

Hallituksen esitys Eduskunnalle laeiksi sähköisistä allekirjoituksista ja viestintähallinnosta annetun lain 2 §:n muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki sähköisistä allekirjoituksista. Sähköisiä allekirjoituksia ja niiden käytössä tarvittavia tuotteita ja palveluita koskevalla lailla edistettäisiin kuluttajien ja muiden käyttäjien luottamusta verkkoliiketoimintaan ja sähköiseen asiointiin. Laki edistäisi uuden ja kasvavan liiketoimintasektorin, varmentamisen kehittymistä. Toteutuessaan laki lisäisi sähköistä kaupankäyntiä ja asiointia sekä tietoyhteiskuntapalvelujen käyttöä.

Lailla säädettäisiin sähköisestä allekirjoituksesta ja sen oikeusvaikutuksista. Laissa määriteltyjen turvallisen allekirjoituksen luomisvälineen ja laatuvarmenteen avulla tehdyille kehittyneelle sähköiselle allekirjoitukselle taattaisiin tasavertainen asema perinteisen käsin tehdyn allekirjoituksen kanssa.

Laki ei koski muuhun tarkoitukseen kuin sähköiseen allekirjoitukseen liittyvien tuotteiden ja palveluiden tarjoamista. Ehdotuksen mukaan sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjonta olisi vapaa elinkeino. Lisäksi annettaisiin tarpeellinen lainsäädäntö sähköisiin allekirjoituksiin liittyvien varmenteiden tarjonnasta, niiden tarjoajien velvollisuuksista ja vastuista sekä henkilötietojen suojasta.

Lailla säädettäisiin laadullisesti korkeatasoisen laatuvarmenteen tarjoajan velvollis-

suuksista, jotka parantavat sähköisen allekirjoituksen luotettavuutta. Velvollisuudet koskisivat muun muassa varmenteen hakijan luotettavaa tunnistamista, turvallisten järjestelmien käyttöä, riittäviä teknisiä ja taloudellisia voimavaroja sekä henkilöstön pätevyyttä. Laissa olisi niin ikään laatuvarmenteen sisältöä koskevat minimivaatimukset. Laatuvarmenteita yleisölle tarjoava varmentaja olisi laissa säädetyin rajoituksin vastuussa virheellisen laatuvarmenteen aiheuttamista vahingoista laatuvarmenteella varmennettuun sähköiseen allekirjoitukseen luottaneelle taholle.

Laatuvarmenteen tarjoajan olisi tehtävä ilmoitus toiminnastaan Viestintävirastolle, joka valvoisi laatuvarmenteiden tarjontaa. Esitykseen sisältyy myös ehdotus viestintähallinnosta annetun lain muuttamisesta. Muutoksella lisättäisiin Viestintäviraston tehtäviin sähköisistä allekirjoituksista annetussa laissa sille säädetyt tehtävät.

Ehdotetuilla laeilla pantaisiin täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu Euroopan parlamentin ja neuvoston direktiivi.

Ehdotetut lait ovat tarkoitettut tulemaan voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytty ja vahvistettu.

SISÄLLYSLUETTELO

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ	1
SISÄLLYSLUETTELO	2
YLEISPERUSTELUT	4
1. Johdanto	4
2. Nykytila.....	7
2.1. Lainsäädäntö ja käytäntö.....	7
Sähköisen allekirjoituksen oikeusvaikutus	7
Sähköisen allekirjoituksen varmentaminen.....	7
2.2. Euroopan yhteisöjen direktiivi sähköisistä allekirjoituksista.....	8
2.3. Kansainvälinen kehitys ja ulkomainen lainsäädäntö	10
Ruotsi, Norja ja Tanska	10
Eräät muut maat.....	11
Kansainväliset järjestöt.....	11
Standardointi	12
2.4. Nykytilan arviointi.....	12
3. Esityksen tavoitteet ja keskeiset ehdotukset.....	13
4. Esityksen vaikutukset	14
4.1. Taloudelliset vaikutukset	14
4.2. Organisaatio- ja henkilöstövaikutukset	14
4.3. Ympäristövaikutukset	15
4.4. Vaikutukset eri kansalaisryhmien asemaan.....	15
5. Asian valmistelu	15
5.1. Valmisteluvaiheet ja -aineisto	15
5.2. Lausunnot.....	16
6. Muita esitykseen vaikuttavia seikkoja	17
YKSITYISKOHTAISET PERUSTELUT	18
1. Lakiehdotusten perustelut	18
1.1. Laki sähköisistä allekirjoituksista.....	18
1 luku. Yleiset säännökset	18
2 luku. Laatuvarmenteiden tarjoaminen.....	22
3 luku. Sähköisen allekirjoituksen oikeusvaikutus ja henkilötietojen käsittely....	33
4 luku. Yleinen ohjaus ja valvonta	35
5 luku. Erinäiset säännökset	36
1.2. Laki viestintähallinnosta	37
2. Tarkemmat säännökset ja määräykset.....	37
3. Voimaantulo	37
4. Sääntämisyjärjestys	37

LAKIEHDOTUKSET	40
sähköisistä allekirjoituksista.....	40
viestintähallinnosta annetun lain 2 §:n muuttamisesta.....	48
LIITE	49
RINNAKKAISTEKSTIT	49
viestintähallinnosta annetun lain 2 §:n muuttamisesta.....	49

YLEISPERUSTELUT

1. Johdanto

Viestinnän ja tietotekniikan kehitys ovat johtaneet sähköisen kaupankäynnin, laajemmin ilmaisten verkkoliiketoiminnan kasvuun. Alan toimintaa ei ole juurikaan erityisesti säännelty, vaan kehitys on ollut pitkälti markkinoiden ohjauksessa. Suomessa harjoitetun viestintäpolitiikan mukaisesti julkinen valta ei ole puuttunut sinänsä suotuisaan verkkoliiketoiminnan kehitykseen lainsäädännöllä.

Merkittävimpiä verkkoliiketoiminnan kasvun hidasteita on se, että kuluttajat ja muut käyttäjät eivät tunne luottamusta verkkoliiketoimintaan. Oikeustoimien tekemistä ei koeta turvalliseksi, kun henkilökohtainen kontakti oikeustoimen toiseen osapuoleen puuttuu. Osapuolten tunnistamiseen ja tietoon viestin säilymisestä muuttumattomana on kaivattu uusia palveluita ja välineitä. Sähköisen allekirjoituksen asema suhteessa perinteiseen allekirjoitukseen on myös aiheuttanut epävarmuutta.

Uusi teknologia tarjoaa koko ajan kehittyneempiä apuvälineitä siihen, että henkilö voi osoittaa tahdonilmaisunsa luotettavasti sähköisellä allekirjoituksella. Riskien täydellinen poistaminen ei ole mahdollista millään menetelmällä. Uusilla korkeatasoisilla varmenteilla päästään kuitenkin erittäin korkeaan turvallisuustasoon ja suureen varmuuteen.

Lainsäädännöllä ei tulisi asettaa esteitä oikeustoimien tekemiselle tietoverkoissa, vaan lainsäädännön tulisi luoda suotuisa ja uusia oikeustoimien toteuttamistapoja tukeva säädösympäristö. Uusien ja entistä luotettavimpien teknologioiden ja palveluiden käyttöä tulisi edistää, mikä edellyttää erityissäännösten antamista sähköisistä allekirjoituksista ja niihin liittyvistä varmenteista. Euroopan yhteisö on jo antanut asiasta direktiivin, Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY sähköisiä allekirjoituksia koskevista yhteisön puitteista, jäljempänä sähköallekirjoitusdirektiivi. Direktiivi tulee saattaa osaksi kansallista lainsäädäntöä 19 päivään

heinäkuuta 2001 mennessä.

Sähköinen allekirjoitus tulisi nähdä millaisena tahansa teknisesti toteutettuna allekirjoituksena, käytetystä teknologiasta riippumatta, jonka avulla allekirjoittajan henkilöllisyys voidaan todeta ja liittää kyseinen henkilö allekirjoituksella vahvistettavaan tahdonilmaisuuksiin. Samalla tulisi kuitenkin huomioida erityisesti kehittyneemmällä tekniikoilla tehdyt sähköiset allekirjoitukset, sillä näiden avulla voidaan lisätä sähköisten allekirjoitusten turvallisuutta ja luotettavuutta huomattavasti. Uutta tekniikkaa hyödyntäviä allekirjoituksia ovat muun muassa niin kutsuttua julkisen avaimen infrastruktuuria hyödyntävät digitaaliset allekirjoitukset. Tulevaisuudessa yleistynevät myös sähköiset allekirjoitukset, jotka hyödyntävät biometristä tunnistamista, esimerkiksi sormenjälkeä, osana allekirjoituksen luomisprosessia.

Sähköisen allekirjoituksen luomiseen liittyy useampia vaiheita kuin allekirjoituksen luomiseen käsin. Toisin kuin reaali maailmassa sähköiseen allekirjoitukseen ei liity ”käsiä”, jota vertailemalla voitaisiin päätellä kenelle allekirjoitus kuuluu. Sähköisiin allekirjoituksiin liittyykin olennaisena osana varmentajan toiminta. Sähköisen allekirjoituksen luotettavuus perustuu siihen, että jokin taho (varmentaja) varmistaa allekirjoittajan henkilöllisyyden. Sähköiseen allekirjoitukseen luottava osapuoli voi tunnistaa allekirjoittajan varmentajan allekirjoittajalle myöntämän varmenteen avulla.

Tällä hetkellä käytetyimmät sähköisten allekirjoitusten toteuttamistekniikat perustuvat julkisen avaimen menetelmään. Allekirjoitus, varmenteen ja varmentajan muodostavat yhdessä julkisen avaimen infrastruktuurin, jonka avulla voidaan lisätä sähköisen asioinnin luotettavuutta. Alla pyritään julkisen avaimen menetelmää kuvaamalla selventämään varmentajan asemaa sähköisen allekirjoituksen käytössä.

Julkisen avaimen menetelmässä hyödynnetään ”avaimia” (bittijonoja), joista toinen on yksityinen ja toinen julkinen. Järjestelmässä luotetaan varmentajaan, joka yhdistää myön-

tämässään 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 avaimeseen perustuvaa salauskäytäntöä kutsutaan epäsymmetriseksi salaukseksi ja se mahdollistaa itse salauksen lisäksi sähköisten allekirjoitusten luomisen.

Sähköinen allekirjoitus perustuu paitsi julkisen avaimen menetelmään myös niin kutsuttuun tiivistefunktion. 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 todentamishjelmistonsa avulla. Vertaamalla tiivisteitä toisiinsa 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 hakemas-

sa 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 tunnistet, esimerkiksi sormenjälkitunnistet, tulevat osittain korvaamaan käyttäjän muistiin perustuvien salasanojen käytön. Yksityinen avain voi olla myös esimerkiksi matkapuhelimen SIM-kortilla tai ohjelmistona allekirjoittajan käyttämässä laitteessa, esimerkiksi henkilökohtaisessa tietokoneessa. Allekirjoittajan tarvitsema välineistö koostuu lähinnä toimikortista, jolla sijaitsevat avaimet, kortinlukijasta, joka on kiinni tietokoneessa, sekä työasemaohjelmistosta.

Julkisen avaimen infrastruktuuriin liittyy huomattava määrä eri toimintoja, joiden laadusta riippuu, miten luotettavasta allekirjoituksesta on kyse. Laadun ja luotettavuuden kannalta olennaista on varmentajan toiminta.

Varmentaja todistaa julkisen avaimen kulluvan tietylle henkilölle. Tätä tarkoitusta varten varmentaja myöntää allekirjoittajalle varmenteen.

Varmenteita on eritasoisia. Eräät varmenteet on mahdollista tilata suoraan tietoverkon avulla. Tällöin henkilöllisyyttä ei erityisen tarkasti tarkisteta. Tiettyihin tarkoituksiin myös näiden varmenteiden tarjoama luotettavuus riittää. Turvallisempia ja luotettavampia varmenteita myönnettäessä on olennaista varmistua varmenteen hakijan henkilöllisyydestä mahdollisimman luotettavalla tavalla. Henkilöllisyydestä varmistuminen on ratkaisevan tärkeää varmenteen luotettavuuden kannalta. Sähköisesti asioitaessa eivät osapuolet voi fyysisesti varmistua toistensa henkilöllisyydestä.

Varmenne sisältää käyttötarkoituksesta riippuen julkisen avaimen lisäksi myös muita tarpeellisia tietoja allekirjoittajasta. Varmenteita voidaan myöntää myös niin sanottuina roolivarmenteina, jolloin varmennetta käytetään esimerkiksi vain liikeyrityksen lukuun toimittaessa.

Varmenteet myönnetään yleensä määräajaksi. Varmenteet voidaan joutua tietyissä tapauksissa myös peruuttamaan. Tämän johdosta on tärkeää, että varmentaja ylläpitää kaikkien käytettävissä olevaa julkista rekisteriä (sulkulista) varmenteista/julkisista avaimista, joiden voimassaolo on päättynyt. Sulkulistalla oleviin varmenteisiin/julkisiin avaimiin ei siis voi luottaa. Varmentaja päivittää sulkulistaa mahdollisimman reaaliaikaisesti.

Varmentaja tarjoaa allekirjoittajalle usein allekirjoituksen luomiseen välttämättömät ohjelmistot ja laitteistot, eli allekirjoitusvälineet. Varmentaja ei välttämättä tee kaikkea varmentamiseen liittyviä toimia itse vaan käyttää alihankkijoita. Esimerkiksi yksityisen avaimen saattaa luovuttaa allekirjoittajalle niin sanottu rekisteröijä, joka suorittaa varmentajan puolesta varmentajalle kuuluvia tehtäviä, kuten käyttäjän luotettavan tunnistamisen. Alihankkijaa saatetaan käyttää myös luomaan yksityinen ja julkinen avain tietyille alustalle. Myös hakemistopalvelut saatetaan ostaa alihankintana niihin erikoistuneilta tietotekniikkayrityksiltä.

Koska varmentamiseen liittyy paljon osatekijöitä ja tahoja, varmenteeseen luottavan tahon kannalta on tärkeää tietää, kuka varmentamistoiminnasta viime kädessä vastaa. Tämä on erityisen tärkeää lakiehdotuksessa määriteltujen luotettavuudeltaan korkeatasoisten laatuvarmenteiden tarjonnassa. Ehdotuksessa vastuu kohdistetaan yhteen tahoon. Ehdotuksen mukaan varmentaja, joka tarjoaa laatuvarmenteita yleisölle on velvollinen korvaamaan varmenteeseen luottavalle taholle syntyneet vahingot, jotka johtuvat laatuvarmenteiden tietojen paikkansapitämättömyydestä.

Varmenteita käytetään paitsi henkilöiden välisessä viestinnässä myös järjestelmien ja

laitteiden välisessä viestinnässä, nimenomaan näiden välisessä tunnistamisenmenettelyssä, palveluiden luotettavuuden tason parantamiseksi. On tavallista, että internetissä erilaiset palvelimet tunnistavat toisiaan varmenteiden avulla. Myös matkaviestinverkko tunnistaa päätelaitteen varmennetekniikkaan perustuvan menetelmän avulla. Näillä puhtaasti teknisillä tunnistamistavoilla ei kuitenkaan ole mitään tekemistä varsinaisen allekirjoittamisen kanssa. Esitetystä laissa säädettäisiin ainoastaan varmenteista, joita käytetään sähköisen allekirjoituksen yhteydessä.

Sähköisiin allekirjoituksiin liittyy paitsi itse allekirjoittaminen myös allekirjoituksen todentaminen. Allekirjoituksen luomisvälineitä (ohjelmia ja laitteita) vastaavat allekirjoituksen todentamisvälineet (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. Välineiden, laitteiden ja ohjelmistojen korkealaatuisuus ja yhteensopivuus pyritään takaamaan laajalla kansainvälisellä standardointiyhteistyöllä, jota on kuvattu esityksen kohdassa 2.3.

Varmenteiden tarjoamiseen sekä sähköisiin allekirjoituksiin liittyviin tuotteisiin perustuva kaupallinen toiminta on voimakkaasti kehityksessä. Kansainvälisesti useat yritykset tarjoavat varmenteita. Alan liiketoimintaa Suomessa harjoittavia yrityksiä on muun muassa Certall Finland Oy, Novotrust Oy, Sonera Smart Trust Oy, F-Secure Oyj ja SSH Communications Security Oy. Myös Väestörekisterikeskus tarjoaa varmenteita.

2. Nykytila

2.1. Lainsäädäntö ja käytäntö

Sähköisen allekirjoituksen oikeusvaikutus

Sähköisiin viesteihin ja todentamiseen liittyviä kysymyksiä on pääosin ratkaistu jo kauan voimassa olleen sääntelyn ja oikeuskäytännön kautta. Yksityisoikeudellisten oikeustoimien muotomääräyksiä koskevat säännökset eivät tunne sähköistä allekirjoitusta. Yksityisoikeudellisten sopimusten osalta lainsäädännössä yleisimmin käytettyjä muotovaatimuksia ovat lähinnä sopimuksen tekeminen kirjallisesti ja sopimuksen allekirjoittaminen. Ilmauksia ”kirjallisesti” tai ”allekirjoittaa” ei ole määritelty tarkemmin lainsäädännössä.

Suomessa noudatettava vapaa todistusharkinta ei edellytä todisteilta tiettyä muotoa. Oikeudenkäymiskaaren 17 luvun 2 §:n mukaan oikeuden tulee päättää, mitä asiassa on pidettävä totena, harkittuaan huolellisesti kaikkia esiin tulleita seikkoja. Vapaa todistusharkinta koskee luonnollisesti myös sähköisiä allekirjoituksia ja niiden avulla tehtyjä oikeustoimia.

Suurin osa yksityisoikeudellisista oikeustoimista on sopimusten perusteella muotovapaita. Näiden oikeustoimien yhteydessä sopimusvapaus ja vapaa todistusharkinta tarjoavat jo nyt hyvän mahdollisuuden käyttää sähköisiä allekirjoituksia ja varmenteita.

Sähköisen allekirjoituksen käyttäminen edellyttää luonnollisesti, että oikeustoimen tekeminen sähköisesti on sallittua ja mahdollista. Se, että tietynlaisen sähköisen allekirjoituksen ja perinteisen allekirjoituksen oikeusvaikutukset tämän lakiesityksen mukaisesti samaistetaan täysin toisiinsa, ei vaikuta esimerkiksi siihen, milloin oikeustoimi edellytetään tehtäväksi paperilla.

Sopimusten osalta kirjallisen muotovaatimuksen täyttymisestä sähköisesti on tarkoitettu erikseen tietoyhteiskunnan palvelujen tarjoamisesta annettavassa laissa, jonka valmistelua varten asetettiin oikeusministeriössä työryhmä (sähkökauppatyöryhmä). Kyseinen työryhmä asetettiin oikeusministeriössä 30 päivänä toukokuuta 2000 valmistelemaan Euroopan parlamentin ja neuvoston sähköistä

kaupankäyntiä koskevan direktiivin (direktiivi tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista, 2000/31/EY) täytäntöön panemiseksi tarvittavaa lainsäädäntöä. Kyseinen direktiivi on pantava kansallisesti täytäntöön 17 päivään tammikuuta 2002 mennessä. Työryhmän 8 päivänä maaliskuuta 2001 päivätystä mietinnöstä pyydettiin lausunnot 27 päivään huhtikuuta 2001 mennessä.

Sähköisen allekirjoituksen varmentaminen

Hallinnon sähköisen asioinnin kehittämisen yhteydessä on säännelty varmennepalveluiden tarjoamisesta. Väestötietolain (507/1993) muutoksella sekä rekisterihallintolain (166/1996) muutoksilla annettiin säännökset Väestörekisterikeskuksen asemasta valtionhallinnon varmennepalveluita hoitavana viranomaisena. Väestötietolakiin otettiin säännökset muun muassa valtionhallinnon varmenneudessa sähköisessä asiointissa käytettävän varmenteen tiedoista, sähköisestä asiointitunnuksesta sekä Väestörekisterikeskuksen mahdollisuudesta tuottaa varmennepalveluita myös muille viranomaisille, yrityksille, yhteisöille ja yksityisille henkilöille.

Henkilökorttilailla (829/1999) annettiin säännökset henkilökortin lisäksi myös sähköisestä henkilökortista. Varmennetussa sähköisessä asiointissa käytettävässä sähköisessä henkilökortissa on aina Väestörekisterikeskuksen varmenne, niin sanottu HST-varmenne (HST, henkilön sähköinen tunnistaminen). Kortille voidaan tallettaa myös muita sovelluksia. Henkilökorttilain säätämisen yhteydessä tehdyllä väestötietolain 23 §:n muutoksella säädettiin muun muassa varmenteen myöntämisessä noudatettavasta menettelystä sekä Väestörekisterikeskuksen mahdollisuudesta myöntää varmenne henkilökortin lisäksi muihinkin alustoihin. Edellä mainitut säädökset tulivat voimaan 1 päivänä joulukuuta 1999.

Sähköisestä asiointista hallinnossa annettu laki (1318/1999) tuli voimaan 1 päivänä tammikuuta 2000. Lailla säädetään sähköisten tiedonsiirtovälineiden käyttämisestä hallintoasiointissa, sähköisen viestin perille saattamiseen liittyvistä vastuukysymyksistä

sekä sähköiseen tunnistamiseen ja varmentamiseen liittyvistä vaatimuksista hallintoasioissa. Lain mukaan hallintoasian vireilepanossa hyväksytään sähköinen allekirjoitus, jos varmentaja ja varmenne täyttävät lain 4 ja 5 §:ssä säädetyt vaatimukset. Lain 7 §:n mukaan varmentamistoiminnassa on noudatettava muun muassa hallintomenettelylakia (598/1982), kielilakia (148/1922), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) ja arkistolakia (831/1994). Nämä vaatimukset koskevat kaikkia niitä varmentajia, joiden varmennetta voidaan käyttää hallinnossa, myös kaupallisen sektorin varmentajia. Tämä on käytännössä johtanut siihen, että eräiden kaupallisen sektorin varmenteiden käyttöalasta on sopimuksin rajattu pois hallintoasiointi, mikä osaltaan vähentää sähköisen asioinnin palveluiden käyttäjien määrää. Lain 33 §:n mukaan sähköisessä asioinnissa kuitenkin hyväksytään aina sähköisellä henkilökortilla oleva Väestörekisterikeskuksen varmenne. Lain 40 §:n mukaan valtiovarainministeriö pitää lain vaatimukset täyttävistä varmenteista luetteloa, johon varmentaja voi lain 41 §:n 1 momentin nojalla vaatia itseään tai varmennetaan koskevan tiedon. Tästä annettavasta päätöksestä haetaan muutosta hallintolainkäyttölain mukaisesti.

2.2. Euroopan yhteisöjen direktiivi sähköisistä allekirjoituksista

Euroopan unionin komissio julkaisi 16 päivänä huhtikuuta 1997 tiedonannon Eurooppalainen sähköisen kaupankäynnin aloite (KOM(97) 157 lopullinen), jossa edellytettiin yhteisen lainsäädännön luomista digitaalisten allekirjoitusten tunnistamiseksi ja vähimmäisvaatimusten asettamiseksi varmentajille. Saman vuoden lokakuun 8 päivänä komissio julkaisi tiedonannon tietoturvan ja luottamuksen varmistamisesta sähköisessä viestinnässä (KOM(97) 503 lopullinen). Tiedonannossa esitettiin tavoite kehittää eurooppalainen digitaalisia allekirjoituksia ja varmennepalveluita koskeva eurooppalainen toimintamalli. Tiedonannossa korostettiin sähköisen allekirjoituksen ja salauksen erottamista toisistaan.

Komission ehdotus Euroopan parlamentin

ja neuvoston direktiiviksi sähköisten allekirjoitusten yhteisestä kehyksestä (EYVL C 325, 23.10.1998) annettiin lokakuussa 1998. Sähköisiä allekirjoituksia koskevasta yhteisestä puitteista annettu Euroopan parlamentin ja neuvoston direktiivi eli sähköallekirjoitusdirektiivi annettiin 30 päivänä marraskuuta 1999 ja se tuli voimaan 19 päivänä tammikuuta 2000.

Sähköallekirjoitusdirektiivi perustuu siihen, että varmennepalvelun tarjonta on sinänsä vapaa elinkeino, mutta vain korkeat laatuvaatimukset täyttävät, direktiivin määrittelemät hyväksytyt varmenteet ovat sellaisia, että niillä varmennetut ja turvallisilla allekirjoituksen luomisvälineillä luodut kehittyneet sähköiset allekirjoitukset on hyväksyttävä oikeusvaikutuksiltaan perinteisen käsinkirjoitetun allekirjoituksen veroisiksi. Direktiivin sääntely keskittyy nimenomaan hyväksytyyn varmenteeseen ja niitä tarjoaviin varmentajiin.

Ehdotetussa laissa sähköisistä allekirjoituksista hyväksytystä varmenteesta käytettäisiin nimeä laatuvarmenne. Seuraavassa on käyty läpi direktiivin pääasiallinen sisältö artikloitain.

1 artikla. Soveltamisala. Direktiivin 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 pätevyteen liittyviin muotomääräyksiin tai asiakirjojen käyttöä koskeviin säännöksiin.

2 artikla. 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.

3 artikla. Markkinoille pääsy. Varmennepalvelujen tarjonta ei saa olla ennakkovaltuutuksen varaista. Jäsenvaltiot voivat kuitenkin ottaa käyttöön tai ylläpitää vapaaehtoisia ak-

kreditointijärjestelmiä. Akkreditointijärjestelmien tulee olla objektiivisia, avoimia, suhteellisia ja syrjimättömiä.

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

Jäsenvaltiot voivat nimetä julkisia tai yksityisiä laitoksia määrittelemään, ovatko turvalliset allekirjoituksen luomismenettimet 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.

4 artikla. Sisämarkkinaperiaatteet. 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 säännöksiin rajoittaa. Jäsenvaltioiden on lisäksi varmistettava, että sähköisiin allekirjoituksiin liittyvät tuotteet liikkuvat vapaasti sisämarkkinoilla.

5 artikla. Sähköisen allekirjoituksen oikeusvaikutukset. Jäsenvaltioiden on varmistettava, että sellaiset kehittyneet sähköiset allekirjoitukset, jotka perustuvat hyväksytyyn varmenteeseen ja jotka on luotu turvallisella allekirjoituksen luomismenettelmällä, 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.

6 artikla. Vastuu. Direktiivin 6 artiklassa säädetään hyväksytyjä 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 hyväksytyyn varmenteen tietojen paikkansapitävyydestä sen myöntämishetkellä ja kaikkien hyväksytyissä varmenteissa ilmoitettavien tietojen sisällyttämisestä 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 hyväksytyyn varmenteen käytöstä.

7 artikla. Kansainväliset näkökohdat. Artiklassa on säännöksiä siitä, miten kolmannen maahan sijoittautuneen varmentajan hyväksytyinä varmenteina yleisölle tarjotut 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 määränemistöllä päätettävistä neuvotteluvaltuuksista näitä kansainvälisiä sopimuksia varten.

8 artikla. Tietosuoja. Jäsenvaltioiden on varmistettava, että varmentajat, akkreditointi-

järjestelmät 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 salanimä 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. Hyväksytyt varmenteita koskevat vaatimukset. Hyväksytyt varmenteen tietosisältöön kuuluu muun muassa tiedot varmennepalvelujen tarjoajasta, allekirjoittajan nimi, mahdolliset allekirjoittajaan liittyvät erityisominaisuudet, allekirjoituksen todentamiseen käytettävät tiedot, varmenteen voimassaoloaika ja varmennepalvelujen tarjoajan kehittynyt sähköinen allekirjoitus.

Liite 2. Hyväksytyt 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.

Liite 3. 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. Allekirjoitusmenetelmät eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoitusmenettelyä.

Liite 4. 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.

2.3. Kansainvälinen kehitys ja ulkomaisen lainsäädäntö

Ruotsi, Norja ja Tanska

Ruotsissa sähköisen allekirjoituksen varmennepalveluja koskeva laki (regeringens proposition 1999/2000:117, lag om kvalificerade elektroniska signaturer, m.m.) on tullut voimaan 1 päivänä tammikuuta 2001. Lailla on saatettu Ruotsissa voimaan sähköallekirjoitusedirektiivin säännökset.

Norjan hallitus antoi lakiehdotuksen (om lov om elektronisk signatur, Ot.prp.nr.82) syyskuussa 2000 parlamentin käsittelyyn. Norjan laki on tullut voimaan 1 päivänä heinäkuuta 2001. Tanskan laki (lov om elektroniske signaturer, lov nr. 417 af 31. maj 2000) tuli puolestaan voimaan 1 päivänä lokakuuta 2000. Kyseisillä laeilla pannaan täytäntöön sähköallekirjoitusedirektiivin säännökset Norjassa ja Tanskassa.

Ruotsin, Norjan ja Tanskan lait ovat hyvin samankaltaisia ehdotetun Suomen lain kanssa. Ruotsi, Norja ja Tanska ovat kansallisissa säädöksissään antaneet kehittyneelle sähköiselle allekirjoitukselle perinteisen käsintehdyn allekirjoituksen oikeusvaikutuksen. Ruotsin laissa ei ole säännöstä, jonka mukaan muiltakaan sähköisiltä allekirjoituksilta ei evätä oikeudellista vaikutusta ja hyväksytävyyttä yksinomaan sen vuoksi, että allekirjoitus on sähköisessä muodossa. Tanskan laissakaan ei ole mainintaa muiden kuin kehittyneiden allekirjoitusten oikeusvaikutuksesta. Norjan laissa sen sijaan mainitaan, että muutkin kuin kehittyneet allekirjoitukset

voidaan rinnastaa käsintehtyyn allekirjoitukseen. Tämän esityksen mukaiseen lakiin otetaisiin sähköisiä allekirjoituksia koskeva säännös, joka rinnastaisi ainakin kehittyneen sähköisen allekirjoituksen oikeusvaikutuksiltaan käsintehtyyn allekirjoitukseen. Suomalaisissa tuomioistuimissa noudatettavan vapaan todistusharkinnan ja sopimusvapauden periaatteen johdosta on selvää, että muidenkaan sähköisten allekirjoitusten oikeudellista vaikutusta ja hyväksyttävyyttä ei Suomessa evättäisi ainoastaan allekirjoituksen sähköisen muodon vuoksi.

Tanskan lainsäädännön keskeisin ero muihin pohjoismaihin on niin sanotun järjestelmien tarkastelijan (revisor) toiminta. Laatuvarmentajien tulee nimetä ulkopuolinen valtion valtuuttama tarkastaja suorittamaan järjestelmiensä tarkastus (revision). Erityistilanteissa telehallintokeskus voi poiketa vaatimuksesta, että kyseisen tahon tulisi olla nimenomaan valtion valtuuttama tarkastaja. Järjestelmien tarkastelija raportoi telehallintokeskukselle, tämän antamien tarkempien määräysten mukaisesti, täyttääkö laatuvarmentajan järjestelmät lain edellyttämät vaatimukset. Vastaavaa järjestelmää ei ole muissa pohjoismaissa, eikä sellaista ehdoteta otettavaksi Suomenkaan lainsäädäntöön.

Ruotsi on hyväksynyt laatuvarmenteessa käytettäväksi varmentajan kehittyneen sähköisen allekirjoituksen lisäksi myös muun vastaavan turvallisuustason sähköisen allekirjoituksen.

Eräät muut maat

Saksan digitaalista allekirjoitusta koskeva laki (Signaturgesetz) tuli voimaan jo 1 päivänä elokuuta 1997 osana laajempaa informaatio- ja viestintäpalveluja koskevaa yleislakia (Informations- und Kommunikationsdienste Gesetz). Laissa oli säännökset muun muassa alalle pääsystä, neuvontavollisuudesta, toiminnan lopettamisesta ja aikaleimasta. Lain nojalla annettiin lisäksi runsaasti teknisiä säännöksiä. Alalle pääsyn on Saksassa kritisoitu olevan liian kallista säännösten aiheuttamien liian raskaiden velvoitteiden vuoksi. Mainittu digitaalista allekirjoitusta koskeva laki (Signaturgesetz) kumottiin 22 päivänä toukokuuta 2001, kun uusi sähköisiä

allekirjoituksia koskeva laki (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderungen weiterer Vorschriften) tuli voimaan. Saksassa on parhaillaan valmisteilla lakiin liittyvä asetetus, jolla tarkennetaan varmennepalvelujen tarjoajia koskevien vaatimusten yksityiskohtia.

Yhdysvalloissa tuli 30 päivänä kesäkuuta 2000 voimaan liittovaltion laki sähköisistä allekirjoituksista (Electronic Signatures in Global and National Commerce Act, Public Law No: 106-229). Lailla taataan lähtökohtaisesti sähköiselle allekirjoitukselle käsintehtyyn allekirjoitukseen rinnastettava oikeusvaikutus. Laissa ei edellytetä sähköisten allekirjoitusten käyttöön liittyen minkäänlaisia varmennepalveluja. Laissa on edellytetty kuitenkin kuluttajan nimenomaista suostumusta sähköisen allekirjoituksen käyttöön. Lisäksi muualla lainsäädännössä asetetut lisävaatimukset esim. muotovaatimusten osalta tietyissä sopimuksissa tai oikeustoimissa saattavat estää sähköisen allekirjoituksen käyttämisen. Yhdysvaltain lain tarkoituksena onkin lähinnä mahdollistaa sähköisen allekirjoituksen ja asiakirjojen käyttö edellyttämällä, että oikeustoimilta ei evättäisi oikeusvaikutuksia ainoastaan sen vuoksi, että kyseinen oikeustoimi on tehty sähköisessä muodossa.

Kansainväliset järjestöt

Yhdistyneiden Kansakuntien, jäljempänä YK, kansainvälisen kauppaoikeuden toimikunnan, jäljempänä UNCITRAL, sähköisen kaupankäynnin työryhmä on tammikuusta 1998 lähtien valmistellut mallilakia sähköisistä allekirjoituksista, jäljempänä mallilaki. Mallilaki ja sen tulkintaan liittyvä opas (Guide to Enactment) on tarkoitus hyväksyä lopullisesti UNCITRAL:n 34. istunnossa kesällä 2001.

UNCITRAL:n mallilain valmistelutyö on tarjonnut YK:n jäsenvaltioille sähköisten allekirjoitusten sääntelyn kehittämisessä tarvittavan kansainvälisen keskustelufoorumin. Mallilakiehdotus on jo sellaisenaan toiminut esimerkkinä lainvalmistelulle erityisesti Euroopan ulkopuolisissa maissa. Mallilain valmistelun yhteydessä esille nostetut ongelmat ja ongelmanratkaisut huomioon ottavia lainsäädäntöhankkeita on ollut vireillä tai jo lop-

puun 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. Euroopan unionin komissio ja jäsenvaltiot ovat myös direktiivin voimaan tulon jälkeen aktiivisesti osallistuneet ja vaikuttaneet mallilain valmisteluun sähköisen kaupankäynnin työryhmässä.

Viimeisin versio mallilaista, joka on UNCITRAL:n verkkosivuilla osoitteessa <http://www.uncitral.org/en-index.htm>, asiakirjassa A/CN.9/WG.IV/WP.88, sisältää sähköallekirjoitusdirektiivin 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 allekirjoituksen turvallisuutta vaarantavasta tapahtumasta.

Standardointi

Sähköallekirjoitusdirektiivin vaatimusten toteuttamiseksi on perustettu Eurooppalaisen teollisuuden ja standardointiorganisaatioiden yhteishanke European Electronic Signature Standardization Initiative, jäljempänä EESSI. EESSI-projektin puitteissa European Telecommunications Standards Institute:ssa, jäljempänä ETSI, ja European Committee for Standardization:ssa, jäljempänä CEN, standardoidaan useita alueita sähköisten allekirjoitusten ja varmennepalveluiden tuotteisiin, järjestelmiin ja palveluihin liittyen.

Standardointityö perustuu julkisen avaimen infrastruktuuriin (Public Key Infrastructure,

jäljempänä PKI), jonka avulla voidaan täyttää turvallisen asioinnin vaatimukset. Ensimmäiset standardointityön tulokset ovat jo valmistuneet vuoden 2000 lopulla ja lisää työalueita valmistuu vuoden 2001 aikana. Standardointityön tarkoituksena on myös tuottaa valmiita ja vapaasti levitettäviä toteutuksia tukemaan markkinoiden kasvua ja standardien yleistymistä.

Standardointielimien ja foorumien kesken tehdään myös laajamittaista Euroopan rajat ylittävää kansainvälistä yhteistyötä. EESSI-projektin tehtäväalueita tehdään ETSI:n ja CEN:n toimesta yhteistyössä muun muassa IETF:n (Internet Engineering Task Force) ja W3C:n (World Wide Web Consortium) kanssa.

2.4. Nykytilan arviointi

Varmenteiden tarjonnan markkinanäkymät arvioidaan hyväksi. Varmenteet ovat kasvussa olennaiseksi keinoksi lisätä luottamusta verkkoviestinnässä. Verkkoliiketoiminnan arvioidaan kasvavan voimakkaasti, jolloin myös varmenteiden kysyntä kasvaa. Vaikka varmennemarkkinat ovatkin vielä pääosin muotoutumatta, laajenee varmenteiden käyttöala jatkuvasti ja niiden oheen kehittyy erilaisia lisäpalveluita, kuten avaimenhallinta- ja notariaattipalveluita.

Oikeustoimen osapuolet voivat yleisen sopimusvapauden periaatteen nojalla vapaasti päättää tekevätkö jonkin oikeustoimen. Oikeustoimen tekemisessä on myös lähtökohtaisesti periaatteena muotovapaus, jonka mukaan oikeustoimi voidaan tehdä osapuolten haluamalla tavalla. Tällä hetkellä sähköisen allekirjoituksen asemasta ja oikeusvaikutuksista on epäselvyyttä, vaikka vapaa todistusharkinta ja sopimusvapaus antavatkin Suomessa hyvät mahdollisuudet sen käytölle.

Verkkoliiketoiminnan edistämiseksi, erityisesti luottamuksen lisäämiseksi, varmenteiden tarjonnasta ja sähköisen allekirjoituksen oikeusvaikutuksista on syytä säätää lailla. Lain antaminen on välttämätöntä myös sähköallekirjoitusdirektiivin säännösten saattamiseksi osaksi Suomen lainsäädäntöä.

Lakiesityksen mukaisella lailla samaistetaisiin sähköallekirjoitusdirektiivin määritelmien mukainen kehittynyt sähköinen allekir-

joitus perinteiseen käsintehtyyn allekirjoitukseen. Mahdollisista muista oikeustoimien muotovaatimuksista säädetään muualla lainsäädännössä. Verkkoliiketoiminnan ja sähköisten palvelujen kehittymisen kannalta olisi ensiarvoisen tärkeää, että esitetyn lain edellytykset täyttävän laatuvarmenteen avulla varmennetun ja turvallisen allekirjoituksen luomisvälineen avulla luodun kehittyneen sähköisen allekirjoituksen käyttö olisi mahdollista niin yksityisellä kuin julkisellakin sektorilla. Tämä olisi keskeinen tekijä myös sähköisten palveluiden helpon käytettävyyden kannalta.

Uudistettaessa sähköisen viranomaisasiointin säädöksiä, voitaisiin viitata hallinnon palveluissa hyväksyttävän varmentamistoiminnan ja varmenteiden osalta tämän lakiehdotuksen mukaisesti säädettyyn lakiin. Samassa yhteydessä tulisi arvioida mahdolliset muutostarpeet Väestötietolaissa säädettyihin varmennetun sähköisen asiointin palveluita koskeviin säännöksiin. Tämä on tarpeen erityisesti Väestötietolain 20 §:ssä määritellyn Väestörekisterikeskuksen myöntämän valtionhallinnon sähköisessä asiointissa käytettävän varmenteen tietosisällön osalta.

Sähköinen allekirjoitus liittyy aina kiinteästi tiettyyn sähköiseen tietosisältöön liittyvään tahdonilmaisuuksiin, kuten esimerkiksi sopimusasiakirjan allekirjoittamiseen. Muita kuin tiettyyn tietosisältöön suoraan liittyviä varmennepalveluita käytetään jo laajalti verkkoympäristössä. Tällaisia palveluita ovat esimerkiksi käyttäjän liittymän tunnistaminen palvelun tarjoamiseksi matkaviestinnässä tai palvelinten välinen tunnistaminen varmennepalvelun avulla. Kyseisten palveluiden tarjonta ei edellytä ehdotetun lain ulottamista niihin.

3. Esityksen tavoitteet ja keskeiset ehdotukset

Kuluttajan luottamuksen lisääminen verkkoasiointiin ja sähköiseen kaupankäyntiin on keskeinen tekijä verkkoliiketoiminnan menestykselle. Varmenteet ovat tässä suhteessa merkittävässä asemassa. Kuluttajan luottamuksen lisäämiseksi on tarkoituksenmukaista säätää korkealaatuisen varmentamisen perusteista, sähköisten allekirjoitusten oikeus-

vaikutuksista ja keskeisistä vastuukysymyksistä lailla. Tätä edellyttää myös sähköallekirjoitusdirektiivi.

Varmentajien toiminta on valtaosin kaupallista toimintaa. Oman erityissektorinsa muodostaa hallinnon sähköinen asiointi, josta on omaa erityislainsäädäntöä. Varmenteiden käyttöalan painopiste tulee selvästi olemaan kaupallisessa käytössä ja tämä korostuu edelleen verkkoliiketoiminnan kasvaessa ja varmenteiden käytön lisääntyessä matkaviestinnän palveluissa. Luotettava varmennetoiminta ja alan kehitys turvataan parhaiten huolehtimalla siitä, että palvelun tarjoajat voivat kilpailla tasapuolisesti keskenään. Myös alalle pääsyn on oltava mahdollisimman helppoa.

Säädösympäristön ei tule luoda ylimääräisillä velvoitteilla turhia kustannusrasitteita liiketoiminnalle, jonka olemassaolo ja menestyminen perustuu käyttäjiltä saavutettavaan luottamukseen. Tavoite toteutettaisiin pitäytymällä sähköallekirjoitusdirektiivin sallimissa rajoissa mahdollisimman kevyessä sääntelyssä keskittyen vain välttämättömiin. Tätä palvelee myös sääntelyn keskittäminen laatuvarmenteita yleisölle tarjoavaan varmentajaan, jättäen varmennetoiminnalle tyypilliset varmentajan apunaan käyttämät tahot, kuten esimerkiksi sulkulistan ylläpitäjät, yksityisten avainten valmistajat tai varmenteen usein käyttäjälle luovuttavat niin sanotut rekisteröijät välittömän sääntelyn ulkopuolelle. Laatuvarmenteita yleisölle tarjoava varmentaja huolehtisi sopimuksin mainittujen tahojen kanssa velvoitteiden toteutumisesta. Laatuvarmenteita yleisölle tarjoava varmentaja olisi kuitenkin se taho, joka vastaisi ulospäin varmennustoiminnan luotettavuudesta. Tämä selkeyttäisi tilannetta käyttäjän kannalta, koska ongelmatilanteissa vastuurajapinnat olisivat selkeämmät. Tämä helpottaisi ja selkeyttäisi myös laatuvarmenteita yleisölle tarjoavien varmentajien valvontaa.

Varmentamisen kokonaisuudessa on useita osa-alueita ja uusia palveluita on koko ajan kehittymässä. Tavoitteena on antaa suotuisat kehittymisedellytykset näille uusille palveluille. Tämä on tarkoitus toteuttaa keskittämällä ehdotetun lain säädöksiä sähköallekirjoitusdirektiivin rajoissa erityisesti sähköiseen allekirjoitukseen ja siinä tarvittaviin laa-

tuvarmenteisiin. Varmentamiseen liittyvät muut palvelut, kuten kehityksessä olevat aikaleima- tai notariaattipalvelut jäisivät vapaiksi elinkeinoksi muun lainsäädännön alaiseksi.

Lakiehdotuksen tavoitteena on myös lisätä sähköisen asioinnin palveluiden käyttäjäkuntaa. Tällä hetkellä voimassa olevista sähköistä asiointia koskevista säännöksistä johtuvien rasitteiden ja epävarmuuden vuoksi kaupallisten varmenteiden käyttöalasta on yleensä rajattu pois julkishallinnon palvelut. Tilanetta ei sähköisen asioinnin palveluiden kokonaisuuden kannalta voida pitää tarkoituksenmukaisena. Tavoitteena on luoda edellytykset kokonaisuudelle, jossa kansalainen voisi valita turvallisen varmenteen ja asioida sillä sekä kaupallisissa että julkisissa palveluissa. Tarkoituksenmukaista olisi pyrkiä tilanteeseen, jossa turvalliset varmenteet määriteltäisiin yhdessä paikassa, jotta käyttäjä saisi mahdollisimman selkeää ja täsmällistä tietoa eri palveluihin kelpaavista varmenteista. Kokonaisuuden toimivuus on riippuvainen myös sähköisestä asioinnista hallinnossa annetun lain muuttamisesta.

Lakiehdotuksella selkeytettäisiin sähköisen allekirjoituksen oikeusvaikutuksia. Kuten jo edellä on mainittu, Suomessa vapaa todistusharkinta ja sopimusvapaus tarjoavat jo nyt mahdollisuuden käyttää sähköistä allekirjoitusta. Ennakoitavuuden lisäämiseksi säädettäisiin kuitenkin sähköallekirjoitusdirektiiviä vastaavasti laatuvarmenteen ja turvallisen allekirjoituksen luomisvälineen avulla tehdyn kehittyneen sähköisen allekirjoituksen vastaavan perinteistä käsin tehtyä allekirjoitusta. Osapuolet voisivat kuitenkin edelleen sopia vapaasti muunlaistenkin sähköisten allekirjoitusten käytöstä. Muut mahdolliset oikeustoimiin liittyvät muutovaatimukset vaikuttaisivat niistä säädetyn tai sovitun mukaisesti.

Esityksellä pyritään myös selkeyttämään varmentamiseen liittyviä vastuusuhteita. Esityksellä säädettäisiin laatuvarmenteita yleisölle tarjoavan varmentajan vastuusta. Tällainen varmentaja vastaisi erikseen laissa määritellyissä tapauksissa laatuvarmenteeseen luottaneelle syntyneistä vahingoista, ellei varmentaja voisi käännetyä todistustaakan mukaisesti osoittaa toimineensa huolellisesti. Allekirjoittajalle puolestaan säädettäisiin

velvollisuus viipymättä pyytää laatuvarmenteen myöntäneeltä varmentajalta laatuvarmenteensa peruuttamista, jos allekirjoittajalla on perusteltu syy epäillä allekirjoituksen luomistietojen oikeudetonta käyttöä.

4. Esityksen vaikutukset

4.1. Taloudelliset vaikutukset

Luotettavan ja tehokkaan varmenteiden tarjonnan arvioidaan osaltaan merkittävästi edistävän verkkoliiketoiminnan harjoittamisen edellytyksiä. Verkkoliiketoiminnan taloudellinen merkitys kasvaa lähivuosina nopeasti. Verkkoliiketoiminta parantaa tuottavuutta, minkä vuoksi ehdotuksella on myönteisiä vaikutuksia kansantalouteen. Vaikutusten määrää on kuitenkin vaikea arvioida, koska varmennemarkkinat ovat vasta kehityksessä ja erilaisia varmenteisiin liittyviä palveluita tultaneen tarjoamaan muiden palveluiden yhteydessä liitännäispalveluina, esimerkiksi matkaviestintäpalveluihin liitetynä. Tämän johdosta taloudellisten vaikutusten kohdistumista erisuuruisiin yrityksiin on myös vaikea arvioida.

Ehdotuksen välittömät työllisyysvaikutukset ovat vähäiset. Työpaikat varmenteita tarjoavissa yrityksissä ja niiden alihankkijoissa lisääntyvät. Ehdotuksen välillisiä työllisyysvaikutuksia on vaikea arvioida.

Ehdotuksen arvioidaan kasvattavan myös käytettävissä olevien hallinnon sähköisten asiointipalveluiden käyttöä varmenteiden käytön lisääntyessä.

Ehdotuksella ei ole vaikutusta valtion talousarvioon.

4.2. Organisaatio- ja henkilöstövaikutukset

Varmennetoiminnan valvontatehtävien hoitaminen ehdotetaan annettavaksi Viestintäviraston tehtäväksi. Viestintäviraston henkilöstötarve kasvaa alustavien arvioiden mukaan 2-3 henkilöllä. Henkilöstötarve saattaa nousta tästä, riippuen varmenteita tarjoavien yritysten määrästä tulevaisuudessa ja siitä, millaisiksi markkinat yleisesti muodostuvat. Viestintävirasto rahoittaa menonsa tuloilla, jotka kerätään valvottavilta tahoilta valvon-

tamaksulla. Kokonaismenoiksi arvioidaan 340 tuhatta euroa (2 miljoonaa markkaa) vuodessa.

Sähköisten allekirjoitusten käytön yleistymisen myötä myös sähköinen asiointi julkishallinnossa lisääntynee. Tämä tulee ajan mittaan muuttamaan asiakaspalvelu- ja toimitushenkilöstön tarvetta ja tehtäviä. Periaatteessa tämä saattaa lisätä työttömyyttä, mikäli asiaan ei kiinnitetä huomiota. Koska kansalaisten valmiudet sähköiseen asiointiin kasvavat kuitenkin melko hitaasti, julkishallinnon työvoiman tarpeen mahdollinen väheneminenkin on hidasta. Toisaalta työvoiman tarpeen voidaan arvioida lisääntyvän nimenomaan sähköiseen asiointiin liittyvissä tehtävissä. Resurssien siirtämisellä perinteisemmistä asiakaspalvelutehtävistä uusiin tehtäviin sekä henkilöstön kouluttamisella hallitaisiin mahdolliset työllisyysvaikutukset. Sähköisen asioinnin lisääntyminen julkishallinnossa ei näin ollen tule lisäämään työttömyyttä, mikäli rakennemuutoksen työllisyysvaikutuksiin varaudutaan ennakoitua.

4.3. Ympäristövaikutukset

Lailla ei voida arvioida olevan välittömiä ympäristövaikutuksia. Asioiden käsittely sähköisessä muodossa vähentää paperimuotoisten asiakirjojen määrää. Sähköisen allekirjoituksen käytön vaikutuksia esimerkiksi paperinkulutukseen on kuitenkin mahdotonta arvioida.

4.4. Vaikutukset eri kansalaisryhmien asemaan

Sähköisten palveluiden lisääntyessä ja asioiden hoitamisen yhä automatisoituessa tulee sähköisen allekirjoituksen merkitys kasvamaan. Paperiasiakirjojen täyttäminen ja lähettäminen vähenee siirryttäessä yhä kattavampaan asiakirjojen sähköiseen käsittelyyn. Kansalaisten valmiudet ja mahdollisuudet käsitellä asioita sähköisesti kasvavat jatkuvasti. Fyysisen asioinnin vähentyessä asioiden hoitaminen helpottuu ja erityisesti tietyt erityisryhmät, kuten esimerkiksi liikuntarajoitteiset henkilöt, hyötyvät sähköisestä asioiden hoitamisesta. Sähköisten palveluiden ja sähköisen asioinnin lisääntyessä voidaankin

katsoa yhä useampien palveluiden olevan entistä tasapuolisemmin käyttäjien ulottuvilla.

5. Asian valmistelu

5.1. Valmisteluvaiheet ja -aineisto

Lakiesitys on valmisteltu virkatyönä liikenne- ja viestintäministeriössä kuullen laajasti eri osapuolia. Sähköallekirjoitusdirektiivin käsittelyn ja lain valmistelun aikana pidettiin sähköisistä allekirjoituksista julkiset kuulemistilaisuudet oikeusministeriössä ja liikenneministeriössä.

Liikenne- ja viestintäministeriö on ehdotuksen valmistelun aikana tehnyt yhteistyötä sähköisestä asioinnista hallinnossa annetun lain valmistelleen oikeusministeriön kanssa. Oikeusministeriö valmistelee parhaillaan koko viranomaiskenttää koskevaa sähköisen asioinnin yleislakia (laki sähköisestä asiointista viranomaistoiminnassa), jonka voimaantulon yhteydessä kumottaisiin sähköisestä asioinnista hallinnossa annettu laki. Valmisteilla olevaan lakiesitykseen ei tulisi varmenteita ja varmentamista koskevia säädöksiä, vaan niiden osalta olisi tarkoitus viitata tämän lakiesityksen mukaiseen lakiin.

Valmisteltaessa ja annettaessa lakia sähköisestä asioinnista hallinnossa tiedettiin myöhemmin annettavan yleislain edellyttävän todennäköisesti sähköisestä asiointista hallinnossa annetun lain muuttamista. Eduskunta edellytti lakia annettaessa hallituksen huolehtivan siitä, että mikäli lakia on muutettava, eduskunnalle annetaan siitä yleislakiehdotuksesta erillinen esitys. Eduskunta edellytti lisäksi, että eduskunnalle annetaan erillisen valmistelun pohjalta lakiehdotus, joka koskee julkisella sektorilla toimivien varmentajien akkreditointijärjestelmän luomista tehokkaammin ja tarkemmin säänneltynä.

Lakien ristiriitaisuuden välttämiseksi nyt ehdotetun yleislain säätäminen edellyttää vähintäänkin varmentamistoimintaa koskevien säännösten muuttamista sähköistä asiointia hallinnossa koskevassa laissa siten, että muutokset tulevat voimaan samanaikaisesti yleislain kanssa. Tavoitteena olisi, että sähköistä asiointia hallinnossa koskeva laki kumottaisiin oikeusministeriössä valmisteilla olevan sähköistä asiointia viranomaistoiminnassa

koskevan lain voimaantulon yhteydessä ja kaikki varmentamista ja varmenteita koskevat säädökset sisältyisivät tämän lakiesityksen mukaiseen lakiin. Tarkoituksenmukaista olisi, että kyseinen oikeusministeriön valmisteleva lakiesitys ja nyt ehdotettu lakiesitys käsiteltäisiin ja tulisivat voimaan samanaikaisesti. Koska oikeusministeriön valmistelevan lakiesityksen osalta notifiointimenettely teknisiä standardeja ja määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä annetun Euroopan parlamentin ja neuvoston direktiivin 98/34/EY, muut. 98/48/EY, (niin kutsuttu transparenssidirektiivi) nojalla on tätä lakiesitystä annettaessa kesken, voitaneen tämän lakiesityksen käsittely kuitenkin aloittaa jo ennen oikeusministeriön lakiesityksen valmistumista.

Koska varmennemarkkinat ovat vasta kehittyneissä ja siinä mahdollisesti tarvittavien alan toimijoiden yhteistyö on toistaiseksi pääosin muotoutumatta, ei ole ajankohtaista säädellä lain tasolla mahdollisten kokonaisuutta edistävien akkreditointijärjestelmien asemaa, rakennetta tai suhdetta eri toimijoihin.

Varmentamistoiminnan yleistymisen kannalta olisi toivottavaa, että kaikki sähköisiin allekirjoituksiin luottavat tahot hyväksyisivät ainakin yleislaissa määritellyllä laatuvarmenteella varmenneet ja turvallisen allekirjoituksen luomisvälineen avulla luodut kehittyneet sähköiset allekirjoitukset. Näin varmentajien ei tarvitsisi erikseen harkita täyttääkö heidän tarjoamansa laatuvarmenne julkisen hallinnon asettamat vaatimukset.

Lakiesitys on ilmoitettu teknisiä standardeja ja määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä annetun Euroopan parlamentin ja neuvoston direktiivin 98/34/EY, muut. 98/48/EY, (niin kutsuttu transparenssidirektiivi) nojalla Euroopan yhteisöjen komissiolle (Suomen ilmoitus 2001/125/FIN, 12.3.2001). Komission tiedonannossa SG(2001) D/50601 esitetyt huomautukset, sekä komission tiedonannolla SG(2001) D/51365 toimitetut Ruotsin esittämät huomautukset on otettu huomioon lakiesityksen jatkovalmistelussa. Lakiesityksestä tehty huomautukset eivät jatkaneet odotusajan määräaikaa, joka on päättynyt 12 päivänä kesäkuuta 2001.

5.2. Lausunnot

Esitysluonnoksesta on pyydetty lausunnot ministeriöiden lisäksi laajasti eri alojen viranomaisilta ja valtion laitoksilta sekä yrityssektorilta kaupan ja teollisuuden edustajilta.

Lausunnon antoivat oikeusministeriö, sisäasiainministeriö, kauppa- ja teollisuusministeriö, puolustusministeriö, opetusministeriö, sosiaali- ja terveysministeriö, työministeriö, valtiovarainministeriö, Ahvenanmaan maakuntahallitus, arkistolaitos, Huoltovarmuuskeskus, keskusrikospoliisi, Kilpailuvirasto, Kuluttajavirasto, pääesikunta, Rahoitustarkastus, Telehallintokeskus (nykyinen Viestintävirasto), Tietosuojavaltuutetun toimisto, Verohallitus ja Väestörekisterikeskus.

Lausunnon antoivat myös Certall Finland Oy, CSC-Tieteellinen laskenta Oy, Elisa Communications Oy, Ficom ry, Finnet-liitto ry, Gramex ry, Helsingin kauppakamari, Keskuskauppakamari, Kopiosto ry, Kuluttajat-Konsumenterna ry, ICL Invia Oy, Mainostajien liitto, Markkinointiviestinnän Toimistojen Liitto, Merita Pankki Oy, Mittatekniikan keskus, Niksu Oy, Novotrust Oy, Osuuspankkikeskus, Päijät-Hämeen Puhelin Oy, Sampo Pankki Oy, SanomaWSOY Oy, Siemens Oy, Sonera Smart Trust, Sosiaali- ja Terveysalan Tutkimus- ja Kehittämiskeskus STAKES, Suomen ATK-oikeudellinen yhdistys ry, Suomen Pankkiyhdistys, Suomen Patenttiasiamiesyhdistys ry, Suomen Posti Oy, Suomen Suoramarkkinointiliitto ry, Suomen Vakuutusyhtiöiden Keskusliitto, Suomen Yrittäjät ry, Säveltäjien Tekijänoikeustoimisto Teosto ry, Teknologian kehittämiskeskus Tekes, Teollisuuden ja työnantajien keskusliitto, Tietotekniikan kehittämiskeskus TIEKE ry ja Työeläkevakuuttajat TELA ry.

Yleisesti ottaen esitysluonnokseen suhtauduttiin myönteisesti ja lakiehdotuksen katsottiin edistävän sähköisten palvelujen tarjonnan mahdollisuuksia.

Ahvenanmaan maakuntahallitus on lausunnossaan kiinnittänyt huomiota lain soveltamisalaan liittyviin erityiskysymyksiin maakunnan alueella kuten esimerkiksi ruotsin kielen asemaan ja henkilötietolain soveltamiseen maakunnassa. Maakuntahallitus on lisäksi lausunnossaan kiinnittänyt huomiota

siihen, että ehdotuksen mukaan laatuvarmenten myöntäminen edellyttää ilmoitusta toiminnan aloittamisesta valvovalle viranomaiselle, jollaisena ehdotuksen mukaan toimii Viestintävirasto. Maakuntahallitus katsoo, että Ahvenanmaan itsehallintolain nojalla laatuvarmentajien toiminnan sääntely kuuluu kuitenkin Ahvenanmaan maakuntapäivien lainsäädäntövaltaan.

6. Muita esitykseen vaikuttavia seikkoja

Esitys liittyy osaltaan edellä mainittuun sähköisestä asioinnista hallinnossa annettuun lakiin. Oikeusministeriö valmistelelee parhailaan koko viranomaiskenttää koskevaa sähköisen asioinnin yleislakia (laki sähköisestä asioinnista viranomaistoiminnassa), jonka voimaantulon yhteydessä kumottaisiin sähköisestä asioinnista hallinnossa annettu laki. Valmisteilla olevaan lakiesitykseen ei tulisi varmenteita ja varmentamista koskevia säännöksiä, vaan niiden osalta olisi tarkoitus viitata tämän lakiesityksen mukaiseen lakiin. Tarkoituksenmukaista olisi, että kyseinen oikeusministeriön valmisteleva lakiesitys ja nyt ehdotettu lakiesitys käsiteltäisiin ja tulisivat voimaan samanaikaisesti. Koska oikeusministeriön valmistelevan lakiesityksen osalta notifiointimenettely teknisiä standar-

deja ja määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä annetun Euroopan parlamentin ja neuvoston direktiivin 98/34/EY, muut. 98/48/EY, (niin kutsuttu transparensidirektiivi) nojalla on tätä lakiesitystä annettaessa kesken, voitaneen tämän lakiesityksen käsittely kuitenkin aloittaa jo ennen oikeusministeriön lakiesityksen valmistumista.

Esitys liittyy myös oikeusministeriön valmistelevaan lakiin tietoyhteiskunnan palvelujen tarjoamisesta, jonka valmistelua varten perustettiin 30 päivänä toukokuuta 2000 oikeusministeriössä erillinen työryhmä (sähkökauppatyöryhmä). Valmisteilla olevassa lakiesityksessä säädettäisiin muun muassa sopimusten osalta kirjallisen muotovaatimuksen täyttymisestä sähköisesti. Sähkökauppatyöryhmä asetettiin valmistelevaan Euroopan parlamentin ja neuvoston sähköistä kaupankäyntiä koskevan direktiivin (direktiivi tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista, 2000/31/EY) täytäntöön panemiseksi tarvittavaa lainsäädäntöä. Kyseinen direktiivi on pantava kansallisesti täytäntöön 17 päivään tammikuuta 2002 mennessä. Työryhmän 8 päivänä maaliskuuta 2001 päivätyyn mietintöön on pyydetty lausunnot 27 päivään huhtikuuta 2001 mennessä.

YKSITYISKOHTAISET PERUSTELUT

1. Lakiehdotusten perustelut

1.1. Laki sähköisistä allekirjoituksista

1 luku. Yleiset säännökset

1 §. *Lain tarkoitus.* Lain tarkoituksena olisi edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa. Tarkoituksena olisi lisäksi edistää sähköisen kaupankäynnin ja sähköisen asiointin tietosuojaa ja tietoturvaa.

Sähköisten allekirjoitusten käyttöä pyrittäisiin edistämään asettamalla laissa määritelty laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla tehty kehittynyt sähköinen allekirjoitus oikeudellisesti samaan asemaan kuin omakätisesti kirjoitettu allekirjoitus.

Sähköisiin allekirjoituksiin liittyvien tuotteiden ja palveluiden tarjonnan edistämiseen pyrittäisiin muun muassa varmistamalla kyseisten tuotteiden ja palveluiden vapaa liikkuvuus Euroopan talousalueella lain 4, 5 ja 8 §:stä ilmenevällä tavalla.

Sähköisen kaupankäynnin ja sähköisen asiointin tietosuojaa ja tietoturvaa sekä yritysten ja kuluttajien luottamusta varmenteiden tarjontaa kohtaan pyrittäisiin edistämään sääntämällä laissa laatuvarmenteen ominaisuuksista, varmentajan velvollisuuksista ja vahingonkorvausvelvollisuudesta sekä varmentajiin kohdistuvasta viranomaisvalvonnasta.

Lain 1 ja 3 §:llä pantaisiin täytäntöön direktiivin 1 artiklan 1 kohta.

2 §. *Määritelmät.* Pykälän 1 kohdan mukaan sähköisellä allekirjoituksella tarkoitettaisiin allekirjoittajan henkilöllisyyden todentamisen välineenä käytettävää toiseen sähköiseen tietoon liittyvää tietoa. Sähköinen allekirjoitus perustuu siihen, että sähköiset tiedot liitetään toisiinsa tavalla, jossa niistä muodostuu ainutkertainen yhdistelmä, joka mahdollistaa allekirjoittajan todentamisen.

Julkisen avaimen tekniikalla toteutetussa sähköisen allekirjoittamisen ja tunnistamisen

ympäristössä sähköinen allekirjoitus toteutetaan siten, että allekirjoittaja salaa viestistä tiivistealgoritmeilla muodostetun sanomatiivisteen yksityisellä avaimellaan. Salattu tiiviste toimii sähköisenä allekirjoituksena, joka lähetetään muun sähköisen viestin mukana.

Kehittynyt sähköinen allekirjoitus määriteltäisiin pykälän 2 kohdassa. Sähköisen allekirjoituksen tulee täyttää 2 kohdan a-d alakohdassa säädetyt erityiset vaatimukset, jotta se voisi olla kehittynyt sähköinen allekirjoitus.

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 4 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.

Allekirjoittajalla tarkoitettaisiin 3 kohdan mukaan luonnollista henkilöä, jolla on laillisesti hallussaan allekirjoituksen luomistiedot. Allekirjoittaja ei 3 kohdan määritelmän mukaan voisi koskaan olla oikeushenkilö, mutta allekirjoittaja voisi kuitenkin toimia edustamansa luonnollisen henkilön tai oikeushenkilön puolesta. Siten myös niin kutsutuilla roolivarmenteilla tehdyt allekirjoitukset, joissa luonnollinen henkilö toimii esimerkiksi edustamansa yrityksen nimissä, sisältyisivät allekirjoittajan määritelmään. Esimerkiksi yrityksen laillinen edustaja voidaan merkitä allekirjoitusvarmenteeseen 7 §:n 2 momentin 9 kohdan edellyttämällä tavalla. Samassa tarkoituksessa voidaan käyttää myös lisävarmennetta, josta ilmenee henkilön oikeus toimia yrityksen puolesta.

Allekirjoituksen luomistiedoilla tarkoitettaisiin 4 kohdan mukaan sitä ainutkertaista tietokokonaisuutta, 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 sanomatiiviseen salaamiseen, saadaan aikaan ainutkertainen salakirjoitus, joka aukeaa ainoastaan yksityistä avainta vastaavalla julkisella avaimella.

Allekirjoituksen luomisvälineitä olisivat 5 kohdan mukaan ohjelmistot ja laitteet, joita käytetään apuna luotaessa sähköistä allekirjoitusta. Julkisen avaimen järjestelmässä allekirjoituksen luomisväline voi sisältää esimerkiksi tiivistä algoritmin sanomatiiviseen laskemiseksi, salausalgoritmin sanomatiiviseen salaamiseksi sekä allekirjoittajan yksityisen avaimen. Lisäksi luomisvälineessä on erityisiä ohjelmistoja allekirjoituksen luomista varten.

Allekirjoituksen todentamistiedoilla tarkoitettaisiin 6 kohdan mukaan tietokokonaisuutta, jonka avulla vastaanottaja voi todentaa vastaanottamansa sähköisen allekirjoituksen. Julkisen avaimen järjestelmässä tietokokonaisuus on niin kutsuttu julkinen avain.

Varmenteella tarkoitettaisiin 7 kohdassa sähköistä todistusta, joka liittyy allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan henkilöllisyyden.

Varmentaja olisi 8 kohdan mukaan luon-

nollinen henkilö tai oikeushenkilö, joka tarjoaa sähköisissä allekirjoituksissa tarvittavia varmenteita.

Sähköisiin allekirjoituksiin liittyvällä tuotteella tarkoitettaisiin 9 kohdan mukaan laitteistoa tai ohjelmistoa tai niiden merkityksellistä osaa, joka on tarkoitettu varmennepalvelujen tarjoajan käyttöön tämän tarjotessa sähköisiin allekirjoituksiin liittyviä palveluja tai käytettäväksi sähköisten allekirjoitusten luomiseen tai todentamiseen.

Sähköisiin allekirjoituksiin liittyvällä palvelulla tarkoitettaisiin 10 kohdan mukaan sähköisiin allekirjoituksiin liittyvien varmenteiden sekä muiden sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaa. Tällaiseksi palveluksi katsottaisiin siten esimerkiksi erilaiset varmenteisiin liittyvät oheispalvelut, kuten rekisteröintipalvelut, aikaleimapalvelut, laskentapalvelut ja neuvontapalvelut.

3 §. *Soveltamisala.* Lakia sovellettaisiin sähköisiin allekirjoituksiin sekä palveluntarjoajiin, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä tuotteita tai palveluita yleisölle.

Lakia sovellettaisiin nimenomaan sähköisiin allekirjoituksiin liittyvien tuotteiden ja palvelujen tarjontaan. Lähtökohtana olisi sähköisiin allekirjoituksiin liittyvien tuotteiden ja palveluiden vapaa liikkuvuus EU:n sisämarkkinoilla lakiehdotuksen 4 §:n mukaisesti. Laissa annettaisiin kuitenkin sähköallekirjoitusdirektiivin täytäntöön panemiseksi tarvittavat säädökset erityisesti sähköisiin allekirjoituksiin tarvittavien varmenteiden tarjonnasta. Laissa säädettäisiin erityisesti laatuvarmenteita yleisölle tarjoavien varmentajien velvollisuuksista ja viranomaisvalvonnasta.

Yksinomaan muuhun kuin allekirjoitustarkoitukseen käytettävien varmenteiden tarjontaan lakia ei sovellettaisi, koska muiden varmenteiden käyttö on luonteeltaan erilaista. Lain soveltamisalan ulkopuolelle jäävä varmenteiden käyttötarkoitus olisi muun muassa varmenteen käyttö yksinomaan tunnistamiseen tai viestinnän salaamiseen.

Käytettäessä varmenteita osapuolten tunnistamiseen taustalla on yleensä osapuolten välinen erillinen liike- tai sopimussuhde. Varmenne on tällöin apuväline sopimussuh-

teen toteuttamisessa. Tunnistamisvarmenteen avulla käyttäjä voi esimerkiksi tunnistausta sellaisessa maksullisessa palvelussa, jonka käytöstä hän on tehnyt erillisen sopimuksen palvelun tarjoajan kanssa. Myös erilaiset laitteet ja järjestelmät tunnistavat toisiaan verkoviestinnässä varmennetekniikan avulla.

Teknisesti samaa varmennetta voidaan käyttää eri käyttötarkoituksiin. Sähköisen allekirjoituksen todentamiseen käytettävää varmennetta voidaan käyttää myös pelkkään tunnistamiseen. Henkilön tunnistaminen onkin yksi sähköisen allekirjoituksen käyttötarkoituksista. Myös allekirjoituksen luomis- ja todentamistietoja, kuten yksityistä avainta ja julkista avainta, voidaan käyttää myös tunnistautumisen ja salaustarkoituksessa. Mikäli kyseessä on varmenne, jota käytetään sähköisen allekirjoituksen todentamiseen, sovellettaisiin varmentajaan ja varmenteeseen tämän lain säännöksiä.

Lakia sovellettaisiin sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaan yleisölle. Yleisöllä tarkoitettaisiin käyttäjäryhmää, joka ei ole ennalta rajattu esimerkiksi työ-, virka- tai asiakassuhteen perusteella. Lakia ei siten sovellettaisi suljettuun käyttäjäryhmään. Laki ei koskisi esimerkiksi yrityskonsernin sisäiseen käyttöön tarkoitettujen varmenteiden tarjoamista. Laki ei soveltuisi myöskään vapaaehtoiisiin siviilioikeudellisiin sopimuksiin, joilla on sovittu sähköisen allekirjoituksen käytöstä tietyn, rajatun osanottajajoukon kesken. Avoimena käyttäjäryhmänä taas tulisi pitää ainakin sellaisia tapauksia, joissa varmenteeseen luottava osapuoli ei ole minkäänlaisessa sopimus-suhteessa varmentajaan eikä allekirjoittajaan. Yleisön käsitteen tarkempi tulkinta jää oikeuskäytännön varaan.

Ehdotettu laki olisi sähköisiä allekirjoituksia sekä niihin liittyvien tuotteiden ja palvelujen tarjontaa koskeva yleislaki. Sähköisten allekirjoitusten käytöstä hallinnossa olisi lisäksi voimassa mitä siitä erikseen säädetään. Lainsäädäntöä sähköisestä viranomaisasiointista valmistellaan oikeusministeriössä. Tarkoituksena on, että sähköisestä asiointista hallinnossa annettu laki tullaan samassa yhteydessä kumoamaan. Tavoitteena on, että tämän lakiesityksen mukaisen lain varmenteita ja varmentajia koskevat säännökset so-

veltuisivat lähtökohtaisesti myös hallinnon viranomaisasiointissa. Sähköistä viranomaisasiointia koskevassa laissa keskityttäisiin lähinnä itse asiointiprosessin sääntelyyn.

Lisäksi on mahdollista, että jonkin tietyn hallinnonalan sähköisistä palveluista on säädettävä erikseen kyseisten palvelujen erityispiirteiden vuoksi. Tämä saattaa olla mahdollista esimerkiksi sosiaali- ja terveystieteiden ja palveluiden vapaasta liikkumisesta sisämarkkinoilla. Tällä pykälällä pantaisiin täytäntöön direktiivin 4 artiklan sisämarkkinaperiaatteet.

4 §. *Palvelujen ja tuotteiden vapaa liikkuvuus.* Pykälässä säädettäisiin tämän lain mukaisten sähköisiin allekirjoituksiin liittyvien tuotteiden ja palveluiden vapaasta liikkumisesta sisämarkkinoilla. Tällä pykälällä pantaisiin täytäntöön direktiivin 4 artiklan sisämarkkinaperiaatteet.

5 §. *Turvallinen allekirjoituksen luomisväline.* Pykälässä säädettäisiin sellaisista vaatimuksista, jotka allekirjoituksen luomisvälineen tulee täyttää, jotta sitä voidaan pitää turvallisena allekirjoituksen luomisvälineenä. Ehdotetun lain 18 §:n mukaan sellainen kehittänyt sähköinen allekirjoitus, joka perustuu lain 7 §:ssä määriteltyyn laatuvarmenteeseen ja on tehty turvallisen allekirjoituksen luomisvälineen avulla täyttää lailla asetetun allekirjoituksen muotovaatimuksen.

Turvallisen allekirjoituksen luomisvälineen olisi riittävän luotettavasti varmistettava 1 momentin 1-5 kohdan vaatimusten täyttyminen. Riittävän luotettavalla tarkoitettaisiin mahdollisimman suurta luotettavuutta, joka voidaan saavuttaa käyttämällä hyväksi parhaimpia mahdollisia teknisiä ratkaisuja.

Momentin 1 kohdan mukaan luomisvälineen on luotettavasti varmistettava allekirjoituksen luomistietojen ainutkertaisuus ja luotattavuus. 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 suoritamat 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 suoritettavat 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 biometrisillä tunnistemenetelmillä.

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

Turvallisiin allekirjoituksen luomisvälineisiin liittyy runsaasti vireillä olevaa standardointityötä. Direktiivin yhtenä tavoitteena onkin koordinoita ja koota yhteen eurooppalaista standardointityötä siten, että Euroopan yhteisöjen komissio voisi vahvistaa ja julkaista sähköisiä allekirjoitusvälineitä koskevia yleisesti tunnustettujen standardien viitenumeroita Euroopan yhteisöjen virallisessa lehdessä, jäljempänä EYVL. Komissiota avustaa direktiivin 9 artiklan 1 kohdan mukaan sähköisten allekirjoitusten komitea, jonka tehtävinä direktiivin 10 artiklan mukaan on 3 artiklan 4 kohdan mukaisten perusteiden tarkentaminen (perusteet, joiden mu-

kaan jäsenvaltiot määrittelevät, onko tarkastuslaitos nimettävä) ja 3 artiklan 5 kohdan mukaisesti vahvistettujen ja julkaistujen yleisesti tunnustettujen standardien tarkentaminen (sähköisiin allekirjoituksiin liittyvien tuotteiden standardit).

Lakiehdotuksen 5 §:n 2 momentin 1 kohdan mukaan komission vahvistamien ja EYVL:ssä julkaistujen yleisesti tunnustettujen standardien mukaisen turvallisen allekirjoituksen luomisvälineen katsottaisiin aina täyttävän 5 §:n 1 momentissa säädetty vaatimukset. Pykälän 2 momentin 2 kohdan mukaan turvallisen allekirjoituksen luomisvälineen vaatimukset täyttäisi myös sellainen allekirjoituksen luomisväline, jonka vaatimusten arviointitehtävään nimetty tarkastuslaitos on turvalliseksi allekirjoituksen luomisvälineeksi hyväksynyt. Tarkastuslaitoksen tulisi olla nimenomaan kyseiseen arviointitehtävään nimetty sekä sijaita Suomessa tai muussa ETA-alueeseen kuuluvassa valtiossa. Direktiivin 3 artiklan 4 kohdan 2 alakohta edellyttää, että tällaisen laitoksen antama todistus luomisvälineen turvallisuudesta on tunnustettava kaikissa EU:n jäsenvaltioissa. Tarkastuslaitoksesta säädettäisiin lakiesityksen 6 §:ssä.

Pykälän 1 momentilla pantaisiin täytäntöön direktiivin liite 3. Pykälän 2 momentin 1 kohdan säännöksellä sekä 11 §:n 2 momentilla pantaisiin täytäntöön direktiivin 3 artiklan 5 kohta. Pykälän 2 momentin 2 kohdan säännöksellä pantaisiin täytäntöön direktiivin 3 artiklan 4 kohdan 2 alakohta.

6 §. *Tarkastuslaitos.* Ehdotetun 1 momentin perusteella Viestintävirasto voisi tarvittaessa nimetä tarkastuslaitoksia, joiden tehtävänä olisi selvittää, vastaako allekirjoituksen luomisväline 5 §:n 1 momentissa säädettyjä vaatimuksia. Tarkastuslaitos voisi olla joko yksityinen tai julkinen laitos.

Edellä 5 §:n perusteluissa mainittu direktiivin 9 artiklan mukainen sähköisten allekirjoitusten komitea on sopinut tarkastuslaitoksille asetettavista vähimmäisvaatimuksista, jotka Euroopan yhteisöjen komissio on vahvistanut 6 päivänä marraskuuta 2000 tehdyllä päätöksellä (Komission päätös 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 lopull.).

Komitean asettamien edellytysten mukaisesti tarkastuslaitoksen tulisi 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 tulisi olla asianmukaista eikä se saisi esimerkiksi syrjiä ketään, joka haluaa käyttää sen palveluita. Tarkastuslaitoksen tulisi käyttää selkeitä turvallisen allekirjoituksen luomisvälineen arviointikäytänteitä ja sen tulisi kirjata kaikki olennaiset arviointikäytänteitä koskevat tiedot. Kenen tahansa tulee voida käyttää laitoksen palveluita.

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

Viestintävirasto nimeäisi tarkastuslaitokset hakemuksen perusteella. Hakemuksen tulisi sisältää hakijan yhteystietojen ja kaupparekisteriotteen tai vastaavan selvityksen lisäksi selvitys 2 momentin tarkoittamien edellytys-

ten täyttymisestä hakijan toiminnassa. Viestintävirasto antaisi myös tarvittaessa ohjeita hakemukseen sisällytettävistä tiedoista ja niiden toimittamisesta Viestintävirastolle.

Viestintävirasto valvoisi tarkastuslaitoksen toimintaa. Tarkastuslaitoksen tulisi ilmoittaa Viestintävirastolle sellaisista toimintansa muutoksista, joilla on vaikutusta tarkastuslaitoksen nimeämisen edellytyksiin. Jos tarkastuslaitos ei enää täyttäisi asetettuja vaatimuksia tai se toimisi säännösten vastaisesti, Viestintäviraston tulisi peruuttaa nimeämis päätös.

Tarkastuslaitos voisi arviointitehtävässä käyttää apunaan laitoksen ulkopuolisia henkilöitä. Henkilöllä tarkoitettaisiin sekä yksityistä henkilöä että oikeushenkilöä. Tarkastuslaitos kuitenkin vastaisi myös apunaan käyttämiensä henkilöiden työstä. Tarkastuslaitoksen tulisi varmistaa ja kyetä osoittamaan apunaan käyttämänsä henkilön pätevyys kyseisiin tehtäviin.

Säännöksellä pantaisiin täytäntöön direktiivin 3 artiklan 4 kohdan 1 alakohta ja edellä mainittu komission päätös tarkastuslaitoksille asetettavista vähimmäisvaatimuksista (Bryssel, 06/11/2000, K(2000) 3179 lopull.).

2 luku. **Laatuvarmenteiden tarjoaminen**

7 §. *Laatuvarmenne.* Laatuvarmenteella tarkoitettaisiin varmennetta, joka täyttää 2 momentissa säädetyt vaatimukset ja jonka myöntänyt 10-15 §:ssä säädetyt vaatimukset täyttävä varmentaja. Laissa käytettäisiin nimitystä ”laatuvarmenne”, jolla tarkoitettaisiin samaa kuin direktiivin 2 artiklan 10 kohdan määritelmän ”hyväksytyllä varmenteella”. Pykälässä säädettäisiin laatuvarmenteen vähimmäisvaatimuksista.

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

Allekirjoittajan nimen tulisi 3 kohdan mukaan kuulua laatuvarmenteen tietosisältöön. Jos nimi olisi salanimi, olisi sen selkeästi käytävä ilmi varmenteesta.

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

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

Laatuvarmenteessa tulisi 6 kohdan mukaan olla sen yksilöivä tunnus. Luotettava varmennetoiminta edellyttää, että varmenteet voidaan erottaa toisistaan. Tunnus voisi olla juokseva sarjanumero tai muu yksilöllinen merkijono.

Momentin 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 8 kohdan mukaan ilmentävä laatuvarmenteesta. Rajoitus voi koskea esimerkiksi oikeustoimen rahamääräistä tai muuta vastaavaa rajoitusta. Rajoituksella voidaan esimerkiksi rajoittaa varmenteen käyttö vain tiettyihin oikeustoiimiin.

Pelkkä nimi ei välttämättä yksilöi allekirjoittajaa riittävästi. Allekirjoittajaan liittyvien erityisten tietojen tulisi 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. Esimerkiksi Väestörekisterikeskuksen myöntämässä varmenteessa tällainen tieto on väestötietojärjestelmään tallennettu sähköinen asiointitunnus. Erityinen tieto ei voi kuitenkaan olla allekirjoittajan henkilötunnus.

Säännöksellä pantaisiin täytäntöön direktiivin 2 artiklan 10 kohdan määritelmä ja direktiivin liite 1. Pykälän 2 momentin 3 koh-

dalla pantaisiin lisäksi täytäntöön direktiivin 8 artiklan 3 kohta.

8 §. *Muun kuin Suomeen sijoittautuneen varmentajan tarjoama laatuvarmenne.* Pykälässä säädettäisiin niistä edellytyksistä, joiden täytyessä muualle kuin Suomeen sijoittautuneen varmentajan varmenteiden katsottaisiin täyttävän 7 §:ssä säädetyt vaatimukset. Laatuvarmenteeksi voitaisiin katsoa ainoastaan tietosisältönsä puolesta asianmukainen varmenne. Varmenteen tulisi vähintään täyttää 7 §:n 2 momentin vaatimukset.

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

Momentin 2 kohdan mukaan laatuvarmenteeksi hyväksyttäisiin varmenne, jota tarjoaa jossain ETA-valtiossa vapaaehtoiseen akkreditointijärjestelmään liittynyt varmentaja, joka täyttää kyseisessä valtiossa sähköallekirjoitusdirektiivin 1999/93/EY täytäntöön panemiseksi säädetyt kansalliset vaatimukset. Vapaaehtoisia akkreditointijärjestelmiä voi olla useita ja niihin liittyminen ja kuuluminen on vapaaehtoista. Akkreditointijärjestelmiä ollaan perustamassa esimerkiksi Alankomaissa (TTP Netherlands) ja Isossa-Britanniassa (TScheme).

Laatuvarmenteeksi hyväksyttäisiin 3 kohdan mukaan varmenne, jonka takaaajana olisi ETA-valtioon sijoittautunut varmentaja, joka täyttää sijoittautumisvaltiossa sähköallekirjoitusdirektiivin täytäntöön panemiseksi säädetyt kansalliset vaatimukset.

Momentin 4 kohdan mukaan katsottaisiin varmentajan laatuvarmenteena tarjoaman varmenteen täyttävän 7 §:ssä säädetyt 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 pantaisiin täytäntöön direktiivin 7 artiklan 1 kohta.

9 §. *Ilmoitus toiminnan aloittamisesta.* Pykälän 1 momentin mukaan palveluntarjoajan tulisi tehdä Viestintävirastolle ilmoitus ennen kuin se aloittaa laatuvarmenteiden tarjoami-

sen yleisölle. Ilmoituksen tulisi olla kirjallinen. Siitä tulisi ilmetä varmentajan nimi ja yhteystiedot sekä tiedot, joiden perusteella 7 §:ssä ja 10-15 §:ssä säädettyjen vaatimusten täyttyminen voidaan varmistaa. Viestintävirasto voisi antaa tarpeellisia määräyksiä tai suosituksia ilmoitettavien tietojen toimittamisesta ja niiden tarkemmasta sisällöstä. Viestintäviraston määräyksillä ja suosituksilla voitaisiin myöhemmin täsmentää laissa määriteltujen edellytysten toteamiseksi ja valvontatehtävän suorittamiseksi tarvittavia tietoja. Määräyksillä ja suosituksilla ei luotaisi laatuvarmenteiden tarjoajille uusia velvollisuuksia. Mahdollisuus antaa myöhemmin tarkempia määräyksiä ja suosituksia on tarpeen tämänhetkisen varmennetoiminnan kehittymättömyyden ja keskeneräisen standardointitoiminnan vuoksi.

Laatuvarmenteiden tarjonnan aloittaminen ei edellyttäisi Viestintäviraston etukäteistä hyväksyntää, mutta Viestintävirasto voisi ilmoituksen saatuaan viipymättä kieltää laatuvarmenteiden tarjonnan 2 momentissa säädettyllä tavalla, ellei laatuvarmenteesta ja laatuvarmenteita yleisölle tarjoavasta varmentajasta säädetty edellytykset täyty. Kielto koskisi vain oikeutta tarjota varmenteita laatuvarmenteina. Esimerkiksi varmenteen tietosisältöön ei saisi sisältyä tietoa laatuvarmenteesta. Muutoin varmentaja voisi jatkaa varmennetoimintaansa kiellosta huolimatta ja tarjota varmenteita tavallisina varmenteina.

Varmentaja, joka tarjoaa varmenteitaan yleisölle laatuvarmenteina vastaisi kuitenkin aina tämän lakiesityksen mukaisena laatuvarmentajana mahdollisista vahingoista, joita saattaa syntyä siitä, että laatuvarmenteen vaatimuksia täyttämätöntä varmennetta käytetään laatuvarmenteena. Laatuvarmenteita yleisölle tarjoavan varmentajan vahingonkorvausvastuusta säädetään tämän lakiesityksen 16 §:ssä. Viestintäviraston olisi ilmoituksen tekijän intressit ja edellä mainittu laatuvarmenteita yleisölle tarjoavan varmentajan korvausvastuu huomioiden toimittava asiassa viipymättä, jotta varmentaja saa Viestintävirastolta tiedon liiketoimintansa tueksi mahdollisimman nopeasti. Varmentajan olisi myös viipymättä ilmoitettava Viestintävirastolle, jos ilmoitetuissa tiedoissa tapahtuu muutoksia. Ehdotetun lain mukaan Viestintä-

virasto valvoisi laatuvarmenteita yleisölle tarjoavia varmentajia lakiesityksen 4 luvusta ilmenevällä tavalla. Valvontatehtävien toteuttamiseksi Viestintävirasto tarvitsee riittävät ja oikeat tiedot laatuvarmenteita yleisölle tarjoavista varmentajista.

Viestintävirasto pitäisi laatuvarmenteita myöntävistä varmentajista julkista rekisteriä. Rekisteri sisältäisi muun muassa varmentajan nimen ja osoitetiedot siten kuin varmentaja on ne Viestintävirastolle ilmoittanut. Rekisteristä olisi saatavissa tiedot niistä varmentajista, jotka ovat ilmoittaneet Viestintävirastolle tarjoavansa laatuvarmenteita Suomessa. Rekisterin tiedoilla olisi kuitenkin ainoastaan informatiivinen tehtävä. Laatuvarmenteita yleisölle myöntävä varmentaja vastaisi kolmansille osapuolille lakiesityksen 16 §:n mukaisesti mahdollisista toiminnastaan aiheutuneista vahingoista, riippumatta siitä onko kyseinen varmentaja merkitty Viestintäviraston rekisteriin vai ei.

Säännöksellä pantaisiin täytäntöön direktiivin 3 artiklan 1 kohta ja osittain 3 kohta. Direktiivin 3 artiklan 3 kohdan mukaisesta valvontajärjestelmästä säädettäisiin lain 22-28 §:ssä.

10 §. *Laatuvarmenteita yleisölle tarjoavan varmentajan yleiset velvollisuudet.* Pykälässä säädettäisiin laatuvarmenteita yleisölle tarjoavan varmentajan yleisistä velvollisuuksista. Varmentajan olisi toimittava huolellisesti, luotettavasti ja asianmukaisesti. Huolellisuus-, luotettavuus- ja asianmukaisuusvaatimuksilla pyritään lisäämään julkista luottamusta sähköisen asioinnin ja siihen liittyvän varmennetoiminnan turvallisuuteen. Asianmukaisuusvaatimus kohdistuisi lähinnä varmentajan toimintaan asiakaspalvelussa. Huolellisuus- ja luotettavuusvaatimuksen sisältöä on käsitelty tämän pykälän perustelujen lisäksi myös muissa tämän lakiesityksen pykälissä ja niiden perusteluissa.

Varmentajalla olisi myös velvollisuus huolehtia siitä, että sen mahdollisesti apunaan käyttämät henkilöt toimivat huolellisesti ja luotettavasti. Henkilöillä tarkoitettaisiin sekä luonnollisia henkilöitä että oikeushenkilöitä. Laatuvarmenteiden tarjoaja eli se, jonka nimi on varmenteessa, olisi vastuussa kaikista varmentamistoiminnan osa-alueista, vaikka se ostaisikin osan tarjoamisestaan palveluista

tai tuotteista alihankkijoilta. Varmentajan apunaan käyttämien henkilöiden suorittamia tehtäviä voisivat olla esimerkiksi varmennehakemusten vastaanottaminen, varmenteen luominen sekä sulkulistan ylläpito.

Varmentajalla tulisi olla myös harjoitetun toiminnan laajuuteen nähden riittävät tekniset taidot ja taloudelliset voimavarat. Varmentajan tulisi 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.

Pykälän 2 momentin 1 kohdan mukaan varmentajalla tulisi 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 tietoturvasuasioista.

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

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

Varmennepolitiikka on asiakirja, jonka perusteella varmentaja myöntää varmenteita ja

joka käyttäjän pitää tuntea ja hyväksyä. Poliittika määrittelee säännöt varmentajan toiminnalle ja sen perusteella voidaan arvioida varmenteiden käytettävyyttä tiettyyn sovellukseen. Poliittika 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 minimitalon 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.

Momentin 3 kohdassa tarkoitettujen tietojen tulisi olla yleisesti saatavilla. Tietojen katsottaisiin olevan yleisesti saatavilla muun muassa silloin, kun ne olisivat noudettavissa varmentajan toimipaikasta tai saatavilla varmentajan kotisivulla internetissä.

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

Varmentaja ei 3 momentin mukaan saisi 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 olisi tällaisessa tilanteessa tehdä välittömästi 13 §:ssä tarkoitettu ilmoitus.

Säännöksellä pantaisiin täytäntöön direktiivin liitteen 2 kohdat a, e, g, h ja j.

11 §. *Luotettavat laitteet ja ohjelmistot.* Laatuvarmenteita yleisölle tarjoavan varmentajan käyttämien järjestelmien sekä laitteiden ja ohjelmistojen on oltava riittävän turvallisia ja luotettavia sekä suojattuja muutoksilta ja väärentämiseltä. Riittävän turvallisella ja luotettavalla tarkoitettaisiin mahdollisimman suurta luotettavuutta, joka voidaan saavuttaa käyttämällä hyväksi parhaita mahdollisia teknisiä ratkaisuja. Järjestelmät ja sen osat tulisi olla suojattu siten, että vain varmentajan erikseen nimetty henkilöstö voisi tehdä niihin muutoksia ja että muutokset, myös mahdolliset ulkopuolisten tai laitevikojen aiheuttamat, rekisteröityisivät ja tieto niistä säilytettäisiin.

Pykälän 2 momentissa säädettäisiin siitä, että Euroopan yhteisöjen komission vahvistamien, EYVL:ssä julkaistujen yleisesti tunnustettujen standardien mukaiset laitteet ja ohjelmistot katsottaisiin aina 1 momentissa säädettyjen vaatimusten mukaisiksi.

Säännöksellä pantaisiin täytäntöön direktiivin 3 artiklan 5 kohta ja liitteen 2 kohta f.

12 §. *Laatuvarmenteen myöntäminen.* Laatuvarmenteita yleisölle tarjoavan varmentajan tulisi huolellisesti ja luotettavalla tavalla tarkistaa hakijan henkilöllisyys ja muut laatuvarmenteen myöntämisessä ja ylläpidossa tarpeelliset hakijan henkilöön liittyvät tiedot. Hakijan henkilöön liittyviä tietoja voisivat olla ainakin hakijan nimi ja osoitetiedot sekä laatuvarmenteen tietosisältöön 7 §:n 2 momentin mukaisesti kuuluvat tiedot, mukaan lukien varmenteen tiettyyn käyttötarkoitukseen mahdollisesti liittyvät erityiset tiedot.

Laatuvarmenteita yleisölle tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti. Henkilökohtaisella tunnistamisella tarkoitettaisiin sitä, että hakijan on laatuvarmennetta hakiessaan henkilökohtaisesti käytävä varmentajan luona tunnistettavana.

Laatuvarmenteita yleisölle tarjoava varmentaja saisi vaatia laatuvarmenteen hakijalta henkilötunnuksen ilmoittamista henkilöllisyyden tarkistamiseksi. Tämä on tarpeen hakijan luotettavan tunnistamisen takaamiseksi. Henkilötunnuksen ilmoittamisesta on säädetty lakiesityksen 19 §:n 2 momentissa, joka oikeuttaa kaikki varmenteiden tarjoajat vaa-

timaan varmenteen hakijalta henkilötunnuksen ilmoittamista. Tällöin on itsestään selvää, että myös laatuvarmenteita tarjoavalla varmentajalla on kyseinen oikeus. Kaikkia varmentajia koskevaksi on myös 19 §:n 2 momentissa säädetty kieltö sisällyttää henkilötunnusta varmenteeseen. Henkilötunnusta ei siten saa sisällyttää myöskään laatuvarmenteeseen.

Hakijan henkilöllisyyden tarkistaminen luotettavalla tavalla voisi tapahtua hakijan esittämästä luotettavasta asiakirjasta. Luotettavina asiakirjoina voitaisiin pitää ainakin poliisin myöntämää henkilöllisyyden osoittavaa asiakirjaa, passia, henkilökorttia tai vuoden 1990 syyskuun jälkeen myönnettyä ajokorttia.

Laatuvarmenteita yleisölle 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 ainutkertaistietoisuus 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 varmistetaan laatuvarmenteeseen merkittyjen tietojen oikeellisuudesta sekä laatuvarmenteen luovuttamisesta hallintaan oikeutetulle henkilölle. Varmentaja vastaa 16 §:ssä säädetyn mukaisesti muun muassa siitä, että laatuvarmenteeseen merkityt tiedot ovat myöntämishetkellä oikeita ja että laatuvarmenne luovutetaan sen hallintaan oikeutetulle henkilölle. Myöntämishetkeksi katsottaisiin 16 §:n yksityiskohtaisten perustelujen mukaisesti laatuvarmenteen luovutushetki.

Varmentajan tulee 2 momentin mukaan antaa varmenteen hakijalle ennen sopimuksen tekemistä tiedot varmenteen käyttöehdoista mahdollisine käyttörajoituksineen, vapaaehtoisista akkreditointijärjestelmistä, varmentetoiminnan viranomaisvalvonnasta sekä valitus- ja riitojenratkaisumenettelyistä. Käyttöehtoihin sisältyviä tietoja olisivat muun

muassa tiedot mahdollisten hakemistopalvelujen käytöstä, sekä erityisesti laatuvarmenteen peruuttamisesta ja varmenteen merkitsemisestä sulkulistalle. Käyttöehtoihin tulisi sisältyä myös tiedot varmentajan vahingonkorvausvastuusta ja muista velvollisuuksista.

Varmenteen hakijaa tulisi 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. Suomessa toimittaessa kyseiset tiedot tulisi pyrkiä antamaan laatuvarmenteen hakijalle ainakin Suomessa käytössä olevilla virallisilla kielillä.

Säännöksellä pantaisiin täytäntöön direktiivin liitteen 2 kohdat d ja k.

13 §. *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 olisi 2 momentin mukaan viipymättä peruutettava laatuvarmenne, jos allekirjoittaja sitä pyytää. Varmentajan tulisi peruuttaa laatuvarmenne merkitsemällä siitä tieto 14 §:n 3 momentin mukaiselle sulkulistalle. Allekirjoittajan ei tarvitsisi perustella pyyntöään.

Peruuttamispyynnön saapumisajankohtana olisi pidettävä hetkeä jolloin pyyntö on ollut varmentajan käytettävissä siten, että sitä voidaan käsitellä. Sähköisessä muodossa lähetetyn viestin osalta tämä tarkoittaisi ajan-

kohtaa jolloin pyyntö olisi varmentajan käytettävissä vastaanottolaitteessa tai tietojärjestelmässä.

Varmentaja voisi 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 voisi olla myös varmentajan toiminnan päätyminen. Lisäksi varmentaja voisi peruuttaa varmenteen, jos allekirjoittaja rikkoo varmentajan kanssa tehtyä sopimusta tai käyttää varmennetta vastoin sen käyttötarkoitusta. Laatuvarmenteen peruuttamisesta ja peruuttamisen ajankohdasta tulisi 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 säädettäisiin lakiehdotuksen 16 ja 17 §:ssä.

14 §. *Laatuvarmenteita yleisölle myöntävän varmentajan ylläpitämät rekisterit.* Laatuvarmenteita yleisölle tarjoavalle varmentajalle on sähköallekirjoitusdirektiivin 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 yleisölle tarjoava varmentaja arkistoi kaikki asiaankuuluvat varmennetta koskevat tiedot tarkoituksenmukaiseksi ajaksi erityisesti voidakseen esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä.

Laatuvarmenteita yleisölle tarjoavien varmentajien ylläpitämiä rekistereitä koskevalla säännöksellä pyritään takaamaan se, että laatuvarmenteiden käyttöön keskeisesti liittyvät palvelut olisivat mahdollisimman tehokkaasti ja luotettavana käytettävissä. Nimenomaan näiden palveluiden avulla varmentaja toimii luotettavana kolmantena osapuolena, joka todentaa laatuvarmenteella viestin vastaanottajalle viestin lähettäjän ja tämän allekirjoituksen luomistietojen voimassaolon. Lain 14 ja 15 §:ssä säädettäisiin myös tallennettavista tiedoista ja niiden säilyttämisestä.

Laatuvarmenteita yleisölle myöntävän varmentajan tulisi 1 momentin mukaan ylläpitää rekisteriä myöntämistään varmenteista (varmennerekisteri). Rekisteriin tulisi merkitä 7 §:n 2 momentissa määritellyn laatuvarmenteen tietosisällön lisäksi 12 §:n 1 momentissa tarkoitettujen hakijan henkilöön liittyvät tiedot, mukaan lukien tieto laatuvarmentetta myönnettäessä käytetystä hakijan tunnistamismenettelystä, sekä 21 §:ssä tarkoitettujen tiedot varmenteen voimassaolon tarkistamisesta sulkulistalta, silloin kun laatuvarmenteita yleisölle tarjoava varmentaja käyttää 21 §:n mukaista oikeutta tallettaa sulkulistan tarkistustiedot.

Laatuvarmenteita yleisölle tarjoava varmentaja voisi näin ollen tallentaa esimerkiksi tiedon siitä, mistä asiakirjasta tunnistaminen on tehty, ja tallentaa myös tarvittavat tiedot kyseisestä asiakirjasta. Kyseinen tarvittava tieto voisi olla esimerkiksi passin numero tai henkilötunnus. Laatuvarmenteita yleisölle tarjoava varmentaja voisi myös esimerkiksi ottaa valokopioita tunnistamisessa käytetyistä asiakirjoista. Olennaista tietojen tallentamisessa on laatuvarmenteita yleisölle tarjoavalle varmentajalle asetetun huolellisen ja luotettavan tunnistamisen todentaminen. Koska varmentajalla on 16 §:ssä määritelty ankara vahingonkorvausvastuu myöntämänsä laatuvarmenteen tietojen paikkansapitävyydestä, tulee varmentajalla myös olla mahdollisuus tarpeen vaatiessa todistaa toimineensa huolellisesti. Laatuvarmenteen tarkistamista koskevan tiedon tallettaminen olisi tarpeen esimerkiksi varmenteiden käytön laskutusta ja mahdollisia riitatilanteiden selvittämistä varten. Tarkistamista koskevan tiedon käytämisestä säädettäisiin tarkemmin 21 §:ssä.

Laatuvarmenteita yleisölle myöntävän varmentajan tulisi 2 momentin mukaan varmistaa, että laatuvarmenteella varmennettuun kehittyneeseen sähköiseen allekirjoitukseen luottavalla osapuolella on saatavilla 7 §:n 2 momentissa määritelty laatuvarmenteen tietosisältö. Pykälässä ei ole tarkoitus säätää tarkemmin sitä, miten tiedot tulisi olla allekirjoitukseen luottavien osapuolien saatavilla. Varmentaja voisi käyttämistään teknisistä sovelluksista riippuen toteuttaa vaatimuksen tarkoituksenmukaisimmalla tavalla. Jos allekirjoittajan ja varmentajan välisellä sopimuk-

sella sovitaan, että allekirjoittaja itse jakaa viestin mukana myös laatuvarmenteen, tulee varmenteen tietosisältö luottavan osapuolen tietoon ilman erityisiä varmentajan toimenpiteitä. Näissä tapauksissa ei tarvittaisi erillistä varmentajan tarjoamaa palvelua. Varmentaja ja allekirjoittaja voivat myös sopia, että varmentaja luovuttaa varmennerekisteristä allekirjoitukseen luottavalle taholle 7 §:n 2 momentissa määritellyn tietosisällön mukaiset tiedot. Sähköisten allekirjoitusten luotettavuudelle olennaista on, että allekirjoitukseen luottavan osapuolen tietoon tulee laatuvarmenteen tietosisällön mukaiset tiedot.

Laatuvarmenteita yleisölle tarjoavan varmentajan tulisi 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 13 §:n mukaisesti pyytänyt varmentajalta laatuvarmenteensa peruuttamista. Vastuu allekirjoituksen luomistietojen käytöstä allekirjoittajan peruutuspyynnön ja sulkulistalle merkinnän välisenä aikana kuuluisi varmentajalle, joten nopea merkinnän tekeminen olisi varmentajan omassa intressissä. Luomistietojen oikeudettomasta käytöstä on säädetty tarkemmin 17 §:ssä.

Sulkulista tulisi toteuttaa julkisena rekisterinä, koska ainoastaan sulkulistalta allekirjoitukseen luottava osapuoli voi todeta mahdollisen varmenteen peruuttamisen. Sulkulista voidaan toteuttaa esimerkiksi merkitsemällä sulkulistalle ainoastaan laatuvarmenteen yksilöivä tunnus. Tällöin sulkulista ei tule sisältämään laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen haltijan henkilöön liittyviä tietoja. Mikäli sulkulistalle merkitään allekirjoittajan henkilöön liittyviä tietoja, tulisi tietojen merkitsemisestä saada allekirjoittajan nimenomainen suostumus. Tiettyyn laatuvarmenteeseen luottavan osapuolen kannalta riittää, että se voi tarkistaa laatuvarmenteen yksilöivän tunnusteen avulla, onko kyseessä oleva laatuvarmenne peruutettu.

Laatuvarmenteen 7 §:n 2 momentin tietojen ja sulkulistan tulisi 4 momentin mukaisesti olla ympärivuorokautisesti käytettävissä,

koska tietoverkot mahdollistavat asioinnin vuorokaudenajasta riippumatta. Jos varmentaja jakaa 7 §:n 2 momentissa tarkoitettuja tietoja, tulee palvelun olla käytettävissä ympärivuorokautisesti. Jos allekirjoittaja itse jakaa laatuvarmennetta, ei tarvetta erilliseen varmentajan toteuttamaan palveluun olisi, vaan tällöin voitaisiin katsoa, että 7 §:n 2 momentin määrittelemä laatuvarmenteen tietosisältö olisi ympärivuorokautisesti käytettävissä allekirjoittajan jakamana. Laatuvarmenteita yleisölle tarjoavan varmentajan ylläpitämisen sulkulistan tulee kuitenkin aina olla käytettävissä ympärivuorokautisesti.

Säännöksellä pantaisiin täytäntöön direktiivin liitteen 2 kohdat b ja c.

15 §. *Varmennerekisterin tietojen säilyttäminen.* Varmentajalla on velvollisuus luotettavalla ja tarkoituksenmukaisella tavalla säilyttää varmennerekisteriin 14 §:n mukaisesti merkittävät tiedot 10 vuoden ajan laatuvarmenteen voimassaolon päättymisestä. Tiedot voitaisiin säilyttää myös sähköisessä muodossa.

Varmenteiden tarjonnan ja käytön ollessa vielä kehittymätöntä, ei voida täsmällisesti määrittellä niitä tilanteita, joissa varmenteita tullaan jatkossa käyttämään. Näin ollen myös näyttökysymyksiin ja näytön saatavuuteen mahdollisesti liittyviä ongelmia, esimerkiksi väärinkäytöksistä aiheutuvien vahinkojen kohdalla, on mahdotonta täsmällisesti arvioida. Tämän vuoksi olisi perusteltua säätää varmennerekisterin tietojen säilyttämiseksi pitkä, kymmenen vuoden määräaika.

Tietojen säilyttämisessä tulisi käyttää luotettavia järjestelmiä. Tietojen tallettaminen ja tietoihin tehtävät muutokset tulisi tehdä vain varmentajan valtuuttamien, luotettavien henkilöiden toimesta. Lisäksi säilytettävien tietojen turvallisuutta vaarantavat tekniset muutokset tulisi olla tietoja säilyttävän tahon havaittavissa. Henkilötietojen käsittelyn tulisi tapahtua henkilötietolain säännösten mukaisesti. Henkilötietolain soveltamisesta kaikkien varmentajien toimintaan on 19 §:ssä informatiivinen viittaus.

Säännöksellä pantaisiin täytäntöön direktiivin liitteen 2 kohdat i ja l.

16 §. *Laatuvarmenteita tarjoavan varmentajan vahingonkorvausvastuu.* Sähköisten allekirjoitusten käyttö perustuu suurelta osin

luottamukseen varmentajan toimintaa kohtaan. Sähköisten allekirjoitusten käytön yhteydessä mahdollisesti syntyvistä ongelmalanteista 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 sähköallekirjoitusdirektiivi edellyttää laatuvarmenteita yleisölle tarjoavan varmentajan vastuun sääntämistä 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 sopimus-oikeudellista korvausvastuuta koskevien periaatteiden mukaan. Allekirjoituksen luomistietojen oikeudettoman käytön tapauksissa riskin jakautumisesta varmentajan ja allekirjoittajan välillä säädetään erikseen 17 §:ssä.

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

Pykälän 1 momentin 1 ja 2 kohdan mukaan laatuvarmenteita yleisölle tarjoava varmentaja olisi velvollinen korvaamaan vahingon, joka on aiheutunut siitä, että laatuvarmenteeseen merkityt tiedot ovat myöntämishetkellä olleet virheellisiä tai että laatuvarmen-

teessa ei ole 7 §:n 2 momentissa mainittuja tietoja. Myöntämishetkellä tarkoitettaisiin ajankohtaa, jolloin laatuvarmenne luovutetaan hakijan käyttöön. Allekirjoittajan edun mukaista olisi viipymättä ilmoittaa myöntämishetkellä ilmoitetuissa tiedoissa tapahtuvista muutoksista varmentajalle, jotta tämä voisi myöntää uuden, muuttuneita tietoja vastaavan laatuvarmenteen.

Pykälän 1 momentin 3 kohdan mukaan laatuvarmenteita yleisölle tarjoava varmentaja vastaisi vahingoista, jotka ovat aiheutuneet siitä, että laatuvarmenteessa yksilöidyllä henkilöllä ei varmenteen myöntämisaikahankotana ole ollut todentamistietoja vastaavia luomistietoja. Sähköisen allekirjoituksen luotettavuus perustuu siihen, että allekirjoituksen luomistietoja käyttää vain se henkilö, jonka nimi on laatuvarmenteessa. Ongelmatilanteissa laatuvarmenteita yleisölle tarjoavan varmentajan on korvausvastuun välttämiseksi pystyttävä osoittamaan, että se on menetellyt huolellisesti tarkistaessaan 12 §:n 1 momentissa tarkoitettulla 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.

Pykälän 1 momentin 4 kohdan mukaan varmentaja vastaisi vahingoista, jotka aiheutuvat siitä, että luomistietoja ja todentamistietoja ei voisi käyttää yhdessä. Allekirjoituksen luomistietojen ja allekirjoituksen todentamistietojen yhteentoimivuus on välttämätön edellytys sähköisen allekirjoituksen käytölle. Kohdassa säädettäisiin vain niistä tilanteista, joissa laatuvarmenteita yleisölle 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.

Pykälän 1 momentin 5 kohdan mukaan varmentaja vastaisi laatuvarmenteeseen luot-

taneelle vahingoista, jos laatuvarmenne ei ole peruutettu 13 §:ssä säädetyllä tavalla. Kolmannen osapuolen eli sähköisen allekirjoituksen todentajan tulee voida luottaa varmenteen olevan voimassa ja hallintaan oikeutetulla henkilöllä, jollei varmenne ole peruutettu ja merkitty sulkulistalle, jota varmentaja ylläpitää peruutetuista laatuvarmenteista. Allekirjoituksen luomistietojen kadotessa tai tuhoutuessa laatuvarmenteen viipymättömän peruuttaminen ehkäisee tehokkaasti vahinkojen syntymistä. Kohdassa säädetty korvausvastuu koskisi allekirjoittajan tekemän varmenteen peruuttamispyynnön saapumisen jälkeistä aikaa. Ennen peruuttamispyynnön saapumista varmentajalle allekirjoittaja vastaisi aiheutuneista vahingoista 17 §: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.

Pykälän 2 momentin mukaan laatuvarmenteita yleisölle tarjoava varmentaja vapautuisi 1 momentissa tarkoitettusta vastuusta näyttämällä, että vahinko ei ole aiheutunut varmentajan tai sen apunaan käyttämän henkilön huolimattomuudesta. Tämä niin sanottu pre-

sumoitu tuottamsvastuu merkitsee poikkeusta siitä vahingonkorvausoikeudellisesta pääsäännöstä, että vahinkoa kärsinyt on velvollinen näyttämään vahingon aiheuttajan toimineen huolimattomasti. Momentissa säädetty käännetty todistustaakka koskisi ainoastaan vastuun perustetta, joten vahinkoa kärsinyt olisi velvollinen normaaliin tapaan esittämään näytön varmentajan toiminnan ja kärsimänsä vahingon välisestä syy-yhteydestä.

Pykälän 3 momentin mukaan laatuvarmenteita yleisölle tarjoava varmentaja ei vastaisi vahingosta, joka on aiheutunut laatuvarmenteeseen sisältyvän käyttörajoituksen vastaisesta käytöstä. Laatuvarmenteen käyttöä voidaan rajoittaa eri syistä. Laatuvarmente 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 käyttörajoitusten tehokkuudelle suhteessa kolmansiin osapuoliin on, että rajoitus tulee kolmansien tietoon. Käyttörajoitusten tulisi lain 7 §:n 2 momentin 8 kohdan mukaan näkyä laatuvarmenteessa, joten niistä välittyisi aina tieto myös allekirjoituksen todentajalle.

Laatuvarmenteita yleisölle tarjoavan varmentajan toiminnasta aiheutuvaan korvausvastuuseen sovellettaisiin ehdotetun lain ohella vahingonkorvauslakia (412/1974). Tästä ehdotetaan selvyuden vuoksi säädettäväksi pykälän 4 momentissa.

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

Muilta osin laatuvarmenteita yleisölle tarjoavien varmentajien korvausvastuu suhteessa sellaiseen laatuvarmenteeseen luottaneeseen tahoon, johon varmentaja ei ole sopimussuhteessa, määräytyisi kokonaisuudes-

saan vahingonkorvauslain ja yleisten vahingonkorvausoikeudellisten periaatteiden mukaan. Muiden kuin laatuvarmenteita tarjoavien varmentajien korvausvastuu määräytyisi kokonaisuudessaan vahingonkorvauslain ja yleisten vahingonkorvausoikeudellisten periaatteiden mukaan, koska ehdotettua vastuusääntelyä ei sovellettaisi niihin.

Pykälän 4 momentissa säädettäisiin myös ehdotetun 16 §:n korvaussääntelyn ulottamisesta varmenteen yleisölle laatuvarmenteeksi takaavaan varmentajaan. Sähköallekirjoitusdirektiivi edellyttää jäsenvaltioiden varmistavan ainakin, että 16 §:n 1 momentin 1-4 kohdassa mainittu korvausvastuu ulotetaan myös varmenteen yleisölle laatuvarmenteeksi takaaviin varmentajiin. Lakiesityksessä ehdotetaan 16 §:n 1 momentin 1-4 kohdan vastuuperusteiden lisäksi myös 5 kohdan (varmenteen peruuttamatta jättäminen) vastuuperusteiden 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.

Ehdotetulla 16 §:llä pantaisiin täytäntöön direktiivin 6 artikla, joka käsittelee laatuvarmenteita yleisölle tarjoavien varmentajien tai varmenteen yleisölle laatuvarmenteeksi takaavien varmentajien vahingonkorvausvastuuta laatuvarmenteeseen perustellulla tavalla tukeutuvalla. Artiklassa käytetty käsite ”perustellulla tavalla tukeutuva” (who reasonably relies on), on Suomen voimassa olevassa vahingonkorvauslaissa ja –käytännössä tuntematon käsite. Ehdotetussa 16 §:ssä säädettäisiinkin laatuvarmenteita yleisölle tarjoavan varmentajan vahingonkorvausvastuusta ”laatuvarmenteeseen luottaneelle” aiheutuneen vahingon osalta. Koska direktiivin 6 artiklassa asetetaan jäsenvaltioille ainoastaan minimivaatimukset, on 16 §:n mukainen kansallinen sääntely mahdollista. Direktiivin minisääntelystä 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.

17 §. *Vastuu allekirjoituksen luomistietojen oikeudettomasta käytöstä.* Pykälässä säänneltäisiin allekirjoittajan vastuuta allekirjoituksen luomistietojen oikeudettomasta käytöstä aiheutuneesta vahingosta.

Allekirjoituksen luomistietojen oikeudeton käyttö olisi 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 olisi perusteltua säätää periaatteiltaan samansuuntaisista vastuusäännöksistä. Käytännössä merkittävimpana erona esimerkiksi luottokorttien käyttöön on se, että luomistietojen käyttö tullaan sovellettavasta tekniikasta riippuen suojaamaan esimerkiksi salasanalla tai tunnuksella (esim. PIN-koodi). 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 vastaisi luomistietojen oikeudettomasta käytöstä, kunnes peruuttamispyyntö on saapunut varmentajalle 13 §: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, säädettäisiin 2 momentissa kuluttajiin sovellettavista rajoituksista.

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

Pykälän 2 momentin 2 kohdan mukaan kuluttaja voisi 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 voitaisiin jatkossa 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 voitaisiin odottaa kuluttajan luomistietoja säilyttävän. Huolimattomuutta arvioitaessa tulisi ottaa huomioon myös, että allekirjoituksen käyttö liittyy useisiin päivittäisiin toimenpiteisiin, joten luomistietoja tulisi voida kuljettaa allekirjoittajan mukana. Toimikorttia, jolla luomistiedot sijaitsevat tulisi voida kuljettaa esimerkiksi lompakossa. Tulevaisuudessa mahdollisesti matkapuhelimen SIM-kortille talletettavien luomistietojen tapauksessa tulisi luonnollisesti matkapuhelinta voida kuljettaa allekirjoittajan mukana.

Lisäksi allekirjoittajan huolimattomuutta arvioitaessa tulisi erityisesti ottaa huomioon hänen toimintansa luomistietojen käytön suojaukseen liittyvän salasanan tai tunnuksen säilyttämisessä huolellisesti ja siten, että salasanaa tai tunnusta ei säilytetä 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 kat-

soa lainkaan syyllystyneen huolimattomuuteen tai että hänen huolimattomuutensa on ollut lievää. Momentin 3 kohdan mukaan allekirjoittaja voisi joutua vastaamaan luomistietoja oikeudettomasti käyttäneen henkilön tekemistä oikeustoimista aiheutuneista vahingoista vain, jos hän menetettyään luomistietojen hallinnan on laiminlyönyt viipymättä pyytää laatuvarmenteen peruuttamista siten, kuin 13 §:n 1 momentissa säädetään. Ehdotun 3 kohdan säännöksellä pyritäisiin suojaamaan kuluttajaa, jonka voitaisiin katsoa syyllystyneen korkeintaan lievään huolimattomuuteen luomistietojen joutumisessa niiden käyttöön oikeudettomalle henkilölle. Allekirjoittaja vastaisi 3 kohdan tarkoittamissa tapauksissa luomistietojen oikeudettomasta käytöstä aiheutuneista vahingoista siitä hetkestä alkaen, jolloin allekirjoittajan voitaisiin katsoa laiminlyöneen 13 §:n 1 momentissa tarkoitetun laatuvarmenteen peruuttamispyynnön. Lähtökohtana on, että allekirjoittaja pyytäisi laatuvarmenteen peruuttamista välittömästi havaittuaan luomistietojen katoamisen.

Pykälän 3 momentissa säädettäisiin, että sopimusehto, joka poikkeaa 2 momentin säännöksistä kuluttajan vahingoksi olisi mitätön. Kuluttajan asemaa parantava sopimusehto olisi luonnollisesti mahdollinen. Varmentaja voisi siis sopimuksessa sitoutua säädettyä laajempaankin vastuuseen.

Ehdotettua pykälää vastaavaa säännöstä ei sisälly sähköallekirjoitusdirektiiviin. Pykälän säännöksillä on tarpeen kansallisella tasolla täsmentää riskinjakoa allekirjoituksen luomistietojen oikeudettomassa käytössä.

3 luku. **Sähköisen allekirjoituksen oikeusvaikutus ja henkilötietojen käsittely**

18 § *Sähköisen allekirjoituksen oikeusvaikutus.* Pykälässä säädettäisiin sähköisen allekirjoituksen oikeusvaikutuksesta. Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttäisi ainakin laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla tehty kehittynyt sähköinen allekirjoitus.

Oikeustoimille ei ole yleensä asetettu erityisiä muotovaatimuksia. Laissa tai muussa

normissa voidaan kuitenkin erikseen säätää erilaisista muotovaatimuksista. Yksityisoikeudellisten sopimusten osalta lainsäädännössä yleisimmin käytettyjä muotovaatimuksia ovat lähinnä sopimuksen tekeminen kirjallisesti ja sopimuksen allekirjoittaminen. Ilmauksia ”kirjallisesti” tai ”allekirjoittaa” ei ole määritelty tarkemmin lainsäädännössä.

Tällä säännöksellä varmistetaan, että ainakin laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla luotu kehittynyt sähköinen allekirjoitus samaistetaan perinteiseen, käsintehtyyn allekirjoitukseen. Säännös ei vaikuta muiden sähköisten allekirjoitusten pätevyYTEEN. Millainen tahansa sähköinen allekirjoitus voidaan luonnollisesti myös riittauttaa vastaavasti kuin perinteinen käsintehtykin allekirjoitus.

Sähköisen allekirjoituksen käyttäminen edellyttää luonnollisesti, että oikeustoimen tekeminen sähköisesti on sallittua ja mahdollista. Se, että tietynlaisen sähköisen allekirjoituksen ja perinteisen allekirjoituksen oikeusvaikutukset tämän lakiesityksen mukaisesti samaistetaan täysin toisiinsa, ei vaikuta esimerkiksi siihen, milloin oikeustoimi edellytetään tehtäväksi paperilla.

Pykälällä pantaisiin täytäntöön 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:

- 1) allekirjoitus on sähköisessä muodossa;
- 2) se ei perustu laatuvarmenteeseen; tai
- 3) sitä ei ole tehty turvallisen allekirjoituksen luomisvälineen avulla.

On selvää, että suomalaisessa tuomioistuimessa sähköisen allekirjoituksen oikeusvaikutusta ei evättäisi, taikka jätettäisi hyväksymättä todisteena yksinomaan direktiivin 5 artiklan 2 kohdan mainitsemien seikkojen perusteella. Suomalaisissa tuomioistuimissa sovellettavan vapaan todisteiden harkinnan vuoksi, tulee direktiivin kyseisen säännöksen tavoite saavutetuksi Suomessa ilman kansallista sääntelyä.

19 §. *Henkilötietojen käsittely.* Direktiivin 8 artiklan 2 kohdan täytäntöönpano edellyttää varmenteiden tarjonnassa hankittavia henkilötietoja koskevan erityissäännöksen säätämistä. Pykälän 1 momentin mukaan

varmentaja saisi kerätä varmenteen myöntämisessä ja ylläpidossa välttämättömiä henkilötietoja ainoastaan allekirjoittajalta itseltään. Kerättävien tietojen tulisi olla välttämättömiä varmenteen myöntämisessä ja ylläpidossa. Henkilötietojen kerääminen olisi siten rajattu niiden käyttötarkoituksen perusteella. Momentissa tarkoitettua henkilötietojen keräämistä liittyy muun muassa henkilön tunnistamiseen varmennetta myönnettäessä ja varmenteen turvalliseen peruuttamiseen, johon voi liittyä allekirjoittajan henkilötietoihin liittyviä tarkistusmenettelyitä. Laatuvarmenteita yleisölle tarjoavan varmentajan osalta viitattaisiin lisäksi 2 luvun säädöksiin laatuvarmenteen myöntämisestä, ylläpidettävistä rekistereistä ja tietojen säilyttämisestä.

Pykälän 2 momentissa käsiteltäisiin henkilötunnuksen käyttöä varmentajan myöntäessä varmennetta. Varmentaja saisi vaatia varmenteen hakijalta henkilötunnuksen ilmoittamista henkilöllisyyden tarkistamiseksi. Henkilötunnusta ei kuitenkaan saisi sisällyttää varmenteeseen.

Pykälän 3 momentin mukaan tietojen keräämiseen muualta kuin allekirjoittajalta itseltään sekä tietojen käsittelyyn muussa kuin 1 momentissa tarkoitettuun tarkoitukseen tarvittaisiin allekirjoittajan nimenomainen suostumus. Nimenomainen suostumus olisi yleensä annettava kirjallisesti ja siitä tulisi ilmetä minkälaiseen henkilötietojen käsittelyyn lupa on annettu.

Säännöstä sovellettaisiin myös sellaisiin varmentajiin, jotka tarjoavat yleisölle sähköisiin allekirjoituksiin liittyviä muita varmenteita kuin tässä laissa tarkoitettuja laatuvarmenteita. Koska varmennemarkkinat ovat vielä varsin kehittymättömät ja varmenteiden käyttöala tarkemmin määrittymättä, ei ole tarpeenmukaista säädellä tarkemmin varmenteiden myöntämisessä ja ylläpidossa käytettävien henkilötietojen sisällöstä ja käsittelystä, muiden kuin laatuvarmenteita tarjoavien varmentajien osalta.

Henkilötietojen käsittelystä säädetään henkilötietolaissa (523/1999), joka on henkilötietojen käsittelyä koskeva yleislaki. Lakia sovellettaisiin myös varmentajien toimintaan. Ehdotetun pykälän 4 momentissa olisi selvyden vuoksi nimenomainen viittaus henkilötietolakiin.

Lain 19 ja 20 §:llä pantaisiin täytäntöön direktiivin 8 artiklan 1 ja 2 kohta.

20 §. *Väestötietojärjestelmän käyttäminen.* Ehdotetun säännöksen mukaan varmentaja saisi oikeuden hankkia ja tarkistaa varmenteen hakijan henkilötiedot väestötietojärjestelmästä. Tiedot voitaisiin kuitenkin saada vain varmenteen hakijan nimenomaisella suostumuksella.

Selkeyden vuoksi ehdotetaan 2 momentissa säädettäväksi, että varmentajalle henkilön tunnistamisessa tarvittavat tiedot on luovutettava väestötietojärjestelmästä julkisoikeudellisenä suoritteena valtion maksuperustelaimen mukaisesti. Käytännössä se merkitsisi omakustannushintaa. Koska väestötietojärjestelmää ylläpitävä Väestörekisterikeskus toimii itsekin varmentajana, säännöksellä pyritään varmistamaan eri varmentajille tasapuolinen kilpailutilanne.

Säännöstä sovellettaisiin myös sellaisiin varmentajiin, jotka tarjoavat yleisölle sähköisiin allekirjoituksiin liittyviä muita varmenteita kuin tässä laissa tarkoitettuja laatuvarmenteita.

21 §. *Varmenteen voimassaolon tarkistaminen.* Varmentajalla tulisi olla oikeus tallettaa tieto varmenteen voimassaolon tarkistamisesta. Tietoa voitaisiin 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 tulisi 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 voitaisiin luovuttaa ainakin allekirjoittajalle ja sulkulistan tarkastaneelle. Varmentajan lisäksi tiedon tallettamisesta hyötyisivät 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 varmenten tarjoajalla on tieto laskutuksen asianmukaiseksi hoitamiseksi.

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

Ehdotettua pykälää vastaavaa säännöstä ei sisälly sähköallekirjoitusdirektiiviin. Pykälän säännöksillä on tarpeen kansallisella tasolla täsmentää varmenteen voimassaolon tarkistamista koskevien tietojen käsittelyä.

4 luku. Yleinen ohjaus ja valvonta

22 §. *Yleinen ohjaus ja valvonta.* Varmennetoiminnan yleinen ohjaus ja kehittäminen kuuluisi liikenne- ja viestintäministeriölle. Tämä tarkoittaisi lähinnä varmennemarkkinoiden kehittymisen myötä mahdollisesti esiin tulevien tarpeellisten säädöshankkeiden valmistelua ja varmennetoimintaan liittyvien Euroopan yhteisöjen elimien toimintaan osallistumista.

Viestintäviraston tehtävä olisi 2 momentin mukaan valvoa ehdotetun lain noudattamista. Viestintävirasto antaisi tarvittaessa teknisiä määräyksiä ja suosituksia laatuvarmenteita yleisölle tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista. Määräyksiin ja suosituksiin liittyisi ainoastaan vähäistä harkintavallan käyttöä ja niillä tarkennettaisiin tarvittaessa laatuvarmenteen ja laatuvarmentajien toiminnalta 7 §:ssä ja 10-15 §:ssä säädettyjen vaatimusten sisältöä. Viestintäviraston määräykset ja suositukset sisältäisivät ainoastaan teknisiä ja merkitykseltään vähäisiä yksityiskohtia. Mahdollisuus antaa tarkempia määräyksiä ja suosituksia on tarpeen tämänhetkisen varmennetoiminnan kehittymättömyyden ja keskeneräisen standardointitoiminnan vuoksi.

Pykälän 3 momentin mukaan tietosuojavaltuutettu valvoisi ehdotetussa laissa annettujen henkilötietojen käsittelyä koskevien säännösten noudattamista. Tehtävänsä suorittaessaan tietosuojavaltuutetulla olisi henkilötietolaissa tarkoitettujen tiedonsaanti- ja tarkastusoikeudet. Muutoksenhausta tietosuojavaltuute-

tun toiminnan osalta säädetään henkilötietolaissa. 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. 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. 28 §:llä pantaisiin täytäntöön direktiivin 3 artiklan 3 kohta.

23 §. *Tiedonsaantioikeus.* Viestintävirastolla olisi oikeus saada sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavilta varmentajilta ja heidän apunaan toimivilta henkilöiltä tietoja salassapitosäännösten estämättä. Henkilöillä tarkoitettaisiin sekä luonnollisia henkilöitä että oikeushenkilöitä. Tiedonsaantioikeus koskisi 22 §:ssä säädettyjen valvontatehtävien suorittamiseksi tarpeellisia tietoja.

24 §. *Tarkastusoikeus.* Viestintäviraston tehtävään määräämällä tarkastajalla olisi oikeus suorittaa tarkastus, jos se olisi tarpeen ehdotetun lain ja sen nojalla annettujen määräysten noudattamisen valvomiseksi. Määräyksillä tarkoitettaisiin Viestintäviraston tämän lain nojalla antamia määräyksiä. Tarkastusta toimittavalla tarkastajalla olisi oikeus tutkia sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavan varmentajan tai tämän apunaan käyttämän henkilön laitteet ja ohjelmistot, joilla voisi olla merkitystä lain ja sen nojalla annettujen määräysten noudattamisen valvonnassa.

Sähköisiin allekirjoituksiin liittyviä laatu-

varmenteita tarjoavan varmentajan tai tämän apunaan käyttämän henkilön olisi päästettävä Viestintäviraston tarkastaja hallinnassaan oleviin valmistus-, liike- ja varastotiloihin. Kyseinen velvollisuus ei koskisi kotirauhan piiriin kuuluvia tiloja.

Viestintävirasto voisi saada virka-apua poliisilta tarkastuksen suorittamista varten. Varmentajan apunaan käyttämällä henkilöllä tarkoitettaisiin tässä pykälässä sekä luonnollista henkilöä että oikeushenkilöä.

25 §. *Vaitiolovelvollisuus.* Eduskunta on edellyttänyt vastauksessaan hallituksen esitykseen laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi (EV 303/1998 vp, HE 30/1998 vp) muun ohella, että tulevaisuudessa suhtaudutaan pidättyvästi viranomaisten tietojen salassapitoa koskevien säännösten sijoittamiseen erityislainsäädäntöön. Koska erityislakeihin sisällytettävät vaitiolosäännökset merkitsisivät poikkeamista tästä tavoitteesta, lakiin ei sisällytetä omaa säännöstä vaitiolovelvollisuudesta vaan viitataan tältä osin lakiin viranomaisten toiminnan julkisuudesta. Kyseisen lain 23 §:n mukaan viranomaisen palveluksessa oleva samoin kuin luottamustehtävää hoitava ei saa paljastaa tietoon tullutta salassa pidettävää tietoa tai muuta tietoa, josta on lailla säädetty vaitiolovelvollisuus. Vaitiolovelvollisuus koskee myös tehtävien päättymisen jälkeistä aikaa. Kyseisiä tietoja ei saa käyttää omaksi taikka toisen hyödyksi tai toisen vahingoksi.

5 luku. Erinäiset säännökset

26 §. *Rangaistussäännös.* Varmentamistoiminnan luotettavuuden kannalta keskeistä on henkilötietojen käsittely varmentajan palvelujen tarjonnassa. Varmentajilta edellytetään luotettavaa henkilötietojen käsittelyä. Tarvittavien henkilötietojen todentamisesta laatuvarmennetta myönnettäessä säädettäisiin esityksen 12 §:ssä. Lakiehdotuksen 14 §:ssä säädettäisiin laatuvarmenteita yleisölle tarjoavien varmentajien velvollisuuksista ylläpitää varmennerekisteriä ja sulkulistaa sekä 15 §:ssä talletettujen tietojen säilyttämisestä. Henkilötietojen käsittelystä säädettäisiin kaikkia varmentajia koskien esityksen 19 §:ssä. Varmentajan tehtäviin onkin luonteesta liitettävissä rikosoikeudellinen vastuu.

Ehdotetussa 26 §:ssä viitattaisiin henkilörekisteririkoksesta ja -rikkomuksesta säädettyyn. Koska varmennerekisterikin on henkilörekisteri, säännös olisi vain informatiivinen viittaus.

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

Viestintäviraston valvontavalta kohdistuu laatuvarmenteiden tarjontaan sekä mahdollisesti myöhemmin nimettävien tarkastuslaitosten toimintaan. Toiminnan keskeyttämishuaka voisi koskea lain soveltamisalaa kuuluvan toiminnan osaa tai koko toimintaa. Tehosteeksi asetetun uhkan tulisi aina olla suhteessa valvottavan tahon virheen tai laiminlyönnin vakavuuteen. Uhkasakon tai teettämisen tulisi olla ensisijainen tehokeino velvoitteiden täyttämiseksi. Toiminnan keskeyttämishuakaa tulisi pääsääntöisesti käyttää vain tilanteissa, jossa valvottava taho ei ole korjannut virhettään tai laiminlyöntiään uhkasakosta tai teettämishuakasta huolimatta.

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

28 §. *Muutoksenhaku.* Lain nojalla annettusta Viestintäviraston päätöksestä valitettaisiin noudattaen, mitä hallintolainkäyttölaissa (586/1996) säädetään. Hallintolainkäyttölain 8 §:n 2 momentin mukaan valitus tehdään hallinto-oikeuteen.

Viestintävirasto voisi määrätä, että sen antamaa päätöstä on noudatettava jo ennen kuin päätös on lainvoimainen. Valitusviranomaisen voisi kuitenkin kieltää päätöksen täytäntöönpanon, kunnes valitus on ratkaistu.

29 §. *Voimaantulo.* Lakiehdotuksen 29 §:ään on otettu tavanomainen voimaantulosäännös.

30 §. *Siirtymäsäännös.* Ehdotettuun lakiin olisi tarpeen ottaa siirtymäsäännös. Säännöksen mukaan sellaisten varmentajien, jotka

lain voimaan tullessa ovat jo aloittaneet laatuvarmenteiden tarjonnan yleisölle, tulisi tehdä 9 §:ssä tarkoitettu ilmoitus kolmen kuukauden kuluessa lain voimaantulosta.

1.2. Laki viestintähallinnosta

2 §. Viestintähallinnosta annetussa laissa (625/2001) säädetään Viestintäviraston tehtävistä. Lain 2 §:ssä on lueteltu eri lakien perusteella Viestintävirastolle kuuluvat tehtävät. Pykälän 1 kohdan luetteloon ehdotetaan lisättäväksi laki sähköisistä allekirjoituksista.

2. Tarkemmat säännökset ja määräykset

Tarkempien määräysten antamistarve saattaa syntyä varmennetoiminnan ja siihen liittyvän teknologian nopean kehityksen vuoksi. Mahdollisuus antaa tarkempia määräyksiä on tarpeen erityisesti tämänhetkisen varmennetoiminnan kehittymättömyyden ja keskenäisen standardointitoiminnan vuoksi. Koska sähköisten allekirjoitusten käytön ja niihin liittyvien varmenteiden tarjonnan kehitystä on vaikeaa arvioida, laissa ei ole voitu ottaa kaikkia mahdollisia esiin tulevia ongelmia huomioon. Tämän vuoksi on tarpeen, että sähköisiin allekirjoituksiin ja varmenteiden tarjontaan liittyviä toimintoja olisi mahdollisuus ohjata myös Viestintäviraston määräyksillä ja suosituksilla.

Viestintävirasto voisi antaa tarpeellisia määräyksiä tai suosituksia 9 §:n nojalla ilmoitettavien tietojen toimittamisesta ja niiden tarkemmasta sisällöstä. Viestintäviraston määräyksillä voitaisiin myöhemmin täsmentää laissa määriteltyjen edellytysten toteamiseksi ja valvontatehtävän suorittamiseksi tarvittavia tietoja.

Viestintäviraston tehtävänä olisi 22 §:n 2 momentin mukaan valvoa ehdotetun lain noudattamista. Viestintävirasto antaisi tarvittaessa teknisiä määräyksiä ja suosituksia laatuvarmenteita yleisölle tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvasuosuista. Viestintäviraston 22 §:n nojalla antamalla teknisillä määräyksillä ja suosituksilla tarkoitettaisiin laatuvarmentelta ja laatuvarmentajien toiminnalta 7 ja 10-15 §:ssä säädettyjen vaatimusten sisältöä selven-

täviä määräyksiä ja suosituksia, jotka sisältäisivät ainoastaan teknisiä ja merkitykseltään vähäisiä yksityiskohtia.

Määräyksillä ei luotaisi laatuvarmenteiden tarjoajille uusia velvollisuuksia ja niiden antamiseen liittyisi ainoastaan vähäistä harkittavallan käyttöä. Mikäli varmennemarkkinoiden tai varmenteisiin liittyvän tekniikan kehitys edellyttää kokonaan uusista varmenteen vaatimuksista tai varmentajan velvollisuuksista säättämistä, se tapahtuisi lain tasolla.

3. Voimaantulo

Lait ehdotetaan tuleviksi voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytty ja vahvistettu. Lakien täytäntöönpanon edellyttämiin toimiin voitaisiin kuitenkin ryhtyä jo ennen kuin ne tulevat voimaan.

4. Säättämjärjestys

Hallituksen esityksessä laiksi sähköisestä asioinnista hallinnossa (HE 153/1999 vp) katsottiin, että varmentajan, yksityisen tai julkisen, toiminta tulee rinnastaa välillisen julkisen hallinnon toimintaan. Perusteeksi tälle kannalle esitettiin, että varmenteen myöntäminen koskee hakijan etua hallitusmuodon 16 §:ssä tarkoitettulla tavalla. Hallintovaliokunnan mietinnössä (HaVM 10/1999 vp) hyväksyttiin hallituksen esityksessä esitetty näkemys varmentamistoiminnan julkisoikeudellisesta luonteesta, vaikka asiantuntijakuulemisessa esitettiin myös päinvastaisia kantoja.

Lakiesityksen perusteluissa todettiin myös, että sähköallekirjoitusdirektiivin täytäntöönpanon yhteydessä voidaan hallinnossa käytettävien varmennepalvelujen asiakkaiden oikeussuojajärjestelyt arvioida uudelleen. Tämä on erityisesti tarpeen varmentajan toiminnassa noudatettavan menettelyn osalta, mistä säädettiin erityisesti mainitun lain 7 §:n 1 momentissa. Kyseisessä momentissa todetaan, että varmenteen myöntämisessä ja ylläpitämisessä samoin kuin niihin liittyvien rekisterien käyttämisessä noudatetaan hallintomenettelylakia, kielilakia, saamen kielen käyttämisestä viranomaisissa annettua lakia (516/1991), viranomaisten toiminnan julki-

suudesta annettua lakia, henkilötietolakia ja arkistolakia.

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. Perustuslain säätämiseen johtaneessa hallituksen esityksessä (HE 1/1998 vp) todetaan, että tarkoituksenmukaisuusvaatimus voi täytyä ”palveluiden tuottamiseen liittyvien tehtävien kohdalla helpommin” kuin esimerkiksi yksilön tai yhteisön keskeisiä oikeuksia koskevan päätöksen teon kohdalla. Edelleen perusteluissa todetaan, että säännös korostaa julkisia hallintotehtäviä hoitavien henkilöiden koulutuksen ja asiantuntemuksen merkitystä sekä sitä, että näiden henkilöiden julkisen valvonnan on oltava asianmukaista.

Nyt annettavan lakiesityksen voidaan katsoa täyttävän yksityisten laatuvarmenteiden tarjoajien toiminnan sääntelyn osalta perustuslain 124 §:n vaatimukset. Tämän johdosta lakiesityksen mukaiset sähköisten allekirjoitusten käyttöön liittyvät laatuvarmenteet voitaisiin hyväksyä myös hallinnon sähköisissä palveluissa asioitaessa. Tämä olisi ensiarvoisen tärkeää sähköisten palvelujen kehittymisen kannalta. Saman laatuvarmenteen ja sen avulla luodun sähköisen allekirjoituksen käytön mahdollistaminen esityksen mukaisesti niin yksityisellä kuin julkisellakin sektorilla olisi myös keskeinen tekijä sähköisten palveluiden helpon käytettävyyden kannalta.

Nyt annettavassa hallituksen esityksessä määriteltäisiin korkeat laatuvaatimukset täytävä laatuvarmenne ja säädeltäisiin laatuvarmenteita yleisölle tarjoavien varmentajien vastuista ja velvollisuuksista sekä laatuvarmenteiden tarjonnan viranomaisvalvonnasta. Lakiehdotuksessa laatuvarmenteiden tarjontaa pidetään ensisijaisesti yksityisoikeudellisena kaupallisena toimintana, jota viranomaiset valvovat. Sähköisissä allekirjoituksissa käytettäviä laatuvarmenteita tarjoavien varmentajien asiakkaiden oikeussuoja tulisi tämän esityksen mukaisin säädöksin siinä määrin tehokkaasti järjestettyä, että varmentamis-

toimintaa ja varmenteita koskevat säännökset voitaisiin kumota sähköistä asiointia koskevasta laista.

Joissakin lakiesityksestä annetuissa lausunnoissa on kiinnitetty huomiota siihen, että esityksessä ei turvataisi riittävästi Suomen kansalaisten kielellisiä oikeuksia. Lisäksi on esitetty arvioita siitä, että luotettavan tunnistamisen takaamiseksi laatuvarmenteen hakijan tunnistamisessa tulisi käyttää ainoastaan poliisin myöntämää asiakirjaa.

Esityksen 12 §:ssä säädettäisiin laatuvarmenteita yleisölle tarjoavien varmentajien velvollisuudesta huolellisesti ja luotettavalla tavalla varmistaa laatuvarmenteen hakijan henkilöllisyys. Laatuvarmenteita yleisölle tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti. Lisäksi laatuvarmenteita yleisölle tarjoavalle varmentajalle asetettaisiin 16 §:ssä säädetyissä tapauksissa ankara vahingonkorvausvastuu laatuvarmenteeseen luottavalle taholle aiheutuneista vahingoista. Esityksen 12 §:ssä säädettäisiin lisäksi laatuvarmenteita yleisölle tarjoavan varmentajan velvollisuudesta ennen sopimuksen tekemistä antaa laatuvarmenteen hakijalle kirjallisesti tiedot laatuvarmenteen käyttöehdoista mukaan lukien mahdolliset käyttörajoitukset, vapaaehtoisista akkreditointijärjestelmistä, varmennetoiminnan viranomaisvalvonnasta sekä valitus- ja riitojenratkaisumenettelyistä. Mainitut tiedot tulee 12 §:n mukaan antaa laatuvarmenteen hakijalle kirjallisesti sellaisessa muodossa, että hakija voi ne vaivatta ymmärtää. Tämän vaatimuksen voitaisiin katsoa Suomen kansalaista palveltaessa lähtökohtaisesti tarkoittavan palvelujen tarjoamista ainakin Suomessa käytettävillä virallisilla kielillä. Näin ollen sekä laatuvarmenteen hakijan kielelliset oikeudet että luotettava tunnistaminen tulisivat asianmukaisesti huomioitua esityksessä.

Varmentamistoiminnan keskeinen tavoite on luotettavan sähköisen asioinnin takaaminen niin kaupallisissa kuin hallinnonkin palveluissa. Myöntämällä laatuvarmenteen varmenteiden tarjoaja antaa varmenteen hakijalle välineet sähköisten palvelujen käyttämiseksi luotettavalla tavalla. Laatuvarmentajille tässä lakiesityksessä asetettujen vaatimusten lisäksi tulisi pyrkiä välttämään tarpeettoman raskaiden velvoitteiden säätämistä varmen-

tamistoiminnalle. Varmenteiden käytön edistämiseksi ja sähköisten palveluiden kehittämiseksi varmentamistoiminnalle ei ole syytä asettaa sellaisia oikeudellisia velvoitteita, joita voidaan pitää jopa kaupan esteinä. Yksityinen asiointi ja asiointi viranomaisten kanssa ei teknisesti tarkasteltuna edellytä erilaisia vaatimuksia eikä säännöksiä. Varmentamistoiminnan asianmukaisuutta valvottaisiin sekä Viestintäviraston että tietosuojavaltuutetun toimesta, joten erityiset menettelylliset oikeusturvatakeet eivät voine enää olla niin keskeisessä asemassa kuin sähköistä asiointia hallinnossa koskevaa lakia säädettäessä.

Tällä lailla täytäntöön pantavan sähköal-leirjoitusdirektiivin 3 artiklan 7 kohdassa säädetään, että jäsenvaltiot voivat asettaa mahdollisia lisävaatimuksia sähköisten allekirjoitusten käytölle julkisella sektorilla. Tällaisten vaatimusten edellytetään kuitenkin olevan objektiivisia, avoimia, suhteellisia ja syrjimättömiä, ja ne saavat liittyä vain kyseessä olevan sovelluksen erityispiirteisiin. Kyseiset lisävaatimukset eivät saa myöskään estää kansalaisille tarjottavia rajat ylittäviä palveluja. Mikäli hallinnon tiettyjen sähköisten palvelujen sovelluksissa ilmenee sellaisia erityispiirteitä, joista tulee säätää tästä lakiesityksestä poiketen, tulisi tällaiset säädökset sisällyttää kyseistä hallinnonala koskevaan erityislainsäädäntöön. Esimerkkeinä mainittakoon sähköinen asiointi sosiaali- ja terveyspalveluissa sekä puolustushallinnon palve-

luissa, joiden kehittämisen yhteydessä tulee miettiä erikseen sähköisten allekirjoitusten ja niihin liittyvien varmenteiden käytön soveltuvuus sekä mahdollisten lisävaatimusten tarve kyseisten alojen erityispiirteet ja lainsäädäntö huomioiden.

Toisaalta hallinnon sähköisen asioinnin piiriin kuuluu huomattava määrä sellaista asiointia, missä ei tarvita lainkaan varmenteita tai niiden avulla tehtyjä sähköisiä allekirjoituksia. Sähköpostin, faxin ja puhelimen välityksellä kuten myös muilla mahdollisilla tavoilla on edelleenkin voitava asioida hallinnossa silloin kun erityisiä tietoturvasuuteen liittyviä vaatimuksia ei asiointiprosessissa tarvitse ottaa huomioon.

Hallitus katsoo, että lakiehdotukset voidaan säätää tavallisessa lainsäätämisyjärjestyksessä. Esityksessä säädettäisiin uusista välineistä, joilla voitaisiin asioida sähköisesti hallinnossa. Edellä esitettyjen varmentamistoiminnan julkisoikeudellista luonnetta, yksilön asemaa varmenteiden myöntämisessä ja elinkeinovaipautta koskevien perustuslakiliityntöjen vuoksi hallitus pitää kuitenkin toivottavana, että eduskunnan perustuslakivaliokunnalle annettaisiin mahdollisuus antaa lausuntonsa esityksestä.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäväksi seuraavat lakiehdotukset:

1.

Laki**sähköisistä allekirjoituksista**

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Lain tarkoitus

Tämän lain tarkoituksena on edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *sähköisellä allekirjoituksella* sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä;

2) *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;

3) *allekirjoittajalla* luonnollista henkilöä, jolla on laillisesti hallussaan allekirjoituksen luomistiedot ja joka toimii itsensä tai edustamansa luonnollisen henkilön tai oikeushenkilön puolesta;

4) *allekirjoituksen luomistiedoilla* allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämää ainutkertaista tietokokonaisuutta, kuten koodeja ja yksityisiä avaimia;

5) *allekirjoituksen luomisvälineellä* ohjelmistoja ja laitteita, joilla yhdessä allekirjoituksen luomistietojen kanssa luodaan sähköinen allekirjoitus;

6) *allekirjoituksen todentamistiedoilla* sähköisen allekirjoituksen todentamisessa käytettävää tietokokonaisuutta, kuten koodeja ja julkisia avaimia;

7) *varmenteella* sähköistä todistusta, joka liittyy allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan henkilöllisyyden;

8) *varmentajalla* luonnollista henkilöä tai oikeushenkilöä, joka tarjoaa varmenteita;

9) *sähköisiin allekirjoituksiin liittyvällä tuotteella* laitteistoa tai ohjelmistoa tai niiden merkityksellistä osaa, jotka on tarkoitettu palveluntarjoajan käyttöön tämän tarjotessa sähköisiin allekirjoituksiin liittyviä palveluja tai käytettäväksi sähköisten allekirjoitusten luomiseen tai todentamiseen; sekä

10) *sähköisiin allekirjoituksiin liittyvällä palvelulla* varmenteiden sekä muiden sähköisiin allekirjoituksiin liittyvien tuotteiden tai palveluiden tarjontaa.

3 §

Soveltamisala

Tätä lakia sovelletaan sähköisiin allekirjoituksiin sekä palveluntarjoajiin, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä tuotteita tai palveluita yleisölle.

Sähköisten allekirjoitusten käytöstä hallinnossa on lisäksi voimassa mitä siitä erikseen säädetään.

4 §

Palvelujen ja tuotteiden vapaa liikkuvuus

Tämän lain mukaiset sähköisiin allekirjoituksiin liittyvät tuotteet ja palvelut saavat liikkua vapaasti sisämarkkinoilla.

5 §

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 säädetty vaatimukset, jos:

- 1) se on Euroopan yhteisöjen komission vahvistamien ja Euroopan yhteisöjen virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukainen; tai
- 2) vaatimusten arviointitehtävään nimetty tarkastuslaitos, joka sijaitsee Suomessa tai muussa Euroopan talousalueeseen kuuluvassa

sa valtiossa, on turvallisen allekirjoituksen luomisvälineen hyväksynyt.

6 §

Tarkastuslaitos

Viestintävirasto voi nimetä tarkastuslaitoksia, joiden tehtävänä on arvioida, täyttääkö allekirjoituksen luomisväline 5 §:n 1 momentissa säädetty 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 ammattitaitoisia 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.

2 luku

Laatuvarmenteiden tarjoaminen

7 §

Laatuvarmenne

Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää 2 momentissa säädetty vaatimukset ja jonka on myöntänyt 10-15 §:ssä säädetty vaatimukset täyttävä varmentaja.

Laatuvarmenteen tulee sisältää seuraavat tiedot:

- 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 käyttörajaukset; sekä
- 9) allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.

8 §

Muun kuin Suomeen sijoittautuneen varmentajan tarjoama laatuvarmenne

Muun kuin Suomeen sijoittautuneen varmentajan laatuvarmenteena tarjoaman varmenteen katsotaan täyttävän 7 §:ssä säädetty 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, täytäntöön panemiseksi säädetty kansalliset vaatimukset; tai

3) varmenteen takaa sellainen varmentaja, joka on sijoittautunut Euroopan talousalueeseen kuuluvaan valtioon ja täyttää kyseisessä valtiossa sähköallekirjoitusdirektiivin täytäntöön panemiseksi säädetty 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.

9 §

Ilmoitus toiminnan aloittamisesta

Varmentajan, jonka tarkoituksena on tarjota laatuvarmenteita yleisölle, on ennen toiminnan aloittamista tehtävä kirjallinen ilmoitus Viestintävirastolle. Ilmoituksen tulee sisältää varmentajan nimi ja yhteystiedot sekä tiedot, joiden perusteella 7 §:ssä ja 10-15 §:ssä säädettyjen vaatimusten täytyminen voidaan varmistaa. Viestintävirasto voi antaa valvontatoiminnan kannalta tarpeellisia määräyksiä ja suosituksia ilmoitettavien tietojen tarkemmasta sisällöstä ja niiden toimittamisesta Viestintävirastolle.

Viestintäviraston on viipymättä ilmoituksen saatuaan kiellettävä varmentajaa tarjoamasta varmenteitaan laatuvarmenteina, jos varmenne ei täytä 7 §:n 2 momentin vaatimuksia tai varmentaja ei täytä 10-15 §:ssä säädettyjä vaatimuksia.

Jos 1 momentissa tarkoitettut tiedot ovat muuttuneet, varmentajan on viipymättä ilmoitettava muutoksista kirjallisesti Viestintävirastolle.

Viestintävirasto pitää laatuvarmenteita myöntävistä varmentajista julkista rekisteriä.

10 §

Laatuvarmenteita yleisölle tarjoavan varmentajan yleiset velvollisuudet

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, on toimittava huolellisesti, luotettavasti ja asianmukaisesti. Varmentajalla on ol-

tava 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 riittävästä 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 se itse tuottaa tiedot.

Varmentaja ei saa tallentaa tai jäljentää allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

11 §

Luotettavat laitteet ja ohjelmistot

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, 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 yhteisöjen virallisessa lehdessä julkaistujen yleisesti tunnustettujen standardien mukainen.

12 §

Laatuvarmenteen myöntäminen

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, tulee huolellisesti ja luotettavalla tavalla tarkistaa laatuvarmenteen hakijan henkilöllisyys ja muut laatuvarmenteen myöntämisessä ja ylläpidossa tarpeelliset hakijan henkilöön liittyvät tiedot. Laatuvarmen-

teita yleisölle tarjoavan varmentajan on tunnistettava hakija henkilökohtaisesti.

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, tulee ennen sopimuksen tekemistä antaa laatuvarmenteen hakijalle tiedot laatuvarmenteen käyttöehdoista mukaan lukien mahdolliset käyttörajoitukset, vapaaehtoisista akkreditointijärjestelmistä, varmennetoiminnan viranomaisvalvonnasta sekä valitus- ja riitojenratkaisumenettelyistä. Tiedot tulee antaa laatuvarmenteen hakijalle kirjallisesti sellaisessa muodossa, että hakija voi ne vaitta ymmärtää.

13 §

Laatuvarmenteen peruuttaminen

Allekirjoittajan on viipymättä pyydettävä laatuvarmenteen myöntäneeltä varmentajalta laatuvarmenteen peruuttamista, jos hänellä on perusteltu syy epäillä allekirjoituksen luomistietojen oikeudetonta käyttöä.

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, 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.

14 §

Laatuvarmenteita yleisölle tarjoavan varmentajan ylläpitämät rekisterit

Laatuvarmenteita yleisölle tarjoavan varmentajan tulee ylläpitää rekisteriä myöntämistään laatuvarmenteista (varmennerekisteri). Rekisteriin tulee merkitä:

- 1) 7 §:n 2 momentissa määritelty laatuvarmenteen tietosisältö;
- 2) 12 §:n 1 momentissa tarkoitetut hakijan henkilöön liittyvät tiedot, mukaan lukien tieto laatuvarmennetta myönnettäessä käytettyä hakijan tunnistamismenettelyistä; sekä

3) 21 §:ssä tarkoitetut tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta, jos laatuvarmenteita yleisölle tarjoava varmentaja käyttää 21 §:n mukaista tallennusoikeutta.

Laatuvarmenteita yleisölle tarjoavan varmentajan tulee varmistaa, että laatuvarmenteella varmennettuun kehittyneeseen sähköiseen allekirjoitukseen luottavalla osapuolella on saatavilla 7 §:n 2 momentissa määritelty varmenteen tietosisältö.

Varmentajan tulee myös ylläpitää peruutetuista laatuvarmenteista julkista rekisteriä (sulkulista). Sulkulistalle on asianmukaisesti ja viipymättä merkittävä tieto laatuvarmenteen peruuttamisesta sekä tarkka peruuttamisajankohta.

Edellä 2 ja 3 momentissa mainittujen tietojen on oltava ympärivuorokautisesti käytettävissä.

15 §

Varmennerekisterin tietojen säilyttäminen

Varmentajan, joka tarjoaa laatuvarmenteita yleisölle, tulee luotettavalla ja tarkoituksenmukaisella tavalla säilyttää varmennerekisterin tiedot 10 vuoden ajan varmenteen voimassaolon päättymisestä.

16 §

Laatuvarmenteita tarjoavan varmentajan vahingonkorvausvastuu

Yleisölle 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 7 §: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 13 §:ssä säädetyllä tavalla.

Varmentaja vapautuu 1 momentissa säädetyistä vastuusta, jos se näyttää, että vahinko ei ole aiheutunut sen omasta tai sen apunaan käyttämän henkilön huolimattomuudesta.

Edellä 1 momentissa tarkoitettu varmentaja ei vastaa vahingosta, joka aiheutuu laatuvarmenteeseen sisältyvän käyttörajoituksen vastaisesta käytöstä.

Laatuvarmenteita yleisölle tarjoavan varmentajan vahingonkorvausvastuusta on muutoin voimassa, mitä vahingonkorvauslaissa (412/1974) säädetään. Mitä tässä pykälässä säädetään, sovelletaan myös varmentajaan, joka takaa yleisölle varmenteen laatuvarmenteeksi.

17 §

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 13 §: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 13 §:n 1 momentissa säädetään.

Sopimusehto, joka poikkeaa 2 momentin säännöksistä kuluttajan vahingoksi, on mitätön.

3 luku

Sähköisen allekirjoituksen oikeusvaikutus ja henkilötietojen käsittely

18 §

Sähköisen allekirjoituksen oikeusvaikutus

Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä.

19 §

Henkilötietojen käsittely

Varmentaja, joka tarjoaa yleisölle varmenteita, saa kerätä varmenteen myöntämisessä ja ylläpidossa välttämättömiä henkilötietoja ainoastaan allekirjoittajalta itseltään. Laatuvarmenteita yleisölle tarjoavan varmentajan osalta säädetään laatuvarmenteen myöntämisestä, ylläpidettävistä rekistereistä ja tietojen säilyttämisestä tarkemmin 2 luvussa.

Varmentaja voi tarkistaessaan varmenteen hakijan henkilöllisyyden vaatia tämän ilmoittamaan henkilötunnuksensa. Allekirjoittajan henkilötunnusta ei saa sisällyttää varmenteeseen.

Henkilötietoja saa ainoastaan allekirjoittajan nimenomaisella suostumuksella:

- 1) kerätä muualta kuin allekirjoittajalta itseltään; tai
- 2) käsitellä muussa kuin 1 momentissa tarkoitettussa tarkoituksessa.

Henkilötietojen käsittelystä on lisäksi voimassa, mitä siitä henkilötietolaissa (523/1999) säädetään.

20 §

Väestötietojärjestelmän käyttäminen

Varmentajalla on oikeus varmenteen hakijan nimenomaisella suostumuksella hankkia ja tarkastaa hakijan ilmoittamat henkilötiedot väestötietojärjestelmästä.

Tiedot väestötietojärjestelmästä luovute-

taan julkisoikeudellisena suoritteena sen mukaan kuin valtion maksuperustelaissa (150/1992) säädetään.

21 §

Varmenteen voimassaolon tarkistaminen

Varmentaja saa tallettaa tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta. Talletettuja tietoja saa käyttää ainoastaan varmenteiden käytön laskutuksen suorittamiseksi tai varmenteella varmennetun sähköisen allekirjoituksen avulla tehtyjen oikeustoimien todentamiseksi.

4 luku

Yleinen ohjaus ja valvonta

22 §

Yleinen ohjaus ja valvonta

Varmennetoiminnan yleinen ohjaus ja kehittäminen kuuluu liikenne- ja viestintäministeriölle.

Viestintäviraston tehtävänä on valvoa tämän lain noudattamista. Viestintävirasto antaa tarvittaessa teknisiä määräyksiä ja suosituksia sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista.

Tietosuojavaltuutetun tehtävänä on valvoa tässä laissa annettujen henkilötietoja koskevien säännösten noudattamista. Tehtävänsä suorittaessaan tietosuojavaltuutetulla on henkilötietolaissa tarkoitettujen tiedonsaanti- ja tarkastusoikeudet. Muutoksenhausta tietosuojavaltuutetun toiminnan osalta säädetään henkilötietolaissa.

23 §

Tiedonsaantioikeus

Viestintävirastolla on oikeus salassapitosäännösten estämättä saada sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavilta varmentajilta ja heidän apunaan toimivilta henkilöiltä 22 §:ssä säädetty-

jen tehtävien suorittamiseksi tarpeelliset tiedot.

24 §

Tarkastusoikeus

Viestintäviraston tehtävään määrämällä tarkastajalla on oikeus tämän lain ja sen nojalla annettujen määräysten noudattamisen valvomiseksi toimittaa tarkastus. Tarkastusta toimittavalla henkilöllä on oikeus tutkia sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavan varmentajan tai tämän apunaan käyttämän henkilön laitteet ja ohjelmistot, joilla voi olla merkitystä tämän lain tai sen nojalla annettujen määräysten noudattamisen valvonnassa.

Sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle tarjoavan varmentajan tai tämän apunaan käyttämän henkilön on tarkastusta varten päästettävä 1 momentissa tarkoitettu tarkastaja valmistus-, liike- ja varastotiloihin.

Viestintävirastolla on oikeus saada virka-apua poliisilta 1 ja 2 momentissa tarkoitettun tarkastuksen suorittamiseksi.

25 §

Vaitiolovelvollisuus

Tämän lain mukaisia tehtäviä suorittavat ovat vaitiolovelvollisia siten kuin siitä säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999).

5 luku

Erinäiset säännökset

26 §

Rangaistussäännös

Rangaistus henkilökisteririkoksesta säädetään rikoslain (39/1889) 38 luvun 9 §:ssä

ja henkilökisteririkkomuksesta henkilötietolain 48 §:n 2 momentissa.

27 §

Hallintopakkeinoit

Jos joku rikkoo tätä lakia tai sen nojalla annettuja määräyksiä, Viestintävirasto voi velvoittaa hänet korjaamaan virheensä tai laiminlyöntinsä. Päätöksen tehosteeksi voidaan asettaa uhkasakko tai uhka, että toiminta keskeytetään osaksi tai kokonaan taikka ettei tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella. Uhkasakosta, keskeyttämisuhasta ja teettämisuhasta on voimassa mitä uhkasakkolaissa (1113/1990) säädetään.

Teettämällä suoritettun toimenpiteen kustannukset suoritetaan valtion varoista ja peritään laiminlyöjältä siinä järjestyksessä kuin verojen ja maksujen perimisestä ulosottotoimin annetussa laissa (367/1961) säädetään.

28 §

Muutoksenhaku

Viestintäviraston tämän lain nojalla tekemään päätökseen haetaan muutosta noudattaen, mitä hallintolainkäyttölaissa (586/1996) säädetään.

Viestintävirasto voi päätöksessään määrätä, että päätöstä on noudatettava ennen kuin se on saanut lainvoiman. Valitusviranomaisen voi kuitenkin kieltää päätöksen täytäntöönpanon, kunnes valitus on ratkaistu.

29 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Ennen tämän lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimiin.

30 §

Siirtymäsäännös

Varmentajan, joka on aloittanut laatuvar-

menteiden tarjonnan yleisölle ennen tämän lain voimaantuloa, tulee kolmen kuukauden kuluessa lain voimaantulosta tehdä 9 §:ssä tarkoitettu ilmoitus.

2.

Laki**viestintähallinnosta annetun lain 2 §:n muuttamisesta**

Eduskunnan päätöksen mukaisesti
muutetaan viestintähallinnosta 29 päivänä kesäkuuta 2001 annetun lain (625/2001) 2 § seuraavasti:

2 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on:

1) huolehtia telemarkkinalaissa (396/1997), radiolaissa (517/1988), postitoimintalaissa (907/1993), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radorahastosta annetussa laissa (745/1998), yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetussa laissa (565/1999) sekä sähköisistä alle-

kirjoituksista annetussa laissa (/) sille säädettyistä tehtävistä; sekä

2) hoitaa muut tehtävät, jotka sille muiden säännösten tai liikenne- ja viestintäministeriön määräysten mukaan kuuluvat.

Tämä laki tulee voimaan _____ päivänä kuuta 20 _____ .

Ennen tämän lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimiin.

Helsingissä 26 päivänä lokakuuta 2001

Tasavallan Presidentti

TARJA HALONEN

Liikenne- ja viestintäministeri *Olli-Pekka Heinonen*

*Liite
Rinnakkaistekstit*

2.

Laki

viestintähallinnosta annetun lain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan viestintähallinnosta 29 päivänä kesäkuuta 2001 annetun lain (625/2001) 2 § seuraavasti:

Voimassa oleva laki

2 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on:

1) huolehtia telemarkkina- (396/1997), radiolaissa (517/1988), posti- toimintalaissa (907/1993), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998) sekä yksityisyyden suojasta televiestinnässä ja teletoinnin tietoturvasta annetussa laissa (565/1999) sille säädetyistä tehtävistä; sekä

2) hoitaa muut tehtävät, jotka sille muiden säännösten tai liikenne- ja viestintäministeriön määräysten mukaan kuuluvat.

Ehdotus

2 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on:

1) huolehtia telemarkkina- (396/1997), radiolaissa (517/1988), posti- toimintalaissa (907/1993), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radiorahastosta annetussa laissa (745/1998), yksityisyyden suojasta televiestinnässä ja teletoinnin tietoturvasta annetussa laissa (565/1999) sekä sähköisistä allekirjoituksista annetussa laissa (/) sille säädetyistä tehtävistä; sekä

2) hoitaa muut tehtävät, jotka sille muiden säännösten tai liikenne- ja viestintäministeriön määräysten mukaan kuuluvat.

Tämä laki tulee voimaan päivänä kuuta 20 .