkeaa tasoa, joka on oikeassa suhteessa riskin suuruuteen. Tällaisessa yhteistyössä olisi apua tietojenvaihdosta ja parhaiden käytäntöjen jakamisesta, joilla pyritään järjestelmien vastavuoroiseen tunnustamiseen.

(21) Tällä asetuksella olisi luotava myös yleiset oikeudelliset puitteet luottamuspalvelujen käytölle. Sillä ei kuitenkaan pitäisi asettaa yleistä velvollisuutta käyttää niitä tai ottaa käyttöön yhteyspistettä kaikkia olemassa olevia luottamuspalveluja varten. Sen ei varsinkaan pitäisi kattaa sellaisten palvelujen tarjoamista, joita tarjotaan yksinomaan määrätyn osallistujajoukon välisissä suljetuissa järjestelmissä ja joilla ei ole vaikutuksia kolmansiin osapuoliin. Esimerkiksi yrityksissä tai julkishallinnossa sisäisten menettelyjen hallinnoimiseksi perustettuihin järjestelmiin, joissa käytetään luottamuspalveluja, ei olisi sovellettava tämän asetuksen vaatimuksia. Ainoastaan yleisölle tarjottujen luottamuspalvelujen, joilla on vaikutuksia kolmansiin osapuoliin, olisi oltava asetuksessa säädettyjen vaatimusten mukaisia. Tämän asetuksen ei myöskään pitäisi kattaa näkökohtia, jotka liittyvät sellaisten sopimusten tai muiden oikeudellisten velvoitteiden vahvistamiseen ja pätevyyteen, joihin sisältyy kansallisessa tai unionin oikeudessa säädettyjä muotovaatimuksia. Lisäksi sen ei pitäisi vaikuttaa kansallisiin muotovaatimuksiin, jotka koskevat julkisia rekistereitä, erityisesti kauppa- ja kiinteistörekistereitä.

(22) Luottamuspalvelujen yleisen rajat ylittävän käytön edistämiseksi niitä olisi voitava käyttää todisteena oikeudellisissa menettelyissä kaikissa jäsenvaltioissa. Luottamuspalvelujen oikeusvaikutukset määritellään kansallisessa laissa, jollei tässä asetuksessa toisin säädetä.

(23) Siltä osin kuin tässä asetuksessa luodaan velvoite tunnustaa luottamuspalvelu, tällainen luottamuspalvelu voidaan olla tunnustamatta vain, jos se, jolle velvoite on osoitettu, ei pysty lukemaan tai tarkastamaan sitä teknisistä syistä, jotka eivät ole sen välittömässä hallinnassa. Tämä velvoite ei saisi kuitenkaan sellaisenaan edellyttää, että julkinen elin hankkii laitteistot ja ohjelmistot, jotka ovat tarpeen kaikkien olemassa olevien luottamuspalvelujen teknistä luettavuutta varten.

(24) Jäsenvaltiot voivat unionin oikeuden mukaisesti pitää voimassa tai ottaa käyttöön luottamuspalveluja koskevia kansallisia säännöksiä siltä osin kuin tällaisia palveluja ei ole täysin yhdenmukaistettu tällä asetuksella. Tämän asetuksen mukaisten luottamuspalveluiden olisi kuitenkin liikuttava vapaasti sisämarkkinoilla.

(25) Jäsenvaltioiden olisi edelleen voitava vapaasti määritellä muun tyyppisiä luottamuspalveluja niiden lisäksi, jotka sisältyvät tässä asetuksessa säädettyyn suljettuun luottamuspalvelujen luetteloon, tunnustettaviksi kansallisella tasolla hyväksytyiksi luottamuspalveluiksi.

(26) Teknologian muutosnopeuden vuoksi tässä asetuksessa olisi omaksuttava lähestymistapa, joka on avoin innovoinnille.

(27) Tämän asetuksen olisi oltava teknologianeutraali. Sen oikeusvaikutusten olisi oltava saavutettavissa millä tahansa teknisellä menetelmällä, kunhan asetuksen vaatimukset täyttyvät.

(28) Erityisesti pienten ja keskisuurten yritysten sekä kuluttajien sisämarkkinoita kohtaan tunteman luottamuksen vahvistamiseksi ja luottamuspalvelujen ja -tuotteiden käytön lisäämiseksi olisi otettava käyttöön hyväksyttyjen luottamuspalvelujen ja hyväksytyn luottamuspalvelun tarjoajan käsitteet, joiden avulla voitaisiin määritellä vaatimukset ja velvoitteet, joilla voidaan varmistaa minkä tahansa käytettävän tai tarjottavan hyväksytyn luottamuspalvelun tai -tuotteen korkea tietoturvataso.

(29) Neuvoston päätöksellä 2010/48/EY ([1]) hyväksyttyyn vammaisten henkilöiden oikeuksia koskevaan Yhdistyneiden kansakuntien yleissopimukseen ja erityisesti kyseisen yleissopimuksen 9 artiklaan sisältyvien velvoitteiden mukaisesti vammaisten olisi voitava käyttää luottamuspalveluja ja niiden tarjoamiseksi tarvittavia loppukäyttäjätuotteita tasavertaisesti muiden kuluttajien kanssa. Näin ollen tarjotut luottamuspalvelut ja niiden tarjoamisessa käytetyt loppukäyttäjätuotteet olisi tehtävä vammaisille esteettömiksi aina kun se on toteutettavissa. Toteutettavuuden arvioinnissa olisi otettava huomioon muun muassa tekniset ja taloudelliset näkökohdat.

(30) Jäsenvaltioiden olisi nimettävä valvontaelin tai valvontaelimiä suorittamaan tämän asetuksen mukaisia valvontatehtäviä. Jäsenvaltioiden olisi myös voitava päättää keskinäisellä sopimuksella toisen jäsenvaltion kanssa valvontaelimen nimeämisestä kyseisen toisen jäsenvaltion alueelle.

(31) Valvontaelinten olisi tehtävä yhteistyötä tietosuojaviranomaisten kanssa esimerkiksi tiedottamalla niille hyväksyttyjä luottamuspalvelun tarjoajia koskevien tarkastusten tuloksista, jos vaikuttaa siltä, että henkilötietojen suojaa koskevia sääntöjä on rikottu. Tietojen antamisen olisi koskettava erityisesti tietoturvapoikkeamia ja henkilötietojen suojan loukkauksia.

(32) Kaikkien luottamuspalvelun tarjoajien olisi noudatettava niiden toimintaan liittyvien riskien mukaisia hyviä tietoturvakäytänteitä, jotta käyttäjien luottamus sisämarkkinoita kohtaan lujittuisi.

(33) Säännökset salanimien käytöstä varmenteissa eivät saisi estää jäsenvaltioita edellyttämästä henkilöiden tunnistamista unionin tai kansallisen oikeuden mukaisesti.

(34) Kaikkien jäsenvaltioiden olisi noudatettava yhteisiä keskeisiä valvontavaatimuksia, jotta hyväksytyille luottamuspalveluille voitaisiin taata vastaava tietoturvataso. Jotta näiden vaatimusten johdonmukainen soveltaminen koko unionissa olisi helpompaa, jäsenvaltioiden olisi otettava käyttöön keskenään vertailukelpoiset menettelyt ja vaihdettava tietoja valvontatoiminnastaan ja alan parhaista käytännöistä.

(35) Kaikkiin luottamuspalvelun tarjoajiin olisi sovellettava tämän asetuksen vaatimuksia, erityisesti tietoturvaa ja vastuuta koskevia vaatimuksia, niiden toimien ja palvelujen asianmukaisen huolellisuuden, avoimuuden ja vastuuvelvollisuuden varmistamiseksi. Kyseisten vaatimusten osalta on kuitenkin asianmukaista tehdä ero hyväksyttyjen ja ei-hyväksyttyjen luottamuspalvelun tarjoajien välillä, luottamuspalvelun tarjoajien tarjoamien palvelujen tyyppi huomioon ottaen.

(36) Kaikkia luottamuspalvelun tarjoajia koskevan valvontajärjestelmän perustamisessa olisi varmistettava tasapuoliset edellytykset niiden toimien ja palvelujen tietoturvalle ja vastuuvelvollisuudelle, jolloin edistetään käyttäjien suojelua ja sisämarkkinoiden toimintaa. Ei-hyväksyttyihin luottamuspalvelun tarjoajiin olisi sovellettava joustavia ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toimien luonteella. Valvontaelimellä ei siis pitäisi olla yleistä velvoitetta valvoa ei-hyväksyttyjä palveluntarjoajia. Valvontaelimen pitäisi toteuttaa toimia vain silloin, kun se saa tietää (esimerkiksi ei-hyväksytyn luottamuspalvelun tarjoajan itsensä tai muun valvontaelimen taholta, käyttäjän tai liikekumppanin ilmoituksen perusteella tai oman tutkintansa perusteella), että ei-hyväksytty luottamuspalvelun tarjoaja ei täytä tämän asetuksen vaatimuksia.

([1]) Neuvoston päätös 2010/48/EY, tehty 26 päivänä marraskuuta 2009, vammaisten henkilöiden oikeuksia koskevan Yhdistyneiden Kansakuntien yleissopimuksen tekemisestä Euroopan yhteisön puolesta (EUVL L 23, 27.1.2010, s. 35).

(37) Tässä asetuksessa olisi säädettävä kaikkien luottamuspalvelun tarjoajien vastuusta. Siinä otetaan erityisesti käyttöön vastuuta koskeva järjestelmä, jonka nojalla kaikkien luottamuspalvelun tarjoajien olisi oltava vastuussa luonnolliselle henkilölle tai oikeushenkilölle aiheutetusta vahingosta, joka johtuu tässä asetuksessa säädettyjen velvoitteiden noudattamisen laiminlyönnistä. Niiden taloudellisten riskien arvioinnin helpottamiseksi, joita luottamuspalvelun tarjoajille saattaa aiheutua tai jotka niiden olisi katettava vakuutuksilla, tässä asetuksessa sallitaan, että luottamuspalvelun tarjoajat asettavat tietyin edellytyksin rajoituksia tarjoamiensa palvelujen käytölle ja että ne eivät ole vastuussa vahingoista, joita aiheutuu tällaiset rajoitukset ylittävästä palvelujen käytöstä. Asiakkaille olisi ilmoitettava rajoituksista asianmukaisesti ennakolta. Tällaisten rajoitusten olisi oltava kolmannen osapuolen tunnistettavissa esimerkiksi siten, että rajoituksia koskevia tietoja sisällytetään tarjotun palvelun ehtoihin ja edellytyksiin, tai muilla tunnistettavilla keinoilla. Näiden periaatteiden toteuttamiseksi tätä asetusta olisi sovellettava kansallisten vastuusääntöjen mukaisesti. Tämä asetus ei näin ollen vaikuta kyseisiin kansallisiin sääntöihin, jotka koskevat esimerkiksi vahinkojen, tahallisuuden tai tuottamuksellisuuden määrittelyä, tai asiaan liittyviin sovellettaviin menettelysääntöihin.

(38) Tietoturvaloukkauksista ja turvallisuusriskien arvioinneista ilmoittaminen on olennaisen tärkeää, jotta asianomaisille tahoille voidaan antaa tarvittavaa tietoa tietoturvaloukkaustapauksissa tai tietojen eheyden ollessa uhattuna.

(39) Jotta komissio ja jäsenvaltiot voisivat arvioida tällä asetuksella perustetun tietoturvaloukkausten ilmoitusmekanismin toimivuutta, valvontaelimiä olisi pyydettävä toimittamaan asiasta tiivistettyä tietoa komissiolle ja Euroopan unionin verkko- ja tietoturvavirastolle (ENISA).

(40) Jotta komissio ja jäsenvaltiot voisivat arvioida tällä asetuksella käyttöön otetun tehostetun valvontamekanismin tuloksellisuutta, valvontaelimiä olisi pyydettävä raportoimaan toiminnastaan. Tämä edistäisi hyvien käytäntöjen vaihtoa valvontaelinten välillä ja antaisi varmuuden keskeisten valvontavaatimusten johdonmukaisesta ja tehokkaasta noudattamisesta kaikissa jäsenvaltioissa.

(41) Hyväksyttyjen luottamuspalvelujen kestävyyden ja jatkuvuuden varmistamiseksi sekä hyväksyttyjen luottamuspalvelujen jatkuvuuteen kohdistuvan käyttäjien luottamuksen lisäämiseksi valvontaelinten olisi varmistettava, että on olemassa säännöksiä toiminnan lopettamista koskevista suunnitelmista ja että tällaisia säännöksiä sovelletaan asianmukaisesti tapauksissa, joissa hyväksytyt luottamuspalvelun tarjoajat lopettavat toimintansa.

(42) Hyväksyttyjen luottamuspalvelun tarjoajien valvonnan helpottamiseksi esimerkiksi silloin, kun palveluntarjoaja tarjoaa palvelujaan toisen jäsenvaltion alueella eikä kuulu valvonnan piiriin siellä tai kun palveluntarjoajan tietokoneet sijaitsevat toisen jäsenvaltion kuin sen sijoittautumisvaltion alueella, olisi perustettava jäsenvaltioiden valvontaelinten keskinäisen avun järjestelmä.

(43) Sen varmistamiseksi, että hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat palvelut täyttävät tässä asetuksessa säädetyt vaatimukset, vaatimustenmukaisuuden arviointilaitoksen olisi tehtävä vaatimustenmukaisuuden arviointi, ja hyväksyttyjen luottamuspalvelun tarjoajien olisi toimitettava sen perusteella laadittavat vaatimustenmukaisuuden arviointikertomukset valvontaelimelle. Kun valvontaelin edellyttää hyväksytyn luottamuspalvelun tarjoajan toimittavan vaatimustenmukaisuuden *ad hoc* -arviointia koskevan kertomuksen, valvontaelimen olisi noudatettava erityisesti hyvän hallintotavan periaatetta, mukaan lukien velvoite esittää päätöstensä perustelut, sekä suhteellisuusperiaatetta. Näin ollen valvontaelimen olisi perusteltava asianmukaisesti päätöksensä, joissa edellytetään vaatimustenmukaisuuden *ad hoc* -arviointia.

(44) Tämän asetuksen tavoitteena on varmistaa johdonmukaiset puitteet luottamuspalvelujen tietoturvan ja oikeusvarmuuden korkean tason takaamiseksi. Tältä osin komission olisi tuotteiden ja palvelujen vaatimustenmukaisuuden arviointia käsitellessään pyrittävä tarvittaessa luomaan synergioita olemassa olevien asiaankuuluvien eurooppalaisten ja kansainvälisten järjestelyjen kuten Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 ([1]) kanssa, jossa vahvistetaan vaatimustenmukaisuuden arviointilaitosten akkreditointia ja tuotteiden markkinavalvontaa koskevat vaatimukset.

([1]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (EUVL L 218, 13.8.2008, s. 30).

(45) Jotta saataisiin aikaan tehokas aloitusprosessi, jonka pitäisi johtaa hyväksyttyjen luottamuspalvelun tarjoajien ja niiden tarjoamien hyväksyttyjen luottamuspalvelujen sisällyttämiseen luotettuihin luetteloihin, olisi edistettävä mahdollisten hyväksyttyjen luottamuspalvelun tarjoajien ja toimivaltaisen valvontaelimen alustavaa yhteydenpitoa, joka helpottaisi hyväksyttyjen luottamuspalvelujen tarjoamista edeltävää asianmukaista taustaselvitystä.

(46) Luotetut luettelot ovat olennaisia tekijöitä rakennettaessa luottamusta markkinatoimijoiden keskuudessa, koska ne osoittavat palveluntarjoajan hyväksytyn aseman valvonnan ajankohtana.

(47) Verkkopalvelujen luotettavuus ja niiden käytön mukavuus ovat käyttäjien kannalta olennaisia tekijöitä, jotta nämä voivat täysimääräisesti hyötyä sähköisistä palveluista ja tietoisesti luottaa niihin. Tätä varten olisi luotava EU:n luotettavuusmerkki hyväksyttyjen luottamuspalvelun tarjoajien tarjoamien hyväksyttyjen luottamuspalvelujen tunnistamiseksi. Tällaisella hyväksyttyjä luottamuspalveluja koskevalla EU:n luotettavuusmerkillä erotettaisiin hyväksytyt luottamuspalvelut selkeästi muista luottamuspalveluista, mikä edistäisi markkinoiden avoimuutta. EU:n luotettavuusmerkin käytön pitäisi olla hyväksytyille luottamuspalvelun tarjoajille vapaaehtoista eikä sen pitäisi luoda mitään muita velvoitteita tässä asetuksessa säädettyjen velvoitteiden lisäksi.

(48) Vaikka sähköisten allekirjoitusten vastavuoroinen tunnustaminen edellyttää korkeaa tietoturvatasoa, tietyissä erityistapauksissa, kuten komission päätöksen 2009/767/EY ([1]) yhteydessä, myös alhaisemmalla tietoturvavarmistuksella toimivat sähköiset allekirjoitukset olisi hyväksyttävä.

(49) Tässä asetuksessa olisi vahvistettava periaate, jonka mukaan sähköisen allekirjoituksen oikeusvaikutuksia ei pitäisi kieltää sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyn sähköisen allekirjoituksen vaatimuksia. Sähköisten allekirjoitusten oikeusvaikutukset määritellään kuitenkin kansallisessa laissa, lukuun ottamatta tässä asetuksessa säädettyjä vaatimuksia, joiden mukaan hyväksytyllä sähköisellä allekirjoituksella olisi oltava samanlaiset oikeusvaikutukset kuin käsin kirjoitetulla allekirjoituksella.

(50) Koska jäsenvaltioiden toimivaltaiset viranomaiset käyttävät tällä hetkellä erilaisia kehittyneiden sähköisten allekirjoitusten muotoja asiakirjojensa sähköiseen allekirjoittamiseen, on tarpeen varmistaa, että jäsenvaltiot kykenevät teknisesti käsittelemään ainakin muutamia kehittyneiden sähköisten allekirjoitusten muotoja vastaanottaessaan sähköisesti allekirjoitettuja asiakirjoja. Kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät kehittyneitä sähköisiä leimoja, olisi vastaavasti välttämätöntä varmistaa, että ne kykenevät käsittelemään ainakin muutamia kehittyneiden sähköisten leimojen muotoja.

(51) Allekirjoittajan olisi voitava antaa hyväksytyt sähköisen allekirjoituksen luontivälineet kolmannen osapuolen hoidettaviksi, kunhan käytössä on tarvittavat mekanismit ja menettelyt, joilla varmistetaan, että allekirjoittajalla on yksinomainen määräysvalta sähköisen allekirjoituksensa luontitietojen käyttöön, ja välineen käytössä noudatetaan hyväksytyille sähköisille allekirjoituksille asetettuja vaatimuksia.

(52) Sähköisten allekirjoitusten luomista etäpalveluna siten, että niiden luomista hallinnoi allekirjoittajan puolesta luottamuspalvelun tarjoaja, ollaan lisäämässä siihen liittyvien monien taloudellisten etujen vuoksi. On kuitenkin varmistuttava siitä, että nämä sähköiset allekirjoitukset tunnustetaan oikeudellisesti samalla tavalla kuin käyttäjän yksinomaisesti hallinnoimassa ympäristössä luodut sähköiset allekirjoitukset. Tämän vuoksi sähköisiä allekirjoituspalveluja etäpalveluna tuottavien palveluntarjoajien on noudatettava erityisiä johtamis- ja hallinnollisia tietoturvamenettelyjä ja käytettävä luotettavia järjestelmiä ja tuotteita, joihin kuuluvat turvatut sähköiset viestintäkanavat, jotta varmistettaisiin sähköisen allekirjoituksen luontiympäristön luotettavuus ja se, että ympäristöä käytetään allekirjoittajan yksinomaisessa määräysvallassa. Jos hyväksytty sähköinen allekirjoitus luodaan etäpalveluna tarjottavaa sähköisen allekirjoituksen luontivälinettä käyttäen, olisi sovellettava tässä asetuksessa vahvistettuja hyväksyttyihin luottamuspalvelun tarjoajiin sovellettavia vaatimuksia.

([1]) Komission päätös 2009/767/EY, tehty 16 päivänä lokakuuta 2009, toimenpiteistä sähköisten menettelyjen käytön edistämiseksi keskitettyjä asiointipisteitä käyttäen palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY mukaisesti (EUVL L 274, 20.10.2009, s. 36).

(53) Hyväksyttyjen varmenteiden voimassaolon keskeyttäminen on luottamuspalvelun tarjoajien vakiintunut toimintakäytäntö useissa jäsenvaltioissa. Se on eri asia kuin sulkeminen, ja se aiheuttaa varmenteen voimassaolon väliaikaisen päättymisen. Oikeusvarmuuden takia varmenteen keskeytystila on aina ilmoitettava selvästi. Tätä varten luottamuspalvelun tarjoajilla olisi oltava velvollisuus ilmoittaa selvästi varmenteen tila ja, jos se on keskeytetty, varmenteen voimassaolon keskeyttämisen tarkka ajanjakso. Tällä asetuksella ei olisi velvoitettava luottamuspalvelun tarjoajia tai jäsenvaltioita käyttämään voimassaolon keskeyttämistä, vaan siinä olisi säädettävä avoimuussäännöistä tapauksissa, joissa tällainen käytäntö on mahdollinen.

(54) Hyväksyttyjen varmenteiden rajat ylittävä yhteentoimivuus ja tunnustaminen on edellytys hyväksyttyjen sähköisten allekirjoitusten rajat ylittävälle tunnustamiselle. Näin ollen hyväksytyille varmenteille ei saisi asettaa pakollisia vaatimuksia, jotka ylittävät tässä asetuksessa säädetyt vaatimukset. Kansallisella tasolla olisi kuitenkin sallittava erityisten attribuuttien, kuten yksilöivien tunnisteiden, sisällyttäminen hyväksyttyihin varmenteisiin edellyttäen, että tällaiset erityiset attribuutit eivät haittaa hyväksyttyjen varmenteiden ja sähköisten allekirjoitusten rajat ylittävää yhteentoimivuutta ja tunnustamista.

(55) Tietotekninen tietoturvasertifiointi, joka perustuu kansainvälisiin standardeihin, kuten ISO 15408 ja siihen liittyvät arviointimenetelmät ja vastavuoroista tunnustamista koskevat järjestelyt, on hyväksyttyjen sähköisen allekirjoituksen luontivälineiden turvallisuuden tarkastamisessa tärkeä väline, jota olisi edistettävä. Innovatiiviset ratkaisut ja palvelut, kuten mobiiliallekirjoitus ja allekirjoitus pilvipalveluna, riippuvat kuitenkin sellaisista hyväksyttyjen sähköisen allekirjoituksen luontivälineiden teknisistä ja organisatorisista ratkaisuista, joita koskevia tietoturvastandardeja ei ehkä vielä ole saatavilla tai joiden osalta ensimmäinen tietotekninen tietoturvasertifiointi on käynnissä. Tällaisten hyväksyttyjen sähköisen allekirjoituksen luontivälineiden tietoturvatasoa voitaisiin arvioida käyttäen vaihtoehtoisia prosesseja ainoastaan silloin, kun tällaisia tietoturvastandardeja ei ole saatavilla tai kun ensimmäinen tietotekninen tietoturvasertifiointi on käynnissä. Näiden prosessien olisi oltava vertailukelpoisia tietoteknisen tietoturvasertifioinnin standardien kanssa siltä osin kuin niiden tietoturvatasot ovat vastaavat. Näitä prosesseja voitaisiin edistää vertaisarvioinnilla.

(56) Tässä asetuksessa olisi vahvistettava hyväksyttyjä sähköisen allekirjoituksen luontivälineitä koskevat vaatimukset kehittyneiden sähköisten allekirjoitusten toiminnan varmistamiseksi. Tämän asetuksen soveltamisalaan ei olisi kuuluttava se järjestelmäympäristö kokonaisuudessaan, jossa tällaiset välineet toimivat. Näin ollen hyväksyttyjen allekirjoituksen luontivälineiden sertifioinnin soveltamisala olisi rajoitettava laitteistoihin ja järjestelmäohjelmistoihin, joita käytetään allekirjoituksen luontivälineessä luotujen, siihen tallennettujen tai siinä käsiteltyjen allekirjoituksen luontitietojen hallinnointiin ja suojaamiseen. Kuten asiaankuuluvissa standardeissa esitetään, allekirjoituksen luontisovellukset olisi jätettävä sertifiointivelvoitteen soveltamisalan ulkopuolelle.

(57) Allekirjoituksen pätevyyttä koskevan oikeusvarmuuden varmistamiseksi on tärkeää yksilöidä ne hyväksytyn sähköisen allekirjoituksen osatekijät, jotka validoinnin suorittavan luottavan osapuolen olisi arvioitava. Yksilöimällä vaatimukset sellaisille hyväksytyille luottamuspalvelun tarjoajille, jotka voivat tarjota hyväksyttyä validointipalvelua luottaville osapuolille, jotka eivät halua tai voi itse suorittaa hyväksyttyjen sähköisten allekirjoitusten validointia, voitaisiin lisäksi edistää yksityisen ja julkisen sektorin investointeja tällaisiin palveluihin. Nämä molemmat tekijät voisivat tehdä hyväksyttyjen sähköisten allekirjoitusten validoinnista helppoa ja sujuvaa kaikille osapuolille unionin tasolla.

(58) Kun tietty transaktio edellyttää oikeushenkilön hyväksyttyä sähköistä leimaa, olisi samalla tavoin hyväksyttävä myös kyseisen oikeushenkilön valtuutetun edustajan hyväksytty sähköinen allekirjoitus.

(59) Sähköisten leimojen olisi toimittava todisteena siitä, että tietty sähköinen asiakirja on lähtöisin tietyltä oikeushenkilöltä, ja varmistettava näin asiakirjan alkuperä ja eheys.

(60) Sähköisten leimojen hyväksyttyjä varmenteita myöntävien luottamuspalvelun tarjoajien olisi toteutettava tarvittavat toimenpiteet määrittääkseen sitä oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden, jolle sähköisen leiman hyväksytty varmenne myönnetään, kun tällainen tunnistaminen on tarpeen kansallisella tasolla oikeudellisen tai hallinnollisen menettelyn yhteydessä.

(61) Tällä asetuksella olisi varmistettava tietojen pitkäaikainen säilyminen sähköisten allekirjoitusten ja sähköisten leimojen pitkän aikavälin oikeudellinen pätevyyden varmistamiseksi ja sen takaamiseksi, että ne voidaan validoida tulevista teknologian muutoksista riippumatta.

(62) Hyväksyttyjen sähköisten aikaleimojen tietoturvan varmistamiseksi tässä asetuksessa olisi edellytettävä kehittyneiden sähköisten leimojen tai kehittyneiden sähköisten allekirjoitusten tai muiden vastaavien menetelmien käyttöä. On ennakoitavissa, että innovointi saattaa johtaa uusiin teknologioihin, joilla voidaan varmistaa vastaava tietoturvan taso aikaleimojen osalta. Kun käytetään muuta menetelmää kuin kehittynyttä sähköistä leimaa tai kehittynyttä sähköistä allekirjoitusta, hyväksytyn luottamuspalvelun tarjoajan olisi osoitettava vaatimustenmukaisuuden arviointikertomuksessa, että tällaisella menetelmällä varmistetaan vastaava tietoturvataso ja että se on tässä asetuksessa säädettyjen velvoitteiden mukainen.

(63) Sähköiset asiakirjat ovat tärkeitä sisämarkkinoilla suoritettavien rajat ylittävien sähköisten transaktioiden jatkokehityksen kannalta. Tässä asetuksessa olisi vahvistettava periaate, jonka mukaan sähköisen asiakirjan oikeusvaikutuksia ei pitäisi kieltää sillä perusteella, että se on sähköisessä muodossa, sen varmistamiseksi, että sähköistä transaktiota ei olla hyväksymättä ainoastaan sillä perusteella, että asiakirja on sähköisessä muodossa.

(64) Käsitellessään kehittyneiden sähköisten allekirjoitusten ja leimojen muotoja komission olisi käytettävä perustana olemassa olevia käytäntöjä, standardeja ja säädöksiä, erityisesti komission päätöstä 2011/130/EU ([1]).

(65) Oikeushenkilöltä peräisin olevan asiakirjan todentamisen lisäksi sähköisiä leimoja voidaan käyttää oikeushenkilön minkä tahansa digitaalisen omaisuuden, kuten ohjelmistokoodin tai palvelimen, todentamiseen.

(66) On olennaisen tärkeää säätää oikeudellisesta kehyksestä, jolla edistetään rajat ylittävää tunnustamista sähköisiin rekisteröityihin jakelupalveluihin liittyvien olemassa olevien kansallisten oikeusjärjestelmien välillä. Tämä kehys voisi myös avata unionin luottamuspalvelun tarjoajille uusia markkinamahdollisuuksia uusien yleiseurooppalaisten sähköisten rekisteröityjen jakelupalvelujen tarjoamiseksi.

(67) Verkkosivustojen todentamispalvelut tarjoavat välineen, jonka avulla verkkosivustolla vieraileva henkilö voi varmistua siitä, että verkkosivuston taustalla on aito ja laillinen taho. Nämä palvelut lisäävät luottamusta verkossa asiointiin, koska käyttäjät luottavat verkkosivustoon, joka on todennettu. Verkkosivustojen todentamispalvelujen tarjoaminen ja käyttö ovat täysin vapaaehtoisia. Jotta verkkosivustojen todentamisesta tulisi kuitenkin keino lisätä luottamusta, antaa käyttäjälle parempia kokemuksia ja edistää kasvua sisämarkkinoilla, tässä asetuksessa olisi säädettävä tietoturvaa ja vastuuta koskevista vähimmäisvelvoitteista palveluntarjoajien ja niiden palvelujen osalta. Tätä varten on otettu huomioon toimialan toteuttamien olemassa olevien aloitteiden, esimerkiksi sertifiointiviranomaisten ja selainohjelmistojen myyjien foorumin (CA/B Forum), tulokset. Lisäksi tämän asetuksen ei pitäisi estää muiden, tämän asetuksen soveltamisalaan kuulumattomien keinojen tai menetelmien käyttöä verkkosivuston todentamiseksi, eikä sen pitäisi estää kolmansista maista peräisin olevia verkkosivustojen todentamispalvelujen tarjoajia tarjoamasta palvelujaan unionin asiakkaille. Kolmannen maan palveluntarjoajan olisi kuitenkin saatava verkkosivustojen todentamispalvelunsa tunnustettua hyväksytyiksi tämän asetuksen mukaisesti vain, jos unionin ja tarjoajan sijoittautumismaan välillä on tehty kansainvälinen sopimus.

(68) Euroopan unionin toiminnasta tehdyssä sopimuksessa olevissa sijoittautumista koskevissa määräyksissä ”oikeushenkilöiden” käsitteen osalta annetaan toimijoille vapaus valita se oikeudellinen muoto, jonka ne katsovat sopivaksi toimintansa harjoittamiseen. Vastaavasti ”oikeushenkilöillä” tarkoitetaan Euroopan unionin toiminnasta tehdyssä sopimuksessa kaikkia jonkin jäsenvaltion lain nojalla perustettuja tai sen alaisia yksikköjä niiden oikeudellisesta muodosta riippumatta.

(69) Unionin toimielimiä, elimiä, laitoksia ja virastoja kannustetaan tunnustamaan tämän asetuksen kattamat sähköinen tunnistaminen ja luottamuspalvelut hallinnollista yhteistyötä varten, käyttäen hyväksi erityisesti olemassa olevia hyviä käytäntöjä ja käynnissä olevien hankkeiden tuloksia tämän asetuksen kattamilla aloilla.

([1]) Komission päätös 2011/130/EU, annettu 25 päivänä helmikuuta 2011, palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY nojalla toimivaltaisten viranomaisten sähköisesti allekirjoittamien asiakirjojen maiden rajat ylittävää käsittelyä koskevista vähimmäisvaatimuksista (EUVL L 53, 26.2.2011, s. 66).

(70) Tämän asetuksen tiettyjen yksityiskohtaisten teknisten näkökohtien täydentämiseksi joustavasti ja nopeasti komissiolle olisi siirrettävä valta hyväksyä säädöksiä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti niiden perusteiden osalta, jotka hyväksyttyjen sähköisen allekirjoituksen luontivälineiden sertifioinnista vastaavien laitosten on täytettävä. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla. Komission olisi delegoituja säädöksiä valmistellessaan ja laatiessaan varmistettava, että asianomaiset asiakirjat toimitetaan Euroopan parlamentille ja neuvostolle yhtäaikaisesti, hyvissä ajoin ja asianmukaisesti.

(71) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa, joka liittyy erityisesti niiden standardien viitenumeroiden ilmoittamiseen, joiden käyttö johtaa olettamaan tässä asetuksessa säädettyjen tiettyjen vaatimusten noudattamisesta. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011 ([1]) mukaisesti.

(72) Hyväksyessään delegoituja säädöksiä tai täytäntöönpanosäädöksiä komission olisi otettava asianmukaisesti huomioon eurooppalaisten ja kansainvälisten standardointijärjestöjen ja -elinten, erityisesti Euroopan standardisointikomitean (CEN), Euroopan telealan standardointilaitoksen (ETSI), Kansainvälisen standardisoimisjärjestön (ISO) ja Kansainvälisen televiestintäliiton (ITU) laatimat standardit ja tekniset eritelmät, jotta voidaan varmistaa sähköisen tunnistamisen ja sähköisten luottamuspalvelujen korkea tietoturvataso ja yhteentoimivuus.

(73) Direktiivi 1999/93/EY olisi kumottava oikeusvarmuuden ja selkeyden vuoksi.

(74) Oikeusvarmuuden varmistamiseksi markkinatoimijoille, jotka jo käyttävät direktiivin 1999/93/EY mukaisia luonnollisille henkilöille myönnettyjä hyväksyttyjä varmenteita, on tarpeen säätää riittävästä siirtymäajasta. Vastaavasti olisi vahvistettava siirtymätoimenpiteet turvallisten allekirjoituksen luontivälineiden osalta, joiden vaatimustenmukaisuus on määritetty direktiivin 1999/93/EY mukaisesti, sekä niiden varmennepalvelujen tarjoajien osalta, jotka myöntävät hyväksyttyjä varmenteita ennen 1 päivää heinäkuuta 2016. Lopuksi on myös tarpeen säätää komission mahdollisuudesta hyväksyä täytäntöönpanosäädökset ja delegoidut säädökset ennen kyseistä päivämäärää.

(75) Tässä asetuksessa vahvistetut soveltamispäivät eivät vaikuta olemassa oleviin velvoitteisiin, joita jäsenvaltioilla jo on unionin oikeuden, erityisesti direktiivin 2006/123/EY, nojalla.

(76) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, vaan ne voidaan suunnitellun toiminnan laajuuden vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi.

(77) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 ([2]) 28 artiklan 2 kohdan mukaisesti, ja hän on antanut lausunnon 27 päivänä syyskuuta 2012 ([3]),

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13).

([2]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, 12.1.2001, s. 1).

([3]) EUVL C 28, 30.1.2013, s. 6.

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

Sisämarkkinoiden asianmukaisen toiminnan varmistamiseksi, pyrkien samalla sähköisen tunnistamisen menetelmien ja luottamuspalvelujen tietoturvan riittävän korkeaan tasoon, tässä asetuksessa:

a) säädetään ehdoista, joiden mukaisesti jäsenvaltiot tunnustavat toisen jäsenvaltion ilmoitetun sähköisen tunnistamisen järjestelmän piiriin kuuluvat luonnollisten henkilöiden ja oikeushenkilöiden sähköisen tunnistamisen menetelmät;

b) säädetään luottamuspalveluja koskevista säännöistä erityisesti sähköisten transaktioiden osalta; ja

c) vahvistetaan oikeudelliset puitteet sähköisille allekirjoituksille, sähköisille leimoille, sähköisille aikaleimoille, sähköisille asiakirjoille, sähköisille rekisteröidyille jakelupalveluille ja verkkosivustojen todentamisen varmennepalveluille.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan jäsenvaltion ilmoittamiin sähköisen tunnistamisen järjestelmiin ja unioniin sijoittautuneisiin luottamuspalvelujen tarjoajiin.

2. Tätä asetusta ei sovelleta sellaisten luottamuspalvelujen tarjoamiseen, joita käytetään yksinomaan kansallisesta oikeudesta tai määrätyn osallistujajoukon välisistä sopimuksista johtuvissa suljetuissa järjestelmissä.

3. Tämä asetus ei vaikuta kansalliseen eikä unionin oikeuteen, joka liittyy sopimusten tekemiseen tai pätevyyteen taikka muihin muotovaatimuksia koskeviin oikeudellisiin tai menettelyllisiin velvoitteisiin.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’sähköisellä tunnistamisella’ prosessia, jossa käytetään tiettyä luonnollista henkilöä, oikeushenkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä vastaavia yksilöiviä tunnistetietoja sähköisessä muodossa;

2) ’sähköisen tunnistamisen menetelmällä’ aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen;

3) ’henkilön tunnistetiedoilla’ tietoja, jotka mahdollistavat luonnollisen henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden toteamisen;

4) ’sähköisen tunnistamisen järjestelmällä’ sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille tai oikeushenkilöä edustaville luonnollisille henkilöille;

5) ’todentamisella’ sähköistä prosessia, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön sähköisen tunnistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen;

6) ’luottavalla osapuolella’ luonnollista henkilöä tai oikeushenkilöä, joka luottaa sähköiseen tunnistamiseen tai luottamuspalveluun;

7) ’julkisen sektorin elimellä’ valtion viranomaista, alueviranomaista tai paikallisviranomaista, julkisoikeudellista laitosta taikka yhden tai useamman tällaisen viranomaisen tai yhden tai useamman tällaisen julkisoikeudellisen laitoksen muodostamaa yhteenliittymää, taikka yksityistä yhteisöä, jonka vähintään yksi kyseisistä viranomaisista, laitoksista tai yhteenliittymistä on valtuuttanut tarjoamaan julkisia palveluja, niiden toimiessa tällaisen valtuutuksen nojalla;

8) ’julkisoikeudellisella laitoksella’ Euroopan parlamentin ja neuvoston direktiivin 2014/24/EU ([1]) 2 artiklan 1 kohdan 4 alakohdassa määriteltyä laitosta;

9) ’allekirjoittajalla’ luonnollista henkilöä, joka luo sähköisen allekirjoituksen;

10) ’sähköisellä allekirjoituksella’ sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon ja jota allekirjoittaja käyttää allekirjoittamiseen;

11) ’kehittyneellä sähköisellä allekirjoituksella’ sähköistä allekirjoitusta, joka täyttää 26 artiklassa säädetyt vaatimukset;

12) ’hyväksytyllä sähköisellä allekirjoituksella’ kehittynyttä sähköistä allekirjoitusta, joka on luotu hyväksytyllä sähköisen allekirjoituksen luontivälineellä ja joka perustuu sähköisten allekirjoitusten hyväksyttyyn varmenteeseen;

13) ’sähköisen allekirjoituksen luontitiedoilla’ yksilöiviä tietoja, joita allekirjoittaja käyttää sähköisen allekirjoituksen luomiseen;

14) ’sähköisen allekirjoituksen varmenteella’ sähköistä todistusta, joka liittää sähköisen allekirjoituksen validointitiedot luonnolliseen henkilöön ja vahvistaa vähintään kyseisen henkilön nimen tai salanimen;

15) ’sähköisen allekirjoituksen hyväksytyllä varmenteella’ sähköisen allekirjoituksen varmennetta, jonka on myöntänyt hyväksytty luottamuspalvelujen tarjoaja ja joka täyttää liitteessä I säädetyt vaatimukset;

16) ’luottamuspalvelulla’ sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu seuraavista:

   a) sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen, sähköisten rekisteröityjen jakelupalvelujen ja kyseisiin palveluihin liittyvien varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai

   b) verkkosivustojen todentamisen varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai

   c) sähköisten allekirjoitusten, leimojen tai kyseisiin palveluihin liittyvien varmenteiden säilyttämisestä;

17) ’hyväksytyllä luottamuspalvelulla’ luottamuspalvelua, joka täyttää tässä asetuksessa säädetyt sovellettavat vaatimukset;

([1]) Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26 päivänä helmikuuta 2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 65).

18) ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määriteltyä elintä, joka on akkreditoitu kyseisen asetuksen mukaisesti pätevästi arvioimaan hyväksyttyjen luottamuspalvelun tarjoajien ja niiden tarjoamien hyväksyttyjen luottamuspalvelujen vaatimustenmukaisuus;

19) ’luottamuspalvelun tarjoajalla’ luonnollista henkilöä tai oikeushenkilöä, joka tarjoaa yhtä tai useampaa luottamuspalvelua joko hyväksyttynä tai ei-hyväksyttynä luottamuspalvelun tarjoajana;

20) ’hyväksytyllä luottamuspalvelun tarjoajalla’ luottamuspalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa hyväksyttyä luottamuspalvelua ja jolle valvontaelin on myöntänyt hyväksytyn aseman;

21) ’tuotteella’ laitteistoja tai ohjelmistoja taikka laitteistojen tai ohjelmistojen merkityksellisiä osia, jotka on tarkoitettu käytettäviksi luottamuspalveluja tarjottaessa;

22) ’sähköisen allekirjoituksen luontivälineellä’ asetuksin varustettua ohjelmistoa tai laitteistoa, jota käytetään sähköisen allekirjoituksen luomiseen;

23) ’hyväksytyllä sähköisen allekirjoituksen luontivälineellä’ sähköisen allekirjoituksen luontivälinettä, joka täyttää liitteessä II säädetyt vaatimukset;

24) ’leiman luojalla’ oikeushenkilöä, joka luo sähköisen leiman;

25) ’sähköisellä leimalla’ sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon viimeksi mainitun tiedon alkuperän ja eheyden varmistamiseksi;

26) ’kehittyneellä sähköisellä leimalla’ sähköistä leimaa, joka täyttää 36 artiklassa säädetyt vaatimukset;

27) ’hyväksytyllä sähköisellä leimalla’ kehittynyttä sähköistä leimaa, joka on luotu hyväksytyllä sähköisen leiman luontivälineellä ja joka perustuu sähköisen leiman hyväksyttyyn varmenteeseen;

28) ’sähköisen leiman luontitiedoilla’ yksilöiviä tietoja, joita sähköisen leiman luoja käyttää sähköisen leiman luomiseen;

29) ’sähköisen leiman varmenteella’ sähköistä todistusta, joka liittää sähköisen leiman validointitiedot oikeushenkilöön ja vahvistaa kyseisen henkilön nimen;

30) ’sähköisen leiman hyväksytyllä varmenteella’ sähköisen leiman varmennetta, jonka on myöntänyt hyväksytty luottamuspalvelujen tarjoaja ja joka täyttää liitteessä III säädetyt vaatimukset;

31) ’sähköisen leiman luontivälineellä’ asetuksin varustettua ohjelmistoa tai laitteistoa, jota käytetään sähköisen leiman luomiseen;

32) ’hyväksytyllä sähköisen leiman luontivälineellä’ sähköisen leiman luontivälinettä, joka täyttää soveltuvin osin liitteessä II säädetyt vaatimukset;

33) ’sähköisellä aikaleimalla’ sähköisessä muodossa olevia tietoja, jotka sitovat muut sähköisessä muodossa olevat tiedot tiettyyn ajankohtaan ja muodostavat todisteen viimeksi mainittujen tietojen olemassaolosta kyseisenä ajankohtana;

34) ’hyväksytyllä sähköisellä aikaleimalla’ sähköistä aikaleimaa, joka täyttää 42 artiklassa säädetyt vaatimukset;

35) 'sähköisellä asiakirjalla' kaikkea sisältöä, joka on tallennettu sähköisessä muodossa, erityisesti tekstinä tai äänenä, visuaalisessa muodossa tai audiovisuaalisena tallenteena;

36) 'sähköisellä rekisteröidyllä jakelupalvelulla' palvelua, jonka avulla tietoa voidaan siirtää sähköisesti kolmansien osapuolten välillä ja joka antaa siirretyn tiedon käsittelyyn liittyviä todisteita, muun muassa vahvistuksen tietojen lähettämisestä ja vastaanottamisesta, ja joka suojaa siirretyt tiedot häviämisen, varkauden, vaurioitumisen tai luvattomien muutosten riskiltä;

37) 'hyväksytyllä sähköisellä rekisteröidyllä jakelupalvelulla' sähköistä rekisteröityä jakelupalvelua, joka täyttää 44 artiklassa säädetyt vaatimukset;

38) 'verkkosivustojen todentamisen varmenteella' todistusta, jonka avulla verkkosivusto voidaan todentaa ja joka liittää verkkosivuston siihen luonnolliseen henkilöön tai oikeushenkilöön, jolle varmenne on myönnetty;

39) 'verkkosivustojen todentamisen hyväksytyllä varmenteella' verkkosivustojen todentamisen varmennetta, jonka on myöntänyt hyväksytty luottamuspalvelujen tarjoaja ja joka täyttää liitteessä IV säädetyt vaatimukset;

40) 'validointitiedoilla' tietoja, joita käytetään sähköisen allekirjoituksen tai sähköisen leiman validointiin;

41) 'validoinnilla' prosessia sen tarkistamiseksi ja vahvistamiseksi, että sähköinen allekirjoitus tai leima on pätevä.

4 artikla

Sisämarkkinaperiaate

1. Toiseen jäsenvaltioon sijoittautuneen luottamuspalvelujen tarjoajan luottamuspalvelujen tarjoamista jäsenvaltion alueella ei saa rajoittaa syistä, jotka kuuluvat tämän asetuksen kattamiin aloihin.

2. Tämän asetuksen mukaisten tuotteiden ja luottamuspalvelujen on saatava liikkua vapaasti sisämarkkinoilla.

5 artikla

Tietojen käsittely ja suojaaminen

1. Henkilötietojen käsittelyssä on noudatettava direktiiviä 95/46/EY.

2. Salanimien käyttöä sähköisissä transaktioissa ei kielletä, sanotun kuitenkaan rajoittamatta salanimille kansallisessa laissa annettavia oikeusvaikutuksia.

II LUKU

SÄHKÖINEN TUNNISTAMINEN

6 artikla

Vastavuoroinen tunnustaminen

1. Kun julkisen sektorin elimen yhdessä jäsenvaltiossa tarjoaman verkkopalvelun käyttö edellyttää kansallisen oikeuden nojalla tai kansallisessa hallinnollisessa käytännössä sähköistä tunnistamista sähköisen tunnistamisen menetelmän ja todentamisen avulla, toisessa jäsenvaltiossa myönnetyt verkkopalvelujen käyttöön tarvittavat sähköisen tunnistamisen menetelmät on tunnustettava ensimmäisessä jäsenvaltiossa kyseisen verkkopalvelun osalta rajat ylittävää todentamista varten edellyttäen, että seuraavat ehdot täyttyvät:

a) sähköisen tunnistamisen menetelmä on myönnetty komission 9 artiklan mukaisesti julkaisemaan luetteloon sisältyvän sähköisen tunnistamisen järjestelmän puitteissa;

b) sähköisen tunnistamisen menetelmän varmuustaso vastaa varmuustasoa, joka on yhtä korkea tai korkeampi kuin asianomaisen julkisen sektorin elimen edellyttämä varmuustaso kyseiseen verkkopalveluun pääsemiseksi ensimmäisessä jäsenvaltiossa, edellyttäen, että kyseisen sähköisen tunnistamisen menetelmän varmuustaso vastaa korotettua tai korkeaa varmuustasoa;

c) asianomainen julkisen sektorin elin soveltaa korotettua tai korkeaa varmuustasoa kyseisen verkkopalvelun käytön osalta.

Tällaisen tunnustamisen on toteuduttava viimeistään 12 kuukauden kuluttua siitä, kun komissio julkaisee ensimmäisen alakohdan a alakohdassa tarkoitetun luettelon.

2. Julkisen sektorin elimet voivat tarjoamiensa verkkopalvelujen rajat ylittävää todentamista varten tunnustaa sähköisen tunnistamisen menetelmän, joka on myönnetty komission 9 artiklan mukaisesti julkaisemaan luetteloon sisältyvän sähköisen tunnistamisen järjestelmän puitteissa ja jonka varmuustaso vastaa matalaa varmuustasoa.

7 artikla

Edellytykset sähköisen tunnistamisen järjestelmien ilmoittamiselle

Sähköisen tunnistamisen järjestelmä voidaan ilmoittaa 9 artiklan 1 kohdan mukaisesti, edellyttäen että kaikki seuraavat ehdot täyttyvät:

a) sähköisen tunnistamisen järjestelmän mukaiset sähköisen tunnistamisen menetelmät on myönnetty:

i) ilmoittavan jäsenvaltion toimesta;

ii) ilmoittavan jäsenvaltion toimeksiannosta; tai

iii) ilmoittavasta jäsenvaltiosta riippumatta niin, että kyseinen jäsenvaltio tunnustaa ne;

b) sähköisen tunnistamisen järjestelmän mukaista sähköisen tunnistamisen menetelmää voidaan käyttää pääsemiseksi ainakin yhteen sellaiseen palveluun, jonka julkisen sektorin elin tarjoaa ja joka edellyttää ilmoittavassa jäsenvaltiossa sähköistä tunnistamista;

c) sähköisen tunnistamisen järjestelmä ja sen puitteissa myönnetty sähköisen tunnistamisen menetelmä täyttävät 8 artiklan 3 kohdassa tarkoitetussa täytäntöönpanosäädöksessä säädetyistä varmuustasoista ainakin yhden vaatimukset;

d) ilmoittava jäsenvaltio varmistaa, että kyseistä henkilöä vastaavat yksilöivät tunnistetiedot on liitetty 8 artiklan 3 kohdassa tarkoitetussa täytäntöönpanosäädöksessä säädettyä asianmukaista varmuustasoa koskevien teknisten eritelmien, standardien ja menettelyjen mukaisesti 3 artiklan 1 kohdassa tarkoitettuun luonnolliseen henkilöön tai oikeushenkilöön kyseisen järjestelmän mukaisen sähköisen tunnistamisen menetelmän myöntämisen ajankohtana;

e) kyseisen järjestelmän mukaisen sähköisen tunnistamisen menetelmän myöntävä osapuoli varmistaa, että sähköisen tunnistamisen menetelmä on liitetty tämän artiklan d alakohdassa tarkoitettuun henkilöön 8 artiklan 3 kohdassa tarkoitetussa täytäntöönpanosäädöksessä säädettyä asianmukaista varmuustasoa koskevien teknisten eritelmien, standardien ja menettelyjen mukaisesti;

f) ilmoittava jäsenvaltio varmistaa, että todentaminen verkossa on mahdollista niin, että mikä tahansa toisen jäsenvaltion alueelle sijoittautunut luottava osapuoli kykenee vahvistamaan sähköisessä muodossa vastaanotetut henkilön tunnistetiedot.

Ilmoittava jäsenvaltio voi muiden luottavien osapuolten kuin julkisen sektorin elinten osalta määrittää kyseisen todentamisen käyttöehdot. Rajat ylittävä todentaminen on tarjottava veloituksetta, kun se suoritetaan julkisen sektorin elimen tarjoaman verkkopalvelun yhteydessä.

Jäsenvaltiot eivät saa asettaa tällaista todentamismahdollisuutta hyödyntäville luottaville osapuolille minkäänlaisia suhteettomia teknisiä erityisvaatimuksia, jos tällaiset vaatimukset estävät tai merkittävästi haittaavat ilmoitettujen sähköisen tunnistamisen järjestelmien yhteentoimivuutta;

g) ilmoittava jäsenvaltio toimittaa vähintään kuusi kuukautta ennen 9 artiklan 1 kohdan mukaista ilmoittamista muille jäsenvaltioille 12 artiklan 5 kohdassa säädetyn velvoitteen täyttämiseksi kuvauksen kyseisestä järjestelmästä 12 artiklan 7 kohdassa tarkoitetuilla täytäntöönpanosäädöksillä vahvistettujen menettelyä koskevien järjestelyjen mukaisesti;

h) sähköisen tunnistamisen järjestelmä täyttää 12 artiklan 8 kohdassa tarkoitetun täytäntöönpanosäädöksen vaatimukset.

8 artikla

Sähköisen tunnistamisen järjestelmien varmuustasot

1. Sähköisen tunnistamisen järjestelmässä, joka on ilmoitettu 9 artiklan 1 kohdan nojalla, on kyseisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien osalta määritettävä matala, korotettu ja/tai korkea varmuustaso.

2. Matalan, korotetun ja korkean varmuustason on oltava seuraavien kriteerien mukaisia:

a) matala varmuustaso tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa rajallisen luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää henkilöllisyyden väärinkäytön tai muuttamisen riskiä;

b) korotettu varmuustaso tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa merkittävän luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävässä määrin henkilöllisyyden väärinkäytön tai muuttamisen riskiä;

c) korkea varmuustaso tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa korkeamman luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on estää henkilöllisyyden väärinkäyttö tai muuttaminen.

3. Asianmukaiset kansainväliset standardit huomioon ottaen ja jollei 2 kohdasta muuta johdu, komissio vahvistaa viimeistään 18 päivänä syyskuuta 2015 täytäntöönpanosäädöksillä tekniset vähimmäiseritelmät, -standardit ja -menettelyt; sähköisen tunnistamisen menetelmien matala, korotettu ja korkea varmuustaso määritellään 1 kohdan soveltamiseksi suhteessa niihin.

Nämä tekniset vähimmäiseritelmät, -standardit ja -menettelyt laaditaan ottaen huomioon seuraavien osatekijöiden luotettavuus ja laatu:

a) menettely sellaisten luonnollisten henkilöiden ja oikeushenkilöiden henkilöllisyyden todistamiseksi ja todentamiseksi, jotka hakevat sähköisen tunnistamisen menetelmien myöntämistä;

b) myöntämismenettely haetuille sähköisen tunnistamisen menetelmille;

c) todentamismekanismi, jolla luonnollinen henkilö tai oikeushenkilö käyttää sähköisen tunnistamisen menetelmää vahvistaakseen henkilöllisyytensä luottavalle osapuolelle;

d) toimija, joka myöntää sähköisen tunnistamisen menetelmiä;

e) muu elin, joka osallistuu hakemukseen sähköisen tunnistamisen menetelmien myöntämiseksi; ja

f) myönnettyjen sähköisen tunnistamisen menetelmien tekniset eritelmät ja turvaominaisuudet.

Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

9 artikla

Ilmoittaminen

1. Ilmoittavan jäsenvaltion on ilman aiheetonta viivytystä ilmoitettava komissiolle seuraavat tiedot ja niiden mahdolliset myöhemmät muutokset:

a) kuvaus sähköisen tunnistamisen järjestelmästä, mukaan lukien sen varmuustasot ja järjestelmän mukaisten sähköisen tunnistamisen menetelmien myöntäjä tai myöntäjät;

b) sovellettava valvontajärjestelmä ja tiedot vastuuta koskevasta järjestelmästä seuraavien osalta:

i) sähköisen tunnistamisen menetelmän myöntävä osapuoli; ja

ii) todentamismenettelyä operoiva osapuoli;

c) sähköisen tunnistamisen järjestelmästä vastaava viranomainen tai vastaavat viranomaiset;

d) tiedot siitä, mikä taho tai mitkä tahot hallinnoivat yksilöivien henkilön tunnistetietojen rekisteröintiä;

e) kuvaus siitä, miten 12 artiklan 8 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä säädetyt vaatimukset on täytetty;

f) kuvaus 7 artiklan f alakohdassa tarkoitetusta todentamisesta;

g) järjestelyt joko ilmoitetun sähköisen tunnistamisen järjestelmän tai todentamisen tai niiden osien, joiden turvallisuus on vaarantunut, keskeyttämistä tai peruuttamista varten.

2. Yhden vuoden kuluttua 8 artiklan 3 kohdassa ja 12 artiklan 8 kohdassa tarkoitettujen täytäntöönpanosäädösten soveltamispäivästä komissio julkaisee *Euroopan unionin virallisessa lehdessä* luettelon tämän artiklan 1 kohdan nojalla ilmoitetuista sähköisen tunnistamisen järjestelmistä sekä niitä koskevat perustiedot.

3. Jos komissio saa ilmoituksen 2 kohdassa tarkoitetun ajanjakson päättymisen jälkeen, se julkaisee *Euroopan unionin virallisessa lehdessä* muutokset 2 kohdassa tarkoitettuun luetteloon kahden kuukauden kuluessa kyseisen ilmoituksen vastaanottamisesta.

4. Jäsenvaltio voi toimittaa komissiolle pyynnön poistaa kyseisen jäsenvaltion ilmoittama sähköisen tunnistamisen järjestelmä 2 kohdassa tarkoitetusta luettelosta. Komissio julkaisee *Euroopan unionin virallisessa lehdessä* vastaavat tarkistukset luetteloon kuukauden kuluessa jäsenvaltion pyynnön vastaanottamisesta.

5. Komissio voi täytäntöönpanosäädöksillä määritellä 1 kohdan mukaisiin ilmoituksiin liittyvät olosuhteet, muotoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

10 artikla

Tietoturvaloukkaus

1. Jos 9 artiklan 1 kohdan mukaisesti ilmoitettuun sähköisen tunnistamisen järjestelmään tai 7 artiklan f alakohdassa tarkoitettuun todentamiseen liittyy loukkaus tai niiden jonkin osan turvallisuus on vaarantunut tavalla, joka vaikuttaa kyseisen järjestelmän rajat ylittävän todentamisen luotettavuuteen, ilmoittavan jäsenvaltion on viipymättä keskeytettävä tai peruutettava kyseinen rajat ylittävä todentaminen tai ne osat, joiden turvallisuus on vaarantunut, ja ilmoitettava asiasta muille jäsenvaltioille ja komissiolle.

2. Kun 1 kohdassa tarkoitettu loukkaus tai turvallisuuden vaarantuminen on korjattu, ilmoittava jäsenvaltio vahvistaa rajat ylittävän todentamisen uudelleen ja ilmoittaa asiasta muille jäsenvaltioille ja komissiolle ilman aiheetonta viivytystä.

3. Jos 1 kohdassa tarkoitettua loukkausta tai vaarantumista ei ole korjattu kolmen kuukauden kuluessa keskeyttämisestä tai peruuttamisesta, ilmoittavan jäsenvaltion on ilmoitettava sähköisen tunnistamisen järjestelmän peruuttamisesta muille jäsenvaltioille ja komissiolle.

Komissio julkaisee *Euroopan unionin virallisessa lehdessä* vastaavat tarkistukset 9 artiklan 2 kohdassa tarkoitettuun luetteloon ilman aiheetonta viivytystä.

11 artikla

Vastuu

1. Ilmoittava jäsenvaltio on vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu 7 artiklan d ja f alakohdassa säädettyjen velvollisuuksien laiminlyönnistä rajat ylittävässä transaktiossa.

2. Sähköisen tunnistamisen menetelmän myöntävä osapuoli on vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu 7 artiklan e alakohdassa tarkoitetun velvollisuuden laiminlyönnistä rajat ylittävässä transaktiossa.

3. Todentamismenettelyä operoiva osapuoli on vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu 7 artiklan f alakohdassa tarkoitetun todentamisen asianmukaisen toiminnan varmistamatta jättämisestä rajat ylittävässä transaktiossa.

4. Edellä olevia 1, 2 ja 3 kohtaa sovelletaan kansallisten vastuusääntöjen mukaisesti.

5. Edellä olevilla 1, 2 ja 3 kohdalla ei rajoiteta kansallisen lain mukaisia osapuolten vastuita transaktiossa, jossa käytetään 9 artiklan 1 kohdan nojalla ilmoitetun sähköisen tunnistamisen järjestelmän piiriin kuuluvaa sähköisen tunnistamisen menetelmää.

12 artikla

Yhteistyö ja yhteentoimivuus

1. Edellä olevan 9 artiklan 1 kohdan nojalla ilmoitettujen kansallisten sähköisen tunnistamisen järjestelmien on oltava yhteentoimivia.

2. Edellä olevan 1 kohdan soveltamiseksi perustetaan yhteentoimivuusjärjestelmä.

3. Yhteentoimivuusjärjestelmän on täytettävä seuraavat kriteerit:

a) se pyrkii olemaan teknologianeutraali ja eikä syrji mitään kansallisia sähköisen tunnistamisen teknisiä erityisratkaisuja jäsenvaltiossa;

b) se noudattaa eurooppalaisia ja kansainvälisiä standardeja, kun se on mahdollista;

c) sillä helpotetaan sisäänrakennetun yksityisyyden suojan periaatteen soveltamista; ja

d) sillä varmistetaan, että henkilötietoja käsitellään direktiivin 95/46/EY mukaisesti.

4. Yhteentoimivuusjärjestelmän on muodostuttava:

a) viittauksesta teknisiin vähimmäisvaatimuksiin, jotka liittyvät 8 artiklan mukaisiin varmuustasoihin;

b) ilmoitettujen sähköisen tunnistamisen järjestelmien kansallisten varmuustasojen kartoittamisesta suhteessa 8 artiklan mukaisiin varmuustasoihin;

c) viittauksesta yhteentoimivuutta koskeviin teknisiin vähimmäisvaatimuksiin;

d) viittauksesta luonnollista henkilöä tai oikeushenkilöä vastaavien yksilöivien tunnistetietojen vähimmäismäärään, joka sähköisen tunnistamisen järjestelmissä on käytettävissä;

e) työjärjestyksestä;

f) riidanratkaisujärjestelyistä; ja

g) yhteisistä toiminnan turvallisuutta koskevista standardeista.

5. Jäsenvaltioiden on tehtävä yhteistyötä seuraavilla osa-alueilla:

a) edellä olevan 9 artiklan 1 kohdan mukaisesti ilmoitettujen sähköisen tunnistamisen järjestelmien yhteentoimivuus niiden sähköisen tunnistamisen järjestelmien kanssa, jotka jäsenvaltiot aikovat ilmoittaa; ja

b) sähköisen tunnistamisen järjestelmien turvallisuus.

6. Jäsenvaltioiden välinen yhteistyö muodostuu seuraavista:

a) sähköisen tunnistamisen järjestelmiä ja erityisesti yhteentoimivuuteen ja varmuustasoihin liittyviä teknisiä vaatimuksia koskevien tietojen, kokemusten ja hyvien käytäntöjen vaihto;

b) edellä olevan 8 artiklan mukaisten sähköisen tunnistamisen järjestelmien varmuustasojen käyttöä koskevien tietojen, kokemusten ja hyvien käytäntöjen vaihto;

c) tämän asetuksen soveltamisalaan kuuluvien sähköisen tunnistamisen järjestelmien vertaisarviointi; ja

d) sähköisen tunnistamisen alan merkityksellisen kehityksen tarkastelu.

7. Komissio vahvistaa viimeistään 18 päivänä maaliskuuta 2015 täytäntöönpanosäädöksin tarvittavat menettelyä koskevat järjestelyt 5 ja 6 kohdassa tarkoitetun jäsenvaltioiden yhteistyön helpottamiseksi edistääkseen luottamuksen ja tietoturvan korkeaa tasoa, joka on oikeassa suhteessa riskin suuruuteen.

8. Komissio antaa 3 kohdan edellytysten mukaisesti ja ottaen huomioon jäsenvaltioiden välisen yhteistyön tulokset viimeistään 18 päivänä syyskuuta 2015 4 kohdassa säädettyä yhteentoimivuusjärjestelmää koskevat täytäntöönpanosäädökset yhdenmukaisten edellytysten asettamiseksi 1 kohdan mukaisen vaatimuksen täytäntöönpanolle.

9. Tämän artiklan 7 ja 8 kohdassa tarkoitetut täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

III LUKU

LUOTTAMUSPALVELUT

1 JAKSO

Yleiset säännökset

13 artikla

Vastuu ja todistustaakka

1. Luottamuspalvelun tarjoajat ovat vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu tässä asetuksessa säädettyjen velvollisuuksien laiminlyönnistä, sanotun kuitenkaan rajoittamatta 2 kohdan soveltamista.

Ei-hyväksytyn luottamuspalvelujen tarjoajan tahallisuutta tai tuottamuksellisuutta koskeva todistustaakka on luonnollisella henkilöllä tai oikeushenkilöllä, joka hakee korvausta ensimmäisessä alakohdassa tarkoitetusta vahingosta.

Hyväksytyn luottamuspalvelun tarjoajan oletetaan toimineen tahallaan tai tuottamuksesta, ellei kyseinen hyväksytty luottamuspalvelun tarjoaja todista, että ensimmäisessä alakohdassa tarkoitettu vahinko on tapahtunut ilman kyseisen hyväksytyn luottamuspalvelun tarjoajan tahallisuutta tai tuottamuksellisuutta.

2. Jos luottamuspalvelun tarjoajat ilmoittavat tarjoamiensa palvelujen käytön rajoituksista asianmukaisesti ennakolta asiakkailleen ja jos kyseiset rajoitukset ovat kolmansien osapuolien tunnistettavissa, luottamuspalvelun tarjoajat eivät ole vastuussa vahingoista, joita aiheutuu ilmoitetut rajoitukset ylittävästä palvelujen käytöstä.

3. Edellä olevia 1 ja 2 kohtaa sovelletaan kansallisten vastuusääntöjen mukaisesti.

14 artikla

Kansainväliset näkökohdat

1. Kolmanteen maahan sijoittautuneiden luottamuspalvelun tarjoajien tarjoamat luottamuspalvelut on tunnustettava oikeusvaikutuksiltaan vastaaviksi kuin unionin alueelle sijoittautuneiden hyväksyttyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut, jos kolmannesta maasta lähtöisin olevat luottamuspalvelut tunnustetaan unionin ja kyseisen kolmannen maan tai kansainvälisen järjestön välillä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti tehdyn sopimuksen nojalla.

2. Edellä 1 kohdassa tarkoitetuissa sopimuksissa on varmistettava erityisesti, että:

a) kolmannessa maassa tai kansainvälisessä järjestössä, jonka kanssa sopimus on tehty, toimivat luottamuspalvelun tarjoajat ja niiden tarjoamat luottamuspalvelut täyttävät unionin alueelle sijoittautuneisiin hyväksyttyihin luottamuspalvelun tarjoajiin ja niiden tarjoamiin hyväksyttyihin luottamuspalveluihin sovellettavat vaatimukset;

b) unionin alueelle sijoittautuneiden hyväksyttyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut tunnustetaan oikeusvaikutuksiltaan vastaaviksi kuin kolmannessa maassa tai kansainvälisessä järjestössä, jonka kanssa sopimus on tehty, toimivien luottamuspalvelun tarjoajien luottamuspalvelut.

15 artikla

Esteettömyys vammaisten näkökulmasta

Tarjotut luottamuspalvelut ja niiden tarjoamisessa käytetyt loppukäyttäjätuotteet on tehtävä vammaisille esteettömiksi aina kun se on toteutettavissa.

16 artikla

Seuraamukset

Jäsenvaltioiden on säädettävä seuraamuksista, joita sovelletaan tämän asetuksen rikkomiseen. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2 JAKSO

Valvonta

17 artikla

Valvontaelin

1. Jäsenvaltioiden on nimettävä valvontaelin, joka on sijoittautunut niiden alueelle, tai keskinäisellä sopimuksella toisen jäsenvaltion kanssa valvontaelin, joka on sijoittautunut kyseiseen toiseen jäsenvaltioon. Kyseinen valvontaelin vastaa valvontatehtävistä nimeävässä jäsenvaltiossa.

Valvontaelimille on annettava tarvittavat valtuudet ja riittävät resurssit tehtäviensä hoitamiseksi.

2. Jäsenvaltioiden on ilmoitettava komissiolle nimeämänsä valvontaelimen nimi ja osoite.

3. Valvontaelimellä on seuraavat tehtävät:

a) nimeävän jäsenvaltion alueelle sijoittautuneiden hyväksyttyjen luottamuspalvelun tarjoajien valvonta sen varmistamiseksi ennakkoon ja jälkikäteen toteutettavin valvontatoimin, että nämä hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset;

b) toimien toteuttaminen tarvittaessa nimeävän jäsenvaltion alueelle sijoittautuneiden ei-hyväksyttyjen luottamuspalvelun tarjoajien suhteen jälkikäteen toteutettavin valvontatoimin, jos sille ilmoitetaan, että nämä ei-hyväksytyt luottamuspalvelun tarjoajat tai niiden tarjoamat luottamuspalvelut eivät väitetysti täytä tässä asetuksessa säädettyjä vaatimuksia.

4. Sovellettaessa 3 kohtaa ja ottaen huomioon siinä säädetyt rajoitukset valvontaelimen tehtäviin sisältyy erityisesti:

a) yhteistyö muiden valvontaelinten kanssa ja tuen antaminen niille 18 artiklan mukaisesti;

b) jäljempänä 20 artiklan 1 kohdassa ja 21 artiklan 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointikertomusten analysointi;

c) muille valvontaelimille ja yleisölle tiedottaminen tietoturvaloukkauksista tai eheyden menetyksistä 19 artiklan 2 kohdan mukaisesti;

d) komissiolle tiedottaminen valvontaelimen tärkeimmistä toimista tämän artiklan 6 kohdan mukaisesti;

e) tarkastusten tekeminen tai vaatimustenmukaisuuden arviointilaitoksen pyytäminen suorittamaan hyväksyttyjen luottamuspalvelun tarjoajien vaatimustenmukaisuuden arviointi 20 artiklan 2 kohdan mukaisesti;

f) yhteistyön tekeminen tietosuojaviranomaisten kanssa erityisesti tiedottamalla niille ilman aiheetonta viivytystä hyväksyttyjä luottamuspalvelun tarjoajia koskevien tarkastusten tuloksista, jos vaikuttaa siltä, että henkilötietojen suojaa koskevia sääntöjä on rikottu;

g) hyväksytyn aseman myöntäminen luottamuspalvelujen tarjoajille ja niiden tarjoamille palveluille sekä kyseisen aseman peruuttaminen 20 ja 21 artiklan mukaisesti;

h) jäljempänä 22 artiklan 3 kohdassa tarkoitetusta kansallisesta luotetusta luettelosta vastaavalle elimelle tiedottaminen hyväksytyn aseman myöntämistä tai peruuttamista koskevista päätöksistään, ellei tämä elin ole myös valvontaelin;

i) lopettamissuunnitelmia koskevien säännösten olemassaolon ja asianmukaisen soveltamisen tarkistaminen tapauksissa, joissa hyväksytty luottamuspalvelun tarjoaja lopettaa toimintansa, 24 artiklan 2 kohdan h alakohdan mukainen tiedon saatavilla pitäminen mukaan lukien;

j) sen edellyttäminen, että luottamuspalvelun tarjoajat korjaavat mahdolliset puutteet tässä asetuksessa säädettyjen vaatimusten täyttämisessä.

5. Jäsenvaltiot voivat vaatia, että valvontaelin perustaa luottamusinfrastruktuurin ja pitää sitä yllä sekä saattaa sen ajan tasalle kansallisen lain edellytysten mukaisesti.

6. Kunkin valvontaelimen on toimitettava komissiolle joka vuosi viimeistään 31 päivänä maaliskuuta kertomus tärkeimmistä toimistaan edellisenä kalenterivuonna sekä tiivistelmä luottamuspalvelun tarjoajilta 19 artiklan 2 kohdan mukaisesti saaduista loukkausilmoituksista.

7. Komissio asettaa 6 kohdassa tarkoitetun vuosikertomuksen jäsenvaltioiden saataville.

8. Komissio voi täytäntöönpanosäädöksillä määritellä 6 kohdassa tarkoitettuun kertomukseen liittyvät muotoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

18 artikla

Keskinäinen avunanto

1. Valvontaelinten on tehtävä yhteistyötä hyvien käytänteiden vaihtamiseksi.

Valvontaelimen on vastaanotettuaan toisen valvontaelimen perustellun pyynnön annettava tälle apua niin, että valvontaelinten toimintaa voidaan harjoittaa johdonmukaisesti. Keskinäinen avunanto voi kattaa erityisesti tietopyynnöt ja valvontatoimet, kuten pyynnöt suorittaa 20 ja 21 artiklassa tarkoitettuihin vaatimustenmukaisuuden arviointikertomuksiin liittyviä selvityksiä.

2. Valvontaelin, jolle avunantopyyntö on osoitettu, voi kieltäytyä noudattamasta pyyntöä millä hyvänsä seuraavalla perusteella:

a) valvontaelimellä ei ole toimivaltaa antaa pyydettyä apua;

b) pyydetty apu ei ole oikeassa suhteessa valvontaelimen 17 artiklan mukaisesti toteuttamiin valvontatehtäviin;

c) pyydetyn avun antaminen olisi ristiriidassa tämän asetuksen kanssa.

3. Jäsenvaltiot voivat tarvittaessa valtuuttaa asianomaiset valvontaelimensä toteuttamaan yhteisselvityksiä, joihin osallistuu henkilöstöä muiden jäsenvaltioiden valvontaelimistä. Asianomaiset jäsenvaltiot hyväksyvät ja ottavat käyttöön tällaisia yhteisiä toimia koskevat järjestelyt ja menettelyt kansallisen lakinsa mukaisesti.

19 artikla

Luottamuspalvelun tarjoajiin sovellettavat tietoturvavaatimukset

1. Hyväksyttyjen ja ei-hyväksyttyjen luottamuspalvelun tarjoajien on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet hallitakseen tarjoamiensa luottamuspalvelujen tietoturvaan kohdistuvat riskit. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu tietoturvataso, ottaen huomioon uusin tekninen kehitys. Erityisesti on toteutettava toimenpiteet tietoturvapoikkeamien vaikutusten ehkäisemiseksi ja minimoimiseksi sekä tällaisten mahdollisten poikkeamien haittavaikutusten ilmoittamiseksi sidosryhmille.

2. Hyväksyttyjen ja ei-hyväksyttyjen luottamuspalvelun tarjoajien on ilman aiheetonta viivytystä mutta joka tapauksessa 24 tunnin kuluessa siitä, kun asia on tullut niiden tietoon, ilmoitettava valvontaelimelle ja tarvittaessa muille asianomaisille elimille, kuten toimivaltaiselle tietoturvasta vastaavalle kansalliselle elimelle tai tietosuojaviranomaiselle, kaikista tietoturvaloukkauksista ja eheyden menetyksistä, joilla on huomattavia vaikutuksia tarjottuun luottamuspalveluun tai sen puitteissa ylläpidettyihin henkilötietoihin.

Jos on todennäköistä, että tietoturvaloukkaus tai eheyden menetys vaikuttaa haitallisesti luonnolliseen henkilöön tai oikeushenkilöön, jolle luottamuspalvelu on tarjottu, luottamuspalvelun tarjoajan on myös tiedotettava luonnolliselle henkilölle tai oikeushenkilölle tietoturvaloukkauksesta tai eheyden menetyksestä ilman aiheetonta viivytystä.

Tarvittaessa ja erityisesti silloin, kun tietoturvaloukkaus tai eheyden menetys koskee kahta tai useampaa jäsenvaltiota, ilmoitetun valvontaelimen on tiedotettava asiasta muiden asianomaisten jäsenvaltioiden valvontaelimille ja ENISAlle.

Ilmoitetun valvontaelimen on tiedotettava asiasta yleisölle tai vaadittava luottamuspalvelun tarjoajaa tiedottamaan siitä, jos se katsoo, että tietoturvaloukkauksen tai eheyden menetyksen julkistaminen on yleisen edun mukaista.

3. Valvontaelimen on toimitettava ENISAlle kerran vuodessa tiivistelmä luottamuspalvelun tarjoajilta saamistaan tietoturvaloukkausta tai eheyden menetystä koskevista ilmoituksista.

4. Komissio voi täytäntöönpanosäädöksillä:

a) määrittää 1 kohdassa tarkoitetut toimenpiteet tarkemmin; ja

b) määritellä 2 kohdan soveltamiseen liittyvät muotoseikat ja menettelyt, mukaan lukien määräajat.

Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

3 JAKSO

Hyväksytyt luottamuspalvelut

20 artikla

Hyväksyttyjen luottamuspalvelun tarjoajien valvonta

1. Vaatimustenmukaisuuden arviointilaitoksen on tarkastettava hyväksytyt luottamuspalvelun tarjoajat vähintään 24 kuukauden välein niiden omalla kustannuksella. Tarkastuksen tarkoituksena on vahvistaa, että hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset. Hyväksyttyjen luottamuspalvelun tarjoajien on toimitettava tarkastuksen perusteella laadittava vaatimustenmukaisuuden arviointikertomus valvontaelimelle kolmen työpäivän kuluessa sen vastaanottamisesta.

2. Valvontaelin voi milloin tahansa tehdä hyväksytyille luottamuspalvelun tarjoajille tarkastuksia tai pyytää vaatimustenmukaisuuden arviointilaitosta suorittamaan hyväksyttyjä luottamuspalvelun tarjoajia koskevan vaatimustenmukaisuuden arvioinnin näiden hyväksyttyjen luottamuspalvelun tarjoajien kustannuksella sen vahvistamiseksi, että ne ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset, sanotun kuitenkaan rajoittamatta 1 kohdan soveltamista. Jos näyttää siltä, että henkilötietojen suojaan liittyviä sääntöjä on rikottu, valvontaelimen on ilmoitettava tarkastustensa tuloksista tietosuojaviranomaisille.

3. Jos valvontaelin vaatii hyväksyttyä luottamuspalvelun tarjoajaa korjaamaan mahdollisen laiminlyönnin tämän asetuksen mukaisten vaatimusten noudattamisessa ja jos kyseinen palvelun tarjoaja ei toimi pyynnön mukaisesti ja valvontaelimen tapauksen mukaan asettaman aikarajan puitteissa, valvontaelin voi erityisesti laiminlyönnin laajuuden, keston ja seuraukset huomioon ottaen perua kyseisen palvelun tarjoajan tai sen tarjoaman puutteellisen palvelun hyväksytyn aseman ja tiedottaa 22 artiklan 3 kohdassa tarkoitetulle elimelle asiasta 22 artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden ajan tasalle saattamista varten. Valvontaelin ilmoittaa hyväksytylle luottamuspalvelun tarjoajalle sen hyväksytyn aseman tai asianomaisen palvelun hyväksytyn aseman perumisesta.

4. Komissio voi täytäntöönpanosäädöksin vahvistaa viitenumeron seuraavia standardeja varten:

a) edellä 1 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitosten akkreditointi ja vaatimustenmukaisuuden arviointikertomus;

b) tarkastusta koskevat säännöt, joiden mukaisesti vaatimustenmukaisuuden arviointilaitokset suorittavat 1 kohdassa tarkoitetun hyväksyttyjen luottamuspalvelun tarjoajien vaatimustenmukaisuuden arvioinnin.

Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

21 artikla

Hyväksytyn luottamuspalvelun aloittaminen

1. Jos luottamuspalvelun tarjoajat, joilla ei ole hyväksyttyä asemaa, aikovat tarjota hyväksyttyjä luottamuspalveluja, niiden on toimitettava valvontaelimelle ilmoitus aikomuksestaan yhdessä vaatimustenmukaisuuden arviointilaitoksen myöntämän vaatimustenmukaisuuden arviointikertomuksen kanssa.

2. Valvontaelin tarkastaa, täyttävätkö luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut tässä asetuksessa säädetyt vaatimukset ja erityisesti hyväksyttyjä luottamuspalvelun tarjoajia ja niiden tarjoamia hyväksyttyjä luottamuspalveluja koskevat vaatimukset.

Jos valvontaelin päättää, että luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut täyttävät ensimmäisessä alakohdassa tarkoitetut vaatimukset, valvontaelimen on myönnettävä luottamuspalvelun tarjoajalle ja sen tarjoamille luottamuspalveluille hyväksytty asema sekä ilmoitettava asiasta 22 artiklan 3 kohdassa tarkoitetulle elimelle 22 artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden ajan tasalle saattamista varten viimeistään kolmen kuukauden kuluttua tämän artiklan 1 kohdan mukaisesta ilmoituksesta.

Jos tarkastusta ei saada päätökseen kolmen kuukauden kuluessa ilmoituksesta, valvontaelimen on ilmoitettava asiasta luottamuspalvelun tarjoajalle ja yksilöitävä viivästyksen syyt ja ajanjakso, jonka aikana tarkastus on saatava päätökseen.

3. Hyväksytyt luottamuspalvelun tarjoajat voivat ryhtyä tarjoamaan hyväksyttyä luottamuspalvelua sen jälkeen kun hyväksytty asema on merkitty 22 artiklan 1 kohdassa tarkoitettuihin luotettuihin luetteloihin.

4. Komissio voi täytäntöönpanosäädöksillä määritellä 1 ja 2 kohdan soveltamiseen liittyvät muotoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

22 artikla

Luotetut luettelot

1. Kunkin jäsenvaltion on laadittava, ylläpidettävä ja julkaistava luotettuja luetteloja, jotka sisältävät tietoa niiden vastuulle kuuluvista hyväksytyistä luottamuspalvelun tarjoajista ja niiden tarjoamista hyväksytyistä luottamuspalveluista.

2. Jäsenvaltioiden on laadittava, ylläpidettävä ja julkaistava suojatusti 1 kohdassa tarkoitetut sähköisesti allekirjoitetut tai leimatut luotetut luettelot muodossa, joka soveltuu automaattiseen käsittelyyn.

3. Jäsenvaltioiden on ilman aiheetonta viivytystä ilmoitettava komissiolle tiedot kansallisten luotettujen luettelojen laatimisesta, ylläpitämisestä ja julkaisemisesta vastaavasta elimestä sekä yksityiskohtaiset tiedot tällaisten luettelojen julkaisupaikasta, luotettujen luettelojen allekirjoittamisessa tai leimaamisessa käytetyistä varmenteista ja niiden tietojen mahdollisista muutoksista.

4. Komissio asettaa julkisesti saataville suojatusti 3 kohdassa tarkoitetut tiedot sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.

5. Komissio täsmentää viimeistään 18 päivänä syyskuuta 2015 täytäntöönpanosäädöksillä 1 kohdassa tarkoitetut tiedot ja määrittelee 1–4 kohdan soveltamiseen liittyvät luotettujen luetteloiden tekniset eritelmät ja muotoseikat. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

23 artikla

Hyväksyttyjä luottamuspalveluja koskeva EU:n luotettavuusmerkki

1. Sen jälkeen kun 21 artiklan 2 kohdan toisessa alakohdassa tarkoitettu hyväksytty asema on merkitty 22 artiklan 1 kohdassa tarkoitettuihin luotettuihin luetteloihin, hyväksytyt luottamuspalvelun tarjoajat voivat käyttää EU:n luotettavuusmerkkiä osoittaakseen yksinkertaisella, tunnistettavalla ja selkeällä tavalla niiden tarjoamat hyväksytyt luottamuspalvelut.

2. Käyttäessään EU:n luotettavuusmerkkiä 1 kohdassa tarkoitettujen hyväksyttyjen luottamuspalvelujen yhteydessä hyväksyttyjen luottamuspalvelun tarjoajien on varmistettava, että niiden verkkosivulla on käytettävissä linkki asianomaiseen luotettuun luetteloon.

3. Komissio vahvistaa viimeistään 1 päivänä heinäkuuta 2015 täytäntöönpanosäädöksillä eritelmät hyväksyttyjä luottamuspalveluja koskevan EU:n luotettavuusmerkin muodosta ja erityisesti sen esittämistavasta, koostumuksesta, koosta ja mallista. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

24 artikla

Hyväksyttyjä luottamuspalvelun tarjoajia koskevat vaatimukset

1. Hyväksytyn luottamuspalvelun tarjoajan on myöntäessään hyväksyttyä varmennetta luottamuspalvelulle tarkastettava asianmukaisin menetelmin ja kansallisen lain mukaisesti sen luonnollisen henkilön tai oikeushenkilön henkilöllisyys ja mahdolliset muut attribuutit, jolle hyväksytty varmenne myönnetään.

Ensimmäisessä alakohdassa tarkoitetut tiedot on tarkastettava hyväksytyn luottamuspalvelun tarjoajan toimesta joko suoraan tai kolmatta osapuolta käyttäen kansallisen lain mukaisesti:

a) luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan läsnä ollessa; tai

b) etäältä käyttäen sähköisen tunnistamisen menetelmää, jonka osalta on ennen hyväksytyn varmenteen myöntämistä varmistettu luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan läsnäolo ja joka täyttää 8 artiklassa säädetyt ”korotettua” tai ”korkeaa” varmuustasoa koskevat vaatimukset; tai

c) käyttäen a tai b alakohdan mukaisesti myönnettyä hyväksytyn sähköisen allekirjoituksen tai hyväksytyn sähköisen leiman varmennetta; tai

d) käyttäen muita kansallisella tasolla hyväksyttyjä tunnistamismenetelmiä, jotka tarjoavat fyysistä läsnäoloa vastaavan varmuuden. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava varmuuden vastaavuus.

2. Hyväksyttyjä luottamuspalveluja tarjoavan hyväksytyn luottamuspalvelun tarjoajan on

a) ilmoitettava valvontaelimelle kaikista muutoksista hyväksyttyjen luottamuspalvelujensa tarjoamisessa sekä aikomuksesta lopettaa tämä toiminta;

b) palkattava henkilöstöä ja tarvittaessa alihankkijoita, joilla on tarvittava asiantuntemus, luotettavuus, kokemus ja pätevyys ja jotka ovat saaneet tarvittavaa koulutusta tietoturvaa ja henkilötietojen suojaa koskevista säännöistä, ja noudatettava eurooppalaisia tai kansainvälisiä standardeja vastaavia hallinnollisia menettelyjä ja johtamismenettelyjä;

c) ylläpidettävä 13 artiklan mukaisen vahinkovastuun riskin suhteen riittäviä taloudellisia varoja ja/tai hankittava asianmukainen vastuuvakuutus kansallisen lain mukaisesti;

d) ilmoitettava ennen sopimussuhteen aloittamista henkilöille, jotka haluavat käyttää hyväksyttyä luottamuspalvelua, selkeästi ja kattavasti kyseisen palvelun käytön tarkoista ehdoista ja edellytyksistä, muun muassa sen käyttöä koskevista rajoituksista;

e) käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta ja joilla varmistetaan niiden tukemien prosessien tekninen tietoturva ja luotettavuus;

f) käytettävä luotettavia järjestelmiä sille annettujen tietojen tallentamiseen tarkastettavissa olevassa muodossa siten, että

i) tiedot ovat julkisesti haettavissa vain, jos siihen on saatu tietojen kohteena olevan henkilön suostumus,

ii) ainoastaan valtuutetut henkilöt voivat syöttää tietoja ja tehdä muutoksia tallennettuihin tietoihin,

iii) tietojen aitous voidaan tarkastaa;

g) toteutettava tarkoituksenmukaisia toimenpiteitä tietojen väärentämisen ja varastamisen estämiseksi;

h) arkistoitava ja pidettävä saatavilla asianmukaisen ajan, myös sen jälkeen kun hyväksytyn luottamuspalvelun tarjoajan toiminta on lakannut, kaikki tarvittavat tiedot hyväksytyn luottamuspalvelun tarjoajan myöntämistä ja vastaanottamista tiedoista, erityisesti käytettäväksi todisteena oikeudellisissa käsittelyissä ja palvelun jatkuvuuden varmistamiseksi. Tällaisia arkistoja voidaan ylläpitää sähköisessä muodossa;

i) ylläpidettävä ajan tasalla olevaa toiminnan lopettamissuunnitelmaa, jotta voidaan varmistaa palvelun jatkuvuus valvontaelimen 17 artiklan 4 kohdan i alakohdan nojalla tarkastamien säännösten mukaisesti;

j) varmistettava, että henkilötietoja käsitellään lainmukaisesti direktiiviä 95/46/EY noudattaen;

k) kun kyse on hyväksyttyjä varmenteita myöntävistä hyväksytyistä luottamuspalvelun tarjoajista, perustettava varmennetietokanta ja pidettävä se ajan tasalla.

3. Jos hyväksyttyjä varmenteita myöntävä hyväksytty luottamuspalvelujen tarjoaja päättää sulkea varmenteen, sen on kirjattava kyseinen sulkeminen varmennetietokantaansa ja julkaistava varmenteen sulkemistila oikea-aikaisesti ja joka tapauksessa 24 tunnin kuluessa pyynnön vastaanottamisesta. Sulkeminen tulee voimaan välittömästi sen julkaisemisen yhteydessä.

4. Hyväksyttyjä varmenteita myöntävien hyväksyttyjen luottamuspalvelun tarjoajien on 3 kohtaan liittyen annettava kaikille luottaville osapuolille tietoa niiden myöntämien hyväksyttyjen varmenteiden voimassaolo- tai sulkemistilasta. Tämä tieto on asetettava saataville ainakin varmennekohtaisesti jatkuvasti ja myös varmenteen voimassaolon päätyttyä automaattisella tavalla, joka on luotettava, maksuton ja tehokas.

5. Komissio voi täytäntöönpanosäädöksin vahvistaa tämän artiklan 2 kohdan e ja f alakohdan vaatimukset täyttäviin luotettaviin järjestelmiin ja tuotteisiin sovellettavien standardien viitenumerot. Jos luotettava järjestelmä tai tuote vastaa näitä standardeja, sen katsotaan olevan tässä artiklassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

4 JAKSO

Sähköiset allekirjoitukset

25 artikla

Sähköisten allekirjoitusten oikeusvaikutukset

1. Sähköisen allekirjoituksen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen sähköisten allekirjoitusten vaatimuksia.

2. Hyväksytyllä sähköisellä allekirjoituksella on oltava samanlaiset oikeusvaikutukset kuin käsin kirjoitetulla allekirjoituksella.

3. Yhdessä jäsenvaltiossa myönnettyyn hyväksyttyyn varmenteeseen perustuva hyväksytty sähköinen allekirjoitus on tunnustettava hyväksytyksi sähköiseksi allekirjoitukseksi kaikissa muissa jäsenvaltioissa.

26 artikla

Kehittyneen sähköisen allekirjoituksen vaatimukset

Kehittyneen sähköisen allekirjoituksen on täytettävä seuraavat vaatimukset:

a) se liittyy yksilöivästi allekirjoittajaansa;

b) sillä voidaan yksilöidä allekirjoittaja;

c) se on luotu käyttäen sähköisen allekirjoituksen luontitietoja, joita allekirjoittaja voi korkealla varmuustasolla käyttää yksinomaisessa valvonnassaan; ja

d) se on liitetty sillä allekirjoitettuun tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

27 artikla

Sähköiset allekirjoitukset julkisissa palveluissa

1. Jos jäsenvaltio vaatii kehittynyttä sähköistä allekirjoitusta julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava ainakin ne kehittyneet sähköiset allekirjoitukset, sähköisten allekirjoitusten hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset sekä hyväksytyt sähköiset allekirjoitukset, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.

2. Jos jäsenvaltio vaatii hyväksyttyyn varmenteeseen perustuvaa kehittynyttä sähköistä allekirjoitusta julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava ainakin ne hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset sekä hyväksytyt sähköiset allekirjoitukset, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.

3. Jäsenvaltiot eivät saa vaatia julkisen sektorin elimen tarjoaman verkkopalvelun käytössä rajojen yli sähköistä allekirjoitusta, jonka tietoturvataso on korkeampi kuin hyväksytyn sähköisen allekirjoituksen.

4. Komissio voi täytäntöönpanosäädöksin vahvistaa kehittyneisiin sähköisiin allekirjoituksiin sovellettavien standardien viitenumerot. Jos kehittynyt sähköinen allekirjoitus vastaa kyseisiä standardeja, sen katsotaan olevan tämän artiklan 1 ja 2 kohdassa sekä 26 artiklassa tarkoitettujen kehittyneitä sähköisiä allekirjoituksia koskevien vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5. Komissio määrittelee kehittyneitä sähköisiä allekirjoituksia koskevat viitemuodot tai, jos käytetään vaihtoehtoisia muotoja, viitemenetelmät täytäntöönpanosäädöksillä viimeistään 18 päivänä syyskuuta 2015 ottaen huomioon olemassa olevat käytännöt, standardit ja unionin säädökset. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

28 artikla

Sähköisten allekirjoitusten hyväksytyt varmenteet

1. Sähköisten allekirjoitusten hyväksyttyjen varmenteiden on täytettävä liitteessä I säädetyt vaatimukset.

2. Sähköisten allekirjoitusten hyväksytyille varmenteille ei saa asettaa pakollisia vaatimuksia, jotka ylittävät liitteessä I säädetyt vaatimukset.

3. Sähköisten allekirjoitusten hyväksyttyihin varmenteisiin voi sisältyä erityisiä valinnaisia lisäattribuutteja. Kyseiset attribuutit eivät vaikuta hyväksyttyjen sähköisten allekirjoitusten yhteentoimivuuteen ja tunnustamiseen.

4. Jos sähköisten allekirjoitusten hyväksytty varmenne on ensimmäisen aktivoinnin jälkeen suljettu, sen voimassaolo päättyy sulkemisajankohdasta lähtien, eikä sen tilaa voida missään olosuhteissa palauttaa.

5. Jäsenvaltiot voivat vahvistaa kansallisia sääntöjä sähköisen allekirjoituksen hyväksytyn varmenteen voimassaolon väliaikaisesta keskeyttämisestä seuraavin edellytyksin:

a) jos sähköisen allekirjoituksen hyväksytyn varmenteen voimassaolo on väliaikaisesti keskeytetty, kyseisen varmenteen voimassaolo päättyy keskeyttämisen ajaksi;

b) keskeyttämisen kesto on ilmoitettava selvästi varmennetietokannassa ja keskeytystilan on käytävä keskeyttämisen keston ajan näkyvästi ilmi palvelusta, joka tarjoaa tietoja varmenteen tilasta.

6. Komissio voi täytäntöönpanosäädöksin vahvistaa sähköisen allekirjoituksen hyväksyttyihin varmenteisiin sovellettavien standardien viitenumerot. Jos sähköisen allekirjoituksen hyväksytty varmenne vastaa kyseisiä standardeja, sen katsotaan olevan liitteessä I säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

29 artikla

Hyväksyttyjä sähköisen allekirjoituksen luontivälineitä koskevat vaatimukset

1. Hyväksyttyjen sähköisen allekirjoituksen luontivälineiden on täytettävä liitteessä II säädetyt vaatimukset.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa hyväksyttyihin sähköisen allekirjoituksen luontivälineisiin sovellettavien standardien viitenumerot. Jos hyväksytty sähköisen allekirjoituksen luontiväline vastaa kyseisiä standardeja, sen katsotaan olevan liitteessä II säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

30 artikla

Hyväksyttyjen sähköisen allekirjoituksen luontivälineiden sertifiointi

1. Jäsenvaltioiden nimeämien asianmukaisten julkisten tai yksityisten tahojen on sertifioitava hyväksyttyjen sähköisen allekirjoituksen luontivälineiden vaatimustenmukaisuus liitteessä II säädettyjen vaatimusten kanssa.

2. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitetun julkisen tai yksityisen tahon nimi ja osoite. Komissio asettaa nämä tiedot jäsenvaltioiden saataville.

3. Edellä 1 kohdassa tarkoitettu sertifiointi perustuu toiseen seuraavista:

a) tietoturvan arviointiprosessi, joka on tehty noudattaen jotakin toisen alakohdan mukaisesti vahvistettuun luetteloon sisältyvää tietoteknisten tuotteiden tietoturva-arviointia koskevaa standardia; tai

b) muu kuin a alakohdassa tarkoitettu prosessi, edellyttäen että siinä käytetään vertailukelpoisia tietoturvatasoja ja että 1 kohdassa tarkoitettu julkinen tai yksityinen taho ilmoittaa menettelystä komissiolle. Tätä prosessia voidaan käyttää ainoastaan, jos a alakohdassa tarkoitetut standardit puuttuvat tai jos a alakohdassa tarkoitetun tietoturvan arviointiprosessin suorittaminen on kesken.

Komissio vahvistaa täytäntöönpanosäädöksillä luettelon a alakohdassa tarkoitettua tietoteknisten tuotteiden tietoturva-arviointia koskevista standardeista. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

4. Siirretään komissiolle valta antaa 47 artiklan mukaisesti delegoituja säädöksiä, jotka koskevat tämän artiklan 1 kohdassa tarkoitetuille nimetyille tahoille asetettavia erityisvaatimuksia.

31 artikla

Sertifioitujen hyväksyttyjen sähköisen allekirjoituksen luontivälineiden luettelon julkaiseminen

1. Jäsenvaltioiden on ilman aiheetonta viivytystä ja viimeistään kuukauden kuluttua sertifioinnin saattamisesta päätökseen ilmoitettava komissiolle tiedot 30 artiklan 1 kohdassa tarkoitettujen tahojen sertifioimista hyväksytyistä sähköisen allekirjoituksen luontivälineistä. Niiden on ilman aiheetonta viivytystä ja viimeistään kuukauden kuluttua sertifioinnin peruuttamisesta ilmoitettava komissiolle myös tiedot sähköisen allekirjoituksen luontivälineistä, joita ei enää sertifioida.

2. Saamiensa tietojen perusteella komissio laatii ja julkaisee luettelon sertifioiduista hyväksytyistä sähköisen allekirjoituksen luontivälineistä sekä ylläpitää sitä.

3. Komissio voi täytäntöönpanosäädöksillä määritellä 1 kohdan soveltamiseen liittyvät muotoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

32 artikla

Hyväksyttyjen sähköisten allekirjoitusten validointia koskevat vaatimukset

1. Hyväksytyn sähköisen allekirjoituksen validointiprosessilla vahvistetaan hyväksytyn sähköisen allekirjoituksen pätevyys, edellyttäen että:

a) allekirjoitusta tukeva varmenne oli allekirjoitushetkellä liitteen I mukainen hyväksytty sähköisen allekirjoituksen varmenne;

b) hyväksytyn varmenteen on myöntänyt hyväksytty luottamuspalvelun tarjoaja ja se oli voimassa allekirjoitushetkellä;

c) allekirjoituksen validointitiedot vastaavat luottavalle osapuolelle annettuja tietoja;

d) varmenteen allekirjoittajaa edustava yksilöivä tietokokonaisuus on annettu oikein luottavalle osapuolelle;

e) jos allekirjoitushetkellä on käytetty salanimeä, sen käytöstä on selkeästi ilmoitettu luottavalle osapuolelle;

f) sähköinen allekirjoitus on luotu hyväksytyllä sähköisen allekirjoituksen luontivälineellä;

g) allekirjoitettujen tietojen eheyttä ei ole loukattu;

h) edellä 26 artiklassa säädetyt vaatimukset täyttyivät allekirjoitushetkellä.

2. Hyväksytyn sähköisen allekirjoituksen validointiin käytettävän järjestelmän on annettava luottavalle osapuolelle validointiprosessissa oikea tulos, ja sen on annettava luottavalle osapuolelle mahdollisuus huomata mahdolliset tietoturvaan vaikuttavat poikkeamat.

3. Komissio voi täytäntöönpanosäädöksin vahvistaa hyväksyttyjen sähköisten allekirjoitusten validointiin sovellettavien standardien viitenumerot. Jos hyväksyttyjen sähköisten allekirjoitusten validointi vastaa kyseisiä standardeja, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

33 artikla

Hyväksyttyjen sähköisten allekirjoitusten hyväksytty validointipalvelu

1. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä validointipalvelua voi tarjota ainoastaan hyväksytty luottamuspalvelun tarjoaja, joka:

a) tarjoaa validointia 32 artiklan 1 kohdan mukaisesti ja

b) tarjoaa luottaville osapuolille validointiprosessin tuloksen automaattisesti tavalla, joka on luotettava ja tehokas ja joka sisältää hyväksytyn validointipalvelun tarjoajan kehittyneen sähköisen allekirjoituksen tai kehittyneen sähköisen leiman.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa 1 kohdassa tarkoitettuun hyväksyttyyn validointipalveluun sovellettavien standardien viitenumerot. Jos hyväksyttyjen sähköisten allekirjoitusten validointipalvelu vastaa kyseisiä standardeja, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

34 artikla

Hyväksyttyjen sähköisten allekirjoitusten hyväksytty säilyttämispalvelu

1. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua voi tarjota ainoastaan hyväksytty luottamuspalvelun tarjoaja, jonka käyttämät menettelyt ja teknologiat ovat sellaisia, että niillä voidaan jatkaa hyväksytyn sähköisen allekirjoituksen luotettavuutta senkin jälkeen, kun niiden teknologinen luotettavuusaika on päättynyt.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa hyväksyttyjen sähköisten allekirjoitusten hyväksyttyyn säilyttämispalveluun sovellettavien standardien viitenumerot. Jos hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua koskevat järjestelyt vastaavat kyseisiä standardeja, 1 kohdassa säädettyjen vaatimusten mukaisuuden katsotaan täyttyvän. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5 JAKSO

Sähköiset leimat

35 artikla

Sähköisten leimojen oikeusvaikutukset

1. Sähköisen leiman oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen sähköisten leimojen vaatimuksia.

2. Hyväksyttyyn sähköiseen leimaan liitetään olettama tietojen eheydestä ja niiden tietojen alkuperän oikeellisuudesta, joihin hyväksytty sähköinen leima on liitetty.

3. Yhdessä jäsenvaltiossa myönnettyyn hyväksyttyyn varmenteeseen perustuva hyväksytty sähköinen leima on tunnustettava hyväksytyksi sähköiseksi leimaksi kaikissa muissa jäsenvaltioissa.

36 artikla

Kehittyneitä sähköisiä leimoja koskevat vaatimukset

Kehittyneen sähköisen leiman on täytettävä seuraavat vaatimukset:

a) se liittyy yksilöivästi leiman luojaan;

b) sillä voidaan yksilöidä leiman luoja;

c) se on luotu käyttäen sähköisen leiman luontitietoja, joita leiman luoja voi korkealla varmuustasolla käyttää valvonnassaan sähköisen leiman luomiseen; ja

d) se on liitetty kohteenaan olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

37 artikla

Sähköiset leimat julkisissa palveluissa

1. Jos jäsenvaltio vaatii kehittynyttä sähköistä leimaa julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava vähintään kehittyneet sähköiset leimat, sähköisten leimojen hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset leimat sekä hyväksytyt sähköiset leimat, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.

2. Jos jäsenvaltio vaatii hyväksyttyyn varmenteeseen perustuvaa kehittynyttä sähköistä leimaa julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava ainakin hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset leimat sekä hyväksytyt sähköiset leimat, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.

3. Jäsenvaltiot eivät saa vaatia julkisen sektorin elimen tarjoaman verkkopalvelun käytössä rajojen yli sähköistä leimaa, jonka tietoturvataso on korkeampi kuin hyväksytyn sähköisen leiman.

4. Komissio voi täytäntöönpanosäädöksin vahvistaa kehittyneisiin sähköisiin leimoihin sovellettavien standardien viitenumerot. Jos kehittynyt sähköinen leima vastaa kyseisiä standardeja, sen katsotaan olevan tämän artiklan 1 ja 2 kohdassa sekä 36 artiklassa tarkoitettujen kehittyneitä sähköisiä leimoja koskevien vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5. Komissio määrittelee kehittyneitä sähköisiä leimoja koskevat viitemuodot tai, jos käytetään vaihtoehtoisia muotoja, viitemenetelmät täytäntöönpanosäädöksillä viimeistään 18 päivänä syyskuuta 2015 ottaen huomioon olemassa olevat käytännöt, standardit ja unionin säädökset. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

38 artikla

Sähköisten leimojen hyväksytyt varmenteet

1. Sähköisten leimojen hyväksyttyjen varmenteiden on täytettävä liitteessä III säädetyt vaatimukset.

2. Sähköisten leimojen hyväksytyille varmenteille ei saa asettaa pakollisia vaatimuksia, jotka ylittävät liitteessä III säädetyt vaatimukset.

3. Sähköisten leimojen hyväksyttyihin varmenteisiin voi sisältyä erityisiä valinnaisia lisäattribuutteja. Kyseiset attribuutit eivät vaikuta hyväksyttyjen sähköisten leimojen yhteentoimivuuteen ja tunnustamiseen.

4. Jos sähköisen leiman hyväksytty varmenne on ensimmäisen aktivoinnin jälkeen suljettu, sen voimassaolo päättyy sulkemisajankohdasta lähtien, eikä sen tilaa voida missään olosuhteissa palauttaa.

5. Jäsenvaltiot voivat vahvistaa kansallisia sääntöjä sähköisten leimojen hyväksyttyjen varmenteiden voimassaolon väliaikaisesta keskeyttämisestä seuraavin edellytyksin:

a) jos sähköisen leiman hyväksytyn varmenteen voimassaolo on väliaikaisesti keskeytetty, kyseisen varmenteen voimassaolo päättyy keskeyttämisen ajaksi;

b) keskeyttämisen kesto on ilmoitettava selvästi varmennetietokannassa, ja keskeytystilan on käytävä keskeyttämisen keston ajan näkyvästi ilmi palvelusta, joka tarjoaa tietoja varmenteen tilasta.

6. Komissio voi täytäntöönpanosäädöksin vahvistaa sähköisten leimojen hyväksyttyihin varmenteisiin sovellettavien standardien viitenumerot. Jos sähköisen leiman hyväksytty varmenne vastaa kyseisiä standardeja, sen katsotaan olevan liitteessä III säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

39 artikla

Hyväksytyt sähköisen leiman luontivälineet

1. Hyväksytyille sähköisen leiman luontivälineille asetettavien vaatimusten osalta sovelletaan soveltuvin osin 29 artiklaa.

2. Hyväksyttyjen sähköisen leiman luontivälineiden sertifioinnin osalta sovelletaan soveltuvin osin 30 artiklaa.

3. Sertifioitujen hyväksyttyjen sähköisen leiman luontivälineiden luettelon julkaisemisen osalta sovelletaan soveltuvin osin 31 artiklaa.

40 artikla

Hyväksyttyjen sähköisten leimojen validointi ja säilyttäminen

Hyväksyttyjen sähköisten leimojen validointiin ja säilyttämiseen sovelletaan soveltuvin osin 32, 33 ja 34 artiklaa.

6 JAKSO

Sähköiset aikaleimat

41 artikla

Sähköisten aikaleimojen oikeusvaikutukset

1. Sähköisen aikaleiman oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyn sähköisen aikaleiman vaatimuksia.

2. Hyväksyttyyn sähköiseen aikaleimaan liitetään olettama aikaleiman osoittaman päivän ja ajankohdan oikeellisuudesta sekä päivään ja ajankohtaan sidottujen tietojen eheydestä.

3. Yhdessä jäsenvaltiossa myönnetty hyväksytty sähköinen aikaleima on tunnustettava hyväksytyksi sähköiseksi aikaleimaksi kaikissa jäsenvaltioissa.

42 artikla

Hyväksyttyjä sähköisiä aikaleimoja koskevat vaatimukset

1. Hyväksytyn sähköisen aikaleiman on täytettävä seuraavat vaatimukset:

a) se sitoo tiedot päivään ja ajankohtaan niin, että voidaan kohtuudella sulkea pois mahdollisuus, että tietoja olisi muutettu huomaamatta;

b) se perustuu virheettömään aikalähteeseen, joka on liitetty koordinoituun yleisaikaan; ja

c) se on allekirjoitettu hyväksytyn luottamuspalvelujen tarjoajan kehittyneellä sähköisellä allekirjoituksella tai leimattu tämän kehittyneellä sähköisellä leimalla tai vastaavalla menetelmällä.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa päivän ja ajankohdan sitomista tietoihin sekä virheettömiä aikalähteitä koskevien standardien viitenumerot. Jos päivän ja ajankohdan sitominen tietoihin ja virheetön aikalähde vastaavat kyseisiä standardeja, niiden katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukaiset. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

7 JAKSO

Sähköiset rekisteröidyt jakelupalvelut

43 artikla

Sähköisen rekisteröidyn jakelupalvelun oikeusvaikutukset

1. Sähköistä rekisteröityä jakelupalvelua käyttäen lähetettyjen ja vastaanotettujen tietojen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että ne ovat sähköisessä muodossa tai että ne eivät täytä hyväksytyn sähköisen rekisteröidyn jakelupalvelun vaatimuksia.

2. Hyväksyttyä sähköistä rekisteröityä jakelupalvelua käyttäen lähetettyihin ja vastaanotettuihin tietoihin liitetään oletama, jonka mukaan tiedot ovat eheitä, nämä tiedot on lähettänyt tunnistettu lähettäjä, ne on vastaanottanut tunnistettu vastaanottaja ja hyväksytyn sähköisen rekisteröidyn jakelupalvelun ilmoittama tietojen lähettämisen ja vastaanottamisen päivämäärä ja kellonaika on oikea.

44 artikla

Hyväksyttyjä sähköisiä rekisteröityjä jakelupalveluja koskevat vaatimukset

1. Hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen on täytettävä seuraavat vaatimukset:

a) niitä tarjoaa yksi tai useampi hyväksytty luottamuspalvelun tarjoaja;

b) niissä varmistetaan korkealla varmuustasolla lähettäjän tunnistaminen;

c) niissä varmistetaan vastaanottajan tunnistaminen ennen tietojen toimittamista;

d) tietojen lähettäminen ja vastaanottaminen on suojattu hyväksytyn luottamuspalvelun tarjoajan kehittyneellä sähköisellä allekirjoituksella tai kehittyneellä sähköisellä leimalla niin, että voidaan sulkea pois mahdollisuus, että tietoja olisi muutettu huomaamatta;

e) kaikki muutokset tietojen lähettämisessä tai vastaanottamisessa tarvittavissa tiedoissa ilmoitetaan selkeästi tietojen lähettäjälle ja vastaanottajalle;

f) tietojen lähettämisen, vastaanottamisen ja muuttamisen päivämäärä ja ajankohta ilmoitetaan hyväksytyllä sähköisellä aikaleimalla.

Kun tietoja siirretään kahden tai useamman hyväksytyn luottamuspalvelun tarjoajan välillä, a–f alakohdan vaatimuksia sovelletaan kaikkiin näihin palveluntarjoajiin.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa tietojen lähettämis- ja vastaanottamisprosesseihin sovellettavien standardien viitenumerot. Jos tietojen lähettämis- ja vastaanottamisprosessi vastaa kyseisiä standardeja, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8 JAKSO

Verkkosivustojen todentaminen

45 artikla

Verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset

1. Verkkosivustojen todentamisen hyväksyttyjen varmenteiden on täytettävä liitteessä IV säädetyt vaatimukset.

2. Komissio voi täytäntöönpanosäädöksin vahvistaa verkkosivustojen todentamisen hyväksyttyihin varmenteisiin sovellettavien standardien viitenumerot. Jos verkkosivustojen todentamisen hyväksytty varmenne vastaa kyseisiä standardeja, sen katsotaan olevan liitteessä IV säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

IV LUKU

SÄHKÖISET ASIAKIRJAT

46 artikla

Sähköisten asiakirjojen oikeusvaikutukset

Sähköisen asiakirjan oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sen takia, että se on sähköisessä muodossa.

V LUKU

SÄÄDÖSVALLAN SIIRTO JA TÄYTÄNTÖÖNPANOSÄÄNNÖKSET

47 artikla

Siirretyn säädösvallan käyttäminen

1. Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.

2. Siirretään komissiolle määräämättömäksi ajaksi 17 päivästä syyskuuta 2014 30 artiklan 4 kohdassa tarkoitettu valta antaa delegoituja säädöksiä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 30 artiklan 4 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

4. Heti kun komissio on antanut delegoidun säädöksen, komissio antaa sen tiedoksi yhtäaikaisesti Euroopan parlamentille ja neuvostolle.

5. Edellä olevan 30 artiklan 4 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

48 artikla

Komiteamenettely

1. Komissiota avustaa komitea. Tämä komitea on asetuksessa (EU) N:o 182/2011 tarkoitettu komitea.

2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.

VI LUKU

LOPPUSÄÄNNÖKSET

49 artikla

Uudelleentarkastelu

Komissio tarkastelee uudelleen tämän asetuksen soveltamista ja antaa Euroopan parlamentille ja neuvostolle kertomuksen viimeistään 1 päivänä heinäkuuta 2020. Komissio arvioi erityisesti, olisiko tämän asetuksen tai sen tiettyjen säännösten, mukaan lukien 6 artikla, 7 artiklan f alakohta sekä 34, 43, 44 ja 45 artikla, soveltamisalaa asianmukaista muuttaa, ottaen huomioon tämän asetuksen soveltamisesta saatu kokemus sekä tekninen, markkinoihin liittyvä ja oikeudellinen kehitys.

Ensimmäisessä kohdassa tarkoitettuun kertomukseen liitetään tarvittaessa lainsäädäntöehdotuksia.

Lisäksi komissio antaa Euroopan parlamentille ja neuvostolle ensimmäisessä kohdassa tarkoitetun kertomuksen jälkeen neljän vuoden välein kertomuksen edistymisestä tämän asetuksen tavoitteiden saavuttamisessa.

50 artikla

Kumoaminen

1. Kumotaan direktiivi 1999/93/EY 1 päivästä heinäkuuta 2016.

2. Viittauksia kumottuun direktiiviin pidetään viittauksina tähän asetukseen.

51 artikla

Siirtymätoimenpiteet

1. Turvallisia allekirjoituksen luontivälineitä, joiden vaatimustenmukaisuus on määritetty direktiivin 1999/93/EY 3 artiklan 4 kohdan mukaisesti, pidetään tämän asetuksen mukaisina hyväksyttyinä sähköisen allekirjoituksen luontivälineinä.

2. Direktiivin 1999/93/EY mukaisesti luonnollisille henkilöille myönnettyjä hyväksyttyjä varmenteita pidetään tämän asetuksen mukaisina sähköisten allekirjoitusten hyväksyttyinä varmenteina niiden voimassaolon päättymiseen saakka.

3. Direktiivin 1999/93/EY mukaisen hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan on toimitettava valvontaelimelle vaatimustenmukaisuuden arviointikertomus mahdollisimman pian mutta viimeistään 1 päivänä heinäkuuta 2017. Kyseistä varmennepalvelujen tarjoajaa pidetään tämän asetuksen mukaisena hyväksyttynä luottamuspalvelun tarjoajana siihen saakka, kun vaatimustenmukaisuuden arviointikertomus on toimitettu ja valvontaelin on saattanut loppuun sen arvioinnin.

4. Jos direktiivin 1999/93/EY mukainen hyväksyttyjä varmenteita myöntävä varmennepalvelujen tarjoaja ei toimita valvontaelimelle vaatimustenmukaisuuden arviointikertomusta 3 kohdassa tarkoitetussa määräajassa, kyseistä varmennepalvelujen tarjoajaa ei pidetä tämän asetuksen mukaisena hyväksyttynä luottamuspalvelun tarjoajana 2 päivästä heinäkuuta 2017.

52 artikla

Voimaantulo

1. Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

2. Tätä asetusta sovelletaan 1 päivästä heinäkuuta 2016, lukuun ottamatta seuraavia säännöksiä:

a) asetuksen 8 artiklan 3 kohtaa, 9 artiklan 5 kohtaa, 12 artiklan 2–9 kohtaa, 17 artiklan 8 kohtaa, 19 artiklan 4 kohtaa, 20 artiklan 4 kohtaa, 21 artiklan 4 kohtaa, 22 artiklan 5 kohtaa, 23 artiklan 3 kohtaa, 24 artiklan 5 kohtaa, 27 artiklan 4 ja 5 kohtaa, 28 artiklan 6 kohtaa, 29 artiklan 2 kohtaa, 30 artiklan 3 ja 4 kohtaa, 31 artiklan 3 kohtaa, 32 artiklan 3 kohtaa, 33 artiklan 2 kohtaa, 34 artiklan 2 kohtaa, 37 artiklan 4 ja 5 kohtaa, 38 artiklan 6 kohtaa, 42 artiklan 2 kohtaa, 44 artiklan 2 kohtaa, 45 artiklan 2 kohtaa, 47 artiklaa ja 48 artiklaa sovelletaan 17 päivästä syyskuuta 2014;

b) asetuksen 7 artiklaa, 8 artiklan 1 ja 2 kohtaa, 9 artiklaa, 10 artiklaa, 11 artiklaa ja 12 artiklan 1 kohtaa sovelletaan 8 artiklan 3 kohdassa ja 12 artiklan 8 kohdassa tarkoitettujen täytäntöönpanosäädösten soveltamispäivästä;

c) asetuksen 6 artiklaa sovelletaan kolmen vuoden kuluttua 8 artiklan 3 kohdassa ja 12 artiklan 8 kohdassa tarkoitettujen täytäntöönpanosäädösten soveltamispäivästä.

3. Jos ilmoitettu sähköisen tunnistamisen järjestelmä sisällytetään komission 9 artiklan nojalla julkaisemaan luetteloon ennen tämän artiklan 2 kohdan c alakohdassa tarkoitettua päivää, kyseisen järjestelmän mukaiset sähköisen tunnistamisen menetelmät on tunnustettava 6 artiklan nojalla viimeistään 12 kuukauden kuluttua järjestelmän julkaisemisesta, mutta tämän artiklan 2 kohdan c alakohdassa tarkoitetun päivän jälkeen.

4. Sen estämättä, mitä tämän artiklan 2 kohdan c alakohdassa säädetään, jäsenvaltio voi päättää, että sähköisen tunnistamisen järjestelmän mukaiset toisen jäsenvaltion 9 artiklan 1 kohdan nojalla ilmoittamat sähköisen tunnistamisen menetelmät tunnustetaan ensimmäisessä jäsenvaltiossa 8 artiklan 3 kohdassa ja 12 artiklan 8 kohdassa tarkoitettujen täytäntöönpanosäädösten soveltamispäivästä alkaen. Asianomaiset jäsenvaltiot ilmoittavat asiasta komissiolle. Komissio julkistaa nämä tiedot.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 23 päivänä heinäkuuta 2014.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*
M. SCHULZ	S. GOZI

LIITE I

SÄHKÖISTEN ALLEKIRJOITUSTEN HYVÄKSYTTYJÄ VARMENTEITA KOSKEVAT VAATIMUKSET

Sähköisten allekirjoitusten hyväksyttyjen varmenteiden on sisällettävä:

a) tieto, ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa, siitä, että varmenne on myönnetty sähköisen allekirjoituksen hyväksyttynä varmenteena;

b) tietokokonaisuus, joka yksiselitteisesti edustaa hyväksytyt varmenteet myöntävää hyväksyttyä luottamuspalvelun tarjoajaa ja sisältää ainakin tiedon jäsenvaltiosta, johon tarjoaja on sijoittautunut, ja

— oikeushenkilön osalta: nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa,

— luonnollisen henkilön osalta: henkilön nimi;

c) ainakin allekirjoittajan nimi tai salanimi; jos käytetään salanimeä, tämä on ilmoitettava selvästi;

d) sähköisen allekirjoituksen validointitiedot, jotka vastaavat sen luontitietoja;

e) tiedot varmenteen voimassaoloajan alkamisesta ja päättymisestä;

f) varmenteen tunniste, jonka on oltava kyseisen hyväksytyn luottamuspalvelun tarjoajan osalta yksilöivä;

g) myöntävän hyväksytyn luottamuspalvelun tarjoajan kehittynyt sähköinen allekirjoitus tai kehittynyt sähköinen leima;

h) sijainti, josta g kohdassa tarkoitettua kehittynyttä sähköistä allekirjoitusta tai kehittynyttä sähköistä leimaa tukeva varmenne on saatavilla veloituksetta;

i) niiden palvelujen sijainti, joista voi selvittää hyväksytyn varmenteen voimassaolon tilan;

j) jos sähköisen allekirjoituksen validointitietoihin liittyvät sähköisen allekirjoituksen luontitiedot sijaitsevat hyväksytyssä sähköisten allekirjoitusten luontivälineessä, tieto tästä ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa.

LIITE II

HYVÄKSYTTYJÄ SÄHKÖISEN ALLEKIRJOITUKSEN LUONTIVÄLINEITÄ KOSKEVAT VAATIMUKSET

1. Hyväksytyillä sähköisen allekirjoituksen luontivälineillä on tarkoituksenmukaista tekniikkaa ja menettelytapoja käyttäen varmistettava ainakin, että

   a) sähköisen allekirjoituksen luomisessa käytettävien sähköisen allekirjoituksen luontitietojen luottamuksellisuus taataan kohtuudella;

   b) sähköisen allekirjoituksen luomisessa käytettäviä sähköisen allekirjoituksen luontitietoja voi käytännössä esiintyä vain kerran;

   c) sähköisen allekirjoituksen luomisessa käytettävät sähköisen allekirjoituksen luontitiedot eivät kohtuullisella varmuudella ole pääteltävissä ja sähköinen allekirjoitus on luotettavasti suojattu väärentämiseltä kulloinkin saatavilla olevan teknologian mukaisesti;

   d) laillinen allekirjoittaja voi luotettavasti suojata sähköisen allekirjoituksen luomisessa käytettävät sähköisen allekirjoituksen luontitiedot muiden käytöltä.

2. Hyväksytyt sähköisen allekirjoituksen luontivälineet eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoittamista.

3. Allekirjoittajan puolesta tapahtuvasta sähköisen allekirjoituksen luontitietojen muodostamisesta ja hallinnoinnista voi vastata ainoastaan hyväksytty luottamuspalvelun tarjoaja.

4. Allekirjoittajan puolesta sähköisen allekirjoituksen luontitietoja hallinnoivat hyväksytyt luottamuspalvelun tarjoajat voivat kahdentaa sähköisen allekirjoituksen luontitietoja ainoastaan varmuuskopiointitarkoituksiin edellyttäen, että seuraavat vaatimukset täyttyvät, sanotun kuitenkaan rajoittamatta 1 kohdan d alakohdan soveltamista:

   a) kahdennettujen tietokokonaisuuksien tietoturvan on oltava samalla tasolla kuin alkuperäisten tietokokonaisuuksien;

   b) kahdennettujen tietokokonaisuuksien määrä ei saa ylittää vähimmäismäärää, joka on tarpeen palvelun jatkuvuuden varmistamiseksi.

LIITE III

SÄHKÖISTEN LEIMOJEN HYVÄKSYTTYJÄ VARMENTEITA KOSKEVAT VAATIMUKSET

Sähköisten leimojen hyväksyttyjen varmenteiden on sisällettävä:

a) tieto, ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa, siitä, että varmenne on myönnetty sähköisen leiman hyväksyttynä varmenteena;

b) tietokokonaisuus, joka yksiselitteisesti edustaa hyväksytyt varmenteet myöntävää hyväksyttyä luottamuspalvelun tarjoajaa ja sisältää ainakin tiedon jäsenvaltiosta, johon tarjoaja on sijoittautunut, ja

— oikeushenkilön osalta: nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa,

— luonnollisen henkilön osalta: henkilön nimi;

c) ainakin leiman luojan nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa;

d) sähköisen leiman validointitiedot, jotka vastaavat kyseisen sähköisen leiman luontitietoja;

e) tiedot varmenteen voimassaoloajan alkamisesta ja päättymisestä;

f) varmenteen tunniste, jonka on oltava kyseisen hyväksytyn luottamuspalvelun tarjoajan osalta yksilöivä;

g) myöntävän hyväksytyn luottamuspalvelun tarjoajan kehittynyt sähköinen allekirjoitus tai kehittynyt sähköinen leima;

h) sijainti, josta g kohdassa tarkoitettua kehittynyttä sähköistä allekirjoitusta tai kehittynyttä sähköistä leimaa tukeva varmenne on saatavilla veloituksetta;

i) niiden palvelujen sijainti, joista voi selvittää hyväksytyn varmenteen voimassaolon tilan;

j) jos sähköisen leiman validointitietoihin liittyvät sähköisen leiman luontitiedot sijaitsevat hyväksytyssä sähköisten leimojen luontivälineessä, tieto tästä ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa.

LIITE IV

VERKKOSIVUSTOJEN TODENTAMISEN HYVÄKSYTTYJÄ VARMENTEITA KOSKEVAT VAATIMUKSET

Verkkosivustojen todentamisen hyväksyttyjen varmenteiden on sisällettävä:

a) tieto, ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa, siitä, että varmenne on myönnetty verkkosivustojen todentamisen hyväksyttynä varmenteena;

b) tietokokonaisuus, joka yksiselitteisesti edustaa hyväksytyt varmenteet myöntävää hyväksyttyä luottamuspalvelun tarjoajaa ja sisältää ainakin tiedon jäsenvaltiosta, johon tarjoaja on sijoittautunut, ja

— oikeushenkilön osalta: nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa,

— luonnollisen henkilön osalta: henkilön nimi;

c) luonnollisten henkilöiden osalta: ainakin sen henkilön nimi, jolle varmenne on myönnetty, tai salanimi. Jos käytetään salanimeä, tämä on ilmoitettava selvästi;

oikeushenkilöiden osalta: ainakin sen oikeushenkilön nimi, jolle varmenne on myönnetty, ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa;

d) luonnollisen henkilön tai oikeushenkilön, jolle varmenne on myönnetty, osoitteen osatiedot, mukaan luettuina ainakin kaupunki ja valtio, tarvittaessa virallisissa rekistereissä olevassa muodossa;

e) luonnollisen henkilön tai oikeushenkilön, jolle varmenne on myönnetty, käyttämät verkon aluetunnukset;

f) tiedot varmenteen voimassaoloajan alkamisesta ja päättymisestä;

g) varmenteen tunniste, jonka on oltava kyseisen hyväksytyn luottamuspalvelun tarjoajan osalta yksilöivä;

h) myöntävän hyväksytyn luottamuspalvelun tarjoajan kehittynyt sähköinen allekirjoitus tai kehittynyt sähköinen leima;

i) sijainti, josta h kohdassa tarkoitettua kehittynyttä sähköistä allekirjoitusta tai kehittynyttä sähköistä leimaa tukeva varmenne on saatavilla veloituksetta;

j) niiden varmenteen voimassaolotilaan liittyvien palvelujen sijainti, joista voi selvittää hyväksytyn varmenteen voimassaolon tilan.