LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 53/2005
Viestintä

Laki sähköisistä allekirjoituksista 14/2003

Vaikutusten arviointi

Liikenne- ja viestintäministeriö
Helsinki, 2005

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä
28.6.2005

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Krogerus & Co. Oy	Selvitys
Lauri Railas, Jan Vidjeskog	Toimeksiantaja Liikenne- ja viestintäministeriö
	Toimielimen asettamispäivämäärä

Julkaisun nimi

Laki sähköisistä allekirjoituksista 14/2003. Vaikutusten arviointi

Tiivistelmä

Selvityksen tarkoituksena on arvioida sähköisistä allekirjoituksista annetun lain tavoitteiden toteutumista ja lain käytännön vaikutuksia. Selvitystä varten on kartoitettu keskeisten alan toimijoiden näkemyksiä lain toimivuudesta, esiin tulleista ongelmista, alan kehityssuunnista ja mahdollisista muutostarpeista. Selvitys käsittää sekä oikeudellisten kysymysten kartoituksen että tietoa käytössä olevista varmenteista ja muista allekirjoitustoteutuksista sekä sähköisen tunnistamisen menetelmistä.

Selvitystyössä havaittiin, että lain 18 §:ssä tarkoitetut, laatuvarmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset, jotka on luotu turvallisella allekirjoitusten luomisvälineellä, ovat vielä hyvin vähäisessä käytössä. Tämä johtuu paitsi tarvittavien lukijalaitteiden vaatimuksesta myös käytössä olevien palvelujen vähäisyydestä. Olennaista on myös se, että useimmat arkielämän toimenpiteet voidaan toteuttaa muotovapaasti ilman laatuvarmennetasoisella allekirjoituksella tehtyä tahdonilmaisua. Suomessa on edelleen vain yksi laatuvarmenteita myöntävä varmentaja, Väestörekisterikeskus. Teleoperaattorit ovat äskettäin ryhtyneet tarjoamaan matkapuhelimien avulla toimivaa mobiilivarmennetta, joka perustuu VRK:n laatuvarmenteeseen. Ulkomaisista varmenteista käytetään erityisesti palvelinvarmenteita, mutta laatuvarmenteiden kansainvälisiä markkinoita ei käytännössä vielä ole olemassa. Varmenteita käytetään yleisesti sähköiseen etätunnistamiseen ja palveluja, joissa varmenteita voi käyttää tunnistautumiseen, on lisääntyvässä määrin. Pankit ovat kuitenkin luoneet oman tunnistautumisstandardinsa (TUPAS2) ja pankkitunnisteita käytetään tällä hetkellä huomattavasti enemmän kuin varmenteita julkisissa ja yksityisissä sähköisissä palveluissa.

Selvityksessä katsotaan, että lakiin ei kohdistu välittömiä muutostarpeita, koska lakia ei infrastruktuurin kehittymättömyyden vuoksi juurikaan vielä sovelleta käytäntöön. Aika ei sen vuoksi ole vielä kypsä lain säännösten yksityiskohtaiseksi arvioimiseksi. Koska varmennetoiminta on kuitenkin kehittymässä, sääntelyä tulee tarkastella uudelleen muutaman vuoden sisällä, mieluiten myös yhteisötasolla.

Avainsanat (asiasanat)

sähköinen allekirjoitus, kehittynyt sähköinen allekirjoitus, digitaalinen allekirjoitus, varmentaja, varmenne, laatuvarmenne, mobiilivarmenne, sähköinen tunnistaminen, verkkopankkitunniste, sähköinen asiointitunnus

Muut tiedot

Yhteyshenkilö/LVM Juha Perttula
Raportti julkaistu vain verkkojulkaisuna.

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 53/2005	1795-4045 (verkkojulkaisu)	952-201-406-0 (verkkojulkaisu)

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
90	suomi		julkinen

Jakaja	Kustantaja
Liikenne- ja viestintäministeriö	Liikenne- ja viestintäministeriö

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum
28.6.2005

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Krogerus & Co. Oy	Rapport
Lauri Railas, Jan Vidjeskog	Uppdragsgivare Kommunikationsministeriet
	Datum för tillsättandet av organet

Publikation

Effekter av lagen om elektroniska signaturer 14/2003

Referat

Utredningen gjordes som konsultarbete på uppdrag av trafik- och kommunikationsministeriet och dess syfte var att värdera lagen av elektroniska signaturer, särskilt uppfyllelsen av lagens målsättningar och dess praktiska påverkan. I utredningen har man utrett branschens centrala aktörers åsikter om lagens funktion, om de problem som uppstått, om branschens utvecklingslinjer samt möjliga revisionsbehov av lagen.

I utredningen har man märkt att avancerade elektroniska signaturer avsedda i lagens 18 §, som baseras på ett kvalificerat certifikat och som skapas av en säker anordning för skapande av signaturer, används ytterst lite. Detta beror på krav av en särskild kortläsare, samt på bristen av tjänster som står till förfogande för kortinnehavaren. Väsentligt är dock att de flesta vardagliga transaktionerna faktiskt vidtas relativt formfritt utan att bekräfta viljeförklaring med en avancerad elektronisk signatur. I Finland finns det fortfarande bara en tillhandahållare av certifikattjänster, Befolkningsregistret, som utfärdar kvalificerade certifikat. Teleoperatörerna har nyligen börjat erbjuda Befolkningsregistrets medborgarcertifikat via mobiltelefoner. Utländska servercertifikat används i regel, men det finns ingen internationell marknad för kvalificerade certifikat. Certifikat används regelmässigt för elektronisk distansidentifiering och det finns ett växande antal av tjänster som tillåter identifieringen med Befolkningsregistrets certifikat. Bankerna har dock skapat sin egen identifieringsstandard (TUPAS2) och bankernas identifieringsmedel används i mycket högre grad i offentliga och privata tjänster än identifiering med certifikat.

Utredningen anser att det inte finns direkta ändringsbehov av lagen för tillfället, eftersom lagen än så länge tillämpas ytterst sällan i praktiken. Därför är tiden inte lämplig för att revidera lagens bestämmelser i detalj. Eftersom certifieringsverksamheten trots allt är under utveckling, borde regelverket granskas på nytt om några år, gärna också på Europeiska unionens nivå.

Nyckelord

elektronisk signatur, avancerad elektronisk signatur, digital signatur, certifikatutfärdare, certifikat, kvalificerat certifikat, mobilcertifikat, elektronisk identifiering, nätbanksidentifierare, elektronisk kommunikationskod

Övriga uppgifter

Kontaktperson vid ministeriet är Juha Perttula.

Seriens namn och nummer	ISSN	ISBN
Kommunikationsministeriets publikationer 52/2005	1795-4045 (nätpublikation)	952-201-406-0 (nätpublikation)

Sidoantal	Språk	Pris	Sekretessgrad
90	finska		offentlig

Distribution	Förlag
Kommunikationsministeriet	Kommunikationsministeriet

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication
28 June 2005

Authors (from body; name, chairman and secretary of the body)	Type of publication
Krogerus & Co. Oy	Report
Lauri Railas, Jan Vidjeskog	Assigned by Ministry of Transport and Communications
	Date when body appointed

Name of the publication

Impacts of the Act on Electronic Signatures 14/2003

Abstract

This study was commissioned by the Ministry of Transport and Communications Finland and it was done for the purpose of verifying the extent to which the objectives of the Electronic Signatures Act (14/2003) have been reached, and of assessing the impact of the Act. The study was commenced by a survey among central interest groups on their views regarding the feasibility of the Act, any problems that have emerged, the developments in the market and any changes required by these developments. The study contains sections on legal issues as well as information on the use of certification services and other forms of electronic signatures and identification.

The study takes note of the fact that advanced electronic signatures envisaged in Article 18 of the Act, which are based on a qualified certificate and which are created by a secure-signature-creation device, are very rarely used. This is because there is need to use a separate card reader and the small availability of services, in connection of which electronic signatures can be used. Another matter is that most normal transactions can be executed free of form without resorting to a signature based on a qualified certificate in the expression of will. There is only one certification authority issuing qualified services in Finland, the Population Register Centre (VRK). Finnish telecommunications operators have recently started to offer the VRK qualified certificate for citizens through mobile phones. Foreign certification services are used in connection with server certificates, but no trans-border market of qualified certificates exists at the moment. VRK´s certificates are generally used in connection with identification at a distance and there are an increasing number of services providing this possibility. Finnish banks have, however, created their own electronic identification standard (TUPAS2) and bank identifiers based on it are in a much wider use in public and private electronic services that certificates.

The study concludes that there are no imminent needs to amend the Act for the time being, since it is rarely applied in practice due to the slow development of the commercial infrastructure. The time is therefore not ripe for a comprehensive and detailed revision of the provisions of the Act. Since there are developments in the provision of certification services, the regulatory framework for electronic signatures should be assessed again, also at a Community level, in a few years´ time.

Keywords

Signature, electronic signature, advanced electronic signature, digital signature, secure-signature-creation device, certificate-service-provider, certificate, qualified certificate, mobile certificate, electronic identification, net bank identifier, electronic communication code

Miscellaneous

Contact person at the Ministry Mr Juha Perttula

Serial name and number		ISSN	ISBN
Publications of the Ministry of Transport and Communications 53/2005		1795-4045 (electronic version)	952-201-406-0 (electronic version)
Pages, total 90	Language Finnish	Price	Confidence status Public
Distributed by Ministry of Transport and Communications		Published by Ministry of Transport and Communications	

Esipuhe

Sähköisistä allekirjoituksista annettu laki (14/2003) tuli voimaan 1.2.2003. Liikenne- ja viestintäministeriö teetti selvityksen kyseisen lain vaikutuksista. Tavoitteena oli selvittää, mitä käytännön vaikutuksia ja seuraamuksia lain säätämisestä on havaittavissa sekä mitä lainsäädännön muutostarpeita on ilmennyt.

Selvitystä varten tuli haastatteluin ja kyselyin selvittää kaikkien keskeisten, suomalaisten alan toimijoiden ja asiantuntijoiden näkemyksiä lain toimivuudesta ja mahdollisista esiin tulleista ongelmista sekä lähitulevaisuudessa esiin tulevista alan kehityssuunnista ja niistä mahdollisesti johtuvista muutostarpeista. Selvityksessä tuli myös arvioida mm. mahdollisen lisäsääntelyn tarve esimerkiksi aikaleimojen ja muiden nykyisin sääntelemättä olevien lain soveltamisalaan läheisesti kuuluvien ilmiöiden osalta.

Lainsäädännön ohella selvityksessä kartoitettiin myös käytäntöä sen selvittämiseksi, mitä lain soveltamisalaan kuuluvia toimijoita, palveluja ja tuotteita Suomen markkinoilla on. Samalla selvitettiin, mitä varmenteiden ja muiden allekirjoitustoteutusten avulla käytettäviä palveluja Suomessa on tällä hetkellä käytössä.

Selvitystä tullaan hyödyntämään kansallisen lainsäädännön muutostarpeiden arvioinnissa ja jatkossa sähköisistä allekirjoituksista annetun direktiivin kehittämistä koskevassa työssä. Selvityksen pohjalta tullaan laatimaan myös eduskunnan lain säätämiseen liittyvässä vastauksessaan vuoden 2005 loppuun mennessä liikenne- ja viestintäministeriöltä edellyttämä selvitys sähköisistä allekirjoituksista annetun lain vaikutuksista ja soveltamisesta.

Selvityksen teki konsulttityönä Krogerus & Co. Oy liikenne- ja viestintäministeriön toimeksiannosta. Tutkimuksen pääasiallisena toteuttajana toimi lakimies Lauri Railas ja alkuvaiheessa myös asianajaja Jan Vidjeskog asianajotoimisto Krogerus & Co. Oy:stä. Liikenne- ja viestintäministeriössä selvityksestä vastasi neuvotteleva virkamies Juha Perttula.

Liikenne- ja viestintäministeriö haluaa kiittää kaikkia niitä lukuisia osapuolia, jotka joko asiantuntijoina tai muutoin edesauttoivat selvityksen valmistumista.

Helsingissä 28 päivänä kesäkuuta 2005

Juha Perttula
Neuvotteleva virkamies

SISÄLLYS

1. JOHDANTO 1

1.1. Tehtävänasettelu 1

1.2. Tutkimuksen toteuttaminen 2

2. LAKI JA SEN TAVOITTEET 3

2.1. Yleistä 3

2.2. Peruskäsitteistöä 4

2.2.1. Mikä on allekirjoitus ja mihin sitä käytetään? 4

2.2.2. Mikä on sähköinen allekirjoitus? 5

2.2.3. Lain peruskäsitteitä 9

2.2.4. Sähköinen tunnistaminen ja sähköinen allekirjoitus 14

2.2.5. Varmenneorganisaation tarjoamia lisäpalveluita 19

3. VARMENTEITA ERI TARKOITUKSIIN 20

3.1. Väestörekisterikeskuksen laatuvarmenteet 20

3.2. Kansalaisvarmenteen käytön edistäminen 21

3.3. Mitä varmenteita on käytössä? 24

3.3.1. Valtionhallinto, ministeriöt ja valtion laitokset 24

3.3.2. Erityisesti terveydenhuolto ja sosiaalitoimi 25

3.3.3. Kunta- ja paikallissektori 26

3.3.4. Palvelut yrityksille, julkisen rahoituksen hakeminen 27

3.3.5. Muita palveluita yrityksille 27

3.3.6. Palvelut yksityisille 28

3.3.7. Yksityinen sektori, operaattorit, tietoliikenneteollisuus ja teknisten palveluiden tarjoajat 29

3.3.8. Yksityinen sektori, pankit ja vakuutuslaitokset 30

3.3.9. Yksityinen sektori, kauppa 32

3.3.10. Yksityinen sektori, logistiikka 32

3.3.11. Yhteenvetoa 33

3.3.12. Muita varmenteita 35

3.3.13. Ulkomaisten varmenteiden käyttö organisaatioissa 37

3.3.14. Ulkomaiset sovellukset 38

3.4. Kansainvälistä vertailua 39

4. TOIMIJOIDEN NÄKEMYKSIÄ 40
4.1. Lain toimivuus 40
4.2. Tuleva kehitys 41
4.3. Pitääkö lakia muuttaa? 43
4.3.1 Lain soveltamisala 43
4.3.2. Laajempi sähköisen allekirjoituksen käsite 43
4.3.3. Vastuusäännösten tarkistaminen 44
4.3.4. Sulkulistan säilyttäminen 47
4.3.5. Luomisvälineen turvallisuus 48
4.3.6. Kuinka laatuvarmenteen hakija tunnistetaan? 50

5. MAHDOLLISIA UUSIA SÄÄNTELYKOHTEITA 50
5.1. Sähköinen tunnistaminen 50
5.2. Aikaleimapalvelut 56
5.3. Luotetut arkistointipalvelut 60
5.4. Notariaattipalvelut 61

6. VARMENNEPALVELUJEN TARJOAMINEN 62
6.1. Julkinen panostaminen varmennepalveluihin 62
6.2. Kilpailunäkökohdat 63
6.3. Tietosuoja 66

7. LAIN ARVIOINTIA 67
7.1. Lain tavoitteiden toteutuminen 67
7.2. Ratkaisuja sääntelyn ongelmakohtiin 70
7.2.1. Välitöntä muutostarvetta ei ole 70
7.2.2. Sääntely lähemmäksi käytäntöä 70
7.2.3. Vastuusääntely 71
7.2.4. Lisäpalvelut 71
7.2.5. Yksityisen toiminnan suhde julkiseen 72

LÄHDEAINEISTOA 73
Säädösaineistoa ja julkista ohjeistusta 73
Muuta lähdeaineistoa 75

LIITTEET

LIITE 1 - KYSELYYN VASTANNEET ORGANISAATIOT 77
Selvitykseen yksityiskohtaisemmin vastanneet organisaatiot tai henkilöt 77
Organisaatiot, jotka ovat antaneet tietoja varmenteiden käytöstä 78
LIITE 2 - KYSYMYKSET 79

1. JOHDANTO

1. 1. Tehtävänasettelu

Euroopan yhteisö hyväksyi Suomen puheenjohtajakaudella 13.12.1999 direktiivin 1999/93/EY yhteisön sähköisistä allekirjoituksia koskevista puitteista. Suomi saattoi direktiivin voimaan tammikuussa 2003 voimaan astuneella lailla sähköisistä allekirjoituksista (14/2003).

Liikenne- ja viestintäministeriö antoi 15.11.2004 asianajotoimisto Krogerus & Co. Oy:lle tehtäväksi laatia arvio kyseisen lain vaikutuksista (hanke no. 43917). Toimeksiannon mukaisesti selvityksessä tulee selvittää ja arvioida, mitä käytännön vaikutuksia ja seuraamuksia lain säätämisestä on havaittavissa sekä mitä lainsäädännön muutostarpeita on ilmennyt. Eduskunta oli lain säätämiseen liittyvässä vastauksessaan EV 221/2002 vp edellyttänyt että liikenne- ja viestintäministeriö antaa vuoden 2005 loppuun mennessä selvityksen sähköisistä allekirjoituksista annetun lain vaikutuksista ja soveltamisesta.

Selvitystä varten tuli haastatteluin ja/tai kyselyin selvittää kaikkien keskeisten alan suomalaisten toimijoiden, yritysten, tietoyhteiskunnan palvelujen tarjoajien, tietoyhteiskunnan palvelujen tarjontaa suunnittelevien tahojen, julkishallinnon, järjestöjen, yliopistojen ja muiden asiantuntijoiden näkemyksiä lain toimivuudesta ja mahdollisista esiin tulleista ongelmista sekä lähitulevaisuudessa esiin tulevista alan kehityssuunnista ja niistä mahdollisesti johtuvista muutostarpeista. Selvityksessä tuli myös arvioida mahdollisen lisäsääntelyn tarve esimerkiksi aikaleimojen ja muiden nykyisin sääntelemättä olevien lain soveltamisalaan läheisesti kuuluvien ilmiöiden osalta.

Lainsäädännön ohella selvityksessä kartoitetaan käytäntöä sen selvittämiseksi, mitä lain soveltamisalaan kuuluvia toimijoita, palveluja ja tuotteita, kuten laatuvarmenteet ja muut varmenteet sekä niihin liittyvät tuotteet sekä muut sähköisen allekirjoituksen toteutukset, Suomen markkinoilla on tällä hetkellä. Tämän lisäksi selvitetään karkeasti kansainvälisellä tasolla, onko muualla käytössä jotain sellaisia sähköisiin allekirjoituksiin liittyviä tuotteita ja sovelluksia, jotka saattaisivat soveltua myös Suomen markkinoille.

Samalla selvitetään, mitä varmenteiden ja muiden allekirjoitustoteutusten avulla käytettäviä palveluja Suomessa on tällä hetkellä käytössä ja mikä on sähköisten allekirjoitusten käytön todellinen määrä näissä palveluissa. Tässä suhteessa erotellaan allekirjoitusten eri toteutustavat ja

esimerkiksi varmenteiden käytön osalta niiden käyttö toisaalta tunnistamiseen ja toisaalta varsinaisen sähköisen allekirjoituksen laatimiseen.

Käytännön selvittämiseksi arvioidaan laatuvarmenteiden ja muiden varmenteiden hyödyntämisen välisiä eroja, eli esimerkiksi, kuinka paljon ja mihin tarkoituksiin henkilökorteilla olevia allekirjoitusvarmenteita ja toisaalta henkilökorteilla olevia tunnistautumiseen käytettäviä varmenteita käytetään ja mitkä ovat keskeisiä syitä mahdollisiin eroihin.

Selvityksessä tuli ottaa huomioon sähköisiä allekirjoituksia koskevan direktiivin sääntely siltä osin kuin selvityksessä arvioidaan kansallisen sääntelyn muutosmahdollisuuksia. Lisäksi tuli ottaa huomioon Viestintäviraston lain nojalla antamat määräykset ja niitä koskevat suositukset sekä Viestintäviraston maksuja koskevaan asetukseen sisältyvä varmennemaksuja koskeva sääntely. Erityisesti selvityksessä tuli kiinnittää huomiota niihin sähköisiä allekirjoituksia koskevan lain säännöksiin, jotka eroavat joltain osin direktiivistä tai eivät perustu siihen.

Selvityksessä tuli ottaa huomioon myös kansainväliset kehityssuunnat ja tarpeellisilta osin myös liikenne- ja viestintäministeriön ja komission viime aikoina teettämät selvitykset.

1.2.Tutkimuksen toteuttaminen

Tutkimuksen pääasiallisena toteuttajana on toiminut aluksi asianajaja Jan Vidjeskog ja sittemmin lakimies Lauri Railas asianajotoimisto Krogerus & Co. Oy:stä. Vidjeskogia ja Railasta ovat avustaneet oikeustieteen ylioppilaat Aki Kallio, Henna Kinnunen, Heta Rönkkö ja Marja Välilä samasta toimistosta. Selvityksestä vastaavana toimiston osakkaana on toiminut asianajaja Juha-Pekka Katainen.

Tutkimus on käynnistetty useiden keskeisimpien toimijoiden, Viestintäviraston, Väestörekisterikeskuksen, tietosuojavaltuutetun, teleoperaattorien ja pankkien edustajien tapaamisella. Tapaamisissa on alustavasti kartoitettu keskeisiä ongelmanasetteluita lain soveltamisalaan tai siihen läheisesti liittyvien kysymysten osalta. Alustavan kartoituksen perusteella on laadittu 33 kysymystä lakiin ja sen soveltamiseen läheisesti liittyvistä seikoista. Kysymykset on ryhmitelty niin, että ensin esitetään yleisempiä kysymyksiä, jonka jälkeen keskitytään itse lakiin, sen soveltamisalaan ja yksittäisiin määräyksiin liittyviin kysymyksiin.

Kysymykset on lähetetty yhteensä 134 toimijalle, jotka edustava eri aloja julkishallinnosta kauppaan ja kuljetuselinkeinoihin. Vastaajien joukossa on ollut valtionhallinnon eri organisaatioita ja asiantuntijavirkamiehiä, yrityksiä, järjestöjä ja tutkijoita. Vastauksia tuli lopulta 75, joista sisältökysymyksiin on vastattu enemmälti 45 tapauksessa. Monet muut vastaajat ovat ilmoittaneet, että koska sähköiset allekirjoitukset eivät ole käytössä, heillä ei ole edellytyksiä tai kiinnostusta vastata kyselyyn. Monet vastaajat ovat kuitenkin antaneet tietoja varmenteiden käytöstään, jota ei useinkaan ollut. Kirjallisten vastausten lisäksi on erikseen haastateltu Tietosuojavaltuutettu Reijo Aarniota, toimitusjohtaja Reijo Sventoa FiCOM ry:stä sekä Jüri Voorea Eesti Sertifitseerimiskeskus AS:stä. Kokonaisuudessaan palautetta on antanut 78 organisaatiota tai henkilöä, jotka on lueteltu tämän raportin liitteessä 1.

Yhteensä 14 vastaajaa sekä liikenne- ja viestintäministeriön edustaja osallistuivat 17.2.2005 järjestettyyn tilaisuuteen, jossa käsiteltiin kyselyn keskeisiä kysymyksiä ja keskusteltiin selvityksen kannalta keskeisistä kysymyksenasetteluista. Tämän jälkeen on vastauksia vielä vastaanotettu mm. kauppa- ja teollisuusministeriöstä ja kuluttajavirastosta. Asianajotoimisto Krogerus & Co. Oy on jättänyt selvityksen ministeriölle 27. huhtikuuta 2005. Selvityksen on kirjoittanut OTT Lauri Railas. Selvityksessä esitetyt mielipiteet ovat kirjoittajan, eivät toimeksiantajan näkemyksiä.

2. LAKI JA SEN TAVOITTEET

2.1. Yleistä

Hallituksen esityksessä todetaan, että sähköisiä allekirjoituksia ja niiden käytössä tarvittavia tuotteita ja palveluita koskevalla lailla edistettäisiin kuluttajien ja muiden käyttäjien luottamusta verkkoliiketoimintaan ja sähköiseen asiointiin. Lain on tarkoitus edistää uuden liiketoimintasektorin, varmentamisen kehittymistä. Toteutuessaan laki lisäisi sähköistä kaupankäyntiä ja asiointia sekä tietoyhteiskuntapalvelujen käyttöä.

Sähköisellä allekirjoituksella ymmärretään sähköisessä muodossa olevaa tietoa, joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä.

Sähköistä allekirjoitusta voidaan käyttää eri tarkoituksiin sähköisin menetelmin tapahtuvasta asioinnista sähköiseen kaupankäyntiin. Sähköisiä allekirjoituksia koskeva direktiivi luettelee johdantolauseissaan sähköisten allekirjoitusten erilaisia käyttötilanteista alkaen kaupankäynnistä julkisella sektorilla tapahtuvaan käyttöön, kuten esimerkiksi julkisiin hankintoihin, verotukseen, sosiaaliturvaan, terveydenhuoltoon ja oikeushallintoon liittyvät käyttötilanteet.

Sähköisen kaupankäynnin ja asioinnin lainsäädännön tehtävänä on mahdollistaa sähköisten menetelmien käyttö paperilla tapahtuvien toimintojen asemesta. Sähköiseen maailmaan muodostetaan menettelylliset tai käsitteelliset vastineet monille fyysisen eli paperimaailman ilmiöille kuten allekirjoituksille, kirjalliselle muodolle ja sen erityiskysymyksinä mm. alkuperäisille asiakirjoille ja sopimusehtojen tekemiselle sopimuksen osaksi.

Laatuvarmenteella varmennettu kehittynyt sähköinen allekirjoitus, joka on luotu turvallisella allekirjoituksen luomisvälineellä, muodostaa lain 18 §:n mukaisesti ainakin vastineen käsintehdylle allekirjoitukselle. Muille kuin nämä kriteerit täyttäville sähköisille allekirjoituksille ei luoda lainsäädännöllä vahvistettua allekirjoituksen asemaa, mutta lain taustalla olevan direktiivin 5 artiklan 2 kohdassa samoin kuin lain esitöissä todetaan, että muukin allekirjoitus voi täyttää vaatimukset tapauskohtaisesti.

2.2 Peruskäsitteistöä

2.2.1. Mikä on allekirjoitus ja mihin sitä käytetään?

Historiallisesti tarkasteltuna allekirjoitukselle on annettu erilaisia määritelmiä ja merkityksiä.[1] Suomen lainsäädäntö ei sisällä perinteisen allekirjoituksen toteuttamistavan ja oikeusvaikutusten yleistä määrittelyä. Lainsäädännössämme on itse asiassa sangen vähän allekirjoitusta koskevia vaatimuksia. Ankarimmillaan Suomen laki vaatii omakätistä allekirjoitusta todistajien läsnä ollessa (testamentti), mutta aineellinen oikeus tuntee myös muita mahdollisuuksia tehdä allekirjoitus, kuin käsintehty allekirjoitus, esimerkiksi merilain 13 luvun 46 § mahdollistaa sen, että konossementti on varustamon taholta mekaanisesti allekirjoitettu, jolloin allekirjoitus tapahtuu esimerkiksi painokoneella, leimalla tai lävistämisellä. Mekaaninen allekirjoitus sallitaan myös laissa sähköisestä asi-

[1] Allekirjoitusvaatimuksesta kansainvälisen kaupan piirissä, ks. UN/CEFACT Recommendation 14 (1979), Annex I, http://www.unece.org/cefact/rec/rec14/rec14_1979_inf63.pdf

oinnista viranomaistoiminnassa. Lain vaatimus allekirjoituksesta voi seurata kuitenkin myös kirjallista muotoa koskevasta vaatimuksesta.[2]

Allekirjoitusta voidaan tarkastella myös funktionaalisesti. Allekirjoitus palvelee todistelutarkoitusta liittämällä asiakirja allekirjoittajaan. Allekirjoituksella on myös seremoniallisia funktioita, sillä allekirjoituksen vaatimus herättää allekirjoittajan huomion tapahtumaan ja ehkäisee harkitsemattomia toimenpiteitä tämän taholta. Lain ja tapaoikeuden edellyttämissä tilanteissa allekirjoitus ilmaisee kirjoittajan hyväksyvän allekirjoitetun tietosisällön ja usein sen, että tietosisällöllä on oikeusvaikutuksia. Allekirjoituksella on myös logistisia ja tehokkuusmerkityksiä. Kirjallisessa sopimuksessa oleva allekirjoitus ilmaisee transaktion selvyyden ja lopullisuuden. Joissakin tapauksissa kirjallisessa muodossa ilmaistut sitoumukset liittyvät itse asiakirjan lailliseen hallintaan. Allekirjoitusta käytetään tällöin hallinnan luovutuksen ohella osoittamaan asiakirjaan liittyvien oikeuksien siirtyminen.

2.2.2. Mikä on sähköinen allekirjoitus?

Mikäli allekirjoituksen tekotapoja tarkastellaan laajasti, sähköisellä allekirjoituksella voidaan ymmärtää myös paperilla olevien kuvioiden digitalisoituja vastineita, tietokoneella eri tavoin kirjoitettuja merkintöjä tai jopa viestin osoitetietoja.

Teknologianeutraliteettiperiaatteen mukaan lainsäädännössä ei suoraan aseteta estettä minkään tyyppisen sähköisen allekirjoituksen käytölle. Sähköisiä allekirjoituksia voivat olla monenlaiset toimenpiteet, joilla tietty tietosisältö liitetään allekirjoittajaan. YK:n kansainvälisen kauppaoikeuden toimikunnan UNCITRAL:in laatiman, vuonna 1996 hyväksytyn sähköistä kaupankäyntiä koskevan mallilain[3] artikla 7(1)(a) katsoo, että sähköisessä toimintaympäristössä allekirjoituksen oikeudelliset perusfunktiot on toteutettu tavalla, joka identifioi viestin lähettäjän ja vahvistaa että lähettäjä hyväksyy viestin sisällön.

Sähköisille allekirjoituksille asetetaan kuitenkin tietoturva- ja muita luotettavuutta koskevia vaatimuksia lähinnä siksi, että fyysinen tarkastelumahdollisuus puuttuu. UNCITRAL:in mallilain artikla

[2] Oikeustoimilakikomitean mietinnössä, Kom 1990:20, s. 58, katsotaan, että kirjallista muotoa koskeva vaatimus sisältäisi myös allekirjoitusvaatimuksen. Muotovaatimukset voivat olla varsinaisia, jolloin muotovaatimuksen noudattaminen on edellytyksenä pätevän oikeustoimen syntymiselle. Ne voivat olla epävarsinaisia, jolloin muotovaatimuksen noudattamatta jättäminen ei tee oikeustointa pätemättömäksi, mutta on säädetty todistelun helpottamiseksi. .

7(1)(b) asettaa joustavan turvallisuusvaatimuksen. Menetelmien tulisi olla yhtä luotettavia kuin on tarkoituksenmukaista sitä tarkoitusta varten, johon viesti tuotetaan tai kommunikoidaan.[4] Tätä voitaisiin kutsua käyttöaluetta koskevaksi suhteellisuudeksi. Vastaava periaate on myös vuodelta 2001 peräisin olevan UNCITRAL:in sähköisiä allekirjoituksia koskevan mallilaissa[5]

Sähköisiä allekirjoituksia koskeva lainsäädäntö samoin kuin muu sähköisiä asiakirjoja koskeva lainsäädäntö voi olla minimalistista. Tällöin lainsäädännössä vain todetaan tavoitteiden yleinen luonne jättäen yksityiskohdat osapuolten harkintaan. Sähköisten allekirjoitusten kohdalla tämä korostaa asiayhteyden merkitystä ja jättää itse allekirjoituksen ominaisuudet vähemmälle. Tällöin luottavalla osapuolella on pitkälle riski välineiden valintaan ja käyttöön nähden.

Toinen teknologiaorientoituneempi lähestymistapa joko määrittelee käytettävän teknologian tai ainakin sen kuinka teknologialla saavutetaan oikeusvaikutuksia. Tässä lähestymistavassa korostetaan tietoturvaa ja allekirjoitettavan tiedon eheyttä, ja se rakentuu usein luotetun kolmannen osapuolen käyttämiselle allekirjoituksen varmentamisessa. Varmentaja takaa allekirjoituksen aitouden ja allekirjoittajan henkilöllisyyden. Lain käytännössä vaatima kehittynyt teknologia takaa pitkälle allekirjoituksen peruuttamattomuuden ja viestin eheyden.[6]

---

[3] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, General Assembly Resolution 51/162 of 16 December 1996. Artikla 5bis on lisätty mallilakiin vuonna 1998.

[4] Huomioon otettavien kriteerien osalta ks. mallilain Guide to Enactment, ss. 33 -34.

[5] UNCITRAL Model Law on Electronic Signatures Art. 6(1). “Where the law requires the signature of a person, that requirement is met in relation to the data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.” Mallilain artiklan 6 kohta 3 sisältää kuitenkin allekirjoituksen luotettavuutta koskevia lisävaatimuksia, jotka vastaavat sähköistä allekirjoitusta koskevan direktiivin kehittyneelle sähköiselle allekirjoitukselle asettamia vaatimuksia ja joiden täyttyminen täyttää myös kohdassa 1 tarkoitetun luotettavuusvaatimuksen.

[6] Salausjärjestelmät jaetaan symmetrisiin salausjärjestelmiin, joissa viestin salaus ja purku tapahtuvat samalla avaimella. Epäsymmetrisessä salauksessa toisella avaimella salataan ja toisella taas salaus puretaan. Salaus tapahtuu julkisella avaimella, joka asetetaan kaikkien nähtäväksi (= julkinen avain), purku taas yksityisellä avaimella. Julkisen avaimen järjestelmää kutsutaan PKI-järjestelmäksi (public key infrastructure = PKI) Yksityinen avain on käytännöllistä laittaa toimikortille. Toimikortti eli älykortti, sirukortti, suoritinkortti, englanniksi smart card, sisältää prosessorin ja muistia.

Keskeisellä sähköisen allekirjoituksen tekniikalla, julkisen avaimen järjestelmällä tehtyä sähköistä allekirjoitusta, jota säännönmukaisesti kutsutaan myös digitaaliseksi allekirjoitukseksi nimenomaan PKI-tekniikkaa tällöin tarkoittaen, käytetään tietoturvan ylläpitotarkoituksessa ja sillä voidaan varmistaa tiedon kiistämättömyys (non-repudiation) sekä tiedon eheys ja muuttumattomuus (integrity); tätä tarkoitusta palvelevat salausjärjestelmät eli kryptografia, ja PKI-tekniikka on itse asiassa salaustekniikka. Sähköistä allekirjoitusta tehtäessä yksityistä avainta käytetään allekirjoitukseen ja julkista avainta allekirjoituksen tarkistamiseen. Julkisen avaimen järjestelmällä tarkoitetaan usein niitä toimenpiteitä ja käytäntöjä, joiden perusteella julkisen avaimen tietoverkossa kohtaava voi olla varma, kenen hallussa vastaava yksityinen avain on.

Yleisesti katsotaan, että PKI soveltuu hyvin tiedonsiirron aikaiseen salaukseen, mutta heikosti pitkäaikaissäilytykseen. PKI-tekniikkaan perustuva salauskin on teoriassa murrettavissa, jos käytettävissä on riittävä tietokoneteho. Elokuussa 2004 tehdyssä testissä kokeiltiin onnistuneesti kvanttikryptografiaa salauksessa käytetyn avaimen siirtämiseen lähettäjältä vastaanottajalle. Transaktiokohtaisen avaimen käyttö nopeuttaa salauksen purkamista huomattavasti.

Yhdysvalloissa ja Kanadassa on oltu yleisesti minimalistisen lähestymistavan kannalla. Digitaalisia allekirjoituksia erityisesti sääntelevät lait[7] edustavat puolestaan selkeästi vastakkaista lähestymistapaa. Sekä EU-direktiivi että UNCITRAL:in sähköisiä allekirjoituksia koskeva mallilaki sijoittuvat näiden kahden lähestymistavan välimaastoon. Voidaan sanoa, että direktiivi on laadittu digitaalisten allekirjoitusten käyttämää PKI-tekniikkaa silmällä pitäen, mutta se on kirjoitettu teknologianeutraalisti eikä rajaa mitään allekirjoitusten toteutustapoja pois hyväksyttävien allekirjoitustoteutusten piiristä.

Sähköisistä allekirjoituksista annetussa lain sisältämässä sähköisen allekirjoituksen määritelmässä tulee esille allekirjoituksen tarkoitus eli henkilöllisyyden todentaminen ja yhdistäminen sähköiseen tietoon tai viestiin. Viestin alkuperä voidaan todeta yksiselitteisesti liittyvän tiettyyn sähköiseen identiteettiin (authentication). Yleinen tulkinta on, että direktiivissä ja laissa oleva sähköisen allekirjoituksen määritelmä liittyy ensisijaisesti tiedon alkuperän toteamista, ei lähettävän henkilön tai tahon henkilöllisyyden selvittämistä.[8] Sähköinen identiteetti voidaan yhdistää todelliseen henkilöön varmenteella, jolla viestin lähettäjä tunnistetaan (identification). Tieto sähköisessä muodossa ilmenee tiedostoissa, joka on kulloinkin tietty rajoitettu tietosisältö, minkä lisäksi tietosisältöön voi kuulua normaalin tarkasteltavan viestin ulkopuolella olevia teknisiä osia. Tämä tietosisältö vastaa asiakirjan käsitettä. Allekirjoittaja yksilöi itsensä suhteessa asiakirjassa olevaan tietoon. Mikäli allekirjoitettava tietosisältö on tahdonilmaisu esimerkiksi sopimussuhteessa, allekirjoituksella todetaan sopimussidonnaisuutta koskevan tahdonilmaisun olemassaolo ja peruuttamattomuus.

Tämä allekirjoituksen funktio mielletään usein keskeiseksi. Allekirjoittajan lain mukainen määritelmä sisältääkin toiminnan itsensä tai edustamansa luonnollisen tai oikeushenkilön puolesta. Lain 18 §:ssä viitataan oikeustoimen ja sähköisen allekirjoituksen suhteeseen. Lain 5 §:n 1 momentin 5 kohdassa edellytetään, ettei luomisväline estä tietosisällön esittämistä allekirjoittajalle ennen allekirjoittamista. Tämä on allekirjoittajan kannalta keskeinen määräys.

---

[7] Näin mm. Saksan EU-direktiiviä edeltävä Signaturgesetz , Bundesgesetzblatt 1997 I 1872 (Artikel 3 Informations- und Kommunikationsdienstegesetz, Bundesgesetzblatt 1997 I 1870) sekä Viron laki vuodelta 2000, (RT I 2000, 26, 150)

[8] Thomas Myhr, Regulating a European eID, A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005, s. 12; Study for the European Commission – DG Information Society "The Legal and Market Aspects of Electronic Signature – Legal and markety aspects of the application of Diorective 1999/93/EC and practical applications in the Member States, the EEA, the Candidate and the Accession countries, s. 28; Direktiivi 1999/93/EY, johdantolause 8.

Sähköisiä allekirjoituksia voidaan tehdä laatuvarmenteilla, jotka sähköisiä allekirjoituksia koskevan lain 18 §:n mukaisten kriteerien täyttyessä täyttävät aina lakiin perustuvat allekirjoitusvaatimukset. Laatuvarmenteiden käyttö edellyttää varmennuksen lisäksi, että sekä varmennettavalla että luottavalla osapuolella on käytössä tekniset ja organisatoriset keinot niiden käyttöön.

Sähköisiä allekirjoituksia voidaan tehdä erityislainsäädännön, nimenomaisen tai hiljaisen sopimuksen tai kauppatavan perusteella muilla varmenteilla kuin laatuvarmenteilla, kuten ohjelmistovarmenteilla, pankkitunnisteilla, skannatuilla ja/tai telekopioiduilla käsintehdyillä allekirjoituksilla, koneellisesti tehdyillä allekirjoituksilla, kuten sähköiseen asiakirjaan sähköisesti lyötävillä leimoilla tai vaikkapa sähköpostiviestin loppuun koneellisesti lisätyllä nimellä tai salanimellä. Luettelo ei luonnollisesti ole tyhjentävä. Esimerkiksi hallituksen esityksessä arvioitiin, että tulevaisuudessa yleistyvät sähköiset allekirjoitukset, jotka hyödyntävät biometristä tunnistamista. Muihin kuin käsintehtyihin allekirjoituksiin lukeutuvat mekaaniset allekirjoitukset, kuten lävistykset, jotka usein mainitaan sähköisten allekirjoitusmuotojen yhteydessä.

Allekirjoitustapoja voidaan ryhmitellä eri tavoin. Esimerkiksi ainakin TUPAS2-standardiin perustuvat pankkitunnisteet ovat ns. vahvan tunnistamisen menetelmä (ks. jäljempänä), minkä vuoksi ne ovat riittävän luotettavia monissa käyttötilanteissa myös allekirjoituskäytössä. Mekaaniset allekirjoitustavat ovat allekirjoittajan tunnistamisen osalta yleensä epäluotettavampia, mutta voivat silti täysin täyttää vaihdannan tarpeet mikäli väärennöksiä esiintyy vähän tai osapuolet tuntevat toisensa hyvin. Käytetyn allekirjoitusmenetelmän luotettavuustaso vaikuttaa osapuolten vastuunjakoon. Mitä epäluotettavampi menetelmä on käytössä, sitä suuremmaksi muodostuu luottavan osapuolen riski ja huolellisuustaso.[9]

Vastuunjakoon ja osapuolilta vaadittuun huolellisuustasoon vaikuttaa myös se, onko allekirjoitus luotetun kolmannen osapuolen varmentama. Esimerkiksi laatuvarmenteet, monet ohjelmistovarmenteet ja ulkopuolisille palveluntarjoajille esitetyt pankkitunnisteet ovat luotetun kolmannen osapuolen[10] varmentamia. Ulkopuolinen varmentaja, joka tehtävänä on varmentaa allekirjoittajan henkilöllisyys ja allekirjoituksen aitous, kantaa lain ja sopimusehtojen[11] mukaisen vastuun toiminnastaan.

[9] Ks. UNCITRAL Model Law on Electronic Signatures, artikla 11.
[10] Trusted Third Party tai Certification Authority (CA)

Monia sähköisen allekirjoituksen toteutustapoja käytetään sopimusperusteisesti. Esimerkiksi Nordean vaihtuvien salasanojen käyttöön perustuvien pankkitunnisteiden käytön pohjana on sopimus asiakkaan ja pankin välillä sekä Nordean ja ulkopuolisen palveluntarjoajan välinen sopimus tunnistuspalvelusta. Sopimuksella sovitaan, mitä menettelyä pidetään allekirjoituksena.[12] Erityislakiin tai kauppatapaan perustuvat allekirjoitustavat ovat taas lähtökohtaisesti aina avoimien käyttäjäryhmien käytettävissä olevia menetelmiä. Esimerkiksi tuomioistuimen kanssa asioitaessa voidaan sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) 20 §:n mukaan käyttää koneellista allekirjoitusta ja merilain 13 luvun 46 § samoin kuin Kansainvälisen kauppakamarin ICC:n hyväksymät Yhdenmukaiset remburssisäännöt UCP500 sallivat erilaiset sähköiset ja mekaaniset kaupallisten asiakirjojen, kuten konossementtien allekirjoitustavat. Sähköisistä allekirjoituksista annetun lain 18 § määrittelee puolestaan allekirjoitustoteutuksen, joka täyttää aina lain vaatimukset ja on siten yleiskäyttöinen.

Sopimusjärjestelyjen ja lakimääräysten lisäksi on kuitenkin aina huomattava se, että monien kehittyneempien allekirjoitustoteutusten käyttö edellyttää teknillisiä järjestelyjä, kuten tietokoneohjelmien saatavilla oloa ja yhteensopivuutta tai lukijalaitteiden käyttöä. Siten allekirjoitustoteutuksen käyttökelpoisuus on aina riippuvainen osapuolten tahdosta.

Allekirjoitustoteutuksen riittävyyttä ja toteutukseen käyttöön liittyvää vastuunjakoa arvioidaan viime kädessä aina tuomioistuimessa. Kun sopimusoikeudessamme vallitsee sopimusvapaus ja vapaan todistusharkinnan periaatteet, ratkaisee viime kädessä tuomioistuin kunkin allekirjoitus toteutuksen riittävyyden.

2.2.3 Lain peruskäsitteitä

Sähköisen kaupankäynnin ja asioinnin lainsäädännön tehtävänä on mahdollistaa sähköisten menetelmien käyttö erityisesti paperilla tapahtuvien toimintojen asemesta. Sähköiseen maailmaan rakennetaan siten sille tyypilliset toiminnalliset vastineet (functional equivalents) monille paperimaailman ilmiöille kuten allekirjoituksille, kirjalliselle muodolle, alkuperäisille asiakirjoille sekä sopimusehtojen tiedoksiannolle. Tällöin ei pyritä toteuttamaan perinteisen muodon toteutumista mah-

[11] Ks. esimerkiksi Sonera CA Certificate Policy, Sonera Class 2 Certificate, Valid as from January 22, 2004, Version 2.1. TeliaSonera Finland Oyj, 22.1.2004.
[12] Esimerkiksi Sampo ilmoittaa allekirjoituspolitiikassaan (http://www.sampo.fi/ehdot/suomi/copy2/html, vierailtu 2.3.2005), että pankin asiakasnumero ja PIN-luku vastaavat asiakkaan perinteistä tunnistamista henkilöllisyyttä osoitta-

dollisimman hyvin sähköisessä ympäristössä, vaan perinteisen muodon taustatavoitteet pyritään toteuttamaan sähköiselle ympäristölle ominaisella tavalla.[13]

Sähköisiä allekirjoituksia koskevan lain mukainen allekirjoitus täyttää muualla lainsäädännössä olevat allekirjoitusta koskevat vaatimukset. Lain 18 §:ssä todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen

(1) kehittynyt sähköinen allekirjoitus, joka
(2) perustuu laatuvarmenteeseen ja
(3) on luotu turvallisella allekirjoituksen luomisvälineellä.

Laki asettaa ehdottomasti lain vaatimukset täyttävälle sähköiselle allekirjoitukselle ja varmentajan toiminnalle toiminnallisia, teknisiä ja organisatorisia vaatimuksia. Vertailun vuoksi todettakoon, että laki tietoyhteiskunnan palvelujen tarjoamisesta 2002/458 sisältää 12 §:ssä kirjallista muotoa koskevan vaatimuksen täyttämistä sähköisessä muodossa koskevat vaatimukset. Pykälässä todetaan, että jos sopimus lain mukaan on tehtävä kirjallisesti, vaatimuksen täyttää myös sellainen sähköinen sopimus, jonka sisältöä ei voi yksipuolisesti muuttaa ja joka säilyy osapuolten saatavilla. Jos sopimus on lain mukaan allekirjoitettava, sovelletaan mitä sähköisistä allekirjoituksista erikseen säädetään. Lainkohdan vaatimukset ulottuvat myös sopimussuhteisiin kuuluviin osapuolten ilmoituksiin ja muihin toimenpiteisiin, joiden lain mukaan on oltava kirjallisia tai allekirjoitettuja. Varsinaista kirjallista muotoa koskevat vaatimukset ilmaistaan siten toiminnallisin tavoittein, joiden tekninen toteuttamistapa on osapuolten valittavissa. Mitään organisatorisia vaatimuksia, esim. sopimuksen tallentamista luotetun kolmannen osapuolen haltuun, tai täsmennettyjä teknisiä vaatimuksia kuten sopimusehtojen sinetöimistä sähköisin allekirjoituksin ja/tai aikaleimoin, ei nimenomaisesti edellytetä. Mitään kirjallista muotoa vastaavia sähköisiä toteutustapoja ei sähköistä kaupankäyntiä koskevassa laissa ole siis myöskään kvalifioitu lähtökohtaisesti lain vaatimuksia täyttäviksi.

Erot lähestymistavassa toisaalta sähköisten allekirjoitusten ja toisaalta kirjallisen muodon täyttämistä koskevien vaatimusten välillä selittynevät sillä, että sähköisistä allekirjoituksista annettu laki perustuu lähes yksinomaan direktiiviä säädettäessä tehtyihin valintoihin, kun taas lakia tietoyhteis-

---

vasta asiakirjasta ja turvakortin avainlukua vastaava kertakäyttöinen turvaluku vastaa asiakkaan omakätistä allekirjoitusta.

[13] Ks. Laine-Ponka, ss. 1032-1035.

kunnan palvelujen tarjoamisesta saatettiin implementoitaessa kansallisella tasolla valita ne keinot, jolla sähköistä kaupankäyntiä sääntelevän direktiivin varsin yleisluonteinen vaatimus toteutetaan.

Laatuvarmenteella varmennettu kehittynyt sähköinen allekirjoitus, joka on luotu turvallisella allekirjoituksen luomisvälineellä, muodostaa lain 18 §:n mukaisesti ainakin vastineen käsintehdylle allekirjoitukselle. Sen seikan, että kriteerit täyttävät menetelmät asetetaan oikeudellisesti samanarvoiseen asemaan kuin käsintehty allekirjoitus, ei tule vähentää muiden menetelmien oikeudellista asemaa[14] Muilta sähköisiltä allekirjoituksilta kuin tässä lainkohdassa mainituilta ei voida kiistää allekirjoituksen asemaa ainoastaan sillä perusteella, että allekirjoitus ei ole lainkohdassa mainittujen kriteerien mukainen. Tätä direktiivin 1999/93/EY artiklan 5 (2) mainittua sääntöä ei ole otettu Suomen lakiin sen vuoksi, ettei sen toteaminen ole välttämätöntä sopimusvapauden ja vapaan tuomioistuinten todistusteorian vallitessa. Direktiivin implementoiminen Suomen lainsäädäntökulttuurin periaatteiden mukaisesti on kuitenkin luonut epätietoisuutta, jota lakia laadittaessa ei ajateltu.[15]

Laki ja direktiivi sisältävät runsaasti peruskäsitteitä, jotka saattavat olla sellaisenaan tuntemattomia paperimaailmassa. Esimerkiksi sähköisessä maailmassa esiintyy ulkopuolinen varmentaja, joka käytännössä suorittaa ulospäin hieman vastaavanlaista autentikointitehtävää kuin julkinen notaari. Sähköisten allekirjoitusten parissa toimivat organisaatiot käyttävät kaupallisessa tai hallinnollisessa tarkoituksessa samanlaisia peruskäsitteitä, mutta silti sähköisten allekirjoitus- ja tunnistamis- menetelmien yhteydessä käytettävä terminologia on vaikeasti lähestyttävää ja aiheuttaa helposti sekaannuksia, mikä kävi ilmi myös selvitystä tehtäessä.

Lain mukainen kehittynyt sähköinen allekirjoitus on allekirjoitus, joka liittyy yksiselitteisesti allekirjoittajaan, allekirjoittaja voidaan yksilöidä, se on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan ja se on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita (eheyden vaatimus).

Sähköisistä allekirjoituksista annetussa laissa ovat teknisiä käsitteitä allekirjoituksen luomistiedot, luomisvälineet ja todentamistiedot. Varmenteella tarkoitetaan sähköistä todistusta, joka liittää allekirjoituksen todentamistiedot (kuten julkiset avaimet) allekirjoittajaan ja vahvistaa allekirjoittajan

[14] Myös lain 18 §:ssä tarkoitettu allekirjoitus voidaan kiistää. Tällainen kiistäminen voi perustua normaalisti lähinnä muihin kuin teknisiin ominaisuuksiin, kuten allekirjoittamaan pakottamiseen tai organisaation sisäiseen toimivallan puuttumiseen. Oikeudellista estettä ei sinänsä ole myöskään esimerkiksi allekirjoituksen luomisvälineen turvallisuuden osalta, mutta on vaikeampaa, jos standardien vaatimukset on täytetty. Laissa tarkoitettua laatuvarmentajaa voi kohdata kiistämistilanteessa vahingonkorvausseuraamus, ellei tämä näytä toimineensa huolellisesti.

henkilöllisyyden. Useiden henkilöiden ja varmentajien varmenteista syntyy usein puumainen hierarkia, jonka juurena on ns. juurivarmentajan varmenne. Varmentaja on kolmas osapuoli, joka salakirjoittaa julkisen avaimen omalla yksityisellä avaimellaan merkiksi sen luotettavuudesta. Varmentajaan tulee kaikkien voida luottaa, minkä vuoksi tämän toiminnan luotettavuuteen kohdistuu suuria odotuksia. Varmenteen antaa usein ulkopuolinen varmentaja, luotettu kolmas osapuoli, joka takaa allekirjoittajan henkilöllisyyden. Varmentajalla on toimintaansa varten usein varmennepolitiikka ja laatuvarmentajalla täytyy jo lain mukaan olla sellainen[16] Muiden varmenteiden kuin laatuvarmenteiden osalta on ajateltavissa, että esim. käytetty tietojärjestelmä myöntää varmenteen eli antaa henkilöllisyydestä ja/tai allekirjoituksesta todistuksen. Tällöinkin tietojärjestelmän toimittaja tai ylläpitäjä vastaa sen toiminnasta tavalla tai toisella.

Laatuvarmenne on varmenne, joka sisältää lain 7 §:n 2 momentin mukaiset tiedot, ja jonka on myöntänyt varmentaja, joka täyttää 10 - 15 §:ssä asetetut, toiminnalliset, tekniset ja organisatoriset vaatimukset.[17]

Allekirjoituksen luomisvälineellä tarkoitetaan fyysisen laitteen ja sen toiminnan mahdollistavien ohjelmistokomponenttien muodostamaa kokonaisuutta. Esimerkkinä toimii toimikortti, sen lukijalaite, lukijalaitteen ajurit sekä selainkäytön mahdollistavat ohjelmistomodulit. Turvallinen allekirjoituksen luomisväline varmistaa riittävän luotettavasti, että allekirjoituksen luomistiedot ovat käytännössä ainutkertaisia ja että ne säilyvät luottamuksellisina; allekirjoituksen luomistietoja ei voida päätellä muista tiedoista, allekirjoitus on suojattu väärentämiseltä; allekirjoittaja voi suojata allekirjoituksen luomistiedot muiden käytöltä ja luomisväline ei muuta allekirjoitettavia tietoja eikä estä tietojen esittämistä allekirjoittajalle ennen allekirjoittamista, eli allekirjoittajan on tiedettävä mitä allekirjoittaa.

Luomisväline on aina turvallinen, jos

1) Se on EU:n komission (artikla 9-komitea) vahvistamien ja virallisessa lehdessä julkaistujen standardien mukainen tai

[15] Laatuvarmenteiden markkinoimisen yhteydessä on toisinaan puhuttu ”lakisääteisestä allekirjoituksesta”.
[16] Varmennepolitiikka voi esimerkiksi vaatia, että varmenteen hakija on tunnistettava luotettavasti henkilöllisyystodistuksesta, hukkunut sirukortti on asetettava sulkulistalle tai että yksityisestä avaimesta ei kortin valmistusvaiheessakaan saa jäädä kopiota mihinkään. Laatuvarmenteiden osalta monet varmennepolitiikalle asetettavat vaatimukset sisältyvät jo lakiin ja Viestintäviraston määräyksiin.

2) vaatimusten arviointitehtävään nimetty tarkastuslaitos (Suomi tai ETA), on luomisvälineen hyväksynyt

Komissio on tähän mennessä vahvistanut useita PKI-pohjaisia standardeja.[18] Käytännössä, jos luomisväline ei ole standardien mukainen, allekirjoitusvälineiden hyväksyttäminen tapahtuu tapauskohtaisesti eikä välttämättä arviointitehtävään nimetyn tarkastuslaitoksen toimesta.[19]

Varmentaja on luotettu kolmas osapuoli (Trusted Third Party, Certification Authority), joka oikeustoimen tai muun sähköisen kommunikaation yhteydessä antaa todistuksen allekirjoittajan henkilöllisyydestä. Sähköisesti asioitaessa eivät osapuolet voi fyysisesti varmistua toistensa henkilöllisyydestä esimerkiksi henkilöllisyystodistuksen esittämisen tai allekirjoitusnäytteen avulla. Näin ollen luotettava varmentamistoiminta on tärkeää sähköisen asioinnin ja vaihdannan edistämiseksi. Varmentamiselle ja varmenteelle asetetaan laissa vaatimuksia, jotka koskevat kuitenkin vain laatuvarmenteita. Muiden varmenteiden ja muiden allekirjoitusmenetelmien osalta laki ei sisällä juurikaan sääntelyä paitsi tietosuojan ja valvonnan osalta, ja ne on jätetty pitkälti sopimuskäytännön varaan.

Laatuvarmentajana toimiminen asettaa organisaatiolle lukuisia vaatimuksia, vaikka monia tehtäviä voidaankin hoitaa alihankintana. Alihankkijoiden käyttäminen on kaupallinen järjestely, jolla laatuvarmentaja ei kuitenkaan voi välttää vastuutaan luottavaan osapuoleen nähden, vaikka se voikin sopimusteitse luoda itselleen takautumisvastuuteitä. Suomeen on syntynyt vain yksi laatuvarmentaja, Väestörekisterikeskus. Muina varmentajina kuin laatuvarmentajina toimivat mm. teleoperaattorit ja pankit. Laatuvarmentamisesta syntyy usean osapuolen välinen ketju, jossa pohjana on laatuvarmentajan kantama käännetyn todistustaakan mukainen vastuu, mutta jossa muiden osapuolten kuin luottavan osapuolen vastuuasema määräytyy monimutkaisten sopimuskonstruktioiden pohjalta, jossa vastuuta siirretään ketjussa eteenpäin.

---

[17] Sähköisiä allekirjoituksia koskevassa direktiivissä ja sen pohjalta laaditussa laissa on määritelty varmenteen käsite, jota käytetään niissä nimenomaan allekirjoituksen tarkoituksessa. Alan kaupallinen terminologia näyttää kuitenkin antaneen varmenteelle laajemman sisällön.

[18] Mm. CWA 14169. Ks. jäljempänä Turvalliset sähköisen allekirjoituksen luomisvälineet, Vaatimusten arviointi, Liikenne- ja viestintäministeriön julkaisuja 52/2004. Ks. myös Komission päätös 2003/511/EY, tehty 14 päivänä heinäkuuta 2003, sähköisiin allekirjoituksiin liittyviä tuotteita koskevien yleisesti tunnustettujen standardien viitenumeroiden julkaisemisesta Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY mukaisesti; EYVL L 175, 15.7.2003, s. 45.

[19] Turvalliset sähköisen allekirjoituksen luomisvälineet, s. 7. Arviointi voidaan suorittaa tapauskohtaisesti kansallisten valvontaviranomaisten toimesta.

2.2.4. Sähköinen tunnistaminen ja sähköinen allekirjoitus

Henkilön sähköinen tunnistaminen on pidettävä erillään allekirjoituksesta. Kuten edellä todettiin, allekirjoituksessa viestin allekirjoittajan sähköinen henkilöllisyys yhdistetään johonkin sähköiseen tietosisältöön ja sähköinen henkilöllisyys ja todellinen henkilön identiteetti on samalla yhdistetty toisiinsa. Sähköisessä tunnistamisessa on kyse jälkimmäisestä vaiheesta, jossa sähköinen ja todellinen henkilöllisyys liitetään toisiinsa. Tunnistamisen asemasta puhutaan joskus myös todentamisesta.

Sähköisen tunnistamisen tekniikoita ovat varmenteiden lisäksi lähinnä käyttäjätunnukseen ja salasanaan, vaihtuviin salasanoihin sekä biometriikkaan[20] perustuvat tunnistamisjärjestelmät.

Fyysisessä maailmassa henkilö tunnistetaan ennen kaikkea henkilöllisyystodistuksen perusteella. Tällöin henkilön on oltava pääsääntöisesti itse paikalla tunnistamistapahtumassa. Sähköisen tunnistamisen menetelmiä käytetään ns. etätunnistamiseen. Sähköisessä maailmassa tunnistamisfunktioita käytetään asiointipalveluissa käyttöoikeutta ja tapahtuman hyväksymistä varten. Tunnistamista koskeva velvollisuus voi seurata lainsäädännöstä. Esimerkiksi rahoitusalalla on lukuisia asiakkaan tunnistamista koskevia lakeja.[21] Terveystietoja voi luovuttaa vain asianosaiselle tai holhoojalle. Tunnistamisvelvollisuus voi olla myös tosiasiallista esimerkiksi vastuuseuraamuksen välttämiseksi. Esimerkiksi kuljetusyrityksen on säännönmukaisesti tunnistettava tavaran rahtikirjaan merkitty vastaanottaja, ellei vastaanottaminen tapahdu siihen oikeuttavaa asiakirjaa, kuten konossementtia, vastaan.

Termiä tunnistaminen voidaan käyttää, kuten aikaisemmassa selvityksessä tehty erottelu osoittaa, sekä autentikoinnin että identifioinnin merkityksessä. Autentikointi perustuu henkilön omaan valintaan eli hän esittää väitteen henkilöllisyydestään. Identifioinnissa taas tunnistetaan kuka henkilö on ilman tämän henkilöllisyydestään esittämää väitettä.[22] Laki sähköisistä allekirjoituksista ei nimenomaisesti käsittele henkilön tunnistamista ilman allekirjoitustarkoitusta.[23] Toisaalta on katsottu, että

[20] Biometriikassa kyse voi olla esimerkiksi sormenjäljestä, kämmenen rakenteesta, kasvotunnistuksesta, silmän iriksestä tai verkkokalvosta, sormen rakenteesta tai äänen tunnistamista.
[21] Luottolaitoslaki(1607/1993), vakuutusyhtiölaki (1062/1979), laki sijoituspalveluyrityksistä (579/1996), sijoitusrahastolaki (48/1999) sekä laki rahanpesun selvittämisestä ja ehkäisemisestä. (68/1998, viimeksi muutettu lailla 365/2003) Sen lisäksi alan viranomaiset ovat laatineet määräyksiä, ohjeita ja kannanottoja.
[22] LVM:n selvitys nro 44/2203.
[23] Tähän liittyvä kysymys on se, voidaanko lain katsoa käsittelevän tiedon autentikoinnin lisäksi myös subjektin autentikointia. Esimerkiksi PIN-koodi, jota käytetään pankkitilin tarkasteluun, ei ole sähköinen allekirjoitus, mutta jos PIN-koodilla tehdään sähköinen allekirjoitus, on se sähköisiä allekirjoituksen määritelmän piirissä.

sähköisiä allekirjoituksia koskevan direktiivin määräykset soveltuvat myös henkilön tunnistamiseen, mikä kanta on tullut esille mm. standardointityössä.[24] Tällä tarkoitetaan sitä, että sähköisten allekirjoitusten ominaisuudet eivät rajoitu tietosisällön ja allekirjoittajan sähköisen identiteetin yhdistämiseen, vaan voivat toimia myös allekirjoittajan identiteetin osoittamiseksi. Direktiivin 5 artiklan 2 kohta on saman artiklan 1 kohtaa selkeämmin kytkettävissä allekirjoitusvälineiden tunnistamisfunktioihin. Tämä tarkoittaa sitä, että määräys, jonka mukaan muut kuin kehittyneet sähköiset allekirjoitukset nauttivat todistusvoimaa, antaa todistusvoimaa tällaisille allekirjoituksille myös puhtaassa henkilön tunnistamistarkoituksessa. Vastaava tulkinta voidaan esittää myös 5 artiklan 1 kohdassa tarkoitetuista kehittyneistä sähköisistä allekirjoituksista.

Yhdeksi keskeiseksi kysymykseksi voidaan nostaa se, tulisiko lain nimenomaista soveltamisalaa laajentaa tunnistamiseen, nimenomaan edellä mainitussa autentikoinnin merkityksessä, jolloin lakiin kirjattaisiin yksityiskohtaisia tunnistamiseen liittyviä vaikutuksia.

Tunnistamisen erikoistapauksena puhutaan yleisesti vahvasta tunnistamisesta, jolloin usein esitetyn nyrkkisäännön mukaan kaksi seuraavasta kolmesta kriteeristä täyttyy:

1) Tunnistettavalla henkilöllä on esittää jokin ominaisuus, joka on vain hänellä ja on osa häntä. (”mitä olet”),
2) tunnistettavalla henkilöllä on esittää jokin tieto, jonka vain hän tietää (”mitä tiedät”); ja
3) tunnistettavalla henkilöllä on esittää jokin fyysinen väline, jonka vain hän omistaa (”mitä sinulla on”)

Kahden kriteerin vaatimus ei kuitenkaan ole ehdoton. Esimerkiksi biometrinen tunnistaminen voi perustua vain yhteen kriteeriin, joka liittyy fysiologisiin ominaisuuksiin. Vahva tunnistaminen on tietoturvakäsite eikä sillä ole pohjaa lainsäädännössä, sillä tunnistamista ei ole säännelty yleisellä tasolla. Käytännössä vahvan tunnistamisen toteuttaminen on kuitenkin oikeudellisesti merkityksellistä, sillä se vaikuttaa tunnistamiseen velvollisen tahon huolellisuuden arviointiin lain tai sopimussuhteen perusteella.

Monet sähköisen allekirjoituksen menetelmät soveltuvat yleisesti henkilön tunnistamiseen, jolloin henkilön identiteettiä ei välttämättä yhdistetä mihinkään tietosisältöön allekirjoitustarkoituksessa,

[24] Ks. Thomas Myhr, Regulating a European eID, A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005, ss. 11-15.

vaan oikeuksiin, kuten esimerkiksi tietojärjestelmään kirjautumiseen ja tietojärjestelmässä olevan tiedon saantiin ja käyttöön. Tunnistetun henkilön halutessa tehdä tahdonilmaisun, joka liittyy johonkin tiettyyn määriteltyyn tietosisältöön, on näihin tarkoituksiin käytössä eri menetelmiä.

Merkille pantava erityismääräys henkilön sähköiseen tunnistamiseen liittyen on sisäasianministeriön asetus rahanpesun estämisestä ja selvittämisestä (89072003), jonka 4 §:ssä säännellään etätunnistamista. Asetuskohdassa todetaan, että ”jos henkilö tai sen puolesta tai asiamiehenä toimiva ei ole läsnä henkilöllisyyttä todennettaessa, henkilön on tunnistauduttava sähköisesti laatuvarmennetta tai muuta tietoturvallista ja todisteellista tunnistautumistekniikkaa käyttäen.” Tämä menetelmä ei kuitenkaan ole sinänsä aina riittävä sillä erityisestä syystä lain mukainen ilmoitusvelvollinen voi etätunnistaa henkilön hankkimalla tämän henkilöllisyyden todentamiseksi tarvittavan selvityksen käyttämällä lähteitä, joista selvitys voidaan luotettavasti saada. ”Muulla tietoturvallisella ja todisteellisella tunnistautumistekniikalla” tarkoitetaan sellaista varmennetta, joka täyttää sähköisestä allekirjoituksesta annetussa laissa (14/2003) laatuvarmenteelle asetetut vaatimukset.[25] Nämä vaatimukset perustunevat käsitteelliseen sekaannukseen. Laatuvarmenteet ovat allekirjoitusvarmenteita, joita siis käytettäisiin tunnistautumistarkoituksiin rahanpesun ehkäisemistä koskevassa yhteydessä. Rahanpesutransaktiot ovat tietenkin oikeustoimia, jotka edellyttävät allekirjoitusfunktion käyttämistä jossakin vaiheessa. Joka tapauksessa säännöksen voidaan katsoa kuvastavan laatuvarmennetasoisen tunnistamisratkaisun käyttökelpoisuutta suurta tietoturvallisuutta vaativassa sähköisessä etätunnistamisessa.

Liikenne- ja viestintäministeriön selvityksessä on kuvattu varmenteisiin perustuva sähköisen tunnistus- ja allekirjoitustapahtumaa seuraavasti:

...rekisteröinti:

1. Henkilön henkilöllisyys varmistetaan rekisteröintipisteessä hyväksyttävällä ja luotettavalla menetelmällä.
2. Henkilölle generoidaan avainpari, julkinen ja yksityinen avain, joista yksityinen avain luovutetaan käyttäjälle. Julkinen avain ja henkilötiedot tallennetaan varmenteeseen, jonka varmentaja sähköisesti allekirjoittaa. Käyttäjälle luovutetaan joko viittaus varmenteeseen tai itse varmenne.
3. Varmenne tallennetaan varmennehakemistoon.

[25] Keskusrikospoliisi, Rahanpesun selvittelykeskus: Rahanpesun torjunnan parhaat käytänteet, s. 14.

...tunnistaminen

4. Tunnistava taho generoi tunnistushaasteen, joka lähetetään tunnistettavalle henkilölle sähköisesti allekirjoitettavaksi.
5. Käyttäjä allekirjoittaa tunnistushaasteen eli salaa sen omalla yksityisellä avaimellaan. Allekirjoitus ja käyttäjän varmenne tai viittaus varmenteeseen lähetetään tunnistavalle taholle.
6. Tunnistava taho noutaa varmennehakemistosta käyttäjän ilmoittaman varmenneviittauksen perusteella käyttäjän varmenteen, jos käyttäjä ei ole sitä allekirjoituksen yhteydessä itse toimittanut.
7. Tunnistava taho tarkastaa varmenteen voimassaolon ja muuttumattomuuden. Voimassaolo tarkistetaan voimassaolopäiväyksestä sekä varmistamalla, että varmenne ei ole sulkulistalla. Sulkulista on varmennehakemiston yhteydessä. Varmenteen muuttumattomuus tarkastetaan tarkastamalla varmenteen myöntäjän varmenteeseen tekemä sähköinen allekirjoitus. Jos varmenteen voimassaoloaika on päättynyt, varmenne on sulkulistalla tai varmenteen myöntäjän tekemän sähköisen allekirjoituksen tarkastaminen epäonnistuu, käyttäjän tunnistaminen epäonnistuu.
8. Jos varmenne on hyväksyttävästi tarkastettu, tunnistava taho tarkastaa käyttäjän toimittaman tunnistehaasteen allekirjoituksen. Tällöin salattu tunnistushaaste eli allekirjoitus puretaan varmenteessa olevalla julkisella avaimella. Jos salauksen purun tuloksena saatu vastine on identtinen alkuperäisen tunnistushaasteen kanssa, tunnistus hyväksytään.

...allekirjoitus

9. Allekirjoittava taho generoi allekirjoituksen ja lähettää sen ja käyttämänsä varmenteen tai viittauksen varmenteeseen luottavalle osapuolelle.[26]
10. Luottava osapuoli noutaa varmenteen, jos sitä ei ole aikaisemmin toimitettu, sekä sulkulistan.
11. Luottava osapuoli tarkastaan varmenteen voimassaolon päiväyksestä ja ettei sitä ole merkitty sulkulistalle. Varmenteen eheys tarkistetaan varmentajan sähköisestä allekirjoituksesta.
12. Salattu tietosisältö puretaan varmennettavan varmenteessa olevalla julkisella avaimella.[27].

[26] Allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste allekirjoittajan salaisella avaimella. Salattu tiiviste eli sähköinen allekirjoitus liitetään välitettävän aineiston mukaan. Aineiston eteen liitetään otsikkokenttä, joka kertoo lähettäjän.
[27] Luottava osapuoli purkaa julkisella avaimella salatun tiivisteen, laskee vastaanottamastaan tietoaineistosta tiivisteen ja vertaa näin saamiaan tiivisteitä toisiinsa. Ks. TIVEKE - Tietoturva, http://palvelut.tieke.fi/arkisto/tiveke/turva/turva-2.htm

Varmentaminen tunnistamis- ja allekirjoitustarkoituksiin ovat selkeästi toisistaan erotettavia tapahtumia. Niitä varten käytetään esimerkiksi Väestörekisterikeskuksen kansalaisvarmenteessa eri pinlukuja. Tunnistamis- ja allekirjoitusvarmenteita tarjotaan siis kaupallisesti yhdessä, mutta oikeudellisesti tunnistamisvarmenne ei ole laatuvarmenne kun taas allekirjoitusvarmenne on sitä. Eri käyttötarkoitukset ja varmentajan sitoutuminen tuodaan esille sopimuksessa ja varmennepolitiikassa, joka ilmaisee, mihin varmentaja sitoutuu. Aivan pelkästään tunnistamiseen käytettävästä varmenteesta ei voida tehdä ilmoitusta Viestintävirastolle laatuvarmenteiden tarjoamisesta, koska lakia ei sovelleta varmenteisiin, joilla ei voida lainkaan tehdä allekirjoituksia. Koska allekirjoituksella on säännönmukaisesti oikeusvaikutuksia, on allekirjoituksen merkitystä korostava tietokoneruutuun tuleva ilmoitus käytössä esimerkiksi Viron digitaalisen allekirjoituksen toteutuksessa. Kuitenkin teknisesti tunnistautumis- ja allekirjoitusvarmenne vastaavat pitkälle toisiaan. Väestörekisterikeskuksen varmennepohjaiseen sähköiseen tunnistamiseen ja allekirjoitukseen pätevätkin samat tietoturvatasot.

TUPAS2 -standardiin perustuvat pankkitunnisteet ovat käytössä sekä tunnistautumis- että allekirjoitustarkoituksissa. Esimerkiksi Sampo Pankin palveluavaimet sisältävät asiakasnumeron, jotka yhdessä pin-luvun kanssa vastaavat asiakkaan perinteistä tunnistamista henkilöllisyyttä osoittavasta asiakirjasta, ja kertakäyttöinen turvaluku taas on käytössä allekirjoitettaessa asiakirjoja sähköisesti. Pankkitunnisteita on sekä yritys- että yksityiskäytössä.[28] Jos käyttäjätunnus on henkilö- eikä organisaatiokohtainen, yhdistyy pankkitunnisteeseen roolitunnistus.

Aina ei allekirjoitusfunktiota palveluissa kuitenkaan käytetä, vaan tunnistetun henkilön tahdonilmaisun olemassaolo todetaan käytännössä muulla tavoin, esimerkiksi verkkosivulla tai sovelluksessa olevaa ikonia painamalla tai muutoin, jolloin tunnistamisessa käytetyllä menetelmällä on myös eräänlainen tahdonilmaisuun liittyvä tunnistusfunktio. Tällainen allekirjoitusjärjestely, joka on käytössä mm. Nordea Rahoituksessa, perustuu säännönmukaisesti palvelun tarjoajan ja käyttäjän väliseen sopimukseen, jossa tunnistautuvan henkilön rooli ilmenee tunnisteesta.

Kun tunnistautuminen tehdään tapahtuman hyväksymistä varten, voidaan tunnistautumisen katsoa olevan osa tahdonilmaisua, ellei tätä varten ole luotu erillistä, yleensä korkean tietoturvatason menettelyä. Esimerkiksi fyysiseen tilaan pääsyyn voidaan yhdistää maksutapahtuma siten, että tilaan saapuminen aktivoi maksun. Liikenne- ja viestintäministeriön selvityksessä ´Sähköisen tunnistami-

[28] Sammon allekirjoituspolitiikka, http://www.sampo.fi/ehdot/suomi/copy2.html, vierailtu 2.3.2005.

sen menetelmät ja niiden sääntelyn tarve´ todetaan että teknisessä mielessä ainoa riittävän turvallinen ja kiistämätön menetelmä on varmennepohjainen sähköinen allekirjoitus, koska menetelmän avulla asiointiosapuolet voivat todentaa allekirjoitetun sopimuksen sisällön ja allekirjoittajan henkilöllisyyden. Tällä tarkoitetaan kuitenkin nimenomaisesti teknistä kiistämättömyyttä, koska allekirjoitus yhdistetään tietosisältöön yksiselitteisesti. Käytäntö ei kuitenkaan näytä seuranneen tätä, vaan esimerkiksi pankkitunnisteita käytettäessä allekirjoituksen pätevyyttä ja kiistämättömyyttä voidaan tavoitella palvelusopimuksissa olevin määräyksin. Pankkitunnisteiden käyttöön liittyvät allekirjoitusmenetelmät saavat kauppatapaan rinnastettavaa uskottavuutta, mutta toisaalta niitä ei ole oikeudellisesti testattu peruuttamattomuuden eikä allekirjoitetun tietosisällön määrittelyn osalta. Erityisesti kuluttajasuhteissa voidaan kiistämättömyys kyseenalaistaa. On myös huomattava, että rahanpesun estämisestä ja selvittämisestä annetun sisäasianministeriön asetuksen (890/2003) 4 §:ssä tarkoitettu sähköinen etätunnistaminen ei olisi mahdollista kuin varmenneratkaisuilla, joskin tällainen tulkinta perustuu lähinnä KRP:n Rahanpesun selvitelykeskuksen julkaisemiin Rahanpesun torjunnan parhaisiin käytänteisiin[29], jotka on muotoiltu ristiriitaisella tavalla.

2.2.5. Varmenneorganisaation tarjoamia lisäpalveluita

Varmennustoiminta voi käsittää erilaisia lisäpalveluita. Näitä ovat esimerkiksi aikaleimapalvelut, sähköisten asiakirjojen notariaattipalvelut, asiakirjojen arkistointi, riitojenratkaisupalvelut, pääsynvalvontaa tukevat palvelut, salakirjoitusohjelmistojen levittäminen sekä key escrow ja key recovery-palvelut[30].

29

http://www.poliisi.fi/intermin/images.nsf/files/111880F83D17EDF3C2256E36002E3A0B/$file/Rahanpesun+torjunnan+parhaat+käytänteet.pdf, vierailtu 14.4.2005. Asiakkaan tunnistamista koskevat yhteisötason säännökset jättävät kansallisen tason harkintaan tunnistamismenetelmät. Neuvoston direktiivi 308/91/ETY rahoitusjärjestelmän rahanpesutarkoituksiin käyttämisen estämisestä vaatii 3 artiklassa todistusvoimaisen asiakirjan käyttämistä tunnistamiseen. Direktiiviä ollaan uusimassa, ja komission ehdotuksen (KOM(2004) 448 lopullinen) mukaan vaaditaan tunnistamista ”luotettavien ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen” perusteella. Aina ei mekaaninen etätunnistaminen kuitenkaan riitä, vaan ehdotuksessa mainituissa tapauksissa rahalaitoksen tulisi suorittaa muita varmistustoimenpiteitä.

30 Key-Escrow/Key Recovery-järjestelmässä valtuutetulle taholle voidaan tietyissä tapauksissa antaa mahdollisuus salatun liikenteen tai aineiston purkuun. Järjestelmässä yksi tai useampi luotettu osapuoli säilöö salaiset avaimet tai palautusavaimet (recovery keys), joiden avulla voidaan määrittää salauksessa tai sen purussa käytetty avain.

3. VARMENTEITA ERI TARKOITUKSIIN

3.1. Väestörekisterikeskuksen laatuvarmenteet

Toimeksiantoon on kuulunut selvittää, mitä lain soveltamisalaan kuuluvia toimijoita ja palveluja/tuotteita (laatuvarmenteet ja muut varmenteet sekä niihin liittyvät tuotteet, muut sähköisen allekirjoituksen toteutukset) erityisesti Suomen markkinoilla on tällä hetkellä.

Julkinen sektori on näytellyt keskeistä roolia lain toteuttamisessa. Väestörekisterikeskus, joka on ensimmäinen ja tällä hetkellä ainoa laatuvarmentaja Suomessa, tarjoaa käyttötarkoituksesta riippuen

- **työ- tai organisaatiovarmenteita**, jotka sisältävät laatuvarmenteen allekirjoitustarkoitusta varten ja muun varmenteen tunnistamiseen, ja
- **kansalaisvarmenteita,** jossa on laatuvarmenne allekirjoitustarkoistuksiin ja muu varmenne tunnistamiseen. Varmenteissa on ilmaistu sen käyttötarkoitus, ja varmentajan vastuu määräytyy tämän käyttötarkoituksen mukaan.

Väestörekisterikeskuksen kansalaisvarmenne perustuu sirukorttalustan käyttöön. Sen jälkeen kun sirullisen henkilökortin käyttöä edistävät lakimuutokset astuivat voimaan 1.9.2003, otettiin käyttöön uusi viisi vuotta voimassa oleva sirullinen henkilökortti. Kaikki henkilökortit ovat nykyisin sirullisia. Sirullinen henkilökortti ja Kela-kortti yhdistyivät kesäkuussa 2004 niin, että kansalaiset voivat halutessaan saada sairausvakuutustiedot painettuina henkilökortin pintaan. Sähköistä henkilökorttia kutsutaan yleisesti HST-kortiksi. HST-kortti sisältää mm. kansalaisvarmenteen[31], haltijansa nimen ja sähköisen asiointitunnuksen, haltijansa julkisen avaimen, voimassaoloajan sekä varmentajan allekirjoituksen ja lisäksi muut lain vaatimat asiat. Kortilla oleva siru sisältää haltijansa kaksi yksityistä avainta, haltijan varmenteen, joka on myös saatavissa julkisesta hakemistosta, sekä varmentajan varmenteen.[32]

Huhtikuun 2005 loppuun mennessä markkinoilla olevien laatuvarmenteiden lukumäärä oli 62 012 kappaletta. Kortin hinta on 40 euroa. Kortti käy sähköiseen asiointiin ja lisäksi matkustusasiakirjana

[31] Varmenne on tyyppiä X.509v3.

Pohjoismaissa, EU-maissa, Sveitsissä ja San Marinossa. Sähköinen asiointi edellyttää kuitenkin kortinlukijaohjelmistoa ja lukulaitetta. Ohjelmiston voi ladata Väestörekisterikeskuksen verkkosivuilta, mutta lukulaite tulee lunastaa käyttöön 15 euroa hinnasta. Sähköisen henkilökortin myöntää poliisi ja sitä sääntelee väestötietolain (507/1993) 23 §, sekä henkilökorttilaki (829/1999).

Kansalaisvarmennetta voi käyttää eri alustoilla ja kanavariippumattomasti. Lokakuussa 2004 tuli OP-pankkiryhmän asiakkaille mahdolliseksi saada kansalaisvarmenne Visa Electron-maksukorttiin. Lisäksi Väestörekisterikeskus on kehittänyt yhteistyössä kolmen operaattorin, Telia Sonera Finland Oyj:n, Elisa Oyj:n ja DNA:n kanssa mobiilikansalaisvarmenteen käyttöön perustuvaa matkapuhelin palvelua sähköiseen tunnistamiseen ja allekirjoitukseen.

3.2. Kansalaisvarmenteen käytön edistäminen

HST-ryhmä, joka perustettiin vuonna 2002, ja joka jatkaa niin kutsutun Pro HST -ryhmän käynnistämää yhteistyötä on avoin, kansalaisvarmenteen yleistymistä edistävien sirukorttien liikkeellelaskijayhteisöjen muodostama yhteistyöelin. HST-ryhmän jäseneksi voi periaatteessa liittyä useitakin laatuvarmentajia, joiden kanssa kehitetään varmenteiden yleistä käytettävyyttä ja tunnettuutta.

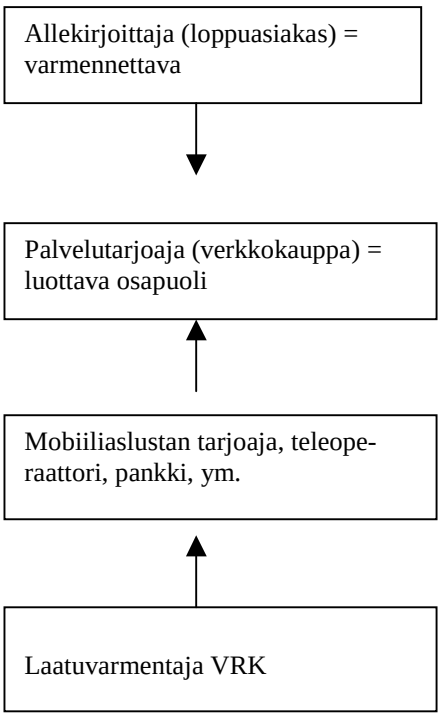
HST-ryhmän jäseniä ovat tällä hetkellä Luottokunta, DNA Finland Oy, Elisa Oyj, Osuuspankkikeskus - OPK osuuskunta, Svenska Handelsbanken Ab (julk.) Suomen sivukonttoritoiminta, Säästöpankit ja paikallisosuuspankit, TeliaSonera Finland Oyj sekä Väestörekisterikeskus.

HST-ryhmän päämääränä on kehittää kansalaisvarmenteen ja muidenkin laatuvarmenteiden yleistymistä ja yleiskäyttöisyyttä siten, että niiden käyttö on kustannustehokasta, luotettavaa ja helppoa sekä kuluttajalle, asiointipalvelun tarjoajalle, sirukortin liikkeellelaskijalle että varmentajalle. Ryhmä pyrkii myös eri tavoin edistämään yhteistyötä sähköisten asiointipalvelujen tarjoajien kanssa, jotta avoimeen tietoverkkoon voidaan luoda henkilökohtaisia asiointipalveluja ja siten toteuttaa todellisia vaihtoehtoja erilaisine turvallisuusratkaisuineen nykyisille palvelutavoille. Jatkuvasti kehittyvän teknologian tarjoamat mahdollisuudet tulee ottaa huomioon. Tavoitteisiin pyritään mm. pilottihankkeiden ja työryhmätyöskentelyn avulla. Ryhmä on ollut mukana tukemassa mm. Hämeenlinnan seudun HST-hanketta (ks. jäljempänä).

[32] HST-varmenteiden ”osapuolia” ovat varmentaja eli Väestörekisterikeskus, kortin valmistaja ja yksilöijä eli Setec, varmennehakemiston ylläpitäjä Elisa, sulkupuhelinpalvelun ylläpitäjä Luottokunta, rekisteröijä eli poliisi sekä itse varmenteen haltija. Varmennejärjestelmän tuottaa Fujitsu Oyj.

HST-ryhmän alatyöryhmiä ovat arkkitehtuurit ja liiketoimintamallit -työryhmä, viestintä ja markkinointi -työryhmä sekä palveluiden tarjoajat -työryhmä, johon kuuluu myös HST-ryhmän ulkopuolisia jäseniä.[33]

Kansalaisvarmenne on tulossa käyttöön myös mobiilivarmenteena. Tämä tarkoittaa sitä, että matkapuhelinoperaattori tarjoaa palveluntuottajille ja matkapuhelimen käyttäjille allekirjoitus- ja tunnistautumispalvelua, joka perustuu VRK:n laatuvarmenteelle ja operaattorin älykorttialustalla eli liittymäkortilla oleville varmennetoiminnallisuuksille. Tätä oli edeltänyt keskustelu siitä, mikä kortti toimisi varmenteen käyttöalustana. Kansalaisvarmenne tulee kännykän sirukorttiin, jota haetaan operaattorilta erikseen (mahdollisesti yksi tai kaksi korttipaikkaa käytössä). Lisäksi sim -kortille tulee mahdollisesti operaattoreiden omia varmenteita. Esimerkkinä mobiilivarmenteen käyttötarkoituksesta on tilanne, jossa Internet-sivulla voidaan pyytää tunnistautumaan kännykällä, jolloin verkkopalvelin yhdistää kännykkään tunnistamista ja/tai allekirjoitusta varten. Palvelu voi siis olla joko mobiilipalvelu tai pc-käyttöliittymää hyödyntävä palvelu, jossa tunnistaminen tai allekirjoitus hoidetaan matkapuhelimen avulla. Mobiilivarmenteessa muodostuu Suomessa seuraava rakenne:



[33] Työryhmän kokoonpano on Kesko Oyj, Suomen Osuuskauppojen Keskuskunta SOK, Finnair Oyj, MTV Oy, Elisa Oyj, Finnet Oy, TeliaSonera Finland Oyj, Svenska Handelsbanken Ab (julk.) Suomen sivukonttoritoiminta, Osuuspankkikeskus - OPK osuuskunta, Yliopiston Apteekki, KohdematkatKaleva Oy, TietoEnator Oyj, Espoon kaupunki, Kaupan Keskusliitto ja Väestörekisterikeskus.

Keskeisiä sopimussuhteita tässä yhteydessä ovat:

1) Loppukäyttäjä, tässä allekirjoittaja ← etämyyntisopimus → palveluntuottaja (luottava osapuoli)
2) Loppukäyttäjä, tässä alustan haltija ← sopimus varmenneominaisuuksilla varustetusta liittymäkortista → Operaattori (korttialustan liikkeellelaskija)
3) Loppukäyttäjä, tässä varmenteen haltija ← kansalaisvarmennesopimus → Varmentaja
4) Palveluntuottaja ← tunnistamis - ja allekirjoituspalvelusopimus → Operaattori (tunnistamis- ja allekirjoituspalvelun tarjoaja)
5) Operaattori ← sopimus mobiileista kansalaisvarmenteista operaattorin liittymäkorttialustalla→ Varmentaja

Kun käyttäjillä on eri operaattorien liittymät, yhteentoimivuus toteutetaan ”roamaamalla” varmenteet tekstiviestikanavaa pitkin. Operaattorit voivat välittää allekirjoitus- ja tunnistamispalveluja useiden eri operaattoreiden loppukäyttäjille. Tähän yhteyteen on myös vakioitu lisäpalveluja.

Helmikuun puolivälissä 2005 tehtiin Suomen ja maailman ensimmäinen laatuvarmenteisiin perustuvan ETSI-standardien mukaisen mobiilin allekirjoituspyynnön välittäminen operaattorin verkkorajojen yli. Operaattoripuolelta on esitetty näkemys, jonka mukaan siinä vaiheessa kun suomalainen toteutus saadaan sellaiseen vaiheeseen, että se tarjoaa perustoiminnallisuuden ohella myös istunnon integriteetin turvaa ja roskapostin estoa, niin ko. suositus voidaan julkaista julkiseen käyttöön ja mobiilit sähköiset allekirjoituspyynnöt ja allekirjoitukset, sekä tunnistukset saadaan ”roamaamaan” eli toimimaan verkkorajojen yli. Tällöin tilanne on teknisesti analoginen tekstiviestien lähettämisen kanssa sujuvasti yli operaattorien verkkorajojen.

Väestörekisterikeskus tarjoaa varmenteita myös muille alustoille, tällä hetkellä ainakin virkamieskortille. Kesäkuun 1 päivänä 2004 voimaan tulleen väestötietolain muutoksen myötä henkilökortti ja sairausvakuutuskortti on voitu yhdistää yhdeksi yhteiseksi valtion viranomaisen antamaksi sähköisessä asioinnissa käytettäväksi asiointikortiksi.

Muita kotimaasta käsin toimivia varmennepalvelujen tarjoajia ovat Sonera CA ja Elisa.

3.3. Mitä varmenteita on käytössä?

Kyselyssä tuli selvittää, mikä on laatuvarmenteiden ja ja muiden varmenteiden hyödyntämisen välinen ero, eli mihin tarkoituksiin henkilökorteilla olevia allekirjoitusvarmenteita (laatuvarmenne) ja henkilökorteilla olevia tunnistamiseen käytettäviä varmenteita (ei-laatuvarmenne) käytetään ja mitkä ovat keskeiset syyt mahdollisiin eroihin.

Seuraavassa organisaatiokohtaista palautetta siitä, ketkä käyttävät laatuvarmenteita ja muita varmenteita tänä päivänä. Tilanne elää luonnollisesti koko ajan ja jotkut yksityiskohdat saattavat olla muuttuneet jo ilmoitusajankohdan jälkeen.

3.3.1. Valtionhallinto, ministeriöt ja valtion laitokset

- Valtiovarainministeriössä ei ole käytössä sähköisen allekirjoituksen toteutuksia. Laatuvarmenteita käytetään tunnistauduttaessa verkkoon VPN-etäyhteydessä osassa organisaatiota ja eräiltä osin luottamuksellista sähköpostia salattaessa ja purettaessa.

  Sisäasiainministeriö käyttää varmenteita tiimipostissa. Kuluvan vuoden aikana otetaan kuitenkin käyttöön sähköiset asiointikortit, jotka perustuvat VRK:n laatuvarmenteeseen, ja joilla on 18.000 käyttäjää sekä keskitetty käyttöoikeuksien hallintajärjestelmän. Ministeriö tulee käyttämään varmennetta tunnistamiseen, allekirjoitukseen ja salaukseen. Useimmissa omissa palveluissa ja asiakkaille suunnatuissa palveluissa otetaan käyttöön asteittain yhtenä vaihtoehtona kansalaisvarmenne. Tällä hetkellä hanke on edennyt niin, että tuotantokäytössä on jo nyt maistraateissa n. 300 - 400 varmennetta, VRK:ssa noin 120 sekä etätyössä ja pilottikäytössä noin 200 varmennetta.

- VRK käyttää itse kansalais- ja organisaatiovarmenteita. Asiointikortti sisältää organisaatiovarmenteen, jossa on myös allekirjoitustarkoituksiin käytettävä laatuvarmenne.

- Viestintäviraston työntekijöillä on käytössä VRK:n organisaatiovarmenteeseen perustuva sirukortti. Viestintävirastossa on käytössä myös PGP-ohjelmisto, jolla voidaan salata ja allekirjoittaa sähköpostiviestejä ja asiakirjoja. Sirukorttia voidaan käyttää myös verkkoon kirjautumisessa. Sähköisten allekirjoitusten osalta mahdollisuuksia myös muiden asiakirjojen kuin sähköpostiviestien, lähinnä viraston sisäisten lomak-

keiden, sähköiseen allekirjoittamiseen ollaan kartoittamassa. Tällä hetkellä Viestintävirastossa käytetään tunnistautumisvarmennetta verkkoon kirjautumiseen sekä sähköpostiviestien salaamiseen ja allekirjoittamiseen. Allekirjoitusvarmenne ei ole käytössä Viestintävirastossa.

- Tullilaitoksessa on sähköisten allekirjoitusten sovellusten käyttö näköpiirissä, mutta käyttöä ei vielä ole.

- Rahoitustarkastuksen käytössä ei ole sähköisen allekirjoituksen sovelluksia. Henkilökunnan PKI-pohjaista toimikorttia käytetään organisaation sisäisessä toiminnassa tunnistautumiseen. Salaukseen käytetään PGP-varmenteita.

3.3.2. Erityisesti terveydenhuolto ja sosiaalitoimi

- Terveydenhuollon oikeusturvakeskus tulee laatimaan STM:n toimeksiannosta vuosina 2005 - 2006 terveydenhuollon valtakunnallisen **ammattivarmenne**palvelun, jonka kokeilukäyttö alkaa vuonna 2005. Tuotantokäyttöön ammattivarmenne tulee mm. sähköisen reseptin järjestelmässä, jonka piirissä käyttäjinä tulee olemaan yhteensä noin 30.000 lääkärien, hammaslääkärien ja farmasian alan ammattihenkilöä. Näköpiirissä on kuitenkin käyttäjämäärän kasvu yli sadan tuhannen, kun sairaanhoitajatason ammattihenkilötkin tulevat mukaan käyttäjiksi. Suunnitteilla oleva varmennepalvelu kattaa sekä julkisen että yksityisen terveydenhuoltosektorin. Tavoitteena on aikanaan laajentaa kehitettävä ammattivarmennemenetelmä tarvittavassa laajuudessa myös sosiaalihuollon puolelle.

- Pohjois-Karjalan sairaanhoitopiirissä on käytössä sähköinen allekirjoitus. Sovellus on Avaintechnologies-tuote *X-sign*, ja salausmenetelmä perustuu PKI:hin. Allekirjoitus on käytössä potilasjärjestelmä HealthNetissä. Siellä allekirjoitusta käytetään sähköreseptipilotissa sekä erilaisten projektien testeissä. Toteutuksessa on kyse allekirjoituksesta, tunnistus tapahtuu erikseen sovellusohjelmaan kirjautuessa. Laatuvarmenteita käytetään sähköreseptipilotissa ja erilaisten projektien testeissä, tunnistautumisvarmenteita käytetään joissakin organisaatioiden välisissä yhteyksissä VPN-putken muodostamiseen. Kokeilussa henkilökorttiin kytketty laatuvarmenne varmentaa henkilön statuksen lääkärinä. Resepti kirjoitetaan kehittyneellä sähköisellä allekirjoituksella.

- Varsinais-Suomen sairaanhoitopiiri on laatinut oman varmennepolitiikan,[34] joka kattaa piirin omille avaimille myönnettyjä varmenteita, joiden varmentaja on sairaanhoitopiiri itse. Varmennepolitiikka ei liity sähköisistä allekirjoituksista annetun lain mukaisiin laatuvarmenteisiin ja varmenteiden käyttö rajoittuu asiointiin Varsinais-Suomen sairaanhoitopiirin kanssa.

- KELA viittaa vastauksessaan e-reseptipilottiin, jossa tunnistaminen ja allekirjoitus on erotettu toisistaan. E-reseptissä on käytössä VRK:n ja Terveydenhuollon oikeusturvakeskuksen varmentama ammattilaiskortti. Tunnistaminen mahdollistaa lääkärille ja farmaseutille/proviisorille sisäänkirjautumisen järjestelmään ja allekirjoituksella varmistetaan tallennetut tiedot. KELA:n omissa sähköisissä asiointipalveluissa käytetään Verohallituksen ja Työvoimatoimiston kanssa yhteistyössä toteutettua ns. Katve-tunnistusta, jossa tällä hetkellä hyväksytään pankkitunnisteet ja VRK:n kansalaisvarmenne. Laatuvarmenteen käyttö on ollut korttikannan vähäisyyden takia vähäistä, kenties yhden prosentin luokkaa.

3.3.3. Kunta- ja paikallissektori

- Hämeenlinnan seudun HST-hankkeessa on luotu palveluportaali eli *Aina.fi*- asiointitiympäristö, joka tarjoaa yhteyden varmennekortilla toimiviin sekä eräisiin muihin palveluihin. Palvelut on eritelty erikseen yksityishenkilöille ja yhteisöille.[35] Aina.fi-portaalista on yhteys mm. Osuuspankin verkkosivuille, Keskon Plussa-sivuille, eri viranomaisiin sekä alueen kirjastoihin.

- Pääkaupunkiseudun kaupungeilla on tarkoitus toteuttaa yhteishanke, jonka tuloksena pääkaupunkiseudun asukkaiden ja kunkin kaupungin välisessä asioinnissa olisi käytössä vahva tunnistus ja sähköinen allekirjoitus vuoden 2005 loppuun mennessä.

- useiden kuntien tietyt palvelut, kuten päivähoitohakemusten tekeminen, onnistuvat HST- kortin avulla tapahtuvan tunnistautumisen avulla.

[34] Varsinais-Suomen sairaanhoitopiirin varmennepolitiikka, Versio 1.0, 09.10.2003
[35] Ks. http://betula.htk.fi/ainaasiointi/service/ainaasiointi/public/main.vm?pageid=0.

3.3.4. Palvelut yrityksille, julkisen rahoituksen hakeminen

- Raha-automaattiyhdistyksessä on tutkittu lain mukaisen sähköisen allekirjoituksen käyttöä lähinnä avustustoiminnan sähköisen asioinnin palveluita suunniteltaessa. Toistaiseksi RAY:llä ei ole ollut käyttöä laatuvarmenteille sähköistä allekirjoitusta varten. Sen sijaan tunnistautumisvarmenteita RAY:ssä käytetään mm. henkilöiden ja automaattien etäyhteyksissä.

- Suomen Akatemialle ja TEKES:ille osoitetut rahoitushakemukset voidaan allekirjoittaa sähköisesti laatuvarmenteella.

3.3.5. Muita palveluita yrityksille

- Patentti- ja rekisterihallituksen palveluissa voi käyttää HST-korttia patenttihakemusten tekemiseen. Patenttihakemuksia tekevät lähinnä patenttiasiamiestoimistot. Käytössä on sekä tunnistautumis- että allekirjoitusvarmenne. Sähköisen patenttihakemuksen lähettämisen voi tehdä tunnistautumisvarmenteen avulla, sen sijaan allekirjoitusvarmenne tarvitaan itse hakemuksen allekirjoittamiseen. Patentti- ja rekisterihallitus on neuvotellut Euroopan patenttiviraston EPO:n kanssa järjestelyn, jossa HST-korttia voidaan käyttää myös EPO:n suuntaan. Patentti- ja rekisterihallituksessa on vireillä myös projekti yhdistysrekisterissä asioinnin mahdollistamisesta sähköisessä muodossa.

- Maatalousyrittäjien eläkelaitoksen MELA:n palvelut ovat yrityskäytössä HST-kortin avulla (tunnistautumisvarmenne). Sähköisen tunnistautumisen jälkeen asiakas pääsee katsomaan laskelmaa maatalousyrittäjän eläkkeestä ja ansioluettelosta.

- Elma TYVI on yrityksille ja yhteisöille tarkoitettu palvelu, jonka avulla ne voivat tehdä sähköisiä ilmoituksia viranomaisille ja muita lakisääteisiä tietoja keräävälle viranomaisille. HST-kortit liitetään ElmaTYVI-palvelun käyttäjätunnuksiin. Järjestelmä yhdistää tämän tunnuksen HST-korttiin ja yhteen HST-korttiin voi olla sidoksissa vain yksi TYVI-käyttäjä ja yhteen TYVI-käyttäjään voi olla sidoksissa vain yksi HST-kortti. Ilmoitusten teko voisi sisältää allekirjoitusfunktion, mutta tätä ei näytä vaadittavan, vaan tunnistautuminen ja erillinen ilmoitusikonin painaminen riittävät.

3.3.6. Palvelut yksityisille

- Muuttoilmoituksen postiin ja maistraattiin voi tehdä sähköisesti HST-kortilla. Allekirjoitusvarmenne ei ole käytössä.

- Postin verkkopalveluja käytettäessä voi tunnistautua HST-kortilla, pankkitunnuksin tai postin käyttäjätunnuksilla.

- Valtakunnallinen lomakepalvelu, Lomake.fi, välittää HST-kortilla toimivia palveluja. Suurin osa Lomake.fi-palvelusta on käytettävissä ilman tunnistautumista. Palvelu sisältää kuitenkin myös toimintoja, jotka edellyttävät käyttäjän tunnistamista. Tällaisia toimintoja ovat esimerkiksi käyttäjän oma arkisto ja joidenkin verkkolomakkeiden täyttäminen ja allekirjoittaminen. Oman arkiston käyttö edellyttää tunnistautumista sirullisen henkilökortin avulla. Verkkolomakkeiden allekirjoittaminen voi tapahtua lomakkeesta riippuen joko sirullisella henkilökortilla tai verkkopankkitunnisteilla. Verkkopankkitunnisteet mahdollistavat myös maksun tekemisen lomakkeen täyttämisen yhteydessä. Allekirjoitustavan määrittelee aina lomakkeen tuottanut organisaatio. Allekirjoitus- ja tunnistusfunktiot eivät kuitenkaan ole selkeästi eriteltyjä.

- Yksityinen henkilö on voinut tarkistaa työeläketietonsa Eläketurvakeskuksessa.[36] On myös luotu työeläkejärjestelmän yhteinen tunnistuspalvelu, jossa HST-kortilla tai verkkopankkitunnuksilla voidaan päästä Melan, työeläke.fi:n, Kuntien eläkelaitoksen, Eläke-Fennia Onlinen, Varman Eläkearvio-palvelun ja Merimieseläkekassan palveluihin.

- Työvoimatoimistossa asioiminen on mahdollistettu HST-kortin ja verkkopankkitunnusten avulla. Sama koskee verohallintoa ja Kansaneläkelaitosta. Kyse on tunnistautumisesta.

[36] Tämä palvelu, www.tyoelake.fi, on menestynyt myös EU:n sähköisen hallinnon kilpailussa, jossa se selvisi viiden parhaan joukkoon.

- Väestörekisteritietojen tarkistaminen HST-kortin avulla on mahdollistettu. Tällöinkin kyse on tunnistautumisesta.

3.3.7. Yksityinen sektori, operaattorit, tietoliikenneteollisuus ja teknisten palveluiden tarjoajat

- Elisa Oyj:ssä on organisaation sisäisessä käytössä sähköisen allekirjoituksen ja tunnistamisen mahdollistava organisaation toimikortti (henkilökortti). Varmentajana toimii Elisa itse. Myönnetyt varmenteet eivät ole laatuvarmenteita. Sähköisen allekirjoituksen ja tunnistamisen toiminnot on erotettu toisistaan. Käytössä olevat sovellukset ovat työasemaan ja lähiverkkkoon kirjautuminen, etäyhteydelle kirjautuminen ja sähköpostin salaus ja allekirjoitus. Tällä hetkellä laatuvarmenteita ei ole organisaation sisäisessä käytössä.

- TeliaSonera Oyj on mukana mobiilikansalaisvarmennetta koskevassa hankkeessa ja tarjoaa mobiileihin kansalaisvarmenteisiin perustuvia tunnistamis- ja allekirjoituspalveluja liittymäasiakkailleen ja sähköisten palvelujen tarjoajille.

- TeliaSonera toimii itse myös varmentajana (Sonera CA) ja tarjoaa organisaatiovarmenteita (toimikortti, USB token, mobiilivarmenne ja ohjelmistovarmenne). Lisäksi Sonera CA myöntää palvelinvarmenteita sähköisissä palveluissa. Varmenteita voidaan käyttää esimerkiksi sähköpostissa, työasemaan sisäänkirjautumisessa ja etäyhteyksissä. Sonera CA:n myöntämiä mobiilivarmenteita voidaan hyödyntää organisaatiokäyttöön tarkoitetuissa sähköisissä allekirjoituksissa ja henkilön tunnistamisessa. Sonera ilmoittaa, että vaikka sen itsensä liikkeelle laskemat mobillivarmenteet eivät ole laatuvarmenteita, sovelletaan niiden myöntämisessä ja teknisessä toteutuksessa laatuvarmennekriteerejä. Sonera tarjoaa sähköisten palvelujen tuottajille myös lomakepalveluja, joiden osana voidaan hyödyntää sähköisiä allekirjoituksia.

- Nokia Group ilmoittaa, ettei sen käytössä ole tällä hetkellä laatuvarmenteita. Sen sijaan muita varmennesovelluksia käytetään yhtiössä ohjelmistopakettien eheyden ja alkuperän varmistamiseen.

- Segco Oy:n käytössä on sähköisen allekirjoituksen sovelluksia ja yhtiö tarjoaa palve luita, joilla tuotetaan allekirjoitusvarmenteita. Käytetyissä toteutuksissa on kyse sekä

tunnistamisesta että allekirjoituksesta ja salauksesta. Segco ei käytä laatuvarmenteita muutamaa palvelua lukuun ottamatta. Tunnistamisvarmenteita käytetään käyttäjätunnistukseen, tietoliikenteen salaamiseen ja sähköpostin salaukseen ja allekirjoitukseen.

- Valimo Wireless Ltd ilmoittaa, että sovelluksia ja palveluita on tarjolla ja käytössä on tunnistus- ja allekirjoitusratkaisuja, kuitenkin allekirjoittaminen on vasta alkuvaiheessa ja tarve on keskittynyt ensisijaisesti tunnistamiseen. Valimo Wirelessin käytössä on laatuvarmenteita ja yhtiö on myös organisaatiolaatuvarmenteiden osalta VRK:n jälleenmyyjä. Yhtiö ilmoittaa, että laatuvarmenteille on kysyntää valtionhallinnon sisäisessä käytös-sä, sen sijaan muut organisaatiot eivät edellytä laatuvarmenteita vaan kaikki yleiset varmenneratkaisut kelpaavat. Yhtiöllä on kokemusta ulkomaisista varmenteista ja sen tiedossa on Suomen markkinoille sopivia varmenteita, joilla tarkoitettaneen muita kuin laatuvarmenteita.

- Aldata, Fujitsu, TietoEnator ja WMData tuottavat palveluja tai tuotteita ja ovat mukana erilaisissa pilotti- ja tuotantotason hankkeissa mm. sähköisen lääkemäärityksen, sairaanhoidon, sosiaalitoimen ja sähköisten kauppapaikkojen alueella. Sähköisen allekirjoituksen volyymisovelluksia ei vielä ole. Laatuvarmenteita on käytössä WMDatalla pilotin osana ja TietoEnatorilla sisäisessä käytössä luottamuksellisen viestinnän salaamisessa.

3.3.8. Yksityinen sektori, pankit ja vakuutuslaitokset

- Pankkien omia verkkopalvelutunnisteita on käytössä Nordealla (solo), Osuuspankilla, Sammolla, Ålandsbankenilla, Säästöpankeilla (sp/pop-tunniste), Ålandsbankenilla on e-tunnistepalvelu, ja Tapiolalla on verkkopankki. Pankit viittaavat aineistossaan sekä tunnistautumiseen että allekirjoituskäyttöön, esimerkiksi lainahakemuksen allekirjoitukseen. Myös Handelsbankenilla on käytössä käyttäjätunnus ja kertakäyttöinen salasana. Handelsbanken ei viittaa allekirjoituskäyttöön. Pankki käyttää Ruotsissa varmenteeseen perustuvaa allekirjoitusta, jonka myös sikäläinen verottaja hyväksyy (ks. jäljempänä).

- Pankit tarjoavat Suomen Pankkiydistyksen TUPAS-standardin mukaisia tunnisteita myös muille palveluntarjoajille ja siis myös muuhun käyttöön kuin pankkiasiointiin.[37] Esimerkiksi Nordea käyttää Solo-tunnuksia Suomessa verkkopankkiasiakkaidensa tunnistamiseen (v. 2004 n. 60.000.000 sisään kirjautumista) sekä toimeksiantojen vahvistamiseen, jotka Nordea luokittelee allekirjoituksiksi (yhteensä satoja miljoonia, maksutapahtumia vuonna 2004 noin 75.000.000). Nordea tarjoaa tunnistustapaa (”E-tunniste”) myös muille palveluntarjoajille ja ilmoittaa, että vuonna 2004 tätä koskevia sopimuksia oli 116 ja näissä oli tapahtumia yhteensä 787.000 kappaletta.[38] E-tunnisteen käyttömahdollisuuksia ovat palveluun rekisteröityminen, sitovien sopimusten tekeminen ja allekirjoittaminen sähköisesti, hakemusten, lomakkeiden ja ilmoitusten jättäminen luotettavasti sekä ajanvaraukset sekä lisäturvan saaminen verkkomaksamiseen. Samat palvelut hyväksyvät yleisesti muidenkin pankkien sähköisiä tunnisteita ja osa myös HST- kansalaisvarmenteen. Nordealla ei ole käytössään laatuvarmenteita, mutta kylläkin useita muita eri teknologioihin perustuvia varmenteita.

- Monet rahoitus- ja vakuutusalalla olevat yritykset ovat kyselyssä maininneet varmennekäytännöistään. Vakuutusmeklariyritys Marsh ilmoittaa, että käytössä ei varsinaisesti ole sähköisen allekirjoituksen toteutuksia eikä laatuvarmenteita. Joidenkin asiakkaiden kanssa on käytössä salausohjelmistoja, joiden ominaisuuksiin kuuluu sähköinen allekirjoitus (sign & encrypt). Ohjelmia voi käyttää myös pelkästään allekirjoitukseen. Howden Insurance Brokers ilmoitaa, ettei allekirjoitustoteutuksia ole käytössä, mutta sen taholla uskotaan kehittyneen sähköisen allekirjoituksen yleistymiseen sirullisten henkilökorttien ja kortinlukijoiden yleistyessä. Yhtiössä katsotaan, että vakuutus- ja vakuutusmeklarialalla kehittynyt sähköinen allekirjoitus tarjoaisi useita asioiden hoitamista helpottavia käyttömahdollisuuksia. Vakuutusalan toimeksiannoissa ei-

[37] Näissä tapauksissa käyttäjä valitsee verkkopalvelun sivuilta oman pankkinsa tunnistusnapin ja kirjautuu pankin palveluun samalla tavalla kuin omaan verkkopankkiinsa. Tunnistamisen yhteydessä pankki välittää järjestelmään asiakkaansa henkilötiedot, nimen ja henkilötunnuksen. Asiakas näkee mitkä tiedot hänestä välitetään sekä myös sen, mihin palveluun tiedot välitetään. Hyväksyttyään tunnistautumisen asiakas siirtyy takaisin alkuperäiseen palveluun (Verkkoasiointia pankkitunnuksilla, Avainasiakas 1/2005, s. 21).

[38] Nordea ilmoittaa esimerkkeinä käyttökohteista julkishallinnon palvelut, kuten veroviranomaisten, KELA:n, työministeriön ja Eläketurvakeskuksen ja TEKES:in palvelut, lomake.fi-palvelun, Koulutusrahaston, Tyvi-palvelut sekä Perhelomat ry:n palvelut. Lisäksi e-tunnistetta voi käyttää kaupunkien ja niiden liike- ja oppilaitosten kanssa asioitaessa ja erikseen mainittuina kaupunkeina ovat Vantaa, Espoo, Iisalmi, Seinäjoki, Harjavalta, Oulu, Turku, Kotka, Jyväskylä ja Tampere. Monet ammattiliitot ja järjestöt hyväksyvät E-tunnisteen: YTK, IAET, Kemian työttömyyskassa, TU ry, Ammatinharjoittajien ja yrittäjien työttömyyskassa, Lähi- ja perushoitajien työttömyyskassa, Merkonomien työttömyyskassa, Teollisuuden toimihenkilöiden työttömyyskassa, Tietotekniikan Liitto ry, YTY ry, Suora ry, Erko ry, OAJ

vät varmenteet ole käytössä. Esimerkiksi If Vahinkovakuutusyhtiö ja Tapiola ilmoittavat että sähköiset allekirjoitukset eivät ole käytössä. Samoin ilmoittavat monet meklariyritykset.

3.3.9. Yksityinen sektori, kauppa

- Kesko ilmoittaa, että sillä on käytössä kansalaisvarmenteeseen perustuva kuluttajien tunnistuspalvelu osoitteessa http://www.plussa.com. Palvelussa on siis käytössä laatuvarmenteet. Tällä hetkellä vain 0,05 % em. palvelun rekisteröidyistä käyttäjistä käyttää kansalaisvarmennetta tunnistautumiseen. Keskon käsityksen mukaan sähköisten allekirjoitustekniikoiden käyttö tullee yleistymään, mutta sen tärkeimmät sovellukset liittynevät jatkossa sovellusten väliseen tiedonsiirron tietoturvasta huolehtimiseen (web-service security). HST-korttia käytetään Plussa-palvelussa vain tunnistautumiseen. Kesko-konserniin kuuluvan Anttila Oy:n verkkokauppa NetAnttila ei käytä sähköisen allekirjoituksen sovelluksia.

- SOK on mukana HST-ryhmässä, mutta ilmoittaa, ettei sen käytössä ole sähköisen allekirjoituksen sovelluksia.

- Europetukku Oy:öön vastaanotettavissa tilauksissa varmennetaan asiakkaan sosiaaliturvatunnus. Varmenneohjelma näyttää, onko sosiaaliturvatunnus annettu oikein vai väärin. Sosiaaliturvatunnuksen käyttö varmennustarkoituksiin perustuu asiakkaan suostumukseen.

3.3.10. Yksityinen sektori, logistiikka

- John Nurminen Oy ilmoittaa käyttävänsä ulkomaisia palvelinvarmenteita joissakin tapauksissa.

- World Courier (Finland) Oy ilmoittaa käyttävänsä pankkitunnisteita maksuliikenteessä. Yrityksen intranetissä on käytössä sähköinen tunnistus, joka on rajoitetusti käytössä myös asiakkaille.

---

ry ja Tradenomiliitto ry. E-tunnisteteen hyväksyvien yritysten joukossa on Verified by Visa, Pohjola, Ilmarinen, SOK, Suomen Posti, TeliaSonera, Radiolinja, DNA, Saunalahti, Cubio, MTV3, RP Oy, Veikkaus ja Fintoto Oy.

- Nordic Freight Oy, Schenker Oy, Silja Line Oy, UPS SCS (Finland) Oy ja VR Cargo Oy ilmoittavat, että sähköisen allekirjoituksen sovelluksia ei ole käytössä.

- liikenne- ja viestintäministeriön tuella on käynnistynyt sähköistä rahtikirjaa koskeva Kultis-projekti, joka on tällä hetkellä läpikäynyt kartoitusvaiheen.[39] Sen yhteydessä on kiinnitetty huomiota mm. tavaran vastaanottokuittauksen toteuttamiseen sähköisessä muodossa. Tällöin on huomiota kiinnitettävä sekä vastaanottajan todentamiseen, että kuittauksen yhdistämiseen sähköiseen rahtikirjatietoon. Toimikortteihin perustuvien varmenteiden ohella tarkastelun piirissä ratkaisua etsittäessä voivat olla myös RFID (radio frequency identification) -tunnisteet.

3.3.11. Yhteenvetoa

Yhteenvetona vastauksista voidaan todeta, että sirukorttiin perustuvat VRK:n varmenteet ovat käytössä sisäisesti yksittäisissä virastoissa, patenttiasioissa sekä PRH:n ja EPO:n kanssa asioitaessa, KATVE-projektin mukaisesti työministeriön, verohallinnon ja KELA:n palvelujen tarjonnassa, erilaisten hallinnon lomakkeiden ja ilmoitusten täyttämisessä ja yksittäisissä kaupallisissa palveluissa, kuten Osuuspankin palveluissa ja Kesko Plussa-palveluissa. Yksityisten palvelujen osalta kuitenkin ainoastaan Osuuspankin käyttämässä Visa Electron-sirukortissa on allekirjoituskäyttömahdollisuus.

HST-kortin käyttö on KATVE-projektin piiriin kuuluvia palveluja tarjottaessa toistaiseksi marginaalisen vähäistä pankkitunnisteiden käyttöön verrattuna. Julkinen sektori ja viranomaiset ovat kuitenkin ottaneet kansalaisvarmenteeseen liittyviä ratkaisuja käyttöön selvästi enemmän kuin yksityinen sektori. Tekniikkaa myyvät yritykset toteavatkin, ettei yksityinen asiakassektori ole ollut nimenomaisesti kiinnostunut laatuvarmenteisiin liittyvästä tekniikasta.

HST-korttien allekirjoituskäytön vähäisyyteen on syynä myönnettyjen korttien ja palvelujen vähäinen määrä sekä todennäköisesti käyttötottumusten puuttuminen sekä allekirjoittaja- ja palveluntarjoajapuolella. Kansalaisvarmenteeseen perustuvaa sähköisen allekirjoituksen käyttöä on lähinnä pilottikokeiluissa, mutta sähköisen allekirjoituksen volyymisovelluksia ei vielä juuri ole. Terveydenhuollon pilottikokeilussa allekirjoituksen käyttö resepteissä perustuu asetukseen sähköisen lää-

[39] Ks. www.aino.info.

kemääräysten kokeiluista, jossa laatuvarmenteeseen perustuvan allekirjoituksen vaatimus on selkeästi asetettu.[40]. Toinen alue, jossa laatuvarmenteeseen perustuvaa allekirjoitusta käytännössä vaaditaan, on patenttihakemusten sähköinen jättäminen. Monet tavalliset ilmoitusasiat voidaan usein hoitaa pelkkää tunnistautumisfunktiota käyttäen, vaikka ilmoitus sisältäisikin tahdonilmaisun. Viranomainen määrää sen varmuustason, jota tunnistautumisessa ja tahdonilmauksen tekemisessä on saavutettava, myös lakisääteisen allekirjoitusvaatimuksen ollessa kyseessä.[41]

Mobiilivarmenteen käyttöön tulo saattaa muuttaa kuvaa tältä osin jonkin verran. Sitä mukaa kuin sirukorteilla olevia varmenteita opitaan käyttämään, voi myös näiden allekirjoitusfunktio tulla käyttöön jossain laajuudessa. Tämä edellyttää kuitenkin, että palveluntarjoaja ryhtyy vaatimaan allekirjoitusfunktion käyttöä. Tyypillisesti tämä voisi tapahtua esimerkiksi luottohakemusten allekirjoittamisessa. Mikäli laatuvarmenteiden allekirjoitusfunktion tarjoamaa varmuustasoa ei haluta tai arvioida tarvitsevan palveluissa tavoitella, ei vaatimusta aseteta eikä lain tarkoittamien laatuvarmenteiden käyttö laajene nykyisestä.

Muuna sähköisen allekirjoituksen toteutuksena on Suomessa käytössä pankkien muuttuvien salasanojen käyttö allekirjoitustarkoituksiin, joista meillä on käytössä erityisesti kertakäyttöalasanoihin perustuva pankkien TUPAS 2 – tunnistamisstandardi.[42]

Muuttuviin salasanoihin perustuvien TUPAS-pankkitunnisteiden käyttö on hyvin laajamittaista. Käyttäjiä arvioidaan olevan 2,5 miljoonaa. Pankkitunnisteiden käyttö sisältää siis myös mahdollisuuden mm. muuttuvin salasanoin tapahtuvaan sähköiseen allekirjoitukseen. Pankkien tarjoamia tunnistuspalveluja on tarjottu sopimusperusteisesti myös ulkopuolisille palveluntarjoajille sekä yksityiselle että julkiselle sektorille. Pankkien tunnistamistoiminta ja varmennetoimintaa muistuttavat palvelut perustuvat siis sopimuksiin osapuolten välillä, eli ne eivät ole yleisyydestään huolimatta

[40]Sosiaali- ja terveysministeriön asetus 771/2003, joka on sittemmin uusittu. Asetuksen 6 § toteaa, että ”sähköisessä lääkemääräyksessä tulee olla sen laatijan nimi ja hänet varmentava sähköinen allekirjoitus, joka perustuu sähköisistä allekirjoituksista annetussa laissa tarkoitettuun laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä”. Sähköisen allekirjoituksen käyttöön tulee liittää toiminto, jolla käyttäjän oikeus määrätä lääkkeitä tarkastetaan automaattisesti.

Vertailun vuoksi voidaan todeta, että lääkemääräysten antamista perinteisemmässä maailmassa sääntelee Lääkelaitoksen määräys (10/2002, 18.12.2002) Lääkkeiden toimittaminen. Sen mukaan lääkemääräys on annettava joko kirjallisesti (paperilla), telefaxilla tai puhelimitse. Lääkärin allekirjoitusvaatimusta ei kirjallisessa reseptissä ole asetettu, mutta puhelinresepti on proviisorin tai farmaseutin allekirjoituksellaan varmennettava. Toisaalta muotovaatimuksena on pääsääntöisesti KELA:n kaavakkeen käyttäminen, jossa allekirjoitukselle on varattu paikkansa.

[41] Ks. laki sähköisestä asioinnista viranomaistoiminnassa 13/2003 ja HE 17/2002 vp ss. 38-39.

täysin avoimille käyttäjäryhmille suunnattuja palveluja. Lisäksi pankkitunnisteet toimivat yhteen suuntaan, eli jos pankki haluaa ottaa yhteyttä tunnistautujaan päin, otetaan tähän yhteyttä esimerkiksi puhelimitse.[43] Myös mobiilivarmenteiden kohdalla edellytetään sopimusjärjestelyjä, mutta operaattorien välisten yhteentoimivuutta koskevien järjestelyjen vuoksi mobiilivarmenteet voivat muuttua yleiskäyttöisiksi. Kansainvälistä ulottuvuutta TUPAS-standardilla ei toistaiseksi ole mahdollisesti Pohjoismaita ja Baltiaa lukuunottamatta.

Muita sähköisiä tunnistautumismenetelmiä ovat käyttäjätunnuksen ja salasanan käyttö yhdessä tai erikseen, biometriset tunnisteet kuten sormenjäljet ja radiotaajuustunnisteet. Sähköiset etätunnistautumismenetelmät ovat pääsääntöisesti sopimusperusteisia. Sopimuksilla voidaan luoda ns. *federated identity*, jossa osapuoli tunnistaa toisensa sopimuksen luomin keinoin.[44] Sopimusjärjestelyjen lisäksi voi tunnistamisesta olla erillisiä vaatimuksia. Esimerkiksi julkishallinto ohjeistaa omia tunnistamisvaatimuksiaan.[45] Lainsäädännöllä tai viranomaisohjeistuksella saatetaan lisäksi asettaa tunnistamisvaatimuksia myös yksityisten välisissä suhteissa.[46]

3.3.12. Muita varmenteita

Hallinnon ja yritysten käytössä on useita laatuvarmenteita kevyempiä varmenteita, kuten PGP ja ohjelmistovarmenteet. PKI- ja toimikorttipohjaiset ratkaisut ovat saavuttaneet suosiota lähinnä julkishallinnon tai yritysten sisäisessä käytössä, jolloin käyttäjäpiiri on ennalta rajattu.

PGP (Pretty Good Privacy) on käytössä organisaatioiden kuten virastojen sisäisessä käytössä sekä yhteyksissä yksittäisiin asiakas- tai sidosryhmiin. PGP on periaatteessa PKI-pohjainen sähköpostien salausjärjestelmä, mutta se perustuu symmetrisen ja epäsymmetrisen kryptografian yhdistelmään.[47] PGP:ssä salattava sanoma tiivistetään, jonka jälkeen muodostetaan tapahtumakohtainen avain, joka

---

[42] Vastausten yhteydessä on esitetty viittaus väitteeseen, jonka mukaan USA:ssa pohjoismainen kertakäyttösalasanakäytäntö ei olisi mahdollinen, sillä se periaatteessa mahdollistaa asiakkaan verkossa tekemiensä toimenpiteiden kiistämisen perusteella, että pankki tietää salasanat.

[43] Pankit voivat markkinoida tuotteitaan asiakkaille ilman näiden tunnistamista, mutta kun sopimusta ryhdytään markkinointitoimen jälkeen solmimaan, on asiakas luonnollisesti tunnistettava.

[44] Federated identity mahdollistaa sen, että yrityksessä A toimiva henkilö voi käyttää henkilökohtaisia tunnisteitaan myös asioidessaan yrityksen B järjestelmissä tietyiltä osin. Yritys A varmentaa siis työntekijänsä tähän tarkoitukseen.

[45] Ks. Tunnistaminen valtionhallinnon verkkopalveluissa, VM 6/01/2003, 29.9.2003

[46] Sisäasiainministeriön asetus 890/2003 rahanpesun estämisestä ja selvittämisestä sekä Rahanpesun torjunnan parhaat käytänteet, Keskusrikospoliisi, Rahanpesun selvittelykeskus, (http://www.poliisi.fi/intermin/images.nsf/files/111880F83D17EDF3C2256E36002E3A0B/$file/Rahanpesun+torjunnan+parhaat+käytänteet.pdf), vierailtu 14.4.2005

[47] PGP:stä on olemassa Internet Engineering Task Forcen standardi RFC2440.

salataan vastaanottajan julkiselle avaimelle. Tämän jälkeen vastaanottaja avaa yksityisellä avaimellaan istuntokohtaisen avaimen. Tapahtumakohtaisen avaimen käyttö nopeuttaa salauksen purkamista, sillä se perustuu symmetriseen kryptografiaan. Toisaalta julkisen avaimen järjestelmä mahdollistaa tapahtumakohtaisen avaimen turvallisen jakelun. PGP ei yleensä sisällä luotetun kolmannen osapuolen toimimista varmentajana.

Ohjelmistovarmenteet eli softavarmenteet ovat PKI-pohjaisia varmenteita, joita operaattorit tarjoavat Suomessa lähinnä yritysten sisäisen sähköpostin salaamiseen.[48] Ohjelmistovarmenteet ovat tietoturvatasoltaan älykorttipohjaisia varmenteita heikompia, koska allekirjoituksen luomistiedon yksinomainen hallussa olo ei ole samalla tavoin kontrolloitavissa kuin älykortin kanssa. Tämän vuoksi ohjelmistovarmenteet häviävät tietoturvallisuusmielessä vaihtuville salasanoille. Ruotsissa sikäläistä julkishallinnon kansalaisille myöntämää varmennetta koskeva ohjeistus perustuu pitkälle ohjelmistovarmenteisiin ja myös pankit käyttävät niitä.

Palvelinvarmenne auttaa tunnistamaan palvelun tarjoajan. Palvelinvarmenne on siis tunnistusvarmenne. Palvelinvarmenne mahdollistaa selaimen ja palvelimen tai kahden palvelimen välisen tietoliikenteen. Esimerkiksi Väestörekisterikeskuksen myöntämän palvelinvarmenteen käyttötarkoitus voidaan määrittää käyttökohteen mukaisesti tunnistamiseen (server authentication), asiakkaan tunnistamiseen (client authentication) tai kumpaankin samanaikaisesti.[49] Palvelinvarmenteet ovat laajalti yritysten ja muiden organisaatioiden käytössä.

Sähköpostivarmenne on voi olla mikä tahansa varmennetyyppi, usein kuitenkin ohjelmistovarmenne. Sähköpostivarmennetta käytetään organisaatioiden käytössä olevia, usean henkilön toimesta seurattavia sähköpostiosoitteita varten. Näitä osoitteita ovat esimerkiksi kirjaamo-, tilaus- ja toimenpiteiden välittämiseen käytettävät sähköpostiosoitteet, joihin saapuvat viestit pitävät sisällään käsittelyyn liittyvää luottamuksellista tietoa. Organisaation sähköpostiosoitteeseen saapuvat salatut

[48] esimerkiksi Microsoft Passport.

[49] WWW-sivujen selailun suojaukseen käytetään useimmiten SSL-protokollaa (Secure Sockets Layer). SSL mahdollistaa yhteyden vahvan salaamisen käyttäjän www.selainohjelmiston ja www.palvelimen välillä. Yhteyden salaamisen lisäksi SSL-protokolla mahdollistaa molempien osapuolien vahvan tunnistamisen varmenteiden avulla. SSL tukee myös henkilövarmenteiden hyödyntämistä, jolloin käyttäjä voi todistaa oman henkilöllisyytensä www.palvelimelle. Merkittävimmät selainohjelmien valmistajat ovat sisällyttäneet selaimiinsa lukkoa kuvaavan ikonin, jonka tila kertoo, onko kyseisellä sivustolla käytössä SSL-salaus vai ei. Selain varmistaa, että sertifikaatti on osa päävarmentajaan johtavaa ehjää ketjua. Ongelmaksi voi kuitenkin muodostua, jos sertifikaattien varmentajat eivät edellytä hakijoilta riittävää selvitystä esimerkiksi oikeudesta domain-nimeen, sertifikaatissa mainitun organisaation juridista olemassaoloa ja oikeustoimikelpoisuutta tai organisaation edustajan valtuuksia hakea sertifikaattia edustamansa organisaation nimiin. Jos riittäviä tarkistuksia ei tehdä, varmennettava sivusto voi olla jäljittelijän pystyttämä. Myös yhteyksissä pankkien palvelimiin käytetään SSL-protokollaa.

viestit avataan sähköpostivarmenteen avulla. Organisaatio voi myös käyttää sähköpostivarmennetta organisaatiosta lähtevien sähköpostien allekirjoittamiseen. Myös sähköpostivarmenteita on yritysten ja organisaatioiden käytössä yleisesti.

Ajopiirturivarmenne on tieliikenteen valvontalaitteeseen eli ajopiirturiin liittyvä todistus. Ajopiirturilla ja digitaalisilla piirturikorteilla valvotaan kuorma- ja linja-autonkuljettajien ajo- ja lepoaikoja, joista on säädetty tieliikenteen sosiaalilainsäädännön yhdenmukaistamisesta annetulla neuvoston asetuksella (ETY) N:o 3820/85.[50] Ajopiirturikorttien myöntäjää kutsutaan myös varmentajaksi. Varmenteet myöntää Ajoneuvohallintokeskus AKE, joka toimii Suomen kansallisena varmenneviranomaisena. Suomalaiset varmenteet on allekirjoitettu EU-tason juurivarmenteella. EU-tason varmenneviranomainen ERCA (European Root Certification Authority) toimii EU-komission alaisuudessa.

3.3.13. Ulkomaisten varmenteiden käyttö organisaatioissa

Selvityksessä ei tullut esille ulkomaisten laatuvarmenteiden käyttöä Suomessa.

Sen sijaan muita ulkomaisia varmenteita on käytössä. Yleisimmin käytössä lienevät Verisignin myöntämät palvelinvarmenteet. Käytössä on myös Euroopan ajopiirturivarmenteiden juurivarmenne ERCA. Pohjoismaiset pankit ovat luonnollisesti tekemisissä muissa Pohjoismaissa käytettävien varmennekäytäntöjen kanssa, jotka perustuvat mm. ohjelmistovarmenteisiin.

Ulkomaisten varmenteiden käytön edistämiseksi julkisen sektorin palveluissa on keskusteltu eri maiden viranomaisten kesken. Hallinnollista ja varmentajien kesken tehtävää yhteistyötä ja kokemuksia vaihdetaan ns. Porvoon ryhmässä.[51]

Yleisesti ottaen vastauksista nousee esille se johtopäätös, että laatuvarmenteet ovat varsin kansallisia hankkeita pienin poikkeuksin. Patenttiasioissa Euroopan patenttivirasto EPO hyväksyy VRK:n myöntämän laatuvarmenteen. Suomen HST-kortti käy Itävallassa sähköisenä tunnisteena ja Suomen ja Viron välille on pyritty kehitettämään yhteistyötä laatuvarmenteiden käytön osalta.

---

[50] Ks- Laki ajopiirturikorttien myöntämisen järjestämisestä 629/2004.

[51] Kansainvälinen Porvoo-ryhmä perustettiin Porvoossa vuonna 2002 EU:n eEuropen alla toimineen Smart Card Charterin Public Identity-hankkeen yhteydessä pidetyssä kansainvälisessä konferenssissa. Porvoo-ryhmään kuuluu hallinnon

EU-direktiiviin perustuvien laatuvarmenteiden yhteentoimivuudessa on havaittu ongelmia standardien olemassaolosta huolimatta, eikä laatuvarmenteille ole olemassa kypsiä eurooppalaisia markkinoita.[52]

3.3.14. Ulkomaiset sovellukset

Yhtenä selvitettävänä kysymyksenä on ollut, onko muualla käytössä jotain sellaisia sähköisiin allekirjoituksiin liittyviä tuotteita tai sovelluksia, jotka saattaisivat soveltua myös Suomen markkinoille.

Suurin osa varmenteita hyödyntävistä ohjelmistoista on ulkomaisia. Kokemukset ulkomaisista palveluntarjoajista ovat lähinnä kokemuksia palvelinvarmenteiden tarjoajista, kuten Verisign. Tanskan ja Ruotsin mallit reseptien tunnistuksessa on nostettu vastauksissa esille Suomen oloja ajatellen.

Vastauksista on ilmennyt, että varmenteita koskevia tuotteita ja sovelluksia tulee markkinoille koko ajan ja monet niistä sopisivat Suomen oloihin. Esimerkiksi Nokia katsoo, että ohjelmiston alkuperään ja eheyteen tähtäävät sähköiseen allekirjoitukseen perustuvat tuotteet, *Symbian signed* ja *Java verified* sopisivat Suomen markkinoille.

Ulkomaiset, dokumenttien hallintaan ja sisällön suojaamiseen ja toisaalta eheyteen liittyvät tuotteet nostetaan kyselyyn annetuissa vastauksissa esille monien palveluntarjoajien toimesta. Tyypillisesti jälkimmäisissä sovelluksissa sähköisen allekirjoituksen käyttö on piilotettua. Tällöin eheyden suojaamisessa käytetään allekirjoitusta vastaavia salausmenetelmiä, mutta ei allekirjoitustarkoituksiin.

Pankkisektorilla tarkkaillaan kansainväliseen käyttöön soveltuvien IDENTRUS-varmenteiden[53] kehitystä. Nämä varmenteet perustuvat PKI-tekniikkaan.

---

edustajia Euroopan maista ja kokouksissa on ollut mukana myös osallistujia yksityiseltä sektorilta. Lisäksi Euroopan komission edustajia on osallistunut seminaareihin.

[52] Ks. lähemmin ”The legal and market aspects of electronic signatures”, Interdisciplinary centre for Law and Information Technology”, CUL, Leuven, 2003.

[53] Ks. http://www.identrus.com/, vierailtu 5.4.2005.

Tähän kysymykseen on annettu vastauksia suhteellisen vähän ja vastaukset eivät nosta esille mitään sellaista, mikä aiheuttaisi lainsäädäntötarpeita, esim. uudenlaisten kehittyneiden allekirjoitustapojen muodossa.

3.4. Kansainvälistä vertailua

Ensimmäinen sähköisiä allekirjoituksia koskeva lainsäädäntö syntyi Yhdysvalloissa Utahin osavaltiossa vuonna 1995. Viimeisin edistysaskel ollut Kiinan lainsäädäntö, joka perustuu digitaaliseen allekirjoitukseen ja valvottujen (laatu)varmentajien toimintaan luotettavina kolmansina osapuolina. Monet kehityshankkeet, kuten edellä mainittu IDENTRUS, perustuvat PKI-pohjaiseen tekniikkaan.

Voidaan yleisesti kuitenkin todeta, että Keski-Euroopassa on tiukempi suhtautuminen varmenteiden käyttöön. Esimerkiksi Saksa vaatii verkkolaskuihin laatuvarmenteen tasoista tunnistamista. Kuudes arvonlisäverodirektiivi (2001/115/EY) sallii erilaiset käytännöt tässä suhteessa, samoin julkisia hankintoja koskevat direktiivit (2004/18/EY ja 2004/17/EY). Suomi on molempien direktiivien kohdalla ajanut mahdollisuutta valita kansallisesti lievemmät menetelmät ja onnistunut tavoitteessaan. On kuitenkin otaksuttava, että sen jälkeen kun julkisia hankintoja koskevat direktiivit on pantu täytäntöön ja sähköiset hankintamenettelyt mahdollistettu, esimerkiksi tarjouskilpailuihin osallistumiseksi yritysten olisi ajoittain hankittava kehittyneisiin sähköisiin allekirjoituksiin liittyvää teknologiaa. On huomattava, että sähköiset hankinnat on ensimmäinen sektori, jolla yritykset käyttävät EU-lainsäädännön tunnustamia allekirjoituksia asioidessaan muun jäsenvaltion kuin oman maansa viranomaisten kanssa.[54]

Kansainvälinen kauppa ja sisämarkkinakauppa sekä kansainvälinen hallintoviranomaisten yhteistyö voivat jatkossa luoda tilanteita, joissa yrityksille ja hallintoviranomaisille on hyötyä laatuvarmenteiden käyttöönotosta. Vaikka PKI-tekniikkaan perustuvien laatuvarmenteiden käyttö ei ole yleistynyt, ja niiden suoma turvataso voi olla ylimitoitettu moniin tarkoituksiin, on lähinnä niitä koskevan lainsäädännön levinneisyys ja Euroopan tasolla direktiiviin perustuva lainsäädäntö sekä standardointi kuitenkin edellä muita sähköisiä allekirjoitus- ja tunnistustekniikoita, joissa vastaavaa yhteis-

[54] Ks. Komission tiedonanto neuvostolle, Euroopan Parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Toimintasuunnitelma sähköisten julkisten hankintojen sääntelykehyksen täytäntöönpanemiseksi, Bryssel 13.12.2004.
Hanke nimeltä ”Bridge/Gateway CA” käynnistettiin osana HVT-ohjelmaa (HVT = hallintojen välinen tietojenvaihto) vuonna 2002 tarkoituksena käsitellä niiden sähköisten todistusten tunnustamista ja luotettavuutta, joita eri maiden varmenneviranomaiset myöntävät eri kansallisten viranomaisten vaihtaessa turvattua sähköpostia ja allekirjoituksia.

työtä ei ole.[55] Kun sähköistä tunnistamista ja allekirjoitusta tarvitaan juuri etätransaktioissa, jollaisia rajanylittävät transaktiot ovat, on laatuvarmenteiden käyttö yksi todennäköinen ja keskeinen vaihtoehto. Yhteentoimivuus edellyttää yhteistä lähestymistapaa, johon laatuvarmennetta koskevat vaatimukset tarjoavat vaihtoehdon.

Virossa on noin 700.000 kansalaisella jo sähköinen henkilökortti ja niiden levinneisyys kasvaa koko ajan. Virossa on tarjolla noin 150 sähköistä palvelua, joissa voidaan käyttää tunnistus- ja allekirjoitusvarmennetta. Kansalaiset käyttävät kuitenkin huomattavasti yleisemmin pankkitunnisteita ja sähköistä henkilökorttia käyttää vain noin 3 % laatuvarmenteiden piirissä olevien sähköisten palvelujen käyttäjistä. Virossa pankkitunnisteilla voi tehdä veroilmoituksen. Allekirjoituskäyttöä on kuitenkin merkittävässä määrin olemassa. Allekirjoitustilanteessa tietojärjestelmä huomauttaa allekirjoittajalle, että tämän tekemällä toimenpiteellä on oikeusvaikutuksia, mikä vastaa myös kuluttajansuojatarpeisiin.

Ruotsin kehitys poikkeaa Suomen ja Viron kehityksestä sikäli, ettei maahan ole syntynyt toistaiseksi yhtään laatuvarmentajaa. Sähköinen asiointi perustuukin ohjelmistovarmenteille. Julkinen sektori eli valtionkonttori on kuitenkin määrittänyt varmennestandardin kaupallisille toimijoille ja harjoittaa valvontatoimintaa varmentajien suhteen sikäli kuin kyse on asioinnista valtion viranomaisten kanssa. Useat pankit ovat muodostaneet yhteisen varmentajatoiminnon ja käytössä on sähköinen henkilökortti. Ruotsissa voi veroilmoituksen jättää ilmoituksen yhteydessä tulleita kirjautumis- ja allekirjoitussalasanoja käyttämällä, mikäli ilmoittaja hyväksyy veroehdotuksen. Jos ilmoittaja haluaa tehdä muutoksia, vaaditaan kuitenkin sähköinen henkilökortti.

4. TOIMIJOIDEN NÄKEMYKSIÄ

4.1. Lain toimivuus

Laki on soveltamisalallaan sinänsä toimiva, mutta sen määräyksiä on sovellettu käytännön tilanteisiin lähinnä vasta pilottikokeiluissa. Sen vuoksi ja palautteen huomioiden, on mahdotonta antaa käytännön kokemuksiin perustuvia näkemyksiä kuin joidenkin yksityiskohtien osalta lain soveltа-

[55] Sen jälkeen kun Yhdysvallat ryhtyy vaatimaan biometrisiä tunnisteita passeihin vuoden 2005 lopulla, joutuvat EU-maat ja muut maat muuttamaan passinmyöntämiskäytäntöjään. Kyse ei ole kuitenkaan sähköisestä etätunnistamisesta vaan matkustusasiakirjan väärentämismahdollisuuden minimoimisesta.

misesta. Haastatteluissa ja kyselyissä esitetyt arviot ovat paljolti aikaisempien, jo lain valmisteluvaiheessa esitettyjen näkemysten toistamista.

Kysymykseen voi vastata käymällä läpi lain ja sen taustalla olevan direktiivin tavoitteet. Käsintehdylle allekirjoitukselle on luotu lain vaatimukset täyttävä sähköinen vastine, joka on otettavissa sekä viranomais-, yritys- että kuluttajakäyttöön.

Lain tarkoittama sähköinen allekirjoitus on infrastruktuuriltaan verraten raskas järjestelmä. Valtiovarainministeriö toteaa kommenteissaan, että tekniikka vaatii vielä loppukäyttäjiltä ylimääräistä ponnistelua ja koko konsepti on vaikea ymmärtää. Yksi sähköisiä allekirjoituksia koskevan lainsäädännön perusongelma on, että lainsäädännöllä luodaan vastine oikeudellisesti niin epäyhtenäiselle oikeudelliselle käsitteelle kuin allekirjoitukselle. Teleoperaattorien taholta on viestitetty, että käännettyyn todistustaakkaan ja varmentajan rajoittamattomaan vastuuseen perustuvat vastuusäännöt, maksut ja sähköisiin asiointitunnuksiin liittyvä politiikka estävät uusien laatuvarmentajien syntymistä. Toisaalta laatuvarmenteiden kysyntä erityisesti yksityisellä sektorilla on ollut vielä pientä. Tähän on syynä rinnakkaisen sähköisen asiointimahdollisuuden, pankkitunnusten käytön tarjoaminen monissa palveluissa ja allekirjoitustarpeiden vähäisyys, todennäköisesti myös yleinen tottumattomuus sähköiseen asiointiin. Näistä syistä ei laatuvarmentajia ole markkinoille tullut Väestörekisterikeskuksen lisäksi. Ruotsissa ei toistaiseksi ole ainuttakaan laatuvarmentajaa.

Lain tarkoittamana laatuvarmentajana tullee jatkossakin olemaan yksinomaan Väestörekisterikeskus. Laatuvarmennepalveluita välittävät organisaatiot, kuten teleoperaattorit ja pankit toimivat Väestörekisterikeskuksen kanssa yhteistyössä ja vastuut jaetaan monimutkaisten sopimusrakenteiden avulla. VRK:n yhteistyökumppanina on myös poliisi, joka hoitaa rekisteröinnin sähköisen henkilökortin myöntämisen yhteydessä.

4.2. Tuleva kehitys

Seuraavassa eräiden toimijoiden taholta esitettyjä näkemyksiä siitä, mikä kehitys voisi jatkossa olla.

Tullin mielestä vuorovaikutteisen asioinnin lisääntyessä vahvan tunnistamisen tarve lisääntyy, jolloin on tärkeää, että vahva tunnistaminen voidaan toteuttaa esimerkiksi sähköisellä henkilökortilla. Allekirjoituksen merkitystä ei nähdä keskeisenä. Sähköisen henkilökortin ja sen lukulaitteiden tulisi olla lähes ilmaisia, jotta menetelmät voisivat yleistyä.

Viestintävirasto toteaa, että laissa on esitetty tietoturvatasoltaan erittäin korkean tason menetelmä, jollaisen käyttöön kaikilla palveluntarjoajilla ei ole tarvetta. Palveluntarjoajan intressi käyttäjän tunnistamisesta perustuu sen itse tekemään riskianalyysiin. Viestintävirasto arvelee, ettei mobiilivarmennetta käytettäisi juurikaan allekirjoitustarkoituksiin, vaan vahvaan tunnistamiseen.

Valtiovarainministeriö katsoo, että sähköinen allekirjoitus ei ole hallinnossa ongelma, eikä siihen ole tarvetta laajemmin panostaa. Allekirjoitusten käyttö viestien alkuperän varmistamisessa saattaa kuitenkin nousta odotettua merkittävämpään asemaan roskapostin torjumisen tarpeen kasvaessa. Samoin toteaa Segco, joka katsoo, että PKI-pohjaisessa asioinnissa voitaisiin varsin tehokkaasti rajata businessasiointi muusta häiritsevästä asioinnista. Segco katsoo, että sähköisen identiteetin kiistämättömyys ja eheys on nähty teknisenä asiana, vaikka kyseessä on prosessi. Segco uskoo, että organisaatiovarmenne ja mobiilivarmenne eli sirukorttien käyttö yleistyvät jatkossa voimakkaasti ja että niitä tullaan integroimaan keskenään erityyppisillä gateway-ratkaisuilla. Nokia arvelee, että kehitys on hidasta, mutta että siihen pitäisi silti panostaa kansainvälisessä yhteistyössä.

Useimmat yksityiskohtaisesti kyselyyn vastanneet katsovat, että laatuvarmenteiden infrastruktuurin käyttö tulee lisääntymään. HST-kortteja käytettäisiin siten jatkossa enemmän vahvan tunnistamisen toteutuksena. Allekirjoitusmahdollisuuden olemassaolo voi jonkin verran lisätä laatuvarmenteisiin perustuvan sähköisen allekirjoituksen käyttöä.

Elisa katsoo, että laatuvarmennetasoinen tunnistaminen tai allekirjoitus olisi riittävä yleinen taso, mutta kuluttajakaupassa ja pankkitoiminnassa pankkitunnisteet olisivat käytössä siirtymäkaudella varmenneteknologian yleistyessä. Lisäksi todetaan, että nykyinen sähköiseen allekirjoitukseen perustuva lainsäädäntö on harhaanjohtava verrattuna markkinakäytäntöön, jossa tunnistamisen merkitys korostuu. Voitaisiin ajatella, että tunnistus- ja allekirjoitusvarmenteita kohdeltaisiin yhtäläisesti laatuvarmenteina, koska niiden turvataso on käytännössä yhtä hyvä. Tätä tarkoitusta varten voitaisiin lain määritelmiä täydentää sopivassa yhteydessä.

4.3. Pitääkö lakia muuttaa?

4.3.1. Lain soveltamisala

Pankkien taholta on nostettu esille, että lakiin voitaisiin kirjata yksityiskohtaisissa perusteluissa oleva toteamus, että lakia ei sovelleta sähköisiin allekirjoituksiin liittyvien tuotteiden tai palvelujen tarjontaan suljetulle käyttäjäryhmälle. Toisaalta tämä seikka sisältyy jo yleisölle tarjoamisen käsitteeseen soveltamisalasäännöksessä. Yleisö on käyttäjäryhmä, johon kuuluu sekä varmenteiden haltija että luottavat osapuolet.

Vastauksissa on myös katsottu, ettei laki ota selkeästi kantaa organisaatiovarmenteella tehtyyn sähköiseen allekirjoitukseen ja että lain 9 § rajaa organisaatiovarmenteen säädöksen ulkopuolelle. Laki ei ilmaise ollenkaan varmentajan, joka tarjoaa varmenteita työntekijöilleen eikä yleisölle, myöntämän varmenteen kriteerejä. Tällä hetkellä organisaatiovarmenteella ei ole lakia, joka ohjaisi sen käyttöä ja tulkitsisi sitä. Väestörekisterikeskus myöntää organisaatiolaatuvarmenteita, mutta tämä tapahtuu nimenomaan yleisölle annettavien varmenteiden avulla, mutta joita luonnollisesti myönnetään myös organisaation sisäiseen käyttöön, jos tämä on tarpeen.

Mitään välitöntä muutostarvetta lain soveltamisalan täsmentämiseksi ei ole tältä osin olemassa, sillä kyse on lähinnä lain ymmärrettävyydestä.

4.3.2. Laajempi sähköisen allekirjoituksen käsite

Vaihtoehtoisia allekirjoitusratkaisuja tarjoavien pankkien taholla on katsottu, että olisi harkittava direktiivin artiklan 5 kohdan 2 periaatteiden sisällyttämistä lakiin. Artiklakohdassa tuodaan esille kielto diskriminoida muita kuin 1 kohdassa mainittuja, laatuvarmenteisiin perustuvia allekirjoitustapoja. Laissa voitaisiin todeta joko suoraan tai epäsuorasti, että myös muut sähköiset allekirjoitukset kuin kehittyneet sähköiset allekirjoitukset, jotka perustuvat laatuvarmenteeseen ja jotka on luotu turvallisella allekirjoituksen luomisvälineellä voivat vastata käsintehtyä allekirjoitusta.[56] Sekä sähköisiä allekirjoituksia koskevan lain että sähköistä asiointia viranomaistoiminnassa koskevan lain

[56] Komission teettämässä selvityksessä ”The Legal and Market Aspects of Electronic Signatures” todetaan, että useat jäsenvaltiot ovat implementoineet direktiivin jättämällä kohdan 2 kokonaan tai osittain pois. Selvityksen sivulla 6 todetaan, että oikeuskäytännön vähäisyys ei mahdollista tällaisen implementointitavan vaikutusten arviointia, mutta että direktiivin soveltamista on tarkkailtava jatkossa.

perusteluissa todetaan, ettei muulta sähköiseltä allekirjoitukselta saa evätä todistusvoimaa pelkästään muodollisilla perusteilla, vaan että ratkaisu tulisi tapahtua tapauskohtaisesti.

Muun allekirjoituksen hyväksyminen käyttötilanteen mukaan on sopimusvapauden vallitessa Suomessa varsin ilmeinen. Silti laki olisi informatiivisempi ja todellista käytäntöä paremmin vastaava, jos kyseessä oleva direktiivikohta olisi kirjattu lakiin. Laki sähköisestä asioinnissa viranomaistoiminnassa (13/2003) viittaa nimenomaisesti sähköisistä allekirjoituksista annetun lain 18 §:n mukaiseen menettelyyn. Esitöiden kautta päästään toki tulkintaan, että myös muut allekirjoitustavat voidaan tapauskohtaisesti hyväksyä, mutta itse lakitekstin laajempi muotoilu olisi kuitenkin tarkoituksenmukaisempaa. Komission toimesta teetetty selvitys viittasikin direktiivikohdan täsmentämisen tarpeeseen.[57] Jos muutos tehtäisiin, laki tulisi lähemmäksi UNCITRAL:in mallilakia, jossa sähköistä allekirjoitusta tarkastellaan nimenomaan käyttötarkoituksen vaatimasta suhteellisesta näkökulmasta. Tämäntyyppinen lähestymistapa on mm. Saksan lainsäädännössä.

Lailla sähköisistä allekirjoituksista (14/2003) ja nimenomaisesti lailla tietoyhteiskunnan palvelujen tarjoamisesta (458/2002) on toteutettu se yhteisön jäsenvaltioille osoitettu vaatimus, että sähköinen sopimustoiminta olisi tehtävä mahdolliseksi. Vapaan todistusharkinnan vallitessa yleisesti sääntely on kohdistettu juuri laissa olevien vaatimusten täyttämiseen sähköisessä muodossa.

4.3.3. Vastuusäännösten tarkistaminen

Sähköisiä allekirjoituksia koskevan lain (14/2003) 16 §:n mukaan yleisölle laatuvarmenteita tarjoava varmentaja on vastuussa vahingosta, joka laatuvarmenteeseen luottaneelle on aiheutunut siitä, että

- laatuvarmenteeseen merkityt tiedot ovat varmenteen myöntämishetkellä olleet virheellisiä,
- varmenteessa ei ole lain 7 §:n 2 momentissa mainittuja tietoja,
- laatuvarmenteessa yksilöidyllä henkilöllä ei varmenteen myöntämishetkellä ollut hallussaan varmenteessa mainittuja ja määriteltyjä allekirjoituksen todentamistietoja vastaavia allekirjoituksen luomistietoja,
- varmentajan tai tämän apunaan käyttämän henkilön luomat allekirjoituksen luomis- ja todentamistiedot eivät ole yhteensopivia, taikka

[57] Ibid. s. 13. Suosituksesta ei ilmene, halutaanko itse direktiivikohdan sanamuotoa muuttaa vai riittäisikö esimerkiksi komission tiedonannon tapainen selvitys yleisön informoimiseksi.

- varmentaja tai tämän apunaan käyttämä henkilö ei ole peruuttanut laatuvarmennetta lain 13 §:ssä säädetyllä tavalla.

Varmentaja vapautuu 1 momentissa säädetystä vastuusta näyttämällä, että vahinko ei ole aiheutunut sen omasta tai sen apunaan käyttämän henkilön huolimattomuudesta. Varmentaja ei vastaa vahingosta, joka aiheutuu laatuvarmenteeseen sisältyvän käyttörajoituksen vastaisesta käytöstä. Tämän mukaisesti on varmentajalla käänteinen todistustaakka. Vahinkoa kärsineen on sanamuodosta johtuen käytännössä näytettävä toteen syy-yhteys varmentajan laiminlyönnin ja vahingon välillä. Lain vastuupykälässä on lisäksi viittaus vahingonkorvauslakiin (412/1974).

Monet teleoperaattorit ja pankit katsovat, että laatuvarmenteita tarjoavan varmentajan sähköisiä allekirjoituksia käsittelevästä laista seuraavat vahingonkorvausvastuut ovat liiketoiminnallisesta näkökulmasta kohtuuton riski. Näiden näkemyksen mukaan laatuvarmentajalle tulisi sallia mahdollisuus rajata vahingonkorvausvastuut, myös tilanteissa, joissa laatuvarmentaja on aiheuttanut vahingon. Lain mukaista vastuuta[58] on operaattoreiden mukaan käytännössä mahdotonta vakuuttaa. Vastuusäännös estää joidenkin käsitysten mukaan yksityisten organisaatioiden ryhtymistä laatuvarmentajiksi.

Direktiivi ei kuitenkaan salli laatuvarmentajien vastuun osalta rajoituksia. Toisaalta varmentaja voi rajoittaa sen transaktion arvon, jossa varmenteita voidaan käyttää myös taloudellisin kriteerein, mitä käyttörajoituksen mahdollisuutta ei ole ilmaistu Suomen lakitekstissä, joskin se on selkeästi tuotu esiin lain perusteluissa. Mikäli EU:n piirissä syntyy keskustelua direktiivin avaamisesta laatuvarmentajien ja muiden varmentajien välisen vastuun eron tasoittamiseksi, voidaan vastuunrajoitusmahdollisuus nostaa keskusteluissa esille. Vastuusääntely on kuitenkin keskeinen elementti varmentajan toimintaan luottavan luottamuksen kannalta ja erottaa laatuvarmenteet muista varmenteista. Vastuu koskee lähinnä varmenteen tietosisällön oikeellisuutta, joka on varmentajan toiminnan

[58] Lain säännöksistä ei voida poiketa siten, että varmentaja rajoittaisi korvausvastuutaan. Vahingonkorvauslaki, johon sähköisistä allekirjoituksista annetussa laissa viitataan, sisältää kuitenkin sovittelusäännön (2:1:2), jonka mukaan korvausta voidaan sovitella, jos korvausvelvollisuus harkitaan kohtuuttoman raskaaksi ottaen huomioon vahingon aiheuttajan ja vahinkoa kärsineen varallisuusolot ja muut olosuhteet. Tätä säännöstä on sovellettu myös sopimussuhteissa, vaikka sopimussuhteet eivät pääsääntöisesti kuulukaan vahingonkorvauslain soveltamisalaan.

Toinen vahingonkorvauslaissa oleva säännöstö, joka voi tulla sovellettavaksi, on lain 4 luvussa oleva kanavointisäännöstö varmentajan henkilökunnan vastuusta. Kun vahingonkorvauslaissa säädetään korvattavaksi varallisuusvahinko kun vahinko on aiheutettu rangaistavaksi säädetyllä teolla tai julkista valtaa käytettäessä taikka milloin muissa tapauksissa on erittäin painavia syitä, ei laki sähköisistä allekirjoituksista tee tällaista rajausta vaan luottavan osapuolen kärsimät vahingot voivat olla ja käytännössä ovatkin juuri varallisuusvahinkoja.

keskeisin tarkoitus. Lisäksi varmentajan toiminnasta on muiden täysin mahdotonta esittää näyttöä. Nykyinen vastuusääntely on siten helposti perusteltavissa.

Kaupallisen varmennustoiminnan esteenä on, ettei vakuutusturvaa laatuvarmennustoimintaa varten ole saatujen lausuntojen perusteella nykyisillä säännöillä helposti saatavissa. Toisaalta tekniikka ja inhimillinen toiminta ei ole erehtymätöntä, ja elinkeinotoiminnassa on sangen vähän esimerkkejä vastuusta, jossa mitään vastuunrajoitusta ei voi käyttää - ehkä selkein tällainen tapaus on tuotevastuu kolmannelle henkilölle aiheutetusta vahingosta. Tuotevastuusta aiheutuvat vahingot ovat pääsääntöisesti henkilö- ja esinevahinkoja, kun taas varmentamistoiminnan virheistä aiheutuu puhtaita varallisuusvahinkoja.

Vertailun vuoksi voidaan todeta, ettei perinteisiä käsintehtyjä allekirjoituksia varmenna kukaan, ellei allekirjoituksen todistajia käytetä. Mahdollisuus keskustelun avaamiseen voi syntyä, mikäli EU:ssa haluttaisiin pohtia toimia kaupallisen laatuvarmennustoiminnan lisäämiseksi. Punnittavaksi tulisi se, kuinka paljon lisäaktiviteettia tulisi ja kuinka suuria vastuunrajoituksia käyttäjät olisivat valmiita sallimaan. Luottavaan osapuoleen ei ole sopimussuhdetta ja vastuunrajoituksen saattaminen kolmatta osapuolta velvoittavaksi voidaan oikeudellisesti kyseenalaistaa. Mahdollisuus vastuunrajoitukseen, mikäli sellainen haluttaisiin sallia, voitaisiin asettaa laissa asettamalla vähimmäisvastuu kuljetuslainsäädännön tavoin.[59] Muu vahingonkorvausoikeudellinen sääntely, meillä vahingonkorvauslaki, voi mahdollistaa vahingonkorvausten tuomitsemisen kohtuullisella tasolla. Vaikka vastuunrajoitukset olisi sallittu, ei varmentaja yleisen periaatteen mukaan voisi poistaa vastuutaan törkeästä huolimattomuudesta.

Miljoonaluokan transaktioita tuskin tehdään pelkästään varmenteisiin luottaen, mutta jos järjestelmät eivät ole vastuumielessä luotettavia, juuri mitään transaktioita ei voida tehdä sähköisesti. Ajateltavissa oleva vastuun vähimmäistaso transaktiota kohden saattaisi olla 500.000 - 1.000.000 euron luokkaa.[60] Sähköisen kaupankäynnin sääntelyn painopiste ei ole yksittäiset suuret transaktiot, jotka käytännössä hoidetaan perinteisin menetelmin. Pienehköt kuluttajatransaktiot, kuten lentolippujen

[59] Kuljetusoikeuden piirissä käydään keskustelua sopimusvapauden sallimisesta myös vastuusäännösten osalta.
[60] Jonkinlaista suuntaviivaa varmentajan vastuutasosta kaupallisilla markkinoilla tarjoaa kuljetuskaupan sopimuksia ja asiakirjaliikennettä hoitava Bolero.net. Asiakirjojen ja sanomien välityksestä ja validoinnista sekä varmentajana toimimisesta järjestelmä ottaa 100.000 Yhdysvaltain dollarin suuruisen vastuun kuhunkin käyttäjään nähden samasta virheestä tai laiminlyönnistä aiheutuneesta vahingosta. Järjestelmä hyväksyy miljoonan dollarin kokonaisvastuun kun vaatijoita samasta tapahtumasta on useita, ja vuotta kohden kaikkiaan 10 miljoonan dollarin vastuukaton. Ks. Bolero Standard Terms – Operational Service Contract, http://www.boleroassociation.org/downloads/op_sc.pdf, vierailtu 3.8.2003.

tilaaminen ovat kuitenkin siirtyneet sähköisen kaupankäynnin piiriin luottokorttiyhtiöiden kantaessa virheriskejä. Keskisuuret, korkeintaan muutaman sadan tuhannen euron suuruiset ja toistuvat transaktiot lienevät kriittisimpiä sähköisen kaupankäynnin menetelmien toimivuuden testauskohteita. Transaktion arvoon perustuva käyttörajoitusmahdollisuus on jo olemassa, mutta käyttörajoitukset voivat olla kaupallisessa varmennetoiminnassa hankalammin markkinoitavia ja rajoittavampia kuin transaktiokohtainen vastuunrajoitus. Vertauksena voidaan sanoa, että esimerkiksi rahdinkuljettajan olisi hankalaa rajoittaa palvelunsa jonkin arvon alittaviin rahteihin. On toisaalta mahdollista, että laatuvarmennetoimintaan liittyvät riskit tulevat kehityksen myötä myös vakuutusalalle helpommin hahmotettaviksi, jolloin rajoitusta ei tarvittaisi.

Toisena vastuukysymyksenä on nostettu esille kysymys siitä, kenen vastuulla on tarkistaa ja näyttää jälkikäteen toteen, oliko kuluttajan hallussa ollut allekirjoituksen luomisväline turvallinen allekirjoituksen tekohetkellä. Sähköisiä allekirjoituksia koskevan lain 5 §:ssä on määritelty luomisvälineen turvallisuusvaatimukset sekä kuinka niiden olemassaolo todennetaan. Turvallisen luomisvälineen käsitettä voidaan tarkastella myös ominaisuuksien muuttumattomuuden näkökulmasta. Toisaalta esille nousevat myös varmentajan kontrollimahdollisuudet käyttäjän hallussa oleviin välineisiin sekä laatuvarmentajan yleinen huolellisuusvelvollisuus. Myös luomisvälineen hyväksyvä tarkastuslaitos omaa vastuuta hyväksymästään luomisvälineestä. Lainsäädännön muutoksia ei luomisvälineen turvallisuutta koskevan kysymyksen osalta ole toivottu ja kysymys onkin sangen monitahoinen yksityiskohtaisesti säänneltäväksi.

Laissa erityisesti säänneltyjen kehittyneiden sähköisten allekirjoitusten toistaiseksi vähäisen käytön vuoksi eivät niiden käyttöön liittyvät erilaiset vastuutilanteet liene käytännössä vielä aktualisoituneet.

4.3.4. Sulkulistan säilyttäminen

Laissa ei ole määritelty, kuinka kauan sulkulistaa ja sen tarkastamista koskevat tiedot tulisi säilyttää. Väestörekisterikeskus on ilmoittanut, että säilyttäminen on ohjeistettu tapahtuvaksi periaatteessa ikuisesti. Käytännössä ongelmaa ei siis juuri ole olemassa, ellei käytäntö muutu.

Sulkulistan tarkastaminen tehdään käytännössä yleensä reaaliaikaisesti. Voidaan ajatella, että tämä voitaisiin määritellä myös oikeudellisena velvollisuutena. Jos luottavan osapuolen edellytetään tarkistavan sulkulista transaktion yhteydessä, seuraa tämän laiminlyömisestä helposti varmentajan

vapautuminen vastuusta. Tämän vuoksi velvollisuus tarkistaa sulkulista ajallaan seuraa käytännössä jo muutenkin. Kyse on kuitenkin siitä, tarvitaanko sähköisiä allekirjoituksia pidempiaikaisiin käyttötarkoituksiin, joissa tarkistaminen tapahtuu vasta esimerkiksi kymmenien vuosien päästä. Sulkulistan säilyttämisellä on merkitystä varmentajan tai luottavan osapuolen vastuunjaon tekemiseksi. Sillä voi olla merkitystä myös muissa kuin varmentajaan liittyvissä suhteissa. Säilyttämisvelvollisuuksien kannalta ovat kaupallisissa suhteissa olennaisia myös yleiset siviilioikeudelliset vanhentumisajat, sillä sähköisiä allekirjoituksia voidaan tarvita näytön aikaansaamiseksi esimerkiksi sopimusvelvoitteen syntymisestä. [61] Vanhentumisaikojen umpeen kulumisen jälkeenkin syntyy tilanteita, joissa alkuperäisen oikeustoimen pätevyys voi joutua tarkasteltavaksi. Tällaisia olisivat esimerkiksi velkasuhteissa olevat kuittausvaatimukset sekä erilaiset transaktiot perhe- ja perintöoikeuden kannalta tarkasteltuina. On huomattava, että yleinen oikeustoimien muotovapaus vähentää allekirjoituksen pätevyyden merkitystä, joten sulkulistalla olevat merkinnät eivät sellaisinaan todennäköisesti synnytä tai evää oikeustoimen oikeusvaikutuksia. Tämä seikka tietenkin puhuu sulkulistamerkintöjen säilyttämistä vastaan. Mikäli sähköisiä allekirjoituksia jossain vaiheessa voitaisiin käyttää kiinteistön saantokirjojen kaltaisissa konstitutiivisissa asiakirjoissa, olisi sulkulistan säilyttämisen seurattava saantoja koskevien moitekanteiden nostamismahdollisuutta.

Koska VRK laatuvarmentajana on ottanut sen kannan, että sulkulistoja säilytetään ainakin toistaiseksi käytännössä jatkuvasti, eivät lailla tehdyt täsmennykset säilyttämisvelvollisuuteen ole välttämättömiä tässä vaiheessa.

4.3.5. Luomisvälineen turvallisuus

Viestintävirasto on huomauttanut, että laissa tai direktiivissä ei oteta kantaa siihen, kuinka luomisvälineen turvallisuus todetaan, ellei sitä totea tarkastuslaitos. Tässä yhteydessä voidaan viitata Liikenne- ja viestintäministeriön tekemään selvitykseen Turvalliset sähköisen allekirjoituksen luomisvälineet, Vaatimusten arviointi (Liikenne- ja viestintäministeriön julkaisuja 52/2004). Täyttääkseen vaatimukset luomisvälineen on oltava joko EU:n hyväksymien standardien mukainen tai sen on täytettävä suoraan EU-direktiivin vaatimukset. Jos luomisvälineen on hyväksynyt tarkastuslaitos tai se on standardin mukainen, täyttää se aina direktiivin vaatimukset. Jos kumpikaan ehto ei täyty, on luomisväline silti mahdollista katsoa turvalliseksi. Käytännössä tällöinkin on jonkun tehtävä tehtävä kyseinen arviointi, viimekädessä valvovan viranomaisen, jollei kukaan muu sitä tee.

[61] Ks. Laki velan vanhentumisesta 728/2003.

TeliaSonera Finland katsoo puolestaan, että turvallinen allekirjoituksen luomisväline tulisi määritellä tavalla, joka tarjoaa mahdollisuuden tarjota hyväksyttyjä tällaisia välineitä riittävän joustavasti. Nyt ei ole selvää, tarkoitetaanko turvallisella allekirjoituksen luomisvälineellä esim. pelkästään sirukorttia vaan myös mahdollisesti kortinlukijaa, ohjelmistoja ja jopa käyttöjärjestelmää, mikä tekee yhtälöstä varmenteen käyttäjän näkökulmasta hyvin monimutkaisen ja vaikeasti hallittavan.[62] Esimerkiksi matkapuhelinten osalta tällaisten vaatimusten täyttäminen tarkastuslaitosten hyväksyminä on käytännössä mahdotonta.

Elisa Oyj ilmoittaa, että turvallisia allekirjoituksen luomisvälineitä (secure signature-creation-device) eli ennen kaikkea turvaevaluoituja ja sertifioituja älykortteja on huonosti saatavilla markkinoilla ja näihin liittyy liiketoiminnallisesta näkökulmasta katsottuna kohtuuttoman suuria kustannuksia. Elisan mielestä vaatimustasoa tulisikin kohtuullistaa. Elisa katsoo, että Suomessa ei ole käytössä turvallista allekirjoituksen luomisvälinettä, sillä markkinoilla ei ole käytännössä saatavissa turvaevaluoituja turvallisen allekirjoituksen luomislaitteen vaatimukset täyttäviä älykortteja. Elisa onkin ehdottanut luomisvälineitä koskevan vaatimustason hienoista madaltamista.

Liikenne- ja viestintäministeriön teettämässä selvityksestä ´Turvalliset sähköisen allekirjoituksen luomisvälineet, Vaatimusten arviointi´ ilmenee, että EU:n jäsenmaissa on allekirjoitusvälineiden arviointitoiminta vielä alkuvaiheessaan ja epäselvyyttä vallitsee siitä, onko etukäteen suoritettava allekirjoitusvälineen hyväksyttäminen ylipäätään tarpeellista vai ei. Monissa maissa arviointi ilmoitetaan suoritettavan tapauskohtaisesti joko muiden maiden arviointilaitosten tai oman maan valvontaviranomaisten toimesta, jos arvioinnille ilmenee tarvetta. Tällainen käytäntö luo käytännössä joustavuutta. Itse asiassa varmentaja ottaa itse riskin joustaessaan luomisvälineelle asetetuista vaatimuksista. Lainsäädäntöön ei tällaista lievempää tulkintaa voida ottaa direktiivin velvoittavuuden vuoksi ja direktiivin vaatimuksista joustaminen olisi taas jäsenvaltioiden lojaliteettiperiaatteen vastaista. Periaatteessa asia olisi siis ratkaistava eurooppalaisella tasolla. Lainsäädäntöä voi tällöinkin olla epämielekästä muuttaa pelkästään väliaikaisista kaupallisista syistä. Toisaalta valvontaviranomainen voi yksittäistapauksessa huomioida väliaikaiset ongelmat.

[62] Liikenne- ja viestintäministeriön julkaisu 52/2004 ´Turvalliset sähköisen allekirjoituksen luomisvälineet. vaatimusten arviointi´ katsoo luomisvälineen olevan fyysisen laitteen ja sen toiminnan mahdollistavien ohjelmistokomponenttien muodostama kokonaisuus. Esimerkkeinä mainitaan toimikortti, sen lukijalaite, lukijalaitteen ajurit sekä selainkäytön mahdollistavat ohjelmistomodulit. Vastaavasti matkapuhelin ja allekirjoitusominaisuuden sisältävä SIM-kortti muodostavan allekirjoituksen luomisvälineen.

Edellä mainitussa selvityksessä katsotaan kuitenkin, että luomisvälineen määritelmä tulisi lainsäädännössä tarkentaa, sillä sen sisällöstä vallitsee kirjava joukko käsityksiä eri toimijoiden joukossa. Standardit määrittelevät luomisvälineelle asetettavia vaatimuksia, joten luomisvälineen käsite täsmentyy tätä kautta. Itse lakiteksti ei sinänsä anna johtoa siitä, mistä täsmälleen on kysymys.

4.3.6.Kuinka laatuvarmenteen hakija tunnistetaan?

Laatuvarmentajan on tunnistettava hakija henkilökohtaisesti sähköisiä allekirjoituksia koskevan lain 12 §:n nojalla. On esitetty, että tämä kohta voitaisiin tarkistaa kuulumaan siten, että varmenteen hakija voidaan tunnistaa laatuvarmenteella. Tämä varmistaisi tarkoituksenmukaisemman varmenteiden rekisteröimisen ja uusimisen. Jos kortin haltija kuitenkin on luovuttanut korttinsa ja pinkoodin jonkun muun käyttöön, voi väärinkäytöksiä ilmetä. Rekisteröintiprosessi on kriittinen kohta varmenteissa koska sen jälkeen henkilöllisyyttä ei enää tarkisteta mitenkään vaan luotetaan varmentajaan. Väärinkäytökset ovat kuitenkin rikosoikeudellisenkin tarkastelun piirissä, joten varmentaja ei ole ainoa käytössä oleva kontrollimekanismi.

Laatuvarmennetasoinen tunnistamisratkaisu voitaisiin mahdollistaa esimerkiksi varmennetta uusittaessa. Tässä yhteydessä olisi kuitenkin harkittava muutoksen kytkemistä mahdolliseen sähköisen tunnistamisen sääntelyn kehittämiseen.

5. MAHDOLLISIA UUSIA SÄÄNTELYKOHTEITA

5.1. Sähköinen tunnistaminen

Liikenne- ja viestintäministeriön selvityksessä ´Sähköisen tunnistamisen menetelmät´, Liikenne- ja viestintäministeriön Julkaisuja 44/2003, katsottiin, että henkilön sähköisen tunnistamisen ja teknisen valvonnan osalta tarvetta sääntelylle on olemassa. Selvityksessä asetuttiin kuitenkin sille kannalle, että käyttäjätunnuksella ja salasanalla sekä vaihtuvilla salasanoilla ja varmenteilla tapahtuva käyttäjän tunnistaminen on nykyisellään varsin toimivaa, eikä vaadi tällä hetkellä muutoksia tai lisäyksiä nykyiseen lainsäädäntöön. Sen sijaan uusien biometristen tunnistusmenetelmien katsottiin asettavan vaatimuksia sääntelylle. Yhtenä vaihtoehtona selvityksessä pohdittiin ´laatubiotunnisteen´ käsitteen kehittämistä.

Sähköinen tunnistaminen on yksi etätunnistamisen muoto ja käytännössä useissa tapauksissa erittäin käyttökelpoinen tunnistamismuoto. Esimerkkinä säännöistä, joissa säännellään yksityiskohtaisesti sähköistä tunnistamista, on keskusrikospoliisin rahanpesun selvittelykeskuksen julkaisema ´Rahanpesun torjunnan parhaat käytänteet´, jossa edellytetään tunnistamista laatuvarmenteella tai muulla tietoturvallisella ja todisteellisella tunnistautumistekniikalla.[63] On huomattava, ettei laatuvarmenteita ole sellaisenaan luotu tunnistautumis- vaan allekirjoitustarkoituksiin, jolloin siis allekirjoitusfunktiota olisi käytettävä tunnistautumiseen.

Olivatpa rahanpesua koskevat kotimaiset ohjeistukset onnistuneita tai ei, on rahanpesun valvonta sekä kansallista että rajat ylittävää toimintaa. On luonnollista, että rajat ylittävissä etätunnistautumisissa sähköiset tunnistamismahdollisuudet ovat erityisen käyttökelpoisia. Sitä mukaa kuin esimerkiksi rahoituspalvelujen yhteismarkkinat edistyvät, syntyy entistä enemmän tilanteita sähköistä etätunnistamista varten. Palvelun tarjoajan on tunnistettava asiakkaansa, kuten rahanpesutapauksessa, ja asiakkaan on luotettavasti tunnistettava palvelun tarjoaja petosten torjumiseksi.[64] Liikekumppanin tunnistamisvelvollisuudesta voidaan antaa erityissäännöksiä, mutta henkilön tunnistaminen on yleensä normaalin huolellisuuden piiriin kuuluvaa toimintaa, ja institutionalisoitujen välineiden luominen tätä tarkoitusta varten vaikuttanee henkilöiden todistamistaakkaan. Jos yleisesti tunnustettuja menetelmiä on käytetty, voidaan huolellisuutta yleensä tällöin katsoa noudatetun.

Rajat ylittävien transaktioiden lisääntymisen ohella myös terrorismin ja rikollisuuden torjunta saattaa asettaa uusia vaatimuksia, joita on tarkasteltava tietenkin yhdessä tietosuojaa ja yksityiselämän suojaa koskevien vaatimusten kanssa. Laatuvarmennetekniikka voisi toimia yleisesti tunnustettuna tunnistautumisen välineenä ainakin Euroopan tasolla, mutta sen lisäksi tarvittaisiin yhteentoimivuuden edistämistä eri maissa käytettyjen varmenteiden käytettävyyden edistämiseksi muissa jäsenmaissa.[65]

---

[63] Muulla tietoturvallisella ja todisteellisella tunnistautumistekniikalla tarkoitetaan sellaista varmennetta, joka täyttää sähköisistä allekirjoituksista annetussa laissa (14/2003) laatuvarmenteelle asetetut vaatimukset. Kuten aikaisemmin on todettu, vaatimukset ovat epäjohdonmukaisia.

[64] Ks. Euroopan parlamentin ja neuvoston direktiivi 2002/65/EY, annettu 23 päivänä syyskuuta 2002, kuluttajille tarkoitettujen rahoituspalvelujen etämyynnistä ja neuvoston direktiivin 90/619/ETY sekä direktiivien 97/7/EY ja 98/27/EY muuttamisesta, EYVL L 271, 9.10.2002 s. 16. Direktiivi ei sisällä tunnistamista tai tunnistautumista koskevia määräyksiä, mutta kansallisten viranomaisten määräykset voivat säännellä asiaa.

[65] Tekniikka ei normaalisti sinänsä luo uusia tunnistustarpeita. Etäasioinnin luonteeseen kuuluu transaktioiden tekeminen ja tietojen vaihto sellaisen tahon kanssa, jota ei voida tunnistaa fyysisesti henkilöllisyystodistuksesta, konttorin tai liikepaikan perusteella, ja etäasioinnissa maksu tapahtuu säännönmukaisesti luotolla. Myös se seikka, että transaktiota tehdään koneiden kanssa, tuo oman lisänsä sähköisen tunnistamisen tarpeeseen.

Voidaan katsoa, että rahanpesua varten laaditut, vaikkakin käsitteellisesti joltain osin ristiriitaiset säännöt toimivat kuitenkin viitteenä siitä, että laatuvarmennetasoista tunnistautumisratkaisua kannattaisi pohtia lainsäädännön tasolla. Mikäli luotettavia sähköisiä tunnistautumisratkaisuja säänneltäisiin lainsäädännössä yhdessä paikassa, voitaisiin muualla lainsäädännössä viitata esimerkiksi tietyt perusvaatimukset täyttävään tunnistautumisvarmenteeseen tapauksissa, joissa henkilön vahva tunnistaminen on tarpeen. Sinänsä ei ole mitään syytä rajoittaa luotettavan tunnistamisen mahdollisuutta laatuvarmenteisiin, jos muutkin ratkaisut täyttävät luotettavat tunnistustarpeet.[66]

Sääntelytarvetta ei tulisi tarkastella vain nykyisten erityisalojen sääntöjen perusteella, vaan eurooppalaisen tietoyhteiskunnan infrastruktuuria tulisi tarkastella kokonaisuutena tulevaisuuden kannalta. EU on luonut runsaasti sääntöjä informaatioyhteiskuntaa varten, mutta kehitys ei monilla aloilla ole ollut Eurooppa-neuvoston Lissabonissa vuonna 2000 asettamien tavoitteiden mukainen, eikä sähköisen asioinnin sääntelyn todellista tarvetta siis voida vielä täysin arvioida.[67] Monet alakohtaiset säännöt, kuten rahoituspalvelujen etämyyntiä koskeva direktiivi, on vasta implementoitu jäsenmaissa eivätkä ole muodostuneet käytännön kannalta vielä keskeisiksi. On kuitenkin syytä uskoa, että sähköisen asioinnin merkitys sisämarkkinoilla kasvaa ja uudenlaisia tarpeita sähköiseen etätunnistamiseen voi syntyä, pontimenaan tietenkin tarve sovittaa yhteen tehokkuusnäkökohdat ja korkea tietosuojan ja tietoturvan taso.

Esimerkiksi terveydenhuollon alalla, jossa sähköisen asioinnin osalta ollaan tekemässä pilottikokeiluja, luodaan palveludirektiivin avulla yhteismarkkinoita. Terveyspalvelujen yhteismarkkinat saattavat luoda uusia tarpeita sähköiseen etätunnistamiseen. Toisena esimerkkinä voidaan mainita, että kansalaiset voivat meillä asioida HST-kortin ja pankkitunnisteiden avulla eläke- ja sosiaaliturva-asioissaan. Kun työvoima liikkuu vapaasti ja eläketurvaa karttuu useiden maiden laitoksiin, voivat nämäkin asiointimahdollisuudet joskus ylittää rajat. Kysymys on tietenkin myös organisatorisista järjestelyistä ja standardoinnista.

Liikenne- ja viestintäministeriö lähetti vuonna 2003 julkaisemansa selvityksen lausuntokierrokselle, jossa saadut vastaukset on julkaistu ministeriön kotisivuilla. Tämän lisäksi on todettava, että kansallisen tietoturvastrategian yhteydessä on keväällä 2005 käynnistynyt liikenne- ja viestintäministeriön vetovastuulla hanke ´Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja´, joka pyr-

[66] Tämäntyyppistä ratkaisua on puoltanut Terveydenhuollon oikeusturvakeskus.

kii edistämään biometriaa hyödyntävää tietoturvallista palvelukehitystä ja alan toimijoiden toimintamahdollisuuksia. Hankkeessa pyritään edistämään biometriaa hyödyntäviä palveluja koskevaa luottamusta biometriaan yksityisyyden suojan näkökulmasta liittyvien tietoturva- vaatimusten arvioinnilla ja analysoinnilla. Lisäksi pyritään arvioimaan lainsäädännön mahdollisia muutostarpeita jatkossa.

Kirjallisuudessa esiintyy myös näkemys, jonka mukaan sähköisiä allekirjoituksia koskeva direktiivi itse asiassa joiltakin osin antaisi oikeusvaikutuksia sähköisille allekirjoituksille myös tunnistamistarkoituksessa.[68] Selkeämmin tämä koskee direktiivin 5 artiklan 2 kohtaa. Tätä kohtaa ei ole sellaisenaan sisällytetty Suomen sähköisiä allekirjoituksia koskevaan lakitekstiin, mutta sen periaatteet ovat tavallaan jo oikeusjärjestyksessämme sisällä.

Näkemykset sähköisen tunnistamisen lainsäädännön tarpeesta vaihtelevat. Väestörekisterikeskus katsoo, että sähköistä tunnistamista koskeva lainsäädäntöä olisi laadittava samoin periaattein kuin sähköistä allekirjoitusta koskien, eli ainakin tietty laissa kriteereiltään yksilöity menetelmä täyttäisi kehittyneet tunnistamisvaatimukset. Tämän lisäksi lakia tulisi muokata pitämään tunnistamis- ja allekirjoitusfunktiot toisistaan selvemmin erillään. Nykyinen laki antaa Väestörekisterikeskuksen mukaan ymmärtää, että sähköistä allekirjoitusta voidaan käyttää myös tunnistamiseen, mikä ei vastaa teknisten standardien ja käytössä olevien varmennekenttien mukaista jaottelua. VRK:n mielestä sähköistä allekirjoitusta koskevassa laissa voisi selventää, että varmennus tapahtuu sopimuksen mukaiseen käyttötarkoitukseen. Kun laki ei käsittele tunnistamista, täytyy käyttötarkoituksia sopimuksessa ja tiedottamisessa kuvattaessa käyttää käsitteitä, joita laissa ei ole. Myös Tietosuojavaltuutettu on tukenut sähköisen tunnistamisen sääntelyä yleisesti.

Kun allekirjoittajan vahva tunnistaminen on kehittyneen sähköisen allekirjoituksen käytön sivutuote, joka täyttää saman tietoturvatason kuin allekirjoitusvarmenne, ja varmennekäytännössä esiintyy tarve laatuvarmennetasoiseen tunnistautumiseen, voitaisiin lakiin helposti lisätä tunnistusvarmenteen käsite, joka olisi laatuvarmenne allekirjoitusvarmenteen tavoin. Tällöin varmentaja varmentaisi tunnistautuvan henkilön oikean henkilöllisyyden tai pseudonyymin samalla vastuulla kuin allekirjoituksen. Siinä missä laatuvarmenteeseen, kehittyneeseen sähköiseen allekirjoitukseen

---

[67] Ennen vuosituhannen vaihdetta vallinneet arviot sähköisen kaupankäynnin kehityksestä eivät toteutuneet, mutta toisaalta UNCTAD:in julkaisemat E-Commerce and Development Report 2002 ja 2003 kertovat, että kehityksessä on ollut vain vuoden viive.

[68] Thomas Myhr, Regulating a European eID, A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005, ss. 11 - 15 ja siinä mainittu lähde.

ja turvalliseen allekirjoituksen luomismenetelmään perustuva allekirjoitus täyttävät käsintehdyn allekirjoituksen vaatimukset, vastaisivat vastaavasti muotoiltavat vaatimukset täyttävän sähköisen tunnistamismenetelmän käyttäminen henkilön tunnistamista viranomaisen antaman henkilöllisyystodistuksen perusteella.[69]

HST-kortilla on kaksi varmennetta, toinen allekirjoitus- ja toinen tunnistamistarkoitukseen, joista allekirjoitusvarmenne on laatuvarmenne ja tunnistautumisvarmenne taas ei. Mikäli tunnistautumislaatuvarmenne määriteltäisiin lakitasolla, säännöksessä[70] tulisi nimenomaisesti todeta, ettei kyseinen varmenne ole välttämättä ainoa saman turvallisuustason täyttävä tunnistuskeino, joten muutkin markkinoilla käytössä olevat menetelmät voivat täyttää luotettavan tunnistautumisen tai vahvan tunnistamisen vaatimukset. Lisäksi perusteluissa voitaisiin todeta, että tunnistamisen tarve ja taso määräytyvät tilanteen mukaan, ellei erityissäännöksissä nimenomaisesti määriteltäisi käytettäviä menetelmiä, kuten on laita rahanpesun suhteen.

Monien teleoperaattorien näkökulma sähköisen tunnistamisen sääntelyyn on myös myönteinen. Nämä katsovat, että laatuvarmenteiden yleisen käytön ja tarjoamisen näkökulmasta tulisi lainsäädännössä myös huomioida muutkin kuin sähköisen allekirjoituksen soveltamisalueet. Käytännössä laatuvarmenteiden tarjoaminen on säädetty sähköisen allekirjoituksen näkökulmasta, jolloin muiden sovellusalueiden tarkastelu sähköisen allekirjoituksen kautta ei ole aina selkeää ja tarkoituksenmukaista. On myös katsottu, että tunnistus- ja allekirjoitusvarmenteita olisi kohdeltava yhtäläisesti laatuvarmenteina, koska niiden turvataso on käytännössä yhtä hyvä. Myös varmenneteknologian tuottajat kannattavat selkiinnyttämistä ja tunnistamisen sääntelyä.

Tunnistamisen sääntely herättää myös vastustusta alan toimijoiden keskuudessa mm. pankkisektorilla ja Viestintävirastossa. On katsottu, että uuden toimialan ja monelta osin teknisesti elinkaarensa alussa olevien palvelujen sääntely lainsäädännössä ei ole perusteltua. Lisäsääntely aiheuttaa ensi kädessä kustannuksia, sillä olemassa olevat järjestelyt kuten TUPAS-standardi voitaisiin joutua

---

[69] Henkilön tunnistaminen henkilöllisyystodistuksen perusteella on tapaoikeuteen ja viranomaiskäytäntöön perustuva toimenpide. Ks. Keskusrikospoliisi, Rahanpesun selvittelykeskus, Rahanpesun torjunnan parhaat käytänteet, jossa todetaan (s. 12), että ”(l)uonnollisen henkilön henkilöllisyyden todentamisen on perustuttava luotettavaan asiakirjaan tai sähköiseen varmenteeseen. Luotettavia viranomaisen myöntämiä tunnistamisasiakirjoja ovat ainakin voimassaoleva a) ajokortti, b) poliisiviranomaisen antama henkilökortti, c) passi sekä d) kuvallinen Kela-kortti.” Muuhun asiakirjaan perustuvan henkilöllisyyden todentamisen luotettavuus perustuu yksittäistapauksselliseen kokonaisharkintaan.

[70] Mikäli sääntely tapahtuisi sähköisiä allekirjoituksia koskevassa laissa 14/2003, voitaisiin säännökset ottaa lain 18 §:ään, jossa säännellään lain mukaisen sähköisen allekirjoituksen oikeusvaikutukset. Pykälään voitaisiin liittää myös sähköisiä allekirjoituksia koskevan direktiivin 5 artiklan 2 kohta. Pykälään liitettäisiin sähköisen tunnistamisen vaikutusta koskevat maininnat.

tarkistamaan. Sähköisen kaupan ja asioinnin sääntelyssä on aina ongelmana teknologianeutraliteetti ja teknologian kehittyminen. Viestintävirasto katsoo, että avoimiin käyttäjäryhmiin soveltuvia tunnistus- ja allekirjoitusmenetelmiä olisi kyllä kehitettävä, mutta toisaalta yleiset sopimus- ja todistusoikeudelliset sekä kuluttajaopit kantavat pitemmälle kuin hätäisesti tiettyä ilmiötä varten laadittu lainsäädäntö. Hallinnon puolella voi olla kuitenkin olla tarvetta ohjeistukseen tai erityissääntelyyn. Tullilaitos viittaa valtiovarainministeriön ohjeeseen ja toteaa, että tunnistautumisvelvollisuus tulee muusta lainsäädännöstä. Selvityksen yhteydessä käydyssä keskustelussa esiintyi halua pitää tunnistamisen sääntely vain ´parhaiden käytäntöjen´ tasolla.

Laki sähköisistä allekirjoituksista ei kuitenkaan liene oikea sääntely-ympäristö sähköisen tunnistamisen laajemmalle sääntelylle, jossa huomioitaisiin myös eri menetelmien tietosuojavaatimukset. Toisaalta laki voisi, ainakin mahdollisen tulevaisuudessa tapahtuvan kokonaisuudistuksen yhteydessä, käsitellä laatuvarmenteiden ja tunnistamisen suhdetta myös lakitasolla. Voidaan pitää epätyydyttävänä, että valtaosassa tapauksia, joissa laatuvarmenneteknologiaa käytetään, eivät juridiset hyödyt, ennen kaikkea varmentajan korvausvastuu koidu luottavan osapuolen hyväksi samalla sitovuudella, koska kyseessä ei ole laatuvarmenne. Tämä perustuu myös käytettyihin määritelmiin. Varmenne tunnetaan direktiivissä ja laissa vain allekirjoituksen todentamiseen käytettävien tietojen yhdistämisessä henkilöön vahvistaen tämän henkilöllisyyden. Määritelmässä ei puhuta allekirjoitustarkoituksesta, vaikka tätä lienee tarkoitettu. Direktiivin sanamuoto ei kuitenkaan estä kansallisessa lainsäädännössä tehtävää laajempaa määritelmän käyttöä, eikä siitä johtuvia vastuu- ym. lisäseuraamuksia sähköisten allekirjoitusten käyttöä koskevien seuraamusten lisäksi.

Kehittyneen sähköisen allekirjoituksen määritelmään kuuluu, että sillä voidaan yksilöidä allekirjoittaja ja todeta sanoman eheyden säilyttäminen. Laatuvarmenteelle direktiivissä ja laissa asetetut vaatimukset täyttyvät niitä sovellettaessa myös tunnistamisfunktioiden osalta. Tämän vuoksi laissa voitaisiin tehdä selkeämpiä rinnastuksia tunnistamis- ja allekirjoitusfunktioiden välillä. Rinnastus käsittäisi selkeitä oikeusvaikutuksia, jos laatuvarmentajan käännetyn todistustaakan mukainen vastuu samalla täsmennettäisiin toteutuvaksi pelkästään tunnistamista varmennettaessa ja lain soveltamisala laajennettaisiin myös pelkkään tunnistamiseen. Tunnistamisen vaatimuksen täyttäminen todistusvoimaisella tavalla vaikuttaisi myös tunnistusvaatimuksen esittäjän vastuun arvioinnissa käytettävänä tekijänä aineellisessa lainsäädännössä olevien velvoitteiden, kuten salassapitovelvoitteiden noudattamiseen liittyvien tai rahanpesun ehkäisemiseen liittyvien tunnistustarpeiden yhteydessä. Tällaisiksi ”laatutunnistusvarmenteiksi” voitaisiin jatkossa tarpeen mukaan nimetä myös muita tunnistusvarmenteita, kuten biotunnisteita.

5.2. Aikaleimapalvelut

Aikaleimalla ymmärretään suppeammin sähköistä todistusta, joka sisältää viittauksen kohteena olevan tiedoston hash-koodin ja ajanmäärityksen. Todistuksen antaa aikaleimapalvelun tarjoaja epäsymmetrisellä PKI-tekniikkaan perustuvalla salauksella eli digitaalisella allekirjoituksella. Aikaleima yleisemmässä merkityksessä voi tarkoittaa mitä tahansa ajan määritystä, jonka tietojärjestelmä lisää tiedostojen metatietoon tai lokitietoihin. Ajanmäärityksellä on myös tekninen merkitys, sillä monien ohjelmien käyttö voi kompastua virheelliseen ajanmääritykseen. Aikaleimaa tarkastellaan tässä yhteydessä ensiksi mainitussa merkityksessään.

Aikaleimapalvelujen tarjoamisen aloittamista tässä merkityksessä tiettävästi harkittiin Väestörekisterikeskuksessa vuosituhanteen vaihteessa, mutta siitä luovuttiin kustannussyistä. Mittatekniikan keskus MIKES seuraa kuitenkin julkiseen ja yksityiseen sähköiseen asiointiin liittyvien aikaleimausten tarpeellisuutta. MIKES on ollut aiemmin mukana laajassa valtakunnallisessa sähköisen asioinnin pilottihankkeessa, jota koordinoi Väestörekisterikeskus.

Aikaleima osoittaa tapahtuman tai toimenpiteen täsmällisen ajan ja kiinnittää varmenteen kansallisesti oikeaan aikaan. Tämä on tarpeen silloin kun laki asettaa toimenpiteelle jonkin aikarajan, tai toimenpiteen ajankohtaan liittyy joitakin oikeusvaikutuksia, kuten se seikka, onko varmenne ollut allekirjoituksen laatimishetkellä voimassa vai ei. Käytettäessä kehittyneitä sähköisiä allekirjoituksia ei nimittäin ilman eri toimenpiteitä voida välttämättä tietää, tehtiinkö sähköinen allekirjoitus itse asiassa varmenteen voimassaoloaikana vai ei. Aikaleimat edesauttavat myös kehittyneiden sähköisten allekirjoitusten pitkäaikaista arkistointia tietojärjestelmien kehittyessä.

Lisäkäyttöä aikaleimoille voisi tulla muun EU-lainsäädännön yksityiskohtaisten vaatimusten täyttämisestä.

- Sähköisen kaupankäynnin direktiivissä 2000/31/EY ja siihen perustuvassa kansallisessa laissa[71] vaaditaan, että tietoyhteiskunnan palvelujen tarjoaja pitää tiettyjä tietoja verkkoasiakkaan saatavilla ja myös sopimusehdot siten, että asiakas voi tallentaa ja toisintaa ne. Todistustaakka on palvelun tarjoajalla. Mikäli verkkosivujen pitäjä aika-

[71] Laki tietoyhteiskunnan palvelujen tarjoamisesta 458/2002.

leimaa verkkosivujensa sisällön säännöllisesti, hän voi näyttää toteen edellä mainittujen vaatimusten täyttämisen.

- Sähköisen viestinnän tietosuojalaki (516/2004) mm. sisältää suoramarkkinointia koskevia vaatimuksia, jolloin markkinointiviestinnän lähettäjällä on näyttövelvollisuuksia, joiden täyttämisessä aikaleimat voisivat olla käyttökelpoisia.

- Aikaleimoilla voitaisiin tyydyttää arvonlisäverodirektiivin 2001/115/EY vaatimukset, jotka edellyttävät, että verkkolaskujen autenttisuus ja eheys pitää näyttää toteen.

- Uudet julkisten hankintojen direktiivit tuovat esille sähköisten julkisten hankintojen menettelyt. Nämä menettelyt ovat yksityiskohdiltaan osin vielä täsmentymättä, mutta ajanmääritykset voivat olla oleellisia eri vaiheiden, kuten tarjousten tekemisen ja avaamisen kannalta. Kuntaliitto on katsonut aikaleimapalvelun olevan julkisten hankintojen kannalta tärkeä.

Aikaleimoja on tähän mennessä säännelty ainakin Saksan, Italian ja Viron lainsäädännössä.

Saksan digitaalisia allekirjoituksia käsittelevä laki[72] vuodelta 1997 ja sen nojalla annettu asetus sisälsi aikaleiman määritelmän ja vaatimuksen, että varmentajan tuli pyynnöstä varustaa aikaleimalla sähköinen tieto. Lisenssiä varten tuli osoittaa riittävien resurssien olemassaolo aikaleimapalvelun tarjoamiseen. Aikaleimoja koskeva lain 6 § sisälsi joukon palvelun luotettavuuteen liittyviä vaatimuksia mm. viivytysten välttämiseksi. Laki on sittemmin korvattu EU-direktiivin mukaisella lailla.

Viron digitaalisia allekirjoituksia koskeva laki (RT I 2000, 26, 150, täydennetty useaan otteeseen) vuodelta 2000 sisältää luvussa IV määräyksiä aikaleimapalveluista ja aikaleimoja koskevien palvelujen tarjoamisesta.[73] Viron lain

- 23 § sisältää aikaleiman määritelmän,
- 24 § asettaa joitakin aikaleimapalveluille tarkoitettuja yleisempiä vaatimuksia,

[72] Signaturgesetz , Bundesgesetzblatt 1997 I 1872 (Artikel 3 Informations- und Kommunikationsdienstegesetz, Bundesgesetzblatt 1997 I 1870)

[73] Ks. aikaleimapalveluista virolaisen palveluntarjoajan Cybernetica AS:n aineisto Timestamping Service and digital signature applications, http://www.timestamp.cyber.ee/ato/principles.html, vierailtu 14.2.2005.

- 24 ja 25 § asettavat vaatimuksia aikaleimapalvelujen tarjoajille,
- 27 § määrittää aikaleimapalvelujen tarjoamisessa käytettävien aikaleimausperiaatteiden sisällön,
- 28 § määrittelee aikaleimapalvelun tarjoajan velvollisuudet
- 29 § asettaa työntekijöille luotettavuusvaatimuksen
- luku V sisältää määräyksiä myös aikaleimapalvelun tarjoamisen lopettamisesta
- 38 § asettaa kaikille palvelun tarjoajille vahingonkorvausvelvollisuuden
- 39§ velvoittaa palvelun tarjoajan vakuuttamaan vastuunsa

Sähköisiä allekirjoituksia koskeva direktiivin johdantolauseessa 6 todetaan, että varmennepalvelujen määritelmän ei tulisi rajoittua varmenteiden antamiseen ja ylläpitoon, vaan sen pitäisi käsittää myös sähköisiä allekirjoituksia käyttävät tai niihin liittyvät palvelut, kuten rekisteröinnin, aikaleimat, luetteloiden ylläpitämisen sekä tietotekniset ja konsulttipalvelut. Myös direktiivin artikla 2(11) sisältää laajan varmennepalvelujen tarjoajan määritelmän. Tämän vuoksi aikaleimapalvelujen tarjoajat ovat samojen sääntöjen alaisia kuin varmennepalvelujen tarjoajat. Käytännössä tämä tarkoittaa erityisesti tietosuojamääräyksiä ja niitä velvoitteita, jotka koskevat muitakin kuin laatuvarmentajia ja -varmenteita, kuten valvonta ja palvelujen vapaa liikkuvuus. Toisaalta direktiivi asettaa alkuperämaaperiaatteen valvonnan periaatteen varmentajien, myös aikaleimavarmentajien, toiminnalle. Aikaleimavarmentajille ei saa asettaa ennakkolupavaatimusta. Vapaaehtoisia akkreditointijärjestelmiä voidaan asettaa, kunhan nämä toimivat objektiivisin, avoimin, suhteellisin ja syrjimättömin kriteerein. Direktiivin mukaiset laatuvarmenteet liittyvät kuitenkin vain identiteetin varmentamiseen, eivät muuhun.

Aikaleimojen sääntelyä lakitasolla ovat toivoneet Väestörekisterikeskus sekä eräät yksityiset toimijat. On arvioitu, että aikaleimojen käyttötarve tulee lisääntymään. Nokia katsoo, että yleisen digitaalisen ajan määrittäminen olisi kannatettavaa, mikä korostaa kansainvälisen yhteistyön ja standardoinnin merkitystä. Aikaleimojen yhteys pitkäaikaissäilytykseen ja varmenneketjun jatkuvuuteen ovat merkittäviä tekijöitä, samoin aikaleimojen käyttökelpoisuus erityislainsäädännön, kuten sähköisen viestinnän tietosuojalain täyttämisessä. Rahoitustarkastuksen mielestä aikaleimat ovat tarpeen ainakin arvopaperikaupan toimeksiannoissa[74] sekä varmenteiden peruuttamistilanteissa (sulkulistapalvelu).

---

[74] Kirjallisuudessa on viitattu myös käyttökelpoisuuteen sisäpiirisääntöjen soveltamisessa.

Monet toimijat, kuten Viestintävirasto ja Kesko ovat kuitenkin kyseenalaistaneet sääntelytarpeen. On vedottu siihen, että pelkkä ajanmääritys on teknisesti yksinkertaista erilaisten lokien ja yksinkertaisten ja halpojen laitteiden avulla. Nämä laitteet voivat käyttää esimerkiksi gps-satelliittiyhteyttä. ajan hakemiseen. On silti todettava, että aikaleimapalvelulle on olennaista, että joku vahvistaa kiistämättömästi tietyn ajan ja yhteyden toimenpiteeseen. Epävirallisemmat ajanmääritykset voivat tulla hyväksytyiksi vapaan todistusharkinnan pohjalta. Esimerkiksi tullilaitos on katsonut, että hallinnossa asiakirjan lähettämisellä on paljon suurempi merkitys kuin allekirjoituksen laatimisajankohdalla. Monet yksityistä sektoria edustavat vastaajat ovat katsoneet, että tekniikka ei ole aukoton eikä sitä voi lainsäädännöllä saada sellaiseksi. Tämän vuoksi olisi parempi jättää asia sopimuksenvaraiseksi ja kehittyvien parhaiden käytäntöjen varaan.

Aikaleimapalvelujen sääntelykysymys on eräänlainen paradoksi sikäli, että monet katsovat että palvelut eivät ole teknisesti ja kaupallisesti vielä niin kehittyneitä, että niitä kannattaisi lähteä sääntelemään. Toisaalta aikaleimoja on säännelty jo Euroopan ensimmäisissä sähköisiä allekirjoituksia koskevissa kansallisissa laeissa. Lienee selvää, että sähköiseen viestintään liittyviä ajanmääritystä voidaan teknisesti toteuttaa ei-säännellyillä tavoilla, ja suomalaisessa oikeuskulttuurissa vallitsevan vapaan todistusharkinnan periaatteen johdosta ei aikaleiman kaltaisia institutionaalisille todistuskeinoille välttämättä löydy samanlaista tarvetta kuin formaalisia keinoja korostavissa oikeusjärjestelmissä.

On nähtävissä, että aikaleimat ja niitä koskevat palvelut voivat osoittaa käytännön tarpeellisuutensa sitä mukaa kuin laissa erityisesti säänneltyjen sähköisten allekirjoitusten käyttö lisääntyy. Mikäli aikaleimojen käytölle löytyy yllä kuvatun kaltaisia oikeudellis-kaupallisia perusteita, olisi harkittava aikaleimojen sääntelyä. Tämä voitaisiin tehdä siinä vaiheessa kun on aihetta lain kokonaistarkasteluun, todennäköisesti muutaman vuoden päästä. Sääntelyä ei tulisi luoda palvelujen kehityksen kahlitsemiseksi, vaan eräänlaisen näytöllisen oikeudellisen instituution luomiseksi. Sen vuoksi lain säännökset voisivat olla pitkälle ohjeellisia.

Aikaleimapalvelujen osalta voitaisiin myöhemmin uudistamisen yhteydessä lisätä lakiin aikaleiman ja sitä koskevan palvelun määritelmä ja perusvaatimukset. Laatuvarmenteilla varmennettavia sähköisiä allekirjoituksia koskevat vastuusäännöt voitaisiin linkittää aikaleimojen käytön sääntelyyn laatuvarmenteiden käytön yhteydessä. Viestintävirastolle voitaisiin antaa oikeus antaa yksityiskohtaisempia määräyksiä aikaleimapalvelujen tarjoamisesta ja niissä noudatettavista periaatteista.

Selkeintä olisi luonnollisesti toteuttaa uudistus yleiseurooppalaiselta pohjalta. Direktiivi ei kuitenkaan aseta estettä aikaleimojen kansalliselle sääntelylle, kunhan edellä mainittuja yhteisöoikeuden periaatteita kunnioitetaan.

5.3. Luotetut arkistointipalvelut

Jotkut toimijat, kuten sisäasiainministeriö ja eräs vakuutusalalla toimiva yritys, katsovat, että tulevaisuutta ajatellen laissa tulisi ottaa kantaa sähköisesti allekirjoitettujen sähköisten asiakirjojen pitkäaikaissäilytykseen ja allekirjoituksen jälkikäteiseen (yli 10 vuotta) todentamiseen liittyviin ongelmiin. Myös sulkulistan säilyttämistä koskevaa sääntelyä pitäisi joiden tahojen mielestä selkeyttää.

Tietoyhteiskuntaan siirtyminen edellyttää myös sähköisten asiakirjojen ja allekirjoitusten luotettavaa arkistointia. Sähköistä kaupankäyntiä koskeva direktiivi 2000/31/EY velvoittaa jäsenmaat huolehtimaan, että sopimuksentekoprosessin oikeudelliset perusteet eivät aseta esteitä sähköisten sopimusten käyttämiselle, eivätkä johda siihen, että sähköisiltä sopimuksilta evätään oikeudellinen pätevyys. Tämä johtaa jatkossa myös arkistointipalveluihin kohdistuviin oikeudellisiin vaatimuksiin, joihin kiinnitetään huomiota sähköisten allekirjoitusten osalta.

Kirjallisuudessa[75] esitetty prosessinkuvaus on seuraava: arkistoija lisää arkistoimansa asiakirjan luotettavuutta allekirjoittamalla sen sähköisesti. Kun PKI-pohjainen allekirjoitus takaa asiakirjan eheyden, toimii arkistoijan allekirjoitus ”sinettinä”. Monet asiakirjat on allekirjoitettu sähköisesti lain vaatimalla tavalla. Sähköisen allekirjoituksen ja asiakirjan yhteys olisi turvattava. Käytännössä tämä tarkoittaisi seuraavaa prosessia: Asiakirjan tietosisältö ja sähköinen allekirjoitus tulisi yhdistää, ja yhdistämisessä muodostuva hash-koodi tulisi tallentaa riippumattomalle yksikölle, joka aikaleimaa koodin. Aikaleima tulee liittää asiakirjan metatietoon säilytettäväksi. Sähköisten allekirjoitusten osalta myös allekirjoituksen tekemisaika olisi arkistoitava, mikä edellyttää allekirjoituksia koskevien aikaleimojen arkistointia. Arkistoijan täytyy tuottaa asiakirjan arkistoinnin validointiketju.

Edellä viitatussa kirjallisuudessa on esitetty, että sähköisten asiakirjojen ja niiden allekirjoitusten arkistoimiseksi tulisi luoda luotettujen arkistointipalvelujen (Trusted Archival Service) oikeudelli-

[75] Arkistopalvelujen sääntelystä ks. lähemmin Dumortier-Van den Eynde, Electronic Signatures and Trusted Archival Services sekä komission toimesta teetetty tutkimus The Legal and Market Aspects of Electronic Signatures.

nen järjestelmä.[76] Tämä järjestelmä perustuisi arkistoijan ankaran vastuun periaatteelle. Tällaisen oikeudellisen järjestelmän luominen tulisi tehdä yhteisölainsäädännön puitteissa. Nykyinen yhteisölainsäädäntö ei aseta estettä kansallisille lainsäädäntötoimille, jos yhteisöoikeuden vaatimukset, kuten syrjintäkielto huomioidaan. Arkistointiin liittyviä kysymyksiä tulisi tarkastella myös standardoinnin näkökulmasta, kuten on tehtykin.

Toimijoiden kesken käydyssä keskustelussa on ilmennyt, että julkisella puolella arkistolaitoksen norminantovaltuudet ovat riittäviä, joten siis muutoksia sähköisiä allekirjoituksia koskevaan lakiin ei sen vuoksi tarvita. Kansalliset käytännöt, joissa vain todetaan arkistointivaiheessa allekirjoitusten oikeellisuus ja luotetaan myöhemmin näihin merkintöihin, ovat vallalla.[77] Alkuperäinen sähköinen allekirjoitus menettää pitkälle oikeudellisen merkityksensä arkistointivaiheessa. Toinen sääntelyn kohde, yksityiset arkistointipalvelut eivät puolestaan ole kustannustehokkaita eivätkä palveluntarjoajat pysty tarjoamaan riittävän edullisia arkistointipalveluja yritystarpeisiin. Tällaisiin ongelmiin ei voida puuttua sähköisiä allekirjoituksia koskevalla lainsäädännöllä. Kirjanpitolainsäädäntö sallii sähköisten laskujen käytön ja sisältää arkistointivelvoitteen. Tilitoimistot huolehtivat sangen usein tästä arkistoinnista eikä asia ole aiheuttanut toistaiseksi sellaisia ongelmia, joihin tulisi puuttua lainsäädännöllä. Yksityiset toimijat korostavatkin erityissääntelyn ja käytäntöjen merkitystä yleislainsäädännön asemesta.

5.4. Notariaattipalvelut

Notariaattipalveluilla ymmärretään palveluja, joissa esimerkiksi pankki tarkastaa asiakirjan omalta kannaltaan eli ”validoi” sen. Notariaattipalvelut käsittävät mm. asiakirjojen evaluoinnin, sulkulistan tarkistamisen, salauksen purkamisen ja tarkastamisen. Palvelu voidaan toteuttaa omaan tai toisen

[76] The Legal and Market Aspects of Electronic Signatures esittää, että myös rekisteröityä sähköistä postia koskevat palvelut tulisi lainsäätäjän toimesta huomioida.

[77] Arkistolaitoksen nykyinen näkemys tyypillisestä sähköisen allekirjoituksen käyttötarkoituksesta on seuraava; sähköisen allekirjoituksen suurin merkitys on asiakirjan alkuperäisyyden ja eheyden turvaamisessa lähettäjän ja vastaanottajan välisen siirron aikana. Arkistolaitoksen näkemyksen mukaan sähköinen allekirjoitus menettää suurelta osin merkityksensä kun 1) asiakirjan alkuperäisyys ja eheys on todennettu, 2) todentamisesta on tehty merkinnät diaariin tai se on muutoin luotettavasti rekisteröity, 3) asiakirja tai sen tietosisältö on siirretty vastaanottajan luotettavaan tietojärjestelmään.

Näkemys perustuu arkistolaitoksen nykyiseen tietämykseen ja sitä voidaan joutua teknisen ja toiminnallisen kehityksen myötä tarkistamaan. Nykyinen tulkinta mahdollistaa kuitenkin sen, että nykyisellä tekniikalla vaikeasti säilytettävää sähköistä allekirjoitusta ei tarvitse ryhtyä säilyttämään, vaan olennaista on säilyttää tieto sähköisen allekirjoituksen käytöstä ja asianmukaisuudesta. Se, että asia on ylipäätään otettu viranomaisen käsittelyyn, osoittaa edellytysten olleen aikanaan kunnossa. Tämä voidaan puolestaan osoittaa edellä mainitulla diaari- tai muulla rekisteröintimerkinnällä.

lukuun. Vain jälkimmäinen on kuitenkin sääntelyn kannalta kiinnostavaa. Notariaattipalvelujen täsmällistä sisältöä ja siihen kohdistuvia vaatimuksia on vaikea määritellä lainsäädännöllä. Myös vastuukysymykset voidaan jättää yleisten sopimusoikeudellisten periaatteiden varaan.

Keski-Euroopassa notariaattipalvelut ovat enemmän käytettyjä kuin Suomessa. Tämän vuoksi sääntelytarpeita on Suomessa vähemmän eikä sääntelyä ole kovin selkeästi toivottu miltään taholta. Yksityisellä puolella on tässäkin yhteydessä huomioitava tilintarkastajien suorittaman valvonnan merkitys.

6. VARMENNEPALVELUJEN TARJOAMINEN

6.1. Julkinen panostaminen varmennepalveluihin

Tällä kysymyksellä on kaksi ulottuvuutta. Ensinnäkin väestötietojärjestelmä ja varmentaminen mahdollistavat yhteiskunnallisen varmennepalvelutoiminnan. Edistämällä tällaista toimintaa yhteiskunta edistää tietoyhteiskunnan kehittämistä, joskin samalla yksityisen sektorin kilpailumahdollisuuksia rajoittaen. Lain keskeisenä lähtökohtana on vapaan kilpailun mahdollistaminen ja sitä kautta sekä parhaiden sovellusten voittaminen markkinoilla että hintojen markkinavetoinen määräytyminen, mikä ei tosin toteudu tällä hetkellä. Kilpailun puuttuminen saattaa haitata myös menetelmien kehittymistä.

Toinen julkinen ulottuvuus on luotettavan varmenneteknologian käyttöönotto julkisten viranomaisten toimesta. Esimerkiksi laatuvarmenteiden käyttöönotto julkisissa palveluissa edistää näitä palveluja koskevien kaupallisten ratkaisujen tarjoamista ja lisää käyttökokemuksia näistä palveluista, mikä edesauttaa niiden kehittämistä.

Monet toimijat julkisella, mutta myös yksityisellä sektorilla katsovat yhteiskunnan panostuksen tärkeäksi. Valtiovarainministeriö on kuitenkin pidättyvämmällä kannalla. Sen mukaan sähköinen allekirjoitus ei ole hallinnossa ongelma, eikä siihen ole tarvetta laajemmin panostaa. Allekirjoitusten käyttö viestien alkuperän varmistamisessa saattaa nousta odotettua merkittävämpään asemaan roskapostin torjumisen tarpeen kasvaessa. Samoin toteaa Segco, jonka mukaan PKI-pohjaisessa asioinnissa voitaisiin varsin tehokkaasti rajata business-asiointi muusta häiritsevästä asioinnista, koska sekä kommunikaation alkuperä, että sisältö ovat luotettavasti todennettavissa. Segco katsoo,

että sähköisen identiteetin kiistämättömyys ja eheys on nähty lähinnä teknisenä asiana, vaikka kyseessä on prosessi. Monien mukaan julkishallinto voisi ennakkoluulottomasti käyttää korkean teknologian ja palveluprosessin omaavia palvelutuottajia ja organisaatiovarmenteita sekä käyttää kotimaista liiketoimintaosaamista. Lisäksi tulisi luoda kotimaista yhteistyötä alan toimijoiden kanssa. Tuloksena olisi, että Suomi saisi hyvän markkina-aseman tietotekniikan ja sähköisen asioinnin kärkimaiden joukossa. Toisaalta pankkitunnisteita tarjoavat pankit suhtautuvat kriittisesti yhteen teknologiaan panostamiseen kilpailusyiden vuoksi.

6.2. Kilpailunäkökohdat

Henkilötietoihin perustuva VRK:n varmennejärjestelmä ilmentää julkisen sektorin panostusta sähköisen kaupankäynnin infrastruktuurin kehittämiseen. Julkisella viranomaisella on lakisääteisiä tehtäviä väestötietojen ylläpidon suhteen, mitkä tiedot muodostavat sitten ”alustan” myös toiminnalle varmentajana. Tälle tielle on lähdetty monissa maissa:

- Suomessa laatuvarmentajana toimii VRK, jolla on myös väestötietojärjestelmään liittyviä tehtäviä,
- monissa Aasian maissa, kuten Singaporessa, on noudatettu samanlaista mallia kuin Suomessa.
- Englannissa on pitkään vastustettu kansalaisten henkilötietojen rekisteröintiä, mutta nyt se on mahdollistettu, mikä mahdollistaisi kansalaisvarmenteen mukaisia ratkaisujen kehittämisen.
- Viro on toiminut edelläkävijänä. Eesti Sertifitseerimiskeskus AS on pankkien omistama yritys, mutta se toimii yhteistyössä julkisen sektorin kanssa tavoitteenaan koko väestön varustaminen sähköisin henkilökortein.
- Suomi on puolestaan toiminut edelläkävijänä mobiilivarmenteissa. Toisaalta pankkitunnisteita käytetään käytännössä huomattavasti enemmän.

Direktiivi ja laki perustuvat kuitenkin sille ajatukselle, että laatuvarmentaminen ei välttämättä ole julkisen vallan taholta tapahtuvaa toimintaa, vaan että sitä harjoitettaisiin laajalti kaupallisin perustein. Laissa on määräyksiä valvonnasta, luomisvälineiden tarkastuslaitoksista jne. Väestörekisterikeskus on valtion keskusviranomainen ja tarjoaa palveluksiaan vahvistettujen maksuperusteiden

mukaisesti. Keskusteluissa on paikoin noussut esille kilpailuneutraliteettiongelma VRK:n ja yksityisten toimijoiden, kuten operaattorien, välillä.[78]

Teleoperaattorien taholta on kiinnitetty huomiota siihen, että henkilötietojen käsittely koskeva sähköisiä allekirjoituksia koskevan lain 19 § kieltää henkilötunnuksen sisällyttämisen varmenteeseen. Tämä säännös on operaattorien mukaan hyvin merkittävä este varmenteiden käytölle henkilön sähköisessä tunnistamisessa. Henkilön sähköinen tunnistaminen perustuu pitkälti siihen, että henkilö voitaisiin yksilöidä yksiselitteisesti ja yleiskäyttöisesti. Tätä tarvetta varten on mm. väestötietojärjestelmään muodostettu sähköinen asiointitunnus. Henkilötunnusta koskevan kiellon on ilmaistu olevan varmenteita syrjivää suhteessa muihin palveluihin, koska esimerkiksi viranomaisasioinnissa laajasti käytössä olevissa pankkien tarjoamissa TUPAS-palveluissa henkilötunnus voidaan luovuttaa palveluntuottajalle. Tämä luovuttaminen on kuitenkin asianomaisen henkilön suostumuksen varaista.

Teleoperaattorien taholta on lisätty, että tässä yhteydessä kannattaisi myös arvioida onko henkilötunnuksen kieltävä pykälä Suomessa toimivia laatuvarmentajia syrjivä ja mahdollisesti ristiriidassa sähköisiä allekirjoituksia koskevan lain 4 §:n kanssa (palvelujen ja tuotteiden vapaa liikkuvuus sisämarkkinoilla) ja 8 §:n kanssa, jos sama kielto ei koskisi muissa EU-maissa liikkeelle laskettavia varmenteita. Esimerkiksi Ruotsissa tällaista rajoitusta ei tiettävästi laatuvarmenteille ole olemassa, joskaan laatuvarmennustoimintaa ei toisaalta ole syntynyt.

Edelleen on lisätty koskien lain 20 §:ää, että varmentajan oikeus hakea ja tarkastaa varmenteen hakijan henkilötiedot väestötietojärjestelmästä kannattaisi yksiselitteisesti ulottaa koskemaan myös sähköistä asiointitunnusta. Kaikille suomalaisille on muodostettu väestötietojärjestelmään sähköinen asiointitunnus tai asiointitunnuksen luonnissa tarvittava tekninen tunnistetieto. Väestötietolain 507/1993 20 §:n mukaan VRK:n myöntämässä kansalaisvarmenteessa varmenteen haltijan yksilöivänä tunnistetietona on sähköinen asiointitunnus. Tämä on numeroista ja tarkastusmerkistä muodostettu tietojoukko, jonka avulla yksilöidään varmennetun sähköisen asioinnin osapuolet. Luonnollisen henkilön sähköinen asiointitunnus ei sisällä henkilöön liittyviä tunnistetietoja. Väestötietojärjestelmään merkittävälle henkilölle talletetaan sähköisen asiointitunnuksen luomisessa tarvittava

[78] Kilpailuvirasto on lausunnossaan sisäasiainministeriölle (Dnro 619/72/2002, 19.8.2002) katsonut, ettei VRK:n asemaa liiketaloudellisena toimijana tulisi vahvistaa lainsäätäjän toimesta. Paras ratkaisu olisi Kilpailuviraston näkemyksen mukaan Väestörekisterikeskuksen toiminnan keskittäminen yksinomaan peruspalveluluontoisiin kansalaisille suunnattuihin toimintoihin. Sähköistä asiointitunnusta koskevat kysymykset eivät ole olleet kilpailuviraston käsiteltävänä.

tekninen tunnistetieto, joka merkitään henkilön sähköiseksi asiointitunnukseksi silloin, kun hänelle myönnetään varmenne. Väestötietolain 21 §:n 4 momenttiin on kirjattu kielto käyttää teknistä tunnistetietoa muuhun kuin sähköisen asiointitunnuksen luomiseen sekä väestötietojärjestelmän sisäisenä teknisenä tunniste- ja tarkistustietona.[79]

Monet yksityistä sektoria edustavat vastaajat katsovat, että sähköinen asiointitunnus (SATU) tulisi julkisen vallan taholta luovuttaa muiden käytettäväksi tuotantokustannuksin, sillä nykyinen tilanne estää palvelujen kehittämistä. Väestötietojärjestelmään luotua henkilöllisyyden yksilöivää sähköistä asiointitunnusta ei Väestörekisterikeskuksen mukaan voida nykyisellä lainsäädännöllä (väestötietolaki) luovuttaa sisällytettäväksi kuin kansalaisvarmenteeseen. Tätä näkemystä ei kuitenkaan yleisesti jaeta.

Väestörekisterikeskuksen mukaan sähköisen asiointitunnuksen luovuttaminen on teknisesti ja juridisesti mahdoton ajatus. Teknisesti sen vuoksi, että tällä hetkellä sähköinen asiointitunnus luodaan vasta kansalaisvarmennetta tehtäessä, eikä sitä ole oikeastaan olemassa tätä ennen. Juridisesti sen vuoksi, että Väestörekisterikeskus ei voi vastata tuottamiensa tietojen käsittelyn tasosta toisen organisaation järjestelmissä.

Teknisen esteen osalta ei kuitenkaan liene estettä generoida SATU:a myös muussa yhteydessä. Juridisen esteen osalta on todettava, että luovutuksensaajina toimisivat nimenomaan tarkasti säännellyt ja valvotut laatuvarmentajat. Myös henkilötunnuksia luovutetaan VRK:n toimesta muissa vastaavissa tilanteissa. Sähköisiä allekirjoituksia koskevan lain perusteella luovutuksensaajana toimivat varmentajat vastaavat myös satun käsittelystä varmenteen osana. Väestörekisterikeskus ei ole tästä vastuussa.

VRK:n mukaan on meneteltävä siten, että jokaiselle varmentajalle syntyy oma, henkilön yksilöivä tunnistetieto. Yhteentoimivuuden saavuttamiseksi yhtenäinen tunnistetieto olisi kuitenkin tarpeen ja sellaisen käyttö alentaisi varmennetoiminnan kustannuksia yleisesti.

---

[79] Väestötietolain 21 §:n perusteluissa todetaan: ”Tekninen tunnistetieto on tarkoitettu käytettäväksi ainoastaan sähköisen asiointitunnuksen luonnissa sekä väestötietojärjestelmän sisäisenä teknisenä tunniste- ja tarkistustietona. Teknisen tunnistetiedon käyttötarkoituksesta ehdotetaan säädettäväksi pykälään lisättävässä uudessa 4 momentissa.”

Tällä hetkellä ongelma ei liene kuitenkaan suoraan lainsäädännöstä johtuva. Lain kokonaisuudistuksen yhteydessä voitaisiin Väestötietolakiin tai lakiin sähköisistä allekirjoituksista selvyyden vuoksi ottaa maininta siitä, että sähköistä asiointitunnusta voisivat käyttää myös muut varmentajat myöntämänsä laatuvarmenteen yhteydessä. On selvää, ettei tässä yhteydessä voitaisi tehdä eroa suomalaisen ja muualta ETA-alueelta tulevan varmentajan välillä.

6.3. Tietosuoja

Tietosuojakysymysten osalta voidaan todeta, että henkilö- eli sosiaaliturvatunnusta ei saa sähköisiä allekirjoituksia koskevan lain 19 §:n 2 momentin mukaan sisällyttää varmenteeseen. Tämän vuoksi käytetään sähköistä asiointitunnusta, joka ei sisällä henkilöön liittyviä tunnistetietoja. Tietosuoja ja tehokkuusnäkökohdat muodostuvat helposti vastakkaisiksi intresseiksi. Tietosuojan osalta uhkakuvana on järjestelmien murtuminen. Sen vuoksi olisi parempi että identifioimisjärjestelmät olisivat mahdollisimman hajallaan. Tämä kuitenkin haittaa yhteistyötä varmentajien kesken, sillä jokainen varmentaja joutuu tällöin luomaan varmenteet oman asiakastiedostonsa pohjalta.

Tietosuojakysymykset ovat esillä myös sulkulistan ylläpidossa. Sulkulistan tarkastusmerkintöjä seuraamalla saadaan tietoa transaktioista. Sen vuoksi sähköisiä allekirjoituksia koskevan lain 21 §:n mukaan varmentajan sulkulistalta tehdystä varmenteen voimassaolon tarkistamisesta kerättyjä tietoja saa käyttää ainoastaan varmenteiden käytön laskutuksen suorittamiseksi tai varmenteella varmennetun sähköisen allekirjoituksen avulla tehtyjen oikeustoimien todentamiseksi.

Tietosuojavaltuutettu on katsonut, että mikäli sähköistä tunnistamista lähdettäisiin lakitasolla laajemmin sääntelemään, ei sama laki voi helposti kattaa sähköistä allekirjoittamista ja tunnistamista tietosuojan näkökulmasta, koska tietosuojaan liittyviä täsmennyksiä tarvitaan eri laajuudessa tunnistamis- ja allekirjoitusfunktioiden osalta. Henkilötietolaki ja sähköisen viestinnän tietosuojalaki ovat tietosuojan osalta noudatettavia säännöksiä. Henkilötietolaki kattaa yleislakina kaikkien henkilötietojen käsittelyn.

7. LAIN ARVIOINTIA

7.1. Lain tavoitteiden toteutuminen

Lain vaikutusten arviointi on tehtävä huomioiden, että lailla on tarkoitettu säännellä vain varmenteiden käyttöä allekirjoitustarkoituksiin. Laki perustuu direktiiviin, joka käytännössä rakentuu PKI-tekniikan pohjalle huolimatta muodollisesta teknologianeutraalisuudestaan. Jotkut maat, kuten Viro, ovat luoneet lainsäädäntöä nimenomaan digitaalisiin allekirjoituksiin, joka käytännössä tarkoittaa PKI-pohjaisen tekniikan käyttöä.

Allekirjoituksen merkitys tahdonilmaisun vahvistajana ei ole pohjoismaisessa oikeuskulttuurissa suuri. Tuomioistuimet käyttävät vapaata todistusharkintaa ja allekirjoitus voidaan korvata muilla tahdonilmaisun osoittamisen keinoilla. Vain harvat oikeustoimet edellyttävät allekirjoittamista. Direktiivin ja lain periaatteena on lisäksi, että myös muut sähköisen allekirjoituksen tekniikat voivat tilanteen mukaan täyttää allekirjoitusvaatimuksen. Julkisen sektorin kanssa asioidessa allekirjoitusvaatimus ei myöskään ole pääsääntönä, vaan viranomainen voi pyytää (myös sähköistä) allekirjoitusta, jos katsoo sellaisen aiheelliseksi.

Lain tarkoittaman laatuvarmenteeseen perustuvan allekirjoituksen toteuttaminen käytännön oloissa edellyttää huomattavan oikeudellis-teknisen infrastruktuurin luomista. Lain soveltaminen laajamittaisesti edellyttää, että yksityiset kuluttajat käyttäisivät sähköisiä allekirjoitusvälineitä. Allekirjoituksen toteuttaminen vaatii lisäksi lukulaitteen ja erityisen tietokoneohjelman omistamista. Sekä kortin että lukulaitteen kustannuksia on pidetty korkeina. Myös tekniikka on monimutkaista monelle käyttäjälle. Palveluja, joihin laatuvarmenne on käytettävissä, on toistaiseksi vielä vähän.

Laki sähköisistä allekirjoituksista ei sääntele suoraan sähköistä tunnistamista, mutta laatuvarmennetasoisia ratkaisuja käytetään myös ns. vahvaan tunnistamiseen. Varmennestandardeissa ja -tuotteissa erottelu tunnistamisen ja allekirjoituksen varmenteiden välillä on selvä ja varmentajan lakisääteinen vastuu koskee vain allekirjoitusta. Käytännössä sähköinen tunnistaminen tapahtuu pääsääntöisesti muilla tavoin kuin varmenteilla, lähinnä pankkien TUPAS2-standardin mukaisilla vaihtuvilla salasanoilla.

Yksi mahdollisuus olisi laajentaa sähköisistä allekirjoituksista annetun lain soveltamisalaa sähköiseen tunnistamiseen tai luoda sähköisestä tunnistamisesta omaa lainsäädäntöä. Sähköallekirjoitus-

lakiin voitaisiin toisaalta helposti kirjata laatuvarmennetasoisen ratkaisun käyttäminen tunnistamiseen, mikä edesauttaisi korkeatasoisten varmenteiden tuotteistusta ja menekkiä. Mikäli uudistus tehtäisiin EU-lainsäädännössä, voitaisiin tunnistamisen ja allekirjoituksen rajaa selventää yhteisötasolla ja luoda ainakin yksi yhdenmukainen menettely, jonka avulla luotettava sähköinen etätunnistaminen voisi tapahtua. Luonnollisesti tällainen sääntely ei voisi olla muita menetelmiä syrjivää.

Toisaalta voidaan esitettyjen kommenttien perusteella katsoa, että lain asettama jako tunnistamiseen ja allekirjoitukseen on suomalaiselle oikeusajattelulle osin kaavamainen, johtuen juuri oikeustoimien muotovapaudesta. Lain mukaisen sähköisen allekirjoituksen edellyttäminen yleisesti lisäisi oikeusvarmuutta, mutta johtaisi oikeustoimien määrämuotoistumiseen, jota ei ole kustannussyistä ole syytä tavoitella. Lainsäädännön yleiseurooppalaista taustaa ja kehitystä ajatellen lain käsitteelliset jaottelut ovat kuitenkin hyväksyttäviä.

Hallintolain 22.2 §:n ja sähköisestä asioinnista viranomaistoiminnassa annetun lain 9 § 2 momentin perusteella viranomainen voi vaatia asiakirjan täydentämistä sähköisellä allekirjoituksella, jos asiakirjan alkuperäisyyttä ja eheyttä on syytä epäillä. Tätä säännöstä ei liene käytännössä sovellettu käytäntöön, mutta teknisesti se voisi tulla sovellettavaksi varsinkin asiakirjan eheyden varmistamiseksi.

Laki sähköisistä allekirjoituksista ja sen taustalla oleva direktiivi soveltuvat sähköisiin allekirjoituksiin ja niitä koskevien palvelujen tarjoajiin ja sisältävät runsaasti käsitteitä ja kriteereitä, joiden muodostama kokonaisuus tekee sähköisistä allekirjoituksista vaikeasti lähestyttävän asiakokonaisuuden. Tätä kokonaisuutta on vaikea käsitellä ja arvioida, ellei omakohtaista käytännön kokemusta ole. Toisaalta lain ja direktiivin soveltamisen ongelmaksi on muodostunut se, että laki sääntelee suoraan vain infrastruktuurin monimutkaisinta osaa, joka on käytännössä toteutettavissa vain yhdenlaisella teknologialla, ja jonka toteuttaminen on kaupallisille toimijoille ollut toistaiseksi epätarkoituksenmukaista, ottaen huomioon vapaan todistusharkinnan ja sopimuksen muotovapauden periaatteet Suomen oikeusjärjestyksessä. Vastaavia kokemuksia on myös muissa Euroopan maissa.

Kun lain tarkoitus on sähköisen oikeudellisen vastineen luominen käsintehdylle allekirjoitukselle, ei laki ole pääsääntöisesti vielä kohdannut käytäntöä, joka on kehittynyt sen ulkopuolella markkinavetoiselta pohjalta keskeisenä elementtinään tunnistaminen. Tämä seikka tuli näkyviin myös tähän selvitykseen saatujen vastausten määrässä ja sisällössä. Lain tarkoittamien allekirjoitusten yleistymiseen tähtääviä hankkeita on julkishallinnossa ja terveydenhuollossa kuitenkin valmisteilla, ja

yksityisellä puolella mobiilivarmenteiden lisääntyminen matkapuhelimien ja muiden sirukorttialustojen välityksellä tulee lisäämään lain soveltamista käytäntöön.

Laki on tarjonnut luotettavan juridisen pohjan allekirjoituksen toteuttamiselle sähköisessä muodossa. Laissa tarkoitettujen kehittyneiden sähköisten allekirjoitusten ja laatuvarmenteiden lisäksi allekirjoituksia toteutetaan mm. muuttuvien salasanojen avulla. Lain teksti yhdistettynä direktiivin sanamuotoon legitimoi pitkälle myös muut sähköiset allekirjoitustavat normaalin vapaan todistusharkinnan lisäksi. Lain olemassaolo on luonut pohjan toiminnalle laatuvarmentajana ja laatuvarmenteiden käytölle. Mobiilivarmenteita koskeva infrastruktuuri on vasta tulossa käyttöön. Varsin monet vastaajat arvioivat, että mobiilivarmenteiden mukaantulo lisäisi laatuvarmenteen käyttöä olennaisesti, tosin esimerkiksi Viestintävirasto arvelee nimenomaan tunnistamisvarmenteiden käytön lisääntyvän.

Monet julkissektoria edustavat vastaajat katsoivat, että julkisen vallan tulisi nykyistä enemmän edistää lain tarkoittaman tekniikan käyttöä. Monet projektit, mm. kuluttajien mobiilivarmenne sekä hallinnon sisäiset toimet mm. terveydenhuollossa viittaavatkin lain soveltamisen lisääntymiseen jatkossa. Tämä tietää sitä, että eri teitä lainsäädännön tarkoittamien laatuvarmenteiden käyttö tulee yleistymään, vaikkei niistä muodostuisikaan yleistä käytäntöä.

Tämä selvitys on laadittu ajankohtana, jolloin laki on ollut voimassa kaksi vuotta. Lailla on hallituksen esityksen mukaan pyritty siihen, että käyttämällä sähköisiä allekirjoituksia ja niiden käytössä tarvittavia tuotteita ja palveluita edistettäisiin kuluttajien ja muiden käyttäjien luottamusta verkkoliiketoimintaan ja sähköiseen asiointiin. Koska laissa nimenomaisesti säännellyt allekirjoitusmenettelyt ovat vasta kehittymässä kaupallisiin käyttötarkoituksiin, ei lailla voida katsoa toistaiseksi olleen suoraa kuluttajien luottamusta edistävää vaikutusta.

Hallituksen esityksessä katsottiin, että laki edistäisi uuden ja kasvavan liiketoimintasektorin, varmentamisen kehittymistä. On todettava, että lailla on luotu puitteet laatuvarmentamiselle, mutta tämä on liiketoimintana jäänyt valtion keskusviraston, Väestörekisterikeskuksen hoidettavaksi. Yksityisiä laatuvarmentajia ei ole syntynyt. Laatuvarmentaminen on myös muissa Euroopan maissa jäänyt vähäiseksi ja julkisen panostuksen merkitys on korostunut palveluiden kehittämisessä. Kysymykseksi nousee, onko kynnys laatuvarmenteiden ja muiden varmenteiden välillä liian korkea vai onko laatuvarmenteiden käytön tarve yksinkertaisesti sangen pieni. Laatuvarmenteen status ei sellaisenaan ole ollut valtti palveluiden markkinoimisessa yksityiselle sektorille eikä kuluttajille.

Hallituksen esityksessä on todettu, että toteutuessaan laki lisäisi sähköistä kaupankäyntiä ja asiointia sekä tietoyhteiskuntapalvelujen käyttöä. Tältä osin on todettava, että lailla on ollut osin tällainen vaikutus nimenomaan tunnistamisen kannalta. Allekirjoitusten suhteen taas esimerkiksi terveydenhuollossa tehtävät uudistukset perustuvat juuri lailla luotuun allekirjoituksia koskevaan oikeudelliseen infrastruktuuriin. Allekirjoituksia varten luotu infrastruktuuri on käyttökelpoinen tunnistamistarkoituksiin ja edistää siten luottamusta myös sähköisessä kaupankäynnissä tunnistamisen osalta. Lain taustalla on lisäksi se direktiivissä mainittu periaate että, muukin kuin laissa kuvattu sähköinen allekirjoitus voi olla pätevä. Tämä lisää myös TUPAS-järjestelmän ja muiden vastaavien järjestelmien oikeudellista arvoa vapaan todistusharkintaperiaatteen ohella.

7.2. Ratkaisuja sääntelyn ongelmakohtiin

7.2.1. Välitöntä muutostarvetta ei ole

Laki sähköisistä allekirjoituksista on ollut voimassa vasta kaksi vuotta. Lain laajamittaisempi soveltaminen edellyttää kaupallisen infrastruktuurin kehittymistä, ja tämä kehitys on osin vielä alkutekijöissään. Aika ei sen vuoksi ole vielä kypsä lain säännösten kattavaksi ja yksityiskohtaiseksi arvioimiseksi. Selvityksessä ei ole tullut esille seikkoja, jotka edellyttäisivät pikaisia muutoksia lakiin. Muutamat edellä pohditut muutokset voitaisiin toteuttaa mahdollisen kokonaisuudistuksen osana myöhemmin. Lain uusi lähempi tarkastelu tulisi tehdä ehkä 2-4 vuoden päästä, ja tällöin tulisi huomioida kehitys EU:ssa ja yleisemmin muissa maissa. Jos PKI-pohjaisten laatuvarmenteiden käyttö tulee lisääntymään, saattaa olla paikallaan harkita muun infrastruktuurin sääntelyä mm. aikaleimojen ja yksityispohjaisten arkistopalveluiden osalta. Vaihtoehtona yleissääntelylle voidaan nähdä joitakin käyttöaloja koskeva erityissääntely.

7.2.2. Sääntely lähemmäksi käytäntöä

Sähköisten allekirjoitusten käyttö on yleistynyt, mutta ei nimenomaisesti lain erityisesti sääntelemässä muodossa vaan esimerkiksi vaihtuvia salasanoja käyttämällä. Kun luodaan lainsäädäntöä sääntelemään teknis-juridista instrumenttia, tulisi lainsäädännössä periaatteessa voida käsitellä asiaa kattavasti siitä huolimatta, että sopimusvapaus säilytetään. Jos lakia tai direktiiviä lähdetään uudistamaan, voitaisiin lainsäädännössä korostaa juuri allekirjoituksen toteutustavan ja käyttötarkoituksen yhteyttä. Tällöin painotettaisiin nykyistä enemmän käyttötarpeen ja tilanteen merkitystä käytet-

tävän allekirjoitusmenetelmän valintaa ohjaavana tekijänä. Laki olisi kirjoitettava informatiivisempaan muotoon lisäämällä siihen direktiivin 5 artiklan kohta 2 tai käyttämällä apuna UNCITRAL:in mallilakia.

Laatuvarmenneteknologian käyttö mahdollistaa myös vahvan sähköisen tunnistamisen. Koska kyseisen teknologian käyttö tunnistautumistarkoituksiin on yleisempää kuin allekirjoituskäyttö, voitaisiin laatuvarmennetasoinen tunnistaminen määritellä laissa allekirjoituskäytön ohella. Tällaiseen tunnistamisinstrumenttiin voitaisiin viitata erityislainsäädännössä, kuten rahanpesua ja terveydenhuoltoa koskevissa säännöksissä - tai jopa sähköisiä allekirjoituksia koskevassa lainsäädännössä itsessään sallimalla laatuvarmenteen hakijan tunnistautua laatuvarmenteella. Laatuvarmennetasoista tunnistamista ei kuitenkaan tulisi yleisesti korottaa ainoaksi ”lakisääteiseksi” tunnistamiskeinoksi, vaan laissa olisi mainittava, kuten allekirjoitusten osalta, että myös muut tunnistamismenetelmät voivat olla käyttökelpoisia. Tämänkaltainen uudistus voitaisiin toteuttaa sähköisiä allekirjoituksia koskevassa laissa. Mikäli sähköistä etätunnistamista katsottaisiin tarkoituksenmukaiseksi säännellä laajemmin lainsäädännössä, tulisi asiaa varten luoda omaa, allekirjoituksista erillistä lainsäädäntöä. Sähköinen etätunnistaminen on myös yhteisölainsäädännön intressissä oleva asia, koska sillä on merkityksensä mm. rikollisuuden torjunnassa, rahoitus- ja muiden etäpalveluiden edistämisessä yhteismarkkinoilla sekä muussa luottamuksellisessa asioinnissa.

7.2.3. Vastuusääntely

Kaupallista laatuvarmennustoimintaa voitaisiin harkita edistettäväksi sallimalla laatuvarmentajankin rajoittaa vastuunsa käytännön kannalta kohtuulliselle tasolle, esimerkiksi 500.000 - 1.000.000 euroon varmennustapahtumaa kohden. Tämä uudistus tulisi toteuttaa yhteisölainsäädännön tasolla, sillä nykyinen direktiivi ei mahdollista vastuunrajoituksia.

7.2.4. Lisäpalvelut

Selvityksessä ei tullut esille markkinoiden tai hallinnon taholta pakottavia syitä ryhtyä sääntelemään yksityiskohtaisesti sähköisiin allekirjoituksiin liittyviä lisäpalveluja, kuten esimerkiksi aikaleima- tai luotettuja sähköisiä arkistointipalveluja. Kansallisella tasolla sääntelyä ei siis tarvitse kehittää. Euroopan unionin tasolla kannattaa kuitenkin seurata kehitystä tarkoin. Mikäli tarpeita ilmaantuu vaikkapa erityislainsäädännössä, esimerkiksi sähköisiä julkisia hankintoja koskevien sääntöjen to-

teuttamiseksi, kannattaa Suomen tukea sääntelyn kehittämistä sellaiselta pohjalta, joka ei rajoita markkinoiden toimimista ja teknistä kehitystä.

7.2.5. Yksityisen toiminnan suhde julkiseen

Toimiva väestötietojärjestelmä on olennainen sekä sähköisten allekirjoitusten että sähköisen tunnistamisen kehittymisen kannalta, sillä varmentajana toimivat organisaatiot voivat perustaa toimintansa julkiseen infrastruktuuriin ja säästää kustannuksia. Kansainvälinen yhteistyö viranomaisten kesken luo rajat ylittävän ulottuvuuden tämän infrastruktuurin kehittämiselle. Infrastruktuurin käyttöä kaupallisessa varmennustoiminnassa tulisi kehittää täsmentämällä väestötietolakia niin, että muillakin laatuvarmentajilla kuin VRK:lla olisi oikeus sisällyttää sähköinen asiointitunnus varmenteeseensa, ja VRK:n olisi tuotettava tunnus tunnistetiedon pohjalta valtion maksuperustelaissa (150/1992) säädettyjen perusteiden mukaisesti.

Julkinen panostus laatuvarmentamistoimintaan lienee jatkossa välttämätön myös laatuvarmenteiden yhteismarkkinoiden tai yleisen liikkuvuuden kehittämiseksi. Vaikka laatuvarmennetasoiset varmenneratkaisut eivät ole saavuttaneet sitä asemaa, jota niillä direktiiviä ja lainsäädäntöä valmisteltaessa arveltiin olevan, olisi todennäköisesti virhe jättää panostamatta varmenteita koskevan oikeudellisen infrastruktuurin edelleen kehittämiseen. Itse asiassa monet toiminnot, joissa infrastruktuuria voitaisiin hyödyntää, eivät vielä ole toiminnassa, ajatellaanpa vain sähköistä hankintatointa yhteisötasolla tai rajat ylittävää palvelujen tarjontaa aloilla, joissa tietosuoja ja tietoturvavaatimukset korostuvat. Luotettavat varmennepalvelut ovat osa sitä infrastruktuuria, jonka varaan tietoyhteiskunnan palveluja voidaan rakentaa. Sen vuoksi myös lainsäädännön kehittämisen tarvetta tulisi arvioida, ei vain tämänhetkisten tarpeiden, vaan myös pitkän aikavälin kysymyksenä. Euroopan kilpailukykyä tultaneen tulevinakin vuosina rakentamaan tietoyhteiskunnan kehittämisen pohjalle.

Lainsäädännöllä olisi kuitenkin myös jatkossa pyrittävä tukemaan kaupallisen varmentamistoiminnan kehittämistä. Mahdollista yhteiskunnan varojen käyttämistä varmennetoiminnan edellyttämän välttämättömän infrastruktuurin ylläpitämiseen tulisi jatkossa arvioida objektiivisesti ja realistisesti, ottaen huomioon sekä aiempi kehityskulku että tämän pohjalta muotoutuneet ajan tasalla olevat näkemykset.

LÄHDEAINEISTOA

Säädösaineistoa ja julkista ohjeistusta

Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista, EYVL L 13, 19.01.2000, s. 12.

Komission päätös 2003/511/EY tehty 14 päivänä heinäkuuta 2003, sähköisiin allekirjoituksiin liittyviä tuotteita koskevien yleisesti tunnustettujen standardien viitenumeroiden julkaisemisesta Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY mukaisesti, EYVL L 175 , 15/07/2003, s. 45.

Komission tiedonanto neuvostolle, Euroopan Parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Toimintasuunnitelma sähköisten julkisten hankintojen sääntelykehyksen täytäntöönpanemiseksi, Bryssel 13.12.2004.

Euroopan parlamentin ja neuvoston direktiivi 2000/31/EY, annettu 8 päivänä kesäkuuta 2000, tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista ("Direktiivi sähköisestä kaupankäynnistä"). EYVL L 178, 17/07/2000, s. 1.

Neuvoston direktiivi 2001/115/EY, annettu 20 päivänä joulukuuta 2001, direktiivin 77/388/ETY muuttamisesta arvonlisäverotuksen laskuttamiselle asettamien vaatimusten yksinkertaistamiseksi, ajanmukaistamiseksi ja yhdenmukaistamiseksi. EYVL L 15 , 17/01/2002 s. 24.

Euroopan Parlamentin ja Neuvoston direktiivi 2004/18/EY,, annettu 31 päivänä maaliskuuta 2004,, julkisia rakennusurakoita sekä julkisia tavara- ja palveluhankintoja koskevien sopimusten tekomenettelyjen yhteensovittamisesta. EYVL L 134 , 30/04/2004 s. 114.

Euroopan Parlamentin ja Neuvoston direktiivi 2004/17/EY,, annettu 31 päivänä maaliskuuta 2004, vesi- ja energiahuollon sekä liikenteen ja postipalvelujen alalla toimivien yksiköiden hankintamenettelyjen yhteensovittamisesta. EYVL L 134, 30/04/2004 s. 1.

Neuvoston direktiivi 91/308/ETY, annettu 10 päivänä kesäkuuta 1991, rahoitusjärjestelmän rahanpesutarkoituksiin käyttämisen estämisestä, EYVL L 166, 28.6.1991.

Ehdotus: Euroopan parlamentin ja neuvoston direktiivi rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen KOM(2004) 448 lopullinen

Laki sähköisistä allekirjoituksista 2003/14, sekä siihen liittyvät

- Hallituksen esitys 197/2001

- Valiokuntamietinnöt

  - LIVM 21/2002vp

- PEVL 2/2002vp
- HaVL 32/2002vp

- Eduskunnan vastaus EV 221/2002vp

Laki sähköisestä asioinnista viranomaistoiminnassa 2003/13

Sähköisen viestinnän tietosuojalaki 2004/516

Henkilötietolaki 1999/523

Väestötietolaki 1993/507

Henkilökorttilaki 1999/829

Laki ajopiirturikorttien myöntämisen järjestämisestä 629/2004

Laki tietoyhteiskunnan palvelujen tarjoamisesta 458/2002.

Laki rahanpesun ehkäisemisestä ja selvittämisestä 68/1998, viimeksi muutettu lailla 365/2003.

Laki velan vanhentumisesta 728/2004.

Lääkkeiden toimittaminen, Lääkelaitoksen määräys 10/2002.

Maksuperustelaki 150/1992.

Sisäasianministeriön asetus rahanpesun estämisestä ja selvittämisestä (890/2003)

Sosiaali- ja terveysministeriön asetus 771/2003 sähköisen lääkemääräyksen kokeilusta

Tunnistaminen valtionhallinnon verkkopalveluissa, VM 6/01/2003, 29.9.2003

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Vahingonkorvauslaki 412/1974

Estonia Digital Signatures Act, Passed 8 March 2000, (RT I 2000, 26, 150) täydennetty useaan otteeseen

Signaturgesetz , Bundesgesetzblatt 1997 I 1872 (Artikel 3 Informations- und Kommunikationsdienstegesetz, Bundesgesetzblatt 1997 I 1870)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, General Assembly Resolution 51/162 of 16 December 1996. Artikla 5*bis* lisätty vuonna 1998.

UNCITRAL Model Law on Electronic Signatures

UN/CEFACT Recommendation 14 (1979), Annex I,
http://www.unece.org/cefact/rec/rec14/rec14_1979_inf63.pdf

Muuta lähdeaineistoa:

Bolero Standard Terms – Operational Service Contract, http://www.boleroassociation.org/downloads/op_sc.pdf, vierailtu 3.8.2003.

E-Commerce and Development Report 2002, UNCTAD/SDTE/ECB/2

E-Commerce and Development Report 2003, UNCTAD/SIDTE/ECB/2003/1

Electronic Signatures and Trusted Archival Services, Jos Dumortier & Sofie Van den Eynde, K.U.Leuven- ICRI, http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=, vierailtu 5.2.2005.

Gregory, J.D., Canadian and American Legislation on Electronic Signatures with reflections on the European Union Directive, International Colloquium, Internet law: European and international approaches, 19-20 November 2001, Paris, http://droit-internet-2001.univ-paris1.fr/ve/ , vierailtu 9.3.2003.

HST arkkitehtuurit ja liiketoimintamallit, Määrittely Versio 1.0, 12.5.2003.

Kilpailuviraston lausunto sisäasiainministeriön lausuntopyyntöön 3.7.2002 koskien väestötietolakia ja henkilökorttilakia, Dnro 619/72/2002, 19.8.2002.

Laine, Juha ja Ponka, Ilja, Kirjallisen muodon täyttäminen sähköisesti, Defensor Legis 2003, ss. 1028-1043.

Lausuntokooste10.2.2004, Liikenne- ja viestintäministeriö, Viestintämarkkinaosasto, Lausuntopyyntö sähköisen tunnistamisen ja teknisen valvonnan sääntelyn ja muiden toimenpiteiden tarpeesta.

Legal Aspects of Trusted Time Services in Europe, Research Paper commissioned by Amano authored by Jos Dumortier, Hannelore Dekeyser, Mieke Loncke, K.U.Leuven, Interdisciplinary Centre for Law & ICT (ICRI), http://www.e-timing.net/legal%20report%20E-timing%20ICRI%20TS.pdf, vierailtu 5.2.2005.

Myhr, Thomas, Regulating a European eID, A preliminary sudy on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005.

Oikeustoimilakikomitean mietintö, Kom 1990:20.

Rahanpesun torjunnan parhaat käytänteet, Keskusrikospoliisi, Rahanpesun selvittelykeskus, (http://www.poliisi.fi/intermin/images.nsf/files/111880F83D17EDF3C2256E36002E3A0B/$file/Rahanpesun+torjunnan+parhaat+käytänteet.pdf), vierailtu 14.4.2005.

Sammon allekirjoituspolitiikka (http://www.sampo.fi/ehdot/suomi/copy2/html, vierailtu 2.3.2005)

Sonera CA Certificate Policy, Sonera Class 2 Certificate, Valid as from January 22, 2004, Version 2.1. TeliaSonera Finland Oyj, 22.1.2004

Study for the European Commission – DG Information Society "The Legal and Market Aspects of Electronic Signatures – Legal and markety aspects of the application of Directive 1999/93/EC and practical applications in the Member States, the EEA, the Candidate and the Accession countries". Interdisciplinary centre for Law & Information Technology, Katholieke Universiteit Leuven, kirjoittaneet Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma ja Patrick van Eecke. September 2003. (viittaus: "The Legal and Market Aspects of Electronic Signatures")

Summary of Responses to the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-signatures in OECD Member Countries, http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final, vierailtu 8.1.2005

Sähköisen tunnistamisen sääntelyn tarve, Liikenne- ja viestintäministeriön julkaisuja 44/2003.

Turvalliset sähköisen allekirjoituksen luomisvälineet, Vaatimusten arviointi, Liikenne- ja viestintäministeriön julkaisuja 52/2004

Timestamping Service and digital signature applications, Cybernetica AS, http://www.timestamp.cyber.ee/ato/principles.html, vierailtu 14.2.2005

TIVEKE - Tietoturva, http://palvelut.tieke.fi/arkisto/tiveke/turva/turva-2.htm, vierailtu 3.5.2005

TUPAS, Pankkien tunnistuspalvelu asiointipalveluntuottajille, Palvelun kuvaus ja palveluntuottajan ohje, Versio 2.0, 13.6.2002, Suomen Pankkiyhdistys.

Varsinais-Suomen sairaanhoitopiirin varmennepolitiikka, Versio 1.0, 09.10.2003

Verkkoasiointia pankkitunnuksilla, Avainasiakas 1/2005, ss. 20-21 (Nordea, kirjoittanut Jari Valtonen)

Väestörekisterikeskus: Varmennuskäytäntö mobiilipäätelaitteen avulla käytettävää mobiilikansalaisvarmennetta varten TeliaSonera Finland Oyj:n liikkeelle laskemilla liittymäkorteilla.

LIITE 1 - KYSELYYN VASTANNEET ORGANISAATIOT

Selvitykseen yksityiskohtaisemmin vastanneet organisaatiot tai henkilöt

Ajoneuvohallintokeskus
DNA Finland Oy
DFDS Transport
Eesti Sertifitseerimiskeskus AS
Elisa Oyj
Evli Securities Plc.
FiCOM ry.
Finnkino Oy
Finnet Oy
Fujitsu Siemens Computers Oy
Handelsbanken
Howden Insurance Brokers Oy
John Nurminen Oy
Kansallisarkisto
Kansaneläkelaitos
Kauppa- ja teollisuusministeriö
Kesko Oyj
Euroopan komissio
Kuluttajavirasto
Lapin yliopisto
Liikenne- ja viestintäministeriö
Marsh Oy
Nokia Group
Nordea
Osuuspankkikeskus
Pohjois-Karjalan sairaanhoitopiiri
Rahoitustarkastus
Raha-automaattiyhdistys
Sampo Oyj
Secgo Oy
Sentera
Sisäasiainministeriö
Suomen Kuljetus ja Logistiikka SKAL ry
Suomen Pankki
Suomen Pankkiyhdistys ry
Teknillinen korkeakoulu
TeliaSonera Oyj
Tietosuojavaltuutettu
Tietotekniikan Liitto ry
Terveydenhuollon oikeusturvakeskus
Transpoint
Tullilaitos
Valimo Wireless Oy
Valtiovarainministeriö
VM Data Oy
Viestintävirasto
Väestörekisterikeskus
World Courier (Finland) Oy

Organisaatiot, jotka ovat antaneet tietoja varmenteiden käytöstä

Ajoneuvorekisterikeskus
Anttila Oy (NetAnttila)
AON Finland Oy
BH Broker House Oy
Danske Bank A/S
Ellos (Redcats Oy)
Europehouse Oy
Filmifriikki Oy
Finnair Cargo Oy
Firstbrokers Oy
H&M Hennes & Mauritz Oy
Heath Lambert Finland Oy
Helsingin kaupunki
Howden Insurance Brokers Oy
International Business Machines Oy Ab
If Vahinkovakuutus Oyj
Kalevala Koru Oy
Nordic Freight Oy
Oikeusministeriö
Optinet Oy
Patentti- ja rekisterihallitus
Pohjantähti Keskinäinen Vakuutusyhtiö
Schenker Oy
Segenmark Oy
Silja Oyj Abp
Stockmann Oyj
Keskinäinen Vakuutusyhtiö Tapiola
UPS SCS (Finland) Oy
Verkkokauppa.com
VR-yhtiöt

LIITE 2 - KYSYMYKSET

LAKI SÄHKÖISISTÄ ALLEKIRJOITUKSISTA 24.1.2003/14

Kysymyksiä lain vaikutuksen arvioinnista.

Ennen kysymysten esittämistä pyydämme Teitä etukäteen tutustumaan lain sisältöön, joka on liitetiedostona.

I. LAIN VAIKUTUSPIIRIIN LIITTYVIÄ YLEISIÄ KYSYMYKSIÄ

1) Onko organisaatiossanne käytössä sähköisen allekirjoituksen sovelluksia tai tarjoatteko palveluja joissa niitä hyödynnetään? Mitä menetelmiä on käytössä? Mikä on allekirjoitusten käytön määrä näissä palveluissa? Onko toteutuksessa kyse tunnistamisesta vai allekirjoittamisesta ja onko nämä toiminnot erotettu toisistaan?

2) Onko organisaationne käytössä laatuvarmenteita? Jos on, kuinka paljon ja mihin tarkoituksiin laatuvarmenteita (allekirjoitusvarmenne) ja toisaalta tunnistamisvarmenteita käytetään?

3) Onko mielestänne näköpiirissä, että lain erityisesti sääntelemien kehittyneiden sähköisten allekirjoitusten ja laatuvarmenteiden käyttö yleistyisi esimerkiksi matkapuhelinoperaattorien tai pankkien toimien kautta? Jos ei, minkä allekirjoitus- tai tunnistumismenetelmän uskotte yleistyvän jatkossa?

4) Pidättekö tarkoituksenmukaisena sitä, että turvalliseen allekirjoitustekniikkaan, joka tunnistaa henkilön sekä takaa sanoman kiistämättömyyden ja eheyden, panostetaan? Pidättekö omissa toiminnoissanne tarkoituksenmukaisena käyttää/hyödyntää ko. tekniikkaa? Aiheuttaako em. seikkoihin panostaminen puolustettavissa olevia kustannuksia saatuun hyötyyn nähden? Kuinka kustannuksia voitaisiin alentaa?

5) Mitä julkishallinto voisi tai mitä sen mielestänne pitäisi tehdä sähköisten allekirjoitusten ja toisaalta sähköisen tunnistamisen menetelmien käytön edistämiseksi ja helpottamiseksi?

6) Asiakirjojen allekirjoitusvaatimukset vaihtelevat oikeustoimittain ja sovellettavasta lainsäädännöstä riippuen. Onko tiedossanne tapauksia, joissa tahdonilmaisu tai oikeustoimi olisi kiistetty ja käsinkirjoitettuun allekirjoitukseen rinnastettavan sähköisen allekirjoituksen puuttuminen olisi aiheuttanut ongelmia

   - kansallisesti
   - kansainvälisesti?

7) Mikä on mielestänne riittävä tunnistamisen ja tahdonilmaisun todentamisen taso Siis mitä tunnistamis- ja allekirjoitusmenetelmiä mielestänne tarvitaan esim.:

   - lääkintähuollossa
   - reseptien kirjoittamisessa

- sosiaalitoimessa
- pankkitoiminnassa ja luotonannossa
- kuluttajakaupassa
- yritysten välisissä transaktioissa jne.

8) Pidättekö riittävänä/välttämättömänä sitä, että puhtaasta tunnistamisesta ja/tai allekirjoittamisesta sovitaan aina erikseen etukäteen toimijoiden välillä, sen lisäksi että on olemassa sopimus varmentajan ja palveluntarjoajan välillä, vai onko tarkoituksenmukaista tavoitella avoimempiin käyttäjäryhmiin soveltuvia tunnistamis- ja allekirjoitusmenetelmiä?

9) Miten palvelun tarjoajat mielestänne voitaisiin saada kiinnostumaan lain soveltamisalaan kuuluvien välineiden käytöstä?

10) Onko Teillä kokemuksia ulkomaisten varmennepalvelun tarjoajien toiminnasta ja ulkomaisten varmenteiden/muiden sähköisen allekirjoituksen menetelmien käytöstä?

11) Onko tiedossanne ulkomaisia sähköisiin allekirjoituksiin liittyviä sovelluksia, jotka soveltuisivat Suomen markkinoille?

II. LAKIIN LIITTYVIÄ YLEISIÄ KYSYMYKSIÄ

12) Onko sähköisiä allekirjoituksia koskeva laki (14/2003) osoittautunut mielestänne toimivaksi? Jos ei ole, niin miksi? Mitä ongelmia tai lain muutostarpeita on tullut esille?

13) Onko laki mielestänne riittävän selkeä esimerkiksi eri toimijoiden velvollisuuksien ja vastuiden osalta?

14) Onko lain soveltamisala tarkoituksenmukainen?

15) Pitäisikö lainsäädännössä säännellä myös pelkkää sähköistä tunnistamista eikä vain sähköistä allekirjoittamista?

16) Tulisiko lakiin sisällyttää täsmällisempiä määräyksiä myös muihin allekirjoituksiin kuin kehittyneisiin sähköisiin allekirjoituksiin liittyvistä kysymyksistä?

17) Tulisiko lakiin vastaavasti sisällyttää määräyksiä myös muista varmenteista kuin laatuvarmenteista nykyisten tietosuojasäännösten lisäksi?

18) Onko lainsäädännössä mielestänne sellaisia aukkoja, jotka edellyttäisivät lisäsääntelyä?

19) Ottaen huomioon, että esimerkiksi allekirjoituksen laatimisajankohdalla voi olla oikeudellista merkitystä, tulisiko lakiin ottaa määräyksiä aikaleimojen käytöstä allekirjoitusten yhteydessä?

20) Ovatko lain vastuusäännökset mielestänne toimivia ja tarkoituksenmukaisia?

21) Tulisiko laissa jotenkin huomioida nykyistä enemmän anonyymin sähköisen asioinnin mahdollistaminen?

22) Direktiivin liite sisältää turvallisia allekirjoituksen todentamisvälineitä koskevia suosituksia. Tulisiko tältä osin olla kansallista sääntelyä?

III. LAIN SISÄLTÖÖN LIITTYVÄT YKSITYISKOHTAISET KYSYMYKSET

23) Onko lain 3 §:n soveltamisalasäännöksen suhteen ilmennyt tulkintaongelmia ja pitäisikö kyseistä lainkohtaa täsmentää?

24) Onko turvallisten allekirjoituksen luomisvälineiden arviointia koskeva sääntely (5 ja 6 §) toimivaa ja riittävää?

25) Lain 7 § 2 momentin 3 kohta sisältää määräyksen laatuvarmenteeseen sisältyvästä allekirjoittajan henkilöllisyyden ilmoittamisesta joko omalla tai salanimellä. Myös samannimiset laatuvarmenteen haltijat täytyy kuitenkin erottaa jollakin keinoilla toisistaan.

    Tulisiko lakia täsmentää sen suhteen kuinka varmennettavan henkilön identifiointi tulisi toteuttaa?

    Tätä tarkoitusta varten on Väestörekisterikeskuksella käytössään sähköinen asiointitunnus (”SATU”). Pitäisikö SATU mielestänne nykyisen sääntelyn perusteella luovuttaa myös VRK:n ulkopuoliseen käyttöön ja ilman merkittäviä kustannuksia?

26) Lain 7 §:n 2 momentin 9. kohta koskee mm. varmenteen roolivarmennekäyttöä. Tulisiko rooli/työvarmenteiden osalta olla lisäsääntelyä?

27) Oletteko havainneet ongelmia lain 8 §:n mukaisen, Euroopan talousalueelta tulevan varmentajan myöntämien laatuvarmenteiden yhteentoimivuudessa kotimaisten varmenteiden kanssa?

28) Ovatko lain laatuvarmentajalle aiheuttamat velvoitteet joltain osin liian raskaita tai toimintaa rajoittavia?

    - 10-12 §§ velvoitteet,
    - ”riittävät taloudelliset voimavarat”,
    - organisaatio ja asiantuntemus,
    - varmennerekisterin ja sulkulistan ylläpito ym.
    - vastuusääntely,
    - Viestintäviraston maksuista annetun lvm:n asetuksen laatuvarmenteiden tarjoajia koskevat maksut

29) Lain 13 §:n mukaan allekirjoittajan on viipymättä pyydettävä laatuvarmenteen myöntäneeltä varmentajalta laatuvarmenteen peruuttamista, jos hänellä on perusteltua syytä epäillä allekirjoituksen luomistietojen oikeudetonta käyttöä. Tällöin laatuvarmenteen tarjoajan on viipymättä peruutettava laatuvarmenne, jos allekirjoittaja sitä pyytää merkitsemällä varmenteen sulkulistalle. Laki sisältää maininnan, jonka mukaan peruuttamispyynnön katsotaan saapuneen varmentajalle silloin kun se on ollut varmentajan käytettävissä siten, että pyyntöä voidaan kä-

sitellä. Lain 17 §:ssä todetaan, että allekirjoittaja vastaa sähköisen allekirjoituksen luomistietojen oikeudettomasta käytöstä, kunnes peruuttamispyyntö on saapunut varmentajalle. Onko kyseinen sääntely mielestänne ollut toimivaa ja tarkoituksenmukaista ja synnyttääkö sääntely mielestänne näyttöongelmia? Olisiko tässä kohtaa syytä säännellä ns. aikaleimoihin liittyviä kysymyksiä?

30) Lain 14 §:ssä mainitun sulkulistan ylläpito on toimintaa, josta voidaan veloittaa, jolloin listan oleminen luottavien osapuolten saatavilla vaatii käytännössä sopimusjärjestelyjä. Kuinka sulkulistan ylläpito tulisi organisoida julkisuus- ja tietosuojakysymysten osalta? Miten listan tietojen tarkastaminen voitaisiin luotettavasti todentaa vastuukysymysten selvittämiseksi ilman että tästä aiheutuu tietosuojaongelmia?

31) Pitäisikö sulkulistan ylläpidon lisäksi säännellä säilyttämistä (aikaa) tai sulkulistan tarkastamista koskevia velvoitteita? Perusteluissa sanotaan, että sulkulista on säilytettävä tarkoituksenmukainen aika. Luottavan osapuolen intressissä on tarkastaa sulkulistalta onko varmenne voimassa, mutta tästä ei ole säännöksiä laissa. Tulisiko sulkulistan tarkastamista säännellä tältä osin?

32) Varmenteen voimassaolon tarkastamista koskevat tiedot: lain 21 § ja siihen liittyvät 14.1 §:n 3 kohta ja 14.2:n loppuosa ovat kansallisia säännöksiä. Ovatko lainkohdat aiheuttaneet tulkintaongelmia? Onko teillä 14.2 §:n käytännön soveltamisesta kokemuksia tai muutoin näkemyksiä?

33) Onko lain 16 §:n vastuusäännösten osalta tullut esille tulkintaongelmia?

Laatuvarmenteisiin perustuvien sähköisten allekirjoitusten käyttö tilanteessa, jossa markkinoilla on yksi, myös viranomaisena toimiva, laatuvarmentaja, on synnyttänyt vastuunjakoon liittyvän sopimusverkoston. Varmentaja ja esimerkiksi eri toimintojen toteuttajat voivat keskenään sopia keskinäisestä vastuustaan. Laatuvarmentajien vastuun poolausmahdollisuus eli yhteisvastuujärjestelyt? Onko todistustaakkasääntö 16 §:n 2 momentissa perusteltu? Tulisiko laatuvarmentajan voida rajoittaa vastuutaan myös suhteessa luottavaan osapuoleen?

33) Onko lain 18 §:n sanamuoto, jonka mukaan kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä, ainakin täyttää laissa olevan allekirjoitusta koskevan vaatimuksen, sellaisenaan riittävä tuomaan esille sen, että myös muut sähköiset allekirjoitukset voivat täyttää tapauskohtaisesti allekirjoitusta koskevan vaatimuksen? Direktiivin 5 artiklan 2 kohta toteaa tämän nimenomaisesti, mutta tätä ei ole otettu eksplisiittisesti Suomen lakiin.