HE 36/2009 vp

Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki vahvasta sähköisestä tunnistamisesta ja sähköisestä allekirjoituksesta. Samalla sähköisistä allekirjoituksista annettu laki ehdotetaan kumottavaksi.

Suurin osa sähköisistä palveluista ei edellytä sähköistä tunnistamista tai sähköisiä allekirjoituksia. Osassa sähköisiä palveluita voidaan kuitenkin muun muassa tehdä erilaisia oikeustoimia. Tällaiset sähköiset palvelut edellyttävät osapuolten välisen luottamussuhteen olemassa oloa. Palvelun käyttäjän on voitava luottaa siihen, että palveluntarjoaja on palveluansa rakentaessaan ottanut huomioon tietoturvan ja yksityisyyden suojan vaatimukset. Palveluntarjoajan on puolestaan voitava luottaa siihen, että etäyhteyden päässä oleva palvelunkäyttäjä on se, joka väittää olevansa. Sähköisten palveluiden ja sähköisen asioinnin kehittyminen edellyttää siten hyvin toimivia sähköisen tunnistamisen palveluita.

Esityksen tavoitteena on luoda perustason sääntely niin sanotun vahvan sähköisen tunnistamisen palveluiden tarjonnalle Suomessa. Tavoitteena on samalla luoda puitteet toimiville vahvan sähköisen tunnistamisen palveluiden markkinoille.

Ehdotettu laki koskisi vain vahvaa sähköistä tunnistamista. Heikko sähköinen tunnistaminen jäisi siten sääntelyn ulkopuolelle. Vahva sähköinen tunnistaminen kohdistuisi luonnollisten henkilöiden tunnistamiseen. Sääntelyn ulkopuolelle jäisivät sellaiset vahvan tunnistamisen menetelmät, joita käytetään suljetuissa ympäristöissä, kuten esimerkiksi tietyn yrityksen omiin tunnistamistarpeisiin.

Ehdotettu laki sisältäisi säännökset siitä, mitä edellytyksiä tunnistusmenetelmän tulee täyttää ollakseen vahvaa. Lisäksi ehdotettu laki sisältäisi säännökset vahvan sähköisen tunnistuspalvelun tarjoajaan ja sen tarjoamaan palveluun kohdistuvista vaatimuksista. Vahvan sähköisen tunnistuspalvelun tarjoamista valvoisi Viestintävirasto.

Sähköistä allekirjoitusta koskevat säännökset vastaisivat voimassa olevaa lakia sähköisistä allekirjoituksista.

Muualla laissa olevat viittaukset sähköisistä allekirjoituksista annettuun lakiin muutettaisiin viittauksiksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Lait on tarkoitettu tulemaan voimaan 1 päivänä syyskuuta 2009.

SISÄLLYS

YLEISPERUSTELUT

1 Johdanto

Sähköisten palveluiden ja sähköisen asioinnin kehitys on Suomessa ja muuallakin Euroopassa ollut hitaampaa kuin vuosituhannen vaihteessa arvioitiin. Tästä huolimatta käyttökokemuksia alkaa kertyä sen verran, että nyt olemme tilanteessa, jossa sähköisten palveluiden kysyntä voi kasvaa huomattavasti. Kysynnän kasvu on seurasta sähköisten palveluiden käyttäjilleen tarjoamista hyödyistä: asioita voi hoitaa kotoa käsin, ilman jonoja ja aukioloajoista piittaamatta.

Sähköisten palveluiden kysynnän arvioidaan lähivuosina voimakkaasti kasvavan, ja tätä kehitystä pyritään tukemaan myös julkisen vallan toimenpitein. Hallitusohjelman mukaan hallitus edistää kansalaisten ja yritysten luottamusta arjen tietoyhteiskunnan palveluihin. Yhtenä keinona tämän luottamuksen edistämiseksi on se, että helppokäyttöistä sähköistä tunnistamista koskevaa lainsäädäntöä uudistetaan.

Sähköinen tunnistaminen on monien sähköisten palveluiden ja sähköisen asioinnin palveluiden mahdollistaja. Sekä palvelujen määrän mutta erityisesti kirjon lisääminen edellyttää jatkossa yhä useammin luotettavaa sähköistä tunnistamista. Käynnissä on joitakin lainsäädäntöhankkeita, joissa etäyhteyksillä tapahtuvan palveluntarjonnan edellytykseksi kaavaillaan luotettavaa sähköistä tunnistamista. Tällaisen lainsäädännön määrä tullee lähivuosina kasvamaan selvästi. Jotta järjestelmä voisi toimia, täytyy olla olemassa myös sellainen säännöstö, jossa määritellään luotettava sähköinen tunnistaminen ja sitä koskevan palveluntarjonnan perusedellytykset.

Jotta helppokäyttöisen vahvan sähköisen tunnistamisen käyttö voisi kasvaa Suomessa huomattavasti, on maahamme luotava edellytykset vahvojen sähköisten tunnistuspalveluiden toimiville markkinoille. Näiden markkinoiden syntymistä edesauttaisi ehdotettu laki, jonka tarkoituksena on säännellä palveluntarjonnan perusperiaatteista.

2 Nykytila

2.1 Lainsäädäntö

Suomessa ei ole voimassa sellaista lakia, joka soveltamisalansa mukaisesti kohdistuisi sähköiseen tunnistamiseen. Sähköistä allekirjoitusta koskee laki sähköisestä allekirjoituksesta, ja lain varmenteita koskevasta sääntelystä on pyritty johtamaan sääntöjä myös varmenteille perustuvaan sähköiseen tunnistamiseen. Lisäksi monet muut lait vaikuttavat vahvaan sähköiseen tunnistamiseen ja sähköisiin allekirjoituksiin. Tällaisia lakeja ovat erityisesti laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), väestörekisteriä ja Väestörekisterikeskuksen tarjoamia varmennepalveluita koskeva lainsäädäntö sekä henkilötietolaki (523/1999).

Laki sähköisistä allekirjoituksista

Laki sähköisistä allekirjoituksista perustuu Euroopan parlamentin ja neuvoston sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin. Soveltamisalansa mukaisesti laki kohdistuu ainoastaan sähköisiin allekirjoituksiin. Lain 2 §:n 1 kohdan mukaan sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä.

Saman pykälän 2 kohdan mukaisesti kehittyneellä sähköisellä allekirjoituksella tarkoitetaan sähköistä allekirjoitusta joka liittyy yksiselitteisesti sen allekirjoittajaan, jolla voidaan yksilöidä allekirjoittaja, joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan, ja joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. Edelleen lain määritelmien mukaan varmenteella tarkoitetaan sähköistä todistusta, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan henkilöllisyyden.

Lain 5 §:n säännökset turvallisen allekirjoituksen luomisvälineestä koskevat kaikkia varmenteita. Pääosa lain säännöksistä koskee kuitenkin ainoastaan laatuvarmenteita ja laatuvarmentajia. Laatuvarmenteella tarkoitetaan sellaista varmennetta, jonka on myöntänyt lain 10-15 §:ssä tarkoitettu laatuvarmentaja. Laatuvarmenteen tunnusmerkkejä ovat myös tieto siitä, että varmenne on laatuvarmenne, tieto varmentajasta ja sen sijoittautumisvaltiosta, allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi, allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja, laatuvarmenteen voimassaoloaika, laatuvarmenteen yksilöivä tunnus, varmentajan kehittynyt sähköinen allekirjoitus, mahdolliset laatuvarmenteen käyttörajoitukset sekä allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.

Lain 18 §:ssä todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä. Sanamuotonsa perusteella laki ei sulje yksiselitteisesti pois sitä mahdollisuutta, että oikeusvaikutuksen voi saada aikaa myös muu kuin laatuvarmenteella luotu kehittynyt allekirjoitus. Pykälällä pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivin 5 artikla. Direktiivin 5 artiklan 2 kohdassa säädetään, että sähköiseltä allekirjoitukselta ei voi evätä oikeudellista vaikutusta ja hyväksyttävyyttä todisteena oikeudellisissa menettelyissä yksinomaan sen vuoksi, että allekirjoitus on sähköisessä muodossa, se ei perustu laatuvarmenteeseen; tai sitä ei ole tehty turvallisen allekirjoituksen luomisvälineen avulla.

Laki sähköisestä asioinnista viranomaistoiminnassa

Lakia sähköisestä asioinnista sovelletaan hallintoasian, tuomioistuinasian, syyteasian ja ulosottoasian sähköiseen vireillepanoon, käsittelyyn ja päätöksen tiedoksiantoon. Lakia sovelletaan soveltuvin osin myös muussa viranomaistoiminnassa. Lain 5 §:n mukaan viranomaisen, jolla on tarvittavat tekniset, taloudelliset ja muut valmiudet, on niiden rajoissa tarjottava kaikille mahdollisuus lähettää ilmoittamaansa sähköiseen osoitteeseen tai määriteltyyn laitteeseen viesti asian vireille saattamiseksi tai käsittelemiseksi. Tällöin on lisäksi kaikille tarjottava mahdollisuus lähettää sähköisesti viranomaiselle sille toimitettavaksi säädettyjä tai määrättyjä ilmoituksia, sen pyytämiä selvityksiä tai muita vastaavia asiakirjoja taikka muita viestejä.

Hallituksen esityksen (HE 17/2002) mukaan viranomaisen asiointipalvelujen järjestämisvelvoite säädettiin suhteellisena ottaen huomioon viranomaisen käytettävissä olevat tiedolliset, taidolliset ja taloudelliset voimavarat. Ehdotonta sähköisten asiointipalvelujen velvoitetta ei katsottu voitavan säätää, koska lain soveltamisala on laaja ja viranomaisten resurssit vaihtelevat.

Lain 9 §:n nojalla vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja. Jos asian vireillepanossa tai muussa käsittelyssä edellytetään allekirjoitettua asiakirjaa, allekirjoitusvaatimuksen täyttää myös sähköisistä allekirjoituksista annetun lain 18 §:ssä tarkoitettu sähköinen allekirjoitus. Viranomaiselle saapunutta sähköistä asiakirjaa ei tarvitse täydentää allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä. Edelleen lain 16 §:n mukaan päätösasiakirja voidaan allekirjoittaa sähköisesti. Viranomaisen sähköisen allekirjoituksen on täytettävä sähköisistä allekirjoituksista annetun lain 18 §:ssä säädetyt edellytykset.

Väestötietolaki

Väestötietolain (507/1993) 5 luvussa on säännökset varmennetun sähköisen asioinnin palveluista. Lain 19 §:n mukaan Väestörekisterikeskuksen tehtävänä on huolehtia siitä, että valtionhallinnon varmennetussa sähköisessä asioinnissa osapuolet voidaan todentaa sekä hallinnon asiakirjat ja viestit tarvittaessa sähköisesti allekirjoittaa ja salata. Väestörekisterikeskus voi tuottaa vastaavia palveluja myös muille viranomaisille, yrityksille, yhteisöille ja yksityisille henkilöille.

Väestötietolain 4 §:ssä säädetään niistä tiedoista, joita Suomen kansalaisesta väestötietojärjestelmään talletetaan. Pykälän 1 kohdan mukaan tällaisia tietoja ovat muun muassa henkilötunnus ja kansalaisvarmenteeseen sisältyvä sähköinen asiointitunnus. Lain 21 §:ssä säädetään sähköisestä asiointitunnuksesta ja 22 ja 23 §:ssä kansalaisvarmenteesta. Lain 21 §:n 3 momentin mukaan tekninen tunnistetieto muutetaan sähköiseksi asiointitunnukseksi silloin, kun henkilölle myönnetään varmenne.

Lain 6 luvussa säädetään väestötietojärjestelmään talletettujen tietojen luovuttamisesta. Kyseiset säännökset eivät sisällä sähköiseen asiointitunnukseen liittyviä luovutusrajoituksia. Väestörekisterikeskus on kuitenkin tulkinnut nykyistä lakia siten, että se ei ole suostunut sähköistä asiointitunnusta koskeviin luovutuspyyntöihin. Parhaillaan on käynnissä hanke väestötietolain kokonaisuudistuksesta. Sen yhteydessä muun muassa ratkaistaan sähköisen asiointitunnuksen käyttömahdollisuudet muissa kuin Väestörekisterikeskuksen varmenteissa.

Henkilötietolaki

Henkilötietolakia sovelletaan yleisesti kaikkeen henkilötietojen käsittelyyn. Ehdotettu laki sisältää jonkin verran henkilötietojen käsittelyä koskevia tarkennuksia henkilötietolain sääntelyyn verrattuna. Pääsääntöisesti henkilötietojen käsittelyssä kuitenkin pitäydytään yleislain sääntelyssä.

Näin ollen myös vahvaa sähköisen tunnistamisen palveluita tarjottaessa on noudatettava muun muassa lain henkilötietojen käsittelyä ja rekisterinpitäjän velvollisuuksia koskevia säännöksiä. Ehdotetun lain kannalta erityisen tärkeitä henkilötietolain säännöksiä ovat 5 §:ssä säädetty huolellisuusvelvoite, informointivelvollisuutta koskeva 24 § ja tietojen suojaamista koskeva 32 §.

Muu lainsäädäntö ja ohjeistus

Edellä mainittujen lisäksi sähköisen tunnistamisen yhteydessä saattaa olla tarve huomioida myös muun lainsäädännön, kuten viranomaisen toiminnan julkisuudesta annetun lain (621/1999) ja yksityisyyden suojasta työelämässä annetun lain (759/2004) sisältämä sääntely.

Olemassa ei ole yleistä sääntelyä siitä, missä tapauksissa palvelu edellyttää vahvaa sähköistä tunnistamista. Yksittäisissä laeissa saattaa olla tällaisia säännöksiä, ja vaikuttaa siltä, että tällaisten säännösten määrä on kasvussa. Liikenne- ja viestintäministeriön kaksivuotisen Luottamus ja tietoturva sähköisissä palveluissa eli LUOTI-ohjelman yhteydessä vahvan sähköisen tunnistamisen käyttötilanteiksi katsottiin yleisesti ottaen taloudellisia tai oikeudellisia sitoumuksia ja luottamuksellisten tietojen, kuten henkilötietolain mukaisten arkaluonteisten henkilötietojen tai organisaation salassa pidettävien tietojen käsittelyä edellyttävät sähköiset palvelut. Julkisen sektorin osalta valtiovarainministeriön ohjeessa 12/2006 on todettu, että vahvaa tunnistamista tarvitaan luottamuksellisissa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa eli sovellus-sovellus-asioinnissa.

2.2 Käytäntö

Sähköinen tunnistaminen

Liikenne- ja viestintäministeriö on asettanut Arjen tietoyhteiskunnan neuvottelukunnan alaisuuteen sähköisen tunnistamisen kehittämisryhmän. Sähköisen tunnistamisen kehittämisryhmä laati syyskuussa 2008 vahvan sähköisen tunnistamisen kansalliset linjaukset, joissa kuvataan sekä yksityisen että julkisen sektorin näkökulmista se toimintaympäristö, jolle vahvan sähköisen tunnistamisen jatkokehittäminen Suomessa perustuu. Linjauksissa ei varsinaisesti ole mitään uutta, vaan ne perustuvat jo olemassa olevaan käytäntöön. Tärkeää on kuitenkin ollut se, että kaikki asiaan liittyvät tulokulmat on esitetty samassa asiakirjassa. Sähköisen tunnistamisen kansalliset linjaukset hyväksyttiin lokakuussa 2008 arjen tietoyhteiskunnan neuvottelukunnassa, jossa ovat edustettuina sähköisen tunnistamisen kehittämisen kannalta tärkeimmät yksityisen ja julkisen sektorin toimijat.

Linjausten ensimmäisessä kohdassa todetaan tarve luoda Suomeen edellytykset toimivien vahvan sähköisen tunnistamisen

markkinoiden syntymiselle. Markkinoille tunnusomaista on tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.

Yleisesti katsotaan, että vahva tunnistaminen koostuu jostain, mitä käyttäjä tietää, kuten esimerkiksi käyttäjätunnus, omistaa, kuten esimerkiksi salasanalista tai kertakäyttöisiä tunnuksia generoiva laite, varmenne tai muu väline, tai on, kuten esimerkiksi sormenjälki. Vähintään kahden näistä vaatimuksista on toteuduttava samanaikaisesti, jotta tunnistustapahtuma täyttää vahvan sähköisen tunnistamisen määritelmän.

Tällä hetkellä kuluttajille suunnattuja vahvan sähköisen tunnistamisen palveluita Suomessa tarjoavat pankit ja Väestörekisterikeskus. Vahvoista menetelmistä selvästi käytetyimpiä ovat pankkien tarjoamat pankkitunnisteet. Markkinoilla on tällä hetkellä yli neljä miljoonaa pankkitunnistetta ja noin 150 000 Väestörekisterikeskuksen tarjoamaa kansalaisvarmennetta. Jopa 99 % tunnistustapahtumista tehdään pankkitunnisteilla.

Linjausten toisen kohdan mukaan keskeisenä edellytyksenä vahvan tunnistamisen markkinoiden syntymiselle ja toimimiselle on osapuolten välinen tehokkaasti toimiva yhteistyö. Tarvitaan avoimia yhteistyöjärjestelyjä, joita edistetään tarvittaessa aktiivisesti. Samalla huolehditaan siitä, etteivät yhteistyöjärjestelyt estä vapaata kilpailua.

Linjausten toisen kohdan perusteluissa kerrotaan, että kansainväliset esimerkit muun muassa Turkista, Virosta ja Norjasta osoittavat, että niissä maissa, joissa sähköinen tunnistaminen on edennyt vertailumaita paremmin, on kyetty kahden tai useamman osapuolen välisiin toimiviin yhteistyöjärjestelyihin. Suomessa on perinteisesti ollut vahvuutena yksityisen ja julkisen sektorin yhteistyö. Toimivien markkinoiden toteuttamiseksi tarvitaan kaikille toimijoille avoimia yhteistyöjärjestelyjä. Markkinoille saattaa syntyä myös joitakin tunnistamis- tai todentamiskeskuksia. Pidemmällä aikavälillä tällaiset keskukset saattavat toimia kansainvälisesti. Tällaisten yhteistyöjärjestelyjen syntymistä on tarvittaessa aktiivisesti edistettävä. Samalla on huolehdittava siitä, että yhteistyöjärjestelyt eivät estä vapaata kilpailua.

Linjausten kolmannessa kohdassa todetaan, että sähköisessä tunnistamisessa erotetaan toisistaan vahva ja heikko tunnistaminen. Lainsäädännöllä säännellään vahvan sähköisen tunnistamisen palveluiden tarjonnan puitteet. Perusteluissa todetaan, että yhdellä luonnollisella henkilöllä voi olla vain yksi todellinen henkilöllisyys, joka on yhteydessä henkilöön oikeussubjektina. Heikossa tunnistamisessa henkilö voi luoda itselleen tai hänelle voidaan luoda useita sähköisiä niin sanottuja identiteettejä, jotka voivat myös poiketa henkilön todellisista ominaisuuksista. Henkilö voi antaa virheellistä tietoa esimerkiksi iästään tai sukupuolestaan.

Sen sijaan vahvalle tunnistamiselle on ominaista, että tunnistamisväline ja sen käyttö voidaan aina viime kädessä yhdistää henkilön todelliseen henkilöllisyyteen. Näin siitä huolimatta, että vahvaa sähköistä tunnistamista käyttävälle palveluntarjoajalle ei palvelun käytön yhteydessä ilmoitettaisi todellisia henkilötietoja, eli kyseessä olisi niin sanottu anonyymi käyttö. Myös vahvassa tunnistamisessa henkilöllä voi olla useita rooleja, joissa hän toimii, ja häneen voidaan liittää eri palveluissa vaihtelevia määriä henkilöstä kertovia tietoja. Henkilöllä voi kuitenkin olla yksi ainoa identiteetti, jonka Suomessa luo valtio.

Edellisessä kappaleessa sanottua voidaan Suomessa entisestäänkin tehostaa sillä, että vahvan tunnistusvälineeseen sisällytetään henkilön yksilöivänä tunnisteena henkilötunnus tai sähköinen asiointitunnus. Parhaillaan eduskunnassa käsiteltävänä olevassa väestötietolain kokonaisuudistuksessa tehdyt nykytilaa muuttavat ratkaisut mahdollistavat sen, että varmentajat voivat varmenteissaan käyttää sähköistä asiointitunnusta. Vahvaa sähköistä tunnistamista tarjoavia palveluntarjoajia on rohkaistava henkilötunnuksen tai sähköisen asiointitunnuksen käyttöön henkilötietoja koskevan sääntelyn huomioon ottaen tiedottamisen, sääntelyn ja muiden tarpeellisten keinojen avulla.

Linjausten neljännen kohdan mukaan vahvan sähköisen tunnistamisen luotettavuus perustuu käytettyyn menetelmään, palvelumallin turvallisiin ja auditoitaviin prosesseihin ja toteutustapoihin, lainsäädännössä vahvan sähköisen tunnistamisen palveluiden tarjoamiselle asetettaviin perusedellytyksiin, vahvan tunnistamisen palvelua tarjoavien ja sitä käyttävien palveluntarjoajien muodostamaan

luottamusverkostoon sekä viranomaisvalvontaan. Näin toteutettu vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen niin yksityisellä kuin julkisellakin sektorilla.

Kohdan perusteluissa todetaan, että suomalaisessa järjestelmässä sekä mahdollinen vahvan sähköisen tunnistusvälineiden tai menetelmien luokittelu että luokittelun hyväksi käyttäminen on jätettävä markkinoiden, eli vahvan tunnistamisen palveluita tarjoavien ja käyttävien palveluntarjoajien sekä loppukäyttäjien omaan harkintaan. Lainsäädännön tasolla Suomessa riittää jako heikkoon eli käytännössä sääntelemättömään ja vahvaan sähköiseen tunnistamiseen, jota ryhdytään sääntelemään lainsäädäntöteitse.

Linjausten viidennessä kohdassa todetaan, että käyttäjien luottamus vahvan sähköisen tunnistamisen palveluihin edellyttää lisäksi, että vahvaa tunnistamista tarjoavat ja käyttävät palveluntarjoajat huolehtivat kuluttajansuojaa ja yksityisyyden suojaa koskevien säännösten huolellisesta noudattamisesta.

Linjausten kuudennen kohdan todetaan, että yksityisen ja julkisen sektorin palveluntarjoajat hankkivat tarvitsemansa sähköisen tunnistamisen palvelut toimivilta vahvan sähköisen tunnistamisen palveluiden markkinoilta. Palveluntarjoajat voivat valita ne vahvan tunnistamisen palvelut, joita käyttävät. Julkinen valta ei rajoita tätä valinnan mahdollisuutta joitakin erityisiä poikkeuksia lukuun ottamatta.

Kohdan perusteluissa todetaan, että palveluntarjoajilla niin julkisella kuin yksityiselläkin sektorilla on oltava valinnan vapaus. Olennaista asiassa on se, että julkisen vallan taholta tätä mahdollisuutta ei rajoiteta mahdollisesti joitakin hyvin harvoja poikkeuksia lukuun ottamatta. Edellytyksenä on joka tapauksessa tällöinkin oltava, että poikkeukset ovat objektiivisia, avoimia, suhteellisia ja syrjimättömiä, ja ne saavat liittyä vain kyseessä olevan palvelun erityispiirteisiin.

Julkisella sektorilla tähän valinnan mahdollisuuteen saattaa kohdistua joitakin rajoituksia voimassa olevan lainsäädännön johdosta. Huomioon saattaa tapauksesta riippuen tulla otettavaksi esimerkiksi kilpailulainsäädännöstä, julkisista hankinnoista tai sähköisestä asioinnista viranomaisessa annettua lainsäädäntöä. Edelleen on otettava huomioon, että valtiovarainministeriö ohjaa julkishallinnon sähköisissä asiointipalveluissa käytettyjä tunnistusratkaisuja. Myös valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI antaa suosituksia ja ohjeita.

Joissakin tapauksessa tilanne voi olla se, että toimijan tarvitsemia vahvan tunnistamisen menetelmiä tai välineitä tai niihin liittyviä palveluita ei ole saatavilla markkinoilta. Tällöin toimija voi joutua kehittämään tarvitsemansa välineen tai palvelun.

Linjausten seitsemännessä kohdassa todetaan, että vahvan sähköisen tunnistamisen palveluiden tarjonta perustuu käyttäjälähtöisyyteen. Jokainen käyttäjä voi valita itselleen sopivimman tunnistamismenetelmän markkinoilla tarjolla olevista vahvan tunnistamisen vaihtoehdoista. Tavoitteena on, että jokainen käyttäjä voi käyttää itselleen sopivinta vahvan sähköisen tunnistamisen menetelmää mahdollisimman monessa tunnistamista tarvitsevassa palvelussa. Samalla on kuitenkin otettava huomioon edellinen linjaus.

Kohdan perustelujen mukaan käyttäjänäkökulma tulee ottaa vahvan sähköisen tunnistamisen peruslähtökohdaksi myös käytännössä. Käyttäjien tulee voida valita käyttöönsä sellainen vahvan sähköisen tunnistamisen menetelmä, joka tuntuu itsestä parhaalta. Usein valinta perustuu johonkin käyttäjän aikaisempaan käyttötottumukseen. Tavoitteena on, että toimivilla markkinoilla tarjolla on muutama vaihtoehtoinen vahvan tunnistusväline, joiden joukosta erilaiset käyttäjät voivat löytää itselleen sopivimman.

Sähköisen tunnistamisen luonteva käyttö edellyttää sitä, että käyttäjille kertyy riittävästi ja toistuvasti käyttökokemuksia tunnistamismenetelmän käytöstä. Jos käyttäjiltä käytännössä vaaditaan usean sähköisen tunnistusvälineen hallintaa, ei käyttökertoja voi välinettä kohti toteutua riittävästi käyttötottumuksen ja sitä kautta käytön mukavuuden takaamiseksi. Käyttäjä voi toki hankkia useamman välineen itse niin halutessaan.

Vahva sähköinen tunnistaminen on sekä käyttäjän että palveluntarjoajan kannalta turvallisempaa kuin heikon tunnistamisen käyttäminen. Esimerkiksi identiteettivarkaudet ovat vahvan sähköisen tunnistamisen menetelmissä helpommin torjuttavissa kuin heikon

tunnistamisen menetelmissä. Myös sellaisissa palveluissa, jotka eivät itsessään välttämättä tarvitsisi vahvaa tunnistamista, tulee siksi viime kädessä pyrkiä siihen, että käyttäjät voisivat käyttää itselleen tuttua ja helppokäyttöistä vahvan tunnistamisen menetelmää. Tämän toteutumiseksi vahvan tunnistustapahtuman kustannustason täytyy olla riittävän edullinen kaikkien toimijoitten kannalta. Toimivien markkinoiden yhtenä tavoitteena onkin pitää hintataso kohtuullisena, mikä toteutuu markkinoilla riittävien vaihtoehtojen ollessa tarjolla.

Vaikka tavoitteena on se, että kukin käyttäjä voisi käyttää valitsemaansa vahvan tunnistusvälinettä mahdollisimman monessa palvelussa, ei palveluntarjoajia voida kuitenkaan pakottaa hyväksymään jotakin välinettä tai vahvan sähköisen tunnistamisen palvelun tarjoajaa. Asiassa on siten huomioitava se, mitä edellisessä linjauksessa todettiin palveluntarjoajien mahdollisuudesta valita. On oletettavaa, että vahvan sähköisen tunnistamisen palveluntarjoajien ja välineiden määrä jää joka tapauksessa rajalliseksi markkinoillamme. Tämän johdosta vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien ja loppukäyttäjien intressien yhteen sovittamisesta ei myöskään muodostune ongelmaa.

Linjausten kahdeksannessa kohdassa todetaan se tosiasiallisesti vallitseva oikeustila, että oikeustoimi voidaan saada aikaan sähköisessä maailmassa sähköisen allekirjoituksen lisäksi myös vahvan tunnistusvälineillä, jos osapuolet niin haluavat.

Kohdan perusteluissa todetaan, että käsitteellisesti on selkeästi erotettava toisistaan vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja oikeustoimien tekeminen sähköisesti. Vahvassa sähköisessä tunnistamisessa tunnistuspalvelua tarjoavat ja sitä käyttävät palveluntarjoajat muodostavat yleensä sopimussuhtein säännellyn verkoston. Sen sijaan sähköisessä allekirjoituksessa peruslähtökohta on se, että allekirjoituspalvelun tarjoaja ei ole sopimussuhteessa allekirjoitukseen luottavan osapuolen kanssa. Määritelmällisesti sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivin mukainen sähköinen allekirjoitus käsittää aina myös tunnistamiselementin. Sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivin mukaan sähköisen allekirjoituksen määritelmä pyrkii olemaan teknologianeutraali, mutta käytännössä sillä tarkoitetaan lähes aina julkisen avaimen järjestelmään perustuvaa sähköistä allekirjoitusta.

Sähköisestä allekirjoituksesta on erotettava oikeustoimen tekemiseen tarvittava tahdonilmaisu. Tämä on erityisen tärkeää Suomessa, jossa hyvin harvaa oikeustointa koskevat tietyt muotovaatimukset. Mikäli oikeustoimi kiistetään, Suomessa vallitsee tuomioistuinten vapaa todistusharkinta. Oikeustoimen tekemiseen tarvittava tahdonilmaisu voidaan saada aikaan Suomessa sähköisen allekirjoituksen lisäksi myös vahvan tunnistamisen menetelmillä, mikäli osapuolet niin haluavat eikä muualla lainsäädännössä ole asetettu oikeustoimelle erityisiä muotovaatimuksia. Suomessa nämä muotovaatimukset ovat hyvin harvinaisia. Mitään osapuolta ei voida yleisesti tai tapauskohtaisesti pakottaa oikeustoimen tekemiseen vahvan sähköisen tunnistamisen välineellä, mutta sellaista vaihtoehtoa haluaville on tarjottava siihen mahdollisuus. Loppukäyttäjän ja palveluntarjoajan yhdenvertaisuus asiassa on tärkeää. Palveluntarjoajan on huolehdittava muun muassa siitä, että käyttäjä on tosiasiassa tietoinen oikeustoimen tekemisestä sekä kaikista muistakin palveluun liittyvistä seikoista.

Linjausten yhdeksännessä kohdassa todetaan se seikka, että sähköinen tunnistaminen ei ole itse tarkoitus vaan luotettavan sähköisen asioinnin mahdollistaja. On olemassa myös sellaisia palveluita, joissa tunnistaminen ei ole lainkaan tarpeen. Vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien on erotettava ne palvelut, joissa tunnistaminen on tarpeen.

Kyseisen kohdan perusteluissa todetaan, että sähköisistä palveluista suuri osa on sellaisia, joissa sähköistä tunnistamista ei lainkaan tarvita. Asiassa on tapahtunut jonkin verran ylilyöntejä siten, että tunnistamista on vaadittu sellaisissakin palveluissa, joissa se ei olisi tarpeen.

Yksityisen sektorin palveluntarjoajien on myös syytä harkita, voitaisiinko heikkoa tunnistamista vähentää myös siten, että nykyistä useampi palvelu olisi käyttäjille avoin. Julkisen sektorin on erityispiirteidensä johdosta

erotettava ne palvelut, joissa tunnistamista voidaan edellyttää.

Linjausten viimeisen eli kymmenennen kohdan mukaisesti Suomi pyrkii aktiivisesti edistämään näitä periaatteita myös EU-tasolla ja kansainvälisillä tasoilla.

Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta

Valtioneuvostossa hyväksyttiin 5 päivänä maaliskuuta 2009 periaatepäätös sähköisestä tunnistamisesta. Sen tarkoituksena on sopia valtioneuvoston sisäisestä työnjaosta sähköisen tunnistamisen alalla tällä hetkellä näköpiirissä olevien tarpeellisten toimenpiteiden osalta.

Sähköisen tunnistamisen jatkokehittämisen osalta tärkeänä pidetään käsillä olevan esityksen lisäksi sitä, että sähköisen tunnistamisen kehittämisryhmä valmistelee kansainvälisiin avoimiin standardeihin perustuvan sähköisen tunnistamisen käytön ja hallinnan toimintamallin vuoden 2009 aikana. Edelleen valtiovarainministeriön vastuulla olevan valtion varmennetuotannon uudelleenorganisointihankkeen tuloksien pohjalta käynnistetään palveluiden jatkokehittäminen vuoden 2009 lopussa.

Julkisen sektorin ohjauksen ja yhteentoimivuuden osalta tarkoituksena on, että valtiovarainministeriö käynnistää vuoden 2009 aikana lainsäädäntötyön, jonka tavoitteena on laatia uutta sitovaa sääntelyä julkisen sektorin sähköisten palveluiden ohjauksesta. Lisäksi valtiovarainministeriö laatii vuoden 2009 aikana suunnitelman julkisen sektorin yhteisen välityspalvelun rakentamisesta ja valmistelee siihen liittyvät hankinnat.

Yritysten ja muiden organisaatioiden tunnistusratkaisujen jatkokehittäminen on kokonaisuuden kannalta ensiarvoisen tärkeää. Sen osalta valtiovarainministeriö, työ- ja elinkeinoministeriön sekä liikenne- ja viestintäministeriö käynnistävät hankkeen, jossa arvioidaan Verohallinnon Katso-järjestelmän jatko sekä laaditaan suunnitelma Patentti- ja rekisterihallituksen roolitietopalvelun käytön laajentamisesta. Hankkeessa myös arvioidaan, miten Patentti- ja rekisterihallituksen tietoja voivat muut toimijat hyödyntää omissa palveluissaan.

Virkamiesten tunnistamisen osalta Kuntaliitto ja valtiovarainministeriö jatkavat VIRTU-hankkeita ja huolehtivat toiminnan käynnistämisestä. Lisäksi valtiovarainministeriö asettaa valtion varmennetuotannon uudelleenorganisointihankkeen tulosten pohjalta tunnistusratkaisujen, kuten esimerkiksi virkakortin käyttöönottoon hankkeen sekä huolehtii tarpeellisesta ohjeistuksesta.

Periaatepäätöksen mukaan tavoitteena on myös, että sosiaali- ja terveysministeriö arvioi uudelleen Sosiaali- ja terveysalan lupa- ja valvontaviraston Valviran roolin varmennepalveluiden tuottajana mahdollisimman nopeasti sen jälkeen, kun valtiovarainministeriö on saanut päätökseen valtion varmennetuotannon uudelleenorganisointia koskevan hankkeen.

Identiteettivarkauksien osalta sisäasiainministeriön johtamissa sisäisen turvallisuuden ohjelmassa ja identiteettiohjelmassa tarkastellaan henkilön yksilöivien tietojen anastamista ja väärän henkilöllisyyden käyttämistä ilmiönä. Hankkeissa selvitetään muun muassa, millaisista ilmenemismuodoista voi olla kysymys ja mikä on niiden aiheuttama uhka kansalaisille nyt ja tulevaisuudessa. Lisäksi selvitetään, miltä osin nykyinen lainsäädäntö, erityisesti rikoslaki, vastaa tähän ongelmakenttään, ja onko tarvetta lisäsääntelylle.

Oikeusministeriö puolestaan asettaa vuoden 2009 aikana työryhmän selvittämään biometristen tunnisteiden käyttämistä sähköisessä tunnistamisessa. Työryhmässä ovat edustettuina ainakin liikenne- ja viestintäministeriö, sisäasiainministeriö ja valtiovarainministeriö.

Sähköinen allekirjoitus

Sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä sähköiseen tunnistamiseen liittyvän palveluntarjoajien muodostaman kehikon ulkopuolella. Sähköisiin allekirjoituksiin liittyykin olennaisena osana varmentajan toiminta. Sähköisen allekirjoituksen luotettavuus perustuu siihen, että jokin taho, yleensä varmentaja, varmistaa allekirjoittajan henkilölli-

syyden. Sähköiseen allekirjoitukseen luottava osapuoli voi tunnistaa allekirjoittajan varmentajan allekirjoittajalle myöntämän varmenteen avulla.

Tällä hetkellä käytetyimmät sähköisten allekirjoitusten toteuttamistekniikat perustuvat julkisen avaimen menetelmään. Allekirjoitus, varmenne ja varmentaja muodostavat yhdessä julkisen avaimen infrastruktuurin. Alla pyritään julkisen avaimen menetelmää kuvaamalla selventämään varmentajan asemaa sähköisen allekirjoituksen käytössä.

Julkisen avaimen menetelmässä hyödynnetään niin sanottuja avaimia eli bittijonoja, joista toinen on yksityinen ja toinen julkinen. Järjestelmässä luotetaan varmentajaan, joka yhdistää myöntämässään varmenteessa tietyn henkilön ja julkisen avaimen toisiinsa. Käytännössä käyttäjällä on siis kaksi avainta, toinen yksityinen ja toinen julkinen. Avaimet toimivat yhteen siten, että julkisella avaimella salattu viesti voidaan avata avainparin yksityisellä avaimella ja päinvastoin. Julkinen avain on nimensä mukaisesti julkinen - kaikkien saatavilla - esimerkiksi varmentajan ylläpitämässä hakemistossa. Yksityinen avain on allekirjoittajan hallussa. Julkinen ja yksityinen avain liittyvät toisiinsa monimutkaisen matemaattisen yhtälön kautta siten, että julkisesta avaimesta ei voi käytännössä johtaa yksityistä tai päinvastoin. Mitä pidemmät avainpituudet on käytössä, sitä turvallisempi menetelmä on kyseessä. Julkiseen ja yksityiseen avaimeen perustuvaa salauskäytäntöä kutsutaan epäsymmetriseksi salaukseksi ja se mahdollistaa itse salauksen lisäksi sähköisten allekirjoitusten luomisen.

Sähköinen allekirjoitus perustuu paitsi julkisen avaimen menetelmään myös niin kutsuttuun tiivistefunktioon. Tiivistefunktiolla mielivaltaisen pituinen viesti tiivistetään tietyn pituiseksi tiivisteeksi. Sähköinen allekirjoitus toteutetaan siten, että allekirjoittaja muodostaa allekirjoitettavasta viestistä tiivistefunktion avulla tiivisteen ja salaa sen yksityisellä avaimellaan. Allekirjoittaja lähettää viestin yhdessä salatun tiivisteen kanssa vastaanottajalle. Vastaanottaja avaa salatun tiivisteen allekirjoittajan julkisella avaimella sekä muodostaa saamastaan viestistä myös tiivisteen oman allekirjoituksen todentamisohjelmistonsa avulla. Vertaamalla tiivisteitä tosiinsa voidaan varmistua viestin eheydestä eli muuttumattomuudesta.

Se, että salattu tiiviste aukeaa allekirjoittajan julkisella avaimella todistaa sen, että allekirjoittajalla on hallussaan julkista avainta vastaava yksityinen avain. Kun julkinen avain on lisäksi varmennettu, eli jokin kolmas osapuoli on myöntänyt allekirjoittajalle varmenteen ja todistanut, että tätä julkista avainta vastaava yksityinen avain kuuluu vain ja ainoastaan kyseiselle allekirjoittajalle, voi viestin vastaanottaja olla varma siitä, että viestin allekirjoittaja on se, joka varmenteessa on ilmoitettu. Varmenne ja julkinen avain voidaan esimerkiksi lähettää viestin mukana tai vastaanottaja voi käydä hakemassa sen varmentajan hakemistopalvelusta.

Sähköisen allekirjoituksen käyttöympäristö on tekninen. Itse toimenpiteet, allekirjoittaminen tai allekirjoituksen todentaminen sekä esimerkiksi hakemistopalveluiden käyttäminen on käyttäjän kannalta lähinnä tavanomaista ohjelmistojen käyttöä. Allekirjoittaminen tapahtuu esimerkiksi klikkaamalla käytettävän ohjelman valikosta kohtaa allekirjoita.

Olennaista sähköisen allekirjoituksen luotettavuudelle on, että yksityiseksi tarkoitettu avain säilyy yksityisenä. Yksityinen avain on yleensä asetettu jollekin alustalle, esimerkiksi toimikortille, jonka käyttö on suojattu esimerkiksi PIN-koodilla tai salasanalla pankkikortin tapaan. Tulevaisuudessa biometriset tunnisteet, esimerkiksi sormenjälkitunnisteet, saattavat osittain korvata käyttäjän muistiin perustuvien salasanojen käytön. Yksityinen avain voi olla myös esimerkiksi matkapuhelimen SIM-kortilla tai ohjelmistona allekirjoittajan käyttämässä laitteessa, esimerkiksi henkilökohtaisessa tietokoneessa.

Sähköisiin allekirjoituksiin liittyy paitsi itse allekirjoittaminen myös allekirjoituksen todentaminen. Allekirjoituksen luomisvälineitä eli ohjelmia ja laitteita vastaavat allekirjoituksen todentamisvälineet eli ohjelmat ja laitteet, joilla allekirjoitus voidaan todentaa. On tärkeää huomata, että varmentaja ei voi viime kädessä mitenkään varmistua, että allekirjoituksen todentajalla on käytössään asianmukaiset, yhteensopivat ja turvalliset todentamisessa tarvittavat ohjelmistot tai laitteistot. Varmentaja tarjoaa hakemistopalvelun ja

sulkulistan, ja on varmenteeseen luottavan kolmannen osapuolen oman edun mukaista tarkistaa näiden avulla varmenteen voimassaolo. Sähköistä allekirjoitusta hyödyntävän todentajan intressissä on hankkia asianmukaiset ja turvalliset todentamisvälineet sekä käyttää varmennetta allekirjoittajasta ja viestin eheydestä varmistuakseen.

Olennainen osa sähköisen allekirjoituksen julkisen avaimen toimintamallia on luottamus. Jotta kaksi ennestään toisiaan tuntematonta osapuolta voisi viestiä keskenään luottamuksellisesti, tarvitaan kolmas osapuoli varmistamaan näiden osapuolten henkilöllisyys. Julkisen avaimen toimintamallissa luottamus perustuu kolmantena osapuolena toimivaan varmentajaan, johon molemmat viestinnän osapuolet luottavat. Varmentaja yhdistää myöntämässään varmenteessa julkisen avaimen ja sen haltijan toisiinsa. Tällöin luottamuksellinen viestintä ja digitaaliset allekirjoitukset onnistuvat, vaikka osapuolet eivät tuntisi toisiaan entuudestaan.

Suomessa on vahvaa osaamista ja useita yrityksiä, jotka valmistavat varmenteita teknisenä välineenä. Tällaisia ovat muun muassa Valimo Wireless Oy, F-Secure Oyj, SSH Communications Security Oy, Tietoenator Oyj ja Nixu Oy. Sähköisistä allekirjoituksista annettu laki ei koske näitä toimijoita, sillä sen soveltamisalasta on suljettu pois pelkkä välineiden valmistaminen, myynti ja maahantuonti. Myös käsillä oleva esitys sisältää vastaavan soveltamisalan rajauksen. Sähköisen allekirjoittamisen palveluita tarjoaa Suomessa tällä hetkellä ainoastaan Väestörekisterikeskus julkisen avaimen teknologiaan perustuvien varmenteiden pohjalta.

Terminologiasta

Varmenteet perustuvat julkisen avaimen (englanniksi public key infrastructure, PKI) järjestelmään, joka toimii siten kuin edellisessä kappaleessa kerrottiin. Usein puhutaan myös PKI-varmenteista. Silloin kun varmenteeseen liitetään korkeintaan teknologiaan viittaava PKI-etuliite, puhutaan varmenteista yleisesti. Varmenteita on perinteisesti käytetty sähköisessä allekirjoituksessa, mutta niitä voidaan käyttää myös sähköisessä tunnistamisessa. Siinä käytössä varmenteiden määrän odotetaan lisääntyvän huomattavasti.

Laatuvarmenteet ovat suomalainen vastine EU:n sähköisiä allekirjoituksia koskevista yhteisön puitteista annetussa direktiivissä luodulle hyväksytyn varmenteen käsitteelle. Tämä on EU:n omaa sisäistä sääntelyä, sillä kansainvälisesti ei tällaisia varmennekategorioita tunneta. Laatuvarmenteella tarkoitetaan sitä, että sellaiseen varmteeseen ja sitä myöntävään varmentajaan kohdistetaan hyvin korkeita laatu- ja muita vaatimuksia. Laatuvarmenteita tarjoaa Suomessa tällä hetkellä vain Väestörekisterikeskus, mutta lainsäädäntö ei estä muiden palveluntarjoajien tuloa markkinoille.

Kansalaisvarmenne on varmenne, jota tarjoaa ja voi tarjota ainoastaan Väestörekisterikeskus. Sen myöntämistä koskee oma lakinsa, väestötietolaki. Kansalaisvarmenne ei perustu EU-lainsäädäntöön. Väestörekisterikeskuksen mukaan kansalaisvarmenne täyttää sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin ja sähköisistä allekirjoituksista annetun lain vaatimukset, ja on näin ollen myös laatuvarmenne. Kansalaisvarmenne voi sijaita lähinnä poliisin myöntämällä henkilökortilla tai passilla.

2.3 Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö

Sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi

Sähköisiä allekirjoituksia koskevista yhteisistä puitteista annettiin Euroopan parlamentin ja neuvoston direktiivi 30 päivänä marraskuuta 1999, ja se tuli voimaan 19 päivänä tammikuuta 2000.

Direktiivin lähtökohtana on se, että varmennepalvelun tarjonta on vapaa elinkeino. Korkeat laatuvaatimukset täyttävät, direktiivin määrittelemät hyväksytyt varmenteet ovat sellaisia, että niillä varmennetut ja turvallisilla allekirjoituksen luomisvälineillä luodut kehittyneet sähköiset allekirjoitukset on ainakin hyväksyttävä oikeusvaikutuksiltaan perinteisen käsinkirjoitetun allekirjoituksen veroisiksi. Direktiivin sääntely keskittyy nimenomaan hyväksyttyyn varmentee-

seen ja niitä tarjoaviin varmentajiin. Ehdotetussa laissa hyväksytystä varmenteesta käytettäisiin nimeä laatuvarmenne, kuten sähköisistä allekirjoituksista annetussa laissakin.

Direktiivin 1 artiklan sisältämän soveltamisalan mukaan tarkoituksena on edistää sähköisen allekirjoituksen käyttöä ja sen oikeudellista tunnustamista. Direktiivillä pyritään luomaan oikeudelliset puitteet sähköisille allekirjoituksille ja tietyille varmennepalveluille, jotta voidaan varmistaa sisämarkkinoiden moitteeton toiminta.

Direktiivillä ei puututa kansallisessa lainsäädännössä tai yhteisön oikeudessa säädettyihin sopimusten ja muiden oikeudellisten sitoumusten tekemiseen ja pätevyyteen liittyviin muotomääräyksiin tai asiakirjojen käyttöä koskeviin säännöksiin.

Direktiivin 2 artikla sisältää määritelmät. Artiklassa on 13 kohtaa sisältävä määritelmäluettelo, joka sisältää direktiivin kannalta keskeisten käsitteiden määritelmät. Artiklassa määritellään muun muassa sähköinen allekirjoitus, useita sähköisen allekirjoituksen tekemisessä tarvittavia osatekijöitä, varmenne ja varmennepalvelun tarjoaja.

Direktiivin 3 artiklassa säädetään markkinoille pääsystä. Varmennepalvelujen tarjonta ei saa olla ennakkovaltuutuksen varaista. Jäsenvaltiot voivat kuitenkin ottaa käyttöön tai ylläpitää vapaaehtoisia akkreditointijärjestelmiä. Akkreditointijärjestelmien tulee olla objektiivisia, avoimia, suhteellisia ja syrjimättömiä.

Jäsenvaltiota velvoitetaan asianmukaisella tavalla järjestämään alueelleen asettautuneiden hyväksyttyjä varmenteita yleisölle myöntävien varmennepalvelujen tarjoajien valvonta.

Jäsenvaltiot voivat nimetä julkisia tai yksityisiä laitoksia määrittelemään, ovatko turvalliset allekirjoituksen luomismenetelmät direktiivin liitteessä 3 vahvistettujen vaatimusten mukaisia. Jäsenvaltioiden on lisäksi tunnustettava edellä mainitun laitoksen tekemä määrittely.

Yleisesti tunnustetun standardin mukainen sähköisiin allekirjoituksiin liittyvä tuote on hyväksyttävä direktiivissä säädettyjen vaatimusten mukaiseksi. Komissio voi julkaista Euroopan yhteisöjen virallisessa lehdessä tällaisten standardien viitenumeroita.

Jäsenvaltiot voivat asettaa lisävaatimuksia sähköisen allekirjoituksen käytölle julkisella sektorilla. Lisävaatimusten tulee olla objektiivisia, avoimia, suhteellisia ja syrjimättömiä. Lisäksi ne saavat liittyä vain kyseessä olevan sovelluksen erityispiirteisiin. Lisävaatimukset eivät saa estää kansalaisille tarjottavia rajat ylittäviä palveluita.

Direktiivin 4 artiklan sisämarkkinaperiaatteiden mukaan direktiivin nojalla annettuja kansallisia säädöksiä on sovellettava kaikkiin jäsenvaltion alueelle sijoittautuneisiin varmennepalvelujen tarjoajiin sekä niiden tarjoamiin palveluihin. Myöskään toisesta jäsenvaltiosta peräisin olevan varmennepalvelun tarjontaa ei saa kansallisin säännöksin rajoittaa. Jäsenvaltioiden on lisäksi varmistettava, että sähköisiin allekirjoituksiin liittyvät tuotteet liikkuvat vapaasti sisämarkkinoilla.

Direktiivin 5 artiklassa säädetään sähköisen allekirjoituksen oikeusvaikutukset. Jäsenvaltioiden on varmistettava, että sellaiset kehittyneet sähköiset allekirjoitukset, jotka perustuvat hyväksyttyyn varmenteeseen ja jotka on luotu turvallisella allekirjoituksen luomismenetelmällä, vastaavat oikeudellisilta vaikutuksiltaan käsin tehtyä allekirjoitusta sekä kelpaavat todisteeksi tuomioistuimissa. Toisaalta oikeudellista vaikutusta tai todistusvaikutusta ei saa evätä muiltakaan sähköisiltä allekirjoituksilta ainoastaan siitä syystä, että ne eivät täytä edellä esitettyjä laatuvaatimuksia.

Direktiivin 6 artiklassa säädetään hyväksyttyjä varmenteita yleisölle tarjoavan vahingonkorvausvastuusta, jos vahinko on syntynyt varmenteeseen perustellulla tavalla luottaneelle. Vahingonkorvausvastuu syntyy tietyissä tapauksissa, jollei varmennepalvelujen tarjoaja pysty todistamaan, ettei hän ole toiminut huolimattomasti.

Direktiivin mukaan varmentaja vastaa edellä mainitulla tavalla ainakin hyväksytyn varmenteen tietojen paikkansapitävyydestä sen myöntämishetkellä ja kaikkien hyväksytyissä varmenteissa ilmoitettavien tietojen sisältymisestä varmenteeseen sekä siitä, että allekirjoitusavain luovutetaan nimenomaan varmenteen haltijalle ja, että allekirjoituksen luomiseen ja todentamiseen käytettävät tiedot toimivat toisiaan täydentävästi, milloin varmentaja on luonut ne molemmat. Lisäksi

varmentaja vastaa varmenteen peruuttamisen tekemättä jättämisestä.

Varmentajalla on oltava oikeus hyväksytyssä varmenteessa ilmoittaa kyseisen varmenteen käyttörajoituksista. Varmenteessa ilmoitettava rajoitus voi koskea myös niiden toimien arvoa, joihin varmennetta voidaan käyttää. Kyseiset rajoitukset tulee olla kolmansien osapuolten tunnistettavissa, eivätkä ne saa olla kohtuuttomia. Varmentaja ei vastaa näiden käyttörajoitusten vastaisesta hyväksytyn varmenteen käytöstä.

Direktiivin 7 artiklassa on säännöksiä siitä, miten kolmanteen maahan sijoittautuneen varmentajan hyväksyttyinä varmenteina yleisölle tarjoamat varmenteet tunnustetaan oikeusvaikutuksiltaan Euroopan yhteisöjen alueella. Tunnustaminen voi tapahtua, jos varmentaja täyttää direktiivin vaatimukset ja on liittynyt direktiivin tarkoittamaan akkreditointijärjestelmään, tai jos yhteisöön sijoittautunut varmentaja takaa varmenteen, tai jos varmenne tai varmentaja on tunnustettu Euroopan yhteisön kolmannen maan tai kansainväliseen maan kanssa tekemän sopimuksen nojalla. Komissio voi antaa neuvostolle ehdotuksia määräenemmistöllä päätettävistä neuvotteluvaltuuksista näitä kansainvälisiä sopimuksia varten.

Direktiivin 8 artiklan sisältämien tietosuojasäännösten mukaan jäsenvaltioiden on varmistettava, että varmentajat, akkreditointijärjestelmät ja valvovat viranomaiset noudattavat yleisessä tietosuojadirektiivissä säädettyjä vaatimuksia. Varmentaja saa hankkia henkilötietoja vain tietojen kohteelta itseltään, tai saatuaan siihen kyseisen henkilön nimenomaisen suostumuksen. Ilman kohteen nimenomaista lupaa tietoja ei myöskään saa kerätä tai muokata muihin tarkoituksiin kuin varmenteen myöntämiseksi ja ylläpitämiseksi. Varmenteessa on saatava käyttää salanimeä todellisen nimen sijasta. Tämä ei kuitenkaan vaikuta salanimestä kansallisella lainsäädännöllä säädettyihin oikeusvaikutuksiin.

Direktiivin 9 ja 10 artiklassa säädetään komissiota avustavasta sähköisten allekirjoitusten komiteasta ja sen tehtävistä. Lisäksi direktiivin 11 ja 12 artiklassa säädetään jäsenvaltioiden ilmoittamisvelvollisuudesta ja direktiivin toteutumisen tarkastelusta.

Direktiivin 13-15 artiklat sisältävät tavanomaiset direktiivin loppusäännökset.

Liite 1 sisältää hyväksyttyjä varmenteita koskevat vaatimukset. Hyväksytyn varmenteen tietosisältöön kuuluu muun muassa tiedot varmennepalvelujen tarjoajasta, allekirjoittajan nimi, mahdolliset allekirjoittajaan liittyvät erityismääreet, allekirjoituksen todentamiseen käytettävät tiedot, varmenteen voimassaoloaika ja varmennepalvelujen tarjoajan kehittynyt sähköinen allekirjoitus.

Liitteestä 2 löytyvät hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajia koskevat vaatimukset. Vaatimuksena on muun muassa palveluiden tarjoamisen edellyttämän luotettavuuden osoittaminen, nopea ja varma hakemistopalvelu sekä luotettava ja nopea varmenteen peruuttamismahdollisuus, henkilön luotettava tunnistaminen varmennetta myönnettäessä, pätevä henkilökunta, turvalliset järjestelmät, riittävät varat tai vakuutukset, kielto tallentaa allekirjoitusavainta, arkistointivelvoite ja tiedotusvelvollisuus käyttäjille varmennetta myönnettäessä.

Liitteessä 3 kerrotaan turvallisia allekirjoituksen luomisvälineitä koskevat vaatimukset. Menetelmän on varmistettava, että allekirjoituksen luomistiedot ovat käytännössä ainutkertaiset eikä niitä voida johtaa, ja että niiden luottamuksellisuus voidaan kohtuudella varmistaa, ja että allekirjoitus on suojattu väärentämiseltä. Allekirjoittajan on myös voitava suojata luomistiedot muiden käytöltä. Allekirjoitus-menetelmät eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoitusmenettelyä.

Liite 4 puolestaan sisältää turvallista allekirjoitusten todentamista koskevat suositukset. Suositusten mukaan menettelyn tulisi muun muassa kohtuullisella varmuudella varmistaa, että todentamistiedot vastaavat todentajalle näkyviä tietoja, allekirjoitus todennetaan luotettavasti, todentaja voi tarvittaessa todeta allekirjoitettujen tietojen sisällön ja että varmenteen aitous ja pätevyys voidaan luotettavasti todentaa.

Euroopan komissio on teettänyt tutkimuksen ”The Legal And Market Aspects Of Eletronic Signatures” sähköisiä allekirjoituksia käsittelevän lain implementoinnin onnistumisesta eri maissa niin juridisesta kuin käytän-

nön näkökulmasta. Tutkimuksen mukaan jäsenvaltiot ovat kyllä implementoineet direktiivin kiitettävän hyvin, mutta säädöksen henki tai sanamuodot on usein ymmärretty väärin.

Tutkimuksessa tulee esiin, että julkisen asioinnin yhteydessä edellytetään tarpeettoman usein laatuvarmenteiden käyttämistä, mikä monasti turhaan vaikeuttaa kansalaisten sähköistä asiointia. Tutkimuksen mukaan myöskään direktiivin 5 artiklan 2 kohdan diskriminointikieltoa ei ole aina ymmärretty oikein, vaan on virheellisesti tulkittu ainoastaan tietyn teknologian täyttävän lain vaatimukset. Tutkimuksessa suositellaankin komission ryhtyvän aktiivisiin toimenpiteisiin kaikkien sidosryhmien informoimiseksi ja niiden tietoisuuden parantamiseksi kyseisen artiklan osalta. Tutkimuksessa painotetaan, että laatuvarmenne ei tarkoita samaa kuin juridisesti hyväksytty allekirjoitus, vaan se on vain yksi tekniikka juridisesti hyväksyttävän sähköisen allekirjoituksen tekemiseksi. Työryhmä suosittelee laatuvarmenne termin painoarvon vähentämistä sähköisen asioinnin edistämiseksi ja lain hengen eli teknologianeutraalisuuden korostamiseksi.

Lisäksi tutkimuksessa todetaan, että markkinoilla ei vielä tällä hetkellä ole luonnollista kysyntää laatuvarmenteille. Tilanteen uskotaan myös jatkuvan hyvin pitkään tulevaisuudessa samanlaisena. Markkinoilla uskotaan usein virheellisesti, että tiettyjen sovellusten tai palveluiden käyttö edellyttäisi laatuvarmenteella tehtyä allekirjoitusta, mikä johdosta palveluntarjoajille aiheutuu turhia kustannuksia ja vaikeuksia palveluiden kehittämisessä.

Vaihtoehtoisia allekirjoitustapoja listatessaan työryhmä nostaa esille pankkien käyttämät vaihtuvat salasanalistat. Pankkitunnusten osalta toivotaan niiden laajaa hyödyntämistä eri verkkopalveluissa, mikä edellyttää yhteistyötä pankkien puolelta. Tämä on jo toteutunut Suomessa, kun pankit ovat tehneet Tupas-standardin ja julkishallinto on antanut suosituksensa Tupaksen hyödyntämisestä. Euroopassa on muun muassa VISA:n johdolla alettu tukimaan mahdollisuutta hyödyntää pankkien tunnistamismenetelmiä entistä laajemmin verkkopalveluissa.

EU:n ohjelmat ja hankkeet

Euroopan unionissa on käynnissä lukuisia ohjelmia, joilla edistetään tai hyödynnetään sähköistä tunnistamista ja sähköistä allekirjoittamista ja niiden hyväksyttävyyttä rajat ylittävissä toiminnoissa.

IDABC (Interchange of Data Between Administrations, suomeksi Yleiseurooppalaisten sähköisten viranomaispalveluiden yhteentoimiva toimittaminen julkishallinnolle, yrityksille ja kansalaisille eli HVTYK) on yhteisön ohjelma, jolla tuetaan EU-lainsäädännön voimaansaattamista parantamalla jäsen- valtioiden välistä sähköistä tiedonvaihtoa. Ohjelma on käynnistynyt jo 1990-luvun puolivälissä, ja sen nykyvaihe perustuu Euroopan parlamentin ja neuvoston päätökseen 2004/387/EY, tehty 21 päivänä huhtikuuta 2004, yleiseurooppalaisten sähköisten viranomaispalveluiden yhteentoimivasta toimittamisesta julkishallinnolle, yrityksille ja kansalaisille (HVTYK). Ohjelma, joka kytkeytyy eEurooppa-ohjelmiin ja laajemmin Lissabonin strategiaan, jakautuu projekteihin (Projects of Common Interest) ja horisontaalisiin toimenpiteisiin (Horizontal Actions and Measures). Ohjelman puitteissa on tehty tutkimus sähköisten allekirjoitusten vastavuoroisesta tunnustamisesta jäsenvaltioiden välillä sähköisen hallinnon tarpeisiin. Tutkimuksessa, jonka alustavat tulokset ovat valmistuneet, on tutkittu sähköisten allekirjoitusten käytön yhtäläisyyksiä ja eroja sekä oikeudelliselta että tekniseltä kannalta eri jäsenvaltioissa ja eräissä muissa valtioissa sähköisessä asioinnissa viranomaisissa. Tutkimuksessa selvitetään ilmenneiden yhtäläisyyksien ja erojen vaikutusta yhteentoimivuuteen ja annetaan suosituksia. Tutkimuksessa ei ole nimenomaisesti paneuduttu sähköistä tunnistamista koskeviin kysymyksiin.

STORK (Secure identity across borders linked) on komission toukokuussa 2008 käynnistämä pilottihanke, jonka tavoitteena on helpottaa julkisten palvelujen käyttöä 13 jäsenvaltiossa. Hankkeessa pyritään luomaan yhteentoimivan sähköisen tunnistuksen malli, joka tunnustetaan vastavuoroisesti muissa jäsenvaltioissa, mutta joka antaa jäsenvaltioille mahdollisuuden säilyttää nykyiset järjestelmänsä ja käytäntönsä. Hankkeessa ovat mu-

kana Euroopan komissio, Alankomaat, Belgia, Espanja, Italia, Itävalta, Luxemburg, Portugali, Ranska, Ruotsi, Saksa, Slovenia ja Yhdistyneet kuningaskunnat sekä Euroopan talousalueen valtioista Islanti. Hanke on osa EU:n kilpailukyvyn ja innovoinnin puiteohjelmaa (CIP).

Hankkeen tavoitteena on, että yritykset, yksityishenkilöt ja julkishallinnon työntekijät voivat käyttää sähköistä henkilöllisyyttään missä tahansa jäsenvaltiossa. Järjestelmä perustuisi kansallisella, alueellisella tai paikallisella tasolla jo toimiviin tieto- ja viestintäteknisiin ratkaisuihin, joita tarjottaisiin rajojen yli. Hankkeessa testataan eräitä monikäyttöisimpiä sähköiseen henkilöllisyyteen perustuvia palveluita määrittelemällä ensin yhteiset eritelmät, joiden perusteella erilaiset kansalliset henkilötunnisteet voidaan hyväksyä muissa osallistujamaissa ja jotka ovat kaikkien saatavilla. Hankkeeseen osallistuvia maita kannustetaankin hyväksymään toistensa sähköiset henkilötunnisteet.

Järjestelmä tarjoaisi turvallisen mahdollisuuden henkilöllisyyden sähköiseen todentamiseen ja kanssakäymiseen julkishallinnon kanssa esimerkiksi tietokoneelta tai jopa matkapuhelimesta käsin. Järjestelmällä ei ole tarkoitus korvata kansallisia järjestelmiä, ja muutkin kuin pilottihankkeessa mukana olevat valtiot voivat hyödyntää sen tuloksia.

PEPPOL (Pan European Public Procurement Online) on toinen tunnistamisen kannalta keskeinen hanke, joka liittyy EU:n kilpailukyvyn ja innoivoinnin ohjelmaan (CIP). Siinä keskitytään julkisen hankintaprosessin rajat ylittäviin näkökohtiin. Euroopan komissio työskentelee yhdessä EU-maista Italian, Itävallan, Ranskan, Saksan, Suomen, Tanskan, Unkarin sekä Euroopan talousalueen maista Norjan kanssa helpottaakseen yritysten mahdollisuuksia osallistua julkisiin tarjouskilpailuihin oman maansa rajojen ulkopuolella. Hankkeessa ei korvata olemassa olevia kansallisia sähköisiä hankintajärjestelmiä vaan täydennetään niitä siten, että ne pystyvät toimimaan yhdessä.

Useat EU:n jäsenvaltiot ovat ottaneet käyttöön järjestelmiä sähköisiin julkisiin hankintoihin. Vaatimukset, jotka koskevat sähköisiä allekirjoituksia hankinta-asiakirjoissa, vaihtelevat jäsenmaittain, mutta hankintamenettelyyn osallistuvilla tarjoajilla on periaatteessa oikeus käyttää oman jäsenvaltionsa vaatimusten mukaisia sähköisiä allekirjoituksia tarjouksissaan. Allekirjoitusvaatimusten taustalla eivät kuitenkaan yleensä ole perinteiset allekirjoitusten tehtävät tahdonilmaisun ilmentäjänä, vaan lähettäjän tunnistaminen erilaisiin viranomaistarkoituksiin.

Komission tiedonanto rajat ylittävien julkisten palveluiden tarjonnan helpottamisesta

Komission antoi 28 päivänä marraskuuta 2008 tiedonantonsa neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle sähköisiä allekirjoituksia ja sähköistä tunnistusta koskevaksi toimintasuunnitelmaksi rajat ylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla (KOM(2008) 798 lopullinen). Toimintasuunnitelman tavoitteena on auttaa jäsenvaltioita toteuttamaan vastavuoroisesti tunnustettuja ja yhteentoimivia sähköisten allekirjoitusten sekä sähköisen tunnistuksen ratkaisuja, jotta helpotettaisiin rajatylittävien julkisten palvelujen tarjoamista sähköisessä ympäristössä. Toimintasuunnitelmassa keskitytään lähinnä sähköisen hallinnon sovelluksiin, mutta myös yritysten sovellukset voivat hyötyä ehdotetuista toimista.

Tiedonanto on jaettu sähköisiin allekirjoituksiin kohdistuviin toimiin ja sähköiseen tunnistamiseen kohdistuviin toimiin. Painopiste on selkeästi sähköisten allekirjoitusten puolella. Niiden osalta komission toimenpiteet jakautuvat niin ikään kahteen ryhmään. Ensimmäinen ryhmä koskee varmennettujen sähköisten allekirjoitusten (QES) ja hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten (QC:hen perustuva AES) rajat ylittävää käyttöä. Komission arvion mukaan tätä aluetta voitaisiin kehittää suhteellisen nopeasti, koska molemmilla allekirjoituksilla on selkeä sähköisiä allekirjoituksia koskevaan direktiiviin perustuva oikeudellinen asema. Lisäksi tällä saralla on jo tehty paljon standardointityötä.

Komissio toteaa, että käytännössä suurin este sähköisten allekirjoitusten rajat ylittävälle käytölle on se, että muista jäsenvaltioista lähtöisin oleviin sähköisiin allekirjoituksiin

ei luoteta. Lisäksi näidenkin allekirjoitusten oikeellisuuden tarkistamiseen liittyy ongelmia. Vastaanottavan osapuolen olisi komission mukaan ensinnäkin pystyttävä tarkastamaan toisessa jäsenvaltiossa hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien (CSP) asema. Toiseksi vastaanottavan osapuolen olisi pystyttävä tarkastamaan allekirjoituksen laatu. Tämä tarkoittaa sitä, että vastaanottavan osapuolen olisi pystyttävä tarkastamaan, onko allekirjoitus kehittynyt sähköinen allekirjoitus, ja onko sen tukena valvotun varmennepalvelujen tarjoajan myöntämä hyväksytty varmenne. Jos kyseessä on varmennettu sähköinen allekirjoitus, vastaanottavan osapuolen olisi myös pystyttävä varmistamaan, onko allekirjoitus luotu turvallisella allekirjoituksen luomismenetelmällä. Komissio toteaa, että kaikki nämä tiedot löytyvät periaatteessa itse allekirjoituksesta ja hyväksytyn varmenteen sisällöstä. Tällä hetkellä näiden tietojen saaminen on kuitenkin vaikeaa, sillä nykyisten standardien ja käytäntöjen soveltamisessa on eroja.

Komission johtopäätös asiassa on, että sähköisten allekirjoitusten validointimenettelyä voitaisiin helpottaa toimittamalla vastaanottavalle osapuolelle tarpeelliset tiedot kansallisella tasolla hyväksytyistä ja valvotuista varmennepalvelujen tarjoajista ja antamalla ohjeistusta nykyisten standardien ja käytäntöjen soveltamisesta yhteentoimivuuden varmistamiseksi.

Asiaintilan parantamiseksi komissio ehdottaa neljää toimenpidettä. Viimeistään vuoden 2009 toisella neljänneksellä olisi laadittava luotettava luettelo valvotuista hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista (Trusted List of Supervised Qualified Certification Service Providers) Euroopan tasolla. Luettelon on tarkoitus sisältää kaikki vaaditut tiedot nykyisistä ja valvotuista hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista. Työ on jo parhaillaan käynnissä palveludirektiivin täytäntöönpanoa valmistelevassa komission työryhmässä.

Lisäksi komission tavoitteena on viimeistään vuoden 2009 kolmannella neljänneksellä saattaa ajan tasalle päätös 2003/511/EY14, jossa vahvistetaan luettelo sähköisiin allekirjoituksiin liittyvien tuotteiden yleisesti tunnustetuista standardeista. Komissio aikoo myös tarkastella päätöksen mahdollista ulottamista muihin sähköisiin allekirjoituksiin liittyviin tuotteisiin kuin komission nykyisen päätöksen soveltamisalaan kuuluviin tuotteisiin. Samoin viimeistään vuoden 2009 kolmannella neljänneksellä komission tavoitteena on laatia yleisiä vaatimuksia koskevat suuntaviivat ja ohjeet auttaakseen sidosryhmiä käyttämään varmennettuja sähköisiä allekirjoituksia ja hyväksyttyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia yhteentoimivalla tavalla. Jatkuvana toimenpiteenä mainitaan se, että jäsenvaltioita kehotetaan säännöllisesti toimittamaan tarpeelliset tiedot komissiolle ja tarvittaessa toteuttamaan toimenpiteitä, jotka perustuvat edellä mainittuihin toimiin.

Toisena sähköisten allekirjoitusten ryhmänä komissio pitää kehittyneitä sähköisiä allekirjoituksia (AES). Niihin liittyy samankaltaisia yhteentoimivuuteen liittyviä kysymyksiä kuin edellä on tuotu esille varmennettujen sähköisten allekirjoitusten ja hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten osalta. Käytännössä kehittyneiden sähköisten allekirjoitusten tilanne on kuitenkin monimutkaisempi, koska niihin liittyy nykyisin useampia oikeudellisia, teknisiä ja organisatorisia rajoitteita.

Sähköisiä allekirjoituksia koskevan direktiivin 2 artiklan 2 kohdassa määritellään kehittyneet sähköiset allekirjoitukset hyvin yleisellä tasolla. Tämän johdosta jäsenvaltiot ovat päätyneet hyvin erilaisiin teknisiin ratkaisuihin ja erilaisiin turvallisuustasoihin. Jäsenvaltiot voivat myös soveltaa tiettyihin sovelluksiin erityisiä kansallisia ratkaisuja, mikä luo lisäesteitä kehittyneiden sähköisten allekirjoitusten rajat ylittävälle käytölle. Tässä tilanteessa vastaanottavalla osapuolella on haasteellinen tehtävä arvioida kehittyneen sähköisen allekirjoituksen oikeellisuus. Samoin on haasteellista arvioida kyseisen allekirjoituksen oikeudellista arvoa tai turvallisuustasoa tietyssä sovelluksessa. Nykyisin nämä tehtävät usein edellyttävät vastaanotetun allekirjoituksen tapauskohtaista arviointia ja käsittelyä.

Komissio toteaa, että kehittyneen sähköisen allekirjoituksen rajat ylittävän käytön helpottamiseksi olisi luotava tarpeelliset

edellytykset, joiden turvin vastaanottava osapuoli voisi luottaa toisesta jäsenvaltiosta lähtöisin olevaan kehittyneeseen sähköiseen allekirjoitukseen. Komission johtopäätöksenä on, että toimintasuunnitelmassa on käytännössä mahdotonta laatia kehittyneitä sähköisiä allekirjoituksia koskevaa yhteistä toimintapolitiikkaa ja yhteisiä perusteita. Yhtenä ratkaisuna voisi kuitenkin olla, että tarkastus- ja validointitehtävät delegoidaan keskitetylle tai hajautetulle validointipalvelujärjestelylle. Näin voitaisiin asteittain poistaa tämä kehittyneiden sähköisten allekirjoitusten yhteentoimivuuden huomattavin este. Komissio ilmoittaa tarkastelevansa vuoden 2009 toisella neljänneksellä toteutettavuustutkimuksen avulla, mitä vaihtoehtoja on käytettävissä tällaisen validointijärjestelyn luomiseksi EU:n tasolle.

Lisäksi komissio saattaa viimeistään vuoden 2009 toisella neljänneksellä ajan tasalle maaprofiilit, jotka on vahvistettu sähköisen hallinnon sovelluksissa käytettävien sähköisten allekirjoitusten vastavuoroista tunnustamista koskevassa IDABC-tutkimuksessa. Viimeistään vuonna 2010 komissio raportoi lisätoimista, joita tarvitaan helpottamaan kehittyneiden sähköisten allekirjoitusten rajat ylittävää käyttöä sen pohjalta, mitä tuloksia saadaan käynnissä olevasta työstä. Jäsenvaltioita pyydetään toimittamaan komissiolle kaikki merkitykselliset tiedot ja huolehtimaan toimien toteuttamisessa tarvittavasta yhteistyöstä erityisesti validointipalvelun perustamiseksi. Jäsenvaltioita pyydetään myös testaamaan validointipalvelua PEPPOL-pilottihankkeessa.

Sähköisen tunnistamisen osalta komissio toteaa, että sähköisen tunnistuksen ratkaisujen yhteentoimivuus on ennakkoedellytys rajat ylittävälle pääsylle sähköisiin julkisiin palveluihin. Tähän saakka sähköisen tunnistuksen keinoja on käytetty vailla jäsenvaltioiden välistä yhteensovittamista. Jos unionissa ei hyödynnetä yhteentoimivia sähköisen tunnistuksen järjestelmiä, luodaan käytännössä uusia esteitä, mikä on ristiriidassa sisämarkkinavälineiden kanssa.

Parhaillaan on käynnissä tiettyjä yhteisiä toimia, joiden tavoitteena on löytää rajat ylittävään sähköiseen tunnistukseen sellainen ratkaisu, jossa voitaisiin turvautua nykyisiin tunnistusratkaisuihin. Sähköisten allekirjoitusten mallin mukaisesti pyritään horisontaaliseen ratkaisuun, johon voitaisiin turvautua alakohtaisissa sovelluksissa ja joka perustuisi sähköisen tunnistuksen järjestelyjen vastavuoroiseen hyväksymiseen. Ratkaistavana on kuitenkin useita kysymyksiä.

Ensimmäisenä askeleena on STORK-pilottihanke. Komissio käynnistää vuoden 2009 loppuun mennessä yhteistyössä jäsenvaltioiden kanssa sähköisen tunnistuksen käyttöä jäsenvaltioissa koskevia erityisiä kyselyitä, joilla täydennetään ja tuetaan STORK-hanketta. Hankkeen tulosten valmistuttua komissio päättää, edellyttääkö sähköisen tunnistuksen EU:n laajuinen tehokas käyttö lisätoimia, ja millaisia tällaiset mahdolliset lisätoimet olisivat. Edelleen jäsenvaltioita kehotetaan viimeistään vuonna 2012 demonstroimaan sähköisen tunnistuksen rajat ylittävän käytön ratkaisuja STORK-pilottihankkeessa.

Muiden maiden lainsäädäntö

Ruotsi

Ruotsin sähköisiä allekirjoituksia koskeva laki (Lag (2000:832) om kvalificerade elektroniska signaturer) sääntelee Ruotsiin sijoittautuneita laatuvarmentajia. Laki on sellaisenaan kuitenkin jäänyt taustalle, koska Ruotsin markkinoille ei ole toistaiseksi tullut laatuvarmenteita myöntäviä varmentajia. Ruotsin laki poikkeaa direktiivistä hienokseltaan siten, että sähköisen allekirjoituksen yleinen määritelmä sisältää allekirjoitetun tiedon eheyden vaatimuksen allekirjoittajan henkilön todentamisen lisäksi.

Telehallintoviranomainen (Post- och telestyrelsen) ylläpitää luetteloa laatuvarmentajista ja valvoo näiden toimintaa. Virastoa koskevassa rahoitusasetuksessa säädetään laatuvarmentajien vuosimaksuista ja tätä täydentää viraston oma maksuasetus (PTSFS 2007:8).

Sähköistä identiteettiä tuottavat Ruotsissa useat kaupalliset toimijat, jotka valitaan julkisissa hankintamenettelyissä. Sähköisen identiteetin tuottajat voivat käyttää väestörekisteritietoja ja henkilötunnuksia. Tunnistamista ei kuitenkaan ole säännelty lailla eikä

sähköisen identiteetin muodostamista ole määritelty. Yleisesti katsotaan kuitenkin, että sähköisen identiteetin muodostamisessa käytetyt menetelmät eivät täytä laatuvarmenteelle asetettavia vaatimuksia. Sähköisen identiteetin voi ladata tietokoneen kovalevylle, mutta älykortti tai aktivointikoodi tulee noutaa postista henkilökohtaisesti tunnistautuen. Laissa tarkoitettujen sähköisten allekirjoitusten osalta todetaan, että varmentajan täytyy noudattaa turvallisia menetelmiä varmennettavien identiteetin toteamiseksi.

Norja

Norjan laki sähköisistä allekirjoituksista (Lov om elektronisk signatur) on vuodelta 2001. Laki perustuu EU-direktiiviin ja käyttää siten samaa käsitteistöä kuin direktiivi. Norjassa ei ole kuitenkaan laatuvarmentajia, joten laki on toistaiseksi jäänyt melko merkityksettömäksi.

Yleisiä lainsäännöksiä sähköisestä tunnistamisesta ei ole luotu. Sähköisen identiteetin luomiseksi on käytössä monien toimijoiden, kuten pankkien ja rahapelilaitoksen myöntämiä älykortteja ja kansallinen järjestelmä on parhaillaan kehitteillä, mutta lopullisia ratkaisuja toteutuksen, valvonnan ja lainsäädännön suhteen ei ole tehty. Olemassa olevat ratkaisut ovat kaupallisia ja yleiset siviilioikeudelliset säännöt määrittävät vastuukysymykset.

Tanska

Tanskassa on muiden EU-maiden tavoin saattanut voimaan sähköisiä allekirjoituksia koskevan direktiivin, mutta sen käytännön merkitys on jäänyt olemattomaksi, koska maassa ei ole laatuvarmentajia, jotka varmentaisivat kvalifioituja sähköisiä alle kirjoituksia. Tanskassa ei ole erillistä lainsäädäntöä sähköisestä tunnistamisesta.

Sähköisiä allekirjoituksia koskeva laki vaatii, että kvalifioitua sähköistä allekirjoitusta hakevan henkilön on tunnistauduttava henkilökohtaisesti. Tämän vuoksi Tanskan hallitus loi standardiin perustuvan yksinkertaisemman OCES-standardiin perustuvan sähköisen allekirjoituksen, jota haettaessa ei tarvitse tunnistautua henkilökohtaisesti. OCES-allekirjoitus on kehittynyt sähköinen allekirjoitus, joka perustuu ohjelmistovarmenteisiin. OCES-allekirjoitusvarmenne voidaan myöntää yksityishenkilöille, yrityksille ja työntekijöille. Varmenteen myöntäminen on periaatteessa avoin eri kaupallisille toimijoille, mutta järjestelmää valvoo maan viestintävirasto, jonka kanssa varmentaja- organisaatio (CA) tekee puitesopimuksen, jossa varmentaja sitoutuu viraston varmennuspolitiikkaan sekä antamaan sille vuosittain kertomuksen toiminnastaan sekä toimintaansa koskeviin tarkastuksiin. Sopimusjärjestely on pitkään ollut voimassa maan suurimman teleoperaattorin kanssa, mutta järjestelmää ollaan uusimassa. Monet sähköisen hallinnon sovellukset hyväksyvät OCES-allekirjoituksen. Järjestelmä tuntee sen, että luottava osapuoli osallistuu varmenteen rahoittamiseen.

Koska OCES-allekirjoitus ei ole direktiivin tarkoittama kvalifioitu sähköinen allekirjoitus, on direktiivin vastuumääräyksistä voitu poiketa siten, että varmentajalla on oikeus rajoittaa vastuutaan sopimussuhteissaan yritysten ja julkisyhteisöjen kanssa, muttei yksityishenkilöiden kanssa. OCES-allekirjoitusta haetaan varmentajan kotisivuilta henkilötunnuksen, kotiosoitteen ja sähköpostiosoitteen avulla. PIN-tunnus, jolla alle kirjoitus aktivoidaan, lähetetään kotiosoitteeseen. Henkilötunnus on olennainen kompo nentti allekirjoitusvarmennetta muodostettaessa, joten varmenne on avoin vain Tanskan henkilötunnuksen omaaville.

Viro

Viron sähköisiä allekirjoituksia koskeva laki vuodelta 2000 perustuu käsitteiltään selkeästi PKI -tekniikkaan. Laki on säädetty ennen maan liittymistä Euroopan unioniin ja on säädetty kansallisista lähtökohdista. Kuitenkin laki sääntelee direktiivin tavoin vain kehittyneitä sähköisiä allekirjoituksia ja laatuvarmenteita. Laatuvarmenteita antavien varmentajien, samoin kuin aikaleimoja myöntävien varmentajien on rekisteröidyttävä kansalliseen rekisteriin. Sähköisten allekirjoitusten aikaleimojen sääntely lailla on Viron lainsäädännön erityispiirre. Viron lakia on viime aikoina haluttu muuttaa siten, että säh-

köinen allekirjoitus voitaisiin antaa myös yrityksen nimissä. Tällaisia allekirjoituksia kutsutaan digitaalisiksi leimoiksi.

Virossa on käytössä sähköinen henkilökortti, jollainen on nykyään lähes jokaisella kansalaisella. Henkilökortin käyttö perustuu, kuten Suomessakin, henkilökorttilakiin. Laatuvarmenteita ollaan ottamassa käyttöön älykorttien lisäksi myös SIM-korteissa. Korttivalikoimaa tullaan kehittämään. Yksityinen sektori ja Viron hallitus ovat sopineet osana maan tietoturvaohjelmaa siitä, että henkilökorttien käyttö tulee entistä enemmän korvaamaan muita tekniikoita.

Viron sähköisiä allekirjoituksia koskevassa laissa todetaan varmentajan vastuu siitä, ettei tämä noudata lain tälle asettamia vaatimuksia. Varmentajalla tulee lisäksi olla vastuuvakuutus. Lain sanamuoto ei vastuukysymysten osalta direktiivin mukainen. Laissa ei todeta käänteistä todistustaakkaa. Varmenteeseen voidaan ottaa käyttörajoituksia. On kuitenkin katsottu, ettei varmentaja vastaa varmenteen käytöstä ulkopuolisille aiheutuneesta vahingosta, vaan tästä vastaa varmenteen haltija.

Sähköinen identiteetti perustuu henkilötunnukseen. Digitaalisia allekirjoituksia koskevassa laissa ei yksilöidä ensitunnistamisen menetelmiä vaan tämä jää varmentajan harkintaan. Sähköisen tunnistamisen suhteen on merkille pantavaa, että lain mukaan sähköisen allekirjoituksen on yksilöitävä henkilö, jonka nimissä se annetaan. Siten laki sääntelee myös sähköisen allekirjoituksen käyttöä tunnistamistarkoitukseen, vaikka tunnistamistoimintoa ei ole laissa yksityiskohtaisesti tarkasteltu. Käytössä olevassa henkilökortissa olevat varmenteet jakautuvat allekirjoitus- ja tunnistusvarmenteisiin.

Digitaalisia allekirjoituksia koskevan lain noudattamista valvoo maan talous- ja viestintäministeriö.

Saksa

Saksan sähköisiä allekirjoituksia koskeva laki (Gesetz über Rahmenbedingungen für elektronische Signaturen) on vuodelta 2001 ja perustuu direktiiviin. Laissa on kuitenkin aikaisemman, vuoden 1997 lain ajalta määräyksiä myös aikaleimoista ja eräät varmentajia koskevat määräykset ovat myös peräisin aikaisemmasta laista. Saksan laki tuntee mm. kvalifioidun aikaleiman. Sähköiset allekirjoitukset jaetaan tavallisiin, kehittyneisiin ja kvalifioituihin sähköisiin allekirjoituksiin. Saksassa on kymmeniä laatuvarmentajia, ja aineellinen lainsäädäntö esimerkiksi sähköisten allekirjoitusten ja julkisten hankintojen osalta on pitkään edellyttänyt kehittyneempiä sähköisen allekirjoituksen muotoja.

Varmentajia koskevat vastuusäännöt ovat laajemmat kuin direktiivissä. Varmentaja vastaa nimenomaisesti myös teknisistä turvallisuusjärjestelmistä. Saksan laissa ei ole lueteltu tämän yksityiskohtaisemmin vastuuperusteita, vaan laatuvarmentajan vastuu määräytyy yleislausekkeen pohjalta.

Laissa ei ole yksityiskohtaisia velvoitteita siitä, kuinka varmenteen hakija olisi tunnistettava, vaan laki velvoittaa tunnistamaan hakijan riittävällä tavalla. Lain noudattamista valvoo energiaa, tietoliikennettä, postia ja rautateitä valvova virasto. Laissa on ilmaistu varmentajien toimintaa valvovien viranomaisten maksut tyypeittäin, mutta maksujen täsmällisempi sisältö on määritelty alemmanasteisilla säädöksillä.

Sähköisiä allekirjoituksia koskeva laki ei sovellu suoraan sähköiseen tunnistamiseen eikä muutakaan sähköistä tunnistamista koskevaa yleislakia ole laadittu. Saksaan ollaan parhaillaan luomassa sähköistä henkilökorttia, jonka olisi määrä tulla käyttöön 2010. Sen erityispiirteisiin kuuluu myös pseudonyymin käyttö. Korttia käyttävä kansalainen voi siten valita, mitä tietoja hän itsestään luovuttaa palveluntarjoajalle. Sormenjälkien kirjaaminen korttiin on vapaaehtoista. Kortti mahdollistaa sähköisten palvelujen käytön eli toimii tunnistautumisvälineenä, ja siihen tulee mahdollisuus sähköisen allekirjoituksen käyttöön.

Itävalta

Itävallassa on säädetty sähköisiä allekirjoituksia koskeva laki EU-direktiivin pohjalta vuonna 2000 ja vastaava asetus viimeksi vuonna 2004. Sähköinen allekirjoitus voidaan myöntää vain luonnolliselle henkilölle, mutta sähköistä hallintoa koskeva erityis-

lainsäädäntö sisältää määräyksiä toisen lukuun tapahtuvasta allekirjoituksen käytöstä.

Laki käyttää turvallisen sähköisen allekirjoituksen määritelmää samassa tarkoituksessa kuin Saksassa puhutaan kvalifioidusta sähköisestä allekirjoituksesta. Sähköisiä allekirjoituksia koskevan lain vastuumääräykset perustuvat EU-direktiiviin, mutta Itävallan lakiin on otettu vaatimus varmentajan vastuuvakuutuksesta.

Viranomaisvalvonta Itävallassa kuuluu maan viestintävirastolle, joka valvoo kaikkia varmentajia, joiden tulee toimittaa sille kirjallinen turvapolitiikkansa. Näin myös sähköistä tunnistamista varten myönnetyt varmenteet ovat periaatteessa valvonnan piirissä. Sähköisiä allekirjoituksista annetun lain mukaisia laatuvarmentajia on tällä hetkellä maassa vain yksi.

Kansalaisten sähköinen identiteetti perustuu henkilötunnukseen, josta on johdettu Suomen sähköistä asiointitunnusta muistuttava PIN-tunnus. Käyttäjä voi valita sen, milloin tunnus julkistetaan. Sähköinen henkilökortti yhdistää tunnistamisen (identification), alkuperän todentamisen (authentication), sähköisen allekirjoituksen sekä mahdolliset valtuutustiedot (mandate). Henkilökorttia voi käyttää myös matkapuhelimen välityksellä (mobiilivarmenne). Henkilökortin voi antaa myös yksityinen taho, kuten pankki. Tunnistaminen ja allekirjoitus eivät kuitenkaan toimintoina poikkea toisistaan, vaan esimerkiksi julkisen hallinnon tiedostoihin kirjautuminen edellyttää sähköisellä allekirjoituksella ilmaistun tahdonilmaisun käyttöä.

Yhdistyneet Kuningaskunnat

Sähköisiä allekirjoituksia koskeva direktiivi on saatettu voimaan kahdella eri lailla, joista keskeisempi on Electronic Signatures Regulations 2002. Laki perustuu sanamuodoiltaan selkeästi direktiiviin. Myös oikeushenkilöt voivat saada sähköisen allekirjoituksen. Vastuukysymysten osalta ei lakiin ole otettu mainintoja direktiivissä sallittuihin vastuunrajoituksiin. Yleisenä periaatteena varmentajan vastuussa sopimussuhteen ulkopuolella olevalle luottavalle osapuolelle on siviilioikeudellinen deliktivastuu (tort liability).

Yhdistyneet kuningaskunnat on päättänyt ryhtyä myöntämään sähköistä henkilökorttia, mitä varten myös keskitetty väestökirjanpito on luotava. Muutos on suuri, sillä maassa ei ole ollut perinteitä väestökirjanpidosta eikä siihen perustuvista rekistereistä. Rekisteröityminen on kuitenkin vapaaehtoista ja tapahtuu käytännössä juuri sähköisen identiteetin luomiseksi henkilökortilla. Järjestelmä on luotu parlamentin säätämällä henkilökorttilailla (Identity Cards Act 2005). Henkilökortti on tarkoitettu erityisesti julkisten palvelujen käyttämiseen ja sen myöntää viranomainen.

Henkilökorttilaki perustuu henkilön rekisteröimiseen väestörekisteriin, minkä perusteella henkilökortti myönnetään. Viranomaiselle on jätetty harkintavaltaa vaatia selvityksiä henkilön identiteetin todentamiseksi väestörekisterijärjestelmässä rekisteröinti- hakemuksen jälkeen. Viranomainen voi vaatia henkilökohtaista käyntiä, henkilön valokuvaamista tai jopa biometristen tunnisteiden ottoa. Laki ei sääntele viranomaisvastuuta kortin myöntämisessä tapahtuvien virheiden osalta, vaan asia ratkaistaan yleisten vahingonkorvausoikeudellisten sääntöjen pohjalta.

Belgia

Belgian laki sähköisistä allekirjoituksista on vuodelta 2001. Laki perustuu melko yksityiskohtaisesti direktiivin määräyksiin. Myös oikeushenkilö voi saada varmenteen.

Sähköistä tunnistamista koskevaa yleislainsäädäntöä ei ole säädetty, mutta Belgiassa on toteutettu henkilökorttiin perustuva sähköinen identiteetti. Henkilökortti perustuu väestörekisterijärjestelmään ja sitä koskevaan lainsäädäntöön. Sähköisestä henkilökortista annettiin asetus vuonna 2003 ja järjestelmä kattaa jo useimmat maassa asuvat henkilöt. Henkilökortti sisältää kvalifioidun sähköisen allekirjoituksen sisältävän varmenteen, jota käytännössä käytetään myös tunnistautumistarkoituksessa. Varmenteen myöntää Certipost, joka on Belgian postin ja maan johtavan tele- operaattorin Belgacomin yhteisyritys. Maan viranomaiset ovat hyväksyneet kolme laatuvarmentajaa, joiden antamat varmenteet hyväksytään sähköisen hallinnon järjestelmissä.

Sähköisen henkilökortin lisäksi myös kaupalliset varmenteet oikeuttavat pääsyyn sähköisen hallinnon tietojärjestelmiin. Näiden osalta vaaditaan aina, että varmennetta hakeva henkilö tunnistetaan kasvotusten. Kaupalliset varmenteet ovat käyttökelpoisia niiden sähköistä henkilökorttia suuremman tietosisällön vuoksi ja siksi, että niitä voidaan käyttää myös salaukseen.

Espanja

Espanjan sähköisiä allekirjoituksia koskeva laki on vuodelta 1999, ja sitä täydentää asetus vuodelta 2000. Lain mukaan myös oikeushenkilö voi saada direktiivin tarkoittaman kvalifioidun sähköisen allekirjoituksen. Espanjassa ei ole yleislakia sähköisestä tunnistamisesta, vaan maassa on panostettu sähköisen henkilökortin kehittämiseen.

Espanjan sähköisiä allekirjoituksia koskeva laki ulottuu selvästi laajemmaksi kuin kvalifioituihin sähköisiin allekirjoituksiin. Laki sisältää vastuusäännöksen, joka kattaa myös muut varmentajat kuin laatuvarmenteita myöntävät varmentajat, mutta joka perustuu direktiivin järjestelmään. Laki sisältää samanlaisen yksityiskohtaisen luettelon varmentajan vastuuvapaus- tai rajoitusperusteista kuten Suomen sähköisiä allekirjoituksia koskevan lain 16 §. Varmentajia koskevat vastuusäännöt voivat käytännössä koskea allekirjoitusten lisäksi myös tunnistautumista, koska sähköistä allekirjoitusta tarkoittavia varmenteita käytetään myös tunnistautumiseen. Laki sisältää myös vaatimuksen, jonka mukaan varmentajalla tulee olla vähintään 3.000.000 vakuutusmäärän kattava vastuuvakuutus. Varmentajat velvoitetaan julkaisemaan varmennepolitiikkansa.

Espanjassa on otettu käyttöön sähköinen henkilökortti, joka mahdollistaa sitä koskevan säädöksen (Real Decreto 1553/2005) mukaan henkilöllisyyden todentamisen ja sähköisen allekirjoituksen kaikissa sähköisen hallinnon sovelluksissa. Säädöksen mukaan henkilökortin saaminen edellyttää fyysistä ensitunnistamista. Myös kortin uusiminen edellyttää fyysistä tunnistamista.

Slovenia

Slovenian laki sähköisistä allekirjoituksista on vuodelta 2000, ja se sisältää myös sähköistä kaupankäyntiä koskevia määräyksiä. Laki perustuu EU-direktiiviin, vaikka Slovenia ei ollut sitä säädettäessä vielä Euroopan Unionin jäsen. Slovenian laki ei sääntele erikseen sähköistä tunnistamista.

Direktiivistä poiketen Slovenian sähköisiä allekirjoituksia koskeva laki tuntee sähköisten allekirjoitusten osalta myös aikaleiman käsitteen. Direktiivin vastuusäännökset on otettu sellaisenaan lakiin. Siinä on kuitenkin lueteltu eräitä varmentajan vastuuperusteita direktiivissä olevien lisäksi. Lakia täydentää asetus, joka sääntelee varmentajille asetettavia vaatimuksia, kuten pakollisen vastuuvakuutuksen, henkilökuntaa ja välineistöä koskevat vaatimukset ja sisäiset säännöt. Julkisomisteinen varmennuslaitos antaa varmenteita virkamieskunnan lisäksi myös yksittäisille kansalaisille ja yrityksille.

Vuonna 2004 sähköisiä allekirjoituksia ja sähköistä kauppaa koskevaan lakiin otettiin määräyksiä sähköisen henkilökorttijärjestelmän kehittämisestä. Järjestelmää ei ole vielä pantu täytäntöön. Henkilökortti on perinteinen henkilöllisyystodistus, joka sisältää laatuvarmenteen. Järjestelmä perustuu henkilötunnuksiin ja erillisiin sähköisiin asiointitunnuksiin.

Turkki

Turkin laki sähköisistä allekirjoituksista on vuodelta 2004. Laki perustuu Euroopan Unionin direktiiviin, mutta sisältää määräyksiä myös mm. valvonnasta, sähköisiin allekirjoituksiin liittyvistä rikoksista ja rangaistuksista. Määritelmäosa sisältää myös aikaleiman määritelmän, vaikkei laki Viron lain tavoin sääntele aikaleimavarmentajien toimintaa yksityiskohtaisesti. Laki puhuu turvallisesta sähköisestä allekirjoituksesta eikä käytä kehittyneen sähköisen allekirjoituksen käsitettä. Turvallinen sähköinen allekirjoitus nostetaan direktiivistä poiketen selkeästi erityisasemaan oikeudellisessa mielessä. Direktiivin tavoin laki jättää sähköisen tunnistamisen sääntelemättä.

Sähköisiä allekirjoituksia koskevat vastuusäännöt ovat direktiiviä yksityiskohtaisemmat vaikka toteuttavatkin direktiivin luoman vastuujärjestelmän perusperiaatteet. Erityismääräyksiä on mm. varmentajan isännänvastuusta työntekijöidensä suhteen eräissä tilanteissa. Varmentajilta edellytetään pakollista vastuuvakuutusta. Laki ei vaadi nimenomaista ensitunnistamista, vaan varmenteen hakija on tunnistettava luotettavasti asiakirjoista.

Lakia valvoo Turkin viestintävirasto. Valvonta koskee kuitenkin vain Turkin lain itsenäisesti määrittelemiä kvalifioituja sähköisiä allekirjoituksia myöntäviä varmentajia sekä aikaleimavarmentajia. Tämä jättää sähköiseen tunnistamiseen liittyvät toiminnot ulkopuolelle.

Kansainväliset järjestöt

OECD

Taloudellisen yhteistyön ja kehityksen järjestö OECD on jo kymmenen vuoden ajan työskennellyt sähköisen tunnistamisen kehittämiseksi. Vuonna 1998 Ottawassa Kanadassa pidetyssä ministerikonferenssissa annettiin julistus (Declaration on Authentication for Electronic Commerce). Järjestö on julkaissut useita vertailevia tutkimuksia sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Kesäkuussa 2007 OECD julkaisi suosituksen (OECD Recommendation for Electronic Authentication), jota täydentävät soveltamisohjeet.

Suosituksessaan OECD suosittelee jäsenmailleen, että nämä ottaisivat teknologianeutraalin lähestymistavan henkilöiden ja organisaatioiden sekä kotimaiseen että rajat ylittävään sähköiseen tunnistamiseen viitaten samalla järjestön omiin tietoturvaa ja tietosuojaa koskeviin toimintaohjeisiinsa (guidelines). Jäsenmaiden tulisi myös tukea sähköiseen tunnistamiseen käytettävien, kaupallisesti toimintakelpoisten ja turvallisten tuotteiden ja palveluiden kehittämistä, tarjontaa ja käyttöä. Niin ikään jäsenmaiden tulee edistää sekä yksityisellä että julkisella sektorilla tunnistamisjärjestelmien kaupallista yhteensoveltuvuutta ja teknistä yhteentoimivuutta (interoperability), jotta järjestelmät palvelisivat sähköistä asiointia ja vaihdantaa yli toimialoja ja oikeusjärjestystä koskevien rajojen ja olisivat otettavissa käyttöön niin kotimaassa kuin kansainvälisesti. OECD suosittaa myös tietoisuuden lisäämistä sähköisen tunnistamisen eduista sekä kansallisesti että kansainvälisesti.

UNCITRAL

Yhdistyneiden Kansakuntien (jäljempänä YK) kansainvälisen kauppaoikeuden toimikunnan (jäljempänä UNCITRAL) hyväksyi 34. istunnossaan kesällä 2001 mallilain sähköisistä allekirjoituksista (jäljempänä mallilaki). Lisäksi on laadittu opas mallilain tulkinnasta (Guide to Enactment).

UNCITRAL:n mallilain valmistelutyö tarjosi YK:n jäsenvaltioille sähköisten allekirjoitusten sääntelyn kehittämisessä tarvittavan kansainvälisen keskustelufoorumin. Mallilaki toimi esimerkkinä lainvalmistelulle erityisesti Euroopan ulkopuolisissa maissa. Mallilain valmistelun yhteydessä esille nostetut ongelmat ja ongelmanratkaisut huomioon ottavia lainsäädäntöhankkeita on ollut vireillä tai jo loppuun saatettu muun muassa Argentiinassa, Australiassa, Brasiliassa, Intiassa, Kanadassa, Koreassa, Meksikossa, Romaniassa, Thaimaassa, Singaporessa ja Uudessa-Seelannissa. Myös sähköallekirjotusdirektiivin valmistelutyössä hyödynnettiin UNCITRAL:n mallilain valmistelutyön tuloksia.

Mallilaki sisältää sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin kaltaisia säännöksiä muun muassa sähköisen allekirjoituksen oikeusvaikutuksista, varmenteen tietosisällöstä, varmentajan vastuusta ja varmenteiden vastavuoroisesta hyväksymisestä. Mallilaki eroaa direktiivistä siinä suhteessa, että se korostaa sopimusosapuolten oikeutta sopia mallilain säännöksistä toisin. Sopimusosapuolten autonomiaa korostava lähtökohta johtuu pääasiassa Yhdysvaltain lainsäädännön voimakkaasta vaikutuksesta mallilain valmisteluun. Toisin kuin direktiivi, mallilaki sisältää myös allekirjoittajan vastuuta koskevia säännöksiä. Mallilaissa allekirjoittajalle asetetaan muun muassa velvoite säilyttää avainta huolellisesti ja velvoite ilmoittaa varmentajalle välittömästi avaimen katoamisesta tai muusta alle-

kirjoituksen turvallisuutta vaarantavasta tapahtumasta.

Muu kansainvälinen yhteistyö

Useat valtiot ovat julkaisseet tunnistamiseen liittyviä toimintaohjelmia. Myös jotkut yksityiset organisaatiot ja ryhmittymät työskentelevät tunnistamisen sekä kansalaisten sähköisen identiteetin ja alan kansainvälisen yhteistyön parissa. Erityisesti voidaan mainita Suomessa perustettu Porvoo-ryhmä. Se on kansainvälinen yhteistyöverkosto, jonka päätavoitteena on edistää eri maiden välillä yhteensopivan, julkisen avaimen teknologiaan sekä älykortteihin ja sirullisiin henkilökortteihin perustuvan sähköisen henkilöllisyyden toteutumista. Tarkoituksena on auttaa varmistamaan turvallista julkisen ja yksityisen sektorin sähköistä asiointia Euroopassa. Ryhmä edistää myös yhteensopivien varmenteiden ja teknisten määritysten käyttöönottoa, tunnistus- ja autentikointimekanismien vastavuoroista hyväksymistä eri maiden välillä sekä maiden rajat ylittävän online-yhteyden toteutumista hallinnon palveluihin.

Standardointi

Sähköisistä allekirjoituksista annetun direktiivin vaatimusten toteuttamiseksi perustettiin vuonna 1999 Eurooppalaisen teollisuuden ja standardointiorganisaatioiden yhteishanke European Electronic Signature Standardization Initiave (jäljempänä EESSI). EESSI:n puitteissa European Telecommunications Standards Institute:ssa (jäljempänä ETSI) ja European Committee for Standardization:ssa (jäljempänä CEN) on standardoitu useita alueita sähköisten allekirjoitusten ja varmennepalveluiden tuotteisiin, järjestelmiin ja palveluihin liittyen. Tärkeimpiä ETSIn standardeja on laatuvarmentajan toimintaa koskeva ETSI TS 101 456 (Policy requirements for CAs issuing qualified signatures). Myös laatuvarmenteen tietosisältö ja sähköisen allekirjoituksen formaatti on standardoitu ETSI:ssä. CEN:ssä on standardoitu muun muassa laatuvarmentajan käyttämien järjestelmien tietoturvavaatimukset sekä vaatimukset turvallisille allekirjoituksen luomisvälineille siten kuin sähköisistä allekirjoituksista annetussa direktiivissä edellytetään. Näiden standardien viitenumerot on myös julkaistu Euroopan yhteisöjen virallisessa lehdessä (EYVL 15.7.2003, L 175/45).

EESSI lopetettiin lokakuussa vuonna 2004. Sähköisiä allekirjoituksia koskeva standardointityö jatkuu edelleen, joskin keskittyen muihin kuin perusvaatimuksiin. ETSI:n TC ESI:ssä painopistealueina ovat sähköinen kirjanpito ja laskutus (digital accounting and invoicing) sekä varmennettu sähköposti (Registered E-mail, REM). CEN:n sähköisen allekirjoituksen välineisiin keskittynyt standardointityöryhmä (CEN/ISSS E-sign) lopetettiin vuonna 2003, mutta CEN:n jäsenet ylläpitävät ja päivittävät edelleen aihealueen standardeja ja CEN:ssä on useita muita työryhmiä, jotka laativat standardeja eri sähköisen asioinnin alueille. Sähköisiin allekirjoituksiin liittyvän standardointityön mahdollisista koordinointitarpeista vastaa EESSI:n lopettamisen jälkeen ICTSB:n (ICT Standards Board) Network and Information Security Steering Group (NISSG).

Maksupalveludirektiivi

Euroopan parlamentti ja neuvosto antoivat 13 päivänä marraskuuta 2007 direktiivin maksupalveluista sisämarkkinoilla (2007/64/EY). Direktiivin tavoitteena on luoda yhtenäinen maksualue, jossa lisääntyneet kokoedut ja kilpailu laskisivat maksujärjestelmien nykyisin korkeita kustannuksia. Direktiivillä perustetaan yhtenäinen lainsäädäntökehikko yhteisön maksamiseen liittyville markkinoille, mikä luo olosuhteet maksujärjestelmien yhdentymiselle ja järkeistämiselle. Direktiivi on käsillä olevan esityksen kannalta merkityksellinen sen vuoksi, että sähköisten tunnistuspalveluiden ja maksupalveluiden tarjoamisessa on joitakin yhteneväisiä piirteitä. Lisäksi vahvan sähköisen tunnistuspalvelun tarjoajat voivat samaan aikaan olla myös maksupalvelun tarjoajia.

Maksupalveludirektiivi on luonteeltaan pääosin täysharmonisointia. Jäsenvaltiot eivät voi direktiivissä mainittuja poikkeuksia lukuun ottamatta kansallisesti säätää tai pitää voimassa muita säännöksiä direktiivillä säänneltävistä seikoista.

Maksupalveluiden tarjoajat jaetaan direktiivin 1 artiklassa neljään ryhmään: luottolaitokset; sähköisen rahan liikkeeseenlaskijat; postit, joilla on kansallisen lainsäädännön perusteella mahdollisuus tarjota maksupalveluita, sekä maksulaitokset, joita ovat muut luonnolliset tai juridiset henkilöt, joille on myönnetty direktiivin mukaisesti toimilupa tarjota maksupalveluita. Direktiivissä säädetään siitä, mitä tietoja maksupalveluista on annettava sekä maksupalvelun käyttäjien ja tarjoajien oikeuksista ja velvollisuuksista.

Direktiivin soveltamisala kattaa 2 artiklan mukaan maksupalvelut, joissa suoritetaan maksuja toisen toimijan puolesta ja joissa ainakin yksi maksupalvelun tarjoaja on sijoittunut EU:n alueelle. Direktiivi soveltuu niin rajat ylittäviin kuin puhtaasti kansallisiin maksupalveluihin. Direktiivi soveltuu lähtökohtaisesti maksuihin missä tahansa valuutassa.

Direktiivin 3 artiklan mukaan soveltamisalan ulkopuolelle jääviä toimintoja ovat muun muassa käteismaksut, lahjakorteilla, sekeillä ja muilla paperipohjaisilla välineillä tehtävät maksut, valuutanvaihto sekä maksupalvelutoimijoiden väliset maksut. Soveltamisalan ulkopuolella jää myös matkapuhelimella sekä muulla digitaalisella tai automaattisen tietojenkäsittelyn välineellä tehdyt maksut, edellyttäen, että sähköisen viestinnän, automaattisen tietojenkäsittelyjärjestelmän tai verkon palveluntarjoaja osallistuu tiiviisti digitaalisen hyödykkeen tai palvelun kehittämiseen, palveluita tai hyödykkeitä ei voida toimittaa ilman palveluntarjoajaa, eikä ole muuta tapaa suorittaa maksu.

Direktiivin kansallinen täytäntöönpano on parhaillaan käynnissä valtiovarainministeriön ja oikeusministeriön johtamista työryhmissä. Kansallisten lakien tulee direktiivin mukaan olla voimassa viimeistään 1 päivänä marraskuuta 2009.

Palveludirektiivi

Euroopan parlamentin ja neuvoston direktiivi 2006/123/EY palveluista sisämarkkinoilla (jäljempänä palveludirektiivi) hyväksyttiin Suomen EU-puheenjohtajakauden lopussa joulukuussa 2006. Palveludirektiivi tulee saattaa voimaan kolmessa vuodessa sen voimaantulosta, eli viimeistään 28 päivään joulukuuta 2009 mennessä. Käsillä olevassa esityksessä säänneltävät palvelut kuuluvat palveludirektiivin soveltamisalaan.

Direktiivin aineellinen sisältö muodostaa eräänlaisen vertailukehyksen, jonka perusteella palvelun tarjoajiin kohdistuvia menettelyjä ja muodollisuuksia tulee arvioida. Menettelyjen ja muodollisuuksien on oltava syrjimättömiä, niiden on perustuttava yleisen edun mukaiseen pakottavaan syyhyn sekä oltava välttämättömiä ja oikeasuhteisia. Jäsenvaltioiden on myös tarkistettava tiettyjä viranomaistoimintoja hallinnollisen yksinkertaistamisen turvaamiseksi.

Hallinnollisen yksinkertaistamisen tehostamiseksi on palveludirektiivissä säädetty, että jäsenvaltioiden on järjestettävä keskitettyjä asiointipisteitä, joiden kautta palveluntarjoajat voivat saada tietoa palvelujen tarjoamiseen liittyvistä kansallisista vaatimuksista. Palveluntarjoajien tulee myös voida suorittaa kaikki palvelun tarjoamiseen liittyvät hallinnolliset menettelyt ja muodollisuudet sähköisesti näiden keskitettyjen asiointipisteiden kautta.

Palveludirektiivi velvoittaa jäsenvaltioita kehittämään viranomaisten välistä hallinnollista yhteistyötä. Rajat ylittävän viranomaisyhteistyön merkitys tulee korostumaan jäsenvaltioiden keventäessä palveluntarjoajiin kohdistuvia hallinnollisia menettelyjä. Yhteistyötä tullaan toteuttamaan muun muassa komission ylläpitämällä sisämarkkinoiden tietojenvaihtojärjestelmällä (IMI, Internal Market Information System).

Palveludirektiivin nojalla jäsenvaltiot joutuvat siten toteuttamaan paitsi lainsäädännöllisiä toimia myös muita toimia, kuten kehittämään sähköisiä hallintomenettelyjä ja hallinnollisen yhteistyön rakenteita. Kansallisen täytäntöönpanon osalta kyse ei siis ole niin sanotusta puhtaasta lainsäädäntöhankkeesta, vaan hankkeessa on toteutettava huomattava määrä käytännön toimenpiteitä direktiivin tehokkaan täytäntöönpanon varmistamiseksi.

Palveludirektiivin kansallinen voimaanpano on parhaillaan käynnissä työ- ja elinkeinoministeriössä. Ehdotetussa laissa palveludirektiivi on myös pyritty huomioimaan siten, että siinä ei ole mitään palveludirektiivin kanssa ristiriitaista. Palveludirektiivi muun

muassa kieltää pääsääntönsä mukaisesti ennakolliset toimiluvat. Vahvan sähköisen tunnistamisen palveluntarjoajiin kohdistuu ainoastaan ilmoitusmenettely, joka on tarpeen, jotta valvova viranomainen voi täyttää omat velvollisuutensa.

Ehdotetut säännökset velvoittavat Viestintävirastoa kieltämään palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena, mikäli palveluun tai palveluntarjoajaan kohdistetut laissa asetetut edellytykset eivät täyty. Palveluntarjoaja voi kuitenkin aloittaa palvelunsa tarjoamisen ilman Viestintäviraston reagointia asiaan. Lisäksi on huomattava, että sääntely ei estä palvelun tarjoamista ylipäätään, vaan ainoastaan sen tarjoamista tietynlaisena palveluna, mikäli edellytykset eivät täyty. Järjestely vastaa täysin sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin perustuvaa laatuvarmenteita koskevaa luvun 4 sääntelyä. Jos siinä asetetut edellytykset eivät täyty, Viestintäviraston on kiellettävä palveluntarjoajaa tarjoamasta palveluaan laatuvarmenteiden tarjontana. Tämä ei kuitenkaan estä palveluntarjontaa sinänsä. Lukuun 4 sisältyy lisäksi tarkastuslaitoksiin kohdistuvaa sääntelyä, jonka mukaan Viestintävirasto nimeää tarkastuslaitokset. Tämä perustuu niin ikään sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin, jota on pidettävä erityissääntelynä suhteessa palveludirektiiviin.

2.4 Sähköinen tunnistamien ja sähköinen allekirjoitus

Sähköisten allekirjoitusten markkinat eivät Suomessa ole lähteneet kehittymään toivotulla tavalla. Sähköisen allekirjoittamisen palveluita tarjoaa tällä hetkellä ainoastaan Väestörekisterikeskus. Sähköinen allekirjoitus ylipäätään on jäänyt hyvin vähäiselle käytölle niin Suomessa kuin muuallakin Euroopassa. Erityisesti kysymykset luottamuksesta sekä vastuista ovat osoittautuneet vaikeiksi ratkaista.

Myös itse sähköisen allekirjoituksen käsite on ongelmallinen sellaisissa maissa kuin Suomessa, jossa hyvin harvojen oikeustointen edellytyksenä on jokin allekirjoituksen kaltainen muotovaatimus. Pankkitunnisteisiin perustuvan sähköisen tunnistamisen avulla on voitu Suomessa tosiasiassa saada aikaan samat oikeusvaikutukset kuin sähköisen allekirjoituksen avulla,. Seurauksena on kuitenkin ollut jatkuva keskustelu siitä, millaisia välineitä ja menetelmiä edellytetään oikeusvaikutusten aikaan saamiseksi missäkin tilanteessa.

Myös jatkossa sähköisten allekirjoituspalveluiden kysyntä ja tarjonta lienevät varsin vähäisiä. Komission pyrkimykset kehittää sähköisten allekirjoitusten rajat ylittävää käyttöä erityisesti laatuvarmenteisiin pohjautuen saattavat hieman lisätä kysyntää. Komission pyrkimyksistä johtuen erityisesti suomalaisten yritysten Euroopan talousalueelle suuntautuvan toiminnan kannalta näyttää ainakin lyhyellä tähtäimellä olevan tärkeää, että lainsäädännöllä varmistetaan Suomessa toimivien laatuvarmenteita yleisölle tarjoavien toimijoiden toimintamahdollisuudet. Luonnollisesti myös sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi edellyttää jatkossakin täytäntöönpanoa.

Sähköisten allekirjoitusten asemesta tarvetta näyttää olevan huomattavasti enemmän sähköiselle tunnistamiselle. Sähköisten palveluiden määrän ja kirjon kasvu edellyttää jatkossa yhä useammin luotettavaa sähköistä tunnistamista. Tämän johdosta Suomessa on tarve synnyttää toimivat vahvan sähköisen tunnistamisen markkinat. Tällä hetkellä vahvaan sähköiseen tunnistamiseen käytetään lähes yksinomaan pankkitunnuksia. Nämä tunnukset tulevat varmasti olemaan käytössä vielä useita vuosia, mutta niiden rinnalle kaivataan lisää palveluita ja palveluntarjoajia. Toimivat, kilpaillut markkinat pitävät huolen myös palveluiden kohtuullisesta hintatasosta.

Olemassa ei ole sähköistä tunnistamista koskevaa lainsäädäntöä. Tämän puutteen johdosta sääntöjä toiminnalle on haettu erityisesti sähköisiä allekirjoituksia koskevasta laista. Koska laki käytännössä koskee ainoastaan laatuvarmenteiden tarjoamista yleisölle direktiiviin perustuen, eivät säännökset ole erityisen hyvin soveltuneet sähköisten tunnistuspalveluiden tarjoamiseen. Lisäksi lain säännöksiä on jossain määrin tulkittu väärin tavalla, joka on luonut orastavalle palveluntarjonnalle liian raskaita vaatimuksia.

Olemassa ei myöskään ole yleisellä tasolla sääntelyä siitä, milloin tarvitaan vahvaa sähköistä tunnistamista. Tyypillisiä käyttötilanteita voisivat olla erityisesti taloudellisia tai oikeudellisia sitoumuksia edellyttävät sähköiset palvelut. Tällaisen yleisen sääntelyn antaminen on tällä hetkellä ja todennäköisesti jatkossakin tarpeetonta, eikä myöskään käsillä oleva esitys sisällä tällaisia säännöksiä.

Olemassa on kuitenkin jo nykyään säännöksi, joissa on kysymys tiettyjä tilanteita koskevasta sääntelystä. Sähköisestä asioinnista viranomaisessa annetun lain 18 § koskee todisteellista sähköistä tiedoksiantoa. Sen 2 momentin mukaan asianosaisen tai tämän edustajan on tunnistauduttava päätöstä noutaessaan. Lisäksi rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetun lain (503/2008) 18 §:ssä on säädetty etätunnistamiseen liittyvästä tehostetusta tuntemisvelvollisuudesta. Pykälän 3 kohdassa säädetään niistä tunnistamistavoista, joita etätunnistamisessa voidaan käyttää.

Jatkossa tällaisten erityisiä tilanteita koskevien säännösten määrä saattaa lisääntyä. Myös tämän mahdollisen kehityskulun kannalta on erittäin tärkeää saada aikaan sääntelykehys, johon muu lainsäädäntö voi nojautua.

Valtiontalouden tarkastusviraston raportti

Valtiontalouden tarkastusvirasto julkaisi keväällä 2008 raporttinsa tunnistuspalveluiden kehittämisestä ja käytöstä julkisessa hallinnossa (161/2008). Raportissaan tarkastusvirasto havaitsi paljon puutteita ja epäkohtia muun muassa viranomaisten välisessä yhteistyössä ja koordinoinnissa, hankintamenettelyissä, Väestörekisterikeskuksen toiminnassa ja sen toiminnan järjestämisessä sekä Terveydenhuollon oikeusturvakeskuksen, Verohallituksen ja tietosuojavaltuutetun toiminnassa.

On selvää, että ehdotetulla lailla voidaan pyrkiä vaikuttamaan vain osaan niistä epäkohdista, joihin tarkastusvirasto on raportissaan kiinnittänyt huomiota. Työ tulee jatkumaan erityisesti vuosina 2009-2010 valtioneuvoston 5 päivänä maaliskuuta 2009 hyväksymässä sähköistä tunnistamista koskevassa periaatepäätöksessä sovitulla tavalla.

Tarkastusviraston raportissa on joitakin huomioita, jotka liittyvät esitykseen. Toiminnan ohjausrakenteiden ja lainsäädännön kehittämisen osalta raportissa todetaan muun muassa, että tarkastusviraston näkemyksen mukaan toiminnan yhdenmukaistaminen ja rationalisointi, valvonnan tehostaminen, tietoturvallisuutta koskevat menettelyt, vapaiden tunnistemarkkinoiden toimivuus sekä erityisesti yksilöiden oikeusturva ja tietosuoja edellyttävät tunnistuspalveluita ja tunnistamista koskevaa lakitasoista sääntelyä. Liikenne- ja viestintäministeriön, valtiovarainministeriön ja oikeusministeriön tulisikin ryhtyä yhteistyössä pikaisiin toimenpiteisiin sähköisen tunnistuksen lainsäädännön kehittämiseksi.

Edelleen tarkastusviraston näkemyksen mukaan Viestintäviraston perimälle varmenteiden määrään perustuvalle varmennemaksulle ei ole tosiasiallisia perusteita ja se on varmennemarkkinoiden toimivuuden kannalta ongelmallinen. Tarkastusvirasto katsoo, että liikenne- ja viestintäministeriön on ryhdyttävä toimenpiteisiin varmennevalvonnan maksujen uudistamiseksi siten, että maksun perusteena on muu kuin varmenteiden määrä.

Tunnistuspalvelumarkkinoiden ja niihin liittyvien riskien osalta tarkastusvirasto kiinnittää huomiota siihen, että nykyisillä tunnistuspalvelumarkkinoilla ei ole todellista kilpailua, vaan tunnisteiden käyttö on keskittynyt verkkopankkitunnisteiden käyttöön. Tähän voi liittyä pitemmällä aikavälillä taloudellisia riskejä. Toisaalta valtionhallinnon omilla toimenpiteillä on ollut vaikutuksensa syntyneeseen tilanteeseen. Tarkastuksessa on ilmennyt, että Väestörekisterikeskuksen toiminta on ollut vuosituhannen vaihteessa markkinoita vääristävää, mikä on ollut osaltaan vaikuttamassa yksityisten vastaavia varmennepalvelutoimintoja harjoittavien toimijoiden toiminnan lopettamiseen. Väestörekisterikeskus ei ole puolestaan pystynyt tarjoamaan käyttökelpoista vaihtoehtoa suurten massojen käyttöön tunnistusvälineeksi.

Edelleen tarkastusvirasto katsoo, että vain tunnistuspalveluiden välinen aito kilpailu pitää huolen siitä, että tunnistustapahtumien hinnat pysyvät kohtuullisina verkkopankkitunnisteita tai muita tunnisteita käytettäessä. Julkisen hallinnon tulee olla avoin tunniste-

markkinoilla kehitettäville uusille tunnistuspalveluratkaisuille. Julkisen hallinnon on huolehdittava kuitenkin uusien tunnistuspalveluiden turvallisuustason tasapuolisesta määrittelystä ja sertifioinnista, jonka perusteella tunnistuspalvelu voidaan hyväksyä julkisen hallinnon käyttöön esimerkiksi vahvaa tunnistusta edellyttäviin sähköisiin palveluihin.

Tarkastusviraston näkemyksen mukaan julkisen hallinnon tulisi keskittyä hyödyntämään jo markkinoilla olemassa olevia sekä kehitettäviä tunnistuspalveluita eikä sen tulisi osallistua suoraan tunnistusvälineiden tuottamiseen. Yksityisten toimijoiden tehtäväksi tulisi jättää tunnistusmenetelmien ja -välineiden kehittäminen ja niiden saattaminen laajaan käyttöön. Julkinen hallinto voi tukea kehitystoimintaa ja luoda edellytyksiä toiminnalle tukimus- ja kehitysrahoituksella, kuitenkin siten, että se ei aiheuta markkinoilla vääristymiä.

Väestörekisterikeskuksen osalta tarkastusvirasto katsoo, että Väestörekisterikeskuksen tulee vastaisuudessa keskittyä vain viranomaistehtäviinsä ja siirtää muut liiketoimintaan tai muuhun kuin ydintoimintaan liittyvät tehtävät markkinoiden hoidettavaksi.

Tarkastusviraston näkemyksen mukaan varmennepalveluinfrastruktuurin hankinta tulisi vastaisuudessa hoitaa täysin ulkoistettuna palveluna. Väestörekisterikeskuksen tehtävänä on tällöin huolehtia palvelun toiminnan laadun varmistamisesta ja viranomaistehtävistä lähinnä rekisteröinnin osalta. Ulkoistaminen ja sovellusvuokraus voivat motivoida myös markkinoilla toimivia IT-toimittajia kehittämään palveluitansa siten, että ne tukevat julkisen hallinnon toimintaa. Toimintamalli olisi valtion IT-strategian mukainen siten, että tällöin ei turvauduttaisi yhteen palvelun toimittajaan. Toisaalta muutkin viranomaiset voisivat tuottaa varmenteita omiin käyttötarkoituksiinsa samasta puitejärjestelyllä hankitusta varmennepalvelukokonaisuudesta ilman Väestörekisterikeskuksen toimimista välikätenä ja kustannuksia lisäävänä toimijana. Myös varmennetoiminnan yleisiä edellytyksiä ja valtion roolia siinä tulisi arvioida uudelleen.

3 Esityksen tavoitteet ja keskeiset ehdotukset

3.1 Tavoitteet

Esityksellä annettaisiin kokonaan uusi laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Samalla nykyinen laki sähköisistä allekirjoituksista ehdotetaan kumottavaksi.

Lain tarkoituksena on edistää vahvan sähköisen tunnistamisen palveluiden tarjontaa ja luoda markkinoille perussäännökset palveluiden tarjontaan. Samalla pyritään varmistamaan, että palveluiden tarjonnassa otetaan huomioon tietoturvan ja tietosuojan vaatimukset. Edistämällä sähköisten tunnistuspalveluiden tarjontaa lain tarkoituksena on edistää sähköisiä palveluita ja sähköistä asiointia yleensä sekä niiden tietosuojaa ja tietoturvaa.

Lailla pyritään luomaan toimivat sähköisen tunnistamisen markkinat antamalla alan toimijoille tietyt perussäännöt. Näiden markkinoiden lähtökohtana ovat tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu. Sähköinen tunnistaminen toimii pääsääntöisesti palveluntarjoajien muodostamassa luottamusverkostossa. Tietyt perussäännöt ja niiden noudattamisen valvonta antavat toisille palveluntarjoajille tiedon siitä, että kaikki alan toimijat täyttävät tietyn perustason omassa toiminnassaan. Tämä helpottaa olennaisesti luottamusverkostojen kehittymistä edelleen.

Lain tarkoituksena on myös mahdollistaa sähköisten allekirjoitusten käyttö ja niihin liittyvien tuotteiden ja palveluiden tarjonta. Lain sähköistä allekirjoittamista koskevan osuuden on tarkoitus panna edelleen täytäntöön EU:ssa voimassa oleva sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi. Sähköisiä allekirjoituksia koskevat osuudet ehdotetaan kuitenkin annettavaksi kokonaan uudelleen sen johdosta, että muutettu laki olisi rakenteeltaan varsin sekava.

3.2 Keskeiset ehdotukset

Lain keskeiset sisällölliset ehdotukset sisältyvät 3 ja 4 lukuihin. Näistä 3 luku sisältäisi säännökset vahvan sähköisen tunnistamisen palveluiden tarjoamisesta ja 4 luku säännök-

set laatuvarmenteiden tarjoamisesta. Luvut sisältävät tyhjentävät säännökset tietynlaisen palvelun tarjoamisesta. Sähköisiä allekirjoituksia ja kehittyneitä sähköisiä allekirjoituksia voidaan tehdä myös tunnistusvälineillä niiden ominaisuuksista riippuvalla tavalla.

Sähköinen tunnistaminen

Lailla säänneltäisiin vahvan sähköisen tunnistamisen palvelujen tarjoamista. Heikko tunnistaminen jäisi siten täysin sääntelyn ulkopuolelle. Heikon tunnistamisen menetelmät ovat nykyään yleisimmin käytettyjä tunnistamismenetelmiä. Käytännössä tämä tarkoittaa käyttäjätunnusten ja salasanojen yhdistelmiä. Tällaisia tunnistamismenetelmiä käytetään nykyään ja jatkossa esimerkiksi internetin erilaisilla keskustelupalstoilla. Niihin liittyy huomattavia käyttömukavuuteen ja tietoturvaan liittyviä ongelmia, joten niiden käyttöä ei erityisesti pyritä edistämään. Niiden hyvänä puolena on maksuttomuus, minkä johdosta ne sopivat sellaisten palveluiden käyttöön, joissa ei ole kyse taloudellisista eduista tai oikeustoimien tekemisestä. Niiden tarjontaan liittyvistä asioista ei ole tarpeen yrittää säätää laissa.

Sähköisessä tunnistamisessa on mahdollista käsitteellisesti erotella henkilöllisyyden todentaminen eli niin sanottu autentikointi tai verifiointi ja henkilön identifiointi. Henkilöllisyyden todentamisella tarkoitetaan tilannetta, jossa henkilö toimii aktiivisesti eli esittää henkilöllisyydestään väitteen, jonka todenperäisyys tunnistamisessa todennetaan. Identifioinnissa henkilö sen sijaan pyritään tunnistamaan ilman henkilön itsestään esittämää väitettä. Tämä tarkoittaa tietyn henkilön etsimistä suuresta henkilöjoukosta esimerkiksi kasvontunnistukseen perustuvan kameravalvonnan avulla. Identifiointi luokitellaan yleensä passiiviseksi tunnistamiseksi, koska se ei edellytä tunnistettavalta aktiivista toimenpidettä. Tunnistettava ei välttämättä ole tällöin edes tietoinen tunnistamisen tapahtumisesta. Esimerkkinä tämänkaltaisen tunnistamisen mahdollisesta käyttötilanteesta voidaan mainita tekninen kasvontunnistukseen perustuva valvonta.

Ehdotettu laki koskee ainoastaan tarjottavia palveluita ja niiden käyttämistä. Tunnistettavalta edellytetään tällöin aina aktiivista toimintaa. Tämä koskee niin tunnistusvälineen hankkimista kuin yksittäistä tunnistamistapahtumaakin. Ehdotettu laki ei siten lainkaan koske tunnistusmenetelmien passiivista käyttöä.

Laki kohdistuu luonnollisten henkilöiden tunnistamiseen. Luonnolliset henkilöt voisivat muualla lainsäädännössä säädettyjen edustamista koskevien säännösten mukaisesti edustaa toista luonnollista henkilöä tai oikeushenkilöä, mutta roolitiedon liittäminen tunnistamiseen ei kuuluisi ehdotetun lain soveltamisalaan. Nämä palvelut ovat toistaiseksi vielä kehitysvaiheessa.

Ehdotetun lain soveltamisalan ulkopuolelle jäisi sellainen toiminta, jossa on kysymys vahvan sähköisen tunnistusvälineiden valmistamisesta, maahantuonnista tai myynnistä. Lain on siis tarkoitus kohdistua ainoastaan palveluiden tarjontaan. Edelleen lakia sovellettaisiin ainoastaan palveluiden tarjoamiseen yleisölle. Soveltamisalan ulkopuolelle jäisivät siten suljettuihin ympäristöihin tarkoitetut järjestelmät, kuten yritysten sisäisiin tunnistamistarpeisiin käytettävät järjestelmät.

Soveltamisalan ulkopuolelle jäisi myös palveluntarjonta, jossa yhteisö käyttää omaa vahvaa sähköistä tunnistusmenetelmäänsä yksinomaan omien asiakkaidensa tunnistamiseen omissa palveluissaan. Tällaiseen toimintaa sovellettaisiin kuitenkin 3 §:n, 20 §:n 1 momentin, 21-22 §:n, 23 §:n 1 momentin, 25 §:n 1 momentin ja 2 momentin, 27 §:n 1 momentin, 2 momentin 1 kohdan ja 3 momentin sekä 42 §:n 4 momentin säännöksiä. Kyse on kuluttajansuojanäkökulmasta, minkä johdosta tällaista toimintaa valvoisi kuluttaja-asiamies. Ei ole kovin todennäköistä, että tällaisia palveluita syntyisi kovinkaan paljon, sillä ne ovat toimijoille varsin kalliita ja käyttäjien kannalta hankalia.

Lailla säänneltäisiin siis vahvojen sähköisten tunnistuspalveluiden tarjoamista. Määritelmien mukaan tunnistuspalvelun tarjoajalla tarkoitettaisiin sellaista palveluntarjoajaa, joka tarjoaa vahvan sähköisen tunnistamisen palveluita niitä käyttäville palveluntarjoajille tai laskee liikkeelle sähköisiä tunnistamisvälineitä ja menetelmiä tai molempia. Laki sisältäisi siten sekä palveluiden tarjonnan että välineiden liikkeelle laskun. Voi olla, että

yksi palveluntarjoaja toimisi molemmissa rooleissa, mutta varsinkin kehittyneemmässä vaiheessa nämä roolit voisivat erota toisistaan.

Ehdotetun lain 2 §:n 1 kohdan mukaan vahvalla sähköisellä tunnistamisella tarkoitettaisiin menettelyä, jolla yksilöidään henkilö luotettavaa sähköistä menetelmää käyttäen sekä samalla todennetaan tunnisteen aitous ja oikeellisuus. Kohdassa esitetyistä kolmesta kriteeristä kahden on täytyttävä, jotta sähköinen tunnistaminen olisi vahvaa. Lain 8 §:ssä olisi lisäksi asetettu vaatimukset, jotka vahvan sähköisen tunnistamisen on täytettävä. Sen mukaan menetelmän perustana on oltava 17 §:n mukainen huolellinen ensitunnistaminen, jota koskevat tiedot ovat jälkikäteen 24 §:n mukaisesti tarkastettavissa, menetelmällä on voitava yksiselitteisesti tunnistaa vahvan sähköisen tunnistamisvälineen haltija, menetelmällä on voitava riittävällä luotettavuudella varmistua, että ainoastaan vahvan tunnistamisvälineen haltija voi käyttää välinettä, ja menetelmän on oltava riittävän turvallinen ja luotettava ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat.

Palveluntarjoajalle asetettavista edellytyksistä säädetään 9 §:ssä. Kyse on lähinnä siitä, että palveluntarjoajalla ei saa olla tietynlaista rikollista taustaa.

Ehdotetun lain 10 §:n mukaan Suomeen sijoittautuneiden vahvan sähköisen tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle ilmoitus palveluiden tarjonnasta. Viestintävirasto tarkistaisi palveluntarjoajan ja sen tarjoaman palvelun vastaavaan tapaan kuin laatuvarmennepalvelun sähköisen allekirjoittamisen osalta. Pääsääntöisesti valvonta olisi kuitenkin jälkikäteistä valvontaa lain 5 luvun säännösten mukaisesti.

Ehdotetun lain 13-16 §:t sisältävät säännöksiä vahvan sähköisen tunnistuspalvelun tarjonnan perusedellytyksistä. Ehdotettu 13 § sisältää säännökset palveluntarjoajan henkilöstöön kohdistuvista vaatimuksista, taloudellisista voimavaroista ja tietoturvavelvoitteista. Ehdotettu 14 § edellyttää palveluntarjoajalta tunnistamisperiaatteiden olemassa oloa. Ehdotetut 15 ja 16 §:t koskevat tiedonantovelvoitteita. Lisäksi lain 6 ja 7 §:t sisältävät henkilötietojen ja väestötietojärjestelmään tallennettujen tietojen käsittelysäännökset. Viimeksi mainitut säännökset ovat yhteisiä lain 3 ja 4 lukujen palveluntarjoajille.

Ehdotetun lain 17 § sisältää säännökset yleisesti vahvan sähköisen tunnistamisen kulmakivenä pidetystä henkilön ensitunnistamisesta. Pääsääntönä on se, että vahvan sähköisen tunnistuspalvelun tarjoajan on tunnistettava tunnistusvälineen hakija toteamalla henkilöllisyys voimassa olevasta Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista.

Halutessaan vahvan sähköisen tunnistuspalvelun tarjoaja voi käyttää ensitunnistamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia. Ehdotun 51 §:n sisältämän siirtymäsäännöksen mukaan palveluntarjoaja voisi halutessaan käyttää 31 päivään joulukuuta 2012 saakka Suomen valtion viranomaisen vuoden 1990 syyskuun jälkeen myöntämää voimassa olevaa ajokorttia.

Ensitunnistamisen on tapahduttava henkilökohtaisesti, paitsi jos vahvan sähköisen tunnistuspalvelun tarjoajat ovat tehneet keskenään sopimuksen mahdollisuudesta luottaa toistensa tekemään tunnistukseen. Ensitunnistamisen varsinainen ketjuttaminen ei siten ole mahdollista, vaan alkuperäisen ensitunnistamisen tehneen palveluntarjoajan on aina oltava mukana sopimusjärjestelyissä.

Ehdotetussa 5 §:ssä todetaan voimassa oleva oikeustila sen suhteen, että tunnistusvälineillä voidaan tehdä oikeustoimia osapuolten niin halutessa, ellei lainsäädännössä ole erityisiä muotovaatimuksia kyseisen oikeustoimen osalta. Suomessa tällaiset oikeustoimet ovat huomattavassa vähemmistössä. Oikeustoimien tekeminen voidaan kuitenkin kieltää osapuolten välisessä sopimuksessa, tai niille voidaan asettaa oikeustoimen laatua tai euromääriä koskevia rajoituksia. Ehdotettu 18 § sisältää tarkemmat säännökset näistä kielloista ja rajoituksista.

Ehdotettu 19 § muodostaa poikkeuksen 2 luvun pyrkimyksestä teknologianeutraaliteettiin. Sanottu pykälä kohdistuu varmenteiden käyttöön vahvan sähköisen tunnistamisen välineinä, ja sisältää säännökset varmenteen tie-

tosisällöstä. Vastaava laatuvarmenteita koskeva säännös löytyy 30 §:stä.

Ehdotettu 20 § koskee tunnistusvälineen liikkeelle laskemista. Pykälän 3 momentissa todetaan selkeästi, että välineen on oltava henkilökohtainen. Vastaavasti ehdotetussa 23 §:n 2 momentissa kielletään välineen haltijaa luovuttamasta sitä toisen käyttöön.

Ehdotettu 21 § koskee tunnistusvälineen luovuttamista haltijalle. Tarkoitus on, että myös postitse toimittaminen on tietyin edellytyksin sallittua. Ehdotetussa 24 §:ssä säädetään vahvan sähköisen tunnistamisen tapahtumaa ja tunnistamisvälinettä koskevien tietojen tallentamisesta sekä tallennusajoista.

Ehdotetut 25 ja 26 §:t koskevat vahvan sähköisen tunnistamisvälineen peruuttamista tai käytön estämisestä. Kyse voi olla siitä, että välineen haltija tekee ilmoituksen esimerkiksi välineen katoamisesta. Toisaalta on myös tilanteita, joissa palveluntarjoajalla on oltava mahdollisuus peruuttaa väline tai estää sen käyttö.

Ehdotettu 27 sisältää säännökset tunnistusvälineen haltijan vastuusta välineen oikeudettomasta käytöstä. Pääsäännön mukaan vahvan sähköisen tunnistusvälineen haltija vastaa välineen oikeudettomasta käytöstä vain, jos hän on luovuttanut välineen toiselle, jos välineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, tai jos hän on laiminlyönyt ilmoittaa palveluntarjoajalle tai sen ilmoittamalle muulle taholle välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan.

Sähköinen allekirjoitus

Sähköisen allekirjoituksen osalta sääntely vastaisi pääosin sähköisistä allekirjoituksista annetun lain sääntelyä, jolla pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin säännökset. Joissakin pykälissä olevat viittaukset siitä, että laatuvarmenteiden tarjonta on julkisen vallan käyttöä, poistettaisiin. Tämä johtuu siitä esityksen lähtökohdasta, että siinä säännellään puhtaasti yksityistä palveluntarjontaa. Asiaa käsitellään tarkemmin säätämisjärjestystä koskevassa osiossa.

Ehdotetun lain 2 §:n 9 kohdan mukaan sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. Määritelmä on sama kuin sähköisistä allekirjoituksista annetussa laissakin, ja perustuu sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin.

Saman pykälän 10 kohdan mukaisesti kehittyneellä sähköisellä allekirjoituksella tarkoitetaan sähköistä allekirjoitusta, joka liittyy yksiselitteisesti sen allekirjoittajaan, jolla voidaan yksilöidä allekirjoittaja, joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan, ja joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. Kuten edellä todettiin, ehdotetun lain määritelmien mukaan varmennetta voidaan käyttää niin vahvaan sähköiseen tunnistamiseen kuin sähköiseen allekirjoitukseenkin.

Ehdotetun lain 28 § sisältää määräykset turvallisen allekirjoituksen luomisvälineestä. Pykälä vastaa voimassa olevan lain 5 §:ää. Pääosa ehdotetusta 4 luvusta, eli §:t 30-41 koskevat ainoastaan laatuvarmenteita ja laatuvarmentajia. Laatuvarmenteella tarkoitetaan sellaista varmennetta, jonka on myöntänyt lain 33-38 §:ssä tarkoitettu laatuvarmentaja. Laatuvarmenteessa on oltava tieto siitä, että varmenne on laatuvarmenne, tieto varmentajasta ja sen sijoittautumisvaltiosta, allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi, allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja, laatuvarmenteen voimassaoloaika, laatuvarmenteen yksilöivä tunnus, varmentajan kehittynyt sähköinen allekirjoitus, mahdolliset laatuvarmenteen käyttörajoitukset, sekä allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.

Ehdotetun lain 5 §:n 2 momentissa todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja

on luotu turvallisella allekirjoituksen luomisvälineellä. Lisäksi todetaan, että sähköiseltä allekirjoitukselta ei tule evätä oikeusvaikutuksia yksinomaan sen vuoksi, että se on tehty muulla sähköisen allekirjoittamisen tavalla. Säännös vastaa voimassa olevaa lakia, mutta jälkimmäinen virke on lisätty sähköisiä allekirjoituksia koskevan yhteisön direktiivin 5 artiklan 2 kohtaa mukaillen. Tarkoitus ei ole muuttaa voimassa olevaa lakia, vaan selkeyttää kohtaa, jota on toistuvasti tulkittu väärin.

Muut ehdotukset

Esitykseen liittyy 10 muuta lakia. Niitä joudutaan muuttamaan sen johdosta, että esityksellä kumottaisiin laki vahvasta sähköisestä allekirjoituksesta. Viittaukset siihen muutetaan viittauksiksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

Lisäksi sähköisestä asioinnista viranomaisessa annetun lain 18 §:n ja rahanpesusta ja terrorismin rahoittamisen ehkäisemisestä ja selvittämisestä annetun lain 18 §:n tunnistamista koskeviin säännöksiin ehdotetaan lisättäväksi esityksen mukainen tunnistusväline nimenomaisesti hyväksyttäväksi tunnistautumisessa käytettäväksi välineeksi.

Edelleen eräiden vero-oikeutta koskevien lakien sähköistä allekirjoitusta koskevat säännökset muutettaisiin siten, että niissä edellytettäisiin allekirjoitusvaatimuksen kyseessä ollen kehittynyttä sähköistä allekirjoitusta tai muuta hyväksyttävää sähköistä allekirjoitusta.

Oikeusjärjestyksessämme lähtökohtana on se, että vain hyvin harvoja oikeustoimia koskee muotovaatimus. Myös yhteydenotot viranomaisiin ovat yleensä muotovapaita. Silloin, kun allekirjoitusta edellytetään, on kyse muotovaatimuksesta. Kehittyneen sähköisen allekirjoituksen käyttö on silloin paikallaan. Muutetut säännökset eivät kuitenkaan jatkossakaan estäisi muunlaisten allekirjoitusten hyväksymistä.

4 Esityksen vaikutukset

4.1 Taloudelliset vaikutukset

Sähköisiin allekirjoituksiin liittyviä tuotteita ja palveluita on Suomessa tuotettu lähinnä yhteiskunnan rahoituksella. Palveluntarjonnassa ei ole toistaiseksi saatu kannattavaa liiketoimintamallia syntymään. Sähköisten allekirjoitusten tarjoaminen sellaisena kuin palveluntarjonnan oikeudellinen rakenne on ajateltu 1990-luvun alkupuolelta lähtien, tulee olemaan liiketoimintamallin kannalta haastavaa myös jatkossa. Tämä johtuu siitä, että toiminnalle on nimenomaan tunnusomaista se, että allekirjoituspalveluiden tarjoajan ja niihin luottavan osapuolen välillä ei ole sopimussuhdetta. Tällöin ei ole myöskään olemassa luonnollista laskutuspistettä.

Sähköisiä allekirjoituksia koskevasta direktiivistä seuraa laatuvarmenteiden tarjontaan varsin tiukat edellytykset. Tämä on omalta osaltaan saattanut myös vaikuttaa sähköisten allekirjoituspalveluiden markkinoiden heikkoon kehitykseen. Ehdotetun lain toivotaan edistävän sähköisiin allekirjoituksiin liittyvien palveluiden tarjoantaa ja erityisesti muiden varmenteiden tarjontaa, sillä laissa todettaisiin selkeästi se, että sähköisiä allekirjoituksia ja kehittyneitä sähköisiä allekirjoituksia voidaan tehdä myös tunnistusvälineillä niiden ominaisuuksista riippuen. Varmenteiden käyttö tunnistamisessa tulleekin lisääntymään tulevaisuudessa.

Valtiovarainministeriö on asettanut työryhmän pohtimaan valtion varmennetuotannon mahdollista uudelleenorganisointia. Työryhmän on määrä saada työnsä valmiiksi syksyllä 2009. Hankkeessa on erityisen tärkeää selkeyttää Väestörekisterikeskuksen toimintaa toisaalta viranomaisena ja toisaalta palveluntarjoajana. Hanke vaikuttaa suoraan Väestörekisterikeskuksen toimintaan palveluntarjoajana. Sen sijaan käsillä olevan esityksen näkökulmasta Väestörekisterikeskus on yksi palveluntarjoaja muiden joukossa, eikä sillä siten ole suoranaisia vaikutuksia Väestörekisterikeskuksen toimintaan. Käytännössä mahdollinen kilpailun lisääntyminen vaikuttanee kuitenkin asiaan. Johtopäätösten tekeminen muun muassa sen suhteen, voidaanko tai tuleeko ja millaisissa tapauk-

sissa palveluntarjontaan käyttää jatkossa valtion rahoitusta, tapahtuu valtiovarainministeriön työryhmässä.

Sähköisen tunnistamisen osalta liiketoimintamalli on helpommin löydettävissä. Tämä johtuu erityisesti siitä oikeudellisen perusrakenteen erosta sähköisten allekirjoitusten tarjoamiseen verrattuna, että vahvan sähköisen tunnistuspalveluntarjoajien, niitä käyttävien palveluntarjoajien ja välineiden haltijoiden välillä vallitsee sopimuksin säännelty oikeustila. Silti tunnistamisenkaan osalta ei arvioida olevan kyse taloudellisesti erityisen merkittävästä liiketoiminnasta. Sähköinen tunnistaminen ei ole itseisarvo, vaan väline sähköisten palveluiden ja sähköisen asioinnin käyttöön. Sähköisen tunnistamisen välillinen taloudellinen merkitys sähköisten palveluiden ja sähköisen asioinnin palveluiden määrän ja kirjon huomattavan kasvun mahdollistajana on huomattava. Tämä on se seikka, jonka toivotaan tuovan markkinoille uusia toimijoita.

On syytä olettaa, että vahvaa sähköistä tunnistamista tarjoavat palveluntarjoajat ovat suuria toimijoita, ja ainakaan toistaiseksi näköpiirissä ei ole sellaisia toimijoita, joiden liiketoiminta koostuisi ainoastaan tunnistuspalveluista. Ehdotetun lain tarkoituksena on, että markkinoillemme voisi tulla joitakin palveluntarjoaja lisää. Odotettavissa ei kuitenkaan ole, että palveluntarjoajien määrä voisi nousta muutamaa suuremmaksi markkinoillamme, jotka joka tapauksessa ovat kooltaan varsin pienet.

Näköpiirissä olevista mahdollisista uusista palveluntarjoajista pisimmällä lienevät teleyritykset, jotka voisivat mahdollisesti saada mobiilivarmenteensa markkinoille jo vuoden 2009 aikana. Mobiilivarmenteiden tarjonta merkitsisi teleyrityksille todennäköisesti varsin mittavaa SIM-korttien vaihto-operaatiota ja samalla merkittävää taloudellista panostusta. Mobiilivarmenne kuitenkin mahdollistaisi hyvin monenlaisten palveluiden käyttämisen ajasta ja paikasta riippumatta luotettavalla tavalla. Mobiilivarmenteiden menestyminen edellyttänee sitä, että niitä voidaan laskea liikkeelle huomattavia määriä mahdollisimman nopeasti. Ripeä liikkeelle lasku todennäköisesti samalla lisäisi nopeasti uusien palveluiden kysyntää. Tällä olisi suurta taloudellista merkitystä hyvin monille tunnistuspalveluita käyttäville palveluntarjoajille. Laki pyrkii siihen, että ripeä liikkeelle lähtö olisi mahdollista kaikkien uusien tunnistuspalveluntarjoajien osalta.

Esitys ei suoraan vaikuttaisi pankkitunnisteiden käyttöön, vaan niitä voidaan jatkossa käyttää kuten tähänkin saakka. Ehdotettu järjestelmä vahvistanee lyhyellä aikavälillä jossakin määrin pankkitunnusten asemaa luotettavana tunnistusmenetelmänä edellyttäen, että niitä tarjoavat pankit tekevät laissa tarkoitetun ilmoituksen Viestintävirastolle. Päinvastaisessa tapauksessa pankkitunnisteiden käyttö erityisesti julkisen sektorin palveluissa saattaa muodostua kyseenalaiseksi.

Tulevaisuudessa pankit joutunevat harkitsemaan myös sitä, tarjoavatko ne itse tunnistuspalveluita, vai ryhtyvätkö ne käyttämään muiden tarjoamia palveluita, vai kenties molempia. Pankkitunnisteilla on edessään todennäköisesti vielä runsaasti käyttövuosia. Niillä on kuitenkin rajoituksensa erityisesti yhä mobiilimmaksi muuttuvassa maailmassa. Toisaalta on huomattava, että nykyiset pankkitunnisteet ovat pankeille erittäin halpoja, ja asiakkaat maksavat niistä yleensä osana pankkipalveluidensa pakettihintoja. Tämän johdosta markkinoille tulevien mahdollisten uusien tunnistusvälineiden olisi oltava hinnoiltaan erittäin kilpailukykyisiä.

Ehdotettua lakia valvoo Viestintävirasto. Se on nettobudjetoitu laitos, minkä johdosta toimijoiden on maksettava tehdystä valvonnasta. Koska suoraan ei pystytä erottelemaan tehtyjä suoritteita ja niitä vastaavia maksuja, ovat toimijoiden valvonnasta maksamat maksut oikeudelliselta luonteeltaan veroja. Maksujen taso on pyritty määräämään siten, että ne eivät muodostaisi estettä palveluntarjonnan aloittamiselle. Tunnistuspalvelun tarjoajien maksettavaksi tuleva valvontamaksu olisi 12 000 euroa vuosittain. Laatuvarmenteita tarjoavien varmentajien toiminta tarkastetaan vuosittain, minkä johdosta niiden maksettavaksi tulee selkeästi suurempi valvontamaksu. Sen suuruus on 40 000 euroa vuodessa. Väestörekisterikeskuksen kannalta tämä merkitsee maksun selvää pienenemistä nykyiseen verrattuna.

Ehdotetulla lailla ei ole suoraa vaikutusta sen soveltamisalan ulkopuolelle jäävään pal-

veluntarjontaan. Mikäli laki saavuttaa tavoitteensa luoda edellytykset toimiville yleiskäyttöisten tunnistusvälineiden markkinoille, saattaa tarve omien tunnistusratkaisujen laatimiselle vähentyä. Tämä saattaisi tuoda yrityksille kustannussäästöjä sekä samalla lisätä tunnistamistoimintojen turvallisuutta.

4.2 Organisaatiovaikutukset

Ehdotetulla lailla olisi jonkin verran vaikutusta Viestintävirastoon, jonka tehtäväkenttään tulisi myös vahvan sähköisen tunnistamisen palveluiden tarjonnan valvonta. Koska valvonta kuitenkin olisi pääsääntöisesti jälkikäteistä, ei toiminta edellytä merkittävää resurssien lisäämistä. Kaikista eniten työtä Viestintävirastolle aiheutuisi toimijoiden rekisteröintiprosessista, josta säädettäisiin oma erillinen maksunsa.

Tähän saakka sähköisten allekirjoituspalveluiden valvontaan on ollut käytettävissä noin puoli henkilötyövuotta. Sähköisistä allekirjoituksista annetun lain mukaisen ilmoituksen laatuvarmenteiden tarjonnasta on tehnyt ainoastaan Väestörekisterikeskus. Se on maksanut Viestintävirastolle valvontamaksua 80 000 euroa vuosittain.

Jatkossa vahvan sähköisen tunnistamisen palveluiden ja laatuvarmenteiden tarjonnan valvonta edellyttäisi Viestintävirastolta arviolta noin yhden henkilötyövuoden verran työvoimaa. Sähköisten tunnistuspalveluiden mahdollisia tarjoajia oletetaan tällä hetkellä olevan korkeintaan 12. Näistä yhdeksän olisi pankkeja tai niiden muodostamia lain 10 §:n mukaisia palveluntarjoajien yhteenliittymiä ja kolme teleyrityksiä. Koska maksajien määrän oletetaan kasvavan, on samalla voitu pienentää laatuvarmenteita tarjoavien varmentajien maksamaa maksua. Samalla maksun peruste muuttuisi myös niiden osalta palveluntarjoajakohtaiseksi. Toistaiseksi ainoa näköpiirissä oleva laatuvarmenteiden tarjoaja on Väestörekisterikeskus.

Koska valvontamaksut ovat oikeudelliselta luonteeltaan veroja, on niiden määrästä säädettävä lain tasolla. Tämän johdosta on oltava valmius muuttaa lakia nopeallakin aikataululla mikäli nähdään, että nyt säädetty maksutaso tai maksun määräytymisen peruste ei mahdollista Viestintäviraston riittäviä valvontaresursseja tai mikäli sille syntyisi maksuista ylijäämää.

Ehdotetun lain mukaan tietosuojavaltuutetun tehtävänä on valvoa lain henkilötietoja koskevien säännösten noudattamista. Lisäksi Kuluttajaviraston tehtävänä on valvoa sellaista 1 §:n 2 momentissa tarkoitettua palveluntarjontaa, jossa yhteisö käyttää omaa vahvaa sähköistä tunnistusmenetelmäänsä yksinomaan omien asiakkaidensa tunnistamiseen omissa palveluissaan. Näiden säännösten ei voida arvioida merkittävästi lisäävän näiden viranomaisten tehtäviä.

Ehdotetulla lailla ei ole suoranaisia vaikutuksia muiden viranomaisten toimintaan. Väestörekisterikeskuksen varmennetoimintaa arvioidaan valtiovarainministeriön valtion varmennetuotannon uudelleenorganisoinnin hankkeessa. Lisäksi valtioneuvoston sähköistä tunnistamista koskevan periaatepäätöksen mukaan sosiaali- ja terveysministeriö arvioi uudelleen Sosiaali- ja terveysalan lupa- ja valvontaviraston Valviran roolin varmennepalveluiden tuottajana mahdollisimman nopeasti sen jälkeen, kun valtiovarainministeriö on saanut päätökseen valtion varmennetuotannon uudelleenorganisointia koskevan hankkeen.

4.3 Tietoyhteiskuntavaikutukset

Suomi on viime vuosina menettänyt asemaansa tietoyhteiskuntakehityksen edelläkävijänä. Yhtenä syynä tähän tilanteeseen on sähköisten palveluiden ja sähköisen asioinnin palveluiden tarjonnan ja käytön hidas edistyminen. Tällä hetkellä olemme kuitenkin tilanteessa, jossa ihmisille alkaa vähitellen kertyä käyttökokemusta sähköisistä palveluista. On syytä olettaa, että jatkossa sähköisten palveluiden kysyntä voi kasvaa huomattavasti. Kysynnän kasvu on seurasta sähköisten palveluiden käyttäjilleen tarjoamista hyödyistä, sillä asioita voi hoitaa kotoa käsin, ilman jonoja ja aukioloajoista piittaamatta.

Sähköisten palveluiden kysynnän kasvua pyritään tukemaan voimakkaasti julkisen vallan toimenpitein. Sekä palvelujen määrän mutta erityisesti kirjon lisääminen edellyttää jatkossa yhä useammin luotettavaa sähköistä tunnistamista. Käynnissä on joitakin lainsäädäntöhankkeita, kuten esimerkiksi kulutus-

luottoja koskevan lainsäädännön uudistaminen, joissa etäyhteyksillä tapahtuvan palveluntarjonnan edellytykseksi kaavaillaan vahvaa sähköistä tunnistamista. Tällaisen lainsäädännön määrä tullee lähivuosina kasvamaan. Jotta järjestelmä voisi toimia, täytyy olla olemassa myös sellainen säännöstö, jossa määritellään luotettava eli vahva sähköinen tunnistaminen ja sitä koskevan palveluntarjonnan perusedellytykset.

Sähköiset palvelut edellyttävät osapuolten välisen luottamussuhteen syntyä aivan toisella tapaa kuin perinteinen fyysisessä kontaktissa tapahtuva asioiminen. Palvelun käyttäjän on voitava luottaa siihen, että palveluntarjoaja on rakentanut palvelunsa siten, että esimerkiksi tietoturvan ja yksityisyyden suojan vaatimukset on otettu huomioon. Palveluntarjoajan on puolestaan voitava luottaa muun muassa siihen, että etäyhteyden toisessa päässä oleva palvelunkäyttäjä on se, joka väittää olevansa.

Edellä sanotusta seuraa, että vahvan sähköisen tunnistamisen edistäminen on suomalaisen tietoyhteiskunnan kehittymisen kannalta olennainen perustekijä. Luotettavien sähköisten palveluiden ja sähköisen asioinnin palveluiden kehittyminen jatkossa ei näytä mahdolliselta ilman luotettavaa sähköistä tunnistamista ja sitä koskevaa lainsäädäntöä. Samalla voidaan ratkaista joitakin erityisongelmia, kuten esimerkiksi ikärajoituksilla varustettujen sähköisten palveluiden luotettava tarjonta ja käyttö.

Toimivien sähköisen tunnistamisen markkinoiden aikaan saaminen edistäisi huomattavasti sähköisten palveluiden ja sähköisen asioinnin palveluiden kehitystä maassamme. Esityksen tietoyhteiskuntavaikutukset olisivat siten merkittävät.

5 Valmistelu

Valmistelu liikenne- ja viestintäministeriössä

Esitys on valmisteltu liikenne- ja viestintäministeriössä. Valmistelussa on käytetty apuna arjen tietoyhteiskunnan neuvottelukunnan alaisuuteen asetetun sähköisen tunnistamisen kehittämisryhmän asiantuntemusta. Valmistelun kuluessa on käyty alustavia keskusteluja muun muassa Euroopan unionin komission, oikeusministeriön, sisäasiainministeriön, työ- ja elinkeinoministeriön, Viestintäviraston, Rahoitustarkastuksen, Kuluttajaviraston, Väestörekisterikeskuksen, Finanssialan keskusliiton, FiCom ry:n sekä yksittäisten toimijoiden kuten pankkien ja teleoperaattoreiden edustajien kanssa.

Lausunnot ja niiden huomioon ottaminen

Lakiluonnos lähetettiin laajalle lausuntokierrokselle marraskuussa 2008. Lausuntonsa asiassa antoivat oikeusministeriö, opetusministeriö, puolustusministeriö, sisäasiainministeriö, sosiaali- ja terveysministeriö, työ- ja elinkeinoministeriö, valtiovarainministeriö, Huoltovarmuuskeskus, Keskusrikospoliisi, Kilpailuvirasto, Kuluttajavirasto, Pääesikunta, Rahoitustarkastus, Suojelupoliisi, Valtiokonttori, Valtiontalouden tarkastusvirasto, Verohallitus, Viestintävirasto, Väestörekisterikeskus, CSC – Tieteen tietotekniikan keskus Oy, Elinkeinoelämän Keskusliitto, Elisa Oyj, Eläketurvakeskus, F-Secure Oyj, Finanssialan Keskusliitto, Helsingin seudun kauppakamari, IKI ry, Kansaneläkelaitos, Kesko Oyj, Keskuskauppakamari, Logica Suomi Oy, Nordea Pankki Suomi Oyj, OP-Keskus, Samlink Oy Ab, Sampo Pankki, STAKES, STTK ry, Suomen Ammattiliittojen Keskusjärjestö SAK ry, Suomen Asiakkuusmarkkinointiliitto ry, Suomen Kuluttajaliitto ry, Suomen Kuntaliitto, Suomen Yrittäjät, Tampereen kaupunki, Tampereen yliopisto, TeliaSonera Finland Oyj, Terveydenhuollon oikeusturvakeskus, TIEKE Tietoyhteiskunnan kehittämiskeskus ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Tietotekniikan liitto ry, Tietotekniikan tutkimuslaitos HIIT, Valimo Wireless Oy, Ubisecure Solutions Oy ja Viestinnän keskusliitto.

Koska kyseessä olevaa lakia vastaavaa ei ole Euroopassa eikä tiettävästi muuallakaan maailmassa, järjestettiin lausuntokierros varsin varhaisessa vaiheessa, jotta saataisiin palautetta lain perusratkaisuista ennen hallituksen esityksen yksityiskohtien hiomista. Muutama lausunnonantaja kiinnittikin huomiota luonnoksen keskeneräisyyteen.

Kaiken kaikkiaan lakiluonnoksen saama vastaanotto oli varsin myönteinen. Varsinai-

sia lausuntoja saatiin 53 kappaletta. Yhdessäkään niistä ei ilmoitettu vastustettavan lain antamista. Lausunnonantajista 35 ilmoitti suoraan kannattavansa lakiehdotusta ja sen tavoitteita tai arvioivansa sen vaikutukset myönteisiksi. Lausunnoista noin kolmannessa esitettiin ainoastaan yleisluontoisia näkemyksiä aihepiiristä, noin kolmanneksessa ehdotettiin joitakin muutoksia tai tarkennuksia esitykseen ja noin kolmanneksessa näitä muutosehdotuksia oli runsaasti.

Lausunnoissa esitetyt huomiot hajaantuivat suuresti. Ainoastaan muutamaa kohtaa koski useampi kuin yksi huomautus. Saadun palautteen perusteella ehdotetun lain perusratkaisut on säilytetty ennallaan. Alla selostetaan tärkeimmät lausuntojen seurauksena tehdyt muutokset. Merkitykseltään vähäisempiä muutoksia ja tarkennuksia tehtiin huomattava määrä.

Annettujen lausuntojen perusteella merkittävimmät muutokset tehtiin lakiluonnoksen 1 ja 2 lukuihin. Lain 1 pykälän soveltamisalan rajaus, jonka mukaan suljetut järjestelmät eivät kuulu soveltamisalaan, on suoraa seurausta siitä, että lailla pyritään luomaan edellytykset toimivien vahvan sähköisen tunnistamisen markkinoille. Näillä markkinoilla ainoastaan yleiskäyttöisillä välineillä on mahdollisuus kilpailla keskenään. Suljetuissa järjestelmissä palveluntarjonnan ensisijainen päämäärä ei edes ole itse tunnistaminen, vaan tunnistaminen palvelee muita tarkoituksia. Pykälän toiseen momenttiin lisättiin kuitenkin kuluttajansuojanäkökohtien johdosta säännös, jonka mukaan myös tietyissä suljetuissa järjestelmissä on noudatettava joitakin palveluntarjoajan vastuuseen liittyviä ehdotetun lain säännöksiä. Näitä säännöksiä ei valvo Viestintävirasto vaan kuluttaja-asiamies kuluttajasuhteissa.

Määritelmien osalta joissakin lausunnoissa kiinnitettiin huomiota siihen, että 2 §:n 1 kohdan vahvan sähköisen tunnistamisen määritelmässä ei pykälätekstissä mainittu kansainvälisestikin yleisesti vahvan sähköisen tunnistamisen määritelmänä pidettyä kolmea perustetta. Nämä perusteet nostettiin perustelutekstistä pykälätekstiin.

Lain 3 §:ään otettiin kuluttajasuhteissa vallitsevaa pakottavuutta koskeva säännös.

Joissakin lausunnoissa katsottiin, että lakiluonnos ei olisi väljentänyt sähköisistä allekirjoituksista annetun lain sääntelyä siitä, millaisille allekirjoituksille voidaan antaa oikeusvaikutukset. Lausuntojen johdosta oikeusvaikutuksia koskeneet pykälät siirrettiin 3 ja 4 luvuista 2 lukuun ja samalla yhdistettiin. Vaikka sähköisistä allekirjoituksista annettu laki ei ole rajoittanut oikeusvaikutusten syntymistä laatuvarmenteisiin, on lakia tulkittu tällä tavoin monilla tahoilla viime aikoihin saakka. Tämän selventämiseksi 5 §:n 2 momenttiin lisättiin sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 5 artiklan 2 kohdan mukainen virke. Siinä todetaan, että sähköiseltä allekirjoitukselta ei tule evätä oikeusvaikutuksia yksinomaan sen vuoksi, että se on tehty muulla sähköisen allekirjoittamisen tavalla kuin kehittyneellä sähköisellä allekirjoituksella, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä.

Soveltamisalaa koskevan 1 §:n 2 momentin soveltamisalarajoituksissa ei ole rajoitettu sellaisten pykälien soveltamisalaa, jotka koskevat vahvaa sähköistä tunnistamista ja sähköistä allekirjoittamista yleensä. Soveltamisalan rajoitukset kohdistuvat palveluntarjontaa sekä toimintaan, jossa on kysymys yksinomaan vahvan sähköisen tunnistusvälineiden tai sähköisen allekirjoittamisen välineiden valmistamisesta, maahantuonnista tai myynnistä. Ehdotetut 4 ja 5 § eivät koske pelkästään palveluntarjontaa vaan vahvaa sähköistä tunnistamista ja sähköisiä allekirjoituksia yleensä. Toimijat voivat itse harkita, millaiselle vahvalle sähköiselle tunnistamiselle ja sähköiselle allekirjoittamiselle ne antavat oikeusvaikutuksia, elleivät tätä harkintamahdollisuutta rajoita muiden lakien säännökset.

Lain 4 §:n 1 momenttiin lisättiin toteava säännös, jonka mukaan sähköisiä allekirjoituksia ja kehittyneitä sähköisiä allekirjoituksia voidaan tehdä vahvoilla sähköisillä tunnistusvälineillä niiden ominaisuuksista riippuvalla tavalla, jos osapuolet niin haluavat eikä muualta laista muuta johdu. Samalla lain 4 luvusta poistettiin lausuntoversion 23 §:n säännös, jonka mukaan tietynlaisten sähköisen allekirjoittamisen palveluihin olisi sovel-

lettu soveltuvin osin lausuntoversion 2 luvun säännöksiä.

Lista, jota Viestintävirasto olisi lausuntoversion mukaan pitänyt ilmoituksen tehneistä palveluntarjoajista, muutettiin lain 12 §:n mukaisesti rekisteriksi. Samalla Viestintävirastolle asetettiin velvollisuus kieltää palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena, jos palvelu tai palveluntarjoaja ei täytä 3 luvussa asetettuja vaatimuksia. Säännöksestä käy samalla ilmi se seikka, että Viestintäviraston on tarkistettava saamansa ilmoitusten perusteella palveluntarjoaja ja sen toiminta ennen kuin rekisterimerkintä tehdään. Tästä aiheutuu luonnollisesti Viestintävirastolle merkittävästi enemmän työtä kuin lausuntoversion mallista. Tämän johdosta Viestintävirastolle maksettavia maksuja koskevaa pykälää muutettiin samalla niin, että rekisteröitymisestä on suoritettava erillinen maksu.

Lain 3 lukuun lisättiin kokonaan uusi pykälä vahvan sähköisen tunnistusvälineen uusimisesta. Vahvan sähköisen tunnistuspalvelun tarjoajaan kohdistettavat edellytykset otettiin omaan pykäläänsä. Monia 3 luvun vahvan sähköisen tunnistusvälineenhaltijan asemaa turvaavia säännöksiä täsmennettiin ja laajennettiin.

Eniten ristiriitoja lienevät herättäneet ensitunnistamista koskeva pykälä, siirtymäsäännös ja palveluntarjoajan vastuuta koskevat säännökset. Alan keskeiset toimijat ovat ilmoittaneet varsin yksimielisesti haluavansa säilyttää lausuntoversiossa tehdyt perusratkaisut ja pitävänsä näitä ratkaisuja erittäin tärkeinä lain tavoitteiden saavuttamisen kannalta. Tämän johdosta kyseisiä pykäliä on ainoastaan täsmennetty.

6 Riippuvuus muista esityksistä

Eduskunnassa on parhaillaan käsittelyssä hallituksen esitys laiksi väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (HE 98/2008 vp). Ehdotetulla lailla kumottaisiin vuonna 1993 voimaan tullut väestötietolaki (507/1993). Ehdotetun lain tavoitteena on ohjata väestötietojärjestelmän tietojen sekä Väestörekisterikeskuksen varmennetun sähköisen asioinnin tehtävien ja palvelujen ylläpitoa, hyväksikäyttöä sekä järjestelmä- ja palvelukehitystä.

Hallituksen esitys sisältää käsillä olevan esityksen kannalta muutamia erityisen tärkeitä yhtymäkohtia. Näitä ovat erityisesti uudistetut säännökset sähköisen asiointitunnuksen luovuttamisesta ja Väestörekisterikeskuksen varmennetoimintaa koskevasta erityisestä sääntelystä.

Väestötietojärjestelmää koskeva lakiehdotus sisältää henkilötunnuksen ja sähköisen asiointitunnuksen osalta yksityiskohtaiset laintasoiset säännökset niiden sisällöstä, antamisesta, korjaamisesta, muuttamisesta sekä luovuttamisesta. Tunnuksen pysyvyys olisi myös ehdotetussa laissa pääsääntö, mutta ilmeisten kirjoitus- ja teknisten virheiden korjaaminen sekä tunnuksen muuttaminen suojelutarpeesta, väärinkäytön estämisestä ja transseksuaalin sukupuolen vahvistamisesta johtuvista syistä olisi nimenomaisesti säädetty mahdolliseksi.

Esitykseen sisältyy varmennetussa sähköisessä asioinnissa käytettävän sähköisen asiointitunnuksen luovuttamista koskeva uudistus, joka laajentaisi tunnuksen käyttöalaa nykyisestä. Esityksen mukaan asiointitunnus voitaisiin luovuttaa, jos sitä käytetään varmenteen haltijan yksilöivänä tunnistetietona kansalaisvarmenteen käyttöön perustuvan palvelun tai suoritteen tuottamisen yhteydessä. Tältä osin ehdotettu sääntely vastaisi nykytilaa. Lisäksi se voitaisiin luovuttaa Suomeen sijoittuneelle muulle varmentajalle kuin väestörekisterikeskukselle, jos tämä käyttäisi sitä sähköisistä allekirjoituksista annetussa laissa tarkoitetussa varmenteessa varmenteen haltijan yksilöivänä tunnistetietona. Tämä olisi tunnuksen käyttöalan merkittävä laajennus nykytilaan verrattuna ja sen tavoitteena olisi osaltaan tukea ja parantaa sähköisen asioinnin toimintaedellytyksiä.

Esitys sisältää säännösehdotukset, joissa Väestörekisterikeskuksen varmennetun sähköisen asioinnin palvelukokonaisuus on yksityiskohtaisesti määritelty. Palvelukokonaisuus on esityksessä jaettu kahteen itsenäiseen osaan, joista ensimmäinen osa koskee Väestörekisterikeskukselle kuuluvia viranomaistehtäviä eli sen hoidettavaksi säädettyä kansalaisvarmennetta ja siihen välittömästi liittyvää tehtäväkokonaisuutta sekä toinen osa

niitä muita varmennetehtäviä ja -palveluja, joita Väestörekisterikeskuksen olisi mahdollista tarjota esimerkiksi liiketaloudellisina palveluina. Kansalaisvarmennetta lukuun ottamatta säännös ei antaisi Väestörekisterikeskukselle minkäänlaista monopoliasemaa siinä mainittujen palvelujen ja suoritteiden tuottamiseen.

Kansalaisvarmennetta haettaisiin ehdotuksen mukaan aina kirjallisesti poliisilta, joka tunnistaisi hakijan. Muiden Väestörekisterikeskuksen tuottamien varmenteiden hakemismenettelyssä virasto voisi tehdä yhteistyötä muiden viranomaisten sekä yksityisten yritysten ja yhteisöjen kanssa.

YKSITYISKOHTAISET PERUSTELUT

1 Lakiehdotusten perustelut

1.1 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

Terminologiasta. Alan sanastoissa käytetään yleisesti sanoja tunnistaminen ja tunnistus rinnakkaisina termeinä, eikä niiden välille ole tehty todellisia merkityseroja. Tässä laissa käytetään sanaa tunnistaminen silloin, kun se esiintyy yksinään tai yhdyssanan jälkimmäisenä osana. Yhdyssanan ensimmäisenä osana käytetään sanaa tunnistus, jolloin syntyvät yhdyssanat kuten tunnistusväline, tunnistuspalvelu ja tunnistustapahtuma eivät tiettävästi ole vaarassa aiheuttaa sekaannusta muilla aloilla käytetyn terminologian kanssa.

1 luku. **Yleiset säännökset**

1 §. *Soveltamisala.* Pykälässä säädetään lain soveltamisalasta ja sen rajoituksista. Pykälän 1 momentissa määritellään soveltamisala ja 2 ja 3 momenteissa poikkeukset pääsääntöön. Pykälän 4 momentissa vielä täsmennetään soveltamisalaa.

Pykälän 1 momentin mukaan laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Lisäksi laissa säädetään vahvan sähköisen tunnistuspalvelun ja sähköisten allekirjoituspalveluiden tarjoamisesta tällaisia palveluita käyttäville palveluntarjoajille ja yleisölle. Vahvaa sähköistä tunnistamista ja sähköisiä allekirjoituksia koskevat lähinnä 4, 5 ja 28 §:t. Suurin osa ehdotetun lain säännöksistä kohdistuu palveluiden tarjoamiseen.

Palveluita tarjotaan ensinnäkin yleisölle. Sama rajaus on tehty laissa sähköisistä allekirjoituksista. Yleisöllä tarkoitetaan ennalta rajoittamatonta joukkoa ihmisiä. Esimerkiksi työ- tai virkasuhteen perusteella rajatussa joukossa ei ole kysymys yleisöstä.

Toiseksi palveluita tarjotaan tunnistuspalveluita käyttäville palveluntarjoajille. Tunnistuspalvelun tarjonnan tyyppitapauksena voidaan pitää sellaista palvelua, jossa vahvaa sähköistä tunnistamista muun oman palvelunsa tarjoamiseksi käyttävä palveluntarjoaja siirtää tunnistettavan tunnistautumaan oman palvelunsa ulkopuolelle. Tällaiselle järjestelylle on tunnusomaista se, että vahvan sähköisen tunnistuspalvelun tarjoajilla, vahvaa sähköistä tunnistamista käyttävillä palveluntarjoajilla ja tunnistusvälineen haltijoilla on olemassa keskinäinen sopimussuhtein säännelty oikeustila. Erilaiset tunnistus- tai todentamiskeskukset tai muut vastaavat keskitetyt järjestelmät kuuluvat myös ehdotetun lain soveltamisalaan, jos ne tekevät tunnistamisen asiakkaansa puolesta.

Sähköinen allekirjoitus perustuu lähtökohtaisesti erilaiseen oikeudelliseen viitekehykseen kuin vahva sähköinen tunnistaminen. Sähköisessä allekirjoittamisessa allekirjoituspalveluita tarjoavan, yleensä varmentajan, ja allekirjoitukseen luottavan välillä ei ole sopimussuhdetta. Silti varmentaja tarjoaa palvelua allekirjoitukseen luottaville esimerkiksi siten, että se ylläpitää sulkulistaa.

Sähköisen allekirjoittamisen palveluiden osalta sääntely kohdistuu lähinnä laatuvarmenteiden tarjoamiseen. Asiaa säännellään lain 4 luvussa. Lisäksi ehdotetussa 4 §:ssä todetaan, että tunnistusvälineillä voidaan yleensä tehdä myös sähköisiä allekirjoituksia.

Pykälän 2-4 momenteissa soveltamisalaa täsmennetään sulkemalla lain soveltamislasta

pois joitakin tilanteita. Lakia ei ensinnäkään sovelleta ainoastaan yhteisön sisäiseen vahvaan sähköiseen tunnistamiseen tai sähköiseen allekirjoittamiseen käytettävien palveluiden tarjontaan. Kysymyksessä on vahvan sähköisen tunnistuspalvelun tarjoaminen, mutta palvelua ei tarjota yleisölle eikä toiselle palveluntarjoajalle. Sama tunnistuspalvelun tarjoaja voi tarjota samaa palvelua sekä tunnistuspalvelua käyttävälle palveluntarjoajalle käytettäväksi ennalta määräämättömän joukon tunnistamiseen että jollekin yhteisölle käytettäväksi yhteisön sisäisiin tarpeisiin. Edellinen tilanne kuuluu lain soveltamisalaan, kun taas jälkimmäinen ei kuulu.

Mainitut 2 momentin soveltamisalan rajaukset koskevat ainoastaan palvelun tarjoamista. Sen sijaan esimerkiksi 4 ja 5 §:ssä todettu koskee yleisesti vahvaa sähköistä tunnistamista ja sähköisiä allekirjoituksia. Säännös ei rajoita yritysten ja yhteisöjen mahdollisuutta harkita, millaiselle vahvalle sähköiselle tunnistamiselle ja sähköiselle allekirjoittamiselle ne antavat oikeusvaikutuksia. On kuitenkin huomattava, että tätä harkintavaltaa saattavat rajoita muiden lakien säännökset.

Ehdotetun 3 momentin mukaan lain soveltamisalaan eivät kuulu myöskään sellaiset tilanteet, joissa yhteisö käyttää omaa vahvan sähköisen tunnistamisen menetelmäänsä yksinomaan omien asiakkaidensa tunnistamiseksi omissa palveluissaan. Tällaisessa toiminnassa ei ole varsinaisesti lainkaan kysymys vahvan sähköisen tunnistuspalvelun tarjoamisesta, vaan palveluntarjoajan tavoitteena on muun oman palvelunsa tarjoaminen, ja tunnistaminen liittyy siihen ainoastaan sivutuotteena. Ei ole kovinkaan todennäköistä, että tällaiset tiettyyn suljettuun tarkoitukseen käytettävät vahvan tunnistamisen menetelmät yleistyisivät suuresti.

Ehdotettu soveltamisala ja siihen tehdyt rajaukset ovat suoraa seurausta siitä, että lailla pyritään antamaan perussäännöt toimiville yleiskäyttöisten vahvan sähköisen tunnistamisen välineiden markkinoille. Jos välineen käyttäjäpiiri on ennalta rajattu, ei se voi kilpailla avoimilla, yleiskäyttöisiin menetelmiin ja välineisiin tähtäävillä markkinoilla. Yritysten ja organisaatioiden sisäisten järjestelmien käyttäjät eivät myöskään tarvitse samalla tavalla suojaa kuin itse markkinoilta välineensä hankkivat, usein kuluttajan ominaisuudessa toimivat henkilöt. Suojan tarve on pienempi myös tiettyyn suljettuun tarkoitetukseen käytettävien tunnistusvälineiden osalta, sillä niiden käyttöön mahdollisesti liittyvät riskit ovat luonnollisesti pienemmät.

Lisäksi on otettava huomioon, että ehdotettu laki on ensimmäinen pyrkimys säännellä sähköisen tunnistamisen palveluiden tarjontaa maassamme. Palveluiden tarjonta on voimakkaassa kehitysvaiheessa, ja tulevina vuosina on mahdollista, että myös uusia tunnistamismenetelmiä syntyy teknisen kehityksen myötä. Tämän johdosta on erittäin tärkeää, että ehdotettu sääntely antaa toimintamahdollisuudet uusille kehittyville järjestelyille. Uusia menetelmiä voidaan esimerkiksi testata suljetuissa ympäristöissä ennen kuin niitä tarjotaan yleiskäyttöisinä välineinä avoimilla markkinoilla. Sääntelyn piiriin voidaan myöhemmin ottaa sellaisia ilmiöitä, jotka näyttävät tarvitsevan sääntelyä. Sen sijaan jo olemassa olevan sääntelyn purkaminen on huomattavasti haastavampaa. Syntymässä olevien markkinoiden liian tiukka sääntely saattaa johtaa liian raskaiden velvoitteiden asettamiseen ja sitä kautta palveluntarjonnan kuihtumiseen.

Tapauksiin, joissa yhteisö käyttää omaa vahvaa sähköistä tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan sovelletaan kuitenkin 3 §:n, 20 §:n 1 momentin, 21-22 §:n, 23 §:n 1 momentin, 25 §:n 1 momentin ja 2 momentin sekä 27 §:n 1 momentin, 2 momentin 1 kohdan ja 3 momentin säännöksiä. Kyseiset säännökset liittyvät vastuukysymysten ratkaisemiseen. Koska tällaisessa palveluntarjonnassa ei ole kyse vahvan sähköisen tunnistuspalvelun tarjonnasta, Viestintäviraston 42 §:n 2 momentissa säädetty valvontavalta ei koske tällaista toimintaa. Ehdotetun 42 §:n 4 momentin mukaan tällaista toimintaa valvoo kuluttajasuhteissa kuluttaja-asiamies. Muutoin säännöksellä on merkitystä lähinnä juuri vastuukysymyksiä esimerkiksi tuomioistuimissa ratkaistaessa.

On selvää, että jos lain soveltamisalaan kuulumaton toimija haluaa vapaaehtoisesti noudattaa lain palveluntarjoajalle ja tarjottavalle palvelulle asetettuja laadullisia säännöksiä, ei oikeusjärjestyksessämme ole tälle

mitään yleistä estettä. Tällaiset toimijat eivät luonnollisestikaan voi tehdä 10 §:ssä tarkoitettua ilmoitusta eivätkä tulla 12 §:n mukaisesti rekisteröidyksi. Niitä ei myöskään valvota 5 luvun mukaisesti.

Pykälän 4 momentin viimeisen virkkeen mukaan soveltamisalasta on lisäksi suljettu pois vahvan sähköisen tunnistamisen ja sähköisen allekirjoituksen välineiden valmistaminen, maahantuonti ja myynti. Vahvan sähköisen tunnistusvälineiden liikkeelle lasku voidaan erottaa näistä toimista siten, että liikkeelle laskijan ja välineen haltijan välillä vallitsee pääsääntöisesti sopimussuhde. Sähköisen allekirjoittamisen osalta esimerkiksi varmentajan ylläpitämä sulkulista tekee toiminnasta palvelua erotuksena puhtaasta välineen valmistamisesta, maahantuonnista tai myynnistä.

2 §. *Määritelmät*. Pykälän 1 kohdassa määritellään vahva sähköinen tunnistaminen. Sillä tarkoitetaan henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttämällä. Vähintään kahden kolmesta kohdassa mainitusta ehdosta on samalla toteuduttava. Vahva sähköinen tunnistaminen perustuu johonkin, mitä tunnistusvälineen haltija tietää, johonkin, mitä tunnistusvälineen haltijalla on hallussaan tai johonkin tunnistusvälineen haltijan yksilöivään ominaisuuteen.

Ehdotetut kohdat a-c sekä vaatimus siitä, että kahden näistä on toteuduttava, jotta sähköisen tunnistamisen menetelmää voidaan pitää vahvana, vastaavat yleisesti esitettyä kansainvälistä vahvan sähköisen tunnistamisen määritelmää. Kohta a tarkoittaa salasanaa tai salalausetta, jonka käyttäjä joutuu antamaan käyttäjätunnuksensa yhteydessä. Kohta b puolestaan tarkoittaa tunnistusvälinettä, jonka sisältämän tiedon perusteella käyttäjäidentiteetti pystytään määrittämään. Esimerkkejä ovat sirukortti ja tietyllä SIM-kortilla varustettu matkapuhelin. Kohta c tarkoittaa käytännössä jotain käyttäjän biometristä ominaisuutta, kuten sormenjälkeä, kasvojen muotoa tai silmän iiristä.

Vahvan sähköisen tunnistamisen määritelmä pitää aina sisällään myös todentamisen, jolla varmistetaan tunnisteen aitous ja oikeellisuus. Tunnisteella tarkoitetaan tunnistamiseen käytettävää tietoa.

Pykälän 2 kohdassa määritellään tunnistusväline. Määritelmä pyrkii olemaan teknologianeutraali ja kuvaamaan mitä tahansa joko fyysisessä, sähköisessä tai tiedollisessa muodossa olevia asioita, jotka yhdessä muodostavat tunnistusvälineen. Väline voi siis tarkoittaa esimerkiksi SIM-kortille tai muulle kortille sijoitettua varmennetta ja sen käyttämiseen tarvittavaa PIN-koodia, käyttäjätunnusta ja siihen yhdistettyä vaihtuvaa salasanaa, tai sormenjälkeä ja siihen yhdistettävää PIN-koodia. Väline muodostaa yhden kokonaisuuden.

Pykälän 3 kohdassa määritellään tunnistusmenetelmä. Sillä tarkoitetaan kokonaisuutta, jonka muodostavat tunnistusväline ja yksittäisen vahvan sähköisen tunnistustapahtuman toteuttamiseksi tarvittava järjestelmä. Järjestelmällä tarkoitetaan erityisesti tarvittavia laitteita ja ohjelmistoja. Tunnistusmenetelmälle asetettavista edellytyksistä säädetään 8 §:ssä.

Pykälän 4 kohdassa määritellään tunnistuspalvelun tarjoaja. Esityksen 9 §:ssä on asetettu vaatimuksia tunnistuspalvelun tarjoajan luotettavuudelle.

Määritelmän mukaisesti varsinainen tunnistamiseen liittyvä palvelu ja välineen liikkeelle laskeminen voivat tapahtua joko saman tai eri tahon toimesta. Säännös mahdollistaa joustavuuden ja tulevaisuudessa mahdollisesti tapahtuvan eriytymiskehityksen. Samalla se mahdollistaa sen, että ilman palveluntarjoajien välisiä sopimussuhteita järjestetty vahva sähköinen tunnistaminen on myös mahdollista. Suomessa tällaista toimintaa harjoittaa Väestörekisterikeskus. Yleisöllä tarkoitetaan ennalta määrittelemätöntä henkilöjoukkoa kuten 1 §:n 1 momentissakin.

Palveluntarjoaja voi käyttää vahvan sähköisen tunnistamisen menetelmää omien asiakkaittensa tunnistamiseen ja tarjota samaa menetelmää toiselle eli vahvaa sähköistä tunnistamista käyttävälle palveluntarjoajalle. Edellinen tilanne ei kuulu lain soveltamisalaan, kun taas jälkimmäinen kuuluu. Tällainen tilanne on esimerkiksi pankeilla, jotka käyttävät pankkitunnisteita omien asiakkaittensa pankkiasiointiin ja tarjoavat samoja tunnisteita käytettäviksi muissa palveluissa.

Tunnistuspalvelun tarjoaja voi periaatteessa olla luonnollinen henkilö tai oikeushenkilö. Käytännössä muun muassa 13 pykälässä mainittu riittävien taloudellisten voimavarojen vaatimus johtanee siihen, että luonnolliset henkilöt eivät tule toimimaan palveluntarjoajina.

Pykälän 5 kohdassa määritellään tunnistusvälineen haltija. Haltijalla tarkoitetaan tässä laissa aina sitä henkilöä, jolla on vahvan sähköisen tunnistusväline hallussaan laillisen oikeuden nojalla. Jos väline joutuu pois oikeutetulta haltijalta, ei esimerkiksi löytäjästä voi tulla määritelmässä tarkoitettua välineen haltijaa. Koska välineen on oltava 20 §:n 3 momentin mukaisesti henkilökohtainen, on haltija aina samalla se henkilö, jolle väline on annettu. Ehdotetussa 23 §:n 2 momentissa todetaan selkeästi, että vahvan tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

Pykälän 6 kohdassa määritellyllä ensitunnistamisella tarkoitetaan tunnistusvälineen hakijan henkilöllisyyden todentamista välineen liikkeellelaskumenettelyn yhteydessä. Ensitunnistaminen on vahvan sähköisen tunnistamisen luotettavuuden kenties keskeisin peruspilari. Siitä säädetään 17 §:ssä. Ensitunnistaminen on termi, joka on luotu ehdotettua lakia varten. Käyttöön on haluttu ottaa termi, jolla tämä tietty tapahtuma voidaan selkeästi erottaa myöhemmistä, useita kertoja toistuvista tunnistustapahtumista. Pääsääntöisesti tunnistuspalvelun tarjoajan tarvitsee suorittaa ensitunnistaminen vain kerran yhden tunnistusvälineen haltijan osalta.

Pykälän 7 kohdassa määritellään varmenne. Varmenteella tarkoitetaan sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan. Varmennetta voidaan käyttää sekä tunnistuspalveluissa että sähköisen allekirjoituksen palveluissa. Varmenne on luotettavan kolmannen osapuolen sähköisesti allekirjoittama todistus siitä, että tietty julkinen avain kuuluu tietylle avaimen käyttäjälle. Julkisen avaimen lisäksi varmenne sisältää myös muita tietoja, kuten henkilön tai organisaation nimen, varmenteen myöntämispäivän, viimeisen voimassaolopäivän tai yksilöllisen sarjanumeron.

Varmentaja on pykälän 8 kohdan mukaan luonnollinen henkilö tai oikeushenkilö, joka tarjoaa varmenteita. Samoin kuin tunnistuspalvelun tarjoajan osalta, ei ole oletettavaa, että luonnolliset henkilöt voisivat tosiasiassa toimia varmentajina. Ehdotettu kohta vastaa muuten voimassa olevan sähköisistä allekirjoituksista annetun lain 2 §:n 8 kohtaa, mutta siihen on lisätty sana yleisölle, jolloin kyseistä sanaa ei tarvitse toistaa muissa pykälissä. Termiä käytetään ainoastaan sähköisen allekirjoittamisen yhteydessä, vaikka varmenteita voidaan käyttää myös vahvassa sähköisessä tunnistamisessa. Tällöin kuitenkin myös varmentajat kuuluvat teknologianeutraalin termin tunnistuspalvelun tarjoaja piiriin.

Pykälän 9 kohdan mukaan sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. Kohta vastaa sähköisistä allekirjoituksista annetun lain 2 §:n 1 kohtaa.

Sähköinen allekirjoitus perustuu siihen, että sähköiset tiedot liitetään toisiinsa tavalla, jossa niistä muodostuu ainutkertainen yhdistelmä, joka mahdollistaa allekirjoittajan todentamisen. Yksinkertainen sähköinen allekirjoitus on laaja käsite. Sen tarkoituksena on tunnistaa allekirjoittaja ja todentaa tiedot. Kyseessä voi yksinkertaisimmillaan olla sähköpostin allekirjoittaminen henkilön nimellä.

Määritelmä perustuu EU:n sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin, ja se vastaa yleisesti kansainvälisesti käytössä olevaa sähköisen allekirjoituksen määritelmää. Tämä määritelmä pitää aina sisällään myös henkilöllisyyden todentamiselementin.

Pykälän 10 kohdassa määritellään kehittynyt sähköinen allekirjoitus. Määritelmä vastaa voimassa olevan sähköisistä allekirjoituksista annetun lain 2 §:n 2 kohtaa. Kehittyneen sähköisen allekirjoituksen tulee a alakohdan mukaan yksiselitteisesti liittyä sen allekirjoittajaan. Tämä voidaan varmistaa siten, että ainoastaan allekirjoittajalla on hallinnassaan hänen sähköisen allekirjoituksensa tekemiseen tarvittavat allekirjoituksen luomistiedot. Luomistiedot on määritelty ehdotetussa 11 kohdassa.

Kehittyneellä sähköisellä allekirjoituksella tulee b alakohdan mukaan voida yksilöidä allekirjoittaja. Varmentaja ei siten voi myöntää identtistä varmennetta kahdelle eri henkilölle. Henkilöt, joille varmenteita myönnetään, täytyy erottaa toisistaan erityismääreillä tai vähintään varmenteen sarjanumerolla.

Menetelmän, jolla kehittynyt sähköinen allekirjoitus on luotu, tulee c alakohdan mukaan olla sellainen, että allekirjoittaja voi pitää sitä yksinomaisessa valvonnassaan. Tällainen valvontakeino voi muun muassa olla PIN-koodi, jonka avulla vain allekirjoittaja pääsee käyttämään allekirjoituksen luomistietoja, kuten yksityistä avaintaan.

Viimeisen alakohdan mukaan kehittyneen sähköisen allekirjoituksen tulee olla liitetty allekirjoitettavaan tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. Allekirjoituksen tulee siten voida varmistaa allekirjoitettavan tiedon eheys. Julkisen avaimen tekniikalla tehdyssä sähköisessä allekirjoituksessa sanomatiivisteen uudelleen muodostaminen ja vertaaminen viestin mukana tulleeseen sanomatiivisteeseen mahdollistaa sen, että viestin vastaanottaja voi tarkistaa viestin muuttumattomuuden.

Pykälän 11 kohdan mukaan allekirjoituksen luomistiedoilla tarkoitetaan allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämää ainutkertaista tietokokonaisuutta, kuten koodeja ja yksityisiä avaimia. Määritelmä vastaa sähköisistä allekirjoituksista annetun lain 2 §:n 4 kohtaa.

Kyseessä on se ainutkertainen tietokokonaisuus, jota käyttäen voidaan luoda sähköinen allekirjoitus. Julkisen avaimen järjestelmässä allekirjoituksen luomistieto on allekirjoittajan yksityinen avain, joka on ainutkertainen numerosarja. Kun avainta käytetään yhdessä tietyn algoritmin kanssa sanomatiivisteen salaamiseen, saadaan aikaan ainutkertainen salakirjoitus, joka aukeaa ainoastaan yksityistä avainta vastaavalla julkisella avaimella.

Pykälän 12 kohdan mukaan allekirjoituksen luomisvälineellä tarkoitetaan niitä ohjelmistoja ja laitteita, joita käytetään apuna yhdessä allekirjoituksen luomistietojen kanssa sähköisen allekirjoituksen luomiseksi. Määritelmä vastaa sähköisistä allekirjoituksista annetun lain 2 §:n 5 kohtaa.

Julkisen avaimen järjestelmässä allekirjoituksen luomisväline voi sisältää esimerkiksi tiivistealgoritmin sanomatiivisteen laskemiseksi, salausalgoritmin sanomatiivisteen salaamiseksi sekä allekirjoittajan yksityisen avaimen. Lisäksi luomisvälineessä on erityisiä ohjelmistoja allekirjoituksen luomista varten.

Pykälän 13 kohdassa määritellään allekirjoituksen todentamistiedot. Niillä tarkoitetaan sähköisen allekirjoituksen todentamisessa käytettävää tietokokonaisuutta, kuten koodeja ja julkisia avaimia. Kyseessä on siis tietokokonaisuus, jonka avulla vastaanottaja voi todentaa vastaanottamansa sähköisen allekirjoituksen. Julkisen avaimen järjestelmässä tietokokonaisuus on niin kutsuttu julkinen avain. Ehdotettu määritelmä vastaa sähköisistä allekirjoituksista annetun lain 2 §:n 6 kohtaa.

2 luku. Oikeusvaikutukset ja henkilötietojen käsittely

3 §. *Pakottavuus.* Pykälän mukaan tunnistuspalvelun tarjoaja ja tunnistusvälineen haltijana oleva kuluttaja eivät voi sopia toisin lain säännöksistä, ellei laissa nimenomaisesti toisin säädetä. Tällainen sopimusehto on pykälän mukaan mitätön. Sopimusehdon mitättömyys merkitsee sitä, että ehto on osapuolten välisessä sopimussuhteessa vailla vaikutusta. Tuomioistuimen ja kuluttajariitalautakunnan on otettava ehdon mitättömyys huomioon viran puolesta. Säännös ei estä osapuolia tekemästä sopimusta, joka poikkeaa laista tunnistusvälineen haltijan eduksi.

Säännös on pakottava vain kuluttajien osalta. Se vastaa kuitenkin lain peruslähtökohtaa, jonka mukaan muut toimijat erityisesti luottamusverkoston muodostuessa voivat luottaa siihen, että kaikki tunnistuspalvelun tarjoajat noudattavat omassa toiminnassaan tämän lain ja erityisesti sen 3 luvun säännöksiä eräänlaisena minimisääntelynä.

4 §. *Vahva sähköinen tunnistaminen ja sähköiset allekirjoitukset.* Pykälässä todetaan se käytännössä vallitseva tilanne, että sähköisiä allekirjoituksia ja kehittyneitä sähköisiä allekirjoituksia voidaan tehdä myös vahvan sähköisen tunnistamisen menetelmillä ja välineillä niiden ominaisuuksista riippuen. Eh-

dotettu momentti on luonteeltaan toteava, eikä muuta vallitsevaa oikeustilaa. Asian toteaminen ehdotetussa momentissa selkeyttää tilannetta kuitenkin huomattavasti. Säännös ei sulje pois myöskään sitä mahdollisuutta, että sähköisiä allekirjoituksia voidaan välineestä riippuen ehkä tehdä myös heikoilla sähköisillä tunnistusvälineillä. Pykälä koskee kuitenkin ainoastaan vahvan sähköisen tunnistamisen välineitä sen johdosta, että heikot eivät lainkaan kuulu lain soveltamisalaan.

Yksinkertaisimmillaan sähköinen allekirjoitus voi olla esimerkiksi sähköpostiviestin loppuun kirjoitettu henkilön nimi. Julkisen avaimen teknologiaan perustuvilla varmenteilla voidaan puolestaan saada aikaan kehittynyt sähköinen allekirjoitus. Kaikilla vahvoilla sähköisillä tunnistusvälineillä ei välttämättä saada aikaan sähköiseksi allekirjoitukseksi katsottavaa tointa, mutta tämä ei silti sinällään estä tunnistusvälineen käyttämistä oikeustoimien tekemisessä, kuten 5 pykälässä todetaan. Tunnistusvälineen teknisten ja muiden ominaisuuksien lisäksi mahdollisuus tehdä sähköisiä allekirjoituksia saattaa riippua muusta lainsäädännöstä ja osapuolten tahdosta. Osapuolten tahdosta estää tai rajoittaa tunnistusvälineen käyttöä oikeustoimien tekemiseksi säädetään 18 §:ssä.

Mahdollisuus tehdä allekirjoituksia voi olla myös tunnistusvälineeseen liittyvä erillinen ominaisuus. Tunnistusvälineelle voidaan esimerkiksi sijoittaa erityisesti allekirjoittamiseen tarkoitetut allekirjoitusavaimet.

5 §. *Oikeustoimien tekeminen.* Pykälän 1 momentissa todetaan se tosiseikka, että mahdollisuus tehdä sähköisiä allekirjoituksia ei vaikuta pääsääntöisesti mahdollisuuteen tehdä oikeustoimia vahvoilla sähköisillä tunnistusvälineillä, jos osapuolet niin haluavat. Tämä on seurausta siitä, että suurinta osaa Suomessa tehtävistä oikeustoimista ei koske allekirjoittamisen muotovaatimus. Ehdotetulla säännöksellä vahvistetaan tosiasiallisesti voimassa oleva oikeustila. Jo varsin pitkään oikeustoimia on voinut tosiasiallisesti tehdä esimerkiksi pankkitunnuksien avulla.

Momentti ei siis ole oikeutta luova, vaan se on luonteeltaan toteava. Oikeustoimen tekemiseen liittyvät vaikutukset eivät suoranaisesti ole sidoksissa itse tunnistamiseen, vaan oikeustoimien tekeminen vahvan sähköisen tunnistusvälineiden avulla on ominaisuus, joka voidaan liittää tunnistusvälineen käyttöön. Olennaista asiassa on osapuolten tahtotila. Mitään osapuolta, eli tunnistuspalvelun tarjoajaa, sitä käyttävää palveluntarjoajaa eikä myöskään tunnistusvälineen haltijaa voida yleisesti tai tapauskohtaisesti pakottaa oikeustoimien tekemiseen tunnistusvälineillä, mutta sellaista vaihtoehtoa haluaville on tarjottava siihen mahdollisuus. Juuri mahdollisuus oikeustoimien tekemiseen lisää varmasti kiinnostusta tarjota ja hankkia vahvoja sähköisiä tunnistusvälineitä. Palveluntarjoajan on huolehdittava siitä, että käyttäjä on tosiasiassa tietoinen kaikista oikeustoimen tekemiseen liittyvistä seikoista.

Säännös ei estä sitä, että oikeustoimia voidaan mahdollisesti tehdä myös sellaisilla tunnistusvälineillä, jotka eivät täytä tässä luvussa asetettuja edellytyksiä, jos osapuolet niin tahtovat. Ehdotettu kirjaus koskee vain vahvoja sähköisiä tunnistusvälineitä, koska heikko tunnistaminen ei lainkaan kuulu lain soveltamisalaan. Olemassa ei ole yleistä sääntelyä siitä, milloin vahva sähköinen tunnistaminen on tarpeen. Tyypillisiksi käyttötilanteiksi voitaneen katsoa taloudellisia tai oikeudellisia sitoumuksia ja luottamuksellisten tietojen, kuten henkilötietolain mukaisten arkaluonteisten henkilötietojen tai organisaation salassa pidettävien tietojen käsittelyä edellyttävät sähköiset palvelut. Jatkossa lainsäädännössä saatetaan asettaa vahvaa sähköistä tunnistamista koskevia edellytyksiä erikseen säädettävien palveluiden osalta.

Ehdotetussa säännöksessä tarkoitetaan sellaisten oikeustoimien tekemistä, joihin ei muualla lainsäädännössä kohdistu erityisiä muotovaatimuksia. Laissa tai muissa normissa voidaan erikseen säätää erilaisista muotovaatimuksista, mutta tällaiset säännökset eivät oikeusjärjestyksessämme ole kovin yleisiä. Yksityisoikeudellisten sopimusten osalta lainsäädännössä yleisimmin käytettyjä muotovaatimuksia ovat lähinnä sopimuksen tekeminen kirjallisesti ja sopimuksen allekirjoittaminen. Ilmauksia kirjallisesti tai allekirjoittaa ei ole määritelty tarkemmin lainsäädännössä. Myös viranomaisessa asiointiin riittää yleensä muotovapaa yhteydenotto.

Pykälän 2 momentissa säädetään sähköisen allekirjoituksen oikeusvaikutuksesta. Mo-

mentin ensimmäisessä virkkeessä todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla tehty kehittynyt sähköinen allekirjoitus. Säännös vastaa sähköisistä allekirjoituksista annetun lain 18 §:n säännöstä, jolla on pyritty laittamaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 5 artiklan 2 kohta. Sen mukaan jäsenvaltioiden on varmistettava, että sähköiseltä allekirjoitukselta ei voi evätä oikeudellista vaikutusta ja hyväksyttävyyttä todisteena oikeudellisissa menettelyissä yksinomaan sen vuoksi, että allekirjoitus on sähköisessä muodossa, se ei perustu laatuvarmenteeseen tai sitä ei ole tehty turvallisen allekirjoituksen luomisvälineen avulla.

Sähköisistä allekirjoituksista annetun lain 18 §:n tulkinta on kuitenkin Suomessa osoittautunut sillä tavoin ongelmalliseksi, että ainoastaan laatuvarmenteen on katsottu useissa yhteyksissä kelpaavan sähköiseen allekirjoittamiseen. Tämän johdosta asiaa on pyritty selkeyttämään lisäämällä momenttiin toinen virke, joka on peräisin direktiivin 5 artiklan 2 kohdasta. Sen mukaan sähköiseltä allekirjoitukselta ei tule evätä oikeusvaikutuksia yksinomaan sen vuoksi, että se on tehty muulla sähköisen allekirjoittamisen tavalla kuin kehittyneellä sähköisellä allekirjoituksella, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä.

Kuten jo 1 momentin osalta todettiin, oikeustoimille ei Suomessa ole yleensä asetettu erityisiä muotovaatimuksia. Millainen tahansa sähköinen allekirjoitus voidaan luonnollisesti myös riitauttaa vastaavasti kuin perinteinen käsin tehtykin allekirjoitus. Suomalaisissa tuomioistuimissa sovelletaan vapaata todisteiden harkintaa.

Sähköisen allekirjoituksen käyttäminen edellyttää luonnollisesti, että oikeustoimen tekeminen sähköisesti on sallittua ja mahdollista. Ehdotettu säännös ei vaikuta esimerkiksi siihen, milloin oikeustoimi edellytetään tehtäväksi jollain muulla tavalla kuin sähköisesti.

Pykälän 3 momentissa todetaan, että sähköisen allekirjoituksen käytöstä hallinnossa säädetään erikseen. Säännös vastaa sähköisistä allekirjoituksista annetun lain 3 §:n 2 momenttia. Sähköisestä asioinnista viranomaisessa annetun lain 9 §:n nojalla vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja. Jos asian vireillepanossa tai muussa käsittelyssä edellytetään allekirjoitettua asiakirjaa, allekirjoitusvaatimuksen täyttää myös sähköisistä allekirjoituksista annetun lain 18 §:ssä tarkoitettu sähköinen allekirjoitus. Viranomaiselle saapunutta sähköistä asiakirjaa ei tarvitse täydentää allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä. Edelleen lain 16 §:n mukaan päätösasiakirja voidaan allekirjoittaa sähköisesti. Viranomaisen sähköisen allekirjoituksen on täytettävä sähköisistä allekirjoituksista annetun lain 18 §:ssä säädetyt edellytykset. Esitykseen on liitetty myös sähköistä asiointia viranomaisessa koskevan lain muutosehdotukset, joissa viittaukset sähköisistä allekirjoituksista annettuun lakiin on muutettu viittauksiksi tähän lakiin.

6 §. *Henkilötietojen käsittely.* Ehdotetussa 6 §:ssä säädettäisiin henkilötietojen käsittelystä sekä vahvan sähköisen tunnistamispalvelun että varmeisiin perustuvan sähköisen allekirjoituspalvelunkin tarjonnassa. Säännös koskee kaikkia sähköisiä allekirjoituksia tarjoavia varmentajia, siis myös muita kuin laatuvarmenteita tarjoavia varmentajia. Jos sähköisiä allekirjoituksia tarjotaan osana tunnistuspalvelua, kysymys on terminologisesti tunnistuspalvelun tarjoajasta. Sähköisiin allekirjoituksiin liittyviltä osin säännöksellä pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 8 artiklan 1 ja 2 kohdat.

Pykälän 1 momentissa säädettäisiin käsittelyn tarkoituksesta ja perusteista. Tunnistuspalvelun tarjoaja saa käsitellä tunnistusvälineen liikkeelle laskemisessa ja palvelun ylläpidossa sekä tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja. Sähköisiä allekirjoituksia tarjoava varmentaja saa käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja. Henkilötiedot, joiden käsittelyn käsillä oleva säännös mahdollistaa, saattavat vaihdella käytettävistä tunnistusvälineistä ja menetelmistä riippuen.

Yleensä lienee tarpeen käsitellä ainakin välineen haltijan nimeä, yhteystietoja ja yksilöivää tunnusta. Vahvaan sähköiseen tunnistamiseen käytettävien varmenteiden tietosisällöstä on erillinen säännös 19 §:ssä ja laatuvarmenteen tietosisällöstä 30 §:ssä. Ehdotettu momentti täyttää henkilötietolain 7 §:n edellytykset käyttötarkoitussidonnaisuudesta.

Käsittely saa tapahtua henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdissa tarkoitetuilla perusteilla. Tämä tarkoittaa sitä, että henkilötietoja saa käsitellä ainoastaan rekisteröidyn yksiselitteisesti antamalla suostumuksella ja rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja ei siten saa käsitellä henkilötietoja henkilötietolain 8 §:n 1 momentin 3-9 kohtien mukaisilla perusteilla. Sanottu ei luonnollisestikaan estä sitä, että palveluntarjoajalla voi olla muun lain perusteella muussa ominaisuudessa toimiessaan oikeus käsitellä henkilötietoja henkilötietolain 8 §:n 1 momentin muidenkin kohtien perusteella.

Käsittelyllä tarkoitettaisiin säännöksessä samaa kuin henkilötietolain 3 §:n 2 kohdassa eli ehdotuksessa on omaksuttu kyseisen lain sääntelyä vastaava laaja-alainen käsittelytermi. Käsittelyllä tarkoitettaisiin siten kaikenlaista henkilötietojen käsittelyä, kuten esimerkiksi tietojen rekisteröinti, tallentaminen ja hävittäminen.

Henkilötietolain 3 §:n 7 kohdassa on määritelty suostumus. Se tarkoittaa kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Suostumuksen tulee olla rekisteröidyn tietoinen tahdonilmaisu. Rekisteröidyn on siten suostumusta antaessaan pitänyt olla tietoinen siitä, mihin hän suostumuksensa antaa. Suostumuksen on myös aina oltava vapaaehtoinen. Jos suostumuksen olemassaolosta syntyisi kiistaa, todistustaakka suostumuksen olemassaolosta on rekisterinpitäjällä. Suostumus on voimassa toistaiseksi, jollei suostumuksesta muuta ilmene. Rekisteröidyllä on oikeus milloin tahansa peruuttaa suostumuksensa. Henkilötietolain eräissä pykälissä suostumukseen on henkilötietodirektiivin mukaisesti liitetty ilmaisuja, jotka täsmentävät suostumuksen tarkkarajaisuutta. Muun muassa juuri lain 8 §:n 1 momentin 1 kohdassa edellytetään, että rekisteröity on antanut suostumuksensa yksiselitteisesti. Yksiselitteisen suostumuksen vaatimus korostaa rekisteröidyn tahdonilmaisun selkeyttä.

Pykälän 1 momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat lisäksi kerätä henkilötietoja henkilöltä itseltään. Keräämisen tarkoituksen on oltava sama kuin käsittelyssä muutoinkin. Tunnistuspalvelun tarjoaja saa käsitellä tunnistusvälineen liikkeelle laskemisessa ja palvelun ylläpidossa sekä vahvan sähköisen tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja ja sähköisiä allekirjoituksia tarjoava varmentaja saa käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja. Kuten edellä todettiin, henkilötietolain käsittelytermi on laaja ja kattaa myös tietojen keräämisen. Ehdotettuun momenttiin on kuitenkin otettu erillinen lisäys tietojen keräämisestä sen johdosta, että asiasta on nimenomainen säännös sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 8 artiklan 2 kohdassa.

Pykälän 2 momentissa todetaan, että henkilötietoja saa käsitellä muussa kuin 1 momentissa mainitussa tarkoituksessa ainoastaan henkilötietolain 8 §:n 1 momentin 1 kohdassa tarkoitetuilla perusteilla. Käsittelyperusteen rajaaminen ainoastaan henkilön yksiselitteisesti antamaan suostumukseen johtuu siitä, että käsittelyä muussa tarkoituksessa ei voitane useinkaan riittävällä tarkkuudella rajata toimeksiannossa tai sopimuksessa. Myös tämä säännös on seurausta direktiivin 8 artiklan 2 kohdasta.

Sääntely vastaa asiallisesti sähköisistä allekirjoituksista annetun lain 19 §:ää.

Pykälän 3 momentissa säädetään henkilötunnuksen käsittelystä. Henkilötietolain 13 §:n 1 momentin mukaan henkilötunnusta saa käsitellä henkilön yksiselitteisesti antamalla suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän

oikeuksien ja velvollisuuksien toteuttamiseksi.

Henkilötunnuksen käsittely tunnistuspalvelun ja sähköisiin allekirjoituksiin liittyvän varmennepalvelun yhteydessä on välttämätöntä sen johdosta, että palveluiden toteuttaminen luotettavasti nimenomaan edellyttää henkilöiden varmaa erottamista toisistaan. Tämä olisi sinällään jo henkilötietolain 13 §:n 1 momentin mukaan seikka, joka oikeuttaisi henkilötunnuksen käsittelyyn ilman nimenomaista lain säännöstäkin. Asiasta on kuitenkin haluttu ottaa selkeät säännökset pykälään. Tämä on erityisesti tarpeen sen johdosta, että sähköisistä allekirjoituksista annetun lain 19 §:n 2 momentissa on kielletty henkilötunnuksen sisällyttäminen varmenteeseen. Ehdotettu momentti korvaa samalla sähköisistä allekirjoituksista annetun lain säännöksen.

Ehdotetun momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja voi tarkistaessaan hakijan henkilöllisyyden vaatia hakijaa ilmoittamaan henkilötunnuksensa. Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat käsitellä henkilötunnusta rekistereissään. Käsittelyn tarkoituksen on oltava sama kuin 1 momentissa.

Henkilötunnus voidaan sisällyttää tunnistusvälineen tai varmenteeseen silloin, jos välineen tai varmenteen tietosisältö on ainoastaan sellaisen tahon saatavilla, jolle se on välttämätöntä palvelun toteuttamiseksi. Henkilötunnus ei saa kuitenkaan olla saatavissa julkisesta hakemistosta. Jos palvelu on sellainen, ettei sitä voida toteuttaa ilman julkista hakemistoa, palveluntarjoajan täytyy käyttää jotakin muuta yksilöivää tunnusta. Tällöin varmenteeseen voidaan jatkossa sisällyttää esimerkiksi sähköinen asiointitunnus. Eduskunnassa käsittelyssä on laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista, jonka 43 §:n 2 momentin 2 kohdan mukaan sähköinen asiointitunnus voidaan luovuttaa Suomeen sijoittautuneelle varmentajalle, joka käyttää sitä varmenteessa varmenteen haltijan yksilöivänä tunnistetietona.

Pykälän 3 momentin mukaan henkilötietojen käsittelystä vahvan sähköisen tunnistuspalvelun tarjoamisen yhteydessä on muutoin voimassa, mitä henkilötietolaissa säädetään. Palveluntarjoajalle ja sen palveluksessa olevalle henkilötietoja käsittelevälle henkilöstölle ei siis riitä ehdotetun lain säännösten tunteminen, vaan suurin osa henkilötietojen käsittelyn materiaalisista säännöksistä tulee alan yleislainsäädännöstä eli henkilötietolaista. Lisäksi henkilötietojen käsittelystä on jossain määrin kyse myös tämän lain 19, 24, 30, 37 ja 38 §:ssä.

Ehdotetussa 15 §:ssä säädetään tunnistuspalvelun tarjoajan velvollisuudesta antaa tietoja ennen sopimuksen tekemistä. Sen 3 momentissa viitataan henkilötietoja koskevan tiedonantovelvollisuuden osalta henkilötietolakiin.

7 §. *Väestötietojärjestelmään tallennettujen tietojen käyttäminen.* Pykälän 1 momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat hankkia ja tarkastaa hakijan tai haltijan väestötietojärjestelmään tallennetut henkilötiedot henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdissa tarkoitetuilla perusteilla. Kysymys on siis rekisteröidyn yksiselitteisesti antamasta suostumuksesta, rekisteröidyn toimeksiannosta, sellaisen sopimuksen täytäntöönpanemisesta, jossa rekisteröity on osallisena tai sopimusta edeltävien toimenpiteiden toteuttamisesta rekisteröidyn pyynnöstä.

Myös käsittelyn tarkoitus on sama kuin 6 §:ssä. Tunnistuspalvelun tarjoaja saa siis käsitellä tunnistusvälineen liikkeelle laskemisessa ja palvelun ylläpidossa sekä vahvan sähköisen tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja. Sähköisiä allekirjoituksia tarjoava varmentaja saa käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja.

Uuden väestötietolain 4 luvussa on säännökset väestötietojärjestelmään tallennettujen tietojen luovuttamisesta. Tietoja voidaan luovuttaa tiettyihin luvussa mainittuihin tarkoituksiin. Lisäksi lain 34 §:ssä säädetään muusta kuin väestötietolaissa erikseen säädettyyn tarkoitukseen tapahtuvasta tietojen luovuttamisesta. Sen 1 momentissa säädetään eräistä luovutustilanteista. Pykälän 2 momentissa todetaan, että muuten väestötietojärjestelmän tietoja voidaan luovuttaa vain, jos hakijalla on oikeus käsitellä luovutettavia tietoja henkilötietolain tai muun lain perusteella.

Ehdotettu 1 momentin säännös on tarpeen nimenomaan tästä syystä.

Säännös noudattelee sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 8 artiklan 1 ja 2 kohdassa säädettyä.

Pykälän 2 momentissa todetaan, että tiedot väestötietojärjestelmästä luovutetaan julkisoikeudellisena suoritteena sen mukaan kuin valtion maksuperustelaissa (150/1992) säädetään. Käytännössä säännös tarkoittaa omakustannushintaa.

Ehdotettu pykälä vastaa asiallisesti sähköisistä allekirjoituksista annetun lain 20 §:ää

3 luku. Vahva sähköinen tunnistaminen

8 § *Tunnistusmenetelmälle asetettavat vaatimukset.* Pykälän 1 momentissa luetellaan neljä tekijää, jotka ovat edellytyksenä sille, että tunnistuspalveluna tarjottavaa tunnistusmenetelmää voidaan pitää vahvana. Luettelo on laadittu vastaavaan tapaan kuin kehittyneen sähköisen allekirjoituksen määritelmä 2 §:n 10 kohdassa.

Pykälän 1 momentin 1 kohdan mukaan tunnistusmenetelmän perustana on oltava huolellinen ensitunnistaminen, jota koskevat tiedot ovat jälkikäteen tarkastettavissa. Ensitunnistaminen on määritelty määritelmien 6 kohdassa ja siitä säädetään 17 §:ssä. Pääsääntönä ehdotetussa 17 §:ssä on se, että tunnistaminen tapahtuu henkilökohtaisesti poliisin myöntämistä henkilöllisyyden osoittavista asiakirjoista. Lisäksi ehdotetun 24 §:n mukaan tunnistuspalveluntarjoajan on tallennettava tarvittavat tiedot ensitunnistamisesta sekä siinä käytetystä asiakirjasta.

Momentin 2 kohdan mukaan tunnistusmenetelmän edellytyksenä on, että sillä voidaan yksiselitteisesti tunnistaa tunnistusvälineen haltija. Tällä tarkoitetaan muun muassa sitä, että kahdelle henkilölle ei voida myöntää samanlaista tunnistusvälinettä. Henkilöt, joille tunnistusvälineet myönnetään, on myös eroteltava toisistaan henkilökohtaisilla yksilöivillä tunnisteilla.

Momentin 3 kohdan mukaan menetelmällä on voitava riittävällä luotettavuudella varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä. Kyseessä voi olla esimerkiksi PIN-koodi tai biometrinen tunniste, joiden käyttäminen on täysin välineen haltijan hallinnassa.

Momentin 4 kohdan mukaan tunnistusmenetelmän on edelleen oltava riittävän turvallinen ja luotettava ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat. Esimerkiksi, jos tarjottava tunnistusmenetelmä perustuu varmenteisiin, palveluntarjoajan on varmistettava, että käytettävä algoritmi on riittävän vahva ja avainparin pituus riittävä.

Käytössä olevista vahvan sähköisen tunnistamisen menetelmistä selvästi yleisimpiä ovat pankkitunnisteet. Lisäksi käytössä on julkisen avaimen järjestelmään perustuvia varmenteita. Niitä on tarjonnut viime vuosina lähinnä Väestörekisterikeskus, mutta näköpiirissä on se mahdollisuus, että teleyritykset aloittaisivat mobiilivarmenteiden tarjoamisen jo vuonna 2009. Näitä tunnistusvälineitä tarjottaneen vielä pitkälle tulevaisuuteen. Erityisesti julkisen avaimen järjestelmään perustuvien varmenteiden laajamittainen käyttö lienee vasta edessäpäin. Näiden lisäksi lähivuosina saattaa tulla käyttöön biometriikkaan pohjautuvia tunnistusmenetelmiä. Sen sijaan esimerkiksi käyttäjätunnus-salasanaparin käyttö tunnistamismenetelmänä sekä erilaiset syntymäaikaan, kotiosoitteeseen sekä muihin vastaaviin henkilötietoihin perustuvat tiedustelut ovat heikkoa tunnistamista.

Pykälän 2 momentti mahdollistaa vahvan sähköisen tunnistuspalvelun tarjoamisen anonyymisti siten, että tunnistuspalvelua käyttävä palveluntarjoaja ei saa tietoonsa välineen haltijan todellista identiteettiä. Säännös mahdollistaa esimerkiksi sellaiset palvelut, joiden käyttäminen on henkilön iästä riippuvainen, mutta varsinainen tunnistaminen ei ole tarpeen. Henkilön todellinen identiteetti on näissäkin tapauksissa kuitenkin aina selvitettävissä, mikäli se jostain syystä olisi myöhemmin tarpeen. Tällaista tilannetta säätelevät 24 §:n säännökset.

Pykälän 2 momentin avulla pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 8 artiklan 3 kohta. Kuten 4 §:ssä todetaan, sähköisiä allekirjoituksia voidaan tehdä vahvan sähköisen tunnistusvälineillä ja niitä voidaan tarjota osana tunnistuspalveluita.

Pykälän 3 momentti sisältää valtuutussäännöksen, joka on erityisesti tarpeen sen johdosta, että sähköinen tunnistaminen on hyvin tekninen ala, joka kehittyy jatkuvasti. Ehdotetun momentin mukaan Viestintävirasto voi antaa tarvittaessa tarkempia teknisiä määräyksiä 1 momentissa tarkoitetuista seikoista.

9 §. *Tunnistuspalvelun tarjoajalle asetettavat vaatimukset*. Pykälän 1 momentin mukaan tunnistuspalvelun tarjoajana olevan tai sen lukuun toimivan luonnollisen henkilön, palveluntarjoajana olevan yhteisön tai säätiön hallituksen tai hallintoneuvoston jäsenten ja varajäsenten, toimitusjohtajan, vastuunalaisen yhtiömiehen taikka muussa näihin rinnastettavassa asemassa olevien on oltava täysikäisiä, he eivät saa olla konkurssissa eikä heidän toimintakelpoisuutensa saa olla rajoitettu. Toimintakelpoisuuden rajoitukset voivat olla seurausta esimerkiksi vajaavaltaisuudesta.

Pykälän 2 ja 3 momentissa säädetään tunnistuspalvelun tarjoajan luotettavuudesta. Pykälän 2 momentin mukaan palveluntarjoajaa ei pidetä luotettavana, jos 1 momentissa tarkoitettu henkilö on lainvoiman saaneella tuomiolla tuomittu viiden viimeisen vuoden aikana vankeusrangaistukseen tai kolmen viimeisen vuoden aikana sakkorangaistukseen rikoksesta, jonka voidaan katsoa osoittavan henkilön olevan ilmeisen sopimaton harjoittamaan vahvan sähköisen tunnistuspalvelun tarjontaa. Tällainen ilmeinen sopimattomuus voi olla seurausta esimerkiksi riittävän vakavista talousrikoksista tai järjestäytyneen rikollisjärjestön jäsenenä olemisesta.

Pykälän 3 momentin mukaan tunnistuspalveluntarjoajaa ei pidetä luotettavana myöskään silloin, jos 1 momentissa tarkoitettu henkilö on muutoin aikaisemmalla toiminnallaan osoittanut olevansa ilmeisen sopimaton tunnistuspalvelun tarjoajaksi.

Momentissa tarkoitettua ilmeistä sopimattomuutta tunnistuspalvelun tarjontaan voi osoittaa esimerkiksi lainvoimaa vailla oleva tuomio 2 momentissa tarkoitetusta rikoksesta. Säännöstä voidaan soveltaa myös siinä tilanteessa, jossa henkilö on lainvoimaisesti tuomittu vankeusrangaistukseen yli viisi vuotta sitten tai sakkorangaistukseen yli kolme vuotta sitten, jos rikos osoittaa henkilön ilmeistä sopimattomuutta tarjoamaan tunnistuspalvelua.

Henkilön ilmeinen sopimattomuus tunnistuspalvelun tarjoamiseen ei edellytä sitä, että hänet on tuomittu rikoksesta rangaistukseen. Henkilö on voitu myös määrätä liiketoimintakiellosta annetun lain (1059/1985) mukaisesti liiketoimintakieltoon. Kieltoon ovat saattaneet johtaa esimerkiksi verovelvollisuuteen tai kirjanpitoon liittyvät laiminlyönnit. Liiketoimintakieltoon määrääminen ei edellytä, että laiminlyönnistä on tuomittu rangaistus. Jos kielto on edelleen voimassa, ei tunnistuspalvelun tarjoamista voi luonnollisestikaan harjoittaa. Päättynyt liiketoimintakielto on myös otettava luotettavuuden arvioinnissa huomioon.

10 §. *Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toiminnan aloittamisesta.* Pykälän 1 momentin mukaan Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on ennen toimintansa aloittamista tehtävä asiasta ilmoitus Viestintävirastolle. Ilmoituksen on oltava kirjallinen. Säännös kohdistuu Suomeen sijoittautuneisiin palveluntarjoajiin EU:n palveludirektiivin asettamien vaatimusten johdosta. Palveludirektiivi lähtee siitä lähtökohdasta, että jäsenvaltiot kohdistavat lainsäädäntöään nimenomaan alueilleen sijoittautuneisiin palveluntarjoajiin. Direktiivin 16 artiklan 2 kohta muun muassa kieltää jäsenvaltioita rajoittamasta toiseen jäsenvaltioon sijoittautuneen palveluntarjoajan vapautta tarjota palveluita esimerkiksi asettamalla niille velvoite kirjautua jäsenvaltion voimassa olevaan rekisteriin. Selvää luonnollisesti on, että sääntely ei saa olla syrjivää eikä estää palveluiden vapaata liikkumista.

Palveludirektiivin 37 resitaalissa käsitellään sijoittautumisen käsitettä. Sen mukaan palveluntarjoajan sijoittautumispaikan määrittämisessä on noudatettava yhteisöjen tuomioistuimen oikeuskäytäntöä, jonka mukaan sijoittautumisen käsitteeseen kuuluu taloudellisen toiminnan tosiasiallinen harjoittaminen kiinteästä toimipaikasta määräämättömän ajan. Tämä vaatimus voi täyttyä myös, jos yritys perustetaan määräajaksi tai jos se vuokraa rakennuksen tai tilan, josta käsin se harjoittaa toimintaansa. Sijoittautumisen ei tarvitse toteutua tytäryhtiön, sivuliikkeen tai kauppaedustajan liikkeen muodossa vaan sii-

hen riittää toimipaikka, jota johtaa palvelun tarjoajan oma henkilöstö tai henkilö, joka on riippumaton, mutta jolla on lupa toimia pysyvästi yrityksen puolesta, kuten silloin, jos kyseessä olisi kauppaedustajan liike. Määritelmä edellyttää toiminnan tosiasiallista harjoittamista palveluntarjoajan sijoittautumispaikassa, joten pelkkää postilokeroa ei katsota sijoittautumiseksi.

Ehdotetussa 1 momentissa säädetään lisäksi, että ilmoituksen voi tehdä myös sellainen palveluntarjoajien yhteenliittymä, jonka hallinnoimaa palvelua on pidettävä yhtenä tunnistuspalveluna. Tunnistuspalvelun tarjoajien yhteistyöjärjestelyt luottamusverkostossa voivat tulevaisuudessa muodostaa oman oikeushenkilönsä, jolloin tällaisen yhteistyöjärjestelyn on katsottava olevan oma palveluntarjoajansa. Tällöin myös sen olisi tehtävä ilmoitus toiminnan aloittamisesta Viestintävirastolle. Mikäli näin ei ole, vaan yhteistyöjärjestely perustuu osapuolten välisiin sopimuksiin, on yhteistyöjärjestelyn tarpeelliset tiedot ilmoitettava Viestintävirastolle osana 14 §:ssä tarkoitettuja tunnistusperiaatteita. Jos tunnistusvälineen liikkeelle laskeminen ja muu tunnistuspalvelu (issuing/acquiring) eriytyvät omiksi oikeushenkilöikseen ja erillisiksi palvelukokonaisuuksiksi, myös näiden kummankin osalta on molempien palveluntarjoajien tehtävä ilmoitus.

Jatkossa erilaisiin yhteistyöjärjestelyihin osallistuvat palveluntarjoajat joutuisivat tekemään omat ilmoituksensa siinä tapauksessa, että kukin niistä hallinnoisi omaa tunnistusjärjestelmäänsä, ja ainoastaan ulospäin tarjottava palvelurajapinta olisi yhteinen.

Mikäli palveluntarjoajien välinen yhteistyöjärjestely on kuitenkin niin kiinteä, että olennaiset osat palvelusta hoidetaan yhteisen kokonaisuutena hallinnoitavan järjestelyn kautta, palveluntarjoajat voivat myös tehdä yhteisen ilmoituksen. Käytännössä tällainen tilanne saattaa olla kyseessä niin sanotulla 4-pankkiryhmällä, jonka muodostavat Aktia Pankit, säästöpankit ja paikallisosuuspankit. Niiden tunnistuspalvelua hoitaa SAMLINK. Jos palveluntarjoajat tekevät tällaisessa tapauksessa yhteisen ilmoituksen, maksaa ehdotetussa 47 §:ssä tarkoitetun rekisteröimismaksun ja valvontamaksun yhteenliittymä.

Ilmoituksen on ehdotetun 2 momentin mukaan sisällettävä palveluntarjoajan nimi ja täydelliset yhteystiedot, tiedot tarjottavista palveluista, tiedot ehdotetun lain 8, 9, 13 ja 14 §:ssä tarkoitetuista seikoista sekä muut valvonnan kannalta tarpeelliset tiedot. Tiedoilla tarjottavista palveluista tarkoitetaan yleisluontoista selvitystä, sillä tarjottavien palveluiden tekninen toteuttamistapa käy perusteellisesti ilmi 8 §:n edellyttämästä selvityksestä. Mikäli markkinoilla jatkossa tarjotaan erikseen esimerkiksi tunnistusvälineen liikkeelle lasku ja muu tunnistuspalvelu tai mikäli markkinoille tulee sellaisia yhteistyöjärjestelyjä, jotka muodostavat itsenäisen oikeushenkilön, on näiden seikkojen käytävä ilmi ilmoituksesta. Lisäksi tietoihin tarjottavista palveluista kuuluvat myös tiedot siitä, voidaanko tunnistuspalvelun tarjoajan tunnistusvälineillä tehdä sähköisiä allekirjoituksia, ja millaisia nämä allekirjoitukset ovat.

Kyseessä ei ole lupa toiminnan aloittamiseen, vaan ainoastaan ilmoituksen tekeminen. Viestintävirasto selvittää tässä laissa säädettyjen edellytysten täyttymisen ennen kuin palveluntarjoaja ja sen tarjoamat palvelut merkitään 12 §:ssä tarkoitettuun rekisteriin. Palveluntarjoaja voi kuitenkin aloittaa palvelun tarjoamisen jo ennen rekisteriin tehtävää merkintää.

Mikäli ilmoituksessa ei ole annettu kaikkia 1-5 kohdissa tarkoitettuja tietoja tai ne ovat puutteelliset, Viestintäviraston on kehotettava ilmoituksen tekijää täydentämään ilmoitustaan. Ilmoitusvelvollisuuden tavoitteena on se, että valvovalla viranomaisella olisi selkeä tieto niistä palveluntarjoajista, jotka toimintaa Suomessa harjoittavat.

Ehdotetun 3 momentin mukaan tunnistuspalvelun tarjoajan on viipymättä ilmoitettava ehdotetussa 2 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista Viestintävirastolle. Myös tämän ilmoituksen on tapahduttava kirjallisesti. Lisäksi ilmoitus on tehtävä toiminnan lopettamisesta sekä toimintojen siirtymisestä toiselle palveluntarjoajalle.

Ehdotetun 4 momentin mukaan Viestintävirasto voi antaa valvontatoiminnan kannalta tarpeellisia teknisiä määräyksiä ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle. Määräykset, joita Viestintävirasto voisi ehdotetun

momentin nojalla antaa, ovat luonteeltaan teknisiä. Ehdotettu säännös on välttämätön sen johdosta, että kyseessä ovat teknisesti hyvin monimutkainen palveluiden tarjonta, joka kaiken lisäksi kehittyy jatkuvasti. Määräykset ovat tarpeen myös palveluntarjoajien edun kannalta, sillä muutoin niillä voi olla vaikeuksia tietää esimerkiksi sitä, kuinka tarkkoja teknisiä kuvauksia niiltä edellytetään. Sähköisistä allekirjoituksista annetun lain 9 §:n 1 momentti ja ehdotettu 32 §:n 1 momentti sisältävät vastaavat säännökset laatuvarmenteiden osalta.

Viestintävirasto on antanut voimassa olevan lain nojalla 29 päivänä tammikuuta 2003 säännöksen perusteella määräyksen yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle (7/2003 M). Lain voimaan tuloa koskevan 50 §:n 2 momentin mukaan Viestintäviraston sähköisistä allekirjoituksista annetun lain nojalla antamat määräykset ovat voimassa siihen saakka, kunnes uudet määräykset tämän lain nojalla on annettu.

11 §. *Muuhun Euroopan talousalueen jäsenvaltioon sijoittautunut tunnistuspalvelun tarjoaja.* Pykälässä todetaan, että muualle kuin Suomeen sijoittautunut palveluntarjoaja voi tehdä 10 §:ssä pykälässä tarkoitetun ilmoituksen toiminnan aloittamisesta niin halutessaan. Säännös on tarpeen, jotta voidaan varmistaa palveluiden vapaa liikkuvuus Euroopan talousalueella. Palveludirektiivin 16 artiklan mukaan jäsenvaltioiden on kunnioitettava palveluntarjoajien oikeutta tarjota palvelujaan muussa jäsenvaltiossa kuin siinä, johon ne ovat sijoittautuneet. Jäsenvaltiot eivät myöskään saa asettaa palvelutoiminnan aloittamisen tai harjoittamisen ehdoksi alueellaan vaatimuksia, jotka ovat syrjiviä.

Palveludirektiivin VI luvussa säädetään jäsenvaltioiden välisestä hallinnollisesta yhteistyöstä. Luvun 29 artiklan 1 kohdan mukaan sijoittautumisvaltion muun muassa on toimitettava tietoja alueelleen sijoittautuneista palveluntarjoajista toisen jäsenvaltion niitä pyytäessä, kun kyse on toisessa jäsenvaltiossa palveluja tarjoavasta palveluntarjoajasta. Artiklan 2 kohdan mukaan sijoittautumisjäsenvaltion on suoritettava toisen jäsenvaltion pyytämiä tarkistuksia, tarkastuksia ja tutkimuksia sekä annettava tälle tiedot niiden tuloksista ja mahdollisesti toteutetuista toimenpiteistä.

12 §. *Tunnistuspalvelun tarjoajia koskeva rekisteri.* Pykälän 1 momentin mukaan Viestintävirasto ylläpitää julkista rekisteriä 10 §:n mukaisen ilmoituksen tehneistä tunnistuspalvelun tarjoajista. Käytännössä rekisteri on parhaiten löydettävissä Viestintäviraston internetsivuilta. Rekisterin olemassa olo on yksi ajatellun järjestelyn kulmakivistä. Sekä tunnistusvälinettä hankkiva, usein kuluttajan ominaisuudessa toimiva henkilö että tunnistuspalvelua hankkiva palveluntarjoaja joutuvat ratkaisemaan kysymyksen siitä, mihin tunnistuspalvelun tarjoajaan ne voivat luottaa. Viestintäviraston internetsivustolla julkaistava julkinen rekisteri antaa helpolla tavalla tiedon niistä palveluntarjoajista, joiden voidaan lähtökohtaisesti odottaa noudattavan tämän lain säännöksiä, ja jotka ovat viranomaisen valvonnassa. Rekisterin tiedoilla on kuitenkin ainoastaan informatiivinen tehtävä.

Pykälän 2 momentissa säädetään Viestintäviraston velvollisuudesta kieltää palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena, jos palvelu tai palveluntarjoaja ei täytä tässä luvussa asetettuja vaatimuksia. Viestintäviraston tehtävänä on tarkastaa, että palveluntarjoaja ja sen palvelu vastaavat 10 §:n mukaisessa ilmoituksessa kerrotun perusteella tässä laissa ja etenkin sen 3 luvussa asetettuja edellytyksiä. Rekisterimerkinnät voidaan tehdä vasta tämän jälkeen. Kyseessä on valvovan viranomaisen kannalta kaikista eniten työtä aiheuttava vaihe. Tämän johdosta palveluntarjoajan on maksettava Viestintävirastolle 47 §:n 1 momentissa tarkoitettu rekisteröimismaksu.

Lisäksi 2 momentissa todetaan, että Viestintävirasto voi asettaa palveluntarjoajalle määräajan, jonka kuluessa se voi korjata palvelussa tai palveluntarjoajassa havaitun puutteellisuuden, jos puutteellisuutta voidaan pitää ainoastaan vähäisenä. Viestintäviraston on luonnollisesti toiminnassaan otettava huomioon hallintolain (434/2003) säännökset. Jos kysymys on esimerkiksi ilmoituksen puutteellisuudesta, Viestintäviraston on kehotettava palveluntarjoajaa täydentämään asiakirjaa hallintolain 22 §:n 1 momentin mukaisesti.

Pykälässä säädettyä menettelyä ei ole pidettävä palveludirektiivissä tarkoitettuna lupamenettelynä, sillä palveluntarjoaja voi aloittaa palvelun tarjoamisen heti ilmoituksen tehtyvään, ja Viestintäviraston mahdollisuus puuttua asiaan on jälkikäteistä. Säännökset eivät myöskään estä palveluntarjoajaa tarjoamasta palveluaan ylipäätään. Mikäli lain edellytykset eivät täyty, palveluntarjoaja ei saa tarjota palveluaan vahvana sähköisenä tunnistamisena, mutta palveluntarjonta muunlaisena sähköisenä tunnistamisena ei ole estetty. Asia on säännelty vastaavalla tavalla myös laatuvarmenteiden tarjoamisen osalta 32 §:ssä.

13 §. *Tunnistuspalvelun tarjoajan yleiset velvollisuudet.* Pykälän 1 momentissa säädetään tunnistuspalveluntarjoajan henkilöstöön kohdistuvista vaatimuksista. Ehdotetun momentin mukaan tunnistuspalvelun tarjoajan on huolehdittava siitä, että sen palveluksessa olevalla henkilöstöllä on harjoitetun toiminnan laajuuteen nähden riittävät asiantuntemus, kokemus ja pätevyys. Asiantuntemuksella tarkoitetaan sekä teknistä että oikeudellista asiantuntemusta. Esimerkiksi henkilötietojen käsittelyyn liittyvät voimassa olevan lainsäädännön asettamat vaatimukset ovat huomattavat. Asiantuntemuksen, tarvittavan kokemuksen ja pätevyyden, kuten esimerkiksi koulutuksen vaatimukset määräytyvät kunkin henkilön kohdalla hänen hoitamiensa tehtävien mukaan. Suoraan sähköisen tunnistamisen kanssa tekemisissä olevilla on oltava riittävä asiantuntemus esimerkiksi sähköiseen tunnistamiseen liittyvistä teknisistä seikoista sekä tietoturvasta. Ehdotettu momentti vastaa sähköisistä allekirjoituksista annetun lain 10 §:n 2 momentin 1 kohtaa ja käsillä olevan esityksen 33 §:n 2 momentin 1 kohtaa.

Pykälän 2 momentin mukaan tunnistuspalvelun tarjoajalla on oltava riittävät taloudelliset voimavarat harjoitetun toiminnan laajuuteen nähden ja mahdollisen vahingonkorvausvastuun kattamiseksi. Palveluntarjoajan on arvioitava toimintansa tekniseen ja taloudelliseen turvallisuuteen liittyvät riskit, ja ryhdyttävä tarpeellisiin toimenpiteisiin riskien minimoimiseksi. Riittävät taloudelliset voimavarat edellyttävät palveluntarjoajan taloudelta sitä, että taseessa on riittävästi varoja kattamaan riskit. Palveluntarjoaja voi myös varautua mahdollisiin vahingonkorvausvastuisiin vapaaehtoisin vakuutuksin. Ehdotettu 2 momentin alkuosa vastaa sähköisistä allekirjoituksista annetun lain 10 §:n 2 momentin 2 kohtaa ja käsillä olevan esityksen 33 §:n 2 momentin 2 kohtaa.

Pykälän 3 momentti sisältää vaatimukset tunnistuspalvelun tarjoajan palvelun tietoturvasta ja henkilötietolain 32 §:ssä tarkoitetusta tietojen suojaamisesta. Ehdotetun momentin mukaisella palvelujen tietoturvalla tarkoitetaan toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi.

Palvelujen tietoturvalla käsitetään ehdotetussa momentissa samaa kuin sähköisen viestinnän tietosuojalain (516/2004) 19 §:n 1 momentissa. Toiminnan turvallisuudella tarkoitetaan siten muun muassa sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan. Lisäksi toiminnan turvallisuudella tarkoitetaan sitä, että pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan.

Tietoliikenneturvallisuudella tarkoitetaan muun muassa sitä, että viestintäverkoissa välitettävät tunnistamiseen liittyvät viestit eivät paljastu asiaankuulumattomille ja asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä.

Laitteistoturvallisuudella ja ohjelmistoturvallisuudella tarkoitetaan muun muassa sitä, että käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys.

Tietoaineistoturvallisuudella tarkoitetaan muun muassa sitä, että järjestetään tietoai-

neistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti, järjestetään tietoaineistojen varmuuskopiointi ja turvallinen säilytys sekä suojataan tärkeät asiakirjat, tietovarastot ja yksittäiset tiedot.

Näiden toimien on oltava riittäviä eli ne on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. Tällä tarkoitetaan sitä, että täydellistä tietoturvaa ei yleisesti ottaen ole mahdollista saada aikaan ainakaan ilman kohtuuttomia kustannuksia. Tietoturvan tasoon kohdistuvat vaatimukset saattavat vaihdella tarjottavista palveluista johtuen. Jos palveluntarjoaja esimerkiksi tarjoaa biometristen tunnisteiden käyttöön perustuvaa vahvaa sähköistä tunnistuspalvelua, kohdistuu tällaiseen toimintaan korostettu turvallisuusvaatimus. Samoin eroa saattaa olla siinä, tarjoaako palveluntarjoaja tunnistuspalvelua sitä käyttäville palveluntarjoajille vai laskeeko se ainoastaan liikkeelle tunnistusvälineitä. Jälkimmäisessä tapauksessa palveluntarjoajalla ei esimerkiksi ole hallussaan 24 §:n 1 momentin 1 kohdassa tarkoitettuja tietoja, joita täytyisi suojata.

Tietojen suojaamista koskevan henkilötietolain 32 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Ehdotetun 4 momentin mukaan palveluntarjoajan vastaa apunaan käyttämien henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta. Ehdotettu momentti koskee esimerkiksi alihankkijoita. On myös luonnollista, että tunnistuspalveluita tarjoava vastaa hänen palveluitaan käyttävien palveluntarjoajien ja välineen haltijoiden suuntaan sellaisista välineistä, jotka palveluntarjoaja on hankkinut ulkopuoliselta toimittajalta. Vastuu välineen valmistajan tai maahantuojan ja tunnistuspalvelun tarjoajan välillä perustuu näiden kahden välisiin sopimussuhteisiin. Ehdotettu säännös vastaa yleisiä oikeusperiaatteita. Se on kuitenkin haluttu ottaa nimenomaisesti ehdotukseen selvyyden vuoksi.

Ehdotetussa momentissa henkilöllä tarkoitetaan sekä luonnollisia henkilöitä että oikeushenkilöitä. Ehdotettu momentti vastaa pääosin sähköisistä allekirjoituksista annetun lain 10 §:n 1 momentin ja ehdotetun 33 §:n 1 momentin säännöstä.

14 §. *Tunnistusperiaatteet*. Pykälän 1 momentissa edellytetään, että tunnistuspalvelun tarjoajalla on oltava sen itsensä laatimat tunnistusperiaatteet. Näissä periaatteissa määritellään tarkemmin, kuinka palveluntarjoaja täyttää tässä laissa tarkoitetut velvollisuutensa. Erityisen tärkeää on määritellä tarkemmin, kuinka palveluntarjoaja toteuttaa 17 §:ssä tarkoitetun ensitunnistamisen.

Pykälän 2 momentin mukaan tunnistusperiaatteissa on kuvattava tiedot palveluntarjoajasta, tarjottavista palveluista, palveluntarjoajan tärkeimmistä yhteistyökumppaneista, ulkopuolisten arviointilaitosten suorittamista tarkastuksista sekä muut merkitykselliset tiedot, joiden perusteella palveluntarjoajan toimintaa ja luotettavuutta voidaan arvioida.

Tunnistusperiaatteet ovat olennainen väline palveluntarjoajan ja sen tarjoamien palveluiden luotettavuuden arvioinnissa. Tunnistuspalvelun tarjoajan oman edun mukaista on siksi laatia tunnistusperiaatteensa mahdollisimman kattaviksi. Samalla on kuitenkin selvää, ettei palveluntarjoajan tarvitse tunnistusperiaatteissa paljastaa mitään, mikä kuuluu liikesalaisuuksien piiriin.

Tieto palveluntarjoajan tärkeimmistä yhteistyökumppaneista liittyy erityisesti mahdollisesti tulevaisuudessa odotettavissa olevaan markkinoiden kehitysvaiheeseen, jossa palveluntarjoajat saattavat muodostaa erilaisia avoimia yhteistyöjärjestelyitä. Myös tiedot alihankkijoista on syytä antaa, ellei tämä tieto kuulu liikesalaisuuksien piiriin.

Pykälän 3 momentissa edellytetään, että tunnistuspalvelun tarjoaja antaa tunnistusperiaatteissa tiedon myös sähköisistä allekirjoituksista, jos se tarjoaa niitä vahvaan sähköiseen tunnistuspalveluunsa liittyen. Tieto on annettava sähköisten allekirjoitusten toteuttamismenetelmästä, tasosta ja turvallisuustekijöistä. Toteuttamismenetelmässä kysymys

on teknisestä toteuttamistavasta, kuten esimerkiksi siitä, perustuuko palvelu varmenteiden käyttöön. Tasossa on lähinnä kysymys siitä, onko allekirjoitusta pidettävä kehittyneenä sähköisenä allekirjoituksena. Turvallisuustekijöiden avulla voidaan vastata esimerkiksi kysymykseen siitä, voidaanko ja miltä osin allekirjoitusmenetelmän katsoa täyttävän turvalliselle allekirjoituksen luomisvälineelle asetetut edellytykset.

Pykälän 4 momentin mukaan tunnistuspalvelun tarjoajan on pidettävä tunnistusperiaatteensa jatkuvasti ajan tasalla. Tunnistusperiaatteet on myös pidettävä yleisesti saatavilla. Ehdotettu säännös perustuu nimenomaisesti saatavilla pitämiseen, eli palveluntarjoajalla ei ole aktiivista tiedonantovelvoitetta sisäisistä säännöistään. Saatavilla pitäminen voidaan täyttää esimerkiksi internetin avulla palveluntarjoajan kotisivuilla. Varsinainen selon ottaminen periaatteista jää jokaisen oman aktiivisuuden varaan.

15 §. *Tunnistuspalvelun tarjoajan tiedonantovelvollisuus ennen sopimuksen tekemistä.* Pykälän 1 momentissa säädetään seikoista, joista tunnistuspalvelun tarjoajan on annettava tieto ennen sopimuksen tekemistä tunnistusvälineen hakijalle. Tiedot on annettava tunnistuspalvelun tarjoajasta, tarjottavista palveluista ja niiden hinnoista, 14 §:ssä tarkoitetuista tunnistusperiaatteista, osapuolten oikeuksista ja velvollisuuksista, mahdollisista vastuunrajoituksista sekä valitus- ja riitojenratkaisumenettelyistä. Lisäksi tiedot on annettava tunnistusvälineen käyttöehdoista, mukaan lukien tiedot mahdollisista 18 §:ssä tarkoitetuista käyttörajoituksista.

Tiedot palveluntarjoajasta ja tarjottavasta palvelusta on annettava yleisellä tasolla. Tunnistusperiaatteiden osalta tieto on annettava periaatteiden olemassa olosta ja siitä, mistä ne vaivatta löytyvät. Ehdotettu pykälä ei siis edellytä tiedon antamista tunnistusperiaatteiden sisällöstä. Tunnistusperiaatteet sisältävät myös tarkemmat tiedot palveluntarjoajasta ja tarjottavasta palvelusta. Ehdotetun tiedonantopykälän nojalla tiedonannossa on kuitenkin kiinnitettävä erityistä huomiota siihen, että tunnistusvälineen hakija saa tiedot välineen käyttöehdoista, mahdollisista vastuunrajoituksista ja mahdollisista käyttörajoituksista.

Viittauksella osapuolten oikeuksiin ja velvollisuuksiin tarkoitetaan erityisesti 21 §:ää, jossa säädetään tunnistusvälineen luovuttamisesta haltijalle, 23 §:ää, jossa säädetään tunnistusvälineen haltijan velvollisuuksista, 25 ja 26 §:iä, joissa säädetään tunnistusvälineen peruuttamisesta tai käytön estämisestä sekä 27 §:ää, jossa säädetään tunnistusvälineen haltijan vastuusta välineen oikeudettomasta käytöstä.

Viranomaisvalvonnan sekä valitusmenettelyjen osalta tieto on annettava Viestintäviraston ja tietosuojavaltuutetun tunnistuspalvelun tarjoajaan 5 luvun mukaisesti kohdistamasta valvonnasta sekä hakijan tai haltijan oikeudesta saattaa Viestintäviraston tutkittavaksi ehdotetun lain mukainen palveluntarjoajan toimintaa koskeva asia.

Yleisesti ottaen ehdotetussa momentissa tarkoitetut seikat sisältyvät palveluntarjoajan yleisiin sopimusehtoihin. Tiedon antaminen ehdotetussa pykälässä edellyttää kuitenkin palveluntarjoajalta aktiivisia toimenpiteitä. Tilanne on siten toinen kuin edellisessä pykälässä tarkoitettujen tunnistusperiaatteiden kohdalla, sillä niiden osalta edellytetään ainoastaan saatavilla pitämistä.

Sähköisistä allekirjoituksista annetun lain 12 §:n 2 momenttiin sisältyy laatuvarmenteiden tarjoajiin kohdistuva tiedonantovelvoitetta koskeva säännös. Sen piiriin kuuluvat asiat ovat osittain samoja kuin ehdotetussa momentissa. Voimassa olevan lain 12 §:n 2 momenttia vastaava säännös sisältyy ehdotetun 35 §:n 2 momenttiin.

Pykälän 2 momentin mukaan tiedot on annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voi tallentaa ja toisintaa ne muuttumattomina. Jos sopimus tehdään tunnistusvälineen hakijan pyynnöstä sellaista etäviestintä käyttäen, että tietoja ja sopimusehtoja ei voida antaa edellä tarkoitetulla tavalla ennen sopimuksen tekemistä, tiedot on annettava sanotulla tavalla viipymättä sopimuksen tekemisen jälkeen. Tiedot voidaan siten toimittaa esimerkiksi sähköpostin liitteenä PDF-tiedostona. Säännös vastaa kuluttajansuojalain (38/1978) 6 a luvun 11 §:n säännöstä.

Pykälän 2 momentissa todetaan, että henkilötietojen käsittelyä koskevasta tiedonantovelvollisuudesta säädetään henkilötietolaissa.

Säännös, johon erityisesti viitataan, sisältyy henkilötietolain 24 §:ään. Sen 1 momentin mukaan rekisterinpitäjän on henkilötietoja kerätessään huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan, samoin kuin ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä. Tiedot on annettava henkilötietoja kerättäessä ja talletettaessa tai, jos tiedot hankitaan muualta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kun tietoja ensi kerran luovutetaan.

Ehdotetussa 6 §:ssä säädetään henkilötietojen käsittelystä. Tässä pykälässä tarkoitettu tiedonantovelvollisuus on siis täytettävä ennen kuin henkilötietoja aletaan käsitellä.

16 §. *Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa tietoturvaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä.* Pykälässä tarkoitettu velvollisuus ilmoittaa tietoturvaan ja tietojen suojaamiseen kohdistuvista uhkista ja häiriöistä kohdistuu sopimuksen voimassaoloaikaan erotuksena edellisestä pykälästä, jossa tiedonantovelvollisuus kohdistuu aikaan ennen sopimuksen tekemistä.

Pykälän 1 momentin mukainen velvollisuus ilmoittaa edellyttää sitä, että tunnistuspalvelun tarjoaja ilmoittaa palvelua käyttäville palveluntarjoajille, tunnistusvälineen haltijoille sekä Viestintävirastolle palvelun tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä. Myös tietosuojavaltuutetulle on 2 momentin mukaan ilmoitettava, mikäli uhka tai häiriö kohdistuu henkilötietolain 32 §:ssä tarkoitettuun tietojen suojaamiseen. Pykälän 3 momentin mukaan palveluntarjoajan on samalla kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.

Sähköisen viestinnän tietosuojalain 21 § sisältää vastaavantapaisen säännöksen, joka kuitenkin on huomattavasti yksityiskohtaisempi. Ilmoittamisella tunnistuspalvelua käyttäville palveluntarjoajille ja tunnistusvälineiden haltijoille pyritään estämään vahinkojen syntyminen tai paheneminen. Esimerkiksi erilaisissa huijausyrityksissä saattaa olla tärkeää, että olemassa on yleinen tietoisuus meneillään olevasta huijauspyrkimyksestä. Mikäli kyse on teknisestä tietoturvasta, välineiden haltijat voivat pidättyä välineen käytöstä, kunnes vika on korjattu. Kaiken kaikkiaan pyrkimyksenä on estää tai minimoida mahdollisesti aiheutuvat vahingot.

Säännös ei sisällä yksityiskohtaisia ohjeita ilmoittamisesta tai esimerkiksi niistä tavoista, joilla ilmoittaminen voidaan tehdä. Tämä tarkoittaa sitä, että palveluntarjoajan tehtävänä on harkita kulloinkin tehokas ilmoittamistapa. Tapauksesta riippuen ilmoitus voidaan antaa esimerkiksi internetin kautta tai tiedotusvälineiden välityksellä. Joskus myös henkilökohtainen yhteydenotto voi olla tehokkain. Säännös lähtee siitä, että palveluntarjoajan oman edun mukaista on estää tai minimoida vahingot.

Säännös ei sisällä myöskään vaatimusta välittömästä ilmoittamisesta, koska toisinaan voi olla parempi ensin pyrkiä korjaamaan esimerkiksi palveluntarjoajan tiedossa oleva vaan ei yleisesti tiedossa oleva tietoturvaaukko. Harkinta tiedottamisen ajankohdasta jää siis tunnistuspalvelun tarjoajan tehtäväksi.

Viestintävirastolle ja henkilötietojen kyseessä ollen tietosuojavaltuutetulle tehtävien ilmoitusten tarkoituksena on, että valvovat viranomaiset olisivat tietoisia säännöksessä tarkoitetuista uhista ja häiriöistä. Viranomaiset voivat muun muassa tarvittaessa osallistua tiedottamiseen, jotta tieto leviäisi mahdollisimman nopeasti silloin, kun tämänkaltainen toiminta estäisi vahinkoja syntymästä.

17 §. *Tunnistusvälineen hakijan ensitunnistaminen.* Ehdotettuun pykälään sisältyy koko ehdotetun sääntelyn kenties keskeisin säännös. Pykälän 1 momentin mukaan tunnistuspalvelun tarjoajan on tunnistettava tunnistusvälineen hakija huolellisesti. Säännöksessä ensitunnistamisessa käytettäväksi sallittujen asiakirjojen määrä on rajallinen. Henkilöllisyys on todettava voimassa olevasta Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista. Euroopan talousalueen jäsenvaltion viranomaisen myöntämän passin ja henkilökortin sisällyttäminen

säännökseen johtuu siitä, että alueella on olemassa harmonisoidut säännökset passeista ja henkilökorteista. Jos niitä ei hyväksyttäisi ensitunnistamisessa, merkitsisi se estettä sisämarkkinoilla. Myös Sveitsin ja San Marinon kanssa on olemassa sopimukset vastavuoroisesta tunnustamisesta.

Halutessaan tunnistuspalvelun tarjoaja voi käyttää ensitunnistamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia. Velvollisuutta hyväksyä muiden valtioiden passeja ei ole, ja palveluntarjoaja voi valita ne valtiot, joiden viranomaisten myöntämät passit se katsoo voivansa hyväksyä. On selvää, että riskien määrä kasvaa tällaisten passien osalta. Palveluntarjoajan on arvioitava nämä riskit, jotka hän ottaa kantaakseen.

Tunnistuspalvelun tarjoajan kannalta säännös tarkoittaa sitä, että palveluntarjoajan on mahdollista kouluttaa henkilökuntansa tunnistamaan ehdotetussa momentissa luetellut asiakirjat. Jos palveluntarjoaja käyttää hyväkseen mahdollisuutta hyväksyä 1 momentin loppuosassa mainittuja muiden valtioiden viranomaisten myöntämiä passeja, sen on selkeästi määriteltävä, minkä valtioiden passit se hyväksyy. Nämä on myös mainittava palveluntarjoajan tunnistusperiaatteissa. Lisäksi palveluntarjoajan on varmistettava, että asiasta on annettu henkilökunnalle selkeät ja ristiriidattomat ohjeet, ja että henkilökunta myös koulutetaan tunnistamaan asiakirjat riittävällä varmuudella.

Ehdotetussa pykälässä, sen paremmin kuin muissakaan esityksen säännöksissä ei ole erikseen mainintaa mahdollisuudesta käyttää asiamiestä. Koska asiamiehen käyttöä ensitunnistamisessa ei erikseen ole kielletty, tarkoittaa se sitä, että asiamiehen käyttö on sallittua. Tunnistuspalvelun tarjoaja vastaa myös tältä osin apunaan käyttämiensä tahojen toiminnasta siten kuin ehdotetun 13 §:n 4 momentissa todetaan.

Pykälän 1 momentin mukaan ensitunnistamisen on tapahduttava henkilökohtaisesti. Ehdotetun 2 momentin mukaan ensitunnistamisen henkilökohtaisuudesta voidaan poiketa, jos tunnistuspalvelun tarjoajat ovat tehneet keskenään sopimuksen mahdollisuudesta luottaa toistensa tekemään tunnistukseen. Tunnistuspalvelun tarjoajilla ei ole oikeutta käyttää hyväkseen toisen myöntämää tunnistetta ilman keskinäistä sopimusta. Tunnistuspalvelun tarjoajan elinkeinonvapauteen on katsottava kuuluvaksi oikeus päättää asiasta, eli olemassa ei voi olla vapaata oikeutta hyödyntää toisen palveluntarjoajan tekemää ensitunnistamista. Keskinäisyys ei tarkoita sitä, että sopimuksen olisi välttämättä oltava kaksisuuntainen, vaan palveluntarjoajat voivat sopia myös siten, että ainoastaan toinen luottaa toisen liikkeelle laskemaan tunnistusvälineeseen ensitunnistamisessaan. Sen sijaan sopimuksen keskinäisyys estää mahdollisuuden ketjuttamiseen ilman, että alkuperäisen ensitunnistamisen suorittanut tunnistuspalveluntarjoaja on aina mukana sopimusjärjestelyissä.

Palveluntarjoajien on sopimuksessaan määriteltävä se, kuinka vastuu mahdollisesta alkuperäisen ensitunnistamisen virheellisyydestä niiden välillä jakautuu. Suhteessa vahingonkärsineeseen vastaa se tunnistuspalvelun tarjoaja, joka luottaa toisen tekemään ensitunnistamiseen. Jälkimmäinen säännös on looginen sen johdosta, että usein tunnistusvälineen haltija on samalla kuluttaja. Se ei siis kuitenkaan ratkaise kysymystä palveluntarjoajien välisestä regressioikeudesta.

Tunnistusvälineen liikkeelle laskeminen toisen palveluntarjoajan tekemään ensitunnistamiseen luottaen edellyttää lähtökohtaisesti sähköistä prosessia. Pykälän 3 momentin mukaan vastaavalla tavalla sähköisen prosessin avulla voidaan tunnistusvälinettä hakea myös sellaisessa tapauksessa, että tunnistuspalvelun tarjoajalla ja välineen haltijalla on jo olemassa oleva asiakassuhde. Kyse voi olla esimerkiksi siitä, että 20 §:ssä tarkoitettu sopimus ja tunnistusväline on voimassa määräaikaisesti, ja välineen haltija haluaisi jatkaa asiakassuhdetta. Ensitunnistamista ei tarvitse tällaisessa tapauksessa tehdä uudestaan.

Pykälän 4 momentissa todetaan, että jos tunnistusvälinettä hankkivan henkilön henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen suorittaa poliisi. Kyseessä voisi ensinnäkin olla tilanne, jossa haltijalla ei ole mitään ehdotetussa 1 momentissa tarkoitetuista asiakirjoista. Toiseksi kyseessä voisi olla tilanne, jossa henkilöllä olisi kyllä esittää tällainen asiakirja, mutta tunnistuspalveluntarjoajan asiakas-

palvelu ei silti voisi saada riittävää varmuutta, että asiakirja todella kuuluu sen esittävälle henkilölle. Tällainen tilanne voisi esimerkiksi olla kyseessä silloin, kun henkilö esittäisi hyvin vanhan asiakirjan. Jatkossa passien voimassa olo tulee rajoittumaan viiteen vuoteen, joten tämäntyyppiset tilanteet tullevat sen mukana vähenemään. Kolmantena esimerkkinä olisi tilanne, jossa asiakirjaa olisi syytä epäillä väärennetyksi.

Poliisi ilmoittaa lopputuloksen tunnistuspalveluntarjoajalle. Poliisi pystyy suorittamaan tunnistamisen luotettavasti myös esimerkiksi ETA-alueen ulkopuolisten maiden passeista, sillä poliisilla on erityistä tällaista tietotaitoa omaavaa henkilökuntaa. Lisäksi poliisilla on olemassa mahdollisuus käyttää erilaisia tietokantoja henkilöllisyyden varmistamiseksi. Kyseessä on poliisin palvelu, josta maksu määräytyy julkisoikeudellisena suoritteena valtion maksuperustelain mukaan. Maksu peritään sellaisenaan tunnistusvälineen hakijalta.

18 §. *Oikeustoimen tekemiseen kohdistuvat estot ja rajoitukset.* Ehdotetun pykälän 1 momentin mukaan osapuolten välisillä sopimuksilla voidaan tunnistusvälineen käyttäminen oikeustoimien tekemiseen estää, tai oikeustoimien tekemiselle voidaan asettaa sekä käyttötarkoitukseen että tapahtumien rahamääräiseen arvoon liittyviä rajoituksia.

Sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi sisältää laatuvarmenteiden osalta vastaavan sääntelyn 6 artiklan 4 kohdassa. Sähköisistä allekirjoituksista annetussa laissa käyttörajoitukset mainitaan 7 §:n 2 momentin 8 kohdassa, samoin tämän lain 30 §:n 2 momentin 8 kohdassa.

Ehdotetusta momentista käy ilmi, että rajoitukset voivat kohdistua niihin käyttötarkoituksiin, joihin tunnistusvälinettä voi käyttää, Esimerkiksi tehtävien oikeustoimien laatua voidaan rajoittaa. Rajoitukset voivat olla myös euromääräisiä. Mikään ei myöskään estä asettamasta molempia rajoituksia tunnistusvälineeseen.

Rajoitukset eivät voi olla tehokkaita, jos tunnistusvälineeseen luottavat tahot eivät voi saada niitä tietoonsa. Siksi rajoitusten asettamiseen liittyy 2 momentin vaatimus siitä, että tunnistuspalvelun tarjoajan on huolehdittava siitä, että estot tai rajoitukset ovat kaikkien osapuolten tiedossa tai havaittavissa helpolla tavalla. Tämä ei kuitenkaan ole tarpeen, jos tunnistusväline on sellainen, että estojen tai rajoitusten vastainen käyttö on teknisesti estetty. Osa tunnistusvälineistä saattaa olla sellaisia, että rajoitusten vastaiset toimet eivät yksinkertaisesti ole mahdollisia. Osassa välineistä tekniset estot eivät ehkä ole mahdollisia, vaan mahdolliset käyttörajoitukset on erikseen tarkastettava.

Ehdotetussa momentissa todetaan edelleen, että tunnistuspalvelun tarjoaja ei vastaa niistä toimista, jotka on tehty tällaisten estojen tai rajoitusten vastaisesti siitä huolimatta, että palveluntarjoaja on täyttänyt omat edellä mainitut velvoitteensa. Sääntely vastaa sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin ja sähköisistä allekirjoituksista annetun lain sääntelyä laatuvarmenteiden suhteen samoin kuin nyt ehdotettavaa 41 §:n 3 momenttia.

Pykälän 3 momentti sisältää säännöksen siitä, että tunnistuspalvelun tarjoajan on järjestettävä mahdollisuus tarvittaessa tarkastaa tunnistusvälineeseen liittyvät estot tai rajoitukset ympäri vuorokauden. Tarkastamismahdollisuutta ei tarvita silloin, jos välineen käyttö estojen tai rajoitusten vastaisesti on teknisesti estetty.

Pykälän 4 momentin mukaan tunnistuspalvelua käyttävän palveluntarjoajan on tarvittaessa tarkastettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset estot tai käyttörajoitukset tunnistusvälineen käytön yhteydessä. Tarvetta tarkastukseen ei ole silloin, jos tunnistusvälineen käyttö vastoin käyttörajoitusta on järjestetty teknisin estoin. Muutoin asia on aina tarkastettava.

Palveluntarjoajan velvollisuuden kääntöpuolella on ehdotetussa 23 §:ssä mainittu tunnistusvälineen haltijan velvollisuus käyttää välinettä sopimusehtojen mukaisesti.

19 §. *Varmenteen tietosisältö.* Pykälä liittyy tietyllä teknologialla toteutettuun vahvaan sähköiseen tunnistamiseen. Vastaava pykälä sisältyy myös voimassa olevan sähköisistä allekirjoituksista annetun lain 7 §:n 2 momenttiin sekä ehdotettuun 30 §:ään, jotka koskevat laatuvarmennetta. Sanotut pykälät panevat täytäntöön sähköisiä allekirjoituksia

koskevista yhteisön puitteista annetun direktiivin liitteen 1.

Pykälän 1 momentissa säädetään tiedoista, jotka varmennepalvelun tarjoajan on ainakin sisällytettävä varmenteeseen. Säännös ei siis estä muidenkin tarpeellisten tietojen sisällyttämistä. Kyseessä ovat tiedot varmentajasta, varmenteen haltijasta ja haltijan yksilöivästä tunnuksesta, varmenteen voimassaoloajasta, varmenteen yksilöivästä tunnuksesta ja varmenteen mahdollisista käyttörajoituksista. Lisäksi varmenteen tulee sisältää varmenteen haltijan julkinen avain ja tieto sen käyttötarkoituksesta sekä varmentajan kehittynyt sähköinen allekirjoitus.

Tieto varmenteen haltijasta voi olla nimi tai salanimi, josta ilmenee, että se on salanimi. Kuten 8 §:n 2 momentissa todetaan, palvelu voidaan toteuttaa myös sillä tavoin, että tunnistuspalvelun tarjoaja ilmoittaa palvelua käyttävälle palveluntarjoajalle ainoastaan välineen haltijan salanimen tai rajoitetun määrän henkilötietoja. Varmenteen haltijan yksilöivä tunnus voi olla esimerkiksi sähköinen asiointitunnus. Se voi olla myös henkilötunnus, jos 6 §:n 3 momentin edellytykset täyttyvät. Henkilötunnus saa siten tulla ainoastaan varmenteeseen luottavan tahon tietoon, eikä se saa olla saatavissa julkisesta hakemistosta.

Sähköistä asiointitunnusta ei ole tähän saakka luovutettu varmennepalvelun tarjoajille. Eduskunnassa on parhaillaan käsiteltävänä laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista kuitenkin tullee muuttamaan tämän tilanteen. Sanotun lain 43 §:n 2 momentin 2 kohdan mukaan sähköinen asiointitunnus voidaan luovuttaa Suomeen sijoittautuneelle varmentajalle, joka käyttää sähköistä asiointitunnusta varmenteessa varmenteen haltijan yksilöivänä tunnistetietona.

Ehdotettu 3 kohta ei estä sitä, että tunnistuspalveluntarjoaja voi käyttää myös jotakin muuta, esimerkiksi omia järjestelmiään varten luomaansa yksilöivää tunnistetta.

Varmenteen voimassaoloajalla tarkoitetaan sekä voimassaolon alkamis- että päättymisajankohtia. Varmenteen yksilöivä tunnus puolestaan voi olla juokseva sarjanumero tai muu yksilöllinen merkkijono.

Varmenteen tietosisällöstä on käytävä ilmi mahdolliset käyttörajoitukset. Tällä viitataan erityisesti 18 §:ssä tarkoitettuihin rajoituksiin, jotka voivat liittyä joko käyttötarkoitukseen tai euromääriin tai molempiin. Lisäksi varmenteen tulee sisältää varmenteen haltijan julkinen avain ja sen käyttötarkoitus sekä varmentajan kehittynyt sähköinen allekirjoitus.

Pykälän 1 momentissa säädetään siis tiedoista, jotka ainakin on sisällytettävä varmenteeseen. Säännös ei siis toisin sanoen estä sisällyttämästä muista tarpeellisia tietoja. Tällaisia tietoja voivat olla esimerkiksi varmenteen haltijan roolitieto, tieto sovellettavasta varmennepolitiikasta ja tieto tunnistuspalvelun tarjoajan sijoittautumisvaltiosta.

Varmennepolitiikan tunniste (OID Object Identifier) on tieto, jonka avulla löytyy varmennepolitiikan kuvaava dokumentti. Tunnisteen lisäksi varmenteessa voi olla myös suoraan politiikan WEB URL. Varmennepolitiikasta löytyvät aina tiedot varmentajan sijoittautumisesta sekä muut yhteystiedot. Varmennepolitiikasta löytyy lisäksi muun muassa selvitys varmenteiden myöntämisen järjestelyistä.

Pykälän 2 momentin nojalla varmennepalvelun tarjoajan tulee omalta osaltaan varmistaa, että varmennetta sähköiseen tunnistamiseen käyttävällä palveluntarjoajalla on saatavillaan varmenteen tietosisältö. Tietosisältö voi esimerkiksi olla saatavilla joko suoraan varmenteesta itsestään tai varmennepalvelun tarjoajan ylläpitämästä varmennerekisteristä.

20 §. *Tunnistusvälineen liikkeelle laskeminen.* Pykälässä annetaan perussäännöt tunnistuspalvelun tarjoajan ja välineen haltijan välisen sopimussuhteen sääntelemiseksi. Pykälän 1 momentissa todetaan, että tunnistusvälineen liikkeelle laskeminen perustuu välineen hakijan ja tunnistuspalveluntarjoajan väliseen sopimukseen. Lähtökohta lienee ilmeinen, mutta säännöksen kirjaamisella lakiin halutaan korostaa osapuolten itsemääräämisoikeutta. Säännöksen mukaan sopimus on tehtävä kirjallisesti. Tämä ei kuitenkaan estä sopimuksen tekemistä sähköisesti. Tällöin edellytetään, että sopimuksen sisältöä ei voida yksipuolisesti muuttaa ja että se säilyy osapuolten saatavilla.

Pykälän 2 momentin mukaan sopimus voi olla voimassa toistaiseksi tai määräaikaisesti. Tunnistusvälineellä voi olla oma voimassaoloaikansa, joka on lyhyempi kuin sopimuksen voimassaoloaika. Käytännössä tunnistusvälineitä voidaan joutua uusimaan sopimuksen voimassaoloaikana esimerkiksi sen johdosta, että niiden suoritusominaisuudet heikkenevät välinettä käytettäessä tai ajan kuluessa. Itsestään selvää on, että välineen voimassaolo päätetään sopimuksen päättyessä myös irtisanomis- tai purkamistapauksissa.

Pykälän 3 momentin mukaan tunnistusväline myönnetään luonnolliselle henkilölle. Välineen haltija voi kuitenkin edustaa toista luonnollista henkilöä tai oikeushenkilöä. Roolitiedon yhdistäminen henkilöön tapahtuisi erillisessä, joskin ehkä rinnakkaisessa prosessissa. Vahvan sähköisen tunnistamisen toimivuus edellyttää tältä osin jatkossa roolitietopalveluiden kehittymistä. Tällä hetkellä tällaisia palveluita on luotu verottajan tarpeisiin KATSO-yritystunnistuksessa. Lisäksi patentti- ja rekisterihallitus on kehittänyt roolitietopalvelua. Perusroolitiedon saaminen sekä siihen mahdollisesti liitettävä kaupallinen toiminta ovat erittäin tärkeitä sähköisen tunnistamisen kentän jatkokehityskohteita.

Pykälän 3 momentissa todetaan myös, että tunnistusvälineen on oltava henkilökohtainen. Tunnistamisen tarkoitus edellyttää, että tunnistustapahtuma voidaan kohdistaa varmuudella tiettyyn yhteen henkilöön. Vastaavasti ehdotetun 23 §:n 2 momenttiin tunnistusvälineen haltijan yhdeksi velvollisuudeksi on kirjattu se, ettei välinettä saa luovuttaa toisen käyttöön.

21 §. *Tunnistusvälineen luovuttaminen hakijalle.* Ehdotetussa pykälässä säädettäisiin tunnistusvälineen luovuttamisesta hakijalle, joka sen jälkeen on terminologisesti välineen haltija. Säännöksen taustalla on tavoite madaltaa kynnys tunnistusvälineen hankkimiseksi mahdollisimman alhaalle vaarantamatta kuitenkaan turvallisuutta.

Ehdotetun pykälän mukaan tunnistuspalvelun tarjoajan on luovutettava tunnistusväline hakijalle osapuolten sopimuksen mukaisesti siten, että olemassa ei ole vaaraa välineen tai sen käyttöön liittyvien yksilöivien tietojen joutumisesta oikeudettomasti toisen haltuun. Määritelmän mukaisesti tunnistusväline käsittää myös sen käyttöön mahdollisesti liittyvät yksilöivät tiedot. Ehdotettu säännös tarkoittaa hyvin pitkälle samantapaista järjestelyä kuin esimerkiksi luottokorttien suhteen.

Tunnistusvälineen hakijan on voitava päättää, ottaako hän välineen vastaan postitse vaiko ei, jos tunnistuspalvelun tarjoaja tarjoaa tällaisen mahdollisuuden. Palveluntarjoajan on huolehdittava siitä, että esimerkiksi PIN-koodia tai vastaavia välineen käyttöön tarvittavia tietoja ei toimiteta samassa lähetyksessä tai saman päivän postissa esimerkiksi kortin tai SIM-kortin kanssa, ja että välineen ja yksilöivien tietojen toimittaminen tapahtuu muutoin turvallisesti. Absoluuttista turvallisuutta ei kuitenkaan tältäkään osin voida tavoitella, minkä johdosta säännöksessä todetaan, että palveluntarjoajan on riittävällä tavalla varmistauduttava toimittamisen turvallisuudesta.

Tunnistuspalvelun tarjoaja kantaa riskin, joka aiheutuu tunnistusvälineen, mukaan lukien sen käyttöön liittyvät yksilöivät tiedot, lähettämisestä maksajalle. Vastuu siirtyy tunnistusvälineen haltijalle 23 §:n 1 momentin mukaan vasta, kun hän on vastaanottanut tunnistusvälineen. Palveluntarjoajalla on näyttövelvollisuus siitä, että tunnistusvälineen haltija on vastaanottanut välineen ja sen käyttöön mahdollisesti liittyvät yksilöivät tiedot.

22 §. *Tunnistusvälineen uusiminen.* Pykälässä säädetään tunnistusvälineen uusimisesta. Kuten 20 §:n 2 momentissa todetaan, tunnistusvälineellä voi olla oma voimassaoloaikansa, joka on lyhyempi kuin tunnistuspalvelun tarjoajan ja tunnistusvälineen haltijan välisen sopimuksen voimassaoloaika. Väline saatetaan joutua uusimaan aika ajoin, jotta sen moitteeton toiminta voidaan taata. Tunnistuspalvelun tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu väline on korvattava uudella. Oikeus on rajattu tähän nimenomaiseen tilanteeseen. Toimittamisessa noudatetaan 21 §:n säännöksiä. Oikeusministeriössä valmisteilla olevaan maksupalvelulakiin aiotaan ehdottaa sisällöltään vastaavaa säännöstä.

23 §. *Tunnistusvälineen haltijan velvollisuudet.* Pykälässä säädetään pääasiassa asioista, joita täytyy noudattaa yleensä sopimus-

suhteessa. Säännös on kuitenkin tarpeen selvyyden vuoksi.

Pykälän 1 momentin mukaan tunnistusvälineen haltijan on käytettävä välinettä sen myöntämistä ja käyttöä koskevien ehtojen mukaisesti. Erityisesti kyse on mahdollisista käyttötarkoitukseen tai euromääriin liittyvistä ehdotetussa 18 §:ssä tarkoitetuista käyttörajoituksista tai estoista.

Ehdotetun momentin mukaan välineen haltijan on myös säilytettävä väline huolellisesti. Kuten määritelmiä koskevan 2 §:n 2 kohdassa todetaan, tunnistusväline käsittää myös tunnistamiseen tarvittavat yksilöivät tiedot. Yksilöivillä tiedoilla tarkoitetaan esimerkiksi asiakastunnusta, PIN-koodia tai muuta tunnuslukua. Arvioitaessa sitä, millaisia varotoimia tunnistusvälineen haltijalta voidaan kohtuudella edellyttää, on otettava huomioon, että tavanomaiset tunnistusvälineet on yleensä tarkoitettu käytettäviksi usein ja että niitä on sen vuoksi voitava kuljettaa mukana. Tunnistusvälineen haltijalta edellytettäviin kohtuullisiin varotoimiin voidaan yleensä katsoa kuuluvan esimerkiksi sen, että hän säilyttää tunnistusvälinettä ja sen käyttöön liittyviä yksilöiviä tietoja erillään niin, ettei sivullinen voi yhdistää niitä toisiinsa. Tunnistusvälineen haltijalta ei kuitenkaan voida vaatia kohtuuttoman pitkälle meneviä turvajärjestelyjä. Esimerkiksi se, että tunnistusvälineen haltija säilyttää sekä tunnistusvälinettä että tunnuslukua kotonaan, ei vielä sinänsä merkitse sitä, että hän olisi laiminlyönyt huolellisuusvelvoitteensa. Huolellisena menettelynä voidaan yleensä pitää esimerkiksi sitä, että tunnistusvälinettä säilytetään lompakossa tai käsilaukussa ja tunnuslukua kotona lipaston laatikossa.

Varotoimien huolellisuutta arvioidaan kokonaisuutena. Kokonaisarvioinnissa on kiinnitettävä huomiota myös mahdollisiin erityisiin turvajärjestelyihin, joihin tunnistusvälineen haltija on ryhtynyt. Esimerkiksi tunnistusvälineen ja siihen liittyvän tunnusluvun säilyttäminen samassa kassakaapissa tai muussa vastaavassa paikassa, jossa sivulliset vain poikkeuksellisesti voivat päästä niihin käsiksi, ei välttämättä osoita huolimattomuutta.

Tunnistusvälineen haltijalta vaadittaviin kohtuullisiin varotoimiin kuuluu myös se, että hän seuraa välineen tallella oloa olosuhteiden edellyttämällä tavalla. Esimerkiksi tunnistusvälineen haltijan liikkuessa suurissa ihmisjoukoissa tai muissa paikoissa, joissa taskuvarkauksien riski on erityisen suuri, tarkistamisvelvollisuus on korostunut, koska ammattimaisesti suoritettua taskuvarkautta ei yleensä huomata sen tapahtuessa.

Jos tunnistusvälineen haltija laiminlyö momentin mukaisen huolehtimisvelvoitteensa, hän voi joutua vastuuseen maksuvälineen oikeudettomasta käytöstä 27 §:n mukaisesti.

Pykälän 2 momentti sisältää kiellon luovuttaa välinettä toisen käyttöön. Esimerkiksi pankki- tai luottokortin haltija saattaa luovuttaa perheensä jäsenelle kortin ja kertoa sen käyttöön liittyvän yksilöivän tiedon. Periaatteessa luottokorttiyhtiön kannalta asialla ei ole merkitystä niin kauan kuin laskut maksetaan ajallaan. Sen sijaan tunnistusvälineen osalta olennainen kysymys on juuri tiettyyn tunnistusvälineeseen liitettävän henkilön henkilöllisyys. Tämän johdosta myös tunnistusvälineen haltijoiden olisi miellettävä, että välinettä ei saa luovuttaa toisen käyttöön.

Ehdotettu pykälä vastaa sisällöltään varsin pitkälti EU:n maksupalveludirektiivin vaatimuksia, jotka Suomessa pannaan täytäntöön oikeusministeriössä valmisteilla olevalla maksupalvelulailla.

24 §. *Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö.* Pykälässä säädetään tiedoista, jotka ovat tarpeen esimerkiksi, jos joudutaan jälkikäteen selvittämään tunnistamistapahtumaan tai tunnistuspalvelua käyttävän palveluntarjoajan ja tunnistusvälineen haltijan välillä tehtyyn oikeustoimeen liittyviä seikkoja.

Pykälän 1 momentin mukaan tunnistuspalvelun tarjoajan on tallennettava yksittäisen tunnistustapahtuman todentamiseksi tarvittavat tiedot. Ehdotetussa 1 kohdassa tarkoitetuilla tunnistamistapahtumaan liittyvillä tiedoilla tarkoitetaan sitä, mitä tunnistuspalveluntarjoaja ilmoitti tunnistuksen yhteydessä tunnistuspalvelua käyttävälle palveluntarjoajalle, ja mihin seikkoihin tämä ilmoitus perustui. Lisäksi näihin tietoihin sisältyvät muun muassa kellonaika ja päivämäärä.

Lisäksi palveluntarjoajan on tallennettava tarvittavat tiedot 17 §:ssä tarkoitetusta hakijan ensitunnistamisesta sekä ensitunnistami-

sessa käytetystä asiakirjasta. Tarvittavat tiedot voivat olla esimerkiksi passin tai henkilökortin numero. Joissakin tilanteissa voi olla tarpeen säilyttää valokopio käytetystä asiakirjasta. Asian todentaminen jälkikäteen saattaa olla tarpeen, jos tunnistusväline on annettu väärälle henkilölle. Ehdotetussa 17 §:ssä tarkoitetun prosessin selvittäminen saattaa olla tarpeen muun muassa sen selvittämiseksi, mikä taho vastaa mahdollisesti aiheutuneista vahingoista, jos osoittautuu, että tunnistusväline on annettu väärälle henkilölle.

Edelleen palveluntarjoajan on tallennettava tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön mahdollisesti liittyvistä käyttörajoituksista, sekä varmenteen osalta 19 §:ssä tarkoitettu varmenteen tietosisältö.

Ehdotettu 3 kohdan säännös takaa sen, että mahdolliset ehdotetussa 18 §:ssä tarkoitetut käyttörajoitukset ovat selvitettävissä vielä jälkikäteenkin. Myös niiden osalta kyse lienee useimmiten vastuusuhteiden selvittämisestä.

Ehdotettua 4 kohtaa vastaava säännös sisältyy sähköisistä allekirjoituksista annetun lain 14 §:ään ja ehdotettuun 37 §:ään. Kyseisessä pykälässä tarkoitettuun varmennerekisteriin sisällytetään kuitenkin muitakin tietoja.

Pykälän 2 momentti sisältää säännöksen tallentamisajasta. Sen mukaan 1 kohdassa tarkoitetut tiedot on tallennettava 5 vuotta tunnistustapahtumasta. Kohdissa 2-4 tarkoitetut tiedot on puolestaan tallennettava viisi vuotta tunnistuspalvelun tarjoajan ja tunnistusvälineen haltijan välisen asiakassuhteen päättymisestä. Säännös vastaa kuluttajan suojaksi annetun säännöstön ja rahapesusäännöstön vaatimuksia. Samalla se merkitsee sitä, että tunnistuspalvelun tarjoajan on säilytettävä varsin suuri määrä tietoa. Joissakin tapauksissa tietojen säilyttäminen on luonnollisesti myös palveluntarjoajan omien etujen mukaista.

Vertailun vuoksi todettakoon tältä osin, että sähköisistä allekirjoituksista annetun lain mukaan varmennerekisterin tiedot on tallennettava 10 vuoden ajaksi. Ehdotetun 38 §:n mukaan sellainen laatuvarmentaja, joka tarjoaa myös tunnistuspalveluita, voisi säilyttää tässä pykälässä säädetystä huolimatta kaikkia varmennerekisterin tietoja 10 vuotta varmenteen voimassa olon päättymisestä.

Pykälän 3 momentin mukaan tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, ellei tallentaminen ole välttämätöntä 1 momentin 1 kohdan mukaisesti yksittäisen tunnistustapahtuman todentamiseksi. Säännöksen avulla pyritään vähentämään palveluntarjoajan järjestelmiin tallentuvan henkilötiedon määrää.

Pykälän 4 momentti sisältää tietojen käsittelyn tarkoitusta koskevan rajoituksen. Tunnistuspalvelun tarjoaja saa käsitellä tietoja omien tarpeidensa johdosta ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten sekä omien oikeuksiensa turvaamiseksi. Jälkimmäisessä tilanteessa on kyse riitatilanteesta. Tämän lisäksi tunnistuspalveluntarjoaja saa käsitellä tietoja, jos se saa käsittelyä koskevan pyynnön joko tunnistuspalvelua käyttävältä palveluntarjoajalta tai tunnistusvälineen haltijalta tai molemmilta. Tällöin kysymys lienee siitä, että näiden kahden välillä on epäselvyyttä jostakin tunnistamistapahtumasta ja siihen mahdollisesti liittyvästä oikeustoimesta.

Ehdotetun säännöksen mukaan tunnistuspalvelun tarjoajan on tallennettava tieto tunnistustapahtuman käsittelyn ajankohdasta, syystä ja käsittelijästä. Esimerkiksi sähköisen viestinnän tietosuojalain 15 § sisältää vastaavan säännöksen tunnistamistietojen käsittelyä koskevien tietojen tallentamisesta.

Pykälän 5 momentti koskee sellaista palveluntarjoajaa, joka ainoastaan laskee liikkeelle tunnistusvälineitä. Ehdotetun 1 momentin 1 kohdan mukainen tallennusvelvoite ei luonnollisestikaan koske tällaista palveluntarjoajaa, koska sillä ei ole kyseistä tietoa hallussaan. Pykälän 2 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tällöin välineen voimassaolon päättymisestä.

25 §. *Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus*. Pykälän 1 momentin mukaan tunnistusvälineen haltijan on ilmoitettava tunnistuspalvelun tarjoajalle tai tämän nimeämälle muulle taholle välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian. Palveluntarjoajan nimeämällä muulla taholla voidaan tarkoittaa esimerkiksi palveluntarjoajien yhteistä sulkupalvelua. Sitä, onko tun-

nistusvälineen haltija tehnyt ilmoituksen ilman aiheetonta viivytystä, arvioidaan tapauskohtaisesti olosuhteet huomioon ottaen. Ehdotetussa pykälässä ei säädetä katoamisilmoituksen tekemiselle määrättyä muotoa. Ilmoitusvelvollisuutensa laiminlyönyt tunnistusvälineen haltija voi joutua vastuuseen tunnistusvälineen oikeudettomasta käytöstä 27 §:n nojalla.

Pykälän 2 momentin mukaan tunnistuspalvelun tarjoajan on tarjottava mahdollisuus tehdä välineen peruuttamista tai käytön estämistä koskeva ilmoitus milloin tahansa. Palveluntarjoajan on viipymättä peruutettava väline tai estettävä sen käyttö saatuaan asiaa koskevan tiedon.

Ilmaisulla ”milloin tahansa” tarkoitetaan ehdotetussa momentissa sitä, että tunnistusvälineen haltijan tulee voida tehdä ilmoitus kaikkina vuoden päivinä ja kaikkina vuorokaudenaikoina. Palveluntarjoaja voi täyttää velvoitteensa esimerkiksi järjestämällä puhelinpäivystyksen, joka on jatkuvasti auki. Palveluntarjoajan on mitoitettava puhelinpäivystyksen tai vastaavan järjestelyn voimavarat siten, että tunnistusvälineen haltijalla on myös tosiasiallisesti aina mahdollisuus ilmoituksen tekemiseen eikä esimerkiksi puhelinpalvelun ruuhkautuminen estä tai viivästytä sitä.

Pykälän 3 momentissa säädetään, että järjestelmään on asianmukaisesti ja viipymättä merkittävä tieto peruuttamisen ajankohdasta. Tunnistusvälineen haltijalla on oikeus saada pyynnöstä todistus siitä, että hän on tehnyt 1 momentissa mainitun ilmoituksen. Ehdotettu säännös on seurausta siitä, että tunnistusvälineen haltijalla on näyttövelvollisuus siitä, että hän on tehnyt 1 momentissa tarkoitetun ilmoituksen. Tämä velvollisuus on helpompi täyttää ehdotetussa momentissa tarkoitetun todistuksen avulla.

Todistuksella tarkoitetaan säännöksessä mitä tahansa selvitystä, jonka avulla tunnistusvälineen haltija voi myöhemmin yksiselitteisesti ja luotettavasti osoittaa tehneensä ilmoituksen. Jos tunnistusvälineen haltija tahtoo saada todistuksen, hänen on pyydettävä sitä 18 kuukauden kuluessa ilmoituksen tekemisestä. Määräaikaa koskeva säännös ei tietenkään estä palveluntarjoajaa antamasta todistusta, vaikka sitä pyydettäisiin vasta myöhemmin.

Pykälän 4 momentissa asetetaan järjestelmälle vaatimus siitä, että tunnistuspalvelua käyttävä palveluntarjoaja voi tarvittaessa helposti tarkistaa siihen merkityt tiedot ympäri vuorokauden. Jos tunnistusväline on sellainen, että sen käyttö voidaan teknisin keinoin kokonaan estää tai väline sulkea, ei tarkistamismahdollisuuden järjestäminen ole tarpeen.

Pykälän 5 momentin mukaan tunnistuspalvelua käyttävän palveluntarjoajan on tarkistettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset tunnistusvälineen peruuttamista tai käytön estämistä koskevat tiedot tunnistusvälineen käytön yhteydessä. Tarvetta tarkistukseen ei ole silloin, jos tunnistusvälineen käyttö voidaan estää teknisin keinoin tai se voidaan sulkea. Muutoin asia on aina tarkistettava.

Jos tunnistuspalvelu perustuu varmenteisiin ja peruutettuja varmenteita koskevat tiedot annetaan sulkulistan avulla, saa varmennepalvelun tarjoaja 5 momentin nojalla tallentaa tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta. Vaihtoehtoisesti varmentaja voi tallentaa sulkulistan, mikä saattaa vähentää tallennettavan tiedon määrää. Sähköisistä allekirjoituksista annettu laki sisältää sähköisen allekirjoituksen osalta vastaavan säännöksen 21 §:ssä, samoin ehdotettu 39 §.

Ehdotettu pykälä vastaa sisällöltään varsin pitkälti EU:n maksupalveludirektiivin vaatimuksia, jotka Suomessa pannaan täytäntöön oikeusministeriössä valmisteilla olevalla maksupalvelulailla.

26 §. *Tunnistuspalvelun tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö.* Pykälä sisältää tunnistuspalvelun tarjoajan varsin voimakkaan mahdollisuuden puuttua tunnistusvälineen käyttöön. Ehdotettu säännös on kuitenkin perusteltu sen johdosta, että toisen henkilöllisyyden väärinkäytöllä voi olla yksilön kannalta varsin kohtalokkaat seuraukset. Tunnistuspalvelun tarjoajan oikeus peruuttaa väline tai estää sen käyttö on rajattu viiteen tilanteeseen.

Pykälän 1 momentin 1 kohdan mukaan tunnistuspalvelun tarjoajalla on oikeus peruuttaa tai estää tunnistusvälineen käyttö, jos

palveluntarjoajalla on syytä epäillä, että joku muu kuin se, jolle väline on myönnetty, käyttää sitä. Tällainen tilanne voi johtua siitä, että tunnistusvälineen haltija on luovuttanut välineen toisen käyttöön vastoin 23 §:n 2 momentin nimenomaista säännöstä. Kohdassa tarkoitettu tilanne voi kuitenkin olla mahdollinen myös siten, että tunnistusvälineen haltija ei itse ole tietoinen tilanteesta.

Momentin 2 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen on mahdollista myös silloin, jos tunnistuspalvelun tarjoaja havaitsee välineen sisältävän ilmeisen virheellisyyden. Kysymys on tällöin tunnistuspalvelun tarjoajan omasta virheestä, jota hän ei ole havainnut aikaisemmin.

Momentin 3 kohdan mukaan tunnistusväline voidaan peruuttaa tai sen käyttö estää, jos tunnistuspalvelun tarjoajalla on syytä epäillä, että välineen käytön turvallisuus on vaarantunut. Säännös kattaa sekä tilanteet, joissa turvallisuuden vaarantuminen koskee vain kyseistä tunnistusvälinettä, että tilanteet, joissa tunnistusvälineen käyttö on vaarantunut järjestelmään yleisesti liittyvistä syistä.

Momentin 4 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen olisi mahdollista silloin, jos välineen haltija käyttää välinettä olennaisesti sopimusehtojen vastaisella tavalla. Kysymys voisi olla esimerkiksi 18 §:n mukaan asetettujen estojen tai rajoitusten vastaisesta käytöstä. On kuitenkin huomattava, että rikkomuksen on oltava olennainen, jotta palveluntarjoaja voisi käyttää ehdotetussa pykälässä tarkoitettua oikeuttaan.

Momentin 5 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen on mahdollista myös silloin kun välineen haltija on kuollut. Koska tunnistusväline on 20 §:n 3 momentissa todetuin tavoin henkilökohtainen, on paikallaan, että tunnistuspalvelun tarjoaja voi ryhtyä toimiin estääkseen välineen käytön mahdollisuudet tällaisessa tapauksessa.

Pykälän 2 momentin mukaan tunnistuspalvelun tarjoajan on ilmoitettava välineen peruuttamisesta tai käytön estämisestä ja peruuttamisen tai käytön estämisen ajankohdasta sekä peruuttamiseen tai käytön estämiseen johtaneista syistä välineen haltijalle. Ilmoitus on syytä tehdä niin pian kuin mahdollista. Kuten ehdotettu 16 §, myöskään tämä säännös ei sisällä vaatimusta välittömästä ilmoittamisesta. Syynä tähän on se, että toisinaan voi olla parempi ensin pyrkiä korjaamaan esimerkiksi palveluntarjoajan tiedossa oleva vaan ei yleisesti tiedossa oleva tietoturvaaukko. Harkinta tiedottamisen ajankohdasta jää siis tunnistuspalvelun tarjoajan tehtäväksi. Joka tapauksessa on selvää, että sen velvollisuutena on pyrkiä mahdollisten vahinkojen minimoimiseen.

Pykälän 3 momentin mukaan tunnistuspalvelun tarjoajan on palautettava mahdollisuus käyttää välinettä tai annettava välineen haltijalle uusi väline viipymättä 1 momentin 2 ja 3 kohdissa tarkoitetun syyn poistumisen jälkeen. Kohtien 1 ja 4 osalta palveluntarjoajalla on vapaus omasta puolestaan harkita, jatkuuko sopimus välineen haltijan kanssa.

Ehdotettu pykälä vastaa sisällöltään varsin pitkälti EU:n maksupalveludirektiivin vaatimuksia, jotka Suomessa pannaan täytäntöön oikeusministeriössä valmisteilla olevalla maksupalvelulailla.

27 §. *Tunnistusvälineen haltijan vastuu välineen oikeudettomasta käytöstä.* Pykälässä säännellään tunnistusvälineen haltijan vastuusta tilanteessa, jossa toinen henkilö käyttää tai on käyttänyt tunnistusvälinettä oikeudettomasti. Pykälä tulee tyypillisesti sovellettavaksi silloin, kun tunnistusväline on kadonnut tai varastettu ja sen löytänyt tai anastanut henkilö onnistuu käyttämään sitä. On huomattava, että tunnistusvälineen väärinkäyttö on vaikeampaa kuin esimerkiksi tähän saakka on ollut erilaisten maksukorttien. Määritelmän mukaisesti tunnistusvälineen käyttöön liittyy aina vähintään kaksi elementtiä, joista toinen on usein PIN-koodi, kun taas maksukortteja on tähän saakka käytetty yleisesti käsin allekirjoittamalla.

Kuluttajansuojalain 7 luvun 19 §:ssä on nykyisin säännökset, jotka koskevat kuluttajan asemassa olevan tilinhaltijan vastuuta luottokortin tai muun tililuoton käyttöön oikeuttavan tunnisteen oikeudettomasta käytöstä. Vastaavia säännöksiä sisältyy myös muihin lakeihin, kuten viestintämarkkinalakiin. Jäljempänä selostetaan kunkin säännöksen osalta erikseen, miltä osin ehdotettu pykälä sisällöltään vastaa kuluttajansuojalain mainittua pykälää tai poikkeaa siitä. Ehdotettu py-

kälä vastaa sisällöltään pitkälti EU:n maksupalveludirektiivin vaatimuksia, jotka Suomessa pannaan täytäntöön oikeusministeriössä valmisteilla olevalla maksupalvelulailla. Ehdotettuun lakiin ei kuitenkaan ole sisällytetty maksupalveludirektiivistä peräisin olevaa maksupalveluita koskevaa säännöstä kuluttaja-välineenhaltijan 150 euron suuruisesta omavastuusta sen johdosta, että vahvan sähköisen tunnistuspalvelun tarjoamisessa on kyse aivan toisenlaisesti toimintaympäristöstä, johon kyseinen säännös ei ole tarkoitettu.

Säännös vastaa pääperiaatteiltaan myös ehdotetun 40 §:n säännöstä, joka koskee allekirjoittajan vastuuta luomistietojen oikeudettomasta käytöstä laatuvarmenteiden osalta. Käsillä oleva säännös on kuitenkin tarkempi, ja se on pyritty ilmaisemaan vastaavalla tavalla nykyisen lainkirjoitustavan mukaisesti kuin maksupalvelulakikin.

Pykälän 1 momentissa luetellaan tyhjentävästi ne tilanteet, joissa tunnistusvälineen haltija voi joutua vastuuseen tunnistusvälineen oikeudettomasta käytöstä. Momentin 1 kohdan mukaan välineen haltija voi joutua vastaamaan sellaisesta oikeudettomasta käytöstä, joka on seurausta siitä, että tunnistusvälineen haltija on luovuttanut välineen toiselle. Vastaava vastuuperuste sisältyy nykyisin kuluttajansuojalain 7 luvun 19 §:n 1 momentin 1 kohtaan.

Luovutuksella tarkoitetaan säännöksessä vapaaehtoista hallinnan luovutusta, tapahtuipa se missä tarkoituksessa tahansa. Tunnistusvälineen haltijan voidaan katsoa ottavan riskin välineen väärinkäytöstä, vaikka hän luovuttaisi sen toiselle esimerkiksi vain säilytettäväksi. Tämän vuoksi hän voi joutua vastuuseen riskin toteutuessa. Säännöksessä tarkoitetusta luovutuksesta on kysymys vain silloin, kun tunnistusvälineen haltija tietoisesti luovuttaa juuri välineen hallinnan toiselle. Säännös ei siten koske esimerkiksi tilannetta, jossa tunnistusvälineen haltija luovuttaa toisen säilytettäväksi laukun, jossa tunnistusväline on. Jos tunnistusvälineen haltijan tällaista menettelyä pidetään huolimattomana, vastuu voi kuitenkin syntyä momentin 2 kohdan nojalla.

Momentin 2 kohdan mukaan tunnistusvälineen haltija voi joutua vastuuseen välineen oikeudettomasta käytöstä, jos välineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää. Vastaavankaltainen vastuuperuste on nykyisin säädetty kuluttajansuojalain 7 luvun 19 §:n 1 momentin 2 kohdassa. Tunnistusvälineen haltijan velvollisuutta huolehtia välineestä on käsitelty edellä ehdotetun 23 §:n perusteluissa.

Tunnistusvälineen haltija voi momentin 3 kohdan nojalla joutua vastuuseen välineen oikeudettomasta käytöstä, jos hän on laiminlyönyt 25 §:ssä säädetyn velvollisuutensa ilmoittaa tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan. Vastaava vastuuperuste sisältyy nykyisin kuluttajansuojalain 7 luvun 19 §:n 1 momentin 3 kohtaan.

Pykälän 2 momentissa säädetään tilanteista, joissa tunnistusvälineen haltija ei ole vastuussa välineen oikeudettomasta käytöstä, vaikka jokin 1 momentissa säädetty vastuun peruste täyttyisikin.

Momentin 1 kohdan mukaan tunnistusvälineen haltija ei ole vastuussa tunnistusvälineen oikeudettomasta käytöstä siltä osin kuin välinettä on käytetty sen jälkeen, kun hän on ilmoittanut palveluntarjoajalle tai sen ilmoittamalle muulle taholle välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä. Säännös vastaa asiallisesti kuluttajansuojalain 7 luvun 19 §:n 2 momentin 1 kohtaa.

Momentin 2 kohdan mukaan tunnistusvälineen haltija ei ole vastuussa välineen oikeudettomasta käytöstä myöskään, jos tunnistuspalvelun tarjoaja on laiminlyönyt ehdotetussa 25 §:n 2 momentissa säädetyn velvollisuutensa huolehtia siitä, että vahvan sähköisen tunnistuspalvelun käyttäjällä on mahdollisuus tehdä milloin tahansa ilmoitus tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä. Vastaavaa säännöstä ei sisälly kuluttajansuojalain 7 luvun 19 §:ään. Säännös parantaa siten tunnistusvälineen haltijan asemaa nykyiseen verrattuna, ja on luonnollinen seuraus palveluntarjoajalle asetetun velvoitteen rikkomisesta.

Momentin 3 kohdan mukaan tunnistusvälineen haltija ei ole vastuussa välineen oikeudettomasta käytöstä, jos tunnistuspalvelua käyttävä palveluntarjoaja on laiminlyönyt tarkastaa välineeseen liittyvän käyttörajoituksen olemassa olon tai tiedon välineen sulkemisesta tai käytön estämisestä välinettä käytettäessä. Vastaavanlainen säännös on nykyisin kuluttajansuojalain 7 luvun 19 §:n 2 momentin 2 kohdassa. Tunnistuspalvelua käyttävän palveluntarjoajan on tarkistettava nämä tiedot silloin, kun tunnistusvälinettä käytetään. Tarkistaminen ei ole tarpeen, jos väline on sellainen, että sen käyttäminen oikeudettomasti voidaan teknisin keinoin estää. Muussa tapauksessa tunnistuspalvelua käyttävä palveluntarjoaja ottaa riskin vastuun lankeamisesta.

4 luku. Sähköinen allekirjoitus

28 §. *Turvallinen allekirjoituksen luomisväline.* Pykälässä säädetään vaatimuksista, jotka allekirjoituksen luomisvälineen tulee täyttää, jotta sitä voidaan pitää turvallisena allekirjoituksen luomisvälineenä. Turvallisen allekirjoituksen luomisvälineen on riittävän luotettavasti varmistettava 1 momentin 1-5 kohdan vaatimusten täyttyminen. Riittävän luotettavalla tarkoitetaan mahdollisimman suurta luotettavuutta, joka voidaan saavuttaa käyttämällä hyväksi parhaimpia mahdollisia teknisiä ratkaisuja.

Pykälän 1 momentin 1 kohdan mukaan luomisvälineen on luotettavasti varmistettava allekirjoituksen luomistietojen ainutkertaisuus ja luottamuksellisuus. Viestin allekirjoittajan tietokoneessa tai muussa välineessä sijaitsevan ohjelman ja laitteen tulee olla varustettu siten, että se suorittaa allekirjoituksen ja muut tarvittavat toimenpiteet mahdollisimman luotettavalla tavalla ja siten, että allekirjoituksen luomistiedot säilyvät luottamuksellisina. Luottamuksellisuuden varmistaminen tarkoittaa muun muassa sitä, että ohjelmien suorittamat toimenpiteet tapahtuvat siten suojatusti, että esimerkiksi tietokoneeseen asennetun erillisen ohjelman avulla ei voida siepata allekirjoituksen luomistietoja.

Momentin 2 kohdan mukaan turvallisen allekirjoituksen luomisvälineen tulee varmistaa, että allekirjoituksen luomistietoja ei voi päätellä muista tiedoista. Luomisvälineellä suoritetut toimenpiteet eivät siten saisi mahdollistaa pääsyä ainutkertaisiin luomistietoihin. Se voidaan toteuttaa muun muassa ohjelmistollisin asetuksin sekä laitteen tai sen osien rakenteellisin ratkaisuin. Lisäksi turvallisessa allekirjoituksen luomisvälineessä käytetyn salausalgoritmin on oltava riittävän vahva ja avainpituuden riittävä, jottei salauksen lopputuloksesta eli sähköisestä allekirjoituksesta voida päätellä allekirjoituksen luomistietoja, kuten yksityistä avainta.

Turvallisen allekirjoituksen luomisvälineen tulee 3 kohdan mukaan luotettavasti varmistaa, että allekirjoitus on suojattu väärentämiseltä. Käytännössä väärentäminen voidaan estää käyttämällä riittävän vahvaa algoritmia sekä riittäviä avainpituuksia.

Momentin 4 kohdan mukaan turvallisen allekirjoituksen luomisvälineen tulee varmistaa se, että allekirjoittaja voi suojata allekirjoituksen luomistiedot muiden käytöltä. Käytännössä se voi tapahtua suojaamalla esimerkiksi toimikortilla olevat allekirjoituksen luomistiedot salasanalla tai biometrisilla tunnistemenetelmillä.

Momentin 5 kohdan mukaan turvallinen allekirjoituksen luomisväline ei saa muuttaa allekirjoitettavia tietoja. Allekirjoitettavan tiedon on pysyttävä prosessin aikana muuttumattomana. Luomisväline ei saa myöskään estää allekirjoitettavien tietojen esittämistä allekirjoittajalle ennen allekirjoittamista.

Pykälän 2 momentin 1 kohdan mukaan komission vahvistamien ja Euroopan Yhteisöjen virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukaisen turvallisen allekirjoituksen luomisvälineen katsotaan aina täyttävän ehdotetussa 1 momentissa säädetyt vaatimukset. Momentin 2 kohdan mukaan turvallisen allekirjoituksen luomisvälineen vaatimukset täyttää myös sellainen allekirjoituksen luomisväline, jonka vaatimusten arviointitehtävään nimetty tarkastuslaitos on turvalliseksi allekirjoituksen luomisvälineeksi hyväksynyt. Tarkastuslaitoksen tulee olla nimenomaan kyseiseen arviointitehtävään nimetty sekä sijaita Suomessa tai muussa Euroopan talousalueeseen kuuluvassa valtiossa. Direktiivin 3 artiklan 4 kohdan 2 alakohta edellyttää, että tällaisen laitoksen antama todistus luomisvälineen

turvallisuudesta on tunnustettava kaikissa EU:n jäsenvaltioissa. Tarkastuslaitoksesta säädetään ehdotetussa 29 §:ssä.

Pykälä vastaa sähköisistä allekirjoituksista annetun lain 5 §:ää. Pykälän 1 momentilla pannaan täytäntöön direktiivin liite 3. Pykälän 2 momentin 1 kohdan säännöksellä sekä 34 §:n 2 momentilla pannaan täytäntöön direktiivin 3 artiklan 5 kohta. Pykälän 2 momentin 2 kohdan säännöksellä pannaan täytäntöön direktiivin 3 artiklan 4 kohdan 2 alakohta.

29 §. *Tarkastuslaitos.* Pykälän 1 momentin perusteella Viestintävirasto voi tarvittaessa nimetä tarkastuslaitoksia, joiden tehtävänä on selvittää, vastaako allekirjoituksen luomisväline ehdotetun 28 §:n 1 momentissa säädettyjä vaatimuksia. Tarkastuslaitos voi olla joko yksityinen tai julkinen laitos.

Direktiivin 9 artiklan mukainen sähköisten allekirjoitusten komitea on sopinut tarkastuslaitoksille asetettavista vähimmäisvaatimuksista, jotka Euroopan yhteisöjen komissio on vahvistanut 6 päivänä marraskuuta 2000 tehdyllä päätöksellä vähimmäisedellytyksistä, jotka jäsenvaltioiden on otettava huomioon nimetessään sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY 3 artiklan 4 kohdan mukaisia laitoksia; Bryssel, 06/11/2000, K(2000) 3179 lopullinen.

Komitean asettamien edellytysten mukaisesti tarkastuslaitoksen tulee olla toiminnallisesti ja taloudellisesti riippumaton muista alalla toimivista osapuolista. Tarkastuslaitos, sen johto tai allekirjoitusten luomisvälineiden arviointiin osallistuva henkilökunta eivät saa olla turvallisten allekirjoitusten luomismenetelmien suunnittelijoita, valmistajia, toimittajia tai asentajia, eivätkä myöskään varmenteiden tarjoajia tai näiden valtuutettuja edustajia. Mikäli laitos on osa organisaatiota, joka tekee myös muuta kuin tässä pykälässä tarkoitettua tarkastustoimintaa, laitoksen tulee olla tunnistettavissa kyseisen organisaation erillisenä yksikkönä ja organisaation eri toiminnot on voitava selkeästi erottaa toisistaan.

Tarkastuslaitoksen toiminnan tulee olla asianmukaista eikä se saa esimerkiksi syrjiä ketään, joka haluaa käyttää sen palveluita. Tarkastuslaitoksen tulee käyttää selkeitä turvallisen allekirjoituksen luomisvälineen arviointikäytänteitä ja sen tulee kirjata kaikki olennaiset arviointikäytänteitä koskevat tiedot. Kenen tahansa tulee voida käyttää laitoksen palveluita.

Tarkastuslaitoksella tulee olla myös riittävät taloudelliset voimavarat toiminnan asianmukaiseksi järjestämiseksi ja mahdollisen korvausvastuun kattamiseksi. Mahdollisen korvausvastuun kattamiseen voidaan varautua esimerkiksi vastuuvakuutuksella. Lisäksi tarkastuslaitoksella tulee olla riittävästi ammattitaitoista ja puolueetonta henkilöstöä sekä sillä tulee olla toiminnan edellyttämät tilat ja välineistö. Henkilöstöllä tulee olla riittävästi koulutusta ja kokemusta arviointitehtävien luotettavaksi suorittamiseksi erityisesti sähköisten allekirjoituksen tekniikoista ja niihin liittyvistä tietoturvallisuustekijöistä. Henkilökunnan puolueettomuuden takaamiseksi heidän palkkauksensa ei saa riippua tehtyjen vaatimustenmukaisuuden arviointien määrästä tai niiden tuloksista.

Viestintävirasto nimeää tarkastuslaitokset hakemuksen perusteella. Hakemuksen tulee sisältää hakijan yhteystietojen ja kaupparekisteriotteen tai vastaavan selvityksen lisäksi selvitys 2 momentin tarkoittamien edellytysten täyttymisestä hakijan toiminnassa. Viestintävirasto antaa myös tarvittaessa ohjeita hakemukseen sisällytettävistä tiedoista ja niiden toimittamisesta Viestintävirastolle.

Viestintävirasto valvoo tarkastuslaitoksen toimintaa. Tarkastuslaitoksen tulee ilmoittaa Viestintävirastolle sellaisista toimintansa muutoksista, joilla on vaikutusta tarkastuslaitoksen nimeämisen edellytyksiin. Jos tarkastuslaitos ei enää täytä asetettuja vaatimuksia tai se toimii säännösten vastaisesti, Viestintäviraston tulee peruuttaa nimeämispäätös.

Säännös vastaa sähköisistä allekirjoituksista annetun lain 6 §:ää. Säännöksellä pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 3 artiklan 4 kohdan 1 alakohta ja edellä mainittu komission päätös tarkastuslaitoksille asetettavista vähimmäisvaatimuksista. Suomessa ei toistaiseksi ole nimetty yhtään tarkastuslaitosta.

30 §. *Laatuvarmenne.* Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää 2 momentissa säädetyt vaatimukset ja jonka on

myöntänyt 33-38 §:ssä säädetyt vaatimukset täyttävä varmentaja. Ehdotetussa, samoin kuin voimassa olevassa laissa käytetään nimitystä "laatuvarmenne", jolla tarkoitetaan samaa kuin direktiivin 2 artiklan 10 kohdan määritelmän "hyväksytyllä varmenteella". Pykälässä säädetään laatuvarmenteen vähimmäisvaatimuksista.

Laatuvarmenteessa tulee ehdotetun 2 momentin 1 kohdan mukaan olla tieto siitä, että varmenne on laatuvarmenne, ja ehdotetun 2 kohdan mukaan siinä tulee olla varmentajan nimi ja sijoittautumisvaltio. Sijoittautumisvaltio määräytyisi sen mukaan missä taloudellisen toiminnan tosiasiallinen harjoittaminen kiinteästä toimipaikasta tapahtuu. Jos varmentajalla on useita sijoittautumispaikkoja, sijoittautumisvaltioksi katsotaan se valtio, jossa varmentajan varmennetoiminnan keskus sijaitsee.

Allekirjoittajan nimen tulee ehdotetun 3 kohdan mukaan kuulua laatuvarmenteen tietosisältöön. Jos nimi on salanimi, on sen selkeästi käytävä ilmi varmenteesta.

Allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja vastaavien allekirjoituksen todentamistietojen tulee ehdotetun 4 kohdan mukaan olla osa laatuvarmenteen tietosisältöä. Julkisen avaimen järjestelmässä tämä tarkoittaa sitä, että laatuvarmenteen tietosisältöön tulee kuulua yksityistä avainta vastaava julkinen avain.

Laatuvarmenteen tulee ehdotetun 5 kohdan mukaan sisältää tiedot varmenteen voimassaoloajasta. Tietojen tulee sisältää sekä voimassaolon alkamis- että päättymisaika.

Laatuvarmenteessa tulee ehdotetun 6 kohdan mukaan olla sen yksilöivä tunnus. Luotettava varmennetoiminta edellyttää, että varmenteet voidaan erottaa toisistaan. Tunnus voi olla juokseva sarjanumero tai muu yksilöllinen merkkijono.

Ehdotetun 7 kohdan mukaan varmentajan kehittyneen sähköisen allekirjoituksen tulee sisältyä laatuvarmenteeseen. Sillä turvataan varmenteen sisällön muuttumattomuus.

Varmenteen mahdollisten käyttötarkoitusta tai suoritettavien toimien rahallista arvoa koskevien rajoitusten on ehdotetun 8 kohdan mukaan ilmettävä laatuvarmenteesta. Rajoitus voi koskea esimerkiksi oikeustoimen rahamääräistä arvoa. Rajoituksella voidaan myös rajoittaa varmenteen käyttö vain tiettyihin oikeustoimiin.

Pelkkä nimi ei välttämättä yksilöi allekirjoittajaa riittävästi. Allekirjoittajaan liittyvien erityisten tietojen tulisi ehdotetun 9 kohdan mukaan ilmetä laatuvarmenteesta, jos ne ovat tarpeellisia laatuvarmenteen käyttötarkoituksen kannalta. Tällainen tieto voisi olla esimerkiksi tieto oikeudesta toimia jonkin yrityksen nimissä. Erityinen tieto voi olla jokin allekirjoittajan henkilötieto, kuten varmentajan myöntämä tunnus.

Ehdotetussa 3 momentissa todetaan, että jos laatuvarmenteita tarjoava varmentaja tarjoaa myös 3 luvussa tarkoitettua vahvaa sähköistä tunnistuspalvelua, katsotaan 1 momentin vaatimusten täyttävän aina myös 19 §:n 1 momentissa tarkoitetut varmenteen tietosisältöä koskevat vaatimukset. Säännöksellä varmistetaan, että saman palveluntarjoajan tarjoamien varmenteiden tietosisältöihin ei kohdistu ristiriitaisia vaatimuksia.

Pykälällä pannaan täytäntöön direktiivin 2 artiklan 10 kohdan määritelmä ja direktiivin liite 1. Pykälän 2 momentin 3 kohdalla pannaan lisäksi täytäntöön direktiivin 8 artiklan 3 kohta. Ehdotettu pykälä vastaa sähköisistä allekirjoituksista annetun lain 7 §:ää.

31 §. *Muun kuin Suomeen sijoittautuneen varmentajan tarjoama laatuvarmenne.* Ehdotetussa pykälässä säädetään niistä edellytyksistä, joiden täyttyessä muualle kuin Suomeen sijoittautuneen varmentajan laatuvarmenteen tarjoaman varmenteen katsotaan täyttävän tässä laissa säädetyt laatuvarmennetta koskevat vaatimukset. Varmenteen tulisi vähintään täyttää ehdotetun 30 §:n 2 momentin vaatimukset.

Pykälän 1 momentin 1 kohdan mukaan laatuvarmenteeksi hyväksytään varmenne, jonka on tarjonnut toiseen ETA-valtioon sijoittautunut varmentaja. Edellytyksenä on lisäksi, että varmentajan tarjoama varmenne täyttää sijoittautumisvaltiossa laatuvarmenteelle asetetut vaatimukset.

Ehdotetun 2 kohdan mukaan laatuvarmenteeksi hyväksytään varmenne, jota tarjoaa jossain ETA-valtiossa vapaaehtoiseen akkreditointijärjestelmään liittynyt varmentaja, joka täyttää kyseisessä valtiossa sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivin täytäntöön panemiseksi sää-

detyt kansalliset vaatimukset. Vapaaehtoisia akkreditointijärjestelmiä voi olla useita ja niihin liittyminen ja kuuluminen on vapaaehtoista.

Laatuvarmenteeksi hyväksytään ehdotetun 3 kohdan mukaan varmenne, jonka takaajana on Euroopan talousalueen jäsenvaltioon sijoittautunut varmentaja, joka täyttää sijoittautumisvaltiossa sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin täytäntöön panemiseksi säädetyt kansalliset vaatimukset.

Ehdotetun 4 kohdan mukaan katsotaan varmentajan laatuvarmenteena tarjoaman varmenteen täyttävän laatuvarmenteelle asetetut vaatimukset, mikäli varmenne tai varmentaja on tunnustettu Euroopan yhteisön ja yhden tai useamman kolmannen maan tai kansainvälisen organisaation välisen kahden- tai monenvälisen sopimuksen nojalla.

Säännöksellä pannaan täytäntöön direktiivin 7 artiklan 1 kohta, ja se vastaa sähköisistä allekirjoituksista annetun lain 8 §:ää.

32 §. *Ilmoitus toiminnan aloittamisesta.* Ehdotetun pykälän 1 momentin mukaan palveluntarjoajan tulee tehdä Viestintävirastolle ilmoitus ennen kuin se aloittaa laatuvarmenteiden tarjoamisen yleisölle. Ilmoituksen tulee olla kirjallinen. Siitä tulee ilmetä varmentajan nimi ja yhteystiedot sekä tiedot, joiden perusteella 30 §:ssä ja 33-38 §:ssä säädettyjen vaatimusten täyttyminen voidaan varmistaa. Viestintävirasto voi jatkossakin antaa tarpeellisia määräyksiä tai suosituksia ilmoitettavien tietojen toimittamisesta ja niiden tarkemmasta sisällöstä. Viestintävirasto on antanut voimassa olevan lain nojalla 29 päivänä tammikuuta 2003 määräyksen yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle (7/2003 M). Ehdotetun 50 §:n 2 momentin mukaan määräys on voimassa siihen saakka, kunnes Viestintävirasto antaa uuden määräyksen ehdotetun lain perusteella.

Pykälän 2 momentin mukaan laatuvarmenteiden tarjonnan aloittaminen ei edellytä Viestintäviraston etukäteistä hyväksyntää, mutta Viestintäviraston on ilmoituksen saatuaan viipymättä kiellettävä 2 momentissa säädetyllä tavalla laatuvarmenteiden tarjonta, elleivät laatuvarmennetta ja laatuvarmenteita tarjoavaa varmentajaa koskevat edellytykset täyty. Kielto koskee vain oikeutta tarjota varmenteita laatuvarmenteina. Esimerkiksi varmenteen tietosisältöön ei saa sisältyä tietoa laatuvarmenteesta. Muutoin varmentaja voi jatkaa varmennetoimintaansa kiellosta huolimatta ja tarjota varmenteita tavallisina varmenteina.

Varmentaja, joka tarjoaa varmenteitaan laatuvarmenteina vastaa kuitenkin aina tämän lakiesityksen mukaisena laatuvarmentajana mahdollisista vahingoista, joita saattaa syntyä siitä, että laatuvarmenteen vaatimuksia täyttämätöntä varmennetta käytetään laatuvarmenteena. Viestintäviraston on ilmoituksentekijän intressit ja edellä mainittu laatuvarmenteita tarjoavan varmentajan korvausvastuu huomioiden toimittava asiassa viipymättä, jotta varmentaja saa Viestintävirastolta tiedon liiketoimintansa tueksi mahdollisimman nopeasti.

Varmentajan on myös viipymättä ilmoitettava ehdotetun 3 momentin säännöksen mukaan Viestintävirastolle, jos ilmoitetuissa tiedoissa tapahtuu muutoksia. Ehdotetun lain mukaan Viestintävirasto valvoo laatuvarmenteita tarjoavia varmentajia lakiesityksen 5 luvusta ilmenevällä tavalla. Valvontatehtävien toteuttamiseksi Viestintävirasto tarvitsee riittävät ja oikeat tiedot laatuvarmenteita yleisölle tarjoavista varmentajista.

Ehdotetussa 4 momentissa todetaan, että Viestintävirasto pitää laatuvarmenteita tarjoavista varmentajista julkista rekisteriä. Rekisteri sisältää muun muassa varmentajan nimen ja osoitetiedot siten kuin varmentaja on ne Viestintävirastolle ilmoittanut. Rekisteristä on saatavissa tiedot niistä varmentajista, jotka ovat ilmoittaneet Viestintävirastolle tarjoavansa laatuvarmenteita Suomessa. Rekisterin tiedoilla on kuitenkin ainoastaan informatiivinen tehtävä. Laatuvarmenteita yleisölle myöntävä varmentaja vastaa kolmansille osapuolille ehdotetun 41 §:n mukaisesti mahdollisista toiminnastaan aiheutuneista vahingoista riippumatta siitä onko kyseinen varmentaja merkitty Viestintäviraston rekisteriin vai ei.

Pykälässä 5 momentissa todetaan, että laatuvarmenteita tarjoava varmentaja voi tehdä myös 10 §:ssä tarkoitetun ilmoituksen, jos se haluaa tarjota laatuvarmenteiden lisäksi tun-

nistuspalveluita. Säännös on tarpeen selkeyden vuoksi.

Säännöksellä pannaan täytäntöön direktiivin 3 artiklan 1 kohta ja osittain 3 kohta. Se vastaa sähköisistä allekirjoituksista annetun lain 9 §:ää.

33 §. *Laatuvarmenteita tarjoavan varmentajan yleiset velvollisuudet*. Pykälässä säädetään laatuvarmenteita tarjoavan varmentajan yleisistä velvollisuuksista. Ehdotetun 1 momentin mukaan laatuvarmenteiden tarjoaja eli se, jonka nimi on varmenteessa, on vastuussa kaikista varmentamistoiminnan osaalueista, vaikka se ostaisikin osan tarjoamistaan palveluista tai tuotteista alihankkijoilta. Varmentajan apunaan käyttämien henkilöiden suorittamia tehtäviä voivat olla esimerkiksi varmennehakemusten vastaanottaminen, varmenteen luominen sekä sulkulistan ylläpito.

Varmentajalla tulee olla myös harjoitetun toiminnan laajuuteen nähden riittävät tekniset taidot ja taloudelliset voimavarat. Varmentajan tulee huolellisuuden ja luotettavuuden osoittamiseksi muun muassa arvioida toimintansa tekniseen ja taloudelliseen turvallisuuteen liittyvät riskit ja ryhtyä tarpeellisiin toimenpiteisiin näiden riskien minimoimiseksi. Huolellisuus ja luotettavuus edellyttävät myös varmentajan menettelytapojen dokumentoimista.

Ehdotetun 2 momentin 1 kohdan mukaan varmentajalla tulee olla sellainen henkilöstö, jolla on riittävä asiantuntemus, kokemus ja pätevyys. Varmentajan tulee siten huolehtia, että sen palveluksessa olevilla henkilöillä, ja erityisesti sen johtotehtävissä toimivilla, on varmennetoiminnan edellyttämä asiantuntemus, kokemus ja pätevyys. Henkilöstöllä tulee olla riittävä asiantuntemus muun muassa sähköisten allekirjoitusten tekniikasta ja tietoturvallisuusasioista.

Varmentajan tulee ehdotetun 2 momentin 2 kohdan mukaan huolehtia riittävistä taloudellisista voimavaroista toimintansa järjestämiseksi ja mahdollisen vahingonkorvausvastuun varalta. Riittävyyttä arvioidaan suhteessa varmentajan toiminnan laajuuteen. Vaikka varmentajalla olisi vahingonkorvausten kattamiseksi riittävä vastuuvakuutus, tulee sillä olla muutoinkin riittävät taloudelliset voimavarat luotettavan varmennetoiminnan harjoittamiseksi.

Varmentajan tulee ehdotetun 2 momentin 3 kohdan perusteella pitää yleisesti saatavilla tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida. Varmentajan asiakkailla sekä varmenteisiin luottavilla tahoilla tulee olla riittävästi tietoa varmentajan toiminnasta, jotta he voivat arvioida, onko varmenteen luotettavuus heidän tarkoituksiinsa riittävä. Momentin 3 kohdan vaatimus voidaan toteuttaa esimerkiksi varmennepolitiikan ja varmennekäytäntöilmoituksen avulla.

Varmennepolitiikka on asiakirja, jonka perusteella varmentaja myöntää varmenteita ja joka käyttäjän pitää tuntea ja hyväksyä. Politiikka määrittelee säännöt varmentajan toiminnalle ja sen perusteella voidaan arvioida varmenteiden käytettävyyttä tiettyyn sovellukseen. Politiikka on asiakirja, joka vastaa kysymykseen, mitä varmentaja tekee, ja määrittelee siten vaatimuksia varmentajan toiminnalle ja johdolle. Varmennepolitiikka voi olla yhteinen useiden eri varmentajien kesken. Esimerkiksi European Telecommunications Standards Institute (ETSI) on määritellyt perustason varmennepolitiikan minimitason vaatimuksiksi laatuvarmenteita tarjoaville varmentajille.

Varmentajalla tulisi olla dokumentoituna myös omaan organisaatioonsa soveltuva varmennekäytäntö (Certification Practise Statement, jäljempänä CPS), joka on tarkempi kuvaus siitä, miten varmentaja omassa organisaatiossaan toteuttaa varmennepolitiikkaa. Varmennekäytännön avulla esimerkiksi riippumattomat ulkopuoliset tahot voivat todeta, täyttääkö varmentaja politiikan vaatimukset.

Ehdotettujen 3 kohdassa tarkoitettujen tietojen tulee olla yleisesti saatavilla. Tietojen katsotaan olevan yleisesti saatavilla muun muassa silloin, kun ne ovat noudettavissa varmentajan toimipaikasta tai saatavilla varmentajan kotisivulla internetissä.

Ehdotetun 4 kohdan mukaan varmentajan tulee turvata allekirjoituksen luomistietojen luottamuksellisuus silloin, kun se itse tuottaa tiedot. Varmentajan tulee varmistua siitä, että se luovuttaa luomistiedot ainoastaan niiden hallintaan oikeutetulle henkilölle.

Varmentaja ei ehdotetun 3 momentin mukaan saa tallentaa tai jäljentää allekirjoittajalle luovutettuja allekirjoituksen luomistietoja. Allekirjoituksen luomistietojen säilyminen vain allekirjoittajan hallinnassa on olennaisen tärkeää sähköisen allekirjoituksen luotettavuuden toteutumiseksi. Tämän vuoksi varmentajille säädettäisiin velvollisuus olla jäljentämättä tai tallentamatta allekirjoituksen luomistietoja. Allekirjoituksen luomistietojen hävitessä tai tuhoutuessa voisi allekirjoittaja pyytää aina uudet allekirjoituksen luomistiedot varmentajalta. Allekirjoittajan intressissä on tällaisessa tilanteessa tehdä välittömästi 36 §:ssä tarkoitettu ilmoitus.

Säännöksellä pannaan täytäntöön direktiivin liitteen 2 kohdat a, e, g, h ja j. Se vastaa pääsääntöisesti sähköisistä allekirjoituksista annetun lain 10 §:ää. Ehdotetusta pykälästä on kuitenkin poistettu julkiseen hallintotehtävään viitanneet osuudet.

34 §. *Luotettavat laitteet ja ohjelmistot.* Laatuvarmenteita yleisölle tarjoavan varmentajan käyttämien järjestelmien sekä laitteiden ja ohjelmistojen on pykälän 1 momentin mukaan oltava riittävän turvallisia ja luotettavia sekä suojattuja muutoksilta ja väärentämiseltä. Riittävän turvallisella ja luotettavalla tarkoitetaan mahdollisimman suurta luotettavuutta, joka voidaan saavuttaa käyttämällä hyväksi parhaimpia mahdollisia teknisiä ratkaisuja. Järjestelmien ja niiden osien tulee olla suojattu siten, että vain varmentajan erikseen nimeämä henkilöstö voi tehdä niihin muutoksia. Muutosten on lisäksi rekisteröidyttävä ja tieto niistä on säilytettävä myös silloin, kun ne ovat mahdollisten ulkopuolisten toimijoiden tai laitevikojen aiheuttamia.

Ehdotetussa 2 momentissa säädetään siitä, että komission vahvistamien Euroopan yhteisöjen virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukaiset laitteet ja ohjelmistot katsotaan aina 1 momentissa säädettyjen vaatimusten mukaisiksi.

Säännöksellä pannaan täytäntöön direktiivin 3 artiklan 5 kohta ja liitteen 2 kohta f. Säännös vastaa sähköisistä allekirjoituksista annetun lain 11 §:ää.

35 §. *Laatuvarmenteen liikkeelle laskeminen.* Pykälän 1 momentin säännöksen mukaan laatuvarmenteita yleisölle tarjoavan varmentajan tulee huolellisesti ja luotettavalla tavalla tarkistaa hakijan henkilöllisyys ja muut laatuvarmenteen liikkeelle laskemisessa ja ylläpidossa tarpeelliset hakijan henkilöön liittyvät tiedot. Hakijan henkilöön liittyviä tietoja voivat olla ainakin hakijan nimi ja osoitetiedot sekä laatuvarmenteen tietosisältöön 30 §:n 2 momentin mukaisesti kuuluvat tiedot, mukaan lukien varmenteen tiettyyn käyttötarkoitukseen mahdollisesti liittyvät erityiset tiedot. Ehdotetun pykälän terminologiaa on muutettu voimassa olevaan lakiin verrattuna siten, että laatuvarmenteitakaan ei myönnetä, vaan nekin lasketaan liikkeelle. Muutos johtuu siitä, että myöskään laatuvarmenteiden osalta kyse ei enää olisi julkisen vallan käytöstä.

Laatuvarmenteita tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti. Henkilökohtaisella tunnistamisella tarkoitettaisiin sitä, että hakijan on laatuvarmennetta hakiessaan henkilökohtaisesti käytävä varmentajan luona tunnistettavana. Hakijan henkilöllisyyden tarkistaminen luotettavalla tavalla voisi tapahtua hakijan esittämästä luotettavasta asiakirjasta. Luotettavina asiakirjoina voitaisiin pitää samoja asiakirjoja kuin ehdotetun 17 §:n osalta. Henkilötietojen käsittelystä säädetään ehdotetussa 6 §:ssä.

Laatuvarmenteita tarjoava varmentaja vahvistaa laatuvarmenteeseen merkittävällä kehittyneellä sähköisellä allekirjoituksellaan laatuvarmenteen tietojen kuuluvan tietylle henkilölle. Varmenteen luovuttamisen jälkeen allekirjoittajan henkilöllisyyttä ei yleensä enää tarkisteta. Varmennetta myönnettäessä annetaan allekirjoittajalle ainutkertaiset allekirjoituksen luomistiedot. Allekirjoituksen todentaja ei välttämättä lainkaan tunne luomistietoja käyttävää allekirjoittajaa, vaan luottaa varmentajan tekemään tunnistamiseen ja varmentajan laatuvarmenteeseen merkitsemiin tietoihin. Siksi on erityisen tärkeää, että hakijan henkilöllisyys tarkistetaan luotettavasti ja varmistutaan laatuvarmenteeseen merkittyjen tietojen oikeellisuudesta sekä laatuvarmenteen luovuttamisesta hallintaan oikeutetulle henkilölle. Varmentaja vastaa ehdotetun 41 §:ssä säädetyn mukaisesti muun muassa siitä, että laatuvarmenteeseen merkityt tiedot ovat myöntämishetkellä oikeita ja että laatuvarmenne luovutetaan sen hallintaan oikeutetulle henkilölle. Myöntämishetkeksi

katsotaan 41 §:n yksityiskohtaisten perustelujen mukaisesti laatuvarmenteen luovutushetki.

Varmentajan tulee ehdotetun 2 momentin mukaan antaa varmenteen hakijalle ennen sopimuksen tekemistä tiedot varmenteen käyttöehdoista mahdollisine käyttörajoituksineen, vapaaehtoisista akkreditointijärjestelmistä, varmennetoiminnan viranomaisvalvonnasta sekä valitus- ja riitojenratkaisumenettelyistä. Käyttöehtoihin sisältyviä tietoja ovat muun muassa tiedot mahdollisten hakemistopalvelujen käytöstä sekä erityisesti laatuvarmenteen peruuttamisesta ja varmenteen merkitsemisestä sulkulistalle. Käyttöehtoihin tulee sisältyä myös tiedot varmentajan vahingonkorvausvastuusta ja muista velvollisuuksista.

Varmenteen hakijaa tulee myös informoida Viestintäviraston ja tietosuojavaltuutetun varmentajaan kohdistuvasta valvonnasta sekä hakijan oikeudesta saattaa Viestintäviraston tutkittavaksi tämän lain mukaisen laatuvarmenteita yleisölle tarjoavan varmentajan toimintaa koskeva asia.

Tiedot tulisi antaa laatuvarmenteen hakijalle kirjallisesti sellaisessa muodossa, että hakija voi ne vaivatta ymmärtää. Sähköisessä muodossa ja yleisesti luettavissa ja tallennettavissa oleva tieto voitaisiin katsoa kirjallisesti annetuksi.

Säännöksellä pannaan täytäntöön direktiivin liitteen 2 kohdat d ja k. Se vastaa pääsääntöisesti sähköisistä allekirjoituksista annetun lain 12 §:ää, mutta siitä on poistettu julkisen vallan käyttöön viittaavat osuudet.

36 §. *Laatuvarmenteen peruuttaminen.* Varmennetoiminnan turvallisuuden ja luotettavuuden kannalta on tärkeää, että laatuvarmenteen oikeudeton käyttö voidaan estää mahdollisimman varhaisessa vaiheessa. Jos allekirjoituksen luomistiedot on esimerkiksi anastettu tai ne ovat kadonneet, on tärkeää, että allekirjoittaja pyytää viipymättä varmentajalta laatuvarmenteensa peruuttamista. Vahingot jäävät silloin mahdollisimman vähäisiksi.

Allekirjoittajalle ehdotetaan säädettäväksi 1 momentissa nimenomainen velvoite pyytää varmentajalta laatuvarmenteensa peruuttamista, jos hänellä on perusteltu syy epäillä, että luomistietoja voidaan käyttää oikeudettomasti. Varmentajan on 2 momentin mukaan viipymättä peruutettava laatuvarmenne, jos allekirjoittaja sitä pyytää. Varmentajan tulee peruuttaa laatuvarmenne merkitsemällä siitä tieto 37 §:n 3 momentissa tarkoitetulle sulkulistalle. Allekirjoittajan ei tarvitse perustella pyyntöään.

Peruuttamispyynnön saapumisajankohtana on pidettävä hetkeä, jolloin pyyntö on ollut varmentajan käytettävissä siten, että sitä voidaan käsitellä. Sähköisessä muodossa lähetetyn viestin osalta tämä tarkoittaa ajankohtaa jolloin pyyntö on varmentajan käytettävissä vastaanottolaitteessa tai tietojärjestelmässä.

Varmentaja voi ehdotetun 3 momentin mukaan peruuttaa varmenteen myös, jos siihen on erityistä syytä. Erityinen syy voisi olla esimerkiksi allekirjoittajan kuolema tai muu vastaava pakottava syy. Tällainen erityinen syy voi olla myös varmentajan toiminnan päättyminen. Lisäksi varmentaja voi peruuttaa varmenteen, jos allekirjoittaja rikkoo varmentajan kanssa tehtyä sopimusta tai käyttää varmennetta vastoin sen käyttötarkoitusta.

Laatuvarmenteen peruuttamisesta ja peruuttamisen ajankohdasta tulee 3 momentin mukaan aina ilmoittaa allekirjoittajalle. Tämä on tarpeen, jotta allekirjoittaja voi varmistua tekemänsä peruuttamispyynnön onnistumisesta tai mahdollisesta varmentajan aloitteesta tehdystä peruuttamisesta.

Laatuvarmenteita yleisölle tarjoavien varmentajien vahingonkorvausvastuusta ja allekirjoituksen luomistietojen oikeudettomasta käytöstä säädetään 40 ja 41 §:ssä.

Säännös vastaa sähköisistä allekirjoituksista annetun lain 13 §:ää.

37 §. *Laatuvarmenteita tarjoavan varmentajan ylläpitämät rekisterit.* Laatuvarmenteita tarjoavalle varmentajalle on sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin liitteen 2 kohdassa b asetettu velvollisuus varmistaa nopea ja varma hakemistopalvelu sekä luotettava ja viivytyksetön peruuttamismahdollisuus. Direktiivin liitteen 2 kohdassa i edellytetään lisäksi, että laatuvarmenteita tarjoava varmentaja arkistoi kaikki asiaankuuluvat varmennetta koskevat tiedot tarkoituksenmukaiseksi ajaksi erityisesti voidakseen esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä.

Laatuvarmenteita tarjoavien varmentajien ylläpitämiä rekistereitä koskevalla säännöksellä pyritään takaamaan se, että laatuvarmenteiden käyttöön keskeisesti liittyvät palvelut ovat mahdollisimman tehokkaasti ja luotettavina käytettävissä. Nimenomaan näiden palveluiden avulla varmentaja toimii luotettavana kolmantena osapuolena, joka todentaa laatuvarmenteella viestin vastaanottajalle viestin lähettäjän ja tämän allekirjoituksen luomistietojen voimassaolon. Ehdotetussa pykälässä sekä ehdotetussa 37 §:ssä säädetään myös tallennettavista tiedoista ja niiden säilyttämisestä.

Laatuvarmenteita tarjoavan varmentajan tulee ehdotetun 1 momentin mukaan ylläpitää rekisteriä liikkeelle laskemistaan varmenteista (varmennerekisteri). Rekisteriin tulee merkitä 30 §:n 2 momentissa määritellyn laatuvarmenteen tietosisällön lisäksi 35 §:n 1 momentissa tarkoitetut hakijan henkilöön liittyvät tiedot, mukaan lukien tieto laatuvarmennetta myönnettäessä käytetystä hakijan tunnistamismenettelystä. Lisäksi rekisteriin tulee merkitä 39 §:ssä tarkoitetut tiedot varmenteen voimassaolon tarkistamisesta sulkulistalta, silloin kun laatuvarmenteita yleisölle tarjoava varmentaja käyttää 39 §:n mukaista oikeutta tallettaa sulkulistan tarkistustiedot.

Laatuvarmenteita yleisölle tarjoava varmentaja voi näin ollen tallentaa esimerkiksi tiedon siitä, mistä asiakirjasta tunnistaminen on tehty, ja tallentaa myös tarvittavat tiedot kyseisestä asiakirjasta. Kyseinen tarvittava tieto voi olla esimerkiksi passin numero tai henkilötunnus. Laatuvarmenteita yleisölle tarjoava varmentaja voi myös esimerkiksi ottaa valokopioita tunnistamisessa käytetyistä asiakirjoista. Olennaista tietojen tallentamisessa on laatuvarmenteita tarjoavalle varmentajalle asetetun huolellisen ja luotettavan tunnistamisen todentaminen. Koska varmentajalla on 41 §:ssä määritelty ankara vahingonkorvausvastuu myöntämänsä laatuvarmenteen tietojen paikkansapitävyydestä, tulee varmentajalla myös olla mahdollisuus tarpeen vaatiessa todistaa toimineensa huolellisesti. Laatuvarmenteen tarkistamista koskevan tiedon tallettaminen on tarpeen esimerkiksi varmenteiden käytön laskutusta ja mahdollisia riitatilanteiden selvittämistä varten. Tarkistamista koskevan tiedon käyttämisestä säädetään tarkemmin 39 §:ssä.

Laatuvarmenteita tarjoavan varmentajan tulee 2 momentin mukaan varmistaa, että laatuvarmenteella varmennettuun kehittyneeseen sähköiseen allekirjoitukseen luottavalla osapuolella on saatavilla 30 §:n 2 momentissa määritelty laatuvarmenteen tietosisältö. Pykälässä ei ole tarkoitus säätää tarkemmin sitä, miten tiedot tulee olla allekirjoitukseen luottavien osapuolien saatavilla. Varmentaja voi käyttämistään teknisistä sovelluksista riippuen toteuttaa vaatimuksen tarkoituksenmukaisimmalla tavalla. Jos allekirjoittajan ja varmentajan välisellä sopimuksella sovitaan, että allekirjoittaja itse jakaa viestin mukana myös laatuvarmenteen, tulee varmenteen tietosisältö luottavan osapuolen tietoon ilman erityisiä varmentajan toimenpiteitä. Näissä tapauksissa ei tarvita erillistä varmentajan tarjoamaa palvelua. Varmentaja ja allekirjoittaja voivat myös sopia, että varmentaja luovuttaa varmennerekisteristä allekirjoitukseen luottavalle taholle 30 §:n 2 momentissa määritellyn tietosisällön mukaiset tiedot. Sähköisten allekirjoitusten luotettavuudelle olennaista on, että allekirjoitukseen luottavan osapuolen tietoon tulevat laatuvarmenteen tietosisällön mukaiset tiedot.

Laatuvarmenteita tarjoavan varmentajan tulee ehdotetun 3 momentin mukaan huolehtia myös siitä, että peruutetut varmenteet ja niiden tarkka peruuttamisajankohta merkitään asianmukaisesti ja viipymättä sulkulistalle. Allekirjoittajan vastuu allekirjoituksen luomistietojen oikeudettomasta käytöstä lakkaa pääsääntöisesti, kun hän on ehdotetun 36 §:n mukaisesti pyytänyt varmentajalta laatuvarmenteensa peruuttamista. Vastuu allekirjoituksen luomistietojen käytöstä allekirjoittajan peruutuspyynnön ja sulkulistalle merkinnän välisenä aikana kuuluu varmentajalle, joten nopea merkinnän tekeminen olisi varmentajan omassa intressissä. Luomistietojen oikeudettomasta käytöstä on säädetty tarkemmin 40 §:ssä.

Sulkulista tulee toteuttaa julkisena rekisterinä, koska ainoastaan sulkulistalta allekirjoitukseen luottava osapuoli voi todeta mahdollisen varmenteen peruuttamisen. Sulkulista voidaan toteuttaa esimerkiksi merkitsemällä sulkulistalle ainoastaan laatuvarmenteen yk-

silöivä tunnus. Tällöin sulkulista ei tule sisältämään laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen haltijan henkilöön liittyviä tietoja. Mikäli sulkulistalle merkitään allekirjoittajan henkilöön liittyviä tietoja, tulee tietojen merkitsemisestä saada allekirjoittajan nimenomainen suostumus. Tiettyyn laatuvarmenteeseen luottavan osapuolen kannalta riittää, että se voi tarkistaa laatuvarmenteen yksilöivän tunnisteen avulla, onko kyseessä oleva laatuvarmenne peruutettu.

Laatuvarmenteen 30 §:n 2 momentin mukaisten tietojen ja sulkulistan tulee ehdotetun 4 momentin mukaisesti olla ympärivuorokautisesti käytettävissä, koska tietoverkot mahdollistavat asioinnin vuorokaudenajasta riippumatta. Jos varmentaja jakaa 30 §:n 2 momentissa tarkoitettuja tietoja, tulee palvelun olla käytettävissä ympärivuorokautisesti. Jos allekirjoittaja itse jakaa laatuvarmennetta, ei tarvetta erilliseen varmentajan toteuttamaan palveluun ole, vaan tällöin voidaan katsoa, että 30 §:n 2 momentin määrittelemä laatuvarmenteen tietosisältö on ympärivuorokautisesti käytettävissä allekirjoittajan jakamana. Laatuvarmenteita tarjoavan varmentajan ylläpitämän sulkulistan tulee kuitenkin aina olla käytettävissä ympärivuorokautisesti.

Säännöksellä pannaan täytäntöön direktiivin liitteen 2 kohdat b ja c. Se vastaa sähköisistä allekirjoituksista annetun lain 14 §:ää.

38 §. *Varmennerekisterin tietojen säilyttäminen.* Pykälän mukaan laatuvarmenteita yleisölle tarjoavalla varmentajalla on velvollisuus luotettavalla ja tarkoituksenmukaisella tavalla säilyttää varmennerekisteriin ehdotetun 37 §:n 1 momentin mukaisesti tallennetut tiedot 10 vuoden ajan laatuvarmenteen voimassaolon päättymisestä. Tiedot voitaisiin säilyttää myös sähköisessä muodossa.

Varmennerekisterin tietojen säilyttämiselle ehdotettava pitkä, kymmenen vuoden määräaika.olisi edelleen tarpeen sen johdosta, että näyttökysymyksiin ja näytön saatavuuteen mahdollisesti liittyviä ongelmia, esimerkiksi väärinkäytöksistä aiheutuvien vahinkojen kohdalla, on mahdotonta täsmällisesti arvioida.

Tietojen säilyttämisessä tulee käyttää luotettavia järjestelmiä. Tietojen tallettaminen ja tietoihin tehtävät muutokset tulee tehdä vain varmentajan valtuuttamien, luotettavien henkilöiden toimesta. Lisäksi säilytettävien tietojen turvallisuutta vaarantavat tekniset muutokset tulee olla tietoja säilyttävän tahon havaittavissa. Henkilötietojen käsittelyn tulisi tapahtua henkilötietolain säännösten mukaisesti. Henkilötietolain soveltamisesta kaikkien varmentajien toimintaan on ehdotetun 6 §:n 4 momentissa informatiivinen viittaus.

Ehdotetun 2 momentin säännöksillä pyritään välttämään sitä, että saman palveluntarjoajan varmenteisiin ja niihin liittyviin järjestelmiin kohdistuisi ristiriitaisia vaatimuksia. Ehdotetussa 2 momentissa todettaisiin, että jos laatuvarmenteita yleisölle tarjoava varmentaja tarjoaa myös tunnistuspalveluita, voi palveluntarjoaja säilyttää varmennerekisterin tietoja kaikilta osin ehdotetussa 1 momentissa tarkoitetulla tavalla 24 §:n säännösten estämättä.

Säännöksellä pannaan täytäntöön direktiivin liitteen 2 kohdat i ja l. Säännöksen 1 momentti vastaa voimassa olevan sähköisistä allekirjoituksista annetun lain 15 §:ää.

39 §. *Varmenteen voimassaolon tarkistamista koskevan tiedon tallentaminen.* Pykälän mukaan laatuvarmenteita tarjoavalla varmentajalla tulee olla oikeus tallettaa tieto varmenteen voimassaolon tarkistamisesta. Tietoa voidaan käyttää ainoastaan varmenteiden käytön laskutuksen suorittamiseksi tai varmenteella varmennetun sähköisen allekirjoituksen avulla tehtyjen oikeustoimien todentamiseksi.

Tarkistamista koskevan tiedon tallettaminen on tarpeen erityisesti mahdollisten varmentajiin kohdistettujen vahingonkorvausvaatimusten johdosta. Varmentajan tulee voida tallettaa varmenteen voimassaolon tarkistamistieto, jotta se voi erityisesti oikeustoimiin liittyvissä kiistoissa näyttää, onko sulkulista tarkistettu ja onko kyseisenä ajankohtana varmenteen peruuttamisesta ollut tieto sulkulistalla. Tieto tarkistamisesta voidaan luovuttaa ainakin allekirjoittajalle ja sulkulistan tarkastaneelle. Varmentajan lisäksi tiedon tallettamisesta hyötyvät siten mahdollisissa riitatapauksissa myös oikeustoimen osapuolet eli allekirjoittaja ja allekirjoitukseen luottava osapuoli.

On myös mahdollista, että varmenteiden käytöstä tullaan laskuttamaan varmenteen

voimassaolon tarkistanutta osapuolta. Myös tällöin on luonnollisesti tarpeen, että varmenteiden tarjoajalla on tieto laskutuksen asianmukaiseksi hoitamiseksi.

Rajoittamalla varmenteen voimassaolon tarkistamista koskevan tiedon käyttö ainoastaan pykälän mainitsemiin tarkoituksiin, pyritään estämään yksittäistä henkilöä tai yritystä koskevien varmenteiden käyttötietojen kokoaminen.

Ehdotettua pykälää vastaavaa säännöstä ei sisälly sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin. Pykälän säännöksillä on tarpeen kansallisella tasolla täsmentää varmenteen voimassaolon tarkistamista koskevien tietojen käsittelyä. Ehdotettu pykälä vastaa sähköisistä allekirjoituksista annetun lain 21 §:ää.

40 §. *Vastuu allekirjoituksen luomistietojen oikeudettomasta käytöstä.* Ehdotetussa pykälässä säännellään allekirjoittajan vastuuta allekirjoituksen luomistietojen oikeudettomasta käytöstä aiheutuneesta vahingosta.

Allekirjoituksen luomistietojen oikeudetonta käyttöä on kadonneiden tai varastettujen luomistietojen käytön lisäksi luomistietojen käyttö sellaisessa tilanteessa, jossa luomistietojen haltija on alun perin saanut luomistiedot luvallisesti haltuunsa, mutta käyttää niitä sen jälkeen, kun allekirjoittaja on kieltänyt haltijaa käyttämästä luomistietoja tai kun haltijan oikeus luomistietojen käyttöön on muuten lakannut.

Allekirjoituksen luomistietojen oikeudeton käyttö on osittain rinnastettavissa luottokortin tai vastaavan tunnisteen oikeudettomaan käyttöön. Tämän vuoksi on perusteltua säätää periaatteiltaan samansuuntaisista vastuusäännöksistä. Käytännössä merkittävimpänä erona esimerkiksi luottokorttien käyttöön on se, että luomistietojen käyttö tullaan sovellettavasta tekniikasta riippuen suojaamaan esimerkiksi salasanalla tai tunnuksella, kuten esimerkiksi PIN-koodilla. Tulevaisuudessa luomistiedot voidaan suojata esimerkiksi sormenjälkitunnisteella. Tällöin luottokorttien käyttöön verrattuna luomistietojen käyttö tulee olemaan turvallisempaa ja oikeudeton käyttö huomattavasti vaikeampaa.

Pykälän 1 momentin pääsäännön mukaisesti allekirjoittaja vastaa luomistietojen oikeudettomasta käytöstä, kunnes peruuttamispyyntö on saapunut varmentajalle 36 §:n 2 momentin mukaisesti. Merkitystä ei olisi sillä miten luomistiedot ovat joutuneet niiden käyttöön oikeudettomalle.

Koska 1 momentissa säädetyn ankaran pääsäännön soveltaminen kuluttajiin olisi kohtuutonta, säädettään 2 momentissa kuluttajiin sovellettavista rajoituksista.

Pykälän 2 momentin 1 kohdan mukaan kuluttaja voi joutua vastaamaan sellaisista oikeustoimista, joita toinen henkilö on tehnyt oikeudettomasti hänen luomistiedoillaan, jos kuluttaja on luovuttanut luomistiedot toiselle. Luovutuksella tarkoitetaan vapaaehtoista hallinnan luovutusta tapahtuipa se missä tarkoituksessa tahansa.

Pykälän 2 momentin 2 kohdan mukaan kuluttaja voi joutua vastuuseen silloin, kun luomistiedot ovat joutuneet niiden käyttöön oikeudettomalle kuluttajan huolimattomuuden vuoksi, eikä huolimattomuus ole lievää. Lähtökohtana on, että allekirjoittaja säilyttää luomistietoja ja niiden käyttöön liittyvää salasanaa tai tunnusta huolellisesti. Huolimattomuuden arvioinnissa tulisi kiinnittää huomiota luomistietojen ja salasanan tai tunnuksen säilyttämistapaan sekä siihen, miten niiden hallinta on menetetty. Huolimattomuuden arvioinnissa tulisi ottaa huomioon myös sähköisen allekirjoituksen käyttötarkoitus sekä mahdolliset laatuvarmenteesta ilmenevät käyttörajoitukset.

Koska laatuvarmenteella varmennetulla ja turvallisella allekirjoituksen luomisvälineellä luodulla kehittyneellä sähköisellä allekirjoituksella voidaan lähtökohtaisesti tehdä mikä tahansa oikeustoimi, saattaa myös mahdollisilla väärinkäytöksillä olla laajat vaikutukset. Toisaalta laatuvarmenteeseen merkityillä käyttörajoituksilla saattaa olla merkitystä kuluttajan huolimattomuutta arvioitaessa. Mitä vähemmän käyttörajoituksia laatuvarmenteeseen on merkitty, sitä huolellisemmin voidaann odottaa kuluttajan luomistietoja säilyttävän. Huolimattomuutta arvioitaessa tulee ottaa huomioon myös, että allekirjoituksen käyttö liittyy periaatteessa useisiin päivittäisiin toimenpiteisiin, joten luomistietoja tulee voida kuljettaa allekirjoittajan mukana. Toimikorttia, jolla luomistiedot sijaitsevat tulee voida kuljettaa esimerkiksi lompakossa.

Lisäksi allekirjoittajan huolimattomuutta arvioitaessa tulee erityisesti ottaa huomioon hänen toimintansa luomistietojen käytön suojaukseen liittyvän salasanan tai tunnuksen säilyttämisessä huolellisesti. Salasanaa tai tunnusta ei saa säilyttää luomistietojen yhteydessä. Ratkaisevan tärkeää luomistietojen oikeudettoman käytön estämisessä tuleekin olemaan allekirjoittajan huolellinen toiminta salasanan tai tunnuksen säilyttämisessä.

Pykälän 2 momentin 3 kohdassa säädettäisiin tilanteista, joissa allekirjoituksen luomistiedot ovat joutuneet pois allekirjoittajan hallusta siten, että allekirjoittajan ei voida katsoa lainkaan syyllistyneen huolimattomuuteen tai että hänen huolimattomuutensa on ollut lievää. Momentin 3 kohdan mukaan allekirjoittaja voi joutua vastaamaan luomistietoja oikeudettomasti käyttäneen henkilön tekemistä oikeustoimista aiheutuneista vahingoista vain, jos hän menetettyään luomistietojen hallinnan on laiminlyönyt viipymättä pyytää laatuvarmenteen peruuttamista siten kuin 36 §:n 1 momentissa säädetään. Ehdotetun 3 kohdan säännöksellä pyritään suojaamaan kuluttajaa, jonka voidaan katsoa syyllistyneen korkeintaan lievään huolimattomuuteen luomistietojen joutumisessa niiden käyttöön oikeudettomalle henkilölle. Allekirjoittaja vastaa 3 kohdan tarkoittamissa tapauksissa luomistietojen oikeudettomasta käytöstä aiheutuneista vahingoista siitä hetkestä alkaen, jolloin allekirjoittajan voidaan katsoa laiminlyöneen 36 §:n 1 momentissa tarkoitetun laatuvarmenteen peruuttamispyynnön. Lähtökohtana on, että allekirjoittaja pyytää laatuvarmenteen peruuttamista välittömästi havaittuaan luomistietojen katoamisen.

Ehdotettua pykälää vastaavaa säännöstä ei sisälly sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin. Pykälän säännöksillä on tarpeen kansallisella tasolla täsmentää riskinjakoa allekirjoituksen luomistietojen oikeudettomassa käytössä. Pykälä vastaa sähköisistä allekirjoituksista annetun lain 17 §:ää.

41 §. *Laatuvarmenteita tarjoavan varmentajan vahingonkorvausvastuu.* Sähköisten allekirjoitusten käyttö perustuu suurelta osin luottamukseen varmentajan toimintaa kohtaan. Sähköisten allekirjoitusten käytön yhteydessä mahdollisesti syntyvistä ongelmatilanteista ja niiden syistä saattaa muiden kuin varmentajan olla käytännössä vaikea esittää näyttöä. Vahinkoa kärsineen voi olla vaikeaa tai jopa mahdotonta näyttää varmentajan toiminnassa tapahtunutta huolimattomuutta tai laiminlyöntiä. Tästä syystä sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi edellyttää laatuvarmenteita yleisölle tarjoavan varmentajan vastuun säätämistä tavanomaista huolimattomuusvastuuta ankarammaksi. Nimenomainen säännös korvausvastuun perusteista helpottaa myös varmentajan mahdollisuuksia arvioida toimintaansa liittyviä vahingonkorvausriskejä ja järjestää toimintansa niiden mukaisesti.

Pykälän säännökset koskevat ainoastaan varmentajan vahingonkorvausvastuuta suhteessa laatuvarmenteeseen luottaneeseen henkilöön, joka ei ole sopimussuhteessa varmentajaan. Varmentajan ja allekirjoittajan välisessä suhteessa vahingonkorvausvastuu määräytyy lähtökohtaisesti yleisten sopimusoikeudellista korvausvastuuta koskevien periaatteiden mukaan. Allekirjoituksen luomistietojen oikeudettoman käytön tapauksissa riskin jakautumisesta varmentajan ja allekirjoittajan välillä säädetään erikseen ehdotetussa 40 §:ssä.

Pykälän 1 momentissa säädetään seikoista, joita laatuvarmenteita tarjoavan varmentajan tavanomaista huolimattomuusvastuuta ankarampi korvausvastuu koskee. Varmentaja on velvollinen korvaamaan 1-5 kohdissa luetelluista seikoista johtuvan vahingon, ellei varmentaja pysty näyttämään, että vahinko ei ole aiheutunut sen omasta tai sen apunaan käyttämän henkilön huolimattomuudesta. Henkilöllä tarkoitetaan sekä luonnollista henkilöä että oikeushenkilöä. Varmentajan korvausvastuu koskee kaikkea vahingon aiheuttaneeseen seikkaan syy-yhteydessä olevaa vahinkoa vahingon ennakoitavuutta koskevien yleisten vahingonkorvausoikeudellisten periaatteiden mukaisesti.

Pykälän 1 momentin 1 ja 2 kohdan mukaan laatuvarmenteita tarjoava varmentaja on velvollinen korvaamaan vahingon, joka on aiheutunut siitä, että laatuvarmenteeseen merkityt tiedot ovat myöntämishetkellä olleet virheellisiä tai että laatuvarmenteessa ei ole 30 §:n 2 momentissa mainittuja tietoja. Myöntämishetkellä tarkoitetaan ajankohtaa,

jolloin laatuvarmenne luovutetaan hakijan käyttöön. Allekirjoittajan edun mukaista on viipymättä ilmoittaa myöntämishetkellä ilmoitetuissa tiedoissa tapahtuvista muutoksista varmentajalle, jotta tämä voi myöntää uuden, muuttuneita tietoja vastaavan laatuvarmenteen.

Ehdotetun 1 momentin 3 kohdan mukaan laatuvarmenteita tarjoava varmentaja vastaisi vahingoista, jotka ovat aiheutuneet siitä, että laatuvarmenteessa yksilöidyllä henkilöllä ei varmenteen myöntämisajankohtana ole ollut todentamistietoja vastaavia luomistietoja. Sähköisen allekirjoituksen luotettavuus perustuu siihen, että allekirjoituksen luomistietoja käyttää vain se henkilö, jonka nimi on laatuvarmenteessa. Ongelmatilanteissa laatuvarmenteita tarjoavan varmentajan on korvausvastuun välttämiseksi pystyttävä osoittamaan, että se on menetellyt huolellisesti tarkistaessaan 35 §:n 1 momentissa tarkoitetulla luotettavalla tavalla henkilöllisyyden ja että se on luovuttanut allekirjoituksen luomistiedot niiden hallintaan oikeutetulle henkilölle. Jos laatuvarmenteen hakija tai joku muu kuin varmentaja luo allekirjoituksen luomistiedot, joita vastaavat todentamistiedot merkitään laatuvarmenteeseen, tulee varmentajan ennen laatuvarmenteen luovuttamista varmistaa, että hakijalla on hallinnassaan allekirjoituksen luomistiedot.

Ehdotetun 1 momentin 4 kohdan mukaan varmentaja vastaa vahingoista, jotka aiheutuvat siitä, että luomistietoja ja todentamistietoja ei voi käyttää yhdessä. Allekirjoituksen luomistietojen ja allekirjoituksen todentamistietojen yhteentoimivuus on välttämätön edellytys sähköisen allekirjoituksen käytölle. Kohdassa säädetään vain niistä tilanteista, joissa laatuvarmenteita tarjoava varmentaja tai tämän apunaan käyttämä henkilö on luonut sekä luomis- että todentamistiedot. Jos laatuvarmenteen hakija on itse luonut tai muutoin hankkinut allekirjoituksen luomis- ja todentamistiedot ja hankkii vain muita palveluita varmentajalta, varmentaja ei vastaisi tietojen yhteentoimivuudesta.

Ehdotetun 1 momentin 5 kohdan mukaan varmentaja vastaa laatuvarmenteeseen luottaneelle vahingoista, jos laatuvarmennetta ei ole peruutettu 36 §:ssä säädetyllä tavalla. Kolmannen osapuolen eli sähköisen allekirjoituksen todentajan tulee voida luottaa varmenteen olevan voimassa ja hallintaan oikeutetulla henkilöllä, jollei varmennetta ole peruuutettu ja merkitty sulkulistalle, jota varmentaja ylläpitää peruutetuista laatuvarmenteista. Allekirjoituksen luomistietojen kadotessa tai tuhoutuessa laatuvarmenteen viipymätön peruuttaminen ehkäisee tehokkaasti vahinkojen syntymistä. Kohdassa säädetty korvausvastuu koskee allekirjoittajan tekemän varmenteen peruuttamispyynnön saapumisen jälkeistä aikaa. Ennen peruuttamispyynnön saapumista varmentajalle allekirjoittaja vastaa aiheutuneista vahingoista 40 §:ssä säädetyin rajoituksin.

Kuten jo edellä on todettu, on sulkulistan luotettavuus keskeinen tekijä sähköisen allekirjoituksen ja varmenteiden käytölle. Tästä johtuen voidaan katsoa, että huolellisesti toimivan laatuvarmenteeseen luottavan osapuolen intressissä on varmistua sulkulistan tarkistamisesta. Koska laatuvarmenteita yleisölle tarjoava varmentaja vastaa luottavalle osapuolelle vain peruuttamisen tekemisestä, eli laatuvarmenteen merkitsemisestä sulkulistalle, laatuvarmenteeseen luottavan osapuolen huolellisuuden piiriin lähtökohtaisesti jää sulkulistan tarkistaminen. Sulkulistan tarkistus on kuitenkin mahdollista tehdä myös automaattisesti varmentajan ja luottavan osapuolen käyttämien järjestelmien välillä, jolloin luottava osapuoli ei henkilökohtaisesti käy tarkistamassa sulkulistaa. Tällöinkin on luottavan osapuolen intressissä varmistua käyttämänsä järjestelmän ylläpitäjältä, että sulkulistatarkistus tehdään aina automaattisesti. Käytettävistä teknisistä sovelluksista riippuen voidaan siis käyttää erilaisia menetelmiä sulkulistan tarkistamiseksi, mutta laatuvarmenteeseen luottavan osapuolen tulisi lähtökohtaisesti huolehtia siitä, että sulkulista tarkistetaan, jotta hän voi varmistua laatuvarmenteen voimassaolosta.

Ehdotetun 2 momentin mukaan laatuvarmenteita tarjoava varmentaja vapautuu 1 momentissa tarkoitetusta vastuusta näyttämällä, että vahinko ei ole aiheutunut varmentajan tai sen apunaan käyttämän henkilön huolimattomuudesta. Tämä niin sanottu presumoitu tuottamusvastuu merkitsee poikkeusta siitä vahingonkorvausoikeudellisesta pääsäännöstä, että vahinkoa kärsinyt on vel-

vollinen näyttämään vahingon aiheuttajan toimineen huolimattomasti. Momentissa säädetty käännetty todistustaakka koskee ainoastaan vastuun perustetta, joten vahinkoa kärsinyt on velvollinen normaaliin tapaan esittämään näytön varmentajan toiminnan ja kärsimänsä vahingon välisestä syy-yhteydestä.

Ehdotetun 3 momentin mukaan laatuvarmenteita tarjoava varmentaja ei vastaa vahingosta, joka on aiheutunut laatuvarmenteeseen sisältyvän käyttörajoituksen vastaisesta käytöstä. Laatuvarmenteen käyttöä voidaan rajoittaa eri syistä. Laatuvarmenne voi olla esimerkiksi käytettävissä vain tietynlaisiin oikeustoimiin tai ainoastaan tietyn rahallisen arvon alittaviin oikeustoimiin. Esimerkiksi työnantaja voi rajoittaa työntekijälle annetun laatuvarmenteen käytön koskemaan vain työtehtäviä.

Varmentajan riskienhallinnan kannalta on tärkeää, että se ei joudu vastuuseen käyttörajoitusten vastaisesta käytöstä. Edellytyksenä käyttörajoituksien tehokkuudelle suhteessa kolmansiin osapuoliin on, että rajoitus tulee kolmansien tietoon. Käyttörajoituksien tulee ehdotetun 30 §:n 2 momentin 8 kohdan mukaan näkyä laatuvarmenteessa, joten niistä välittyisi aina tieto myös allekirjoituksen todentajalle.

Laatuvarmenteita yleisölle tarjoavan varmentajan toiminnasta aiheutuvaan korvausvastuuseen sovelletaan ehdotetun lain ohella vahingonkorvauslakia (412/1974). Tästä ehdotetaan selvyyden vuoksi säädettäväksi ehdotetussa 4 momentissa.

Siltä osin kuin laatuvarmenteita yleisölle tarjoavan varmentajan vastuu perustuu 1 momentissa lueteltuihin seikkoihin, vahingonkorvauslaista tulevat sovellettavaksi muun muassa vahingonkorvauksen kohtuullistamista, vahinkoa kärsineen myötävaikutusta, useiden vahingosta vastuussa olevien yhteisvastuuta sekä korvausvaatimuksen vanhentumista koskevat säännökset.

Muilta osin laatuvarmenteita tarjoavien varmentajien korvausvastuu suhteessa sellaiseen laatuvarmenteeseen luottaneeseen tahoon, johon varmentaja ei ole sopimussuhteessa, määräytyy kokonaisuudessaan vahingonkorvauslain ja yleisten vahingonkorvausoikeudellisten periaatteiden mukaan.

Ehdotetussa 5 momentissa säädetään myös ehdotetun pykälän korvaussääntelyn ulottamisesta varmenteen laatuvarmenteeksi takaavaan varmentajaan. Sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi edellyttää jäsenvaltioiden varmistavan ainakin, että ehdotetun 1 momentin 1-4 kohdassa mainittu korvausvastuu ulotetaan myös varmenteen yleisölle laatuvarmenteeksi takaaviin varmentajiin. Lakiesityksessä ehdotetaan 1 momentin 1-4 kohtien vastuuperusteiden lisäksi myös 5 kohdan varmenteen peruuttamatta jättämistä koskevan vastuuperusteen soveltamista varmenteen yleisölle laatuvarmenteeksi takaaviin varmentajiin. Väärinkäsitysten välttämiseksi vaikealla teknisellä toimialalla on perusteltua säätää varmenteen takaajan vastuu kokonaisuudessaan yhdenmukaiseksi laatuvarmenteita yleisölle tarjoavien varmentajien vastuun kanssa.

Pykälällä pannaan täytäntöön direktiivin 6 artikla, joka käsittelee laatuvarmenteita yleisölle tarjoavien varmentajien tai varmenteen yleisölle laatuvarmenteeksi takaavien varmentajien vahingonkorvausvastuuta laatuvarmenteeseen perustellulla tavalla tukeutuvalle. Artiklassa käytetty käsite "perustellulla tavalla tukeutuva" (who reasonably relies on), on Suomen voimassa olevassa vahingonkorvauslaissa ja -käytännössä tuntematon käsite. Ehdotetussa pykälässä säädetäänkin laatuvarmenteita yleisölle tarjoavan varmentajan vahingonkorvausvastuusta "laatuvarmenteeseen luottaneelle" aiheutuneen vahingon osalta. Koska direktiivin 6 artiklassa asetetaan jäsenvaltioille ainoastaan minimivaatimukset, on ehdotetun pykälän mukainen kansallinen sääntely mahdollista. Direktiivin minimisääntelystä johtuen on myös mahdollista kansallisesti säätää edellä käsitellyn 1 momentin 5 kohdan vastuuperusteen soveltamisesta myös varmenteen laatuvarmenteeksi takaaviin varmentajiin, vaikka direktiivi ei tätä välttämättä edellyttäisikään. Säännös vastaa voimassa olevan sähköisistä allekirjoituksista annetun lain 16 §:ää.

5 luku. Viranomaisvalvonta

42 §. *Yleinen ohjaus ja valvonta.* Ehdotetun pykälän 1 momentin mukaan liikenne- ja viestintäministeriön yleiseen ohjaus- ja kehit-

tämisvaltaan kuuluisi sähköisen allekirjoituksen lisäksi myös sähköinen tunnistaminen. Voimassa olevan sähköisistä allekirjoituksista annetun lain 22 §:n 1 momentin säännöksen mukaan varmennetoiminnan yleinen ohjaus ja kehittäminen kuuluu liikenne- ja viestintäministeriölle. Ehdotettu muutos nykytilaan verrattuna olisi luonnollinen seuraus ehdotetun lain muuttuneesta soveltamisalasta.

Kuten sähköisten allekirjoitustenkin osalta sähköisen tunnistamisen yleinen ohjaus ja kehittäminen tarkoittaa lähinnä sähköiseen tunnistamiseen liittyvien säädöshankkeiden valmistelua sekä sähköiseen tunnistamiseen liittyvään Euroopan yhteisöjen toimielimien toimintaan osallistumista.

Pykälän 2 momentin mukaan Viestintäviraston tehtävänä on valvoa tämän lain noudattamista lukuun ottamatta 1 §:n 3 momentissa tarkoitettua toimintaa. Viestintävirasto antaa tarvittaessa teknisiä määräyksiä tunnistuspalveluntarjoajien sekä laatuvarmenteita tarjoavien varmentajien ja toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista. Määräyksiin liittyy ainoastaan vähäistä harkintavallan käyttöä ja niillä tarkennetaan tarvittaessa palveluntarjoajien toimintaan ehdotetuissa 3 ja 4 luvuissa kohdistettujen vaatimusten sisältöä. Mahdollisuus antaa tarkempia teknisiä määräyksiä on tarpeen sen vuoksi, että alan voidaan olettaa kehittyvän tulevina vuosina jatkuvasti.

Viestintävirasto on antanut sähköisistä allekirjoituksista annetun lain vastaavan säännöksen nojalla 29 päivänä tammikuuta 2003 määräyksen yleisölle laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista (Viestintävirasto 8/2003 M). Myös tämä määräys on 50 §:n 2 momentin mukaisesti voimassa siihen saakka, kunnes uusi määräys tämän lain nojalla on annettu.

Ehdotetun 3 momentin mukaan tietosuojavaltuutettu valvoo ehdotetussa laissa annettujen henkilötietojen käsittelyä koskevien säännösten noudattamista.

Pykälän 4 momentissa todetaan, että kuluttaja-asiamiehen tehtävänä on valvoa kuluttajasuhteissa sellaista 1 §:n 3 momentissa tarkoitettua toimintaa, jossa yhteisö käyttää omaa vahvaa sähköistä tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan. Kyseessä on siis toiminta, joka ei varsinaisesti kuulu lain soveltamisalaan. Ehdotetun 1 §:n 2 momentin toisen virkkeen mukaan tällaiseen toimintaan sovelletaan kuitenkin 3 §:n, 20 §:n 1 momentin, 21-22 §:n, 23 §:n 1 momentin, 25 §:n 1 momentin ja 2 momentin jälkimmäisen virkkeen sekä 27 §:n 1 momentin, 2 momentin 1 kohdan ja 3 momentin säännöksiä. Säännös on seurausta tarpeesta suojella kuluttajia myös tällaisten palveluiden kyseessä ollen. Tämän johdosta on luonnollista, että säännöstä valvoo juuri kuluttajaviranomainen. Kuluttaja-asiamiehellä olisi asiassa toimivalta myös yleisten valtuuksiensa nojalla, mutta asiasta on syytä ottaa lakiin selkeä säännös.

Lain 42-49 §:llä pannaan myös täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 3 artiklan 3 kohta. Ehdotettu 42 § vastaa osittain sähköisistä allekirjoituksista annetun lain 22 §:ää.

43 §. *Tiedonsaantioikeus.* Pykälässä säädetään valvovien viranomaisten tiedonsaantioikeuksista. Pykälän 1 momentissa todetaan, että Viestintävirastolla on oikeus salassapitosäännösten estämättä saada tunnistuspalvelun tarjoajilta ja laatuvarmenteita tarjoavilta varmentajilta sekä heidän apunaan toimivilta henkilöiltä 42 §:ssä säädettyjen tehtävien suorittamiseksi tarpeelliset tiedot. Henkilöillä tarkoitetaan sekä luonnollisia että oikeushenkilöitä.

Pykälän 2 momentin mukaan tietosuojavaltuutetulla on tehtäväänsä suorittaessaan henkilötietolaissa tarkoitetut tiedonsaantioikeudet. Henkilötietolain 39 §:n 1 momentin mukaan tietosuojavaltuutetulla on salassapitosäännösten estämättä oikeus saada tiedot käsiteltävistä henkilötiedoista sekä kaikki tiedot, jotka ovat tarpeen henkilötietojen käsittelyn lainmukaisuuden valvonnassa.

Säännös vastaa muutoin sähköisistä allekirjoituksista annetun lain 23 §, mutta siihen on lisätty tietosuojavaltuutetun oikeus saada niin ikään tehtäviensä suorittamisen kannalta tarpeelliset tiedot.

44 §. *Viranomaisten välinen yhteistyö ja oikeus luovuttaa tietoja.* Pykälässä annetaan Viestintävirastolle ja tietosuojavaltuutetulle oikeus luovuttaa viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetystä salassapitovelvoitteesta poiketen

Finanssivalvonnalle sellaisia tietoja, jotka ovat tarpeen sen tehtävien suorittamiseksi.

Viestintävirastolla on tarvittava tekninen tietämys sähköiseen tunnistamiseen ja sähköiseen allekirjoitukseen liittyvistä seikoista. Sen johdosta varsinaisen tunnistuspalveluiden ja sähköisen allekirjoittamisen palveluiden tulee olla nimenomaan Viestintäviraston valvottavia. Sen sijaan sitä, kuinka pankit käyttävät pankkitunnisteita omassa pankkitoiminnassaan, valvoo Finanssivalvonta.

Finanssivalvonnan ei ole mahdollista eikä kokonaisuuden kannalta järkevää hankkia vahvaa sähköistä tunnistamista ja sähköisiä allekirjoituksia koskevaa tietämystä oman valvontavastuunsa täyttämiseksi. Tämän johdosta ehdotetussa pykälässä on tarpeen säätää viranomaisten välisestä tiedonkulusta asiassa.

Viranomaisten toiminnan julkisuudesta annetun lain 24 §:ssä on 32-kohtainen lista salassa pidettävistä asioista. Näistä saattaisivat tulla kysymykseen esimerkiksi 7 kohdassa säädetyt tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat tiedot sekä 20 kohdassa tarkoitetut asiakirjat, jotka sisältävät tietoja yksityisestä liike- tai ammattisalaisuudesta.

Ehdotetun 2 momentin mukaan Viestintäviraston ja tietosuojavaltuutetun on tämän lain mukaisia tehtäviä hoitaessaan toimittava tarvittaessa tarkoituksenmukaisessa yhteistyössä Finanssivalvonnan, Kilpailuviraston ja Kuluttajaviraston kanssa. Vastaavia viranomaisten väliseen yhteistyön velvoittavia säännöksiä löytyy lainsäädännöstä runsaasti.

Ehdotettu pykälä korvaa sähköisistä allekirjoituksista annetun lain vaitiolovelvollisuutta koskevan 25 §:n. Muutos on seurausta siitä, että ehdotetussa laissa ei katsota miltään osin olevan kyse julkisen vallan käytöstä.

45 §. *Hallintopakkokeinot.* Pykälän 1 momentin mukaan Viestintävirasto voi lain noudattamista valvovana viranomaisena velvoittaa lakia tai sen nojalla annettuja määräyksiä rikkoneen valvottavan tahon korjaamaan virheensä tai laiminlyöntinsä. Viestintävirasto voi asettaa päätöksensä tehosteeksi uhkasakon, toiminnan keskeyttämisuhan tai teettämisuhan. Velvoittamispäätös ja tehostetta koskeva päätös voidaan tehdä samanaikaisesti tai erikseen.

Viestintäviraston valvontavalta kohdistuu tunnistuspalvelun tarjontaan, johon saattaa liittyä myös sähköisten allekirjoituspalveluiden tarjontaa, laatuvarmenteiden tarjontaan sekä mahdollisesti myöhemmin nimettävien tarkastuslaitosten toimintaan. Toiminnan keskeyttämisuhka voi koskea lain soveltamisalaan kuuluvan toiminnan osaa tai koko toimintaa. Tehosteeksi asetetun uhkan tulee aina olla suhteessa valvottavan tahon virheen tai laiminlyönnin vakavuuteen. Uhkasakon tai teettämisuhan tulee olla ensisijainen tehokeino velvoitteiden täyttämisessä. Toiminnan keskeyttämisuhkaa tulee pääsääntöisesti käyttää vain tilanteessa, jossa valvottava taho ei ole korjannut virhettään tai laiminlyöntiään uhkasakosta tai teettämisuhasta huolimatta.

Viestintäviraston tunnistuspalveluita tarjoaviin kohdistama valvonta on varsin pitkälle jälkikäteistä valvontaa.

Pykälän 2 momentissa on tavanomainen säännös teettämällä suoritetusta toimenpiteestä valtiolle aiheutuneiden kustannusten suorittamisesta ja perimisestä.

46 §. *Tarkastusoikeus.* Pykälässä säädetään tunnistuspalvelun tarjoajan ja laatuvarmenteita tarjoavan varmentejan ja niiden tarjoamien palveluiden tarkastamisesta. Tarkastukset eroavat olennaisella tavalla toisistaan. Tarkastuksen tekee tai teettää Viestintävirasto.

Pykälän 1 momentin mukaan Viestintävirastolla on oikeus tehdä tai teettää tunnistuspalveluntarjoajaa ja sen tarjoamaa palvelua koskeva tarkastus, jos sillä on syytä epäillä tämän lain tai sen nojalla annettujen määräysten noudattamista. Määräyksillä tarkoitetaan Viestintäviraston tämän lain nojalla antamia määräyksiä. Viestintäviraston ehdotetun 3 luvun säännöksiin kohdistuva valvontavalta toteutuu siten pääsääntöisesti jälkikäteisenä valvontana.

Viestintävirasto toteuttaa valvontavaltaansa pääosin edellä ehdotetussa 45 §:ssä säädettyjen hallintopakkokeinojen avulla. Keinovalikoiman uusin ja järein osa olisi ehdotetussa momentissa säädetty oikeus tehdä tai teettää vahvan sähköisen tunnistamispalve1un tarjoajaa ja sen toimintaa koskeva tarkastus, mikäli prosessin kuluessa syntyisi epäilys, että lain säännöksiä ei ole noudatettu. Tämä tar-

kastus ei siis tapahdu vuosittain tai varmuuden vuoksi. Viestintävirasto voisi kaavaillun säännöksen mukaan myös teetättää työn ulkopuolisella. Rikkomuksen on oltava olennainen, jotta 1 tässä momentissa tarkoitettuun tarkastukseen voidaan ryhtyä.

Pykälän 2 momentin nojalla Viestintävirasto tekee tai teettää laatuvarmenteita tarjoavaa varmentajaa ja sen tarjoamaa palvelua koskevan tarkastuksen vuosittain. Laatuvarmenteita tarjoavia varmentajia ja niiden toimintaa tarkastettaisiin siten säännönmukaisesti joka vuosi ilman, että niiden toiminnassa olisi syytä epäillä puutteita tai laiminlyöntejä. Ehdotettu säännös vastaa nykyistä tilannetta.

Pykälän 3 momentin mukaan Viestintävirasto määrää tarkastajan toimittamaan tarkastuksen. Tarkastusta toimittavalla henkilöllä on oikeus tutkia palveluntarjoajien tai niiden apunaan käyttämien henkilöiden laitteet ja ohjelmistot, joilla voi olla merkitystä tämän lain tai sen nojalla annettujen määräysten noudattamisen valvonnassa.

Pykälän 4 momentissa säädetään, että vahvan sähköisen tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien tai niiden apunaan käyttämien henkilöiden on tarkastusta varten päästettävä edellä 3 momentissa tarkoitettu tarkastaja muihin kuin kotirauhan piiriin kuuluviin valmistus-, liike- ja varastotiloihin. Kyseinen velvollisuus ei koskisi kotirauhan piiriin kuuluvia tiloja.

Pykälän 5 momentissa säädetään virka-avusta. Sen mukaan Viestintävirasto voi saada virka-apua poliisilta tarkastuksen suorittamista varten. Tunnistuspalvelun tarjoajan tai laatuvarmenteita tarjoavan varmentajan apunaan käyttämällä henkilöllä tarkoitetaan tässä pykälässä sekä luonnollista henkilöä että oikeushenkilöä.

Pykälän 6 momentissa todetaan, että tietosuojavaltuutetulla on tehtäväänsä suorittaessaan henkilötietolaissa tarkoitetut tarkastusoikeudet. Henkilötietolain 39 §:n 2 momentin mukaan tietosuojavaltuutetulla on oikeus tarkastaa henkilörekistereitä. Tarkastuksen toimittamista varten tietosuojavaltuutetulla ja tarkastuksessa käytettävällä asiantuntijalla on oikeus päästä sellaisiin rekisterinpitäjän ja hänen toimeksiannostaan toimivan hallussa oleviin huoneistoihin, joissa henkilötietoja käsitellään tai henkilörekistereitä pidetään, sekä saada käytettäväkseen tarkastuksen toimittamisessa tarvittavat tiedot ja laitteet. Kotirauhan piiriin kuuluvassa tilassa tarkastuksen saa toimittaa vain, jos esillä olevassa tapauksessa on olemassa yksilöity syy epäillä henkilötietojen käsittelyä koskevia säännöksiä rikotun tai rikottavan. Tarkastus on toimitettava niin, ettei siitä aiheudu rekisterinpitäjälle tarpeettomasti haittaa ja kustannuksia.

Ehdotettu säännös vastaa osittain sähköisistä allekirjoituksista annetun lain 24 §:ää.

47 §. *Viestintävirastolle maksettavat maksut.* Pykälän 1 momentin mukaan 10 §:ssä tarkoitetun ilmoituksen tehneen tunnistuspalvelun tarjoajan tai niiden yhteenliittymän on maksettava Viestintävirastolle vuosittain valvontamaksu, jonka palveluntarjoajakohtainen suuruus on 12 000 euroa. Ilmoituksen tehneen palveluntarjoajien yhteenliittymän tarvitsee siis maksaa ainoastaan yksi maksu.

Kuten edellä ehdotetun 46 §:n osalta todettiin, Viestintäviraston vahvan sähköisen tunnistuspalvelun tarjoajiin kohdistama valvonta on varsin pitkälle jälkikäteistä valvontaa. Vuotuinen tarkastusmaksu koostu siitä, että Viestintävirasto joutuu pitämään yllä vahvaa sähköistä tunnistamista koskevaa tietotaitoaan jatkuvasti sekä vastaamaan tunnistuspalvelua käyttävien palveluntarjoajien sekä tunnistusvälineiden haltijoiden mahdollisiin yhteydenottoihin.

Ehdotetussa momentissa säädetty valvontamaksu olisi kaikille samansuuruinen palveluntarjoajan liikevaihdosta ja liikkeelle laskettujen tunnistusvälineiden määrästä riippumatta. Näin järjestelmä ei rankaisisi markkinoilla olevien tunnisteiden määrän kasvusta. Kyseinen summa olisi toimijoiden kannalta erittäin kohtuullinen. Se on niin pieni, että jos toimija ei pysty sitä maksamaan, ei myöskään täyttyne 13 §:n 2 momentin säännös siitä, että palveluntarjoajalla on oltava riittävät taloudelliset voimavarat toiminnan harjoittamiseksi.

Lisäksi 10 §:ssä tarkoitetun ilmoituksen tehneen tunnistuspalvelun tarjoajan tai palveluntarjoajien yhteenliittymän on suoritettava Viestintävirastolle rekisteröimismaksu, jonka suuruus on 5000 euroa. Rekisteröintiprosessi on se vaihe, josta Viestintävirastolle valvovana viranomaisena aiheutuu eniten työtä.

Tämän johdosta rekisteröinnistä on syytä säätä erillinen maksu. Se suoritetaan ainoastaan kerran.

Pykälän 2 momentin mukaan laatuvarmenteita tarjoavan varmentajan on suoritettava Viestintävirastolle vuosittain tarkastusmaksu, jonka suuruus on 40 000 euroa. Voimassa olevan varmennemaksun määrä on perustunut liikkeelle laskettujen laatuvarmenteiden määrään. Perustetta on arvosteltu, sillä sen on katsottu muodostavan esteen liiketoiminnan kehittämiselle. Myös Valtiontalouden tarkastusvirasto on kiinnittänyt tähän asiaan huomiota. Ehdotetussa laissa valvonnan kustannuksia tullee jakamaan muitakin toimijoita, minkä johdosta Väestörekisterikeskuksen osuutta voitaisiin selkeästi laskea. Koska laatuvarmenteita tarjoavien varmentajien toiminta tarkastetaan 46 §:n 2 momentin mukaan vuosittain, on maksun on oltava selvästi suurempi kuin tunnistuspalvelun tarjoajiin kohdistuva maksu. Laatuvarmenteisiin ja laatuvarmentajiin kohdistuu EU:n sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivissä annettu varsin tiukka sääntely. Tämän johdosta on perusteltua, että toiminta tarkastetaan jatkossakin vuosittain.

Pykälän 3 momentissa todetaan, että rekisteröimismaksun ja valvontamaksu vastaavat niitä kustannuksia, jotka aiheutuvat Viestintävirastolle tässä laissa säädettyjen tehtävien hoitamisesta 46 §:n 1 momentissa tarkoitettuja tehtäviä lukuun ottamatta. Valvontamaksu on säännöksen mukaan suoritettava täysimääräisesti myös toiminnan ensimmäisenä vuotena, vaikka toiminta aloitettaisiin kesken vuotta. Valvontamaksua ei palauteta, vaikka palveluntarjoaja lopettaisi toimintansa kesken vuotta.

Pykälän 1 ja 2 momenteissa tarkoitetuille rekisteröimismaksulle ja valvontamaksulle ei ole selkeästi osoitettavissa Viestintävirastolta saatavaa vastiketta. Kyseessä ovat tämän johdosta veronluonteiset maksut, joita koskevan sääntelyn on täytettävä verolainsäädännön vaatimukset. Veronluontoisen maksun osalta sekä maksun perusteen että määrän on oltava lain tasolla säännelty. Pykälän 1, 2 ja 3 momentit täyttävät nämä vaatimukset. Vastaavanlaisia maksuja ovat muun muassa viestintämarkkinamaksu ja tietoturvamaksu.

Pykälän 4 ja 5 momenteissa on lisää säännöksiä maksun täytäntöönpanoon ja perimiseen liittyen. Ehdotetun 4 momentin mukaan rekisteröimismaksun ja valvontamaksun määrää maksettavaksi Viestintävirasto. Viestintäviraston maksun määräämistä koskevaan päätökseen saa hakea muutosta siten kuin 49 §:n 1 momentissa säädetään. Tarkempia säännöksiä maksujen täytäntöönpanosta voidaan antaa liikenne- ja viestintäministeriön asetuksella.

Pykälän 5 momentissa todetaan tyypillisesti, että rekisteröitymismaksu ja valvontamaksu saadaan periä ilman tuomiota tai päätöstä siinä järjestyksessä kuin verojen ja maksujen täytäntöönpanosta annetussa laissa säädetään. Jollei maksuja suoriteta viimeistään eräpäivänä, maksamattomalle määrälle peritään vuotuista viivästyskorkoa korkolain (633/1982) 4 §:n 1 momentissa tarkoitetun korkokannan mukaan. Viivästyskoron sijasta viranomainen voi periä viiden euron suuruisen viivästysmaksun, jos viivästyskoron määrä jää tätä pienemmäksi.

Pykälän 6 momentissa todetaan, että jos tunnistuspalveluntarjoajan toiminta joudutaan 46 §:n 1 momentin nojalla tarkastamaan, palveluntarjoajalta peritään tarkastuksesta aiheutuneet kustannukset valtion maksuperustelain nojalla. Ehdotetun 46 §:n 1 momentissa tarkoitettu tarkastusoikeus on seurausta siitä, että Viestintävirastolle syntyy epäilys, että lain säännöksiä ei ole noudatettu. Tämä tarkastus ei siis tapahdu vuosittain tai varmuuden vuoksi. Tarkastuksen kustannukset tulevat puhtaasti palveluntarjoajan maksettavaksi. Viestintävirasto voi 46 §:n 1 momentin mukaan myös teetättää työn ulkopuolisella.

6 luku. Erinäiset säännökset

48 §. *Rangaistussäännökset.* Ehdotetussa laissa säädetyn palveluntarjoamisen luotettavuuden kannalta keskeistä on henkilötietojen käsittely sekä tunnistuspalveluiden että laatuvarmenteita koskevien palveluiden tarjonnassa. Palveluntarjoajilta edellytetään luotettavaa henkilötietojen käsittelyä. Ehdotettuun lakiin sisältyy useita säännöksiä henkilötietojen käsittelystä.

Ehdotetussa pykälässä viitattaisiin henkilörekisteririkoksesta ja -rikkomuksesta säädettyyn. Kyseessä on informatiivinen viittaus. Säännös vastaa sähköisistä allekirjoituksista annetun lain 26 §:ää.

49 §. *Muutoksenhaku.* Lain nojalla annetusta Viestintäviraston päätöksestä valitetaan ehdotetun 1 momentin mukaan noudattaen, mitä hallintolainkäyttölaissa (586/1996) säädetään. Hallintolainkäyttölain 8 §:n 2 momentin mukaan valitus tehdään hallinto-oikeuteen.

Ehdotetun 2 momentin mukaan Viestintävirasto voi määrätä, että sen antamaa päätöstä on noudatettava jo ennen kuin päätös on lainvoimainen. Valitusviranomainen voi kuitenkin kieltää päätöksen täytäntöönpanon, kunnes valitus on ratkaistu.

Pykälän 3 momentin mukaan muutoksenhausta tietosuojavaltuutetun toiminnan osalta säädetään henkilötietolaissa. Henkilötietolain 45 §:n 1 momentin mukaan myös tietosuojavaltuutetun tekemään päätökseen haetaan muutosta valittamalla noudattaen, mitä hallintolainkäyttölaissa säädetään. Henkilötietolain 45 §:n 2 momentissa on vastaava säännös kuin edellä 2 momentissa Viestintäviraston päätöksen noudattamisesta muutoksenhausta huolimatta.

Säännös vastaa sähköisistä allekirjoituksista annetun lain 22 §:n 4 momenttia. Säännöksen siirtämistä käsillä olevaan pykälään olisi pidettävä säädösteknisesti perusteltuna. Säännöksen sijoituspaikan muutoksella ei muuteta säännöksen sisältöä.

7 luku. Voimaantulo

50 §. *Voimaantulo.* Pykälä sisältää voimaantulosäännöksen. Laki on tarkoitettu tulemaan voimaan 1 päivänä syyskuuta 2009.

Ehdotetun 2 momentin mukaan lailla kumotaan sähköisistä allekirjoituksista annettu laki 14/2003. Viestintäviraston lain nojalla antamat määräykset ovat kuitenkin voimassa siihen saakka, kunnes uudet määräykset tämän lain nojalla on annettu.

Ehdotetussa 3 momentissa todetaan tavanomaisella tavalla, että ennen tämän lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimiin.

51 §. *Siirtymäsäännös.* Pykälän 1 momentin mukaan vahvan sähköisen tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle 10 §:ssä tarkoitettu ilmoitus kuuden kuukauden kuluessa lain voimaan tulosta. Sinä aikana vahvana sähköisen tunnistuspalveluna ja tunnistuspalvelun tarjoajana pidetään sellaista 1 §:n soveltamisalaan kuuluvaa sähköistä tunnistuspalvelua ja sähköisen tunnistuspalvelun tarjoajaa, joka täyttää 2 §:n 1 ja 4 kohdissa tarkoitetut määritelmät. Kyseisenä kuuden kuukauden siirtymäaikana lain säännöksiä ei siis vielä sovelleta. Tietoa ei myöskään ole olemassa keskitetysti siitä, ketkä ovat palveluntarjoajia. Siirtymäaika on kuitenkin välttämätön sen johdosta, että palveluntarjoajat voivat saattaa palvelunsa vastaamaan lain vaatimuksia, mikä on edellytyksenä 10 §:n mukaisen ilmoituksen tekemiselle.

Pykälän 2 momentin mukaan ennen tämän lain voimaan tuloa liikkeelle laskettuja tunnistusvälineitä pidetään vahvan sähköisen tunnistamisen välineinä sen jälkeen, kun tunnistuspalvelua tarjoava palveluntarjoaja on tehnyt 10 §:ssä tarkoitetun ilmoituksen. Käytännössä tämä tarkoittaa erityisesti siitä, että voimassa olevat pankkitunnisteet ovat lain mukaisia vahvoja sähköisiä tunnistusvälineitä sen jälkeen, kun niitä liikkeelle laskeva pankki on tehnyt 10 §:n mukaisen ilmoituksen Viestintävirastolle. Kyseessä on käytännön sanelema ratkaisu, sillä pankkitunnisteita on laskettu liikkeelle yli neljä miljoonaa. Jos niiden käyttöä ei voitaisi siirtymäsäännöksen avulla jatkaa kuten tähänkin saakka esimerkiksi julkisen sektorin sähköisiin palveluihin tunnistauduttaessa, merkitsisi tämä todella suurta takaiskua suomalaiselle tietoyhteiskuntakehitykselle.

Pykälän 2 momentin mukaan palvelun ja palveluntarjoajan on ilmoitusta tehtäessä täytettävä kaikki tämän lain tunnistuspalvelulle ja tunnistuspalvelun tarjoamiselle asetetut säännökset lukuun ottamatta 17 §:ää. Kaikki muut edellytykset on siis täytettävä, mukaan lukien 20 §:n 3 momentissa edellytettävä tunnistusvälineen henkilökohtaisuus.

Pykälän 3 momentti sisältää säännöksen sellaista tilannetta varten, jossa tunnistuspalvelun tarjoajat ovat tehneet 17 §:n 2 momentissa tarkoitetun sopimuksen mahdollisuudesta luottaa toistensa tekemään ensitunnistami-

seen, eikä ensitunnistamisessa käytetyt tunnistusvälineet liikkeelle laskenut palveluntarjoaja teekään 10 §:ssä tarkoitettua ilmoitusta kuuden kuukauden siirtymäajan kuluessa. Toisen palveluntarjoajan tunnistusvälineisiin luottaneen tunnistuspalvelun tarjoajan on tehtävä ensitunnistaminen tällä tavoin liikkeelle laskettujen tunnistusvälineiden osalta 17 §:ssä tarkoitetulla tavalla viivyttelemättä.

Pykälän 4 momentissa säädetään siirtymästä laatuvarmenteita tarjoavien varmentajien osalta. Sellaisen laatuvarmenteita tarjoavan varmentajan, joka on tehnyt sähköistä allekirjoituksista annetun lain 9 §:n 1 momentin mukaisen ilmoituksen ja jatkanut toimintaansa keskeytyksettä tämän lain voimaan tuloon saakka, ei tarvitse tehdä uutta ilmoitusta 32 §:n 1 momentin mukaisesti. Laatuvarmenteita tarjoava varmentaja voi tällöin antaa Viestintävirastolle vapaamuotoisen kirjallisen ilmoituksen toimintansa jatkumisesta entisellään. Jos sama palveluntarjoaja tarjoaa myös tunnistuspalveluita, ei säännös luonnollisestikaan vapauta 10 §:n mukaisen ilmoituksen tekemisvelvollisuudesta.

Pykälän 5 momentissa säädetään siirtymäajasta yhden ensitunnistamisessa hyväksyttävän asiakirjan suhteen. Säännöksen mukaan tunnistuspalvelun tarjoaja ja laatuvarmenteita tarjoava varmentaja voivat 31 päivään joulukuuta 2012 asti käyttää ensitunnistamisessa Euroopan talousalueen jäsenvaltion viranomaisen 1 päivänä lokakuuta 1990 jälkeen myöntämää voimassa olevaa ajokorttia.

Valtioneuvosto on antanut 17 päivänä elokuuta 2006 asetuksen poliisin myöntämistä henkilöllisyyden osoittavista asiakirjoista. Sen 1 §:ssä todetaan, että poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja, jotka hyväksytään tunnistamisasiakirjana henkilökorttia ja passia haettaessa, ovat henkilökorttilain (829/1999) 1 §:n 1 ja 3 momentissa tarkoitettu voimassa oleva henkilökortti ja passilain (671/2006) 3 §:ssä tarkoitettu voimassa oleva passi. On luonnollista, että tähän tarkoitukseen ei voida hyväksyä muita asiakirjoja.

Käytännön tilanne Suomessa on tällä hetkellä se, että monissa muissa tilanteissa henkilöllisyyden osoittamiseen ajokortti kelpuutetaan. Noin neljällä miljoonalla suomalaisella on passi tai henkilökortti, mutta niitä ei ole totuttu välttämättä kantamaan mukana.

Omat aiemmat kansalliset kokemuksemme, samoin kuin eräät ulkomaiset esimerkit osoittavat, että olennainen tekijä, joka vaikuttaa ihmisten halukkuuteen hankkia itselleen tunnistusvälineitä, on hankkimisen helppous tai vaikeus. Vaatimus siitä, että ajokortti ei kelpaisi ensitunnistusvälineeksi, voi vaikeuttaa tätä menettelyä. Sellainen henkilö, jolla ei lainkaan ole passia tai henkilökorttia joutuisi esimerkiksi ensin hakemaan itselleen passin tai henkilökortin, jotta voisi saada tunnistusvälineen.

Velvollisuutta hyväksyä ajokorttia ei ole, ja palveluntarjoaja voi valita ne valtiot, joiden viranomaisten myöntämät ajokortit se katsoo voivansa hyväksyä. On selvää, että riskien määrä kasvaa ajokorttien kyseessä ollessa. Palveluntarjoajan on arvioitava nämä riskit, jotka hän ottaa kantaakseen.

Ajokorttien suurimmat ongelmat liittyvät myöntöprosessin ja turvatekijöiden heikkouteen. Ajokorttien käyttö henkilöllisyyden toteamisessa vähentyneekin huomattavasti tulevina vuosina 19 päivänä tammikuuta 2013 mennessä kansallisesti täytäntöön pantavan ajokorttidirektiivin 2006/126/EY sekä uudistuksen kohteena olevan ajokorttien myöntöprosessin myötä.

Edellä sanotun johdosta säännöksessä mahdollistetaan ajokorttien käyttö ensitunnistamisessa, mutta ainoastaan siirtymäajan kuluessa.

Säännöksestä on rajattu pois sellaiset ajokortit, joihin liittyvät suurimmat väärinkäyttöriskit. Pois on rajattu ennen vuoden 1990 syyskuun loppua myönnetyt paperiset ajokortit, joiden väärentäminen on hyvin helppoa. Vuoden 1990 valitseminen rajapyykiksi johtuu siis kansallisista syistä.

1.2 Laki sähköisestä asioinnista viranomaistoiminnassa

3 §. *Muu lainsäädäntö.* Pykälän 2 momenttia ehdotetaan muutettavaksi sen johdosta, että esityksellä laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista kumottaisiin samalla sähköisistä allekirjoituksista annettu laki. Viittaus lakiin sähköisistä allekirjoituksista muutetaan viittauksek-

si lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

9 §. *Kirjallisen muodon ja allekirjoitusvaatimuksen täyttyminen.* Pykälän 1 momenttia muutetaan siten, että sähköisistä allekirjoituksista annetun lain 18 §:n asemesta viitataan vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momenttiin.

16 §. *Päätösasiakirjan sähköinen allekirjoittaminen.* Pykälää muutetaan siten, että sähköisistä allekirjoituksista annetun lain 18 §:n asemesta viitataan vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momenttiin.

18 §. *Todisteellinen sähköinen tiedoksianto.* Pykälän 2 momenttia muutetaan siten, että siihen lisätään nimenomaisesti hyväksyttävänä tunnistautumisvälineenä pidettäväksi laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tarkoitettu tunnistusväline.

1.3 Väestötietolaki

19 §. *Varmennettu sähköinen asiointi.* Pykälän 3 momenttia muutetaan siten, että viittaus lakiin sähköisistä allekirjoituksista muutetaan viittaukseksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

20 §. *Varmennetussa sähköisessä asioinnissa käytettävän varmenteen tiedot.* Pykälää muutetaan siten, että sähköisistä allekirjoituksista annetun lain 7 §:n asemesta viitataan vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 30 §:ään.

1.4 Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä

2 §. *Soveltamisala.* Pykälän 3 momenttia muutetaan siten, että viittaus lakiin sähköisistä allekirjoituksista muutetaan viittaukseksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

9 §. *Asiakirjan sähköinen allekirjoittaminen.* Viittaus lakiin sähköisistä allekirjoituksista muutetaan viittaukseksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

1.5 Laki viestintähallinnosta

2 §. *Viestintäviraston tehtävät.* Pykälän 1 kohta muutetaan siten, että viittaus lakiin sähköisistä allekirjoituksista muutetaan viittaukseksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

1.6 Laki rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä

18 §. *Etätunnistamiseen liittyvä tehostettu tuntemisvelvollisuus.* Pykälän 3 kohtaa muutetaan siten, että siihen lisätään nimenomaisesti hyväksyttävänä henkilöllisyyden todenmisvälineenä pidettäväksi laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tarkoitettu tunnistusväline.

1.7 Varainsiirtoverolaki

56 b §. *Sähköinen asiointi ja allekirjoittaminen.* Muutettavaksi ehdotettavan pykälän 2 momentin voimassa oleva sanamuoto on varsin vaikeasti tulkittava, sillä se edellyttää pykälää yksilöimättä sellaista sähköistä allekirjoitusta, joka täyttää sähköisistä allekirjoituksista annetun lain vaatimukset. Momenttia ehdotetaan muutettavaksi siten, että allekirjoitusta edellyttävät ilmoitukset ja muut asiakirjat olisi sähköisessä asioinnissa varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla. Varmentamisella viitataan tässä momentissa yleisesti erilaisiin Verohallinnon käsillä olevan pykälän 3 momentin mukaan hyväksymiin varmenne- ja tunnistamismenetelmiin.

1.8 Laki verotusmenettelystä

93 a §. *Sähköinen asiointi ja allekirjoittaminen.* Pykälän 2 momenttia ehdotetaan muutettavaksi siten, että allekirjoitusta edellyttävät ilmoitukset ja muut asiakirjat olisi sähköisessä asioinnissa varmennettava vah-

vasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla. Varmentamisella viitataan tässä momentissa yleisesti erilaisiin Verohallinnon käsillä olevan pykälän 3 momentin mukaan hyväksymiin varmenne- ja tunnistamismenetelmiin.

1.9 Arvonlisäverolaki

165 §. Pykälän 3 momenttia ehdotetaan muutettavaksi siten, että allekirjoitusta edellyttävät ilmoitukset ja muut asiakirjat olisi sähköisessä asioinnissa varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla. Varmentamisella viitataan tässä momentissa yleisesti erilaisiin Verohallinnon käsillä olevan pykälän 4 momentin mukaan hyväksymiin varmenne- ja tunnistamismenetelmiin.

1.10 Ennakkoperintälaki

6 a §. *Sähköinen asiointi ja allekirjoittaminen.* Pykälän 2 momenttia ehdotetaan muutettavaksi siten, että allekirjoitusta edellyttävät ilmoitukset ja muut asiakirjat olisi sähköisessä asioinnissa varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla. Varmentamisella viitataan tässä momentissa yleisesti erilaisiin Verohallinnon käsillä olevan pykälän 3 momentin mukaan hyväksymiin varmenneja tunnistamismenetelmiin.

1.11 Veripalvelulaki

11 §. *Luovuttajiin liittyvät tiedot.* Pykälää muutetaan siten, että viittaus lakiin sähköisistä allekirjoituksista muutetaan viittaukseksi lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

2 Tarkemmat säännökset ja määräykset

Liikenne- ja viestintäministeriön asetuksella voitaisiin esityksen 47 §:n 4 momentin mukaan antaa tarkempia säännöksiä 47 §:ssä säädettyjen valvontamaksujen ja rekisteröintimaksujen täytäntöönpanosta.

Esityksen 8 §:n 3 momentin mukaan Viestintävirasto voisi antaa tarvittaessa tarkempia teknisiä määräyksiä 8 §:n 1 momentissa säädettyjen tunnistusmenetelmille asetettavien edellytysten täyttymisestä.

Esityksen 10 §:n 5 momentin mukaan Viestintävirasto voisi antaa valvontatoiminnan kannalta tarpeellisia teknisiä määräyksiä ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Sähköisten allekirjoitusten osalta Viestintävirastolla olisi vastaavat oikeudet antaa määräyksiä kuin sähköisistä allekirjoituksista annetussa laissakin. Ehdotetun 32 §:n 1 momentin mukaan Viestintävirasto voisi antaa valvontatoiminnan kannalta tarpeellisia määräyksiä ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Edelleen lakiehdotuksen 42 §:n 2 momentin mukaan Viestintävirasto antaisi tarvittaessa teknisiä määräyksiä tunnistuspalvelun tarjoajien sekä laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista.

3 Voimaantulo

Lait on tarkoitettu tulemaan voimaan 1 päivänä syyskuuta 2009. Ennen lakien voimaantuloa voitaisiin ryhtyä niiden edellyttämiin toimiin. Vahvaa sähköistä tunnistamista ja sähköisiä allekirjoituksia koskevan lakiehdotuksen 51 §:ssä on siirtymäsäännös, jonka mukaan vahvan sähköisen tunnistuspalvelun tarjoajilla olisi lain voimaan tulosta kuusi kuukautta aikaa tehdä lain 10 §:ssä tarkoitettu ilmoitus Viestintävirastolle.

4 Suhde perustuslakiin ja säätämisjärjestys

4.1 Suhde perustuslakiin

Julkisen vallan käyttö

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle.

Perustuslakivaliokunta on käsitellyt hallintotehtävän antamista muulle kuin viranomaiselle esimerkiksi lausunnoissa PeVL 23/2000 vp (arpajaislaki), PeVL 28/2001 vp (laki yksityisistä turvallisuuspalveluista), PeVL 52/2001 vp (laki rahoitus- ja vakuutusryhmittymien valvonnasta), PeVL 53/2001 vp (laki liikepankeista ja muista luottolaitoksista), PeVL 2/2002 vp (laki sähköisistä allekirjoituksista) sekä PeVL 67/2002 vp (laki rahoitustarkastuksesta).

Käsitys siitä, että varmennepalveluiden tarjonta pitäisi katsoa julkisen vallan käytöksi lienee lähtöisin hallituksen esityksestä laiksi sähköisestä asioinnista hallinnossa (HE 153/1999 vp). Siinä katsottiin, että yksityisen tai julkisen varmentajan toiminta tulee rinnastaa välillisen julkisen hallinnon toimintaan. Perusteeksi tälle kannalle esitettiin, että varmenteen myöntäminen koskee hakijan etua hallitusmuodon 16 §:ssä tarkoitetulla tavalla. Hallintovaliokunnan mietinnössä (HaVM 10/1999 vp) hyväksyttiin hallituksen esityksessä esitetty näkemys varmentamistoiminnan julkisoikeudellisesta luonteesta, vaikka asiantuntijakuulemisessa esitettiin myös päinvastaisia kantoja.

Tätä linjaa noudattaen sähköisiä allekirjoituksia koskevan lain hallituksen esityksessä katsottiin, että myös yksityisten laatuvarmenteiden tarjoajien toiminnassa olisi kyse julkisen vallan käytöstä. Perustuslakivaliokunnan lausunnossa (PeVL 2/2002 vp) on todettu hallituksen esityksen mukaisesti, että laatuvarmenteiden tarjoamista on varmenteen oikeusvaikutusten vuoksi pidettävä perustuslain 124 §:ssä tarkoitettuna julkisena hallintotehtävänä. Lausunnossa katsottiin, että laatuvarmenne voidaan rinnastaa viranomaisen myöntämään henkilötodistukseen, kuten passiin tai henkilökorttiin. Varmennetoiminnalla katsottiin siten olevan merkitystä sähköisen liiketoiminnan ja muun asioinnin osapuolten oikeusaseman kannalta.

Edellä mainituissa hallituksen esityksissä todettu näkemys kuvastaa selkeästi sitä tapaa, jolla 1990-luvulla sähköisten allekirjoitusten kehityttyä asiaa hahmotettiin. Sittemmin sekä käytännön kehitys että tapa hahmottaa ilmiötä, jonka kanssa ollaan tekemisissä, ovat muuttuneet.

Käytännössä tilanne on tällä hetkellä se, että sähköisten allekirjoitusten markkinat eivät ole alkaneet toimia sen paremmin Suomessa kuin muuallakaan maailmassa. Suomessa sähköisen allekirjoittamisen palveluita ja laatuvarmenteita tarjoaa ainoastaan Väestörekisterikeskus. Niiden levinneisyys ja käyttö eivät kuitenkaan ole kovin suurta.

Tämän tosiasiallisen tilanteen johdosta sähköisten allekirjoitusten asemesta kehitys on kulkenut kohti sähköisen tunnistamisen välineiden kehitystä. Suomessa vahvan sähköisen tunnistamisen välineitä tarjoavat Väestörekisterikeskus julkisen avaimen järjestelmään pohjautuvilla varmenteillaan ja pankit pankkitunnisteillaan. Noin 99 % kaikista tunnistustapahtumista tehdään pankkitunnisteilla. Tämän johdosta valtiovarainministeriö antoi jo vuonna 2002 ohjeen, jonka mukaan pankkitunnisteet käyvät myös valtionhallinnon sähköisen asioinnin palveluissa asioitaessa. Mahdollisuus sähköiseen asiointiin viranomaisessa ei siten enää ole mitenkään sidoksissa varmenteiden tai laatuvarmenteiden käyttöön.

Myös tapa hahmottaa käsillä olevaa ilmiötä on muuttunut. On puhuttu siitä, että sähköisessä tunnistamisessa ja sähköisessä allekirjoittamisessa luodaan sähköisiä identiteettejä. Jokaisella ihmisellä voi kuitenkin olla vain yksi identiteetti eli henkilöllisyys, jonka Suomessa luo valtio. Tämä identiteetti luodaan, kun ihminen syntyy ja häneen liitetyt henkilötiedot kirjataan väestötietojärjestelmään. Näin syntynyt henkilöllisyys kiinnitetään virallisiin henkilöllisyyttä osoittaviin asiakirjoihin Suomessa poliisin toimesta. Tunnistusvälineellä voidaan kyllä todentaa henkilön identiteetti sähköisessä maailmassa. Henkilöllä voi myös olla useita rooleja, joissa hän toimii, ja häneen voidaan liittää eri palveluissa vaihtelevia määriä henkilöstä kertovia tietoja. Silti tunnistusvälinettä ei voida

verrata viralliseen poliisin myöntämään henkilökorttiin tai passiin. Tätä asiaa selvitetään parhaillaan syvällisesti sisäasiainministeriön johtamassa henkilöllisyyden luomista koskevassa hankkeessa eli identiteettiohjelmassa.

Vahvan sähköisen tunnistamisen palvelun ja varmenteiden tarjonta ovat yksityistä palveluntarjontaa, joihon ei ole tarvetta liittää perustuslain 124 §:n mukaista julkisen vallan käyttöä. Edes laatuvarmennetoiminta ei ole julkisen vallan käyttöä. Sen sijaan Väestörekisterikeskuksen kansalaisvarmenteita koskeva palveluntarjonta on julkisen vallan käyttöä. Tätä toimintaa koskee oma lakinsa, laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista, jota koskeva hallituksen esitys on parhaillaan eduskunnan käsiteltävänä. Siinä säädetään muun muassa kansalaisvarmennetta koskevasta erityisestä myöntämismenettelynsä, jossa poliisin suorittama henkilöllisyyden todentaminen on olennainen osa prosessia. Myös Valtiontalouden tarkastusvirasto on tunnistuspalveluiden kehittämisestä ja käytöstä julkisessa hallinnossa antamassaan raportissa (161/2008) katsonut, että Väestörekisterikeskuksen kansalaisvarmennetoiminnassa on kyse viranomaistoiminnoista, kun taas muu laatuvarmenteiden tai muiden varmenteiden liikkeelle lasku ei tätä ole.

Edellä sanottu tarkastelutavan muutos selkeyttää toimintakenttää olennaisesti. Ehdotetussa laissa säänneltäisiin puhtaasti yksityistä palveluntarjontaa, ja julkisen vallan käyttöä koskeva osuus sähköisten allekirjoitusten palveluiden tarjonnassa säännellään uudessa väestötietolaissa. Samalla ehdotetusta laista poistetaan sähköisistä allekirjoituksista annettuun lakiin verrattuna muutamia yksityiskohtia, jotka viittaavat julkisen vallan käyttöön. Erityisesti salassapitosäännös muutettaisiin oikeudeksi luovuttaa tietoja, ja laatuvarmenteiden myöntäminen muutettaisiin terminologisesti liikkeelle laskemiseksi.

Henkilötietojen käsittely

Perustuslain 10 §:n mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perusoikeusuudistusta koskevan hallituksen esityksen mukaan säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä (HE 309/1993 vp, s. 53). Säännöksen lakiviittaus henkilötietojen suojasta edellyttää perusoikeusuudistuksen tarkoituksen mukaisesti (PeVM 25/1994 vp, s. 6/I) lainsäätäjän säätävän tästä oikeudesta, mutta se jättää sääntelyn yksityiskohdat lainsäätäjän harkintaan.

Perustuslakivaliokunta on käsitellyt henkilötietojen suojaa muun muassa lausunnoissaan PeVL 47/1996 vp (telemarkkinalaki), PeVL 28/1997 vp (laki Euroopan poliisiviraston perustamisesta tehdyn yleissopimuksen ja siihen liittyvän pöytäkirjan eräiden määräysten hyväksymisestä), PeVL 29/1997 vp (laki poliisin henkilörekistereistä), PeVL 26/1998 vp (televiestinnän tietosuojalaki), PeVL 27/1998 vp ja PeVL 27a/1998 vp, (laki yksityisyyden suojasta työelämässä) sekä PeVL 25/1998 vp (henkilötietolaki).

Valiokunta on lausunnoissaan korostanut yleisesti lain yksityiskohtaisten säännösten täsmällisyyden tärkeyttä. Valiokunnan lausuntokäytännön mukaan myös kysymys henkilörekistereihin talletettujen tietojen säilytysajoista kuuluu kyseissä perustuslakikohdassa ilmaistun lailla säätämisen vaatimuksen piiriin. Tärkeitä sääntelykohteita ovat ainakin rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, niiden sallitut käyttötarkoitukset mukaan luettuna tietojen luovutettavuus ja tietojen säilytysaika henkilörekisterissä sekä rekisteröidyn oikeusturva samoin kuin näiden seikkojen sääntelemisen kattavuus ja yksityiskohtaisuus lain tasolla.

Henkilötietojen käsittely on luonnollisesti olennainen tekijä tunnistuspalvelun ja sähköisten allekirjoituspalveluiden tarjonnassa. Perussäännökset henkilötietojen käsittelystä on sijoitettu lakiehdotuksen 6 ja 7 §:iin. Ne koskevat kaikkia sähköisiä allekirjoituksia tarjoavia varmentajia, siis myös muita kuin laatuvarmenteita tarjoavia varmentajia, samoin kuin vahvan sähköisen tunnistuspalvelun tarjoajia. Säännökset pohjautuvat henkilötietolakiin ja sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin 8 artiklan 1 ja 2 kohtiin.

Ehdotetun 6 pykälän 1 momentin mukaan tunnistuspalvelun tarjoaja saa käsitellä vahvan sähköisen tunnistusvälineen liikkeelle laskemisessa, palvelun ylläpidossa sekä tun-

nistustapahtuman toteuttamisessa tarvittavia henkilötietoja. Sähköisiä allekirjoituksia tarjoava varmentaja saa puolestaan käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja. Ehdotettu momentti täyttää henkilötietolain 7 §:n edellytykset käyttötarkoitussidonnaisuudesta.

Sanotun 6 §:n 1 momentin mukaan käsittely saa tapahtua henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdissa tarkoitetuilla perusteilla. Tämä tarkoittaa sitä, että henkilötietoja saa käsitellä ainoastaan rekisteröidyn yksiselitteisesti antamalla suostumuksella ja rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

Pykälän 1 momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat lisäksi kerätä henkilötietoja henkilöltä itseltään. Keräämisen tarkoituksen on oltava sama kuin käsittelyssä muutoinkin.

Pykälän 2 momentin mukaan henkilötietoja saa käsitellä muussa kuin 1 momentissa säädetyssä tarkoituksessa ainoastaan henkilötietolain 8 §:n 1 momentin perusteella. Tämä johtuu siitä, että toimeksiannossa tai sopimuksessa ei ole mahdollista varautua muihin tarkoituksiin riittävällä tarkkuudella.

Pykälän 3 momentissa säädetään henkilötunnuksen käsittelystä. Henkilötietolain 13 §:n 1 momentin mukaan henkilötunnusta saa käsitellä henkilön yksiselitteisesti antamalla suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi.

Henkilötunnuksen käsittely tunnistuspalvelun ja sähköisiin allekirjoituksiin liittyvän varmennepalvelun yhteydessä on välttämätöntä sen johdosta, että palveluiden toteuttaminen luotettavasti nimenomaan edellyttää henkilöiden varmaa erottamista toisistaan. Tämä olisi sinällään jo henkilötietolain 13 §:n 1 momentin mukaan seikka, joka oikeuttaisi henkilötunnuksen käsittelyyn ilman nimenomaista lain säännöstäkin. Asiasta on kuitenkin haluttu ottaa selkeät säännökset pykälään.

Ehdotetun momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat käsitellä henkilötunnusta rekistereissään. Käsittelyn tarkoituksen on oltava sama kuin 1 momentissa. Henkilötunnus voidaan sisällyttää vahvan sähköisen tunnistamisen välineeseen tai varmenteeseen silloin, jos välineen tai varmenteen tietosisältö on ainoastaan sellaisen tahon saatavilla, jolle se on välttämätöntä palvelun toteuttamiseksi. Henkilötunnus ei saa kuitenkaan olla saatavissa julkisesta hakemistosta.

Ehdotetun lain 7 §:ssä säädetään väestötietojärjestelmään tallennettujen tietojen käyttämisestä. Pykälän 1 momentin mukaan tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat hankkia ja tarkastaa hakijan tai haltijan väestötietojärjestelmään tallennetut henkilötiedot henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdissa tarkoitetuilla perusteilla. Käsittelyn tarkoitus on sama kuin 6 §:ssä. Tunnistuspalvelun tarjoaja saa siis käsitellä tunnistusvälineen liikkeelle laskemisessa ja ylläpidossa sekä tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja ja sähköisiä allekirjoituksia tarjoava varmentaja saa käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja.

Tietojen käsittely saa tapahtua myös tältä osin henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdissa tarkoitetuilla perusteilla. Kysymys on siis rekisteröidyn yksiselitteisesti antamasta suostumuksesta, rekisteröidyn toimeksiannosta, sellaisen sopimuksen täytäntöönpanemisesta, jossa rekisteröity on osallisena tai sopimusta edeltävien toimenpiteiden toteuttamisesta rekisteröidyn pyynnöstä.

Tunnistuspalvelun osalta olennainen pykälä henkilötietojen käsittelyn kannalta on 24 §. Siinä säädetään tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentamisesta ja käytöstä. Pykälän 1 momentissa säädetään tallennettavista tiedoista. Näitä ovat yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot, tarvittavat tiedot hakijan ensitunnistamisesta sekä siinä käytetystä asiakirjasta, tiedot vahvan sähköisen tunnistusvälineen käyttöön mahdollisesti liittyvistä

estoista ja käyttörajoituksista sekä varmenteen osalta sen tietosisältö.

Pykälän 2 momentissa säädetään tallennusajasta. Se on tunnistustapahtumatietojen osalta viisi vuotta tunnistustapahtumasta ja muiden tallennettavien tietojen osalta viisi vuotta tunnistuspalvelun tarjoajan ja tunnistusvälineen haltijan välisen asiakassuhteen päättymisestä. Sellaiset tunnistustapahtuman yhteydessä syntyneet henkilötiedot, joiden säilyttäminen ei ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi, on 3 momentin mukaan hävitettävä tunnistustapahtuman jälkeen.

Pykälän 4 momentissa säädetään käsittelyn tarkoituksesta. Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa sekä vahvaa sähköistä tunnistamista käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Lisäksi momentissa säädetään käsittelyn lokitietojen tallentamisesta.

Laatuvarmenteita tarjoavien varmentajien osalta vastaavat säännökset sisältyvät ehdotuksen 37 ja 38 §:iin. Näistä 37 §:ssä säädetään tiedoista, joita palveluntarjoajan on tallennettava varmennerekisteriin ja sulkulistalle. Ehdotetussa 38 §:ssä puolestaan säädetään varmennerekisterin tietojen säilytysajaksi 10 vuotta. Pykälät vastaavat voimassa olevaa sähköisistä allekirjoituksista annetun lain sääntelyä.

Lisäksi henkilötietojen käsittelyä liittyy varmenteiden tietosisältöä koskeviin 19 ja 30 §:iin.

Henkilötietojen käsittelystä on ehdotuksessa säädetty perustuslain 10 §:n edellyttämällä tarkkuudella. Ehdotuksen säännökset eivät ole ristiriidassa perustuslain 10 §:n kanssa.

Elinkeinovapaus

Ehdotusta on tarkasteltava myös perustuslain 18 §:n 1 momentissa säädetyn elinkeinovapauden kannalta. Perustuslain 18 §:n 1 momentin mukaan jokaisella on oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla. Perustuslakivaliokunta on aiemmin käsitellyt elinkeinovapauteen liittyviä kysymyksiä muun muassa lausunnoissa PeVL 47/1996 vp (telemarkkinalaki), PeVL 19/1998 vp (laki televisio- ja radiotoiminnasta), PeVL 28/2001 vp (laki yksityisistä turvallisuuspalveluista), PeVL 61/2002 vp (viestintämarkkinalaki) sekä PeVL 67/2002 vp (laki rahoitustarkastuksesta).

Valiokunta on lausuntokäytännössään todennut, että elinkeinovapautta ei saa rajoittaa ilman erittäin pätevää syytä. Tällaisena syynä voidaan pitää esimerkiksi henkilöiden terveyden ja turvallisuuden suojelemista tai muita tärkeitä ja vahvoja yhteiskunnallisia intressejä. Rajoitusten tulee ilmetä lain tasolta, koska kyseessä on perusoikeuden rajoittaminen.

Valiokunta on lausuntokäytännössään katsonut elinkeinotoiminnan luvanvaraistamisen olevan poikkeuksellisesti mahdollista. Luvanvaraisuudesta on kuitenkin aina säädettävä lailla, jonka on täytettävä perusoikeuden rajoitusta koskevat tarkkarajaisuuden ja täsmällisyyden vaatimukset.

Esityksen 10 §:ssä asetetaan vahvan sähköisen tunnistamispalvelun tarjoajille velvollisuus tehdä toiminastaan ilmoitus Viestintävirastolle. Viestintäviraston on 12 §:n mukaan ilmoituksen saatuaan kiellettävä palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena, jos palvelu tai palveluntarjoaja ei täytä tässä luvussa asetettuja vaatimuksia. Jos puutteellisuutta voidaan pitää ainoastaan vähäisenä, Viestintävirasto voi kehottaa palveluntarjoajaa korjaamaan puutteellisuuden määräajassa. Lisäksi 12 §:n 1 momentissa säädetään, että Viestintäviraston on pidettävä yllä julkista rekisteriä ilmoituksen tehneistä palveluntarjoajista.

Ilmoituksen tekeminen on tarpeen Viestintävirastolle asetetun valvontavallan tehokkaaksi toteuttamiseksi. Järjestelmän kannalta kokonaisuudessaan on myös olennaista, että muut palveluntarjoajat ja vahvan sähköisen tunnistusvälineen hankkimista harkitsevat henkilöt voivat helpolla tavalla saada tiedon siitä, mitä palveluntarjoajia voidaan lähtökohtaisesti pitää luotettavina. Ehdotuksen 10 ja 12 §:ssä säädetty järjestely ei merkitse luvanvaraisuutta, sillä palveluntarjoaja voi tarjota täysin samaa palvelua myös tekemättä ilmoitusta. Tällöin se ei kuitenkaan saa tarjo-

ta palveluaan vahvana sähköisenä tunnistuspalveluna.

Sähköisten allekirjoituspalveluiden osalta ehdotettu laki sisältää vastaavat säännökset 32 §:ssä.

Lisäksi ehdotetun lain 29 §:ssä säädetään tarkastuslaitoksista. Tarkastuslaitokset nimeää Viestintävirasto hakemusten perusteella. Sanotussa pykälässä säädetään nimeämisen edellytyksistä. Pykälä perustuu EU:n sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin.

Sähköisiä allekirjoituksia koskevista yhteisön puitteista annettuun direktiiviin perustuvaa tarkastuslaitosten nimeämistä koskevaa sääntelyä lukuun ottamatta ehdotetussa laissa ei siis säädetä ennakolta annettavan luvan edellyttämisestä palveluntarjoajilta. Ehdotus rajoittaa jossain määrin täysin vapaata elinkeinon harjoittamista, mutta rajoituksia on pidettävä perusteltuina toiminnan luonteen huomioon ottaen. Edellä kerrotuilla perusteilla ehdotus ei tältäkään osin ole ristiriidassa perustuslain kanssa.

Verot ja maksut

Valtion verosta säädetään perustuslain 81 §:n 1 momentin mukaan lailla, joka sisältää säännökset verovelvollisuuden ja veron suuruuden perusteista sekä verovelvollisen oikeusturvasta. Verolaista tulee yksiselitteisesti ilmetä verovelvollisuuden piiri. Lain säännösten tulee olla myös sillä tavoin tarkkoja, että lakia soveltavien viranomaisten harkinta veroa määrättäessä on sidottua. Valtion viranomaisten virkatoimien, palvelujen ja muun toiminnan maksullisuuden sekä maksujen suuruuden yleisistä perusteista säädetään perustuslain 81 §:n 2 momentin perusteella lailla.

Perustuslakivaliokunta on käsitellyt verojen ja maksujen välistä rajanvetoa ainakin rautatielakia koskevassa lausunnossaan PeVL 66/2002 vp, rahoitustarkastusta koskevassa lausunnossa PeVL 67/2002 vp sekä lausunnoissa PeVL 61/2002 vp ja PeVL 3/2003 vp, jotka molemmat koskivat viestintämarkkinalakia. Myös sähköisen viestinnän tietosuojalakia koskevassa perustuslakivaliokunnan lausunnossa PeVL 9/2004 vp on käsitelty asiaa.

Perustuslakivaliokunnan vakiintuneen tulkintakäytännön mukaan maksuille on ominaista, että ne ovat korvauksia tai vastikkeita julkisen vallan palveluista. Muut rahasuoritukset valtiolle ovat sen sijaan valtiosääntöoikeudellisesti arvioiden yleensä veroja.

Perustuslakivaliokunta on lausunnoissaan hahmotellut eräitä seikkoja, jotka maksun tulisi täyttää, jotta se olisi valtiosääntöoikeudellisesti arvioiden maksu eikä vero. Suoritteiden, joista maksu peritään, tulee olla jollakin tavalla yksilöitävissä. Jos rahasuoritus peritään yleisesti jonkin toiminnan rahoittamiseen, kyseessä on valtiosääntöoikeudellisesti pikemminkin vero kuin maksu. Vaikka maksuluonteen edellytyksenä ei olekaan täysi kustannusvastaavuus, maksun suuruuden ja määräytymisperusteiden tulee kuitenkin säilyttää jokin yhteys suoritteen tuottamisesta aiheutuviin kustannuksiin. Mitä suuremmaksi ero maksun ja etenkin julkisoikeudelliseen tehtävään liittyvän suoritteen tuottamisesta aiheutuvien kustannusten välillä kasvaa, sitä lähempänä on pitää suoritusta verona.

Merkitystä voi olla myös sillä, onko asianomaisen suoritteen vastaanottaminen vapaaehtoista vai pakollista. Veron suuntaan viittaa, jos suoritusvelvollisuuden aiheuttamista suoritteista ei voi kieltäytyä ja velvollisuus koskee suoraan lain nojalla tietyt tunnusmerkit täyttäviä oikeussubjekteja.

Rahasuorituksen mahdollisella rajoitetulla käyttötarkoituksella ei perustuslakivaliokunnan lausuntokäytännön mukaan ole merkitystä suorituksen valtiosääntöoikeudellista luonnetta arvioitaessa.

Esityksen 47 §:ssä säädetään Viestintävirastolle maksettavista maksuista. Ilmoituksen tehneen tunnistuspalvelun tarjoajan tai palveluntarjoajien yhteenliittymän on suoritettava Viestintävirastolle rekisteröitymismaksu, jonka suuruus on 5000 euroa. Lisäksi palveluntarjoajan tai yhteenliittymän on suoritettava Viestintävirastolle vuosittain 12 000 euron suuruinen valvontamaksu.

Laatuvarmenteita tarjoavan varmentajan on suoritettava Viestintävirastolle vuosittain 40 000 euron suuruinen valvontamaksu. Jos laatuvarmenteita tarjoava varmentaja tekee myös ilmoituksen vahvan sähköisen tunnistuspalvelun tarjoamisesta, on sen maksettava myös rekisteröitymismaksu.

Maksujen avulla katetaan Viestintävirastolle tiettyjen laissa säädettyjen tehtävien hoitamisesta aiheutuvat kustannukset, mikä viittaa niiden veronluonteisuuteen.

Maksun määräytymisperusteiden yhteyttä suoritteen tuottamisesta aiheutuviin kustannuksiin voidaan arvioida seuraavasti. Maksuissa on ainoastaan yksi maksuluokka. Maksuvelvollisuus määrätään siis yleisin kriteerein kiinnittämättä maksun suuruutta yksilöllisesti mihinkään palveluntarjoajan vastaanottamiin suoritteisiin. Maksuvelvollisuus kytkeytyy yleisesti Viestintäviraston tietynlaisen toiminnan rahoittamiseen, eikä kysymys näin ollen ole Viestintäviraston erikseen yksilöitävissä oleviin suoritteisiin liittyvästä vastikkeesta. Maksuja on tällä kriteerillä arvioituna pidettävä ennemminkin verona kuin maksuna.

Suoritteen vastaanottamisen pakollisuutta voidaan arvioida seuraavasti. Maksut tulevat maksettavaksi, jos yritys tekee ilmoituksen tietynlaisen toiminnan aloittamisesta ja harjoittaa tietynlaista toimintaa. Maksuja on tälläkin kriteerillä arvioituna pidettävä ennemminkin verona kuin maksuna.

Ehdotettu säännös on pyritty laatimaan siten, että siitä ilmenee vähintään verovelvollisuuden ja veron suuruuden perusteet, verovelvollisten oikeusturva ja verovelvollisten piiri perustuslain 81 §:ssä edellytetyllä tavalla. Muista yksityiskohdista voitaisiin tarvittaessa säätää liikenne- ja viestintäministeriön asetuksella, mistä ehdotetaan erillistä valtuutussäännöstä lain 47 §:n 4 momenttiin.

Määräyksenantovaltuudet

Perustuslain 80 §:n 1 momentin mukaan lailla on säädettävä yksilön oikeuksien ja velvollisuuksien perusteista. Perustuslain 80 §:n 2 momentin mukaan muu viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Tällaisen valtuuden tulee olla soveltamisalaltaan täsmällisesti rajattu. Lisäksi perustuslaista johtuu, että valtuuden kattamat asiat on määriteltävä tarkasti laissa.

Perustuslakivaliokunta on käsitellyt asiaa muun muassa lausunnoissa PeVL 19/2002 vp (lääkelaki), PeVL 21/2001 vp (laki turvallisuusselvityksistä), PeVL 34/2000 vp (telemarkkinalaki), PeVL 25/2000 vp (vakuutusyhtiölaki) ja PeVL 23/2000 vp (arpajaislaki).

Perustuslakivaliokunta on lausuntokäytännössään todennut perustuslain 80 §:n 2 momentin soveltamisesta seuraavaa. Asetuksenantovaltuuksiin verrattuna tällaiseen valtuuteen kohdistuu yleistä tarkkarajaisuusvaatimusta pidemmälle menevä vaatimus valtuuden kattamien asioiden määrittelemisestä tarkasti laissa. Valtuuden tulee lisäksi perustuslain nimenomaisen säännöksen mukaan olla soveltamisalaltaan täsmällisesti rajattu (ks. myös esim. PeVL 46/2001 vp , s. 3/I). Muiden viranomaisten norminantovalta on perustuslain näkökulmasta poikkeuksellista (PeVM 10/1998 vp , s. 23/II). Perustuslakiuudistuksen yhteydessä mainittiin esimerkkinä viranomaisen norminantovallasta tekninen ja vähäisiä yksityiskohtia koskeva sääntely, johon ei liity merkittävää harkintavallan käyttöä (HE 1/1998 vp , s. 133/II; ks. myös PeVL 16/2002 vp , s. 2/I).

Perustuslakivaliokunta on toistuvasti myös korostanut, että perustuslain 80 §:n 1 ja 2 momentin säännökset rajoittavat suoraan valtuussäännösten tulkintaa samoin kuin valtuuksien nojalla annettavien säännösten ja määräysten sisältöä (ks. esim. PeVL 48/2001 vp , s. 4). Asetuksella tai viranomaisen määräyksellä ei siten voida antaa yleisiä oikeussääntöjä esimerkiksi yksilön oikeuksien tai velvollisuuksien perusteista eikä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan (PeVL 16/2002 vp , s. 2/II).

Sähköisen tunnistamisen osalta esityksen 8 §:n 3 momentin mukaan Viestintävirasto voisi antaa tarvittaessa tarkempia teknisiä määräyksiä siitä, millaisia edellytyksiä vahvan sähköisen tunnistuspalvelun on täytettävä ollakseen vahvaa. Lisäksi esityksen 10 §:n 5 momentin mukaan Viestintävirasto voi antaa valvontatoiminnan kannalta tarpeellisia teknisiä määräyksiä ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Sähköisten allekirjoitusten osalta Viestintävirastolla olisi vastaavat oikeudet antaa määräyksiä kuin voimassa olevassa sähköi-

sistä allekirjoituksista annetussa laissakin. Ehdotetun lain 32 §:n 1 momentin mukaan Viestintävirasto voi antaa valvontatoiminnan kannalta tarpeellisia määräyksiä ja suosituksia ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Edelleen lakiehdotuksen 42 §:n 2 momentin mukaan Viestintävirasto voisi antaa tarvittaessa teknisiä määräyksiä vahvan sähköisen tunnistuspalvelun tarjoajien sekä laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista.

Norminantovaltuudet on lakiehdotuksessa määritelty mahdollisimman tarkkarajaisesti ja täsmällisesti. Määräysten antamiseen liittyy vain vähäisissä määrin tarkoituksenmukaisuusharkintaa. Teknisten ja tarkempien määräysten antaminen on välttämättömiä sääntelyn kohteen teknisen luonteen, teknisen kehityksen nopeuden ja sääntelyn edellyttämän erityisasiantuntemuksen vuoksi.

Ehdotuksen norminantovaltuuksien ei edellä kerrotuilla perusteilla voida katsoa olevan ristiriidassa perustuslain 80 §:n kanssa.

4.2 Säätämisjärjestyksen arviointi

Edellä kerrotuilla perusteilla lakiehdotus voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. Tästä huolimatta pidetään suotavana, että esityksestä hankitaan perustuslakivaliokunnan lausunto.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

Lakiehdotukset

1.

Laki

vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tässä laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle.

Lakia ei sovelleta yhteisön sisäiseen tunnistamiseen tai sähköiseen allekirjoittamiseen käytettävien palveluiden tarjontaan.

Lakia ei sovelleta myöskään, jos yhteisö käyttää omaa tunnistusmenetelmäänsä yksinomaan omien asiakkaidensa tunnistamiseen lukuun ottamatta:

1) pakottavuutta koskevaa 3 §:ää;

2) tunnistusvälineen liikkeelle laskemista koskevan 20 §:n 1 momenttia;

3) tunnistusvälineen luovuttamista haltijalle koskevaa 21 §:ää;

4) tunnistusvälineen uusimista koskevaa 22 §:ää;

5) tunnistusvälineen haltijan velvollisuuksia koskevan 23 §:n 1 momenttia;

6) tunnistusvälineen peruuttamista ja käytön estämistä koskevaa 25 §:n 1 momenttia ja 2 momenttia;

7) tunnistusvälineen haltijan vastuuta välineen oikeudettomasta käytöstä sääntelevää 27 §:n 1 momenttia, 2 momentin 1 kohtaa ja 3 momenttia; sekä

8) kuluttaja-asiamiehen toimivaltaa koskevaa 42 §:n 4 momenttia.

Lakia ei sovelleta tunnistusvälineiden tai sähköisen allekirjoittamisen välineiden valmistamiseen, maahantuontiin tai myyntiin.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *vahvalla sähköisellä tunnistamisella* henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttämällä perustuen vähintään kahteen seuraavista kolmesta vaihtoehdosta:

a) salasanaan tai johonkin muuhun sellaiseen mitä tunnistusvälineen haltija tietää;

b) sirukorttiin tai johonkin muuhun sellaiseen mitä tunnistusvälineen haltijalla on hallussaan; tai

c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen;

2) *tunnistusvälineellä* esineitä ja yksilöiviä tietoja tai ominaisuuksia, jotka yhdessä muodostavat vahvaan sähköiseen tunnistamiseen tarvittavat tunnisteet, tunnistamisen välineet ja todentamisen välineet;

3) *tunnistusmenetelmällä* kokonaisuutta, jonka yhdessä muodostavat tunnistusväline sekä yksittäisen vahvan sähköisen tunnistustapahtuman toteuttamiseksi tarvittava järjestelmä;

4) *tunnistuspalvelun tarjoajalla* palveluntarjoajaa, joka tarjoaa vahvan sähköisen tunnistamisen palveluita niitä käyttäville palveluntarjoajille tai laskee liikkeelle tunnistusvälineitä yleisölle tai molempia;

5) *tunnistusvälineen haltijalla* luonnollista henkilöä, jolle tunnistuspalvelun tarjoaja on

sopimukseen perustuen antanut tunnistusvälineen;

6) *ensitunnistamisella* tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä;

7) *varmenteella* sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan, ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa sekä sähköisessä allekirjoituksessa;

8) *varmentajalla* luonnollista henkilöä tai oikeushenkilöä, joka tarjoaa varmenteita yleisölle:

9) *sähköisellä allekirjoituksella* sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä;

10) *kehittyneellä sähköisellä allekirjoituksella* sähköistä allekirjoitusta:

a) joka liittyy yksiselitteisesti sen allekirjoittajaan;

b) jolla voidaan yksilöidä allekirjoittaja;

c) joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja

d) joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita;

11) *allekirjoituksen luomistiedoilla* allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämää ainutkertaista tietokokonaisuutta, kuten koodeja ja yksityisiä avaimia;

12) *allekirjoituksen luomisvälineellä* ohjelmistoja ja laitteita, joilla yhdessä allekirjoituksen luomistietojen kanssa luodaan sähköinen allekirjoitus; sekä

13) *allekirjoituksen todentamistiedoilla* sähköisen allekirjoituksen todentamisessa käytettävää tietokokonaisuutta, kuten koodeja ja julkisia avaimia.

2 Luku

Oikeusvaikutukset ja henkilötietojen käsittely

3 §

Pakottavuus

Sopimusehto, joka poikkeaa tämän lain säännöksistä kuluttajan vahingoksi, on mitätön, jollei jäljempänä toisin säädetä.

4 §

Tunnistusvälineillä tehtävät sähköiset allekirjoitukset

Tunnistusvälineillä voidaan tehdä niiden ominaisuuksista riippuen sähköisiä allekirjoituksia ja kehittyneitä sähköisiä allekirjoituksia, jollei muualla laissa tai 18 §:ssä muuta säädetä.

5 §

Oikeustoimen tekeminen

Tunnistusvälinettä voidaan käyttää oikeustoimen tekemiseen, jollei muualla laissa tai 18 §:ssä muuta säädetä.

Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä. Sähköiseltä allekirjoitukselta ei tule kuitenkaan evätä oikeusvaikutuksia yksinomaan sen vuoksi, että se on tehty muulla kuin edellä mainitulla tavalla.

Sähköisen allekirjoituksen käytöstä hallinnossa säädetään erikseen.

6 §

Henkilötietojen käsittely

Tunnistuspalvelun tarjoaja saa käsitellä tunnistusvälineen liikkeelle laskemisessa,

palvelun ylläpidossa sekä tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja henkilötietolain (523/1999) 8 §:n 1 momentin 1 ja 2 kohdassa tarkoitetuilla perusteilla. Sähköisiä allekirjoituksia tarjoava varmentaja saa samoilla perusteilla käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja. Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat edellä mainitussa tarkoituksessa lisäksi kerätä henkilötietoja henkilöltä itseltään.

Henkilötietoja saa käsitellä muussa kuin 1 momentissa mainitussa tarkoituksessa ainoastaan henkilötietolain 8 §:n 1 momentin 1 kohdassa tarkoitetuilla perusteilla.

Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja voi tarkistaessaan hakijan henkilöllisyyden vaatia hakijaa ilmoittamaan henkilötunnuksensa. Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat käsitellä henkilötunnusta rekistereissään 1 momentissa mainitussa tarkoituksessa. Henkilötunnuksen saa sisällyttää tunnistusvälineeseen tai varmenteeseen, jos välineen tai varmenteen tietosisältö on ainoastaan sellaisen tahon saatavilla, jolle se on välttämätöntä palvelun toteuttamiseksi. Henkilötunnus ei saa olla saatavissa julkisesta hakemistosta.

Muilta osin henkilötietojen käsittelystä säädetään 19, 24, 30, 37 ja 38 §:ssä sekä henkilötietolaissa.

7 §

Väestötietojärjestelmään tallennettujen tietojen käyttäminen

Tunnistuspalvelun tarjoaja ja sähköisiä allekirjoituksia tarjoava varmentaja saavat henkilötietolain 8 §:n 1 momentin 1 ja 2 kohdassa tarkoitetuilla perusteilla ja 6 §:n 1 momentissa mainitussa tarkoituksessa hankkia henkilötietoja ja tarkastaa hakijan tai haltijan ilmoittamat henkilötiedot väestötietojärjestelmästä.

Väestötietojärjestelmästä luovutettava tieto on julkisoikeudellinen suorite. Suoritteen maksullisuudesta säädetään valtion maksuperustelaissa (150/1992).

3 luku

Vahva sähköinen tunnistaminen

8 §

Tunnistusmenetelmälle asetettavat vaatimukset

Tunnistusmenetelmän on täytettävä seuraavat vaatimukset:

1) menetelmän perustana on 17 §:n mukainen ensitunnistaminen, jota koskevat tiedot ovat jälkikäteen 24 §:n mukaisesti tarkistettavissa;

2) menetelmällä voidaan yksiselitteisesti tunnistaa tunnistusvälineen haltija;

3) menetelmällä voidaan riittävällä luotettavuudella varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä; ja

4) menetelmä on riittävän turvallinen ja luotettava ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat.

Mitä 1 momentissa säädetään, ei estä palvelun tarjoamista palvelukohtaisesti siten, että tunnistuspalvelun tarjoaja ilmoittaa tunnistuspalvelua käyttävälle palveluntarjoajalle tunnistusvälineen haltijan salanimen tai ainoastaan rajoitetun määrän henkilötietoja.

Viestintävirasto voi antaa tarkempia teknisiä määräyksiä 1 momentissa tarkoitetuista vaatimuksista.

9 §

Tunnistuspalvelun tarjoajalle asetettavat vaatimukset

Tunnistuspalvelun tarjoajana olevan tai sen lukuun toimivan luonnollisen henkilön, palveluntarjoajana olevan yhteisön tai säätiön hallituksen tai hallintoneuvoston jäsenten ja varajäsenten, toimitusjohtajan, vastuunalaisen yhtiömiehen taikka muussa näihin rinnastettavassa asemassa olevien on täytettävä seuraavat edellytykset:

1) heidän on oltava täysikäisiä;

2) he eivät saa olla konkurssissa; ja

3) heidän toimintakelpoisuutensa ei saa olla rajoitettu.

Tunnistuspalvelun tarjoajan on oltava luotettava. Tunnistuspalvelun tarjoajaa ei pidetä

luotettavana, jos 1 momentissa tarkoitettu henkilö on lainvoiman saaneella tuomiolla tuomittu viiden viimeisen vuoden aikana vankeusrangaistukseen tai kolmen viimeisen vuoden aikana sakkorangaistukseen rikoksesta, jonka voidaan katsoa osoittavan henkilön olevan ilmeisen sopimaton harjoittamaan tunnistuspalvelun tarjontaa.

Tunnistuspalvelun tarjoajaa ei pidetä luotettavana myöskään, jos 1 momentissa tarkoitettu henkilö on muutoin aikaisemmalla toiminnallaan osoittanut olevansa ilmeisen sopimaton tunnistuspalvelun tarjoajaksi.

10 §

Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toiminnan aloittamisesta

Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on ennen toiminnan aloittamista tehtävä kirjallinen ilmoitus Viestintävirastolle. Ilmoituksen voi tehdä myös sellainen palveluntarjoajien yhteenliittymä, jonka hallinnoimaa palvelua on pidettävä yhtenä tunnistuspalveluna.

Ilmoituksessa on oltava:

1) palveluntarjoajan nimi;

2) palveluntarjoajan täydelliset yhteystiedot;

3) tiedot tarjottavista palveluista;

4) tiedot 8, 9, 13 ja 14 §:ssä tarkoitetuista seikoista; ja

5) muut valvonnan kannalta tarpeelliset tiedot.

Tunnistuspalvelun tarjoajan on viipymättä ilmoitettava 2 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista kirjallisesti Viestintävirastolle. Ilmoitus on tehtävä myös toiminnan lopettamisesta sekä toimintojen siirtymisestä toiselle palveluntarjoajalle.

Viestintävirasto voi antaa valvontatoiminnan kannalta tarpeellisia teknisiä määräyksiä edellä tässä pykälässä tarkoitettujen ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

11 §

Muuhun Euroopan talousalueen jäsenvaltioon sijoittautunut tunnistuspalvelun tarjoaja

Mitä 10 §:ssä säädetään, ei estä muualle Euroopan talousalueelle sijoittautunutta tunnistuspalvelun tarjoajaa tekemästä mainitussa pykälässä tarkoitettua ilmoitusta.

12 §

Tunnistuspalvelun tarjoajia koskeva rekisteri

Viestintävirasto ylläpitää julkista rekisteriä 10 §:n mukaisen ilmoituksen tehneistä tunnistuspalvelun tarjoajista ja niiden tarjoamista palveluista.

Viestintäviraston on 10 §:ssä tarkoitetun ilmoituksen saatuaan kiellettävä palveluntarjoajaa tarjoamasta palveluaan vahvana sähköisenä tunnistamisena, jos palvelu tai palveluntarjoaja ei täytä tässä luvussa asetettuja vaatimuksia. Jos puutteellisuutta voidaan pitää ainoastaan vähäisenä, Viestintävirasto voi kehottaa palveluntarjoajaa korjaamaan puutteellisuuden määräajassa.

13 §

Tunnistuspalvelun tarjoajan yleiset velvollisuudet

Tunnistuspalvelun tarjoajan on huolehdittava siitä, että sen palveluksessa olevalla henkilöstöllä on harjoitetun toiminnan laajuuteen nähden riittävä asiantuntemus, kokemus ja pätevyys.

Tunnistuspalvelun tarjoajalla on oltava harjoitetun toiminnan laajuuteen nähden riittävät taloudelliset voimavarat toiminnan järjestämiseksi ja mahdollisen vahingonkorvausvastuun kattamiseksi. Palveluntarjoaja voi myös ryhtyä muihin tarpeellisiin toimenpiteisiin mahdollisen vahingonkorvausvastuun varalta.

Tunnistamispalvelun tarjoajan on lisäksi huolehdittava palvelujensa henkilötietolain 32 §:ssä tarkoitetusta tietojen suojaamisesta sekä riittävästä tietoturvasta.

Tunnistuspalvelun tarjoaja vastaa apunaan käyttämiensä henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.

14 §

Tunnistusperiaatteet

Tunnistuspalvelun tarjoajalla on oltava tunnistusperiaatteet, joissa määritellään tarkemmin, kuinka palveluntarjoaja täyttää tässä laissa tarkoitetut velvollisuutensa. Erityisesti on määriteltävä tarkemmin, kuinka tunnistuspalvelun tarjoaja toteuttaa 17 §:ssä tarkoitetun ensitunnistamisen.

Lisäksi tunnistusperiaatteissa on annettava keskeiset tiedot:

1) palveluntarjoajasta;

2) tarjottavista palveluista ja niiden hinnoista;

3) palveluntarjoajan tärkeimmistä yhteistyökumppaneista;

4) ulkopuolisten arviointilaitosten suorittamista tarkastuksista; sekä

5) muista merkityksellisistä seikoista, joiden perusteella palveluntarjoajan toimintaa ja luotettavuutta voidaan arvioida.

Jos tunnistusvälineillä voidaan tehdä sähköisiä allekirjoituksia tai kehittyneitä sähköisiä allekirjoituksia, tunnistuspalvelun tarjoajan on annettava tieto myös niiden toteuttamismenetelmästä, tasosta ja turvallisuustekijöistä.

Tunnistuspalvelun tarjoajan on pidettävä tunnistusperiaatteet yleisesti saatavilla ja ajantasaisina.

15 §

Tunnistuspalvelun tarjoajan tiedonantovelvollisuus ennen sopimuksen tekemistä

Tunnistuspalvelun tarjoajan on ennen tunnistusvälineen hakijan kanssa tehtävän sopimuksen tekemistä annettava hakijalle tiedot:

1) palveluntarjoajasta;

2) tarjottavista palveluista;

3) 14 §:ssä tarkoitetuista tunnistusperiaatteista;

4) osapuolten oikeuksista ja velvollisuuksista;

5) mahdollisista vastuunrajoituksista;

6) valitus- ja riitojenratkaisumenettelyistä;

7) mahdollisista 18 §:ssä tarkoitetuista estoista ja käyttörajoituksista; sekä

8) muista mahdollisista tunnistusvälineen käyttöehdoista.

Edellä 1 momentissa tarkoitetut tiedot on annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voi tallentaa ja toisintaa ne muuttumattomina. Jos sopimus tehdään tunnistusvälineen hakijan pyynnöstä sellaista etäviestintä käyttäen, että tietoja ja sopimusehtoja ei voida antaa edellä tarkoitetulla tavalla ennen sopimuksen tekemistä, tiedot on annettava sanotulla tavalla viipymättä sopimuksen tekemisen jälkeen.

Henkilötietojen käsittelyä koskevasta tiedonantovelvollisuudesta säädetään henkilötietolaissa.

16 §

Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa tietoturvaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoajan on ilmoitettava tunnistuspalvelua käyttäville palveluntarjoajille, tunnistusvälineiden haltijoille sekä Viestintävirastolle palvelun tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä.

Jos uhka tai häiriö kohdistuu henkilötietolain 32 §:ssä tarkoitettuun tietojen suojaamiseen, tunnistuspalvelun tarjoajan on ilmoitettava asiasta 1 momentissa tarkoitettujen tahojen lisäksi tietosuojavaltuutetulle.

Ilmoituksessa on samalla kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.

17 §

Tunnistusvälineen hakijan ensitunnistaminen

Ensitunnistamisen on tapahduttava henkilökohtaisesti. Tunnistuspalvelun tarjoajan on tunnistettava tunnistusvälineen hakija huolellisesti toteamalla hänen henkilöllisyytensä voimassa olevasta Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista. Halutessaan tunnistuspalvelun tarjoaja voi käyttää ensitunnistamisessa myös

muun valtion viranomaisen myöntämää voimassa olevaa passia.

Ensitunnistamisen henkilökohtaisuudesta voidaan poiketa, jos tunnistuspalvelun tarjoajat ovat tehneet keskenään sopimuksen mahdollisuudesta luottaa toistensa tekemään ensitunnistamiseen. Tunnistusvälinettä voidaan tällöin hakea sähköisesti. Tunnistuspalvelun tarjoajien on sopimuksessaan määriteltävä, kuinka vastuu mahdollisesta alkuperäisen ensitunnistamisen virheellisyydestä niiden keskinäisessä suhteessa jakaantuu. Suhteessa vahingon kärsineeseen vastaa se tunnistuspalvelun tarjoaja, joka luottaa toisen tekemään ensitunnistamiseen.

Tunnistusvälinettä voidaan hakea sähköisesti myös silloin, jos hakijalla on voimassa oleva saman tunnistuspalvelun tarjoajan antama tunnistusväline. Ensitunnistamista ei tällöin tarvitse tehdä uudelleen.

Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi. Poliisin tekemästä ensitunnistamisesta tunnistusvälineen hakijalle aiheutuva kustannus on julkisoikeudellinen suorite. Suoritteen maksullisuudesta säädetään valtion maksuperustelaissa.

18 §

Oikeustoimen tekemiseen kohdistuvat estot ja rajoitukset

Tunnistuspalvelun tarjoajan, tunnistuspalvelua käyttävän palveluntarjoajan sekä tunnistusvälineen haltijan välisillä sopimuksilla voidaan tunnistusvälineen käyttäminen oikeustoimien tekemiseen estää. Lisäksi oikeustoimien tekemiselle voidaan asettaa sekä käyttötarkoitukseen että tapahtumien rahamääräiseen arvoon liittyviä rajoituksia.

Tunnistuspalvelun tarjoajan on huolehdittava siitä, että estot tai rajoitukset ovat kaikkien osapuolten tiedossa tai havaittavissa helpolla tavalla. Tunnistuspalvelun tarjoaja voi myös toteuttaa estot tai rajoitukset teknisin keinoin. Tunnistuspalvelun tarjoaja ei vastaa niistä toimista, jotka on tehty estojen tai rajoitusten vastaisesti siitä huolimatta, että tunnistuspalvelun tarjoaja on toiminut huolellisesti.

Tunnistuspalvelun tarjoajan on järjestettävä tunnistuspalvelua käyttävälle palveluntarjoajalle mahdollisuus tarkastaa tunnistusvälineeseen liittyvät estot tai rajoitukset ympäri vuorokauden. Velvollisuutta ei kuitenkaan ole, jos tunnistusvälineen estojen tai rajoitusten vastainen käyttö on teknisin keinoin estetty.

Tunnistuspalvelua käyttävän palveluntarjoajan on tarkastettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset estot tai rajoitukset tunnistusvälineen käytön yhteydessä. Tarkastaminen ei kuitenkaan ole tarpeen, jos tunnistusvälineen estojen tai rajoitusten vastainen käyttö on teknisin keinoin estetty.

19 §

Varmenteen tietosisältö

Jos tunnistusmenetelmä perustuu varmenteeseen, tulee varmenteen sisältää ainakin:

1) tieto varmentajasta;
2) tieto varmenteen haltijasta;
3) varmenteen haltijan yksilöivä tunnus;
4) varmenteen voimassaoloaika;
5) varmenteen yksilöivä tunnus;
6) tieto varmenteen käytön mahdollisista estoista ja rajoituksista;
7) varmenteen haltijan julkinen avain ja tieto sen käyttötarkoituksesta; sekä
8) varmentajan kehittynyt sähköinen allekirjoitus.

Varmennepalvelun tarjoajan tulee omalta osaltaan varmistaa, että tunnistuspalvelua käyttävällä palveluntarjoajalla on saatavillaan varmenteen tietosisältö.

20 §

Tunnistusvälineen liikkeelle laskeminen

Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla.

Sopimus voi olla voimassa toistaiseksi tai määräaikaisesti. Tunnistusvälineellä voi olla

oma voimassaoloaikansa, joka on lyhyempi kuin sopimuksen voimassaoloaika.

Tunnistusväline annetaan aina luonnolliselle henkilölle. Tunnistusvälineen on oltava henkilökohtainen. Tunnistusvälineeseen voidaan tarvittaessa liittää tieto siitä, että henkilö voi tapauskohtaisesti myös edustaa toista luonnollista henkilöä tai oikeushenkilöä.

21 §

Tunnistusvälineen luovuttaminen hakijalle

Tunnistuspalvelun tarjoajan on luovutettava tunnistusväline sen hakijalle siten kuin sopimuksessa on sovittu. Tunnistuspalvelun tarjoajan on riittävällä tavalla varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa.

22 §

Tunnistusvälineen uusiminen

Tunnistuspalvelun tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu tunnistusväline on korvattava uudella. Toimittamisessa noudatetaan tällöin 21 §:n säännöksiä.

23 §

Tunnistusvälineen haltijan velvollisuudet

Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti. Haltijan on säilytettävä tunnistusvälinettä huolellisesti. Haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.

Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

24 §

Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö

Tunnistuspalvelun tarjoajan on tallennettava:

1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot;

2) tarvittavat tiedot 17 §:ssä tarkoitetusta hakijan ensitunnistamisesta sekä siinä käytetystä asiakirjasta;

3) tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön mahdollisesti liittyvistä estoista ja käyttörajoituksista; sekä

4) varmenteen osalta 19 §:ssä tarkoitettu varmenteen tietosisältö.

Edellä 1 momentin 1 kohdassa tarkoitetut tiedot on säilytettävä viisi vuotta tunnistustapahtumasta ja 2—4 kohdassa tarkoitetut tiedot viisi vuotta tunnistuspalvelun tarjoajan ja tunnistusvälineen haltijan välisen asiakassuhteen päättymisestä.

Tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, jollei tallentaminen ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi.

Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä.

Edellä 1 momentin 1 kohta ja 3 momentti eivät koske sellaista palveluntarjoajaa, joka ainoastaan laskee liikkeelle tunnistusvälineitä. Edellä 2 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tällöin tunnistusvälineen voimassaolon päättymisestä.

25 §

Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus

Tunnistusvälineen haltijan on ilmoitettava tunnistuspalvelun tarjoajalle tai tämän nimeämälle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian.

Tunnistuspalvelun tarjoajan on tarjottava mahdollisuus tehdä 1 momentissa tarkoitettu ilmoitus milloin tahansa. Tunnistuspalvelun

tarjoajan on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen.

Tunnistuspalvelun tarjoajan on asianmukaisesti ja viipymättä merkittävä järjestelmään tieto peruuttamisen tai käytön estämisen ajankohdasta. Tunnistusvälineen haltijalla on oikeus saada pyynnöstä todistus siitä, että hän on tehnyt 1 momentissa mainitun ilmoituksen. Todistusta on pyydettävä 18 kuukauden kuluessa ilmoituksesta.

Järjestelmän on oltava sellainen, että tunnistuspalvelua käyttävä palveluntarjoaja voi helposti tarkastaa siihen merkityt tiedot ympäri vuorokauden. Velvollisuutta järjestää tarkastusmahdollisuutta ei kuitenkaan ole, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.

Tunnistuspalvelua käyttävän palveluntarjoajan on tarkastettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset peruutukset ja käytön estot tunnistusvälineen käytön yhteydessä. Tarkastaminen ei kuitenkaan ole tarpeen, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.

Jos tunnistuspalvelu perustuu varmenteisiin ja peruutettuja varmenteita koskevat tiedot annetaan sulkulistan avulla, varmennepalvelun tarjoaja saa tallentaa tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkastamisesta. Vaihtoehtoisesti varmentaja voi tallentaa sulkulistan.

26 §

Tunnistuspalvelun tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö

Sen lisäksi, mitä 25 §:ssä säädetään, tunnistuspalvelun tarjoaja voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:

1) tunnistuspalvelun tarjoajalla on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;

2) tunnistusväline sisältää ilmeisen virheellisyyden;

3) tunnistuspalvelun tarjoajalla on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;

4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti sopimusehtojen vastaisella tavalla; tai

5) tunnistusvälineen haltija on kuollut.

Tunnistuspalvelun tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja peruuttamisen tai käytön estämisen ajankohdasta sekä siihen johtaneista syistä.

Tunnistuspalvelun tarjoajan on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.

27 §

Tunnistusvälineen haltijan vastuu tunnistusvälineen oikeudettomasta käytöstä

Tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä vain, jos:

1) hän on luovuttanut tunnistusvälineen toiselle;

2) tunnistusvälineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää; tai

3) hän on laiminlyönyt ilmoittaa tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan.

Tunnistusvälineen haltija ei kuitenkaan vastaa tunnistusvälineen oikeudettomasta käytöstä:

1) siltä osin kuin tunnistusvälinettä on käytetty sen jälkeen, kun hän on ilmoittanut tunnistuspalvelun tarjoajalle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä;

2) jos tunnistusvälineen haltija ei ole voinut tehdä ilmoitusta välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan sen johdosta, että tunnistuspalvelun tarjoaja on laiminlyönyt 25 §:n 2 momentissa tarkoitetun velvollisuutensa huolehtia siitä, että tunnistusvälineen halti-

jalla on jatkuvasti mahdollisuus tehdä kyseinen ilmoitus; tai

3) tunnistuspalvelua käyttävä palveluntarjoaja on laiminlyönyt 18 §:n 4 momentin tai 25 §:n 5 momentin mukaisen velvollisuutensa tarkastaa tunnistusvälineeseen liittyvän käyttörajoituksen olemassa olon tai tiedon välineen käytön estämisestä tai sulkemisesta.

4 Luku

Sähköinen allekirjoitus

28 §

Turvallinen allekirjoituksen luomisväline

Turvallisen allekirjoituksen luomisvälineen on riittävän luotettavasti varmistettava, että:

1) allekirjoituksen luomistiedot ovat käytännössä ainutkertaisia ja että ne säilyvät luottamuksellisina;

2) allekirjoituksen luomistietoja ei voida päätellä muista tiedoista;

3) allekirjoitus on suojattu väärentämiseltä;

4) allekirjoittaja voi suojata allekirjoituksen luomistiedot muiden käytöltä; sekä

5) luomisväline ei muuta allekirjoitettavia tietoja eikä estä tietojen esittämistä allekirjoittajalle ennen allekirjoittamista.

Allekirjoituksen luomisvälineen katsotaan aina täyttävän 1 momentissa säädetyt vaatimukset, jos:

1) se on Euroopan yhteisöjen komission vahvistamien ja Euroopan unionin virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukainen; tai

2) vaatimusten arviointitehtävään nimetty tarkastuslaitos, joka sijaitsee Suomessa tai muussa Euroopan talousalueeseen kuuluvassa valtiossa, on sen hyväksynyt.

29 §

Tarkastuslaitos

Viestintävirasto voi nimetä tarkastuslaitoksia, joiden tehtävänä on arvioida, täyttääkö allekirjoituksen luomisväline 28 §:n 1 momentissa säädetyt vaatimukset. Tarkastuslaitokset voivat olla yksityisiä tai julkisia laitoksia.

Tarkastuslaitoksen nimeämisen edellytyksenä on, että:

1) tarkastuslaitos on toiminnallisesti ja taloudellisesti riippumaton;

2) sen toiminta on luotettavaa, asianmukaista ja syrjimätöntä;

3) sillä on riittävät taloudelliset voimavarat toiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen korvausvastuun kattamiseksi;

4) sillä on käytössään riittävästi ammattitaitoista ja puolueetonta henkilöstöä; sekä

5) sillä on käytössään toiminnan edellyttämät tilat ja välineistö.

Viestintävirasto nimeää tarkastuslaitokset hakemuksen perusteella. Hakemuksen tulee sisältää hakijan yhteystietojen ja kaupparekisteriotteen tai vastaavan selvityksen lisäksi selvitys 2 momentissa tarkoitettujen edellytysten täyttymisestä hakijan toiminnassa. Viestintävirasto antaa tarvittaessa ohjeita hakemukseen sisällytettävistä tiedoista ja niiden toimittamisesta Viestintävirastolle.

Viestintävirasto valvoo tarkastuslaitoksen toimintaa. Jos tarkastuslaitos ei täytä säädettyjä vaatimuksia tai toimii säännösten vastaisesti, Viestintäviraston on peruutettava nimeämispäätös. Tarkastuslaitoksen on ilmoitettava Viestintävirastolle toimintansa sellaisista muutoksista, joilla on vaikutusta tarkastuslaitoksen nimeämisen edellytyksiin.

Tarkastuslaitos voi arviointitehtävässä käyttää apunaan laitoksen ulkopuolisia henkilöitä. Tarkastuslaitos vastaa myös apunaan käyttämiensä henkilöiden työstä.

30 §

Laatuvarmenne

Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää 2 momentissa säädetyt vaatimukset ja jonka on myöntänyt 33—38 §:ssä säädetyt vaatimukset täyttävä varmentaja.

Laatuvarmenteen tulee sisältää:

1) tieto siitä, että varmenne on laatuvarmenne;

2) tieto varmentajasta ja sen sijoittautumisvaltiosta;

3) allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi;

4) allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja;
5) laatuvarmenteen voimassaoloaika;
6) laatuvarmenteen yksilöivä tunnus;
7) varmentajan kehittynyt sähköinen allekirjoitus;
8) mahdolliset laatuvarmenteen käyttörajoitukset; sekä
9) allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.

Jos laatuvarmenteita tarjoava varmentaja tarjoaa myös 3 luvussa tarkoitettua tunnistuspalvelua, katsotaan 1 momentin vaatimusten täyttävän aina myös 19 §:n 1 momentissa tarkoitetut varmenteen tietosisältöä koskevat vaatimukset.

31 §

Muun kuin Suomeen sijoittautuneen varmentajan tarjoama laatuvarmenne

Muun kuin Suomeen sijoittautuneen varmentajan laatuvarmenteena tarjoaman varmenteen katsotaan täyttävän tässä laissa säädetyt laatuvarmennetta koskevat vaatimukset, jos:

1) varmentaja on sijoittautunut Euroopan talousalueeseen kuuluvaan valtioon ja varmenne täyttää sijoittautumisvaltiossa laatuvarmenteelle asetetut vaatimukset; tai

2) varmentaja on liittynyt Euroopan talousalueeseen kuuluvassa valtiossa vapaaehtoiseen akkreditointijärjestelmään ja täyttää kyseisessä valtiossa sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY, jäljempänä *sähköallekirjoitusdirektiivi*, voimaan saattamiseksi säädetyt kansalliset vaatimukset; tai

3) varmenteen takaa sellainen varmentaja, joka on sijoittautunut Euroopan talousalueeseen kuuluvaan valtioon ja täyttää kyseisessä valtiossa sähköallekirjoitusdirektiivin voimaan saattamiseksi säädetyt kansalliset vaatimukset; tai

4) varmenne tai varmentaja on tunnustettu Euroopan yhteisön ja yhden tai useamman kolmannen maan tai kansainvälisen organisaation välisen kahden- tai monenvälisen sopimuksen nojalla.

32 §

Ilmoitus toiminnan aloittamisesta

Laatuvarmenteita tarjoavan varmentajan on ennen toiminnan aloittamista tehtävä kirjallinen ilmoitus Viestintävirastolle. Ilmoituksen tulee sisältää varmentajan nimi ja yhteystiedot sekä tiedot, joiden perusteella 30 §:ssä ja 33—38 §:ssä säädettyjen vaatimusten täyttyminen voidaan varmistaa. Viestintävirasto voi antaa määräyksiä ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Viestintäviraston on viipymättä ilmoituksen saatuaan kiellettävä varmentajaa tarjoamasta varmenteitaan laatuvarmenteina, jos varmenne ei täytä 30 §:n 2 momentin vaatimuksia tai varmentaja ei täytä 33—38 §:ssä säädettyjä vaatimuksia.

Jos 1 momentissa tarkoitetut tiedot ovat muuttuneet, varmentajan on viipymättä ilmoitettava muutoksista kirjallisesti Viestintävirastolle.

Viestintävirasto pitää laatuvarmenteita myöntävistä varmentajista julkista rekisteriä.

Laatuvarmenteita tarjoava varmentaja voi tehdä myös 10 §:ssä tarkoitetun ilmoituksen, jos se haluaa tarjota laatuvarmenteiden lisäksi tunnistuspalvelua.

33 §

Laatuvarmenteita tarjoavan varmentajan yleiset velvollisuudet

Varmentajalla on oltava harjoitetun toiminnan laajuuteen nähden riittävät tekniset taidot ja taloudelliset voimavarat. Varmentaja vastaa kaikista varmentamistoiminnan osa-alueista, myös mahdollisten varmentajan apunaan käyttämien henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.

Varmentajan tulee:

1) varmistaa, että sen henkilöstöllä on riittävä asiantuntemus, kokemus ja pätevyys;

2) huolehtia riittävistä taloudellisista voimavaroista toimintansa järjestämiseksi ja

mahdollisen vahingonkorvausvastuun kattamiseksi;

3) pitää yleisesti saatavilla varmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida; sekä

4) turvata allekirjoituksen luomistietojen luottamuksellisuus silloin, kun varmentaja itse tuottaa tiedot.

Varmentaja ei saa tallentaa tai jäljentää allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

34 §

Luotettavat laitteet ja ohjelmistot

Laatuvarmenteita tarjoavan varmentajan on huolehdittava siitä, että sen käyttämät järjestelmät sekä laitteet ja ohjelmistot ovat riittävän turvallisia ja luotettavia sekä suojattu muutoksilta ja väärentämiseltä.

Sähköisiin allekirjoituksiin liittyvän laitteen tai ohjelmiston katsotaan täyttävän 1 momentissa säädetyt vaatimukset aina, jos laite tai ohjelmisto on Euroopan yhteisöjen komission vahvistamien, Euroopan unionin virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukainen.

35 §

Laatuvarmenteen liikkeelle laskeminen

Laatuvarmenteita tarjoavan varmentajan tulee huolellisesti ja luotettavalla tavalla tarkistaa laatuvarmenteen hakijan henkilöllisyys ja muut laatuvarmenteen liikkeelle laskemisessa ja ylläpidossa tarpeelliset hakijan henkilöön liittyvät tiedot. Laatuvarmenteita tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti.

Laatuvarmenteita tarjoavan varmentajan tulee ennen sopimuksen tekemistä antaa laatuvarmenteen hakijalle tiedot laatuvarmenteen käyttöehdoista, mukaan lukien mahdolliset käyttörajoitukset, tiedot vapaaehtoisista akkreditointijärjestelmistä, varmennetoiminnan viranomaisvalvonnasta sekä valitus- ja riitojenratkaisumenettelyistä. Tiedot tulee antaa laatuvarmenteen hakijalle kirjallisesti sellaisessa muodossa, että hakija voi ne vaivatta ymmärtää.

36 §

Laatuvarmenteen peruuttaminen

Allekirjoittajan on viipymättä pyydettävä laatuvarmenteen myöntäneeltä varmentajalta laatuvarmenteen peruuttamista, jos hänellä on perusteltu syy epäillä allekirjoituksen luomistietojen oikeudetonta käyttöä.

Laatuvarmenteita tarjoavan varmentajan on viipymättä peruutettava laatuvarmenne, jos allekirjoittaja sitä pyytää. Laatuvarmenteen peruuttamispyynnön katsotaan saapuneen varmentajalle silloin, kun se on ollut varmentajan käytettävissä siten, että pyyntöä voidaan käsitellä.

Laatuvarmenne voidaan peruuttaa myös, jos siihen muutoin on erityistä syytä. Laatuvarmenteen peruuttamisesta ja peruuttamisajankohdasta tulee aina ilmoittaa allekirjoittajalle.

37 §

Laatuvarmenteita tarjoavan varmentajan ylläpitämät rekisterit

Laatuvarmenteita tarjoavan varmentajan tulee ylläpitää rekisteriä myöntämistään laatuvarmenteista (*varmennerekisteri*). Rekisteriin tulee merkitä:

1) 30 §:n 2 momentissa määritelty laatuvarmenteen tietosisältö;

2) 35 §:n 1 momentissa tarkoitetut hakijan henkilöön liittyvät tiedot, mukaan lukien tieto laatuvarmennetta liikkeelle laskettaessa käytetystä hakijan tunnistamismenettelystä ja tarvittavat tiedot tunnistamisessa mahdollisesti käytetystä asiakirjasta; sekä

3) 39 §:ssä tarkoitetut tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta, jos laatuvarmenteita tarjoava varmentaja käyttää 39 §:n mukaista tallennusoikeutta.

Laatuvarmenteita tarjoavan varmentajan tulee varmistaa, että laatuvarmenteella varmennettuun kehittyneeseen sähköiseen alle-

kirjoitukseen luottavalla osapuolella on saatavilla 30 §:n 2 momentissa määritelty varmenteen tietosisältö. Edellä 1 momentin 3 kohdassa tarkoitettuja tietoja ei kuitenkaan tarvitse tallentaa varmennerekisteriin, jos varmentaja huolehtii muulla tavoin siitä, että varmenteeseen luottava osapuoli pystyy esittämään luotettavan näytön sulkulistan asianmukaisesta tarkastamisesta.

Varmentajan tulee myös ylläpitää laatuvarmenteisiin luottavien osapuolten saatavilla olevaa rekisteriä peruutetuista laatuvarmenteista (*sulkulista*). Sulkulistalle on viipymättä merkittävä tieto laatuvarmenteen peruuttamisesta sekä tarkka peruuttamisajankohta.

Edellä 2 ja 3 momentissa mainittujen tietojen on oltava ympärivuorokautisesti käytettävissä.

38 §

Varmennerekisterin tietojen säilyttäminen

Laatuvarmenteita tarjoavan varmentajan tulee luotettavalla ja tarkoituksenmukaisella tavalla säilyttää varmennerekisterin tiedot 10 vuoden ajan varmenteen voimassaolon päättymisestä.

Jos laatuvarmenteita tarjoava varmentaja tarjoaa myös vahvaa sähköistä tunnistuspalvelua, se voi 24 §:n estämättä säilyttää tietoja kaikilta osin 1 momentissa tarkoitetulla tavalla.

39 §

Varmenteen voimassaolon tarkistamista koskevan tiedon tallentaminen

Laatuvarmenteita tarjoava varmentaja saa tallentaa tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta. Tallennettuja tietoja saa käyttää ainoastaan varmenteiden käytön laskutuksen suorittamiseksi tai varmenteella varmennetun sähköisen allekirjoituksen avulla tehtyjen oikeustoimien todentamiseksi.

40 §

Vastuu allekirjoituksen luomistietojen oikeudettomasta käytöstä

Allekirjoittaja vastaa laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen luomistietojen oikeudettomasta käytöstä aiheutuneesta vahingosta, kunnes varmenteen peruuttamispyyntö on saapunut varmentajalle siten kuin 36 §:n 2 momentissa säädetään.

Kuluttajalla on kuitenkin 1 momentissa säädetty vastuu vain, jos:

1) hän on luovuttanut luomistiedot toiselle;

2) luomistietojen joutuminen niiden käyttöön oikeudettomalle on aiheutunut hänen huolimattomuudestaan, joka ei ole lievää; tai

3) hän menetettyään luomistietojen hallinnan muulla kuin 2 kohdassa mainitulla tavalla on laiminlyönyt pyytää laatuvarmenteen peruuttamista siten kuin 36 §:n 1 momentissa säädetään.

41 §

Laatuvarmenteita tarjoavan varmentajan vahingonkorvausvastuu

Laatuvarmenteita tarjoava varmentaja on vastuussa vahingosta, joka laatuvarmenteeseen luottaneelle on aiheutunut siitä, että:

1) laatuvarmenteeseen merkityt tiedot ovat varmenteen myöntämishetkellä olleet virheellisiä;

2) laatuvarmenteessa ei ole 30 §:n 2 momentissa mainittuja tietoja;

3) laatuvarmenteessa yksilöidyllä henkilöllä ei varmenteen myöntämishetkellä ollut hallussaan varmenteessa mainittuja tai määriteltyjä allekirjoituksen todentamistietoja vastaavia allekirjoituksen luomistietoja;

4) varmentajan tai sen apunaan käyttämän henkilön luomat allekirjoituksen luomis- ja todentamistiedot eivät ole yhteensopivia; taikka

5) varmentaja tai sen apunaan käyttämä henkilö ei ole peruuttanut laatuvarmennetta 36 §:ssä säädetyllä tavalla.

Varmentaja vapautuu 1 momentissa säädetystä vastuusta, jos se näyttää, että vahinko ei

ole aiheutunut sen omasta tai sen apunaan käyttämän henkilön huolimattomuudesta.

Varmentaja ei vastaa vahingosta, joka aiheutuu laatuvarmenteeseen sisältyvän käyttörajoituksen vastaisesta käytöstä.

Muilta osin laatuvarmenteita yleisölle tarjoavan varmentajan vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

Mitä tässä pykälässä säädetään, sovelletaan myös varmentajaan, joka takaa yleisölle varmenteen laatuvarmenteeksi.

5 luku

Viranomaisvalvonta

42 §

Yleinen ohjaus ja valvonta

Vahvan sähköisen tunnistamisen ja sähköisten allekirjoitusten yleinen ohjaus ja kehittäminen kuuluvat liikenne- ja viestintäministeriölle.

Viestintäviraston tehtävänä on valvoa tämän lain noudattamista lukuun ottamatta 1 §:n 3 momenttia. Viestintävirasto antaa tarvittaessa teknisiä määräyksiä tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista.

Tietosuojavaltuutetun tehtävänä on valvoa tämän lain henkilötietoja koskevien säännösten noudattamista.

Tämän lain 1 §:n 3 momentin noudattamista tunnistuspalvelun tarjoajan ja kuluttajan välisessä suhteessa valvoo kuluttaja-asiamies.

43 §

Tiedonsaantioikeus

Viestintävirastolla on oikeus salassapitosäännösten estämättä saada tunnistuspalvelun tarjoajilta ja laatuvarmenteita tarjoavilta varmentajilta sekä heidän apunaan toimivilta henkilöiltä 42 §:ssä säädettyjen tehtävien suorittamiseksi tarpeelliset tiedot.

Tietosuojavaltuutetulla on tehtäväänsä suorittaessaan henkilötietolaissa tarkoitetut tiedonsaantioikeudet.

44 §

Viranomaisten välinen yhteistyö ja oikeus luovuttaa tietoja

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Viestintävirastolla ja tietosuojavaltuutetulla on oikeus luovuttaa salassapitosäännösten estämättä Finanssivalvonnalle sellaisia tietoja, jotka ovat tarpeen sen tehtävien suorittamiseksi.

Viestintäviraston ja tietosuojavaltuutetun on tämän lain mukaisia tehtäviä hoitaessaan toimittava tarvittaessa tarkoituksenmukaisessa yhteistyössä Finanssivalvonnan, Kilpailuviraston ja Kuluttajaviraston kanssa sekä keskenään.

45 §

Hallintopakkokeinot

Jos joku rikkoo tätä lakia tai sen nojalla annettuja määräyksiä, Viestintävirasto voi velvoittaa tämän korjaamaan virheensä tai laiminlyöntinsä. Päätöksen tehosteeksi voidaan asettaa uhkasakko tai uhka, että toiminta keskeytetään osaksi tai kokonaan taikka että tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella. Uhkasakosta, keskeyttämisuhasta ja teettämisuhasta säädetään uhkasakkolaissa (1113/1990).

Teettämällä suoritetun toimenpiteen kustannukset suoritetaan valtion varoista ja peritään laiminlyöjältä siinä järjestyksessä kuin verojen ja maksujen täytäntöönpanosta annetussa laissa (706/2007) säädetään.

46 §

Tarkastusoikeus

Viestintävirastolla on oikeus tehdä tai teettää tunnistuspalvelun tarjoajaa ja sen tarjoamaa palvelua koskeva tarkastus, jos sillä on syytä epäillä, että palveluntarjoaja on olen-

naisesti rikkonut tätä lakia tai sen nojalla annettuja määräyksiä.

Viestintävirasto tekee tai teettää vuosittain laatuvarmenteita tarjoavan varmentajan ja sen tarjoamaa palvelua koskevan tarkastuksen.

Viestintävirasto määrää tarkastajan toimittamaan edellä 1 tai 2 momentissa tarkoitetun tarkastuksen. Tarkastusta toimittavalla henkilöllä on oikeus tutkia tunnistuspalvelun tarjoajan ja laatuvarmenteita tarjoavan varmentajan tai niiden apunaan käyttämien henkilöiden laitteet ja ohjelmistot, joilla voi olla merkitystä tämän lain tai sen nojalla annettujen määräysten noudattamisen valvonnassa.

Tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien tai niiden apunaan käyttämien henkilöiden on tarkastusta varten päästettävä 3 momentissa tarkoitettu tarkastaja muihin kuin kotirauhan piiriin kuuluviin valmistus-, liike- ja varastotiloihin.

Viestintävirastolla on oikeus saada virka-apua poliisilta tässä pykälässä tarkoitetun tarkastuksen suorittamiseksi.

Tietosuojavaltuutetulla on tehtäväänsä suorittaessaan henkilötietolaissa tarkoitetut tarkastusoikeudet.

47 §

Viestintävirastolle maksettavat maksut

Edellä 10 §:ssä tarkoitetun ilmoituksen tehneen tunnistuspalvelun tarjoajan tai palveluntarjoajien yhteenliittymän on suoritettava Viestintävirastolle 5000 euron rekisteröimismaksu. Lisäksi tunnistuspalvelun tarjoajan tai yhteenliittymän on suoritettava Viestintävirastolle vuosittain 12 000 euron valvontamaksu.

Laatuvarmenteita tarjoavan varmentajan on suoritettava Viestintävirastolle vuosittain 40 000 euron valvontamaksu. Jos laatuvarmenteita tarjoava varmentaja tekee myös 10 §:ssä tarkoitetun ilmoituksen, on sen maksettava 1 momentissa tarkoitettu rekisteröimismaksu.

Rekisteröimismaksu ja valvontamaksu vastaavat niitä kustannuksia, jotka aiheutuvat Viestintävirastolle tässä laissa säädettyjen tehtävien hoitamisesta 46 §:n 1 momentissa tarkoitettuja tehtäviä lukuun ottamatta. Valvontamaksu on suoritettava täysimääräisesti myös toiminnan ensimmäisenä vuotena, vaikka toiminta aloitettaisiin kesken vuotta. Valvontamaksua ei palauteta, vaikka palveluntarjoaja lopettaisi toimintansa kesken vuotta.

Rekisteröimismaksun ja valvontamaksun määrää maksettavaksi Viestintävirasto. Viestintäviraston maksun määräämistä koskevaan päätökseen saa hakea muutosta siten kuin 49 §:n 1 momentissa säädetään. Tarkempia säännöksiä maksujen täytäntöönpanosta voidaan antaa liikenne- ja viestintäministeriön asetuksella.

Rekisteröimismaksu ja valvontamaksu saadaan periä ilman tuomiota tai päätöstä siinä järjestyksessä kuin verojen ja maksujen täytäntöönpanosta annetussa laissa säädetään. Jollei maksuja suoriteta viimeistään eräpäivänä, maksamattomalle määrälle peritään vuotuista viivästyskorkoa korkolain (633/1982) 4 §:n 1 momentissa tarkoitetun korkokannan mukaan. Viivästyskoron sijasta viranomainen voi periä viiden euron suuruisen viivästysmaksun, jos viivästyskoron määrä jää tätä pienemmäksi.

Jos tunnistuspalvelun tarjoajan toiminta joudutaan 46 §:n 1 momentin nojalla tarkastamaan, tunnistuspalvelun tarjoajalta peritään tarkastuksesta aiheutuneet kustannukset siten kuin valtion maksuperustelaissa säädetään.

6 luku

Erinäiset säännökset

48 §

Rangaistussäännökset

Rangaistus henkilörekisteririkoksesta säädetään rikoslain (39/1889) 38 luvun 9 §:ssä ja henkilörekisteririkkomuksesta henkilötietolain 48 §:n 2 momentissa.

49 §

Muutoksenhaku

Muutoksen hakemisesta Viestintäviraston tämän lain nojalla tekemään päätökseen säädetään hallintolainkäyttölaissa (586/1996).

Viestintävirasto voi päätöksessään määrätä, että päätöstä on noudatettava ennen kuin se on saanut lainvoiman. Valitusviranomainen voi kuitenkin kieltää päätöksen täytäntöönpanon, kunnes valitus on ratkaistu.

Muutoksenhausta tietosuojavaltuutetun päätökseen säädetään henkilötietolaissa.

7 luku

Voimaantulo

50 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Tällä lailla kumotaan 24 päivänä tammikuuta 2003 annettu laki sähköisistä allekirjoituksista (14/2003). Viestintäviraston kumottavan lain nojalla antamat määräykset ovat kuitenkin voimassa, kunnes uudet määräykset annetaan tämän lain nojalla.

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimiin.

51 §

Siirtymäsäännös

Tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle 10 §:ssä tarkoitettu ilmoitus kuuden kuukauden kuluessa lain voimaantulosta. Sinä aikana vahvana sähköisenä tunnistuspalveluna ja tunnistuspalvelun tarjoajana pidetään sellaista 1 §:n soveltamisalaan kuuluvaa sähköistä tunnistuspalvelua ja sähköisen tunnistuspalvelun tarjoajaa, joka täyttää 2 §:n 1 ja 4 kohdassa tarkoitetut määritelmät.

Ennen tämän lain voimaan tuloa tai 1 momentissa tarkoitetun siirtymäajan kuluessa liikkeelle laskettuja tunnistusvälineitä pidetään vahvan sähköisen tunnistamisen välineinä, jos tunnistuspalvelun tarjoaja tekee 10 §:ssä tarkoitetun ilmoituksen 1 momentissa tarkoitetun ajan kuluessa. Tunnistuspalvelun ja tunnistuspalvelun tarjoajan on tällöin täytettävä kaikki tässä laissa niille asetetut vaatimukset lukuun ottamatta 17 §:ssä säädettyjä vaatimuksia.

Jos tunnistuspalvelun tarjoajat ovat tehneet 17 §:n 2 momentissa tarkoitetun sopimuksen mahdollisuudesta luottaa toistensa tekemään ensitunnistamiseen, eikä ensitunnistamisessa käytetyt tunnistusvälineet liikkeelle laskenut palveluntarjoaja ole tehnyt 10 §:ssä tarkoitettua ilmoitusta 1 momentissa tarkoitetussa ajassa, ensitunnistaminen on tällä tavoin liikkeelle laskettujen tunnistusvälineiden osalta tehtävä 17 §:ssä tarkoitetulla tavalla viivyttelemättä.

Sellaisen laatuvarmenteita tarjoavan varmentajan, joka on tehnyt sähköisistä allekirjoituksista annetun lain 9 §:n 1 momentin mukaisen ilmoituksen ja jatkanut toimintaansa keskeytyksettä tämän lain voimaan tuloon saakka, ei tarvitse tehdä uutta ilmoitusta 32 §:n 1 momentin mukaisesti. Laatuvarmenteita tarjoava varmentaja voi tällöin antaa Viestintävirastolle vapaamuotoisen kirjallisen ilmoituksen toimintansa jatkumisesta entisellään.

Sen estämättä, mitä 17 §:n 1 momentissa ja 35 §:n 1 momentissa säädetään, tunnistuspalvelun tarjoaja ja laatuvarmenteita tarjoava varmentaja voivat 31 päivään joulukuuta 2012 käyttää ensitunnistamisessa Euroopan talousalueen jäsenvaltion viranomaisen 1 päivän lokakuuta 1990 jälkeen myöntämää voimassa olevaa ajokorttia.

2.

Laki

sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähköisestä asioinnista viranomaistoiminnassa 24 päivänä tammikuuta 2003 annetun lain (13/2003) 3 §:n 2 momentti, 9 §:n 1 momentti, 16 § ja 18 §:n 2 momentti seuraavasti:

3 §

Muu lainsäädäntö

— — — — — — — — — — — — — — —

Sähköisistä allekirjoituksista sekä niihin liittyvästä tunnistuspalveluiden ja laatuvarmenteiden tarjoamisesta säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) .

9 §

Kirjallisen muodon ja allekirjoitusvaatimuksen täyttyminen

Vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja. Jos asian vireillepanossa tai muussa käsittelyssä edellytetään allekirjoitettua asiakirjaa, allekirjoitusvaatimuksen täyttää myös vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momentissa tarkoitettu sähköinen allekirjoitus.

— — — — — — — — — — — — — — —

16 §

Päätösasiakirjan sähköinen allekirjoittaminen

Päätösasiakirja voidaan allekirjoittaa sähköisesti. Viranomaisen on allekirjoitettava asiakirja siten kuin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momentissa tarkoitetaan.

18 §

Todisteellinen sähköinen tiedoksianto

— — — — — — — — — — — — — — —

Asianosaisen tai tämän edustajan on tunnistauduttava päätöstä noutaessaan. Tunnistautumisessa voidaan käyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitettua tunnistusvälinettä tai laatuvarmennetta tai muuta tunnistautumistekniikkaa, joka on tietoturvallinen ja todisteellinen.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

3.

Laki

väestötietolain 19 ja 20 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 11 päivänä kesäkuuta 1993 annetun väestötietolain (507/1993) 19 §:n 3 momentti ja 20 §:n 1 momentti, sellaisina kuin ne ovat laissa 299/2003, seuraavasti:

19 §

Varmennettu sähköinen asiointi

— — — — — — — — — — — — — — —

Sähköisiin allekirjoituksiin liittyvien Väestörekisterikeskuksen myöntämien varmenteiden tarjoamisesta, varmentajan velvollisuuksista ja vastuista sekä henkilötietojen käsittelystä on lisäksi voimassa, mitä niistä säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ).

20 §

Varmennetussa sähköisessä asioinnissa käytettävän varmenteen tiedot

Väestörekisterikeskuksen henkilölle myöntämään sähköiseen allekirjoitukseen liittyvään varmenteeseen sisältyvistä tiedoista on voimassa, mitä laatuvarmenteeseen sisältyvistä tiedoista säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 30 §:ssä. Väestörekisterikeskuksen myöntämässä kansalaisvarmenteessa varmenteen haltijan yksilöivänä tunnistetietona on jäljempänä 21 §:ssä tarkoitettu sähköinen asiointitunnus. Kansalaisvarmenteeseen sisältyy lisäksi muita varmenteen käytön edellyttämiä välttämättömiä teknisiä tietoja.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

4.

Laki

sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 2 ja 9 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9 päivänä helmikuuta 2007 annetun lain (159/2007) 2 §:n 3 momentti ja 9 § seuraavasti:

2 §

Soveltamisala

— — — — — — — — — — — — — — —

Jollei tästä tai muusta laista muuta johdu, asiakastietojen käsittelyyn sovelletaan, mitä potilaan asemasta ja oikeuksista annetussa laissa (785/1992), jäljempänä *potilaslaki*, sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa (812/2000), jäljempänä *asiakaslaki*, henkilötietolaissa (523/1999), viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) sekä arkistolaissa (831/1994) tai näiden nojalla säädetään.

9 §

Asiakirjan sähköinen allekirjoittaminen

Asiakastietojen eheys, muuttumattomuus ja kiistämättömyys tulee varmistaa sähköisellä allekirjoituksella tietojen sähköisessä käsittelyssä, tiedonsiirrossa ja säilytyksessä. Luonnollisen henkilön sähköisessä allekirjoittamisessa tulee käyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitettua kehittynyttä sähköistä allekirjoitusta. Organisaation ja tietoteknisten laitteiden allekirjoituksessa on käytettävä luotettavuudeltaan vastaavaa sähköistä allekirjoitusta.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

5.

Laki

viestintähallinnosta annetun lain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan viestintähallinnosta 29 päivänä kesäkuuta 2001 annetun lain (625/2001) 2 §:n 1 kohta, sellaisena kuin se on laissa 520/2004, seuraavasti:

2 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on:

1) huolehtia viestintämarkkinalaissa (393/2003), radiotaajuuksista ja telelaitteista annetussa laissa (1015/2001), postipalvelulaissa (313/2001), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998), sähköisen viestinnän tietosuojalaissa (516/2004), eräiden suojauksen purkujärjestelmien kieltämisestä annetussa laissa (1117/2001), vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) sekä verkkotunnuslaissa (228/2003) sille säädetyistä tehtävistä; sekä

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

6.

Laki

rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetun lain 18 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä 18 päivänä heinäkuuta 2008 annetun lain (503/2008) 18 §:n 3 kohta seuraavasti:

18 §

Etätunnistamiseen liittyvä tehostettu tuntemisvelvollisuus

Jos asiakas ei ole läsnä tunnistettaessa ja henkilöllisyyttä todennettaessa (*etätunnistaminen*), ilmoitusvelvollisen tulee rahanpesun ja terrorismin rahoittamisen riskin vähentämiseksi:

— — — — — — — — — — — — — — —

3) todentaa asiakkaan henkilöllisyys vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla tunnistusvälineellä tai laatuvarmenteella taikka muun sähköisen tunnistamistekniikan avulla, joka on tietoturvallinen ja todisteellinen.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

7.

Laki

varainsiirtoverolain 56 b §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 29 päivänä marraskuuta 1996 annetun varainsiirtoverolain (931/1996) 56 b §:n 2 momentti, sellaisena kuin se on laissa 1085/2005, seuraavasti:

56 b §

Sähköinen asiointi ja allekirjoittaminen

— — — — — — — — — — — — — — —

Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

8.

Laki

verotusmenettelystä annetun lain 93 a §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan verotusmenettelystä 18 päivänä joulukuuta 1995 annetun lain (1558/1995) 93 a §:n 2 momentti, sellaisena kuin se on laissa 1079/2005, seuraavasti:

93 a §

Sähköinen asiointi ja allekirjoittaminen

— — — — — — — — — — — — — — —

Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

9.

Laki

arvonlisäverolain 165 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 30 päivänä joulukuuta 1993 annetun arvonlisäverolain (1501/1993) 165 §:n 3 momentti, sellaisena kuin se on laissa 1083/2005, seuraavasti:

165 §

— — — — — — — — — — — — — — — —

Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla.

— — — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

10.

Laki

ennakkoperintälain 6 a §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 20 päivänä joulukuuta 1996 annetun ennakkoperintälain (1118/1996) 6 a §:n 2 momentti, sellaisena kuin se on laissa 1082/2005, seuraavasti:

6 a §

Sähköinen asiointi ja allekirjoittaminen

— — — — — — — — — — — — — — — — —

Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla.

— — — — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

11.

Laki

veripalvelulain 11 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan 1 päivänä huhtikuuta 2005 annetun veripalvelulain (197/2005) 11 § seuraavasti:

11 §

Luovuttajiin liittyvät tiedot

Veren ja sen osan luovuttajalle on ennen luovutusta annettava luovutukseen liittyvät tarpeelliset tiedot sekä henkilötietolain (523/1999) 24 §:n mukaiset tiedot ja luovuttajaa on informoitava tietojen salassapidosta. Luovuttajalta on pyydettävä hänen yksilöintiään koskevat tiedot, luovutuskelpoisuutta arvioitaessa hänen terveydentilaansa liittyvät ja välttämättömät luovuttajan luovutuskelpoisuutta koskevat tiedot sekä luovuttajan omakätinen allekirjoitus tai vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain ( ) mukainen kehittynyt sähköinen allekirjoitus. Lääkelaitos voi antaa tarkempia määräyksiä luovuttajille annettavista ja heiltä pyydettävistä tiedoista.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

Helsingissä 27 päivänä maaliskuuta 2009

Tasavallan Presidentti

TARJA HALONEN

Viestintäministeri *Suvi Lindén*

Rinnakkaistekstit

2.

Laki

sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähköisestä asioinnista viranomaistoiminnassa 24 päivänä tammikuuta 2003 annetun lain (13/2003) 3 §:n 2 momentti, 9 §:n 1 momentti, 16 § ja 18 §:n 2 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Muu lainsäädäntö	*Muu lainsäädäntö*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Sähköisten allekirjoitusten käytöstä ja niihin liittyvistä varmennepalveluista säädetään sähköisistä allekirjoituksista annetussa laissa (14/2003).	Sähköisistä allekirjoituksista *sekä* niihin liittyvistä *tunnistuspalveluiden ja laatuvarmenteiden tarjoamisesta* säädetään *vahvasta* sähköisestä *tunnistamisesta ja* sähköisistä allekirjoituksista annetussa laissa ( ) .
9 §	9 §
Kirjallisen muodon ja allekirjoitusvaatimuksen täyttyminen	*Kirjallisen muodon ja allekirjoitusvaatimuksen täyttyminen*
Vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja. Jos asian vireillepanossa tai muussa käsittelyssä edellytetään allekirjoitettua asiakirjaa, allekirjoitusvaatimuksen täyttää myös sähköisistä allekirjoituksista annetun lain 18 §:ssä tarkoitettu sähköinen allekirjoitus.	Vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja. Jos asian vireillepanossa tai muussa käsittelyssä edellytetään allekirjoitettua asiakirjaa, allekirjoitusvaatimuksen täyttää myös *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momentissa* tarkoitettu sähköinen allekirjoitus.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Voimassa oleva laki	*Ehdotus*
16 §	16 §
Päätösasiakirjan sähköinen allekirjoittaminen	*Päätösasiakirjan sähköinen allekirjoittaminen*
Päätösasiakirja voidaan allekirjoittaa sähköisesti. Viranomaisen sähköisen allekirjoituksen on täytettävä sähköisistä allekirjoituksista annetun lain 18 §:ssä säädetyt edellytykset.	Päätösasiakirja voidaan allekirjoittaa sähköisesti. *Viranomaisen on allekirjoitettava asiakirja siten kuin vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momentissa tarkoitetaan*.
18 §	18 §
Todisteellinen sähköinen tiedoksianto	*Todisteellinen sähköinen tiedoksianto*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Asianosaisen tai tämän edustajan on tunnistauduttava päätöstä noutaessaan. Tunnistautumisessa on käytettävä sellaista varmennetta, joka täyttää sähköisistä allekirjoituksista annetussa laissa laatuvarmenteelle asetetut vaatimukset, tai muuta tunnistautumistekniikkaa, joka on tietoturvallinen ja todisteellinen.	Asianosaisen tai tämän edustajan on tunnistauduttava päätöstä noutaessaan. *Tunnistautumisessa voidaan käyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitettua tunnistusvälinettä tai laatuvarmennetta* tai muuta tunnistautumistekniikkaa*,* joka on tietoturvallinen ja todisteellinen.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

3.

Laki

väestötietolain 19 ja 20 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan 11 päivänä kesäkuuta 1993 annetun väestötietolain (507/1993) 19 §:n 3 momentti ja 20 §:n 1 momentti, sellaisina kuin ne ovat laissa 299/2003, seuraavasti:

Voimassa oleva laki	*Ehdotus*
19 §	19 §
Varmennettu sähköinen asiointi	*Varmennettu sähköinen asiointi*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Sähköisiin allekirjoituksiin liittyvien Väestörekisterikeskuksen myöntämien varmenteiden tarjoamisesta, varmentajan velvollisuuksista ja vastuista sekä henkilötietojen käsittelystä on lisäksi voimassa, mitä niistä säädetään sähköisistä allekirjoituksista annetussa laissa (14/2003).	Sähköisiin allekirjoituksiin liittyvien Väestörekisterikeskuksen myöntämien varmenteiden tarjoamisesta, varmentajan velvollisuuksista ja vastuista sekä henkilötietojen käsittelystä on lisäksi voimassa, mitä niistä säädetään *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa* ( ).
20 §	20 §
Varmennetussa sähköisessä asioinnissa käytettävän varmenteen tiedot	*Varmennetussa sähköisessä asioinnissa käytettävän varmenteen tiedot*
Väestörekisterikeskuksen henkilölle myöntämään sähköiseen allekirjoitukseen liittyvään varmenteeseen sisältyvistä tiedoista on voimassa, mitä laatuvarmenteeseen sisältyvistä tiedoista säädetään sähköisistä allekirjoituksista annetun lain 7 §:ssä. Väestörekisterikeskuksen myöntämässä kansalaisvarmenteessa varmenteen haltijan yksilöivänä tunnistetietona on jäljempänä 21 §:ssä tarkoitettu sähköinen asiointitunnus. Kansalaisvarmenteeseen sisältyy lisäksi muita varmenteen käytön edellyttämiä välttämättömiä teknisiä tietoja.	Väestörekisterikeskuksen henkilölle myöntämään sähköiseen allekirjoitukseen liittyvään varmenteeseen sisältyvistä tiedoista on voimassa, mitä laatuvarmenteeseen sisältyvistä tiedoista säädetään *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 30 §:ssä*. Väestörekisterikeskuksen myöntämässä kansalaisvarmenteessa varmenteen haltijan yksilöivänä tunnistetietona on jäljempänä 21 §:ssä tarkoitettu sähköinen asiointitunnus. Kansalaisvarmenteeseen sisältyy lisäksi muita varmenteen

Voimassa oleva laki	*Ehdotus*
	käytön edellyttämiä välttämättömiä teknisiä tietoja.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

4.

Laki

sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 2 ja 9 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9 päivänä helmikuuta 2007 annetun lain (159/2007) 2 §:n 3 momentti ja 9 § seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Soveltamisala	*Soveltamisala*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Jollei tästä tai muusta laista muuta johdu, asiakastietojen käsittelyyn sovelletaan, mitä potilaan asemasta ja oikeuksista annetussa laissa (785/1992), jäljempänä *potilaslaki*, sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa (812/2000), jäljempänä *asiakaslaki*, henkilötietolaissa (523/1999), viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), sähköisistä allekirjoituksista annetussa laissa (14/2003) sekä arkistolaissa (831/1994) tai näiden nojalla säädetään.	Jollei tästä tai muusta laista muuta johdu, asiakastietojen käsittelyyn sovelletaan, mitä potilaan asemasta ja oikeuksista annetussa laissa (785/1992), jäljempänä potilaslaki, sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa (812/2000), jäljempänä asiakaslaki, henkilötietolaissa (523/1999), viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa( )* sekä arkistolaissa (831/1994) tai näiden nojalla säädetään.
9 §	9 §
Asiakirjan sähköinen allekirjoittaminen	*Asiakirjan sähköinen allekirjoittaminen*
Asiakastietojen eheys, muuttumattomuus ja kiistämättömyys tulee varmistaa sähköisellä allekirjoituksella tietojen sähköisessä käsittelyssä, tiedonsiirrossa ja säilytyksessä. Luonnollisen henkilön sähköisessä allekirjoittamisessa tulee käyttää sähköisistä allekirjoituksista annetussa laissa tarkoitettua kehittynyttä	Asiakastietojen eheys, muuttumattomuus ja kiistämättömyys tulee varmistaa sähköisellä allekirjoituksella tietojen sähköisessä käsittelyssä, tiedonsiirrossa ja säilytyksessä. Luonnollisen henkilön sähköisessä allekirjoittamisessa tulee käyttää *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista*

Voimassa oleva laki	*Ehdotus*
sähköistä allekirjoitusta. Organisaation ja tietoteknisten laitteiden allekirjoituksessa on käytettävä luotettavuudeltaan vastaavaa sähköistä allekirjoitusta.	*annetussa laissa* tarkoitettua kehittynyttä sähköistä allekirjoitusta. Organisaation ja tietoteknisten laitteiden allekirjoituksessa on käytettävä luotettavuudeltaan vastaavaa sähköistä allekirjoitusta. — — — — — — — — — — — — — —
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

5.

Laki

viestintähallinnosta annetun lain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan viestintähallinnosta 29 päivänä kesäkuuta 2001 annetun lain (625/2001) 2 §:n 1 kohta, sellaisena kuin se on laissa 520/2004, seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Viestintäviraston tehtävät	*Viestintäviraston tehtävät*
Viestintäviraston tehtävänä on: 1) huolehtia viestintämarkkinalaissa (393/2003), radiolaissa (1015/2001), postipalvelulaissa (313/2001), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998), sähköisen viestinnän tietosuojalaissa (516/2004), eräiden suojauksen purkujärjestelmien kieltämisestä annetussa laissa (1117/2001), sähköisistä allekirjoituksista annetussa laissa (14/2003) sekä verkkotunnuslaissa (228/2003) sille säädetyistä tehtävistä; sekä — — — — — — — — — — — — — — —	Viestintäviraston tehtävänä on: 1) huolehtia viestintämarkkinalaissa (393/2003), radiotaajuuksista ja telelaitteista annetussa laissa (1015/2001), postipalvelulaissa (313/2001), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998), sähköisen viestinnän tietosuojalaissa (516/2004), eräiden suojauksen purkujärjestelmien kieltämisestä annetussa laissa (1117/2001), *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( )* sekä verkkotunnuslaissa (228/2003) sille säädetyistä tehtävistä; sekä — — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

6.

Laki

rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetun lain 18 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rahanpesusta ja terrorismin rahoittamisen estämisestä ja selvittämisestä 18 päivänä heinäkuuta 2008 annetun lain (503/2008) 18 §:n 3 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
18 §	18 §
Etätunnistamiseen liittyvä tehostettu tuntemisvelvollisuus	*Etätunnistamiseen liittyvä tehostettu tuntemisvelvollisuus*
Jos asiakas ei ole läsnä tunnistettaessa ja henkilöllisyyttä todennettaessa (*etätunnistaminen*), ilmoitusvelvollisen tulee rahanpesun ja terrorismin rahoittamisen riskin vähentämiseksi:	Jos asiakas ei ole läsnä tunnistettaessa ja henkilöllisyyttä todennettaessa (*etätunnistaminen*), ilmoitusvelvollisen tulee rahanpesun ja terrorismin rahoittamisen riskin vähentämiseksi:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
3) todentaa asiakkaan henkilöllisyys sähköisistä allekirjoituksista annetussa laissa (14/2003) tarkoitetulla laatuvarmenteella tai muun sähköisen tunnistamistekniikan avulla, joka on tietoturvallinen ja todisteellinen.	3) todentaa asiakkaan henkilöllisyys *vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa* ( ) tarkoitetulla *tunnistusvälineellä tai* laatuvarmenteella *taikka* muun sähköisen tunnistamistekniikan avulla, joka on tietoturvallinen ja todisteellinen.
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

7.

Laki

varainsiirtoverolain 56 b §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 29 päivänä marraskuuta 1996 annetun varainsiirtoverolain (931/1996) 56 b §:n 2 momentti, sellaisena kuin se on laissa 1085/2005, seuraavasti:

Voimassa oleva laki	*Ehdotus*
56 b §	56 b §
Sähköinen asiointi ja allekirjoittaminen	*Sähköinen asiointi ja allekirjoittaminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa sähköisesti ja jotka on allekirjoitettava, siten kuin siitä erikseen säädetään, katsotaan allekirjoitetuiksi silloin, kun ne täyttävät sähköisistä allekirjoituksista annetun lain (14/2003) vaatimukset.	Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa *veroviranomaiselle* sähköisesti ja jotka on allekirjoitettava, *on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muulla hyväksyttävällä tavalla.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

8.

Laki

verotusmenettelystä annetun lain 93 a §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan verotusmenettelystä 18 päivänä joulukuuta 1995 annetun lain (1558/1995) 93 a §:n 2 momentti, sellaisena kuin se on laissa 1079/2005, seuraavasti:

Voimassa oleva laki	*Ehdotus*
93 a §	93 a §
Sähköinen asiointi ja allekirjoittaminen	*Sähköinen asiointi ja allekirjoittaminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava sähköisistä allekirjoituksista annetun lain (14/2003) 18 §:ssä tarkoitetulla tai muulla hyväksyttävällä tavalla.	Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, *on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa () tarkoitetulla kehittyneellä sähköisellä allekirjoituksella* tai muulla hyväksyttävällä tavalla.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	_____
	Tämä laki tulee voimaan päivänä kuuta 20 .
	_____

9.

Laki

arvonlisäverolain 165 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 30 päivänä joulukuuta 1993 annetun arvonlisäverolain (1501/1993) 165 §:n 3 momentti, sellaisena kuin se on laissa 1083/2005, seuraavasti:

Voimassa oleva laki	*Ehdotus*
165 §	165 §
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava sähköisistä allekirjoituksista annetun lain (14/2003) 18 §:ssä tarkoitetulla tai muulla hyväksyttävällä tavalla.	Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti *ja jotka on allekirjoitettava, on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella* tai muulla hyväksyttävällä tavalla.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

10.

Laki

ennakkoperintälain 6 a §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 20 päivänä joulukuuta 1996 annetun ennakkoperintälain (1118/1996) 6 a §:n 2 momentti, sellaisena kuin se on laissa 1082/2005, seuraavasti:

Voimassa oleva laki	*Ehdotus*
6 a §	6 a §
Sähköinen asiointi ja allekirjoittaminen	*Sähköinen asiointi ja allekirjoittaminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, on varmennettava sähköisistä allekirjoituksista annetun lain (14/2003) 18 §:ssä tarkoitetulla tai muulla hyväksyttävällä tavalla.	Ilmoitukset ja muut asiakirjat, jotka voidaan toimittaa veroviranomaiselle sähköisesti ja jotka on allekirjoitettava, *on varmennettava vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa ( ) tarkoitetulla kehittyneellä sähköisellä allekirjoituksella* tai muulla hyväksyttävällä tavalla.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

11.

Laki

veripalvelulain 11 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan 1 päivänä huhtikuuta 2005 annetun veripalvelulain (197/2005) 11 § seuraavasti:

Voimassa oleva laki	*Ehdotus*
11 §	11 §
Luovuttajiin liittyvät tiedot	*Luovuttajiin liittyvät tiedot*
Veren ja sen osan luovuttajalle on ennen luovutusta annettava luovutukseen liittyvät tarpeelliset tiedot sekä henkilötietolain (523/1999) 24 §:n mukaiset tiedot ja luovuttajaa on informoitava tietojen salassapidosta. Luovuttajalta on pyydettävä hänen yksilöintiään koskevat tiedot, luovutuskelpoisuutta arvioitaessa hänen terveydentilaansa liittyvät ja välttämättömät luovuttajan luovutuskelpoisuutta koskevat tiedot sekä luovuttajan omakätinen allekirjoitus tai sähköisestä allekirjoituksesta annetun lain (14/2003) mukainen kehittynyt sähköinen allekirjoitus. Lääkelaitos voi antaa tarkempia määräyksiä luovuttajille annettavista ja heiltä pyydettävistä tiedoista.	Veren ja sen osan luovuttajalle on ennen luovutusta annettava luovutukseen liittyvät tarpeelliset tiedot sekä henkilötietolain (523/1999) 24 §:n mukaiset tiedot ja luovuttajaa on informoitava tietojen salassapidosta. Luovuttajalta on pyydettävä hänen yksilöintiään koskevat tiedot, luovutuskelpoisuutta arvioitaessa hänen terveydentilaansa liittyvät ja välttämättömät luovuttajan luovutuskelpoisuutta koskevat tiedot sekä luovuttajan omakätinen allekirjoitus *tai vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain ( )* mukainen kehittynyt sähköinen allekirjoitus. Lääkelaitos voi antaa tarkempia määräyksiä luovuttajille annettavista ja heiltä pyydettävistä tiedoista.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____