SÄHKÖISEN TUNNISTAMISEN MUUTTUVA SÄÄDÖSKENTTÄ

Vahvan sähköisen tunnistamisen ja allekirjoittamisen sääntely ja sen muutokset Suomessa sekä vaikutukset sähköisen asioinnin suosioon

Yritysjuridiikan pro gradu -tutkielma

Laatija:
Olli Jääsaari 413689

Ohjaaja:
Professori, OTT Matti J. Sillanpää

22.6.2016
Turku

Sisällysluettelo

Lait ja lyhenteet

1999/39/EY	Euroopan parlamentin ja neuvoston direktiivi 1999/39/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista
AOA	eduskunnan apulaisoikeusasiamies
asiointilaki	laki sähköisestä asioinnista viranomaistoiminnassa (24.1.2013/13)
eIDAS-asetus	Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/39/EY kumoamisesta
EU	Euroopan unioni
(EU) 2015/806	komission täytäntöönpanoasetus (EU) 2015/806, annettu 22. päivänä toukokuuta 2015, hyväksyttyjä luottamuspalveluja koskevan EU:n luotettavuusmerkin muotoon sovellettavista eritelmistä
hallintolaki	hallintolaki (6.6.2003/434)
HAO	hallinto-oikeus
HE	hallituksen esitys
henkilökorttilaki	henkilökorttilaki (28.7.1999/829)
henkilötietolaki	henkilötietolaki (22.4.1999/523)
HO	hovioikeus
IP	Internet Protocol, suom. internet-protokolla
KHO	korkein hallinto-oikeus
KK	kirjallinen kysymys

laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 49§:n muuttamisesta (997/2015)	
luottolaitoslaki	laki luottolaitostoiminnasta (8.8.2014/610)
LVM	liikenne- ja viestintäministeriö
maakaari	maakaari (12.4.1995/540)
maksupalvelulaki	maksupalvelulaki (30.4.2010/290)
OECD	Organization for economic cooperation and development, Taloudellisen yhteistyön ja kehityksen järjestö
oikeustoimilaki	laki varallisuusoikeudellisista oikeustoimista (13.6.1929/228)
rahanpesulaki	laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (18.7.2008/503)
RL	rikoslaki (19.12.1889/39)
Rooma I -asetus	Euroopan parlamentin ja neuvoston asetus (EY) N:o 593/2008, annettu 17 päivänä kesäkuuta 2008, sopimusvelvoitteisiin sovellettavasta laista (Rooma I)
Rooma II -asetus	Euroopan parlamentin ja neuvoston asetus (EY) N:o 864/2007, annettu 11 päivänä heinäkuuta 2007, sopimukseen perustumattomiin velvoitteisiin sovellettavasta laista (Rooma II)
SEUT	Euroopan unionin toiminnasta tehty sopimus
SIM	subscriber identity module
tietoyhteiskuntakaari	tietoyhteiskuntakaari (7.11.2014/917)
tunnistuslaki	laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617)
vahingonkorvauslaki	vahingonkorvauslaki (31.5.1974/412)
varmuustasoasetus	komission täytäntöönpanoasetus (EU) 2015/1502, annettu 8 päivänä syyskuuta 2015, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 910/2014 8 artiklan 3 kohdan mukaisesti
VNa	Valtioneuvoston asetus
VRK	Väestörekisterikeskus
väestötietojärjestelmälaki	laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (21.8.2009/661)

1 JOHDANTO

Vahvaa sähköistä tunnistamista ja allekirjoittamista koskeva säädöskenttä on voimakkaassa muutoksessa. Vuonna 2009 säädettyä lakia vahvasta sähköisestä tunnistamisesta ja allekirjoittamisesta (tunnistuslaki) on muutettu vuoden 2016 alusta ja esitetään muutettavaksi uudelleen. Myös Euroopan komission ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin palveluihin liittyvistä luottamuspalveluista sisämarkkinoilla (ns. eIDAS-asetus) tulee sovellettavaksi 2016 heinäkuusta lähtien. Lisäksi julkishallinnon tapa järjestää sähköisen asioinnin tukipalveluita on muuttumassa, mikä vaikuttanee myös julkishallinnon sähköisiin palveluihin tunnistautumiseen.

Tämän tutkielman tarkoituksena on kuvata vahvan sähköisen tunnistamisen ja allekirjoittamisen nykytila sekä vuoden alusta voimaan tulleet että tulevat muutokset niiltä osin kuin lakimuutoksia on valmisteilla. Erityisesti keskitytään vastuiden jakautumiseen osapuolten välillä. Muutosten vaikutukset vastuun jakautumiseen esitetään muutosten yhteydessä.

Oikeustieteellisestä näkökulmasta aihetta lähestytään lainopin kautta. Tutkin osapuolten välisen vastuun jakautumista tietyissä tilanteissa ja toisaalta tulkiten kuinka jo voimaan astuneet ja vasta esitetyt muutokset lainsäädännössä vaikuttavat. Tässä työssä aihetta pyritään lähestymään objektiivisesti, mutta uusien lakien osalta tukeudutaan vahvasti lakien valmisteluaineistoon, joka puolestaan johtaa helposti teleologiseen eli tarkoitusperäopilliseen tulkintaan. Oikeustapauksia vahvasta sähköisestä tunnistamisesta on vähäisesti, mutta luottokorttien osalta käytäntö on vakiintunutta. Tarkasteltavat vastuukysymykset kuitenkin vastaavat toisiaan ja maksuvälineiden luvatonta käyttöä koskevia ratkaisuja voidaankin analogian keinoin soveltaa myös sähköiseen tunnistamiseen.[1]

Suomessa valittua linjaa vertaillaan myös Viroon, jota pidetään yhtenä edistyneimmistä maista sähköisen asioinnin saralla: jokaisella 15 vuotta täyttäneellä kansalaisella on oltava henkilökortti, jota voidaan käyttää myös sähköiseen tunnistamiseen ja esim. äänestämiseen. Toisaalta vertailua tehdään myös Iso-Britanniaan, missä henkilökorttiprojekti lopetettiin vuonna 2010 ja jossa henkilöllisyyden varmistaminen on täysin ulkoistettu yrityksille. Vaikka pienimuotoista vertailua näihin maihin tehdäänkin, on tutkielman kohteena silti suomalainen oikeus eikä tutkimusote ole oikeusvertaileva.

Pääministeri Juha Sipilän hallitusohjelman tavoitteena on edistää digitalisaatiota ja rakentaa asiakaslähtöisiä palveluita parantamalla viranomaisten välistä tietojenvaihtoa. Samalla on tarkoitus poistaa esteitä digitaalisten palveluiden ja sovellusten tarjoamisel-

---

[1] Peczenik 1995, s. 52–57

ta, myös niiltä palveluilta, joita tarjotaan uusin liiketoimintamallein.[2] Osana tätä hallituksen kärkihanketta on hallitus on tuonut Eduskunnalle esityksen hallinnon yhteisistä sähköisen asioinnin tukipalveluiden keskittämisestä pääosin Väestörekisterikeskukseen.[3]

Lakiehdotus toteuttaa kansallisen palveluarkkitehtuuriohjelman linjauksia, mikä pyrkii luomaan viranomaisten välisen tiedonsiirtokanavan, jota yrityksetkin voisivat käyttää. Se poistaisi päällekkäisyyksiä ja pienentäisi kustannuksia. Esitykseen sisältyy myös uusi julkishallinnon tunnistamispalvelu, joka korvaa käytössä olevat tunnistus.fi- ja Vetuma-palvelut.

Suurelle osalle suomalaisia vahva sähköinen tunnistaminen tarkoittaa pankkitunnuksilla tunnistautumista esimerkiksi Kelan tai Verohallinnon asiointipalveluun. Henkilökortille sisältyvän Väestörekisterikeskuksen myöntämän kansalaisvarmenteen käyttö on kuitenkin jäänyt pieneksi. Pääministeri Sipilän hallitusohjelman voisikin ajatella laajentavan sähköisten palvelujen tarjontaa ja siirtävän painopistettä henkilökohtaisista käynneistä ja paperilomakkeista kohti sähköisiä palveluja.

Viranomaisten sähköisistä palveluista saamia kustannushyötyjä kuitenkin pienentää velvollisuus ylläpitää rinnakkaisia palvelukanavia. Eduskunnan apulaisoikeusasiamies on vastikään moittinut Verohallinnon päätöstä ottaa vastaan yrittäjien lakisääteisiä rakentamisilmoituksia myös sähköisesti. Apulaisoikeusasiamies Sakslinin mukaan Verohallinto on ylittänyt toimivaltansa, sillä velvollisuus sähköiseen asiointiin ei hänen mukaansa ota huomioon pienten yritysten ja yrittäjien mahdollisuuksia kyseisten velvoitteiden toteuttamiseen. Lisäksi apulaisoikeusasiamies kiinnitti huomiota maan eri alueilla toimivien henkilöiden yhdenvertaiseen kohteluun, ilmeisesti viitaten kantelijan esille nostamaan seikkaan maaseudun internet-yhteyksien toimimattomuudesta.[4]

Yhteyksien toimimattomuuteen vetoaminen on jossain määrin kummallista, sillä kaikkialle Suomessa on tietoyhteiskuntakaaren 87 §:n ja Liikenne- ja viestintäministeriön asetuksen perusteella tarjottava yleispalveluna vähintään 2 mbit/s toimiva internet-yhteys.[5] Lisäksi kantelijan mukaan yrittäjältä ei voi edellyttää auton taikka tietokoneen ja internet-yhteyden sekä vahvan sähköisen tunnistusvälineen käyttömahdollisuutta. Yrittäjänä toimiminen vaatii kuitenkin pankkiasiointia, joka henkilökohtaisen palvelun maksujen ja konttoriverkostojen harventamisen myötä on siirtynyt enenevissä määrin internet-palveluksi. Näin ollen hieman ihmettelen päätöstä. Valtion viranomaisten on kuitenkin tulevaisuudessakin tarjottava palvelua paperilomakkein, puhelimitse

---

[2] Hallituksen julkaisusarja 10/2015, s. 26–27

[3] HE 59/2016 vp, s. 1–3

[4] AOA 4653/4/14

[5] LVMa 439/2015

sekä henkilökohtaisesti palvelupisteissä sähköisen palvelukanavan suosion kasvamisesta riippumatta.

Käyttäjän tunnistaminen onkin kiinteä osa digitaalisten palvelujen tarjoamista. Heikkoa tunnistamista, yleisimmin käyttäjätunnuksen ja salasanan avulla, ei ole säädelty, mutta vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annettu laki (tunnistuslaki) sääntelee edellytykset vahvan tunnistuspalvelun tarjoajille, sekä tällaisilla tunnistusvälineillä tehtävien toimenpiteiden vaikutukset. Lakiin on tehty 1.1.2016 voimaan tulleita muutoksia ja 2017 toukokuussa tällaisten tunnistuspalvelun tarjoajien on liityttävä samaan luottamusverkostoon (tunnistuslaki 12 a §). Sen jälkeen tunnistamista vaativan palvelun ylläpitäjän ei tarvitsisi enää tehdä sopimusta jokaisen tunnistusvälineiden myöntäjän kanssa erikseen, vaan yksi sopimus yhden tunnistamista välittävän palvelun kanssa riittäisi siihen, että kaikki myönnetyt välineet ovat käytössä.

Vahvaa sähköistä tunnistamista koskee myös eIDAS-asetus. Asetuksen vaikutukset tulevat olemaan suuret, sillä se pakottaa jäsenvaltiot hyväksymään toisissa maissa rekisteröidyt vahvan sähköisen tunnistamisen menetelmät viranomaispalveluissaan avaten ne myös EU-maiden kansalaisille. Lisäksi asetus sääntelee suoraan luottamuspalveluja, kuten sähköisiä allekirjoituksia.

Sähköisten palvelujen tarjoaminen ei kuitenkaan ole hyödyllistä, jos palveluja ei käytetä, joten palvelujen on annettava käyttäjilleen jotain hyötyä verrattuna muulla tavoin saatavilla olevaan palveluun, esimerkkinä käytettäköön vaikka muutosverokortin tilaamista internet-palvelusta tai käyntiä verotoimistossa. Tämä hyöty voi olla vaikka mahdollisuus asioida myöhään illalla tai matkustus- ja jonotustarpeen poistuminen, jolloin kansalaiselle jää enemmän aikaa tehdä muita asioita.

Käyttäjän kokemat hyödyt otetaan tutkielmassa huomioon tietojärjestelmätieteen tutkimuksessa esitettyjä järjestelmien käyttöönottoa kuvaavia malleja käyttämällä. Mallien avulla on löydetty tiettyjä uusien järjestelmien käyttöönoton ajureita, joiden avulla tarkastellaan kuinka nyt tehdyt sekä esitetyt muutokset lainsäädännössä saattavat vaikuttaa sähköisen tunnistamisen ja allekirjoittamisen suosioon. Ajureiden kautta tarkastelu soveltuu tunnistuspalvelun käyttäjän sekä tunnistamista vaativan palveluntarjoajan näkökulman arvioimiseen, tunnistuspalvelun tarjoajan näkökulmaa niillä ei voida tarkastella. Itse mallit kuvataan tarkemmin luvussa 2.2.

2 SÄHKÖINEN TUNNISTAMINEN JA ALLEKIRJOITUS

2.1 Sähköisen tunnistamisen ja allekirjoituksen käsitteet

Henkilökohtaisessa asioinnissa on joskus tarpeellista tunnistaa jonkin palvelun käyttäjän henkilöllisyys, vaikkapa suurta laitetoimitusta solmittaessa tai kun viranomainen antaa henkilöä koskevia, salassa pidettäviä tietoja. Jos henkilö on palveluntarjoajalle tuttu, voi palveluntarjoaja arvioida käyttäjän ulkomuotoa, olemusta ja käyttäytymistä omiin aiempiin kokemuksiinsa ja näin tunnistaa henkilön.

Satunnaisesti valitun henkilön tunnistamisessa täytyy kuitenkin turvautua jonkinlaiseen todisteluun, Suomessa tyypillisesti poliisin myöntämän passin, henkilökortin tai ajokortin avulla. Tällöin henkilöllisyystodistus näyttää tarjoavan vakuutuksen siitä, että kyseinen henkilöllisyys on olemassa. Palveluntarjoajan on arvioitava kyseisen todisteen aitous sekä verrattava henkilön ulkonäköä todisteessa mainittuun.

Sähköisen asioinnin yleistyessä on tullut tarpeelliseksi yksilöidä ja tunnistaa käyttäjä korkealla varmuudella myös silloin kun käyttäjä ei itse ole paikalla. Joissain palveluissa, kuten yritysten tuotekuvastoissa, ei välttämättä ole tarpeellista tietää tarkasti kuka palvelua käyttää, mutta vaikkapa Kelan asiointipalvelussa on tärkeää, ettei salassa pidettäviä tietoja näytetä muille kuin niihin oikeutetuille.

Sähköinen tunnistaminen voidaan jakaa heikkoon ja vahvaan tunnistamiseen. Vahva sähköinen tunnistaminen perustuu kahteen tai useampaan seuraavista vaihtoehdoista (tunnistuslaki 1 §):

- Johonkin, mitä tunnistusvälineen haltija tietää, kuten käyttäjätunnus ja salasana
- Johonkin, mitä tunnistusvälineen haltijalla on hallussaan, kuten sirukortti tai salasanalista
- Johonkin tunnistusvälineen haltijan yksilöivään ominaisuuteen, kuten sormenjälki tai iiriskuva.

Mikäli tunnistaminen perustuu vain yhteen mainituista tiedoista, on kyseessä heikko tunnistamismenetelmä, kuten pelkkä käyttäjätunnus-salasanapari tai soitto tietystä matkapuhelinnumerosta. Heikko tunnistaminen on jätetty sääntelyn ulkopuolelle. Yksittäisten verkkosivujen käyttäjätunnusten ja salasanojen sekä muiden kirjautumistapojen sääntely ja etenkin sääntelyn valvonta olisi hankalaa eikä näkemykseni mukaan toisi mainittavaa hyötyä, toisin kuin vahvojen sähköisten tunnistamismenetelmien sääntely, jolla voidaan kasvattaa luottamusta sähköiseen asiointiin.

Vahvaa sähköistä tunnistamista säännellään pääasiassa tunnistuslailla. Vuoden 2016 heinäkuusta lähtien sovelletaan myös EU:n eIDAS-asetusta, joka tunnistuspalveluiden osalta sääntelee lähinnä unionin sisärajat ylittäviä transaktioita, mutta vaikuttaa myös

kansallisen lainsäädännön kehittämiseen. Myös oikeustoimilaki ja vahingonkorvauslaki vaikuttavat osaltaan.

Käyttäjien tunnistamisen luotettavuus voidaan jakaa käyttäjäidentiteetin ja käyttäjäidentiteetin todentamisen luotettavuuteen. Käyttäjäidentiteetti on joukko käyttäjän henkilöllisyyttä kuvaavia tietoja, vaikkapa nimi, osoite tai sähköinen asiointitunnus. Käyttäjäidentiteetin luotettavuudella kuvataan, kuinka todennäköisesti nämä tiedot kuvaavat identiteetin takana olevaa henkilöä. Käyttäjäidentiteetin luotettavuus on matala, jos tiedot ovat käyttäjän itsensä rekisteröitymisen yhteydessä antamia, kuten vaikkapa sosiaalisen median verkostopalveluissa, kuten Facebookissa. Kyseistä henkilöllisyyttä ei välttämättä ole laisinkaan olemassa. Sen sijaan jos käyttäjä on luotettavasti selvittänyt henkilöllisyytensä vaikkapa virallisella henkilökortilla ja osoitetiedot on haettu väestötietojärjestelmästä, on käyttäjäidentiteetin luotettavuus erittäin vahva.[6] Käyttäjäidentiteetin todentamisen korkea taso taataan tunnistuslaissa velvoittamalla tunnistuspalvelun tarjoaja tarkistamaan ja päivittämään tiedot väestötietojärjestelmästä, joten vahvaan sähköiseen tunnistamiseen luottavat palveluiden tarjoajat voivat olla luottavaisia, että tunnistuspalvelun ilmoittama henkilöllisyys todella on olemassa.

Käyttäjäidentiteetin todentamisen luotettavuus tarkoittaa käyttäjän tunnistamisessa käytettävän menetelmän luotettavuutta. Esimerkiksi henkilöllisyyden todentaminen opiskelijakortista on mahdollista, mutta luotettavampaa on turvautua viranomaisen myöntämään henkilöllisyystodistukseen. Heikon luotettavuuden ääripäässä kulkevat käyttäjän itse suullisesti tai kirjallisesti antamiin tietoihin luottaminen tai anonyymin asioinnin salliminen. Vaikkapa kuluttajaelektroniikkaa myyvän liikkeen ei pääsääntöisesti tarvinne tunnistaa asiakastaan, mikäli myytävä tavara maksetaan välittömästi.

Sähköisten allekirjoitusten osalta samojen tunnistamisen kriteerien on täytyttävä, mutta tiedot on aina liitetty johonkin muuhun sähköiseen tietoon, esimerkiksi asiakirjaan. Käyttäjä tunnistetaan samoin periaattein kuin vahvassa sähköisessä tunnistamisessa. Myös allekirjoittaminen jaetaan kehittyneisiin sähköisiin allekirjoituksiin ja muihin sähköisiin allekirjoituksiin. Kehittyneet sähköiset allekirjoitukset luodaan menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan niin, että hänet ja hänen henkilöllisyytensä voidaan yksilöidä ja liittää allekirjoitettuun dokumenttiin siten, että mahdolliset muutokset voidaan havaita (tunnistuslaki 2 §).

Sähköistä allekirjoitusta koskevat säännökset löytyvät pääosin tunnistuslain 4. luvussa. Tärkeää on huomioida laatuvarmenteen määritelmä, sillä vain laatuvarmenteita tarjoavan varmentajan on ilmoitettava toiminnan aloittamisesta Viestintävirastolle ja toisaalta laissa säädetyt velvollisuudet koskevat vain laatuvarmenteita tarjoavia varmentajia.

---

[6] VAHTI 12/2006, s. 18–19

Laatuvarmenteen tulee sisältää:
1) tieto siitä, että varmenne on laatuvarmenne;
2) tieto varmentajasta ja sen sijoittautumisvaltiosta;
3) allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi;
4) allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja;
5) laatuvarmenteen voimassaoloaika;
6) laatuvarmenteen yksilöivä tunnus;
7) varmentajan kehittynyt sähköinen allekirjoitus;
8) mahdolliset laatuvarmenteen käyttörajoitukset; sekä
9) allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.
(Tunnistuslaki 30.2 §)

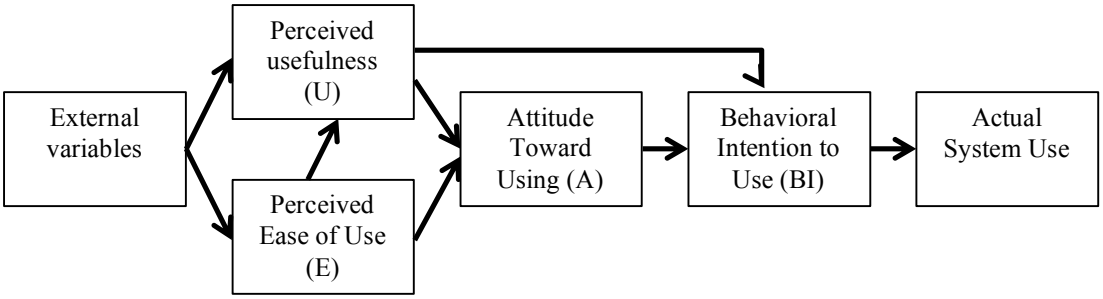
Lisäksi laatuvarmenteen myöntäjän, aivan kuten tunnistuspalvelun tarjoajan, tulee täyttää laissa asetetut vaatimukset, tai myönnetty varmenne ei ole laatuvarmenne. Varmentajalle asetetut vaatimukset luetellaan tunnistuslain 33–38 §:ssä sisältäen säännöksiä yleisistä velvollisuuksista, varmenteiden liikkeelle laskemisesta ja peruuttamisesta sekä laitteista, ohjelmistoista ja ylläpidettävistä rekistereistä.

Suomessa sähköiseen tunnistamiseen liittyviä julkaisuja ovat tuottaneet lähinnä viranomaiset omilla raporteillaan ja ohjeillaan. Nimenomaisesti sähköistä allekirjoitusta ja tunnistamista koskevista tieteellisistä tutkimuksista tulee erityisesti mainita Ilja Ponkan 2013 julkaistu väitöskirja, jossa tunnistuslaki käydään perusteellisesti läpi suomalaisen velvoiteoikeuden näkökulmasta. Tomi Voutilainen on puolestaan vuonna 2009 julkaistussa väitöskirjassaan käsitellyt ICT-oikeutta sähköisessä hallinnossa, mutta sähköistä tunnistamista koskevat jaksot perustuvat silloin vireillä olleeseen lainsäädäntöhankkeeseen, jonka perusteella tunnistuslaki annettiin.

2.2 Tietojärjestelmätieteen malleja sähköisten palveluiden käytön ajureista

Sähköisten palveluiden ja tietokonesovellusten käyttöönottoa on tutkittu laajasti ja sekä työntekijöiden että kuluttajien käyttäytymiselle on luotu useita malleja. Yksi laajimmin tunnetuista malleista lienee Technology Acceptance Model (TAM). TAM:n perusajatus on, että tietojärjestelmän käyttöönottoon vaikuttaa pääasiassa käyttäjän kokema hyöty (*perceived usefulness*) ja koettu helppokäyttöisyys (*perceived ease of use*). Koetulla hyödyllä tarkoitetaan tässä sitä, kuinka paljon tehokkaammin käyttäjä suorittaa tehtävän

järjestelmän avulla kuin ilman sitä, ja koetulla helppokäyttöisyydellä, kuinka vaivatonta järjestelmän käyttäminen on.[7]



Kuvio 1 Technology Acceptance Model (Davis, Bagozzi & Warshaw 1989, s. 985)

TAM on tutkimuksissa selittänyt tyypillisesti 40 % tietojärjestelmien käyttöaikomuksista ja käytöstä, ja malli selittää niiden käyttöä paremmin kuin *theory of reasoned action*, jolle TAM perustuu, tai *theory of planned behaviour*, joka on *theory of reasoned actionin* laajennus. Technology Acceptance Modelia on julkaisemisensa jälkeen laajennettu kattamaan myös yhteisön subjektiiviset normit, eli mitä käyttäjälle tärkeät ihmiset olettavat hänen tekevän tai jättävän tekemättä.[8]

Technology Acceptance Model näkyy myös osana UTAUT-mallia, joka pyrkii yhdistämään useita tietojärjestelmien käyttöönottoa kuvaavia malleja yhdeksi, kattavammaksi malliksi. UTAUT, eli Unified Theory of Acceptance and Use of Technology, luokittelee käyttöönoton ajureiksi odotetun hyödyn (*performance expectancy*), odotetun vaivan (*effort expectancy*), sosiaalisen paineen (*social influence*) ja käyttöolosuhteet (*facilitating conditions*), joihin vaikuttavia tekijöitä ovat sukupuoli, ikä, kokemus ja järjestelmän käytön vapaaehtoisuus.[9]

Mallia on myöhemmin täydennetty kattamaan erityisesti kuluttajien käyttöönottotilanteita alkuperäisen UTAUT-mallin keskittyessä työelämään. UTAUT2-mallissa on otettu huomioon, että erityisesti hedonistiset ajurit, kuten ilo ja nautinto sekä arjesta pakeneminen, sekä palvelun käytön hinta vaikuttavat enemmän kuluttajien omissa valinnoissa kuin niissä, joita työpaikalla tehdään.[10]

Odotettu hyöty ja odotettu vaiva vastaavat suurin piirtein TAM:n koettua hyötyä ja koettua helppokäyttöisyyttä, joten tässä tutkielmassa käytetään UTAUT2-mallia TAM:n

---

[7] Davis, Bagozzi & Warshaw 1989, s. 985–986

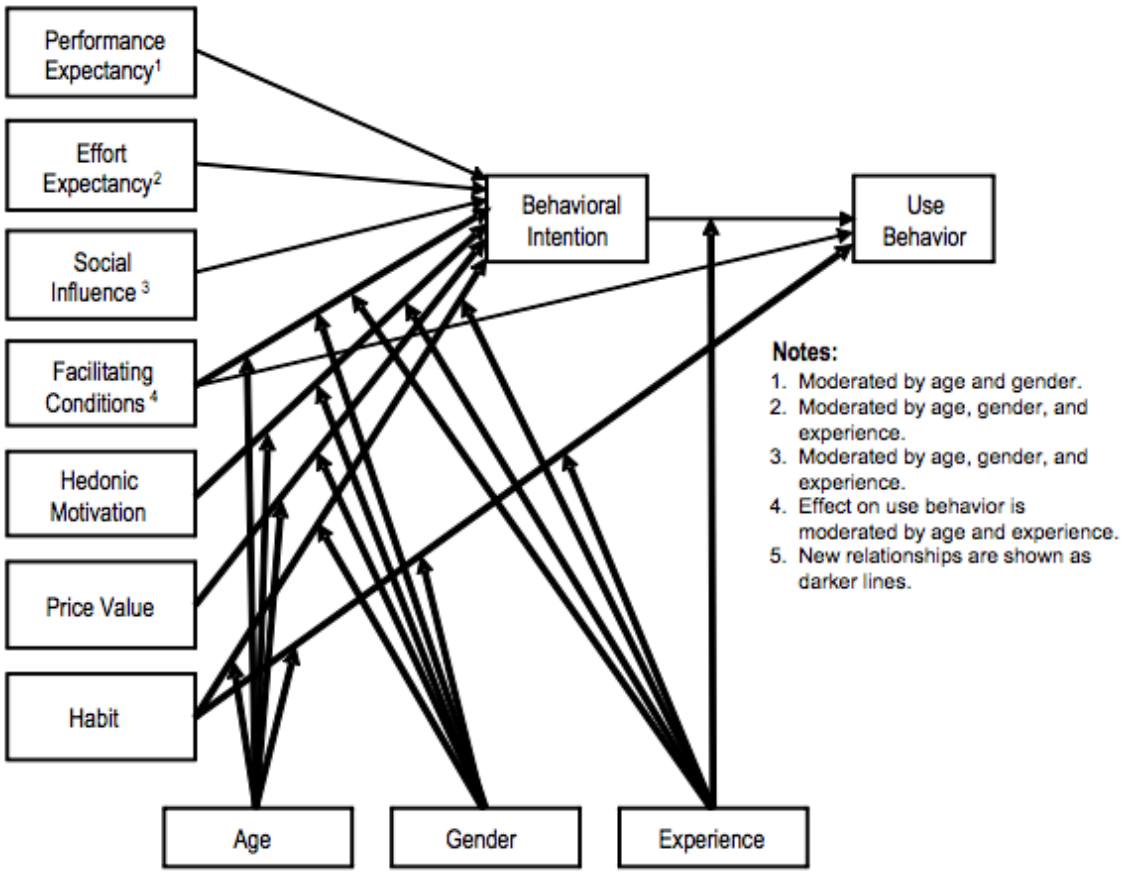
[8] Pikkarainen ym. 2004, s. 226

[9] Venkatesh ym. 2003, s. 446–455

[10] Venkatesh, Thong & Xu 2012, s. 157–162

sijaan. Valinta mahdollistaa yksityiskohtaisemman jaottelun järjestelmän käyttämisen ajureihin, joka puolestaan helpottaa lainsäädännön muutosten vaikutusten arviointia. Lisäksi UTAUT2-mallin on todettu kuvaavan järjestelmien käyttöönottoa kuin muiden Technology Acceptance Modelin jatkeiden.[11]

Yksi TAM:n kritiikin kohteista on, ettei se suoraan huomioi aiempia käyttökokemuksia, joilla on suuri vaikutus tietojärjestelmän myöhempään käyttöön.[12] Asia kuitenkin otetaan huomioon UTAUT2-mallissa tottumuksina, eikä tämän tutkielman kohteena olevilla säädösten muutoksilla voida suoraan vaikuttaa käyttäjien tottumuksiin, vaikka merkittävät muutokset tunnistuspalveluiden toteuttamistavassa kieltämättä vaikuttavat myös tottumusten kautta.



Kuvio 2 Unified Theory of Acceptance and Use of Technology 2, eli UTAUT2 (Venkatesh, Thong & Xu 2012, s. 160)

[11] Rondan-Cataluña, Arenas-Gaitán & Ramírez-Correa 2015

[12] Halilovic & Cicic 2013

2.3 Aikaisempaa empiiristä tutkimusta sähköisen asioinnin ajureista

Suomessa Pikkarainen ym. on esittänyt Technology Acceptance Modeliin perustuvan mallin verkkopankin käytön tutkimiseen. Mallissa on ajureina koetun hyödyn ja helppokäyttöisyyden lisäksi verkkopankin käytöstä koettu nautinto, saatavilla oleva tieto verkkopankista ja sen käytöstä, tietoturva ja yksityisyys sekä internet-yhteyden nopeus. Internet-yhteyden nopeudella ei ollut tutkimuksen mukaan Suomessa tilastollista merkitystä, kuten ei myöskään iällä tai sukupuolella. Tutkimuksen mukaisesti tärkeimpiä käytön ajureita olivat koettu hyöty sekä saatavilla oleva tieto verkkopankista ja sen käytöstä.[13] Verkkopankista ja sen käytöstä saatavilla olevan tiedon voi kuitenkin katsoa vaikuttavan suoraan palvelun käytöstä koettuun hyötyyn sekä koettuun helppokäyttöisyyteen, joten Pikkaraisen ym. esittämän mallin sijaan voi käyttää TAM-mallia tai uudempaa UTAUT2-mallia.

UTAUT2-mallia on käytetty mm. tutkimuksessa, missä selvitettiin kuinka yli 55-vuotiaat espanjalaiset käyttävät verkkopankkiaan. Tuloksena oli, että hedonistinen motivaatio, sosiaalinen paine ja käyttöolosuhteet eivät olleet tilastollisesti merkittäviä ajureita. Myöskään sukupuoli ei ollut selittävä tekijä. Sen sijaan koettu hyöty ja helppokäyttöisyys, hinta-laatu-suhde ja tottumukset olivat merkittäviä ajureita.[14] Tulos ei yllätä, sillä verkkopankin käytöstä saatava hyöty on lähinnä utilitaristista, kuten laskujen maksamista, eikä siitä oleteta saatavan välitöntä mielihyvää. Toisaalta voidaan myös ajatella, että verkkopankkia käyttämällä voi antaa itsestään nykyaikaisen kuvan ja saada siten hedonistista hyötyä, mutta verkkoasioinnin hyötyjen on todettu olevan ensisijaisesti utilitaristisia myös tällä jaottelulla.[15]

Tilastoista voidaan todeta, että Suomessa 80 % kansalaisista on asioinut viranomaisen kanssa verkossa vuonna 2015 (EU-kansalaisista 46 %) ja 59 % on lähettänyt viranomaiselle lomakkeen verkossa (EU 26 %).[16] Suurimmat syyt sähköisen asioinnin välttämiselle EU:ssa ovat henkilökohtaisen käynnin suosiminen sekä sähköisestä palvelusta huolimatta vaadittu paperilomakkeen tai henkilökohtaisen käynnin vaatimus.[17]

Suomessa keväällä 2001 toteutetussa haastattelututkimuksessa todettiin tärkeimmiksi asiakkaiden kokemiksi hyödyiksi asioinnin vaivattomuus, rahalliset säästöt sekä parantunut palvelun laatu. Samassa tutkimuksessa havaittiin, ettei sukupuoli ole Suomessa-

---

[13] Pikkarainen ym. 2004, s. 226–231

[14] Arenas-Gaitán, Peral-Peral & Ramón-Jerónimo 2015, s. 12, 15

[15] Koski 2002, s. 95–96, 99–100

[16] Eurostat 2016

[17] Euroopan komissio 2014, s. 19

kaan merkittävä tekijä verkkopankin käytössä.[18] UTAUT2-malliin sidottuna merkittävimmiksi ajureiksi osoittautuivat Effort Expectancy, Price Value ja Performance Expectancy.

Taiwanissa veroilmoituksen tekemiseen sähköisesti vaikutti eniten koettu hyöty, luottamus järjestelmään ja yhteensopivuus, sekä luottamus omiin kykyihin.[19] Ylipäänsä helppokäyttöisyys, koettu hyöty, aiemmat tietokoneen käyttökokemukset, luottamus verkkopalveluihin ja koetut riskit on useissa tutkimuksissa nähty suurimmiksi sähköisen viranomaisasioinnin ajureiksi.[20]

Palveluntarjoajien kannalta sähköiset palvelut helpottavat heidän asiakkaidensa asiointia. Ne mahdollistavat palvelun missä ja milloin vain, näin ollen mahdollisesti kasvattaen asiakastyytyväisyyttä tai lisäten asiointikertoja. Sähköisen itsepalvelukanavan käyttäminen henkilökohtaisen asioinnin tai puhelinsoiton sijaan saattaa myös aiheuttaa kustannussäästöjä, joskin tämä näkemys on ainakin Suomen julkishallinnon palveluissa kyseenalaistettu.[21]

Teknisen toimivuuden ohella itsepalvelu edellyttää, että käyttäjä ymmärtää, mistä palvelussa on kysymys.[22] Esimerkiksi muutosverokortin voi nykyisin tilata Verohallinnon internet-sivuston kautta, mutta jos kansalainen ei ymmärrä ennakonpidätyksen käsitettä tai mitä häneltä kysyttävät tiedot, mm. saatava merimiestyötulo, tarkoittavat, voi hän katsoa lopputuloksen olevan niin epävarma, että on hyödyllisempää asioida verovirastossa henkilökohtaisesti, jolloin todennäköisyys saada oikeanlainen muutosverokortti on lähtökohtaisesti hyvä. EU-kansalaisten sähköisestä viranomaisasioinnista suurimpina kokemat hyödyt, ajan säästö, mahdollisuus asioida missä ja milloin vain, rahan säästö ja palvelun saamisen yksinkertaistuminen, yhtenevät TAM- ja UTAUT2-mallien kanssa.[23]

Paperilomakkeella tietoa kerättäessä on tärkeää saada kerralla mahdollisimman paljon tietoa lisätietopyyntöjen viedessä aikaa. Esimerkkinä voidaan käyttää samaa muutosverokorttilomaketta kuin aiemmin. Sähköisellä lomakkeella lisätietoja voitaisiin pyytää lisää riippuen aiemmista valinnoista, jolloin oletuksena näkyvissä voisi olla vaikkapa vain kohta palkkatulolle ja erillinen valinta josta pääsee täyttämään myös muita tulolajeja. Sähköisessä kanavassa palveluiden sisällä on mahdollista tehdä edellä mainitun

---

[18] Villberg 2002, s. 76, 80; Koski & Villberg 2002, s. 71

[19] Hung, Chang & Yu 2006

[20] Lee, Kim & Ahn 2011, s. 223

[21] HE 59/2016, s. 22; VTV 2016, s. 41–42, 37, 48

[22] Koski & Villberg 2002, s. 65–66

[23] Euroopan komissio 2014, s. 20

kaltaisia parannuksia, ja lisää hyötyjä voidaan saada tarjoamalla palveluja asiakaslähtöisesti.[24]

Julkishallinnon tavoitteena on tällainen asiakaslähtöisyys, jossa palvelua tarvitsevan ei tarvitse tietää mikä viranomainen palvelua tarjoaa, ja tämä puolestaan saattaa edellyttää palveluprosessien uudistamista, jopa viranomaisten välisten rajojen yli. Näin julkishallinto pyrkii parantamaan asiakaslähtöisyyttään, turvaamaan palveluiden saatavuuden ja laadun sekä lisäämään omaa tuottavuuttaan.[25] Kansallinen palveluarkkitehtuuriohjelma pyrkii vastaamaan tähän haasteeseen, joskaan senkään hallintamalli ei Valtiontalouden tarkastuslaitoksen mukaan tue asiakaslähtöisyyttä.[26]

Tutkielman tarkoituksena on kuitenkin pohtia lainsäädännön muutoksia ja niiden vaikutusta sähköisen tunnistamisen ja allekirjoituksen käyttämiseen. Lainsäädännöllä ei voida vaikuttaa käyttäjien ikään, sukupuoleen, kokemukseen tai tottumuksiin. Lisäksi yllä on todettu, ettei hedonistinen motivaatio ole merkittävä tekijä tunnistamista vaativien palveluiden käytössä.

Lainsäädännöllä voidaan sen sijaan vaikuttaa odotettuun hyötyyn ja vaivaan sekä käyttöolosuhteisiin, joskaan käyttöolosuhteiden merkitys ei ole ollut tilastollisesti merkittävä. Lainsäädännöllä on myös suora vaikutus viranomaisasioinnin hinnoitteluun sekä tunnistetun käyttäjän tietojen siirtämiseen luottamusverkostossa. Lisäksi erilaiset vastuuseen ja valvontaan liittyvät säännökset vaikuttavat hinnoitteluun välillisesti. Näin ollen erityisen kiinnostavat UTAUT2-mallin osa-alueet ovat odotettu hyöty, odotettu vaiva ja vastine rahalle. Myöhemmin kuvattujen sähköisen tunnistamisen ja allekirjoittamisen sääntelyn muutosten mahdollisia vaikutuksia pyritään löytämään käyttämällä apuna edellä kuvattuja ajureita.

---

[24] vrt. Gilbert, Balestrini & Littleboy 2004, s. 298

[25] Valtioneuvoston kanslia 2005, s. 26–29.

[26] VTV 2016, s. 49–51

3 SÄHKÖISEN TUNNISTAMISEN JA ALLEKIRJOITTAMISEN NYKYTILA SUOMESSA

3.1 Sähköinen tunnistaminen

Sähköisen tunnistamisen avulla pyritään tunnistamaan jotakin sähköistä palvelua käyttävä henkilö. Kuten jo aiemmin on todettu, koostuu tämä tunnistaminen käyttäjäidentiteetin luotettavuudesta ja käyttäjäidentiteetin todentamisen luotettavuudesta. Joskus tunnistamiseen riittää jokin käyttäjän kannalta näkymätön tunniste, kuten internet-selaimen eväste. Palveluntarjoaja asettaa evästeen, kun käyttäjä ensimmäisen kerran vierailee sivustolla. Kun samalla internet-selaimella käydään sivustolla uudelleen, lukee palveluntarjoaja evästeen, jonka perusteella voi kohtalaisella varmuudella sanoa käyttäjän olevan sama henkilö, tai ainakin joku henkilö samalla tietokoneella.

Käyttäjä on myös mahdollista tunnistaa esim. IP-osoitteen[27] perusteella tietystä käyttöpaikasta tulevaksi. Useilla yrityksillä on kiinteä IP-osoite, jolloin palvelun käytön mahdollistajaksi tai tunnistamisen osatekijäksi voi asettaa vaatimuksen tietystä IP-osoitteesta. Tällöin on todennettu, että käyttäjä pystyy ainakin käyttämään yrityksen tietoverkkoa. Välillä vaaditaan kuitenkin toimenpiteitä myös itse käyttäjältä, esimerkiksi käyttäjätunnuksen ja salasanan syöttämistä.

Huomioitavaa kuitenkin on, että näitä edellä mainittuja heikon tunnistamisen menetelmiä ei juurikaan säännellä lailla. Henkilötietolaki asettaa tiettyjä rajoitteita ja evästeiden asettamisessa on huomioitava tietoyhteiskuntakaaren 205 §, mutta oikeusvaikutukset ovat sopimuspohjaisia.

Vahvaa sähköistä tunnistamista säännellään lailla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Lakia ei kuitenkaan sovelleta, jos tunnistuspalvelua käytetään vain yhteisön sisäisiin tarkoituksiin tai jos tunnistusmenetelmää tarjotaan asiakkaille tunnistamisvälineeksi ainoastaan yhteisön omissa palveluissa. (Tunnistuslaki 1 §).

OECD on julkaissut sähköisestä tunnistamisesta ohjeistusta vuonna 2007. Tarkoituksena on tarjota suuntaviivoja valtioiden rajat ylittävän vahvan sähköisen tunnistamisen mahdollistamiseksi, joten dokumentti on hyvin yleisluontoinen. Kuitenkin se tarjoaa pohjan asioista, jotka on vähintään otettava huomioon lainsäädäntöprosessissa ja sillä saattaa olla käytännön merkitystä arvioitaessa osapuolten huolellisuutta ja asianmukaisuutta vaikkei suositus olekaan muodollisesti sitova. EU:ssa on vuonna 2014 säädetty

[27] Internetin protokollaosoitte on jonkin käyttöpaikan yksilöivä numerosarja, jonka avulla internet-liikenne ohjataan halutulle tietokoneelle.

ns. eIDAS-asetus, joka koskee jäsenvaltioiden rajat ylittäviin transaktioihin ilmoittamia vahvan sähköisen tunnistamisen menetelmiä. Asetus mukailee suurelta osin OECD:n ohjeistusta.

Sähköiset tunnistamismenetelmät voidaankin siis jaotella kolmeen kategoriaan: vahvoihin menetelmiin, jotka on ilmoitettu EU:n jäsenvaltioiden rajat ylittävään tunnistamiseen; vahvoihin menetelmiin, jotka perustuvat kansalliseen lainsäädäntöön; sekä muihin menetelmiin. Kuten on jo todettu, muita menetelmiä ei erikseen säännellä eikä niiden tarkastelu ole tässä kiinnostavaa. EIDAS-asetukseen ja sen vaikutuksiin palataan myöhemmin tässä tutkielmassa, mutta tässä vaiheessa todettakoon, että rajat ylittävään tunnistamiseen ilmoitettuja tunnistusvälineitäkin säädellään aina jonkin jäsenvaltion kansallisella lailla.

Viranomaisten kanssa asioitaessa tulee sovellettavaksi myös hallintolaki sekä laki sähköisestä asioinnista viranomaistoiminnassa (asiointilaki). Ensinnäkin viranomaisen on järjestettävä palvelunsa niin, että hallinnossa asioiva saa palveluita asianmukaisesti ja viranomainen voi suorittaa tehtävänsä tuloksellisesti (hallintolaki 7 §). Lähtökohtaisesti asian vireillepano vaatii viranomaiselle toimitetun asiakirjan, mutta asiakirjaa ei tarvitse allekirjoittaa (hallintolaki 16 §), ellei jossain erityislaissa määrätä tällaista muotovaatimusta. Esimerkiksi kiinteistön kauppakirja on tehtävä kirjallisesti ja sekä myyjän että ostajan on allekirjoitettava se. Kiinteistön kauppa voidaan tehdä myös sähköisesti Maanmittauslaitoksen ylläpitämässä kaupankäyntijärjestelmässä (maakaari 2:1, 5:3).

Viranomaisasiat tulisi pääsääntöisesti pystyä panemaan asioita vireille ilman vahvaa sähköistä tunnistamista. Käytännössä asiointipalvelussa on kuitenkin usein nähtävillä salassa pidettävää tietoa, jota voidaan käyttää avuksi lomakkeen täyttämisessä. Esimerkiksi Verohallinnon asiointipalvelusta on mahdollista tilata itselleen uusi verokortti siten, että edellisen veroilmoituksen tiedot ovat jo valmiiksi täytettynä palvelussa. Tämä parantaa palvelun käyttömukavuutta ja vähentänee virheitä, mutta edellyttää vahvaa sähköistä tunnistamista. Henkilöt, joilla ei ole tunnistusvälineitä, eivät voi kyseisiä palveluita käyttää, vaan joutuvat asioimaan viranomaisen puhelinpalvelussa tai fyysisessä virastossa taikka täyttämään, tulostamaan ja postittamaan paperisen hakemuksen.

3.2 Sähköinen allekirjoitus

Kun sähköisessä tunnistamisessa nimensä mukaisesti vain tunnistetaan käyttäjä, liittyy sähköinen allekirjoitus aina johonkin muuhun tietoon. Tällä tiedon ja sähköisen allekirjoituksen yhdistelmällä voidaan tehdä tahdonilmaisu, joka johtaa oikeustoimeen. Sähköinen allekirjoitus muodostetaan *luomisvälineellä* ja *luomistiedoilla*, joista luomisväline on ohjelmistojen ja laitteiden kokonaisuus, ja luomistiedot puolestaan sisältävät ainutkertaisen tietokokonaisuuden, jota allekirjoituksen luomisessa käytetään. Esimerkik-

si kansalaisvarmenne on luomistieto. Henkilökortin, kortinlukijan, lukijaohjelmiston ja tietokoneen muodostama kokonaisuus luomisväline.[28]

Käytännössä sama väline, kuten pankkitunnukset, voi olla sekä tunnistusväline että allekirjoituksen luomisväline. Erona on, että tunnistusvälinettä käytetään vain tunnistamiseen, kun taas sähköinen allekirjoitus liittyy aina johonkin muuhun tietosisältöön. Tämä ei kuitenkaan estä oikeustoimien tekemistä tunnistusvälineen avulla, mutta silloin palveluntarjoajan tietojärjestelmän on pystyttävä osoittamaan, että oikeustoimi on tunnistautuneen käyttäjän tekemä ja tieto on säilynyt muuttumattomana.[29]

Tiedon muuttumattomuuden todistaminen on suoraviivaista, mikäli asiakirja on allekirjoitettu *kehittyneellä sähköisellä allekirjoituksella*. Kehittyneen sähköisen allekirjoituksen tulee nimittäin liittyä allekirjoitettuun tietoon siten, että muutokset on mahdollista havaita. Lisäksi kehittyneen sähköisen allekirjoituksen tulee yksilöidä ja yksiselitteisesti liittyä allekirjoittajaan sekä olla luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan.[30]

Sähköisiä allekirjoituksia käsitellessä on otettava huomioon, että eIDAS-asetus sääntelee niitä suoraan 1.7.2016 alkaen. Käytännön tasolla moni asia ei kuitenkaan muutu, sillä vastuukysymykset ratkaistaan edelleen kansallisen lainsäädännön mukaisesti ja liikenne- ja viestintäministeriö on valmistelemassa tunnistuslain muutosta, jolla otetaan huomioon eIDAS-asetuksen soveltamisen aloittamisen vaikutukset.[31]

Kuten aiemmin on todettu, ei viranomaisasian vireillepano lähtökohtaisesti vaadi vireillepanoasiakirjan allekirjoittamista. Viranomainen voi kuitenkin kehottaa lähettäjää täydentämään asiakirjan allekirjoituksella, mikäli sillä on peruste epäillä asiakirjan alkuperäisyyttä tai eheyttä (hallintolaki 22 §; asiointilaki 9 §). Jos allekirjoitus vaaditaan, joko viranomaisen kehotuksesta tai mikäli asian käsittelyyn liittyy tällainen muotovaatimus, kelpaa allekirjoitukseksi myös sähköinen allekirjoitus (asiointilaki 9 §). Näin ollen esillä olleen kiinteistön kaupan esimerkissä kauppakirjan voisi laatia myös vapaamuotoisena dokumenttina, jonka myyjä ja ostaja allekirjoittavat kehittyneellä sähköisellä allekirjoituksella. Sähköisessä kaupankäyntijärjestelmässä tehtävään kauppaan verrattuna erona kuitenkin on, että tällöin kaupanvahvistajan on vahvistettava kauppa kaikkien allekirjoittajien läsnä ollessa (maakaari 2:1). Sähköisestä allekirjoituksesta saatavat hyödyt, lähinnä ajasta ja paikasta riippumattomuus, pienenisivät huomattavasti.

Viranomaiselle avoimella sähköpostitse toimitettavien, allekirjoittamattomien asiakirjojen alkuperäisyyttä tulee epäillä. Yleisesti sähköpostien välityksessä käytettävä

---

[28] Tunnistuslaki 2 §

[29] Ponka 2013, ss. 270–271

[30] Tunnistuslaki 2 §

[31] Lisää eIDAS-asetuksesta ks. luku 5 ja tulevasta tunnistuslain muutoksesta ks. luku 6.3

SMTP[32]-protokolla ei tue lähettäjän tarkastamista, joten normaalisti sähköpostin lähettäjän osoitteesta ei voi olla varma. Toisaalta on huomioitava, ettei myöskään kirjeen lähettäjästä saada tietoa, joten pelkästään sähköpostin käyttämisen ei pitäisi olla riittävä peruste vaatia asiakirjan täydentämistä allekirjoituksella.

Eduskunnan apulaisoikeusasiamies Maija Sakslin on päätynyt samaan lopputulokseen ratkaisussaan Dnro 3666/4/10. Tapaus koski maistraattien käytäntöjä evankelisluterilaisesta kirkosta eroamisesta annettujen sähköisten vireillepanoasiakirjojen käsittelyssä. Apulaisoikeusasiamiehen tulkinnan mukaan viestin lähettäminen toisen henkilön sähköpostista tai sähköpostiosoitteesta, jossa ei ole lähettäjän nimeä, ei voi olla säännönmukainen peruste epäillä alkuperäisyyttä.[33]

3.3 Käytössä olevat järjestelmät

3.3.1 Turvallinen pankkitunnistaminen Tupas

Finanssialan keskusliitto ylläpitää useimpien pankkien tunnistamispalveluiden tarjoamiseen käyttämää turvallisen pankkitunnistamisen Tupas-standardia. Tämä antaa tunnistamista tarvitsevalle palveluntarjoajalle mahdollisuuden toteuttaa yksi tekninen ratkaisu, jota voi pienin muutoksin käyttää useiden pankkien tunnistamispalveluiden kanssa.

Tupas-palvelua käytetään yleisesti sähköiseen tunnistamiseen sekä sähköiseen allekirjoittamiseen. Tunnistamisessa palveluntarjoaja voi pyytää pankilta tunnistautuvan henkilön tietoja selväkielisenä tai salattuna, joista jälkimmäinen mahdollistaa ennalta annettujen tietojen, kuten henkilötunnuksen, oikeellisuuden varmistamisen. Palvelua voi käyttää myös yritysten pankkitunnuksilla, jolloin voidaan vahvasti tunnistaa palvelua käyttävä oikeushenkilö.[34]

Tupas-tunnistamisen etuna voidaan pitää sen levinneisyyttä, sillä se on selvästi yleisin sähköisen tunnistamisen keino. Jopa 94 % 18–54-vuotiaista ja 90 % kaikista Finanssialan keskusliiton haastatteluun vastanneista 15–74-vuotiaista käyttää verkkomaksamista maksutapana verkkopankissa, jonne kirjaudutaan samoilla tunnistusvälineillä kuin mitä Tupas-tunnistamisessa käytetään.[35] Käyttöä kuitenkin vaikeuttaa se, että palveluntarjoajan on tehtävä sopimus jokaisen pankin kanssa erikseen. Tämä on ensisijaisesti

---

[32] Simple Mail Transfer Protocol

[33] AOA 3666/4/10, s. 8

[34] Finanssialan keskusliitto 2013a, s. 4; Finanssialan keskusliitto 2013b, s. 4–5

[35] Finanssialan keskusliitto 2015, s. 6, 44

kustannuskysymys pankkien periessä tunnistuspalvelusta kuukausimaksua transaktiokohtaisen maksun lisäksi.

Myös tunnistuspalvelun tarjoajia on selvästi eniten pankkisektorilla: 74:stä rekisteröidystä tunnistamispalvelun tarjoajasta 70 on pankkeja, lisäksi palvelua tarjoaa 3 teleoperaattoria sekä Väestörekisterikeskus. 70 pankista tosin 36 kuuluu POP-pankkeihin ja 25 paikallissäästöpankkeihin, mutta pankkiala pysyy suurimpana tunnistamista tarjoavana sektorina vaikka kummankin edellä mainituista pankkiryhmistä laskisi vain yhtenä.[36] Laatuvarmenteita sähköiseen allekirjoittamiseen tarjoaa Suomessa ainoastaan Väestörekisterikeskus.[37]

3.3.2 Mobiilivarmenne

Mobiilivarmenne on tunnistuspalvelu, jossa käytetään hyväksi matkapuhelimen SIM-kortin hallussapitoa. Mobiilivarmenteita myöntää kolme teleoperaattoria, TeliaSonera Finland Oyj, Elisa Oyj ja DNA Oy. Nämä operaattorit muodostavat keskenään luottamusverkoston, joten tunnistusta tarvitsevan palvelun ylläpitäjälle riittää sopimuksen tekeminen yhden tunnistuspalvelun tarjoajan kanssa. Mobiilivarmenteen käyttämiseen oikeuttavan sopimuksen solmimisen jälkeen kaikkien kolmen operaattorin myöntämillä varmenteilla voi tunnistautua palveluun toisin kuin Tupas-tunnistamisessa, missä sopimus täytyy tehdä jokaisen tunnistuspalvelun tarjoajan kanssa erikseen.[38]

Mobiilivarmenteella hyödynnetään sähköistä asiointitunnusta, joka on Väestörekisterikeskuksen antama luonnollisen henkilön yksilöivä tieto, kuten henkilötunnus, mutta siitä ei voi päätellä henkilön sukupuolta tai syntymäaikaa.[39] Tunnistuspalvelun tarjoaja ylläpitää internet-yhteydellä käytettävää portaalia, jonne tunnistettava käyttäjä ohjataan. Käyttäjä antaa selaimessa puhelinnumeronsa, jonka jälkeen hän kirjoittaa SIM-kortille tallennetun varmenteen käyttöön edellytetyn tunnusluvun puhelimeensa. Tunnistuksen tapahduttua pyydetty tieto käyttäjän identiteetistä siirretään palveluntarjoajalle, jonka palveluun myös käyttäjän selainistunto palautetaan.

Kansanedustaja Ritva Elomaa on 4.5.2016 jättänyt kirjallisen kysymyksen mobiilitunnistautumisesta viranomaispalveluihin prepaid-liittymällä. Edustaja Elomaan mielestä hallituksen tulisi edistää prepaid-liittymän omistajien mahdollisuuksia käyttää mobii-

---

[36] Viestintävirasto 2015

[37] Viestintävirasto 2014

[38] Sonera 2016

[39] FiCom 2011, s. 32

livarmennetta, perusteluna, ettei maksuhäiriömerkinnän saanut henkilö välttämättä saa henkilökohtaista matkapuhelinliittymää, vaan joutuu turvautumaan prepaid-liittymään.[40]

Hallitus ei ole vielä vastannut kysymykseen, mutta vastaus voisi perustua siihen, että henkilökortti ja siihen sisältyvä kansalaisvarmenne myönnetään samoin perustein kaikille, riippumatta luottotietomerkinnöistä. Henkilökortin avulla voi kirjautua lähes kaikkiin viranomaispalveluihin. Lisäksi olisi perin omituista, että hallitus puuttuisi yhteen tekniseen tunnistamismenetelmään, kun tarkoitus on avata sähköisen tunnistamisen markkinat kilpailulle. Edustaja Elomaa toteaa kysymyksensä perusteluissa, ettei monilla kansalaisilla ole henkilökohtaista sopimusta matkapuhelinliittymästä, ja heidänkin pitäisi saada mobiilivarmenne käyttöönsä. Käytännössä Elomaan ehdotus tarkoittaisi ei-henkilökohtaisen välineen käyttämistä tunnistusvälineenä, tai henkilökohtaisen matkapuhelinliittymän säätämistä perusoikeudeksi.

3.3.3 Henkilökortti

Henkilökortti on poliisin Suomen kansalaiselle tai Suomessa vakinaisesti asuvalle ulkomaalaiselle henkilökorttilain (829/1999) perusteella myöntämä todistus henkilöllisyydestä. Henkilökortin tekniseen osaan on sisällytetty Väestörekisterikeskuksen myöntämä kansalaisvarmenne, jonka avulla henkilö voidaan todentaa sähköisessä asioinnissa, ja jolla voidaan allekirjoittaa tai salata asiakirjoja. Suomen kansalaiset, joilla on henkilökortti mukana, voivat matkustaa koko Schengen-alueella sekä eräisiin muihin maihin ilman passia.[41] Alaikäiselle ilman huoltajien suostumusta annettava henkilökortti ei kuitenkaan kelpaa matkustusasiakirjana eikä sitä voi käyttää sähköiseen asiointiin.

Henkilökortin sähköinen osa onkin siis vahva sähköinen tunnistusväline sekä laatuvarmenne, jota voidaan käyttää kehittyneen sähköisen allekirjoituksen muodostamiseen. Väestörekisterikeskus, joka kansalaisvarmenteen myöntää, on ainoa Viestintävirastolle ilmoituksen tehnyt laatuvarmenteiden tarjoaja.[42]

Henkilökortilla olevan sähköisen varmenteen käyttö edellyttää kortinlukijalaitetta sekä -ohjelmistoa. Ohjelmiston saa ladattua ilmaiseksi Väestörekisterikeskuksen internetsivustolta Windows, Mac OS ja Linux-käyttöjärjestelmille. Tietokoneen USB-väylään kytkettävän lukijalaitteen puolestaan joutuu ostamaan itse. Itse kortilla on kaksi erillistä

---

[40] KK 262/2016 vp

[41] Valtioneuvoston asetus matkustusoikeuden osoittamisesta eräissä tapauksissa (1244/2006). Huomioitavaa on, että asetus ei koske pohjoismaita, joiden välillä matkustusoikeus ilman passia syntyy SopS 17/1954 perusteella.

[42] Viestintävirasto 2014

varmennetta – allekirjoitus- sekä todentamis- ja salausvarmenne – joita käytetään erillisillä tunnusluvuilla.

Yksi viranomaisen myöntämän tunnistusvälineen hyviä puolia on, että se myönnetään samoin perustein kaikille kansalaisille ja Suomessa vakinaisesti asuville ulkomaalaisille. Yksityisillä yrityksillä, kuten pankeilla, ei ole velvollisuutta myöntää tunnistusvälineitä kenellekään, vaan ne saavat itse määritellä kriteerit, jotka vaaditaan tunnistusvälineen myöntämiseen. Näin ollen henkilökortti voi käytännössä olla ainoa vahvan sähköisen tunnistamisen menetelmä, jonka maksuhäiriömerkinnän saanut henkilö voi saada, sillä vaikka jokaisella on oikeus tavanomaiseen talletustiliin ja tilin käyttöön tarkoitettuun välineeseen, eivät verkkopankkitunnukset kuulu näihin luottolaitoslain 15:6:n mukaisiin peruspankkipalveluihin.

Kansanedustaja Ritva Elomaa on jättänyt asiaa sivuavan kirjallisen kysymyksen vuonna 2013. Hän kysyy, *miten hallitus aikoo kehittää sähköisen tunnistautumisen menetelmiä lähitulevaisuudessa ja millä menettelyillä kaikille tarkoitettujen julkisten peruspalvelujen käytön ja kansalaisoikeuksien tasapuolinen toteutumien mahdollistetaan tästä näkökulmasta.* Hallinto- ja kuntaministeri Henna Virkkusen vastauksesta voidaan lukea, että kaikkia julkisia peruspalveluita voi käyttää henkilökortilla, jolloin pankkien kieltäytyminen verkkopankkitunnusten tarjoamisesta ei ole oikeus kansalaisoikeuksien näkökulmasta. Sähköisen tunnistautumisen menetelmien kehittämisen osalta ministeri Virkkunen mainitsee kansallisen palveluarkkitehtuuriprojektin (KaPa) ja toteaa, että valtion roolin kasvattamista selvitetään.[43]

Sinänsä ministeri Virkkusen vastaus on järkevä, mutta kaikkiin viranomaispalveluihin ei ole mahdollista kirjautua sähköisellä henkilökortilla. Ihmetystä herättää esimerkiksi Liikenteen turvallisuusvirasto Trafin Oma asiointi -palvelu, jonne kirjaudutaan Vetuma-portaalin kautta. Kuten myöhemmin selvitetään, on jokaisen Vetuma-tunnistamista hyödyntävän palveluntarjoajan tehtävä sopimus erikseen jokaisen tunnistuspalvelun tarjoajan kanssa. Trafin palveluun on mahdollista kirjautua kymmenen eri pankin tai pankkiryhmän verkkopankkitunnuksilla sekä mobiilivarmenteella. Mielenkiintoista on, että valtion toisen viranomaisen tarjoamaa tunnistuspalvelua, henkilökorttia, ei voi käyttää tunnistautumiseen.[44]

---

[43] KK 358/2013 vp

[44] Tilanne 14.5.2016

3.4 Vastuun jakautuminen kansallisessa lainsäädännössä

3.4.1 Vastuun jakautumisesta yleisesti

Sopimusvapaus on lähtökohta kaikessa taloudellisessa toiminnassa, niin myös sähköisten tunnistus- ja allekirjoituspalveluiden tarjoamisessa. Tunnistuslaki tietysti asettaa tiettyjä edellytyksiä lähinnä tunnistuspalveluiden tarjoajille, ja mikäli niitä edellytyksiä ei täytä, ei koko lakia myöskään sovelleta. Tällaisia ovat mm. 9 § vaatimukset tunnistuspalvelun tarjoajan luotettavuudesta. Mitä seuraavaksi todetaan tunnistuspalveluiden tarjoajista, sovelletaan myös laatuvarmenteita tarjoaviin tahoihin, sillä varmenteella voidaan aina todentaa henkilöllisyys (tunnistuslaki 2 §).

Heikomman suoja on toinen periaate, joka näkyy tunnistuslain 3 §:ssä: tunnistuslain vaatimuksista ei voi sopimuksella poiketa kuluttajan vahingoksi. Vahva kuluttajansuoja helpottaa tunnistuspalvelun tarjoajien vertailua ja takaa tietyt vähimmäisoikeudet kiistatilanteissa. Kuluttajansuoja ei ulotu yrityksille tarjottaviin palveluihin, joten tunnistamista vaativien palveluiden tarjoajien ja tunnistuspalveluntarjoajien välisiin sopimuksiin voidaan sisällyttää laista huomattavastikin poikkeavia ehtoja ja vastuunrajoituksia.

Osapuolten väliset oikeudet ja velvollisuudet määritellään lähtökohtaisesti kahdenvälisillä sopimuksilla. Tällaisia sopimuksen tekeviä pareja ovat tunnistusvälineen haltija ja tunnistuspalvelun tarjoaja, tunnistusvälineen haltija ja asiointipalvelun tarjoaja sekä tunnistuspalvelun tarjoaja ja asiointipalvelun tarjoaja. Yleisesti tunnistuspalvelun tarjoaja myöntää tunnistusvälineen sen hakijalle maksua vastaan ja toisaalta välittää tunnistetietoja palveluntarjoajalle myöskin maksua vastaan. Tunnistetietojen välittämisen jälkeen tunnistusvälineen haltija ja palveluntarjoaja voivat tehdä sopimuksia, joissa tunnistuspalvelun tarjoaja ei ole osallisena.

Mikäli jollekin osapuolelle aiheutuisi vahinkoa sopimuksen rikkomisesta, tulee tarkastella sekä sopimusehtoja, tunnistuslakia että vahingonkorvauslakia mahdollisen korvausvelvollisuuden määrittämiseksi. Vahingonkorvauslain lähtökohta on, että tahallisesti tai tuottamuksellisesti aiheutettu vahinko tulee korvata (2:1), muut vahingot jäävät kärsijän vahingoksi.

Vahingonkorvauslain mukaista korvausta määriteltäessä on huomioitava, että puhtaista varallisuusoikeudellisista vahingoista ei voi saada korvausta, ellei tekoa ole aiheutettu rangaistavaksi säädetyllä teolla tai julkista valtaa käytettäessä, tai jollei ole muita erittäin painavia syitä (vahingonkorvauslaki 5:1). Sähköisen tunnistamisen kohdalla tämä lienee yleisin tapahtuma, sillä on kovin vaikea nähdä suoraa syy-yhteyttä tunnistamisen ja henkilövahingon välillä. Vahinkolajiluokittelun mukainen esinevahinko voi kuitenkin syntyä mikäli henkilö saa virheellisen tunnistamisen seurauksena käyttöönsä

esineen, joka vaurioituu tai jonka käyttäminen aiheuttaa sen omistajalle liikevoiton menetystä.[45]

Korvausperusteen lisäksi vahingonkorvauslain mukaisen korvauksen saamiseen tarvitaan lisäksi todennettavissa oleva syy-yhteys sekä selvitys aiheutuneen tappion määrästä. Myös vahingon kärsineen oma myötävaikutus vahinkoon voi alentaa korvauksen määrää.[46]

3.4.2 Tunnistamista vaativan palvelun tarjoajan vastuut

Palveluntarjoajan, joka edellyttää vahvaa tunnistamista osana jotain palveluaan, on täytettävä tietyt ehdot. Tällaisessa palvelussa käsitellään henkilötietoja, ja palveluntarjoajan on noudatettava henkilötietolain vaatimuksia. Henkilötietolain lähtökohtana on, että henkilötietojen käsittelyyn tarvitaan asiallinen syy, kuten asiakas- tai työsuhde, tai rekisteröidyn henkilön lupa. Lisäksi henkilötunnuksen käsittelyyn tarvitaan kyseisen henkilön lupa, jollei kysymyksessä ole rahoitusta, vakuutuksia, vuokrausta, terveydenhuoltoa tai työsuhteita tms. koskeva rekisteri. Palveluntarjoajan on laadittava rekisteristä rekisteriseloste, joka tulee tietyissä tilanteissa lähettää tietosuojavaltuutetulle.[47]

Henkilötietolaki ei siis estä henkilötunnuksen käsittelyä, sillä lupa sen käsittelyyn voidaan nimenomaisesti pyytää ennen tunnistustapahtuman aloittamista. Toisaalta laki ohjaa siihen, ettei henkilötunnusta tallennettaisi tarpeettomasti, vaan pyrittäisiin vahvan tunnistamisen kautta saamaan varmuus vaikkapa luonnollisen henkilön nimestä, jos se on riittävä tieto tarjottavan palvelun kannalta.[48]

Henkilörekisterin pitäjän on varmistuttava riittävästä tietoturvasta, niin teknisesti kuin organisaatiossaan. Riittävän tietoturvan määrittely on luonnollisesti hankalaa, mutta ainakin on määriteltävä tietojen käyttöoikeudet ja suojattava järjestelmä salasanoilla, sekä tarpeen mukaan tallennettava tietojen katselu- ja muutoshistoria. Luvattomien käyttöyritysten on hallituksen esityksen mukaan aiheutettava välitön hälytys rekisterinpitäjälle, mikä nykyisellään kuulostaa melko raskaalta vaatimukselta.[49]

Sopimusoikeudellisten velvoitteiden osalta Danske Bankin, Osuuspankin ja Nordean yleisiin Tupas-sopimuksiin on kirjattu kielto luoda uusia käyttäjätunnuksia tai tunnistautumistietoja ilman pankkien nimenomaista suostumusta, ja sitoumus maksaa pankille se

---

[45] vrt. Ståhlberg & Karhu 2013, s. 290–291

[46] Ståhlberg & Karhu 2013, s. 11–13

[47] HenkilötietoL 8, 10, 13, 36 §

[48] HenkilötietoL 9 §

[49] HenkilötietoL 32 §; HE 96/1998 vp, s. 66

summa jonka pankki on mahdollisesti velvollinen maksamaan palveluntarjoajan tuotteen tai palvelun virheen seurauksena. Sopimukset ovat hyvin samankaltaisia ja niiden sisältö liittyy lähinnä tunnistuspalvelun tekniseen ylläpitoon ja pankkien vastuunrajoituksiin.[50] Kielto luoda uusia tunnuksia näyttäisi olevan puhtaasti liiketaloudellinen, sillä pankkien tunnistuspalveluiden hinnoittelu perustuu kirjautumiskertoihin, joita erillisten tunnusten luominen käytettävään järjestelmään luonnollisesti pienentäisi. Lain tasolla ei rajoiteta, mitä tunnistamisen jälkeen on mahdollista tehdä. Selvästi omien tunnusten luomisesta voi myös sopia toisin, sillä esimerkiksi Turun yliopiston käyttäjätunnukseen liitetyn salasanan (toisin sanoen heikon tunnistamisen menetelmän) voi käydä nollaamassa itsepalveluna[51] vahvan sähköisen tunnistamisen turvin.

3.4.3 Tunnistuspalvelun tarjoajan vastuu

3.4.3.1 Ensitunnistaminen

Jotta Tupas-tunnistamista voidaan käyttää, on tunnistautuvalle henkilölle ensin luotava pankkitunnukset. Sama tilanne on tietysti muidenkin tunnistamiskeinojen kohdalla – tunnistamisväline on luotava ensin. Kun luodaan vahvaan sähköiseen tunnistamiseen kelpaava tunniste, on asiakkaalle tehtävä ns. ensitunnistaminen.

Ensitunnistamisessa tunnistuspalvelun tarjoajan on ennen tunnusten luovuttamista varmistettava hakijan henkilöllisyys virallisesta henkilötodistuksesta tai ajokortista. Tällaisen tunnistamisen on tapahduttava henkilökohtaisesti. Vaihtoehtoisesti hakija voi tunnistautua jollain toisella vahvan tunnistamisen välineellä, mikäli tunnistuspalveluiden tarjoajat ovat niin keskenään sopineet. Näin pankkitunnuksia voisi periaatteessa hakea sähköisesti väestörekisterikeskuksen myöntämällä varmennekortilla tai toisen pankin myöntämillä pankkitunnuksilla. Tällöin tunnistuspalveluiden tarjoajien on keskenään sovittava, miten vastuu virheellisestä tunnistamisesta jakautuu. Vahingon kärsineeseen päin vahingosta vastaa kuitenkin kulloinkin käytetyn tunnistamispalvelun tarjoaja. (Tunnistuslaki 17 §)

> *Esimerkki*: A on saanut haltuunsa B:n sähköisen tunnistamisvälineen, jonka K oyj on myöntänyt. K oyj ja P oyj ovat tehneet sopimuksen toistensa tunnistamiseen luottamisesta. A hakee P oyj:ltä sähköistä tunnistamisvälinettä tunnistautuen B:n välineellä, jonka K oyj on myöntänyt. Tämän jälkeen A kirjautuu

[50] Danske Bank 2012, Nordea 2015b, OP 2013

[51] https://idm.utu.fi, tilanne 13.5.2016

P oyj:n myöntämällä tunnistamisvälineellä X oy:n palveluun, jossa tekee oikeustoimia.

P oyj on vastuussa X oy:lle väärästä tunnistamisesta aiheutuneesta vahingosta. P oyj:n ja K oyj:n välinen vastuu määräytyy heidän tekemänsä sopimuksen perusteella.

Pankkitoiminnassa pankilla on joka tapauksessa velvollisuus tuntea asiakkaansa luottolaitoslain sekä rahanpesulain nojalla. Rahanpesulaissa (18 §) asetetaan vaatimus asiakkaan tuntemisesta, mutta samalla mahdollistetaan myös etätunnistaminen esimerkiksi dokumenttien perusteella. Käytännössä ero on tullut huomioida lähinnä yritysten edustajien kohdalla, joille ei saanut luoda uutta sähköistä tunnistamisvälinettä ellei edustaja käynyt henkilökohtaisesti pankissa tunnistautumassa tai tunnistautunut jonkin muun tunnistamispalvelun tarjoajan vahvan tunnistamisen menetelmällä.

1.1.2016 alkaen ensitunnistamisen henkilökohtaisuutta ei kuitenkaan enää vaadita, vaan sähköistä tunnistamisvälinettä on voitava hakea toisella vastaavan tasoisella sähköisellä tunnistamisvälineellä. Sopimusta toistensa tunnistamiseen luottamisesta ei siis enää tarvita, muuten tilanne ei juurikaan muutu. Jos tunnistamisvälineen hakija tunnistetaan virheellisesti, on tunnistamisvälineen myöntäjä edelleen vastuussa vahingon kärsineisiin nähden ja tunnistuspalvelun tarjoajien välinen vastuu mahdollisessa virheellisessä tunnistamisessa määräytyy kuten missä tahansa muussakin tunnistamistapahtumassa, elleivät osapuolet ole nimenomaisesti toisin sopineet. (Tunnistuslaki 17 §).

Muutos helpottaa tunnistusvälineiden hakemista ja poistaa osaltaan esteitä niiden käyttämiseen. Toisaalta identiteettivarkaus muuttuu huomattavasti vakavammaksi, jos vääriin käsiin joutuneilla tunnuksilla voidaan luoda lisää tunnuksia, joista alkuperäisen tunnistusvälineen oikeutettu haltija ei tiedä eikä niitä osaa sulkea. Uusien palvelujen avaaminen varastetulla identiteetillä kasvattaa uhriksi joutuneen työtä ja kustannuksia huomattavasti. Myös tunnistuspalvelun tarjoajat voivat kärsiä tappioita.[52] Tunnistuspalveluiden tarjoajien olisikin syytä kiinnittää hakijoiden huomio niihin vaaroihin, joita on vahvan sähköisen tunnistusvälineen joutuessa vääriin käsiin, verraten esimerkiksi luottokorttiin, jolla voi vain tehdä maksuja, ei avata uusia tunnistamisvälineitä joilla voi taas tehdä uusia toimia. Hallituksen esityksessä (272/2014) ei kuitenkaan oteta kantaa identiteettivarkauksiin muuten kuin laitteiden tietoturvan kannalta.

Laatuvarmenteen hakija on kuitenkin edelleen tunnistettava henkilökohtaisesti (tunnistuslaki 35 §). Näin ollen kehittyneiden sähköisten allekirjoitusten tekemiseen käytettävän laatuvarmenteen sisältävää henkilökorttia haettaessa on edelleen vierailtava poliisin lupapalvelupisteessä. Lisäksi henkilökorttihakemus on jo henkilökorttilain 6 § perusteella jätettävä henkilökohtaisesti poliisilaitokselle.

---

[52] Anderson, Durbin & Salinger 2008, ss. 176–180

Vuoden 2016 alusta alkaen vahvan sähköisen tunnistusvälineen hakijalla on oltava henkilötunnus ja hakijan tiedot on tarkistettava väestötietojärjestelmästä. Lainsäätäjän tarkoituksena on ollut varmistaa yksiselitteinen yhteys luonnollisen henkilön ja tunnistusvälineen välille, minkä ratkaisu kyllä varmistaa. Ulkomailla asuville ulkomaan kansalaisille tämä aiheuttaa vaivaa, sillä heitä ei Suomen väestötietojärjestelmään merkitä. Käytännössä mahdollinen ongelma tuskin koskee suurta ihmisryhmää, mutta ei edesauta vapaata liikkuvuutta. Useat valtiot kuitenkin pitävät tälläkin hetkellä paikallista henkilötunnusta vahvan sähköisen tunnistusvälineen myöntämisen edellytyksenä, joten Euroopan unionin toiminnasta tehdyn sopimuksen vastainen vapaan liikkuvuuden rajoittaminen tuskin tulee kysymykseen.[53]

Ensitunnistamisen yhteydessä tapahtuva kirjausvirhe on mahdollinen, joskin epätodennäköinen vaihtoehto, etenkin vuodesta 2016 alkaen, jolloin kaikki tunnistuslain piirissä olevat tunnisteet on sidottava henkilötunnukseen ja tiedot on tarkistettava Väestörekisterikeskuksesta. Periaatteessa on kuitenkin mahdollista, että tiedot menevät ristiin, kuten esimerkiksi jos uutta tunnistusvälinettä hakevalle henkilölle syötetään järjestelmään toisen täysin saman nimisen henkilön henkilötunnus. Tällöin tunnistuspalvelun tarjoaja on kuitenkin toiminut vähintäänkin huolimattomasti ja tunnistusvälineen haltijan tulisi huomata virhe nopeasti.

Oma lukunsa on petollinen toiminta ensitunnistamisen yhteydessä, jolloin tunnistusvälineen hakija pyrkii tietoisesti saamaan tunnistusvälineen vääriä tietoja ja asiakirjoja, kuten väärennettyä tai varastettua henkilöllisyystodistusta, käyttämällä. Tällöin tunnistusvälineen hakija syyllistyy kuitenkin rikokseen ja on vahingonkorvausvelvollinen, joskin tunnistuspalvelun tarjoaja on kuitenkin korvausvelvollinen tunnistukseen luottaneisiin nähden. Sähköiseen allekirjoitukseen käytettävän laatuvarmenteen myöntäjä kuitenkin vapautuu tällaisesta vastuusta mikäli pystyy näyttämään ettei vahinko ole aiheutunut heidän huolimattomuudestaan.[54]

FINE:n pankkilautakunnan tapauksessa 32/15 tunnistusvälineen myöntävä pankki oli epäonnistunut ensitunnistamisessa ja antanut verkkopankkitunnukset varastetun ajokortin avulla toisena henkilönä esiintyneelle rikolliselle. Toisessa liikkeessä rikollinen oli yrittänyt avata luotollisen tilin, mutta liike oli epäillyt henkilön olevan joku muu ja pysäyttänyt tilin avaamisen. Vahingon kärsinyt henkilö oli vaatinut tunnistusvälineen myöntäjältä korvausta asian selvittelystä aiheutuneesta harmista ja taloudellisista menetyksistä. Pankkilautakunnan ratkaisusuosituksen mukaan asiaa tuli käsitellä vahingonkorvauslain mukaisesti sopimuksen ulkopuolisena korvausvastuuna, jolloin korvausvaatimuksen esittäjän oli osoitettava vahingon aiheutuneen huolimattomuudesta. Kun va-

---

[53] Tunnistuslaki 7 §; HE 272/2014 vp, s. 6–9, 18–19; väestötietojärjestelmälaki 9 §

[54] Tunnistuslaki 41 §; HE 36/2014 s. 75–77

hingon kärsinyt henkilö oli esittänyt riittävän syyn epäillä tunnistuspalvelun tarjoajan toimineen huolimattomasti ensitunnistamistilanteessa eikä tunnistuspalvelun tarjoaja näyttänyt toimineensa huolellisesti, suositteli lautakunta korvauksen maksamista vahingon kärsineelle.

Tapaus alleviivaa identiteettivarkauden suuria vaikutuksia yksilölle. Rikollinen oli petoksella hankkimallaan tunnistamisvälineellä mm. hakenut pikavippejä ja tehnyt väliaikaisen osoitteenmuutoksen Postin verkkopalvelussa. Vaikka tunnistusvälineen haltija ei tunnistuslain 27 §:n mukaan vastaakaan tunnistusvälineen oikeudettomasta käytöstä identiteettivarkauden yhteydessä, voi väärinkäytösten selvittelystä ja laskujen reklamoinnista aiheutua huomattavasti työtä. PKL:lle osoitetun valituskirjeen lause "asiakas elää painajaista" kuvaa identiteettivarkauden kohteen tunteita, vaikkei sillä suoranaista oikeudellista arvoa olekaan.

Tunnistuspalvelun tarjoajan kannalta ratkaisusuositus asettaa kuitenkin huomattavia dokumentointivaatimuksia ensitunnistamiselle. Lautakunnan näkemyksen mukaan tunnistuspalvelun tarjoajan yleisten tunnistusperiaatteiden selvittäminen ei ollut riittävää, koska vahingon kärsijä oli esittänyt riittävän syyn epäillä huolimattomuutta, ja pankin olisi tullut esittää selvitys miten juuri kyseisessä tunnistamistilanteessa on toimittu. Asiakkaan tunnistaminen on kuitenkin pankissa normaali toimenpide jonka yksittäinen toimihenkilö voi tehdä useita kertoja päivässä, joten käytännössä tunnistamisen suorittajan ja tunnistamiseen käytetyn asiakirjan kopion lisäksi kovin paljoa enempää tietoa ei voitane tallentaa tunnistamisprosessiin käytettävän ajan merkittävästi kasvamatta. Tulevaisuudessa henkilökortin tai passin voimassaolon voi tarkistaa poliisin palvelusta, jolloin tiedon tällaisen tarkastuksen tuloksesta voi tallentaa ja todeta, onko henkilöllisyystodistus ilmoitettu kadonneeksi tai varastetuksi.[55]

Päätös ei kuitenkaan näyttäisi muuttavan vahingonkorvausoikeudessa omaksuttua linjaa, jossa näyttötaakka on lähtökohtaisesti kantajalla, mutta ei yhtä suurena kuin rikosoikeudessa. Joissain tilanteissa näyttötaakka voi olla jopa käännettynä vastaajalle. Rikoksesta ei pankkia kuitenkaan olisi voinut tällä näytöllä tuomita.[56]

Kyseessä oli puhdas varallisuusvahinko, joten sen korvaaminen on vaatinut joko näytön teon rangaistavuudesta tai muita erittäin painavia syitä, sillä kyseessä ei ole ollut julkisen vallan käyttäminen. On totta, että vahinko oli aiheutunut rikollisesta toiminnasta, mutta rangaistavan toiminnan takana oli rikollinen henkilö, ei siis pankki, jolta korvausta vaadittiin. Näin ollen vahingonkorvauksen perusteena ovat erittäin painavat syyt, joiksi pankkilautakunta on ratkaisusuosituksessaan merkinnyt ensitunnistamisen keskeisen merkityksen. Tällaisia syitä voisivat myös olla tunnistuslain 17.4 §, jonka mukaan

---

[55] Poliisihallitus 2016, s. 2

[56] Ståhlberg & Karhu 2013, s. 348

aiempaan tunnistukseen luottava vahvan sähköisen tunnistuspalvelun tarjoaja vastaa tunnistuksen virheellisyydestä suhteessa vahingon kärsineeseen, sekä ammattimaisten palvelusten tarjoajan korotettu huolellisuusvelvollisuus.[57]

Laatuvarmenteita tarjoava varmentaja vastaa vahingosta, joka varmenteeseen luottaneelle on aiheutunut, mikäli vahinko on aiheutunut laatuvarmenteeseen merkittyjen tietojen virheellisyydestä jo myöntämishetkellä, paitsi jos varmentaja pystyy näyttämään, ettei vahinko ole johtunut sen huolimattomuudesta (tunnistuslaki 41 §). Näin ollen laatuvarmenteiden ensitunnistamisen dokumentointivaatimusta voidaan tarkastella samoin perustein kuin PKL:n ratkaisusuosituksessa arvioitua tunnistusvälineen liikkeellelaskijan dokumentointivaatimusta.

3.4.3.2 Tietojen tallentaminen

Tunnistuslain 24 § mukaan tunnistuspalvelun tarjoajan on tallennettava yksittäisen tunnistustapahtuman todentamiseksi tarvittavat tiedot, tarvittavat tiedot hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta, välineen käyttöön liittyvät estot ja rajoitukset sekä varmenteeseen perustuvissa tunnistusmenetelmissä varmenteen tietosisältö. Ensitunnistamisen tietojen tallentamisen vaatimukset ovat yhtenevät rahanpesulain 10 § kanssa.

Tallentamisessa on noudatettava henkilötietolain vaatimuksia. Sähköiseen tunnistamiseen ja allekirjoittamiseen liittyvien henkilötietojen tallentaminen on sallittua, sillä käsittely johtuu laissa säädetystä velvoitteesta ja rekisteröidyllä on asiakassuhde tunnistuspalvelun tarjoajaan. Lisäksi tunnistuspalvelun tarjoaja voi pyytää hakijalta suostumuksen henkilötietojen käsittelyyn, mutta se ei ole tarpeellista muiden kriteerien täyttyessä (henkilötietolaki 8 §). Rekisteristä on laadittava rekisteriseloste (henkilötietolaki 10 §) ja huolehdittava riittävästä tietoturvasta (32 §). Yksittäisen tunnistustapahtuman todentamiseksi tarvittavien tietojen tallentamisessa on mahdollisuuksien mukaan poistettava syntyneet henkilötiedot (tunnistuslaki 24 §).

Tunnistuspalvelun tarjoajan sekä tunnistusta vaativan palvelun tarjoajan on erityisesti huomioitava tunnistuslain 5. luvun edellytykset henkilötietojen siirtämisestä EU:n ulkopuolelle, sillä vaikka verkkopalvelujen tuottaminen kolmannessa maassa sijaitsevalla palvelimella on teknisesti yksinkertaista, asettaa lainsäädäntö sille tiettyjä reunaehtoja.

Mielenkiintoinen kysymys onkin, mitä ovat tarvittavat tiedot hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta. Asiakirjan osalta valokopio itse asiakirjasta on varmasti riittävä, mutta FINE:n pankkilautakunnan näkemyksen mukaan merkintä, että

---

[57] Ståhlberg & Karhu, s. 130

on toimittu yleisten tunnistusperiaatteiden mukaisesti ei riitä todistamaan, että tunnistuspalvelun tarjoaja olisi toiminut huolellisesti.[58] Vakiintunutta oikeuskäytäntöä asiasta ei ole, ainoa tiedossani oleva ensitunnistamiseen liittyvä tuomioistuinratkaisu on Itä-Suomen hallinto-oikeuden päätös, että toisen EU/ETA-jäsenvaltion myöntämän passin on kelvattava ensitunnistuksessa käytettäväksi asiakirjaksi ellei erityinen syy sitä tapauskohtaisesti estä.[59]

3.4.3.3 Tunnistamisen oikeellisuus

Lähtökohtana ja perustana koko sähköisen tunnistamisen ja allekirjoittamisen luotettavuudelle on oikein tehty ensitunnistaminen. Sen jälkeen on vielä varmistettava, että tunnistusvälinettä voi käyttää vain tunnistusvälineen haltija sekä varmistuttava tietoturvasta.

Tunnistusvälineen haltijan yksinomainen oikeus käyttää tunnistusvälinettä varmistetaan pitämällä huoli siitä, että tunnistuspalvelu on riittävän tietoturvallinen, jotta virheellisen tunnistamisen mahdollisuus voidaan riittävällä varmuudella sulkea pois. Ensinnäkin tunnistuspalvelun tarjoajan tulee huolehtia, että se pystyy riittävällä varmuudella toteamaan, tunnistuspalvelun toteutustavasta riippuen, tunnistusvälineen fyysisen osan (esim. älykortti, tunnuslukutaulukko) hallussapidon, yksinomaan tunnistusvälineen haltijan tiedossa olevat koodit tai salasanat sekä tunnistusvälineen haltijan fyysiset ominaisuudet, kuten sormenjäljet. Lisäksi tunnistuspalvelun tarjoajan on pidettävä huolta, että tunnistamisen jälkeen henkilötieto siirretään turvallisesti asiointipalvelun tarjoajalle siten, että palveluntarjoaja voi varmistua tiedon alkuperästä.

Huomionarvoista on myös, että tunnistuspalveluun luottavalla osapuolella ei ole mahdollisuutta arvioida tunnistamisen luotettavuutta, hänelle välitetään ainoastaan henkilötieto. Nordea ja Osuuspankki ovat tunnistuspalvelusopimuksissaan todenneet, etteivät ne vastaa tunnistusvälineen oikeudettomasta käytöstä aiheutuneista vahingoista. Tämä on ymmärrettävää, sillä tunnistuspalvelun tarjoajallakaan ei ole käytettävissään kuin tieto siitä, onko tunnistamiseen edellytetyt tiedot syötetty oikein vai väärin. Näin ollen tunnistamiseen luottaneet pikavippifirmat eivät voisi hakea korvausta pankilta, eivätkä myöskään tunnistusvälineen haltijalta, jollei tämä ole luovuttanut tunnistusvälinettä toiselle, oikeudeton käyttö johdu tämän lievää vakavammasta huolimattomuudesta

[58] PKL 32/15

[59] Itä-Suomen HAO 17.06.2015 15/0193/4

tai tämän laiminlyönnistä tunnistusvälineen katoamisesta ilmoittamisessa. Danske Bankin sopimusehdoissa tällaista vastuunrajoitusta ei ole.[60]

Joka tapauksessa identiteettivarkaus on kriminalisoitu vuonna 2015. Rikoslakiin on lisätty uusi 38:9 a, joka kuuluu seuraavasti:

> *Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.*

Käytännössä usein on kyse myös RL 36:1 mukaisesta petoksesta, jos kolmannen osapuolen erehdyttämisen tarkoituksena on taloudellisen hyödyn hankkiminen tai vahingon aiheuttaminen. Petos voi tulla kysymykseen myös, jos tietojärjestelmän toimintaan puuttumalla saa aikaan lopputuloksen vääristymisen, esimerkiksi kolmannen henkilön henkilötietojen välittämisen tunnistuspalvelusta asiointipalveluun.

3.4.4 Välineen haltijan vastuu

3.4.4.1 Yleiset periaatteet

Lähtökohtaisesti tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä vain, jos

> *1) hän on luovuttanut tunnistusvälineen toiselle;*
> *2) tunnistusvälineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää; tai*
> *3) hän on laiminlyönyt ilmoittaa tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan.*
> (Tunnistuslaki 27.1 §)

Tunnistusvälineen haltija ei kuitenkaan lain 27.2 § mukaan vastaa oikeudettomasta käytöstä sen jälkeen, kun hän on ilmoittanut sen katoamisesta, toisen haltuun joutumisesta tai oikeudettomasta käytöstä; jos katoamisilmoitusta ei ole voitu tehdä; tai jos tunnistusta pyytävä taho ei ole tarkastanut käyttörajoitusten tai tunnusten sulkemisen olemassaoloa. Tunnistuslain vaatimukset ovat käytännössä samat kuin maksupalvelulain

---

[60] Danske Bank 2012; Nordea 2015b, s. 4; OP 2013, s. 1

edellytykset maksupalvelun käyttäjän vastuusta maksuvälineen oikeudettomasta käytöstä, joten tunnistamisvälineiden oikeudettoman käytön tutkimisessa voidaan käyttää hyväksi myös maksukorttien oikeudetonta käyttöä.[61]

Maksupalvelulain 62 §:ssä käyttäjän vastuu rajataan kuitenkin 150 euroon, ellei käyttäjä ole toiminut tahallisesti tai törkeän huolimattomasti. Tunnistuslaissa tätä vastuunrajoitusta ei kuitenkaan ole. Näin ollen pankkitunnusten osalta 150 euron omavastuun rajoitus on olemassa niiltä osin kuin niitä käytetään maksuvälineenä, mutta rajoitusta ei käsittääkseni voi soveltaa sähköisestä tunnistamisesta tai allekirjoittamisesta aiheutuneisiin vahinkoihin.

Omavastuurajoituksen ulottaminen verkkopankkitunnusten käyttöön tunnistamisvälineenä suurentaisi niiden tunnistuspalvelujen tarjoajien vastuuta, joiden tunnistamisväline toimii myös maksuvälineenä, tässä tapauksessa siis pankkien vastuuta. Tämä puolestaan muodostaisi kilpailuetua muille tunnistuspalvelun tarjoajille, joka ei ole toivottavaa, kun tarkoituksena on luoda toimivat tunnistamispalvelujen markkinat sisämarkkinoilla.[62]

Kuitenkin Kouvolan hovioikeus on tapauksissa S 11/637 ja S 11/378, joissa S oli vastuussa puolisonsa S:n nimissä ottamista luotoista jotka puoliso oli hakenut käyttämällä salaa S:n pankkitunnuksia, rinnastanut verkkopankkitunnukset luottokorttiin myös siltä osin kuin tunnuksia oli käytetty uuden luottokortin hakemiseen ja luottosopimuksen tekemiseen.[63] Tapahtumat olivat kyseisissä tapauksissa tapahtuneet ennen tunnistuslain ja maksupalvelulain voimaantuloa, jolloin sovellettavaksi tulivat silloisen kuluttajansuojalain 7. luvun (385/1986) 19 §:n säädökset, joissa käsitellään *luottokortin tai muun tililuoton käyttöön oikeuttavan tunnisteen* oikeudetonta käyttöä. Nykyisten lakien ajalta Suomessa ei tietääkseni ole relevantteja hovi- tai korkeimman oikeuden päätöksiä, joskin FINEn pankkilautakunta on antanut useita ratkaisusuosituksia sekä maksukorttien että verkkopankkitunnusten väärinkäyttöön liittyen.

Myös allekirjoituksen luomistietojen oikeudeton käyttö on kuluttaja-allekirjoittajan vastuulla vain, jos hän on luovuttanut luomistiedot toiselle tai niiden joutuminen toisen käytettäväksi on aiheutunut lievää vakavammasta huolimattomuudesta, tai mikäli hän ei ole pyytänyt laatuvarmenteen peruuttamista viipymättä sen jälkeen, kun hänellä on ollut perusteltu syy epäillä luomistietojen oikeudetonta käyttöä (tunnistuslaki 36 ja 40 §). Erona tunnistusvälineisiin on huomioitava, että velvoite pyytää varmenteen peruuttamista syntyy lain perusteella vasta, kun perusteltu syy epäillä allekirjoitustietojen oikeudetonta käyttöä ilmenee. Tunnistusvälineen haltijanhan tulee ilmoittaa jo tunnistus-

---

[61] Ks. esim. Kouvolan HO 2012:4

[62] HE 36/2009 vp, s. 27, 29; eIDAS-asetus, art. 4 ja johdanto-osan kohta 66

[63] Kouvolan HO 2012:3 ja 2012:4

välineen katoamisesta tai joutumisesta toisen haltuun, ei ainoastaan oikeudetonta käyttöä epäillessään.

Käytännössä laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen luomistiedot liittyvät tällä hetkellä tunnistusvälineeseen, jolloin välineen katoamisesta on ilmoitettava viipymättä. Mikäli vahinko on aiheutunut nimenomaan laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen oikeudettomasta käytöstä, voi vahingonkorvausvastuu jakautua eri tavalla kuin tunnistusvälineen kohdalla. Oikeushenkilöille myönnettyjen laatuvarmenteiden osalta vastuunrajoitusta ei laissa ole, jolloin allekirjoittaja vastaa luomistietojen oikeudettomasta käytöstä aiheutuneesta vahingosta kunnes peruuttamispyyntö on saapunut varmentajalle.

Vastuun jakautuminen oikeudettoman käytön tapauksessa on lähes sama Virossakin, missä sähköinen allekirjoitus aiheuttaa samat seuraukset kuin omakätinen allekirjoitus, paitsi jos allekirjoituksen luomisvälinettä on käytetty ilman välineen haltijan suostumusta. Tällöin allekirjoituksen luomisvälineen haltija on kuitenkin vahingonkorvausvelvollinen allekirjoitukseen luottaneeseen nähden, mikäli luvaton käyttö johtuu allekirjoituksen luomisvälineen haltijan tahallisuudesta tai törkeästä huolimattomuudesta. Todisteluvastuu on luomisvälineen haltijalla.[64]

Huomionarvoista on ero huolimattomuuden arvioinnissa. Pelkän lainkohdan sanamuodon perusteella on katsottava, että Suomessa vahingonkorvausvelvollisuus syntyy huolimattomuudesta hieman herkemmin kuin Virossa, mutta todellista vertailua varten pitäisi tutustua tarkemmin Viron vahingonkorvausoikeuteen sekä mahdollisiin oikeustapauksiin.

Viron sähköallekirjoituslaki ei myöskään määrittele tarkkaan, milloin allekirjoituksen luomisvälineen haltijan vastuu päättyy välineen katoamisesta tai väärinkäytöstä ilmoittamisen jälkeen, vrt. Suomessa varmenteen peruuttamispyynnön perille tulo. Varmentajan velvollisuudeksi on kuitenkin säädetty, että varmenteiden keskeyttämis- ja peruuttamispyyntöjä on vastaanotettava vuorokauden kaikkina aikoina, ja että varmenteilla tehtyjen allekirjoitusten ja leimojen varmentaminen on mahdollista 24 tuntia vuorokaudessa.[65] Käytännössä välineen haltijan vastuu siis päättynee, kun hän on ilmoittanut allekirjoituksen luomisvälineen joutuneen pois hänen hallinnastaan.

---

[64] Estonian Digital Signatures Act, § 3

[65] Estonian Digital Signatures Act, § 22

3.4.4.2 Välineen henkilökohtaisuus

Kuten edellä on todettu, on tunnistusvälineen haltijalla velvollisuus säilyttää tunnistusvälinettään huolellisesti. Velvollisuus pitää tunnistusväline vain omassa hallinnassaan on tunnistuslain lisäksi mainittu suurimpien Suomessa toimivien pankkien verkkopankkisopimuksissa sekä poliisin myöntämän henkilökortin käyttöehdoissa.[66]

Henkilökortin käyttöehdoissa tosin todetaan, että *henkilökorttia ja siihen liittyviä sähköisiä tunnuslukuja saa käyttää vain kortinhaltija tai hänen valtuuttamansa henkilö.* Tämä mahdollistaisi esimerkiksi iäkkään henkilön asioiden hoitamisen hänen kansalaisvarmenteensa avulla, toisin kuin pankkitunnuksilla, joita ei sivullisille saa luovuttaa lainkaan. Samoissa käyttöehdoissa kuitenkin todetaan myös, että *kansalaisvarmenne on standardimuodossa kerrottu henkilötieto, haltijansa sähköinen henkilöllisyys eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi.* Kansalaisvarmenne on henkilökortilla ja varmennetta käytetään korttiin liittyvillä tunnusluvuilla. Ehdot ovat siis ristiriidassa itsensä kanssa. Tunnistuslain 20 §:ssä asetetaan henkilökohtaisuus vahvan tunnistamisvälineen ehdoksi, joten käyttöehtoja on mielestäni tulkittava niin, ettei korttia ja siihen liittyviä tunnuslukuja saa luovuttaa muille. Ristiriidan vuoksi ehtoja olisi kuitenkin muokattava niin, että henkilökorttia ja siihen liittyviä sähköisiä tunnuslukuja saa käyttää vain kortinhaltija.[67]

Sekä OP:n, Nordean että Danske Bankin kuluttaja-asiakkailleen tarjoamat pankkitunnukset ovat henkilökohtaisia ja mahdollistavat tunnistuslain mukaisen vahvan sähköisen tunnistamisen, eikä tunnuksia saa luovuttaa sivullisille. Kaikki kolme pankkia tarjoavat myös verkkopankkitunnuksia yrityksille. Nämä tunnukset saa luovuttaa niiden käyttöön oikeutetuille, eivätkä ne ole tunnistuslain mukaisia vahvoja tunnistamisvälineitä, paitsi Danske Bankilla, jonka kaikki verkkopankkitunnukset ovat henkilökohtaisia. Yrityskohtaisten tunnusten avulla voidaan kyllä tunnistautua niissä palveluissa, joiden kanssa pankki on tehnyt erillisen sopimuksen yritysasiakkaiden tunnistamisesta, mutta tällöin luonnollisen henkilön henkilöllisyyttä ei välitetä palveluntarjoajalle, koska käyttäjän henkilöllisyys ei ole pankin tiedossa.[68]

Yllä mainitut seikat tukevat tulkintaa, ettei yksittäisen luonnollisen henkilön tunnistavaa välinettä voi tehokkaasti luovuttaa toiselle, joskin vastakkaisiakin mielipiteitä voi

---

[66] Nordea 2015a; OP 2014; Danske Bank 2013; Henkilökortin käyttöehdot 2011, s. 2–3

[67] Henkilökortin käyttöehdot 2011, s. 2–3

[68] Nordea 2015a; OP 2014; Danske Bank 2013

esittää tunnistuslain esitöihin ja henkilökortin käyttöehtoihin vedoten.[69] Pankkiasioinnissa toisen henkilön edustaminen sähköisessä asioinnissa on melko helppoa muillakin tavoilla, viranomaisasioinnissa kuitenkin merkittävän hankalaa. Paperinen – tai vahvalla sähköisellä allekirjoituksella varmennettu sähköinen – yleisvaltakirjahan on mahdollista antaa, mutta valtuutuksen toteaminen sähköisen tunnistamisen yhteydessä ei onnistu helposti yleisesti hyväksytyn valtuutustavan puuttuessa. Väestörekisterikeskus on tosin rakentamassa kansallista valtuutusrekisteriä uuden tunnistuksenohjauspalvelun yhteyteen osana kansallista palveluarkkitehtuuriprojektia. Tämän valtuutusrekisterin odotetaan ainakin helpottavan tilannetta.[70]

Tämä ei kuitenkaan poista sitä tosiasiaa, että vahvan sähköisen tunnistusvälineen luovuttaminen toisen käyttöön on mahdollista, joskin kiellettyä. Tunnistusvälineen haltija rikkoo tällöin tunnistuslain 23 § kieltoa luovuttaa välinettä toisen käyttöön sekä todennäköisesti myös sopimusehtoja. Lisäksi tunnistuslain 27 § vastuunrajoitus poistuu, jolloin tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä kunnes hän ilmoittaa asiasta tunnistuspalvelun tarjoajalle. Allekirjoituksen luomistietojen osalta tunnistuslain 40 § asettaa sisällöllisesti vastaavat vaatimukset.

3.4.4.3 Välineen joutuminen sivullisen haltuun

Koska tunnistusvälineen haltija ei vastaa vahingoista, jotka ovat aiheutuneet lievällä huolimattomuudella aiheutetusta tunnistusvälineen joutumisesta toisen haltuun, on tärkeää tarkastella, missä kulkee raja lievän ja muun kuin lievän huolimattomuuden välillä. Tarkastelussa voidaan tukeutua oikeustapauksiin ja FINE:n pankkilautakunnan ratkaisusuosituksiin sekä aiempaan tutkimukseen. Syytä on edelleen muistaa, että huolimattomuuden arviointia tunnistusvälineiden kohdalla voidaan tehdä myös katsomalla maksuvälineiden kohdalla tehtyjä linjanvetoja.

Oikeustapauksia tunnistusvälineisiin liittyen ei Suomessa kovin paljoa ole. Kouvolan hovioikeus on kuitenkin ottanut kantaa tunnistusvälineen säilyttämiseen vuonna 2012, jolloin katsottiin, että käyttäjätunnuksen ja salasanan säilyttäminen samalla lapulla rahapussissa ja tunnuslukulistan säilyttäminen lipastossa oli riittävän huolellista, vaikka tunnistusvälineen haltijan vaimo oli saanut tunnukset oikeudetta käyttöönsä ja vaikka sopimusehdoissa oli kirjattuna vaatimus pitää käyttäjätunnus, salasana sekä salasanalista

---

[69] Ponka 2013, s. 284–288. Ponkan väitöskirjassa käsitellään laajasti valtuutuksen merkitystä ja antamistapoja niin yleisellä tasolla kuin sähköiseen tunnistamiseenkin liittyen, eikä sitä pohdintaa ole mielekästä tässä ruveta toistamaan.

[70] Asiasta enemmän luvussa 6.1

erillään toisistaan. Sen sijaan huolellisuuden vaatimukseksi asetettiin velvollisuus tarkkailla tilitapahtumia, mitä kyseisissä tapauksissa ei ollut tehty.[71] Tunnusten säilyttämisen osalta ratkaisu mukailee hallituksen esitystä, jonka mukaan maksuvälineen säilyttäminen rahapussissa ja tunnusluvun säilyttäminen lipaston laatikossa on riittävän huolellista, joskin oikeustapauksessa kaikki maksu- ja tunnistamisvälineen käyttöön tarvittavat tiedot eivät olleet erillään, vaan ainoastaan kahdessa paikassa.[72]

FINE:n pankkilautakunta on useaan otteeseen katsonut, että käyttäjätunnuksen, salasanan ja tunnuslukutaulukon säilyttäminen samassa paikassa on arvioitava vähintään huolimattomaksi toiminnaksi. Mikäli tunnuksia on säilytetty tällä tavalla, mutta lukitussa kodissa, ei huolimattomuuden kuitenkaan ole katsottu olleen törkeää.[73] Kodin ulkopuolella hävinneiden tunnusten osalta tunnistuspalvelun tarjoajan kannattaakin vedota todennäköisyyteen, että maksuvälinettä ja tunnuslukua, taikka tunnistamisvälineen eri osia, on säilytetty yhdessä helposti tunnistettavassa muodossa, sillä luotettavan selvityksen esittäminen muunlaisesta toiminnasta jää tunnusten haltijan vastuulle.

Allekirjoitusten luomistietojen oikeudettoman käytön vastuunrajoitukset, jotka asiallisesti vastaavat sähköisen tunnistamisen välineiden vastuunrajoituksia, kuitenkin koskevat ainoastaan kuluttajia. Oikeushenkilö vastaa sille myönnetyn, laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen luomistietojen oikeudettomasta käytöstä kunnes pyyntö varmenteen peruuttamisesta on saapunut perille.

3.4.4.4 Välineen katoamisesta ilmoittaminen

Pankkien sopimusehtojen mukaisesti tunnistusvälineen haltijan on välittömästi ilmoitettava tunnistusvälineen katoamisesta tai joutumisesta sivullisen tietoon, taikka jos tällaista epäillään. Velvollisuus syntyy jo osan tunnistusvälineestä, esimerkiksi tunnuslukulistan tai salasanan, kadotessa. Esimerkiksi VRK:n myöntämän henkilökortin katoamisesta on ilmoitettava viipymättä.[74]

Velvollisuus on kirjattu myös lakiin: tunnistuslain mukaisesti tunnistusvälineen katoamisesta on ilmoitettava tunnistuspalvelun tarjoajalle ilman aiheetonta viivytystä katoamisen havaitsemisen jälkeen (tunnistuslaki 27 §). Kysymykseen tulee siis viivytyksen aiheellisuuden arviointi sekä katoamisen havaitsemisen osalta mahdollisen huolimattomuuden arviointi.

---

[71] Kouvolan HO 5.1.2012:3 ja 5.1.2012:4

[72] HE 169/2009 vp, s. 68

[73] ks. esim. PKL 59/11, PKL 20/13, PKL 10/14

[74] OP 2014, s. 3; Danske Bank 2013, s. 2; Henkilökortin käyttöehdot 2011, s. 2

Kuten jo edellä todettiin, on hovioikeudessa asetettu pankkitunnusten haltijalle velvollisuus tarkkailla tilitapahtumia, ja kun näin ei oltu tehty, katsottiin pankkitunnusten haltijan toimineen vähäistä suuremmalla huolimattomuudella.[75] Velvollisuus tarkkailla tilitapahtumia on johdettu KKO:n linjauksesta, jossa Madridissa oleskelleen henkilön olisi pitänyt tarkkailla luottokorttinsa tallellaoloa, jotta hänen toimintansa olisi voitu katsoa huolelliseksi:

> *10. A on ollut tietoinen siitä, että Madridissa oli merkittävä vaara joutua taskuvarkauden uhriksi ja että kaupungissa oli parhaillaan vieläpä erityisen paljon ihmisiä. Kun A on kerrotuin tavoin matkustanut täysissä metroissa ja pitänyt ravintolassa tuolin selkänojalla takkiaan, jonka taskussa lompakko ja luottokortti olivat, jo A:n Madridissa olon ensimmäisen vuorokauden aikana ovat toistuneet sellaiset tilanteet, joihin tunnetusti liittyy suuria katoamis- ja anastusriskejä. Näissä olosuhteissa mainitussa 19 §:n 1 momentissa kortin haltijalta edellytetty riittävä huolellisuus on vaatinut, että A olisi varmistunut kortin tallellaolosta riittävän usein ja erityisesti edellä kerrotunlaisten riskitilanteiden jälkeen. Korkein oikeus katsoo, että A on laiminlyönyt tämän ja että luottokortin oikeudeton käyttö on johtunut tästä hänen huolimattomuudestaan, koska sen johdosta kortin väärinkäyttöä ei ole voitu luottokorttijärjestelmän mukaisesti estää. Käsillä olleet olosuhteet ja A:n välinpitämätön suhtautuminen huomioon ottaen huolimattomuus ei ole ollut lievää. A on siten vastuussa kanteessa tarkoitetusta luottokortin väärinkäytöstä.*[76]

Velvollisuus varmistua kortin tallellaolosta säännöllisin väliajoin on KKO:n päätöksen jälkeen mainittu myös hallituksen esityksessä maksupalvelulaiksi, ja tähän velvollisuuteen on viitattu useissa PKL:n ratkaisuissa.[77]

Aiheettoman viivästyksen arviointiin voi käyttää Korkeimman oikeuden ratkaisua 1994:82, jossa ryöstöstä ilmoittaminen yli kaksi vuorokautta ryöstön jälkeen katsottiin huolimattomaksi toiminnaksi. Vaikka ryöstö oli tapahtunut jo vuonna 1989, katsoivat raastuvanoikeus ja hovioikeus, että käytössä olleet viestintämahdollisuudet eivät estäneet katoamisilmoituksen oikea-aikaista tekemistä. Korkeimpaan oikeuteen huolimattomuutta ei enää viety, sen sijaan korkeimmassa oikeudessa todettiin, että luottokortin myöntäjän on kyettävä näyttämään, että myyjäosapuoli on toiminut huolellisesti vaikka kortinhaltija olisikin laiminlyönyt velvollisuutensa ilmoittaa kortin katoamisesta. Tapaus lienee sovellettavissa myös tunnistuspalvelun tarjoajan vastuuseen ennen katoa-

---

[75] Kouvolan HO 5.1.2012:3

[76] KKO 2006:81

[77] HE 169/2009, s. 68; ks. esim. PKL 27/13, 32/14 ja 42/14.

misilmoituksen vastaanottamista, käytännössä velvollisuuteen tarkistaa tunnistusvälineen voimassaolo. Joka tapauksessa ilmoituksen viivästykseen on aina suhtauduttava kriittisesti, sillä viestintämahdollisuudet ovat vuodesta 1989 parantuneet huomattavasti.

Katoamisesta ilmoittamisen aikamääreeseen otetaan kantaa myös Helsingin hovioikeuden luottokortin käyttöä koskevassa ratkaisussa 2007:2. Luottokortin haltija oli sairaskohtauksen takia joutunut sairaalahoitoon 18.1. ja kotiutunut sieltä 20.1. Häneltä anastetulla luottokortilla oli tehty ostoksia 19–21.1. Katoamisen luottokortin haltija havaitsi vasta 18.2. jolloin ilmoitti siitä myös pankille. Sairaalassaolon aikana tapahtunut väärinkäyttö ei ollut kortinhaltijan huolimattomuutta. Kotiutumisen jälkeistä huolimattomuutta ei puolestaan oltu kiistetty, eikä siihen otettu kantaa sillä 21.1. tehty ostos riitautettiin myyjän huolimattomuuteen vedoten.

4 VUODEN 2016 ALUSSA VOIMAAN TULLEET MUUTOKSET

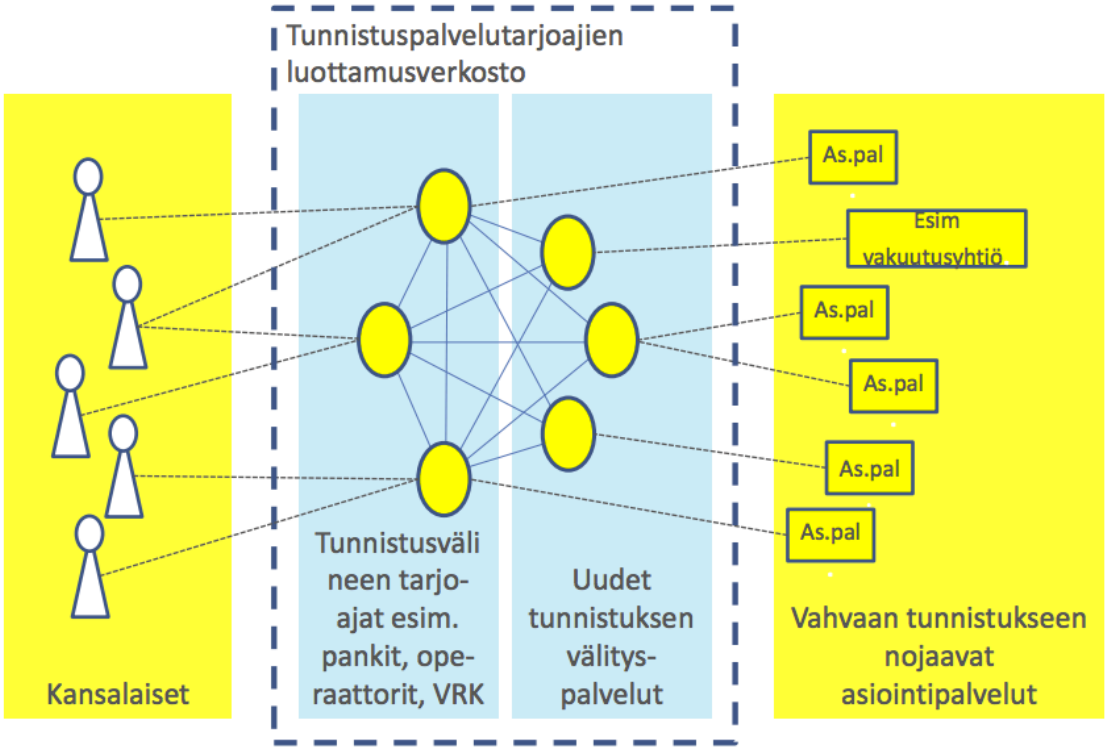
4.1 Kansallinen tunnistuspalvelun tarjoajien luottamusverkosto

Lailla 139/2015 muutettiin useita tunnistuslain kohtia, joista suurimpana muutoksena on lakiin lisätty 12a § koskien tunnistuspalvelun tarjoajien verkostoa. Lisäksi muutettiin vaatimuksia, jotka koskevat ensitunnistamista ja tietojen tarkistamista väestötietojärjestelmästä. Muutokset tulivat voimaan 1.1.2016, joskin 12a §:n soveltaminen aloitetaan vasta 1.5.2017.

Tunnistuslaissa luottamusverkosto määritellään Viestintävirastoon ilmoituksen tehneiden tunnistuspalvelun tarjoajien verkostoksi, ja toisaalta määrätään, että tunnistuspalvelun tarjoaja liittyy osaksi luottamusverkostoa tehdessään ilmoituksen toiminnan aloittamisesta. Luottamusverkostoon kuuluville asetetaan velvollisuus noudattaa tiettyjä hallinnollisia käytäntöjä ja tarjota tiettyjä teknisiä rajapintoja, joilla luodaan edellytykset tunnistuspalveluita tarjoavien ja niitä hyödyntävien toimijoiden väliselle toiminnalle. Tunnistuspalvelun tarjoajien on tehtävä sopimus tarjoamansa tunnistusvälineen käytön mahdollistamisesta kaikissa tunnistuksen välityspalveluissa. Tarkemmasta soveltamisesta määrätään Valtioneuvoston asetuksella 169/2016.

Tavoitteena luottamusverkoston luomisella on kilpailun avaaminen tunnistusmarkkinoilla, sillä tällä hetkellä sähköisen palvelun tarjoaja joutuu käytännössä tekemään sopimuksen sähköisen tunnistamisen palveluista ainakin suurimpien pankkien kanssa, jokaisen kanssa erikseen, sillä yhden pankin myöntämää tunnistusvälinettä ei voi tällä hetkellä käyttää toisen pankin kirjautumispalvelussa. Kun luottamusverkoston myötä tunnistuspalvelun tarjoajat ovat velvoitettuja välittämään tunnistustietoja myös muille tunnistuksen välittäjille, oletetaan tunnistamista tarvitsevien palveluiden tarjoajien valinnanvaran kasvavan ja neuvotteluaseman parantuvan, kun sopimus yhden välityspalvelun kanssa riittää.[78]

[78] HE 272/2014 vp, s. 9



Kuvio 3 Vahvan tunnistuksen toimintamalli luottamusverkostossa (Simola 2015, s. 3)

Sähköisen palvelun tarjoajan kannalta luottamusverkoston rakentuminen helpottaa vahvan sähköisen tunnistamisen käyttöönottoa ja helpottaa sopimushallintaa, kun kaikki vahvat sähköiset tunnistamismenetelmät ovat käytettävissä yhdellä välityspalvelusopimuksella. Myös yksittäinen kansalainen saa hyötyjä, kun hänen tunnistusvälineellään pystyy kirjautumaan mihin tahansa palveluun, riippumatta siitä, kenen kanssa palvelun-tarjoaja on tunnistuksen välityssopimuksen tehnyt. Kansalainen pääsee käyttämään yhä useampia palveluita, eikä hänen tarvitse opetella kuin yksi kirjautumistapa. Luottamus-verkoston tulisikin siis vaikuttaa positiivisesti sekä yksittäisten kansalaisten että säh-köisten palveluiden tarjoajien kokemaan helppokäyttöisyyteen ja sähköisten tunnistus-tapojen hyödyllisyyteen, näin kasvattaen alan markkinoita. Markkinoiden kasvaessa myös sosiaalinen paine käyttää sähköistä tunnistamista kasvaa, kasvattaen markkinoita entisestään.

Käytännössä luottamusverkosto tullee rakentumaan sen toimijoiden kahdenkeskisten sopimusten varaan, joskin Viestintäviraston asettama yhteistoimintaryhmä voi valmis-tella mallisopimuksia ja ohjeita.[79] Kahdenkeskisten sopimusten malli saattaa vaikeuttaa uusien palveluntarjoajien tuloa markkinoille, sillä nykyisillä toimijoilla, toisin sanoen

[79] VNa 169/2016, 3 §

pankeilla ja teleoperaattoreilla, on hyvä neuvotteluasema ja luottamusverkostoon kuuluminen on pakollista. Viranomaisen tulisikin asettaa luottamusverkostosopimusneuvotteluille jokin takaraja sekä säädellä mitä tapahtuu, mikäli osapuolet eivät pääse sopimukseen.

Luottamusverkostoa ja kansallisia luottamuspalveluja koskevaa Viestintäviraston määräystä 72 ollaan parhaillaan valmistelemassa. Määräyksellä tullaan tarkemmin määrittämään luottamusverkoston toimijoiden välisten rajapintojen vaatimukset sekä mm. tarkentamaan tunnistus- ja luottamuspalveluiden ilmoitusvelvoitteita ja vaatimustenmukaisuuden arvioinnin kriteereitä. Tarkoitus on, että uusi määräys olisi voimassa 1.7.2016.[80] Jonkinlainen siirtymäsäännös kuitenkin tarvittaneen, sillä 13.5. päivätyn lausuntopyynnön takaraja on 31.5.2016 ja lausuntojen läpikäynti on aikataulutettu 10.6.2016.[81]

4.2 Henkilötietojen tarkastusvelvollisuus väestötietojärjestelmästä

Vuoden 2016 alusta lähtien tunnistuspalvelun tarjoajan sekä sähköisiä allekirjoituksia tarjoavan varmentajan on vaadittava hakijaa ilmoittamaan henkilötunnuksensa, mikä ei aiemmin ole ollut pakollista. (Tunnistuslaki 6.3 §). Käytännön tasolla muutosta ei tapahtunut, sillä vakiintunut käytäntö oli jo aikaisemmin pyytää henkilötunnusta henkilöllisyyttä tarkastettaessa.[82]

Tunnistusvälineen ja allekirjoituksen luomisvälineen haltijan henkilötiedot on myös hankittava väestötietojärjestelmästä ja päivitettävä sieltä niin, että tiedot ovat ajan tasalla. (Tunnistuslaki 7 §). Aiemmin tämä oli sallittua, mutta ei pakollista. Muutoksen tavoitteena on ollut varmistaa tunnistusvälineen yhdistäminen viranomaisrekisteristä löytyvään luonnolliseen henkilöön ja mahdollistaa luottamusverkoston rakentaminen, sillä tunnistuspalvelun tarjoajan on välitettävä henkilön yksilöivä tieto, käytännössä henkilötunnus tai sähköinen asiointitunnus, toiselle tunnistuspalvelun tarjoajalle, kun näiden välillä siirretään tunnistetietoja.[83]

Käytännössä muutokset vaikeuttavat sähköisen tunnistusvälineen tai allekirjoituksen luomisvälineen myöntämistä ulkomaalaiselle, joka ei ole asunut Suomessa, sillä edellytyksenä on henkilön tietojen tallentaminen väestötietojärjestelmään, jonka edellytyksistä säädetään väestötietojärjestelmälain 9 §:ssä:

---

[80] Viestintävirasto 2016a, s. 2, 11, 14

[81] Viestintävirasto 2016a, s. 19; Viestintävirasto 2016b

[82] HE 272/2014 vp, s. 18

[83] HE 272/2014 vp, s. 18

> *Ulkomaan kansalaista koskevat tiedot talletetaan väestötietojärjestelmään, jos hänellä on Suomessa kotikuntalain (201/1994) mukaan määräytynyt kotikunta ja siellä oleva asuinpaikka. Muuta ulkomaan kansalaista koskevat tiedot voidaan tallettaa väestötietojärjestelmään, jos:*
>
> *1) hänellä on Suomessa kotikuntalaissa tarkoitettu tilapäinen asuinpaikka, ja tallettaminen on tarpeen työskentelyyn, opiskeluun tai muuhun vastaavaan olosuhteeseen liittyvien velvollisuuksien tai oikeuksien toteuttamisen vuoksi;*
>
> *2) tallettaminen johtuu Suomea sitovan kansainvälisen sopimuksen velvoitteiden täyttämisestä; tai*
>
> *3) tallettaminen on hänelle kuuluvien oikeuksien tai hänelle asetettujen velvollisuuksien toteuttamisen tai muun vastaavan erityisen ja perustellun syyn vuoksi tarpeellista.*

Koska sähköisten tunnistuspalvelun tarjoajien on Euroopan unionin toiminnasta tehdyn sopimuksen 56 artiklan palveluiden vapaan liikkuvuuden periaatteen mukaisesti voitava tarjota palveluitaan kaikille EU:n jäsenmaiden kansalaisille, tulisi EU:n kansalaisen pyynnöstään saada itsensä merkityksi Suomen väestötietojärjestelmään, jotta heille voidaan myöntää vahva tunnistus- tai allekirjoitusväline. Tämän ylimääräisen toimenpiteen vuoksi pidänkin todennäköisenä, että ulkomaan kansalaisille Suomessa myönnettävien vahvojen sähköisten tunnistusvälineiden määrät pysyvät pieninä, etenkin kun viranomaisasioinnissa on tulevaisuudessa pystyttävä käyttämään myös muiden EU-jäsenvaltioiden ilmoittamia tunnistusmenetelmiä.

Lain esitöissä oli otettu huomioon, että osa sähköisiä tunnistuspalveluja käyttävistä henkilöistä jäi muutoksen yhteydessä järjestelmän ulkopuolelle, mihin ehdotettiin ratkaisuksi sähköisten tunnistuspalveluiden tarjoamista vain tunnistusvälineen liikkeellelaskijan omiin palveluihin, tai sopimusperusteisesti myös muualle. Tällaista välinettä ei kuitenkaan katsottaisi lain tarkoittamaksi vahvaksi tunnistusvälineeksi, eikä sitä voisi käyttää uusien tunnistusvälineiden luomiseen.[84]

Muutos heikentää vahvojen sähköisten tunnistusvälineiden sekä allekirjoitusvälineiden helppokäyttöisyyttä niiden ulkomaalaisten osalta, jotka eivät ole merkittynä väestötietojärjestelmään. Tiukempi kytkös kuitenkin kasvattaa välineiden luotettavuutta ja siten koko järjestelmästä saatavaa hyötyä.

---

[84] HE 272/2014 vp, s. 19

4.3 Ensitunnistaminen

Vahvan sähköisen tunnistusvälineen hakijan ensitunnistamisen on aiemmin pitänyt lähtökohtaisesti tapahtua henkilökohtaisesti, jollei kahden vahvan sähköisen tunnistuspalvelun tarjoajan välillä oltu tehty sopimusta mahdollisuudesta luottaa toistensa tekemään ensitunnistamiseen. 2016 alussa tunnistuslain 17 § kuitenkin muutettiin niin, että henkilökohtaista tunnistamista vaaditaan vain, jos hakijalla ei ole voimassa olevaa vahvaa sähköistä tunnistusvälinettä. Olemassa olevan tunnistusvälineen avulla on voitava hakea vastaavan tasoista tunnistusvälinettä.

Vastaavan tasoisella viitataan lain esitöiden perusteella ns. eIDAS-asetuksen[85] tarkoittamaan varmuustasoon, joka määritellään kyseisen asetuksen 8 artiklassa sekä komission täytäntöönpanoasetuksessa[86]. Kyseistä varmuustasojaottelua ei kansallisessa lainsäädännössä määritellä ja tunnistamisasetuksen 8 artikla koskee vain järjestelmiä, jotka on ilmoitettu EU:n sisärajat ylittäviä tunnistustapahtumia varten, joten tarkoitus lieneekin ollut harmonisoida kansallista lainsäädäntöä EU:n lainsäädännön kanssa. Varmuustasot määrittelevä täytäntöönpanoasetus ei kuitenkaan ole ollut valmis vielä silloin, kun muutos tunnistuslakiin on hyväksytty, ja kyseistä kohtaa tullaankin selventämään tulevaisuudessa.[87]

Mielenkiintoisempi kysymys on kuitenkin pykälän muotoilu "on voitava hakea". Toimenpiteeseen liittyy tällöin kaksi puolta: Ensitunnistamiseen käytetyn tunnistuspalvelun tarjoajan on sallittava tunnistusvälineensä käyttö uusien tunnistusvälineiden luomiseen, ja uusia tunnuksia luovan palveluntarjoajan on puolestaan hyväksyttävä muiden sähköisten välineiden käyttö tunnistamisvälineiden luomiseen.

Ainakin Danske Bankin, Nordean ja Osuuspankin palveluehdoissa on kielletty uusien tunnistusvälineiden luominen ilman erillistä sopimusta pankin kanssa, ansaintalogiikan perustuessa palveluntarjoajan tunnistustapahtumien määrän mukaan maksamaan palvelumaksuun, jota omien (heikkojenkin) tunnistusvälineiden luominen luonnollisesti

---

[85] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta

[86] Komission täytäntöönpanoasetus (EU) 2015/1502, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti (varmuustasoasetus)

[87] HE 272/2014 vp, s. 5–6; HE 74/2016 vp

pienentäisi.[88] Laissa säädetty mahdollisuus uusien tunnistusvälineiden luomiseen koskee kuitenkin vain vahvan sähköisen tunnistuspalvelun tarjoajia, jotka ovat joutuneet tekemään ilmoituksen toiminnan aloittamisesta ja liittymään tunnistuspalvelun tarjoajien luottamusverkostoon, joten kovin suuria hinnoittelu- ja ansaintalogiikkamuutoksia 17 §:n muutoksesta tuskin seuraa.

Huomiota kuitenkin herättää hallituksen esityksessä maininta, ettei ensitunnistamisen hintaa tai hintaa tunnistusvälineen luomiselle jo olemassa olevan tunnistusvälineen avulla ole tarpeellista säännellä, vaan hinnat määräytyvät markkinaehtoisesti.[89] Velvollisuus mahdollistaa tunnistusvälineiden luominen jo olemassa olevien sähköisten välineiden avulla on kuitenkin kirjattu lakiin, joten onkin kysyttävä, mitä tapahtuu, jos kaksi tunnistuspalvelun tarjoajaa ei pääse sopimukseen ensitunnistamisen hinnasta? Yksi vaihtoehto on, että sähköisen tunnistusvälineen käyttämisen ensitunnistusvälineenä maksaa suoraan tunnistusvälineen haltija, ja hinta määräytyy tunnistusvälineen haltijan ja ensitunnistamiseen käytetyn tunnistuspalvelun tarjoajan välisen sopimuksen mukaan.

Sähköisellä tunnistusvälineellä tehtävä ensitunnistaminen avaa kuitenkin mahdollisuuksia identiteettivarkaille. Kun tähän asti ensitunnistaminen on pitänyt tehdä henkilökohtaisesti, on henkilön ulkonäön varmennettu vastaavan hänen hallussaan ollutta viranomaisen myöntämää henkilöllisyystodistusta taikka ajokorttia. Sähköisen tunnistamisen kohdalla voidaan kuitenkin vain todeta teknisten tietojen täsmäävään, ja mikäli henkilö saa toisen tunnistusvälineen haltuunsa, on olemassa mahdollisuus uusien tunnistusvälineiden luomiseen, joita tunnistusvälineen oikeutettu haltija ei osaa sulkea, koska ei tiedä niiden olemassaolosta.

Viestintävirasto on käsitellyt kysymystä tulevan tunnistus- ja luottamuspalveluita koskevan määräyksensä perusteluissa. Koska ensitunnistamiseen luottava osapuoli kantaa vahinkovastuun, on määräyksen valmistelussa mietitty mahdollisuutta sisällyttää ensitunnistamisen tekniseen rajapintaan tieto alkuperäisen henkilökohtaisen tunnistamisen päivämäärästä, tekijästä, käytetystä henkilöllisyystodistuksesta sekä ketjutettujen tunnistusvälineiden määrästä ja niiden myöntäjistä. Viestintävirasto on myös todennut, että alan toimijat ovat katsoneet sähköisen ensitunnistamisen toimineen ongelmitta tähänkin asti, ja että yhtenä sähköisen ensitunnistamisen suurimpina esteinä on hinta. Näin ollen ensitunnistamisen rajapintaan ei ole ehdotettu lisättäväksi määräyksiä aiemmasta ensitunnistamisesta. Määräysluonnos on tällä hetkellä lausuntokierroksella.[90]

Myös Poliisi on ilmaissut huolensa sähköisten tunnistustapojen rajattomasta ketjuttamisesta, koska tällöin kerran väärän sähköisen henkilöllisyyden saanut henkilö pystyy

---

[88] Danske Bank 2012, s. 2; Nordea 2015b, s. 1; OP 2013, s. 2

[89] HE 272/2014 vp, s. 21

[90] Viestintävirasto MPS 72 luonnos, s. 26–28

uusimaan sen uudelleen ja uudelleen.[91] Tunnistamisvälineen hakeminen olemassa olevalla sähköisellä tunnistamisvälineellä on kuitenkin helppoa, vaikuttaen UTAUT2-mallin odotettuun vaivaan ja TAM-mallin koettuun helppokäyttöisyyteen. Toisaalta identiteettivarkauksien uhka saattaa myös vaikuttaa hakijoiden käyttäytymiseen.

4.4 Muutoksenhaku

Muutoksenhakua on muutettu lailla 997/2015, jolla tarkastuslaitoksen nimeämisen peruuttamista koskevilta asioilta on poistettu valitusluvan tarve korkeimpaan hallinto-oikeuteen valittamiseen. Hallituksen esityksessä muutosta on perusteltu tällaisten asioiden merkityksellisyydellä tarkastuslaitoksen oikeusturvan ja elinkeinon harjoittamisen kannalta. Muilta osin muutoksenhaun sisältö on pysynyt muuttumattomana.[92]

Tällaisen tarkastuslaitoksen tehtävänä on arvioida, täyttääkö allekirjoituksen luomisväline tunnistuslain vaatimukset turvalliselle allekirjoituksen luomisvälineelle, ellei väline ole EU:n tasolla hyväksytyn standardin mukainen, jolloin tarkastuslaitoksen tarkastusta ei tarvita. Tarkastuslaitosten nimeämisestä, valvonnasta ja nimeämisen peruuttamisesta vastaa Viestintävirasto, joten valitusasiat tarkastuslaitosten nimeämisen peruuttamisesta kohdistuvat aina Viestintäviraston päätökseen. (Tunnistuslaki 28–29 §)

Valitusluvan tarpeen poistaminen ei suoraan vaikuta allekirjoituksen luomisvälineen käyttäjään eikä juuri vaikuttane sähköisen allekirjoittamisen ja allekirjoittamisen suosioon. Yksityisellä sektorilla kannustinta ryhtyä lain tarkoittamaksi tarkastuslaitokseksi ei juuri liene ennen kuin muutkin kuin Väestörekisterikeskus ryhtyvät tarjoamaan varmennepalveluita.

---

[91] Poliisihallitus 2016, s. 2–3

[92] HE 230/2014 vp, s. 101

5 EIDAS-ASETUS

5.1 Tavoitteet ja soveltamisala

Euroopan parlamentti ja neuvosto ovat vuonna 2014 antaneet asetuksen sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla (ns. eIDAS-asetus). Asetuksella, joka on jäsenvaltioissa suoraan sovellettavaa oikeutta, mahdollistetaan unionin sisärajat ylittävä vahva sähköinen tunnistaminen ja luodaan yhteiseurooppalainen sääntely luottamuspalveluille. Säädöksiä sovelletaan pääosin 1.7.2016 lukien, joskin tiettyjä poikkeuksia on asetettu.

Asetus on jatkoa aiemmin voimassa olleelle direktiiville 1999/93/EY, jolla säädeltiin sähköisiä allekirjoituksia koskevista yhteisön puitteista. Direktiivin oli arvioitu edistävän sähköisten allekirjoitusmenetelmien yhteentoimivuutta, mikä loisi puitteet sähköisten allekirjoitusten sisämarkkinoille edistäen tämän teknologian käyttöä. Jo vuonna 1997 alkaneessa lainsäädäntötyössä huomioitiin, että unionin kansalaiset tulevat enenevissä määrin asioimaan toisten jäsenvaltioiden viranomaisten kanssa, mitä sähköinen asiointi sujuvoittaisi.[93] Sähköinen tunnistaminen rajat ylittävissä transaktioissa, esimerkiksi terveydenhuollossa tai verotuksessa, ei kuitenkaan yleistynyt suunnitelmien mukaisesti. Muita luottamuspalveluita on säännelty ainoastaan kansallisella tasolla ennen eIDAS-asetuksen voimaan saattamista.

Asetuksella pyritään lisäämään luottamusta sähköisiin transaktioihin tarjoamalla yhteinen pohja mm. tunnistusvälineiden ja luottamuspalveluiden varmuustasoille. Näin pyritään edelleen kehittämään sisämarkkinoita ja varmistamaan niiden toimivuus, poistamaan esteitä sähköisten palvelujen käytössä sekä varmistamaan luottamuspalvelujen riittävän korkea tietoturva. Asetuksella säädetään ehdot, joiden mukaisesti jäsenvaltioiden on tunnustettava toistensa ilmoittamat sähköisen tunnistamisen menetelmät. Sen lisäksi säädetään unioniin sijoittautuneiden luottamuspalvelujen tarjoajien vastuista ja velvollisuuksista sekä itse luottamuspalveluista.[94]

5.2 Rajat ylittävä tunnistaminen

eIDAS-asetus asettaa jäsenvaltioille velvollisuuden hyväksyä toisten jäsenvaltioiden ilmoittamat sähköisen tunnistamisen välineet julkisen sektorin elimen verkkopalvelun

---

[93] Direktiivi 1999/39/EY, johdanto

[94] eIDAS-asetus, johdanto sekä art. 1–2

käyttöön, kun kyseessä on korotetun tai korkean varmuustason tunnistusväline ja verkkopalvelu. Edellytyksenä on, että väline on myönnetty ilmoittavan jäsenvaltion toimesta tai toimeksiannosta tai niin, että jäsenvaltio tunnustaa ne.[95] Tämä mahdollistaa jäsenvaltioille harkinnan tunnistamisvälineiden myöntämisen suhteen, eli onko kyseessä valtion myöntämä väline, kuten henkilökortti, vai onko kansallinen sähköinen tunnistaminen kilpailutettu ja ulkoistettu kaupalliselle toimijalle. Mahdollista on myös, että kaupalliset toimijat tarjoavat omia ratkaisujaan valtion tunnistamisvälineiden lisäksi tai niiden sijaan.

Huomioitavaa on, että ilmoitettuja tunnistuspalveluita voi tarjota myös muiden kuin julkisen sektorin toimijoiden käyttöön, jolloin tunnistuspalvelun tarjoaja voi määrittää palvelulle erityisiä käyttöehtoja tai -maksuja. Julkiselle sektorille tunnistustapahtumia välitettäessä on rajat ylittävä todentaminen tarjottava veloituksetta.[96] Tämä ei käsitykseni mukaan kuitenkaan estä tunnistusvälineen ja tunnistamisen välityspalvelun tarjoajien välisiä sopimuksia hinnoittelusta. Esimerkiksi Suomessa yhteentoimivuusjärjestelmän kansallista solmupistettä esitetään Väestörekisterikeskuksen ylläpidettäväksi suomi.fi-tunnistamisenohjauspalvelun yhteydessä, jolloin vaikkapa pankit voisivat periä pankin ja VRK:n välisen sopimuksen mukaisen maksun VRK:lta.[97]

Rajat ylittävä tunnistaminen helpottanee työvoiman vapaata liikkuvuutta, kun unionin jäsenmaiden kansalaiset voivat asioida toisten jäsenvaltioiden viranomaisten kanssa sähköisesti jo ennen maahantuloa. Saman tunnistamismenetelmän kelpaaminen eri maissa vaikuttaa myös koettuun helppokäyttöisyyteen. Se mahdollistaa tutun ja turvalliseksi koetun käyttöliittymän käyttämisen jo aiemmin totutulla tavalla.[98]

Ilmoittava jäsenvaltio vastaa luonnolliselle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, mikäli se ei varmista varmuustasoasetuksen mukaisesti, että tunnistusvälineen haltijan yksilöintitiedot liittyvät kyseiseen henkilöön välineen myöntämisajankohtana. Käytännössä tämä saavutetaan tarkastamalla henkilötiedot väestötietojärjestelmästä tai kauppa-, yhdistys- tai säätiörekisteristä ensitunnistamisen yhteydessä. Lisäksi ilmoittava jäsenvaltio vastaa tahallisesti tai tuottamuksellisesti aiheutetusta vahingosta, mikäli se ei täytä artiklassa 7 (f) asetettuja velvoitteitaan, lähinnä julkisen sektorin tunnistustapahtumien maksuttomuutta ja kieltoa asettaa suhteettomia erityisvaatimuksia tunnistuspalvelua hyödyntäville luottaville osapuolille.[99]

---

[95] eIDAS-asetus, art. 6–7

[96] eIDAS-asetus, art. 7(f)

[97] HE 74/2016 vp, ehdotettu 42 c §

[98] Ralph, Livia (toim) 2016, s. 11–14

[99] eIDAS-asetus, art. 11(1), art. 7(f)

Sähköisen tunnistamisvälineen myöntäjä vastaa tahallaan tai tuottamuksesta aiheutetusta vahingosta, mikäli se ei varmista varmuustasoasetuksen mukaisesti, että tunnistusväline on liitetty sen haltijaan. Tunnistusvälineen myöntäjä vastaa siis ensitunnistamisen oikeellisuudesta.[100] Lisäksi tunnistuspalvelua ylläpitävä taho vastaa tahallaan tai tuottamuksellisesti aiheutetuista vahingoista, mikäli se ei pidä tietojen varmistamispalvelua yllä niin, että mikä tahansa toisessa jäsenvaltiossa oleva osapuoli kykenee varmistamaan vastaanottamansa tunnistetiedot. Muilta osin vastuun jakautuminen jätetään jäsenvaltioiden päätettäväksi kansallisessa lainsäädännössä.[101]

EIDAS-asetus ei siis sisällä tarkkoja määräyksiä vahingonkorvausvelvollisuudesta muissa kuin edellisessä kappaleessa mainituissa tapauksissa. Myöskään vahingonkorvauksen määrää ei ole säädelty. Rajat ylittävässä transaktiossa lakivalinta tehdään Rooma I -asetuksen mukaisesti, mikäli osapuolten välillä on sopimus eikä lakivalinnasta ole sovittu.

Käytännössä asiointipalvelun tarjoaja tehnee sopimuksen omassa maassaan sijaitsevan tunnistuksen välityspalvelun kanssa, joka vain välittää tunnistustiedot. Mikäli identiteettivarkaus tai petos on tapahtunut tunnistautuvan henkilön maassa, ei tunnistamiseen luottavan tahon ja tunnistusvälineen myöntäjän tai luottavan tahon ja tunnistettavan henkilön välillä ole sopimussuhdetta. Tällaisessa tilanteessa sovelletaan Rooma II -asetusta. Sovellettava laki on tällöin vahingon aiheutumismaan laki. Henkilölle, jonka identiteettiä on luvatta käytetty, aiheutuu vahinko todennäköisesti tämän kotimaassa; tunnistamiseen luottavalle taholle tämän kotimaassa.[102]

5.3 Luottamuspalvelut

Luottamuspalvelut tulevat eIDAS-asetuksen myötä pääosin EU-lainsäädännön piiriin, mikä vähentää kansallisia eroja. Sääntely koskee sähköisiä allekirjoituksia, leimoja ja aikaleimoja, verkkosivustojen todentamisvarmenteita sekä tiettyjä näihin liittyviä palveluita.[103] Tunnistuslain säädökset sähköisistä allekirjoituksista siis korvataan EU-lainsäädännöllä.

Asetuksen mukaan luottamuspalvelut jaetaan hyväksyttyihin ja ei-hyväksyttyihin palveluihin (*qualified* ja *non-qualified trust services*). Luottamuspalvelun tarjoaja vastaa kummassakin tapauksessa tahallaan tai tuottamuksesta aiheutetusta vahingosta laimin-

---

[100] eIDAS-asetus, art. 11(2)

[101] eIDAS-asetus, art. 11(3)–11(5)

[102] Rooma II -asetus, art. 4

[103] eIDAS-asetus, art. 3

lyödessään eIDAS-asetuksen velvoitteita, mutta todistustaakka jakautuu eri tavalla. Hyväksytyn luottamuspalvelun tarjoajan on todistettava, ettei vahinko ole aiheutunut sen tahallisesta tai tuottamuksellisesta laiminlyönnistä, kun ei-hyväksytyn palvelun kohdalla todistustaakka on vahingon kärsijällä.[104]

Hyväksytyille luottamuspalvelujen tarjoajille asetetaan myös muita velvollisuuksia, mm. pakollinen auditointi vähintään kahden vuoden välein sekä ilmoitusvelvollisuus valvontaviranomaiselle, joka ylläpitää luetteloa hyväksytyistä palveluntarjoajista.[105] Hyväksytyt saavat käyttää EU:n luotettavuusmerkkiä osoituksena hyväksytystä asemastaan.

Kuva 1 Luottamuspalveluja koskeva EU:n luotettavuusmerkki (EU 2015/806, liite II)

Sekä hyväksyttyjen että ei-hyväksyttyjen palveluntarjoajien on molempien toteutettava "tarvittavat tekniset ja organisatoriset toimenpiteet" hallitakseen tietoturvaan kohdistuvat riskit ja ilmoitettava tietoturvaloukkauksista valvovalle viranomaiselle, Suomessa Viestintävirastolle, sekä tarvittaessa myös asiakkailleen, 24 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta.[106] Riittävän tietoturvallisuuden vaatimus ei siis merkittävästi eroa siitä, mitä aikaisemmin on säädetty kansallisessa laissa.

Sähköisten allekirjoitusten osalta säädetään nyt yleiseurooppalaisella tasolla, että sähköinen allekirjoitus on yhtä vahva kuin käsin kirjoitettu allekirjoitus. Samaten jäsenvaltion on hyväksyttävä muiden maiden ilmoittamat sähköiset allekirjoitusmenetelmät mikäli se tarjoaa julkisia verkkopalveluita omille kansalaisilleen.[107]

---

[104] eIDAS-asetus, art. 13

[105] eIDAS-asetus, art. 20–21

[106] eIDAS-asetus, art. 19

[107] eIDAS-asetus, art. 25, 27

Oikeushenkilöt eivät kuitenkaan enää voi luoda sähköisiä allekirjoituksia, sillä asetuksen määritelmän mukaisesti sähköinen allekirjoitus liittyy aina allekirjoittajaan, joka puolestaan on aina luonnollinen henkilö. Sen sijaan oikeushenkilöille voidaan myöntää sähköisiä leimoja, joilla voidaan todeta asiakirjan sisällön pysyneen muuttumattomana ja lähteen olevan kyseinen organisaatio.[108] Käytännössä samat tekniset menetelmät soveltuvat sähköisiin allekirjoituksiin ja leimoihin, ero tuntuu olevan lähinnä terminologinen.

5.4 Varmuustasot

EIDAS-asetus määrittelee sähköisille tunnistus- ja luottamuspalveluille tietyt tietoturvallisuuden varmuustasot, joita käyttämällä taataan yhteismitallinen tapa palveluiden tietoturvan varmistamiseen Euroopan unionin sisärajat ylittävissä tapahtumissa. Näin tunnistuspalvelun tarjoaja voi tietyt, varmuustasoasetuksessa tarkemmin määritellyt kriteerit täyttämällä varmistua palvelunsa käyttökelpoisuudesta viranomaistunnistautumiseen koko unionin alueella.

Varmuustasoja ovat *matala*, *korotettu* ja *korkea* (vastaavasti *low*, *substantial* ja *high*, parempi käännös olisikin mielestäni ollut matala, merkittävä ja korkea). Mille tasolle sähköisen tunnistamisen järjestelmä asettuu, määritellään arvioimalla tunnistuspalvelun rekisteröinnin, tunnistamisen menetelmien hallinnan, todentamisen sekä hallinnon ja organisaation luotettavuutta ja laatua arvioimalla.[109]

Viestintävirasto on ehdottanut, että voimassa olevan tunnistuslain mukaiset vahvat sähköisen tunnistamisen ja allekirjoittamisen palvelut katsottaisiin vähintään korotetun varmuustason palveluiksi automaattisesti, sillä ensitunnistamista ja todentamista on säädelty tarkasti myös tunnistuslaissa. Ehdotus selkeyttäisi vanhan lain säädösten mukaisesti myönnettyjen välineiden asemaa siirtymäaikana ja mahdollistaisi uusien, eIDAS-varmuustasojaottelun mukaisten tunnistusvälineiden sähköisen hakemisen jo 1.7.2016 alkaen, jolloin eIDAS-asetuksen määräykset astuvat voimaan.[110]

Varmuustasot kuvaavat, kuinka luotettavasti tunnistautuvan henkilön todellinen ja väitetty identiteetti on sama. Jäsenvaltioissa sovellettavien erilaisten käytäntöjen vuoksi tarvitaan jäsenvaltioille yhteinen tapa arvioida sähköisen tunnistamisen palveluiden sekä luottamuspalveluiden luotettavuutta.

---

[108] eIDAS-asetus, art. 3, 36

[109] eIDAS-asetus, art. 8; varmuustasoasetus, art. 1

[110] Viestintävirasto 2016, s. 21–22

Kun yhteinen arviointitapa on olemassa, on näihin palveluihin luottavien tahojen helppo päättää, kuinka turvallisen välineen johonkin palveluun kirjautumiseen tai jonkin asiakirjan sähköiseen allekirjoittamiseen tarvitaan. Jäsenvaltion viranomaisen ylläpitämään asiointipalveluun on jatkossa voitava kirjautua myös toisen valtion ilmoittaman tunnistuspalvelun avulla, kunhan sen varmuustaso on vähintään yhtä korkea kuin millä jäsenvaltion omat kansalaiset voivat palveluun kirjautua. Sama pätee myös sähköisiin allekirjoituksiin ja leimoihin.

Suomessa toimivaltainen valvontaviranomainen tulee olemaan Viestintävirasto. Sen tuleva määräys koskien tunnistus- ja luottamuspalveluita on parhaillaan lausuntokierroksella. Tuleva määräys 72 tulee olemaan linjassa eIDAS-asetuksen ja sen täytäntöönpanoasetusten kanssa. Määräys asettaa tiettyjä edellytyksiä niin tunnistus- ja luottamuspalveluiden tarjoajille kuin myös arviointi- ja sertifiointilaitoksille, jotka arvioivat tunnistus- ja luottamuspalveluita ja niiden tarjoajia. Nämä vaatimukset ovat suurelta osin viittauksia komission täytäntöönpanoasetuksiin sekä kansainvälisiin standardeihin, mutta sisältävät myös tarkempia määräyksiä mm. tietoturvaloukkausten raportoinnista.

Tietoturvallisuuden varmuustasojen osalta määräyksessä asetetaan kriteerit korotetulle tasolle rekisteröitävistä tunnistuspalveluista. Korkean varmuustason palveluista on tarkoitus antaa erillinen suositus. Tunnistuspalvelun tarjoaja ja auditointilaitos määrittelevät, mille tasolle jokin tunnistuspalvelu voidaan ilmoittaa. Viestintävirasto valvoo toimijoita toimivaltaisena valvontaviranomaisena.[111]

[111] Viestintävirasto MPS 72 luonnos, s. 7, 21–23

6 SUUNNITELLUT MUUTOKSET

6.1 Valtionhallinnon yhteisten sähköisen asioinnin tukipalvelujen muutos

Sähköisen asioinnin osuutta on jo pitkään pyritty kasvattamaan viranomaisasioinnissa. Hallitus on 19.4.2016 ilmoittanut eduskunnalle esityksestään laiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista, jolla pyritään parantamaan julkisia sähköisiä palveluita ja edistämään hallinnon tehokkuutta ja tuottavuutta.[112] Esitys mahdollistaa kansallisen palveluarkkitehtuurimallin mukaisen toiminnan siirtämällä useita tukipalveluita, mm. viestinvälitys- ja tunnistuksenohjauspalvelut, Väestörekisterikeskuksen vastuulle.

Nämä tukipalvelut liittyvät niin sanottuun palveluväylään, jota valmistellaan osana kansallista palveluarkkitehtuuriohjelmaa (KaPa-ohjelmaa). Palveluväylässä sekä julkisorganisaatiot että yksityiset yritykset voivat hakea tietoja useista viranomaisrekistereistä. Näin on mahdollista luoda asiointipalvelu, johon haetaan sekä palvelua ylläpitävän että toisten viranomaisten rekistereissä olevia tietoja, esimerkiksi Kelan etuuksia haettaessa hakemuslomakkeelle voisi automaattisesti hakea Verohallinnolta viimeisen vahvistetun verotuksen tiedot. Eri viranomaisten palveluita pyritään myös keskittämään yhteen uuteen portaaliin ns. palvelunäkyminä, jolloin asiointipalvelut ovat saavutettavissa yhdessä paikassa, korvaten nykyisen suomi.fi-palvelun. [113]

Kustannussäästöt ovat yksi suurimmista lakiesityksen perusteluista. Esimerkiksi Kela laskee säästävänsä vähintään 5 euroa jokaisessa asiointitapahtumassa joka suoritetaan verkossa henkilökohtaisen käynnin tai puhelinsoiton sijaan.[114] Kuitenkin Valtiontalouden tarkastusvirasto on todennut julkisrahoitteisten ICT-projektien hallintomallien olevan usein sekavia, palvelutuotannon ohjauksen puutteellista ja että useita samankaltaisia projekteja on rahoitettu julkisin varoin. Kustannus-hyötylaskelmat ovat olleet puutteellisia tai perustuneet virheellisiin tietoihin ja sähköisten palveluiden kehittämiseen käytetyt rahat ovat säännönmukaisesti ylittäneet budjetoidun.[115] Hallituksen esityksessäkin mainittu viiden euron säästö asiointitapahtumaa kohden on todettu vahvasti arvioon perustuvaksi. Yhden nykyisen viestinvälityspalvelun, kansalaisen asiointitilin, kautta lähetetyn viestin hinnaksi VTV laskee 17 euroa, kun suunnitellut käyttöhinnat olivat

---

[112] HE 59/2016 vp, s. 1

[113] Valtiovarainministeriö 2015

[114] HE 59/2016 vp, s. 22

[115] VTV 2016

enintään 0,35 €/viesti + kirjautumiskustannukset, 0,10–0,15 euroa käyntikertaa kohden.[116]

Saatavia säästöjä laskettaessa on otettava huomioon, että myös sähköisten palveluiden ylläpito maksaa. Palvelujen siirtyminen sähköisiksi ei siis välttämättä aiheuta kustannussäästöjä, vaan saattaa vain siirtää kustannusten kohdistumista asiantuntijatehtäviin suoran asiakaspalvelun sijaan.[117]

Kansalaisen asiointitili suunnitellaan korvattavaksi Suomi.fi-portaalin viestinvälityspalvelulla, jonka kautta viranomaiset voisivat turvallisesti lähettää viestejä kansalaisille. Tätä varten esitetään 11 §:ssä perustettavaksi rekisteri sähköistä tiedoksiantomenettelyä koskevista suostumuksista. Tähän rekisteriin voisi tallentaa yleisen suostumuksen sähköiseen tiedoksiantomenettelyyn, jolloin jokaisen viranomaisen ei tarvitsisi kysyä lupaa erikseen omassa asiointipalvelussaan.

Julkishallinnolla on tuotantokäytössä kaksi luonnollisen henkilön tunnistamisenohjauspalvelua: tunnistus.fi ja Vetuma (verkkotunnistaminen ja -maksaminen). Tunnistus.fi on Kansaneläkelaitoksen, Työ- ja elinkeinoministeriön ja Verohallinnon yhteinen palvelu. Vetuma on puolestaan Valtion tieto- ja viestintäkeskus Valtorin ylläpitämä portaali, jonka käyttäjiksi valtion ja kuntien organisaatiot voivat liittyä.[118] Pääperiaate molemmissa on sama: käyttäjä tunnistautuu pankkitunnuksillaan tai henkilökortillaan tunnistuspalveluun, josta henkilötiedot siirretään edelleen käyttäjän tahtomaan palveluun.

Luonnollisten henkilöiden tunnistamista ollaan hallituksen esityksen myötä siirtämässä Väestörekisterikeskuksen vastuulle siten, että Vetuma ja tunnistus.fi siirretään VRK:lle ja käyttäjät siirretään uuteen palveluväylän yhteydessä ylläpidettävään suomi.fi -tunnistusportaaliin. Maksamisen palvelu kuitenkin siirtyisi Valtiokonttorin vastuulle. Vetuma-portaalissa jokainen sitä käyttävä taho on joutunut tekemään erilliset sopimukset tunnistuspalvelun tarjoajien kanssa, joka on kasvattanut merkittävästi sopimushallinnan kustannuksia. Uudessa mallissa VRK tekee sopimuksen koko hallinnon puolesta, jonka oletetaan johtavan kustannussäästöihin.[119]

Käyttäjän kokemuksen kannalta järjestelmien yhdistäminen parantanee helppokäyttöisyyttä hieman, mutta erityisesti eri viranomaisten palveluiden välisen liikkumisen mahdollistava vahvan tunnistamisen kertakirjautumispalvelu tulee yksinkertaistamaan asiointia silloin, kun on asioitava useiden viranomaisten, esim. Kelan ja asuinkunnan sosiaalitoimiston, kanssa.[120] Kertakirjautumisen mahdollistaminen saattaa pienentää

---

[116] VTV 2016, s. 41–42, 37, 48

[117] Voutilainen 2009, s. 48

[118] Tunnistus.fi 2015; Suomi.fi 2015

[119] HE 59/2016 vp, s. 18, 22, 39

[120] HE 59/2016 vp, s. 37

vahvojen sähköisten tunnistamisten määrää, joka puolestaan voi johtaa tunnistuspalveluiden hintojen korotuspaineisiin.

Suunnitteilla on palveluväylään ja edellä kuvattuun tunnistamismalliin liittyvä rooli- ja valtuutushallintapalvelu, jonka avulla voisi aluksi helposti hakea tiedon mm. alaikäisen huoltajuudesta tai kaupparekisteriin merkitystä oikeudesta yrityksen nimen kirjoittamiseen. Myös organisaatioiden tunnistamiseen ja valtuutushallintaan kehitetty Verohallinnon ylläpitämä KATSO-tunnistuspalvelu siirtyisi VRK:n vastuulle vuoden 2017 alussa, ja suunnitellaan kokonaan lakkautettavaksi kun edellytykset sen sulauttamiseksi tunnistuspalvelun ja asiointivaltuutuspalvelun yhdistelmään ovat olemassa.[121]

Rooli- ja valtuutushallintapalvelua varten ehdotetaan esitetyssä 10 §:ssä Väestörekisterikeskuksen ylläpidettäväksi uutta viranomaisrekisteriä tätä tarkoitusta varten. Asiointivaltuutusrekisterin tietoihin voisi luottaa vahvasti, sillä valtiolla olisi ankara vastuu rekisterin virheellisestä toiminnasta.

Hallituksen esityksessä yrityksen tunnistamisen esitetään hoituvan joko KATSO-tunnusten tai luonnollisen henkilön tunnistuspalvelun ja asiointivaltuutuspalvelun avulla.[122] EIDAS-asetuksen mukaista, myös kansalliseen lainsäädäntöön suunniteltua oikeushenkilön vahvaa sähköistä tunnistusvälinettä ei ole käsitelty lainkaan.[123] Lakiesityksen suurin anti sähköisen tunnistamisen osalta onkin KaPa-ohjelman mukaisen mallin tuominen lainsäädäntöön, mikä mahdollistaa kertakirjautumisen yhdistämisen vahvaan sähköiseen tunnistamiseen. Sillä, mikä viranomainen on vastuussa palvelun tuottamisesta, on palvelun loppukäyttäjän kannalta vähäinen merkitys.

Iso-Britanniassa on henkilökorttiohjelman lopettamisen jälkeen kehitetty Suomen luonnollisten henkilöiden tunnistusportaalia vastaavaa palvelua, nimeltään GOV.UK Verify. Kyseessä on tunnistamisen välityspalvelu, jonka avulla voi kirjautua tiettyjen yhtiöiden myöntämillä tunnistusvälineillä niihin julkishallinnon verkkopalveluihin, jotka ovat ottaneet GOV.UK Verifyn käyttöön. Suurin ero Suomeen on, että valtio ei tarjoa omaa tunnistusvälinettä käytettäväksi, vaan kaikki tunnistusvälineiden tarjoajat ovat kaupallisia yrityksiä, eikä valtio ylläpidä keskitettyä väestötietorekisteriä. Itse asiassa keskitetyn rekisterin puute on yksi kansalaisille esitetyistä perusteista, miksi palvelu on niin turvallinen. GOV.UK Verify -tunnistuksenohjauspalvelu tulee myös olemaan eIDAS-asetuksen mukainen kansallinen yhteyspiste unionin sisärajat ylittävään tunnistautumiseen.[124]

---

[121] HE 59/2016 vp, s. 12, 19, 37–39

[122] HE 59/2015 vp, s. 39

[123] Oikeushenkilön vahvasta tunnistamisesta katso luku 6.3.2

[124] Government Digital Service 2016; Walker & Rea 2014; Hughes 2014a

Keskitetyn väestötietorekisterin puutteesta johtuen julkishallinnon verkkopalvelujen käyttäjän tunnistaminen on monimutkaisempaa. Iso-Britanniassa ratkaisuksi on muodostunut identiteettipalvelun tarjoajien kilpailuttaminen määräajoin, jolloin kansalaiset voivat valita haluamansa palveluntarjoajan kilpailutuksen voittaneista 3–10 yrityksestä. Näiden yritysten on tiettyjen kriteerien puitteissa tarkistettava hakijan henkilöllisyys erilaisista todistuksista ja asiakirjoista, kuten passista, valokuvasta ja tiliotteesta, joiden aitous varmennetaan. Kun yritys on riittävällä varmuudella todennut henkilöllisyyden olemassaolon, on sen vielä varmistuttava, että hakija on se henkilö, joka väittää olevansa, toisin sanoen on varmistuttava käyttäjän identiteetin sekä identiteetin todentamisen luotettavuudesta.[125]

6.2 Uusi henkilökorttilaki

Henkilökorttilakia ollaan parhaillaan uudistamassa ja asiaan liittyen on 7.4.2016 annettu hallituksen esitys uudeksi henkilökorttilaiksi. Lain on tarkoitus tulla voimaan vuoden 2016 loppupuolella.[126] Muutoksen jälkeen henkilökorttia olisi mahdollista hakea täysin sähköisesti aiemmin myönnetyllä vahvalla sähköisen tunnistamisen välineellä, sekä henkilökohtaisesti Poliisin lisäksi myös Suomen edustustoissa ulkomailla. VRK:n myöntämän kansalaisvarmenteen tunnistamis- ja allekirjoitusavaimet säilytettäisiin henkilökortilla ainakin toistaiseksi, sillä tunnistusvälinemarkkinat eivät ole auenneet kilpailulle toivotulla tavalla, eikä kansalaisvarmenne ole sidoksissa asiakkuuteen minkään kaupallisen yhtiön kanssa. Lisäksi sisäministeriö uskoo, että ainakin kansalaisvarmenne ilmoitetaan eIDAS-asetuksen mukaisesti rajat ylittävän sähköisen asioinnin keinoksi.[127]

Uusi täysin sähköinen hakemusmenettely yhdistettynä esitettyyn tunnistuslain muutokseen. Tämän jälkeen ajokorttia ei voi enää käyttää ensitunnistamisen välineenä vahvaa sähköistä tunnistusvälinettä haettaessa, mikä saattaa kasvattaa henkilökortin tällä hetkellä melko pientä suosiota. Poliisi myönsi 2013 ja 2014 noin 135 000 henkilökorttia vuodessa.[128]

Esitetyn henkilökorttilain mukaan Kelalta saatavia sairausvakuutustietoja ei enää voisi sisällyttää henkilökortille. Muutosta perustellaan sairasvakuutustietojen mahdollisuudella muuttua lyhyessäkin ajassa henkilön muuttaessa ulkomaille tai takaisin Suo-

---

[125] Hughes 2014b; Cabinet Office 2014, s. 29–37

[126] HE 41/2016 vp, s. 1

[127] HE 41/2016 vp, s. 14–15, 18, 24

[128] HE 41/2016 vp, s. 5

meen. Myös lääkkeiden erityiskorvattavuudet voivat muuttua. Lisäksi apteekit ovat vuodesta 2013 voineet saada Kela-kortin tiedot sähköisen kyselypalvelun avulla, joten fyysisen kortin tarve on vähentymässä. Sairausvakuutustietojen merkintämahdollisuuden poistamisen odotetaan pienentävän henkilökortin myöntämisen viivettä ja pienentäen Kelan hallinnollista työtä, pienentäen kustannuksia.[129]

Henkilökorttiin liittyvä keskustelu on sikäli mielenkiintoinen, että Virossa ja Iso-Britanniassa on päädytty henkilökorttien osalta täysin poikkeaviin ratkaisuihin. Iso-Britanniassa päätettiin vuonna 2002 ottaa käyttöön henkilökortit ja niihin liittyvä kansallinen henkilörekisteri, joka näyttäisi vastaavan Suomen väestötietorekisteriä, tietosisällön ollessa lähinnä nimi, osoite, sukupuoli, ikä, syntymäpaikka ja kansallisuus. Kortteja pystyi hankkimaan marraskuusta 2009 alkaen, mutta jo toukokuussa 2010 valtio ilmoitti, että henkilökortteihin liittyvä ohjelma lopetetaan ja olemassa olevat kortit mitätöidään.[130]

Virossa puolestaan jokaisella 15 vuotta täyttäneellä kansalaisella sekä jokaisella Virossa asuvalla EU-kansalaisella on oltava valtion myöntämä henkilökortti, joka on voimassa enintään viisi vuotta. Valtion myöntämä varmenne voidaan tallentaa henkilökortin lisäksi myös SIM-kortille, jolloin sitä voidaan käyttää Suomessa operaattorien ylläpitämän mobiilivarmenteen tavoin. Digitaalinen henkilökortti voidaan myöntää myös ulkomaiselle, Viron ulkopuolella asuvalle henkilölle tämän hakemuksesta, jos tällä on yhteys Viron valtioon tai hän haluaa käyttää Viron tarjoamia sähköisiä palveluita, kuten asiakirjojen sähköistä allekirjoitusta.[131]

6.3 Uusi muutos tunnistuslakiin

6.3.1 eIDAS-yhteensopivuus

Hallitus on 10.5.2016 antanut esityksen muutoksesta tunnistuslakiin.[132] Tarkoituksena on sovittaa kansallinen lainsäädäntö yhteen sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annettuun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (ns. eIDAS-asetus) kanssa.[133]

---

[129] HE 41/2016 vp, s. 8, 18, 25–26

[130] BBC News 2010; UK Identity Cards Act, art. 1–3

[131] Estonian Identity Documents Act, § 5–6 , § 20–20[6]

[132] HE 74/2016 vp

[133] HE 74/2016 vp, s. 5

Koska eIDAS-asetus on jäsenvaltioissa suoraan sovellettavaa oikeutta ja siihen sisältyy säännöksiä myös sähköisistä allekirjoituksista, ehdotetaan sähköistä allekirjoitusta koskeva osuus kumottavaksi tunnistuslaista. Koko lain nimi muutettaisiin laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (vrt. laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista).[134]

Tunnistuspalvelun tarjoajalle asetetut vaatimukset määritettäisiin sähköisen tunnistamisen varmuustasoasetuksen mukaiselle korotetulle tasolle. Tämä helpottaa tunnistuspalvelun tarjoajien hallinnointitaakkaa, mikäli he ilmoittavat tunnistusvälineensä myös rajat ylittävän tunnistamisen välineeksi. Myös käyttäjien kannalta yhdenmukaiset kriteerit selkeyttävät tilannetta ja lisäävät helppokäyttöisyyttä. Kansallisilla markkinoilla toimittaessa varmuustasojen määrittely EU-oikeudessa kuitenkin monimutkaistaa sääntelyä nykytilaan verrattaessa.[135]

Lakiehdotuksessa annetaan Väestörekisterikeskukselle tehtäväksi ylläpitää Suomen ja muiden EU-jäsenvaltioiden välistä kansallista solmupistettä, jolla mahdollistetaan toisten jäsenmaiden ilmoittamien tunnistamisvälineiden käyttäminen viranomaisasioinnissa Suomessa, ja vastaavasti Suomen ilmoittamien välineiden käyttö toisissa jäsenvaltioissa. Ehdotetussa toimintatavassa toisesta jäsenvaltiosta saatu sähköinen identiteettitieto muunnetaan solmupisteessä kansalliseen muotoon ja välitetään KaPa-hankkeen tunnistuspalvelun kautta viranomaiselle, jonka palvelua tahdotaan käyttää.[136]

6.3.2 Oikeushenkilöiden tunnistamisvälineet

Tällä hetkellä vahvan sähköisen tunnistusvälineen voi myöntää ainoastaan luonnolliselle henkilölle (tunnistusL 2 §, 20 §). Lakiehdotuksessa on kuitenkin mahdollistettu vahvan sähköisen tunnistusvälineen myöntäminen myös oikeushenkilölle, kunhan oikeushenkilön tiedot tarkastetaan yritys- tai yhteisörekisteristä.[137] Vaatimus perustuu eIDAS-asetukseen, jossa sähköisellä tunnistamisella voidaan yksilöidä joko luonnollinen henkilö, oikeushenkilö tai oikeushenkilöä edustava luonnollinen henkilö.[138]

Käytännössä on vielä epäselvää, kuinka oikeushenkilöiden tunnistusvälineitä hallinnoitaisiin. Esitetyn 20 §:n mukaan "Luonnollisen henkilön ja oikeushenkilön tunnistusvälineiden kytkös on toteutettava sähköisen tunnistamisen varmuustasoasetuksen liit-

---

[134] HE 74/2016 vp, s. 14–15, 54

[135] HE 74/2016 vp, s. 29

[136] HE 74/2016 vp, s. 14, 16–17

[137] HE 74/2016 vp, s. 56

[138] eIDAS-asetus, art. 3

teen kohdan 2.1.4 mukaisesti. Tunnistusvälineen on oltava henkilökohtainen." Mikäli oikeushenkilön vahva tunnistusväline annetaan vain yhden luonnollisen henkilön käyttöön, ei tilanne asiallisesti muutu siitä, että luonnollisen henkilön tunnistusvälineelle olisi tallennettu tieto oikeudesta edustaa oikeushenkilöä. Jos tunnistusväline puolestaan on useamman luonnollisen henkilön käytössä, ei oikeushenkilöä edustavaa luonnollista henkilöä voida todentaa tunnistustapahtuman yhteydessä.

Oikeushenkilönkin tunnistusvälineen tulee täyttää vaatimus vähintään kahdesta eri todentamistekijästä: jotain, mitä haltija tietää; jotain, mitä haltijalla on hallussaan; sekä jostain yksilöivästä ominaisuudesta, esim. sormenjäljestä.[139] Oikeushenkilön kohdalla viimeistä kriteeriä ei ole mahdollista täyttää, joten tunnistamismenetelmän on pohjauduttava johonkin fyysiseen laitteeseen, kuten toimikorttiin tai avainlukulistaan, sekä salasanaan, käyttäjätunnukseen tai näiden yhdistelmään.

Tällainen oikeushenkilön tunnistusväline tarjoaisi mahdollisen välinekohtaiseen valtuuttamiseen, jolloin tietyn välineen haltijalla olisi oikeus edustaa oikeushenkilöä tietyissä asioissa, jotka voitaisiin määritellä välineen teknisissä tiedoissa. Välineeseen liittyvä kelpoisuus pysyy voimassa vaikka henkilöstö yrityksessä vaihtuisikin.[140] Luonnolliseen henkilöön sitomattoman, oikeushenkilön tunnistusvälineen käyttöhallinta voisikin riittää asemavaltuutuksen syntymiseen.[141]

Verohallinto on kuitenkin lausunnossaan todennut, että tunnistusvälineen omistavan organisaation ja välinettä käyttävän luonnollisen henkilön välillä tulisi olla yhteys, ja esittää edustusoikeuden tarkastamista säännöllisesti tai tunnistustapahtuman yhteydessä.[142] Käytännössä Verohallinnon esittämä kytkös rajoittaisi oikeushenkilön tunnistusvälineiden käyttämisen ainoastaan kaupparekisterin (tai vastaavan) mukaisille nimenkirjoittajille ja estäisi asemavaltuutuksella toimimisen. Myös työ- ja elinkeinoministeriö on lausunnossaan kiinnittänyt huomiota oikeushenkilölle myönnettävää tunnistusvälinettä koskeviin epäselvyyksiin.[143]

Myös Iso-Britanniassa voimassa oleva Good Practice Guide toteaa, että yhteisöt eivät voi toimia omasta puolestaan, vaan niiden puolesta toimii aina joku valtuutettu henkilö. Suositus toteaakin, että yhteisön tunnistamisessa tulee tunnistaa sen puolesta toimiva luonnollinen henkilö ja todeta tämän oikeus edustaa oikeushenkilöä.[144]

---

[139] HE 74/2016 vp, s. 57

[140] Ponka 2013, s. 277–280

[141] vrt. Ponka 2013, s. 283

[142] Verohallinto 2016, s. 2

[143] Työ- ja elinkeinoministeriö 2016, s. 2

[144] Cabinet Office 2013

Oikeushenkilöiden tunnistusvälineiden sääntelyä tulisikin selventää. Joko lakiin tulisi selvästi kirjata, että oikeushenkilölle myönnettyä vahvaa sähköistä tunnistusvälinettä saa käyttää ainoastaan luonnollinen henkilö, jolla on viranomaisrekisteriin merkitty oikeus edustaa yhteisöä ja tämän luonnollisen henkilön henkilöllisyys on tarkistettava, kun oikeushenkilön tunnistusvälinettä käytetään; tai että oikeushenkilön tunnistusvälinettä käytettäessä ei tarvitse tunnistaa sitä käyttävää luonnollista henkilöä.

Ensimmäisen vaihtoehdon puolesta ovat ottaneet kantaa Verohallinto sekä työ- ja elinkeinoministeriö.[145] Myös lakiesityksen 20 §:ssä viitataan luonnollisen henkilön ja oikeushenkilön väliseen kytkökseen, joka olisi tehtävä EU:n sähköisen tunnistamisen varmuusasetuksen mukaisesti. Tämä kytkös tulisi varmentaa luotettavasta lähteestä, kuten PRH:n yritys- tai yhteisörekisteristä, ja kytkös pitäisi olla mahdollista siirtää luonnolliselta henkilöltä toiselle kansallisesti hyväksyttyjen menettelyjen mukaisesti. Mitä nämä kansallisesti hyväksytyt menettelyt tulevat olemaan, ei ole vielä tiedossa, sillä hallituksen esityksessä todetaan, että menettelytarpeita on vaikea ennakoida, eikä lakiin siksi ehdoteta tarkempia säännöksiä. Myöskään Viestintäviraston ehdotettuun määräykseen 72 ei sisälly tarkentavia ohjeita.[146]

Myös Euroopan komissio suosittaa, että oikeushenkilöiden sähköisiin leimoihin rakennetaan hallintamekanismi, jolla varmistetaan, että vain sallitut henkilöt voivat käyttää leimaa. Tarkempaa toteutustapaa kytköksen suorittamiseen ei kuitenkaan esitetä edes eIDAS expert groupin julkaisemassa turvallisuustasoja koskevassa ohjeistuksessa.[147]

Toinen vaihtoehto puolestaan mahdollistaisi yhteisön edustamisen asemavaltuutuksella, kunhan oikeustoimilain 10.2 § edellytykset asemavaltuutukselle täyttyvät. Käytännössä vastapuolella ei kuitenkaan olisi mahdollisuutta tietää, kuka sähköistä tunnistetta käyttää. Välineen oikeudetonta käyttöä koskevaa tunnistuslain 27 § ei esitetä muutettavaksi, jolloin tunnistusvälineen haltija, tässä tapauksessa oikeushenkilö, vastaa välineen oikeudettomasta käytöstä vain, jos hän on luovuttanut tunnistusvälineen toiselle, toiminut huolimattomasti tavalla, joka ei ole lievää, tai jättänyt ilmoittamatta katoamisesta kohtuullisessa ajassa.

Jälkimmäisessä vaihtoehdossa tulee tarkasteltavaksi kysymys, onko oikeushenkilön tunnistusväline luovutettu toiselle, jos se on yrityksen tietyn osaston työntekijöiden käytettävissä. Mielestäni ei, sillä yritystä edustaa aina luonnollinen henkilö, ja vastakkainen näkökulma tarkoittaisi, että yritys vastaisi aina tunnistusvälineen oikeudettomasta käytöstä. Vaikka luovutuksen toiselle katsottaisiin tapahtuvan vain, jos tunnistusväline luo-

---

[145] Verohallinto 2016; Työ- ja elinkeinoministeriö 2016

[146] HE 74/2016 vp, s. 33, 60; Viestintävirasto MPS 72 luonnos

[147] eIDAS expert group 2016, s. 16–17; Euroopan komissio 2016

vutetaan organisaation ulkopuolelle, esim. entisen työntekijän mahdollisuutta käyttää tunnistetta ei poisteta, jää näyttötaakka luvattomasta käytöstä kuitenkin tunnistusvälineen haltijalle.

Toisaalta, nykyisin voimassaolevan tunnistuslain 40 § mukaisesti, oikeushenkilö vastaa aina sille myönnetyn, laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen luomistietojen luvattomasta käytöstä siihen asti, että pyyntö varmenteen peruuttamisesta on saapunut perille. Vastaavan rajoituksen sisällyttäminen 27 §:ään selkeyttäisi oikeushenkilöille myönnettävien tunnistusvälineiden vastuun jakautumista, riippumatta siitä, onko tunnistusväline kytketty luonnollisen henkilön tunnistusvälineeseen vai ei.

6.3.3 Auditointi

Lakiesitys sisältää kokonaisen uuden luvun vaatimustenmukaisuuden arvioinnista, kun voimassaolevassa laissa tarkastuslaitos mainitaan vain yhtenä vaihtoehtona turvallisen sähköisen allekirjoituksen luomisvälineen vaatimusten täyttämisen todistamisesta ja määritellään tällaisena arviointilaitoksena toimimisen edellytykset (tunnistusL 28–29 §). Uusi vaatimustenmukaisuuden arviointi perustuu eIDAS-asetukseen ja kattaa luottamuspalvelut sekä tunnistuspalvelut.[148]

Tunnistuspalvelun tulisi osoittaa vaatimustenmukaisuus joko sisäisen, riippumattoman arvioinnin tai ulkoisen arviointilaitoksen tekemällä arvioinnilla. Sisäinen tarkastus riittäisi, mikäli tunnistuspalvelun tarjoaja tarjoaa palveluitaan ainoastaan kansallisessa luottamusverkostossa, ja eIDAS-asetuksen mukaisesti rajat ylittävään tunnistamiseen käytettävän järjestelmän auditointivaatimuksista säädetään EU:n asetuksessa. LVM kuitenkin arvioi, että EU:lle ilmoitettava tunnistusjärjestelmä edellyttää ulkoisen arviointielimen arviointia, vaikka maininta tästä onkin otettu pois lopullisesta hallituksen esityksestä.[149]

Nykyisessä laissa ei aseteta tällaista auditointivaatimusta tunnistuspalvelun tarjoajille, vaan annetaan valvontavastuu Viestintävirastolle. Viestintävirastolle tehtävässä ilmoituksessa toiminnan aloittamisesta tunnistuspalvelun tarjoaja on antanut tiedot mm. tunnistuksen ja tietoturvallisuuden periaatteista, ja Viestintävirasto on tämän ilmoituksen perusteella arvioinut palvelun lainmukaisuuden. Muutoksista on ilmoitettava vähintään kuukautta ennen muutoksen voimaantuloa, ja selvitys tarjottujen palvelujen laajuu-

---

[148] HE 74/2016 vp, s. 35–36

[149] HE 74/2016 vp, s. 36; LVM 2016, s. 26–27

desta, sisältäen tilastoinnin havaituista ongelmista, on annettava valvontaviranomaiselle vuosittain.[150]

Auditointivaatimusta ei lakiesityksestä annetuissa lausunnoissa sinällään kritisoida, vaan pidetään jopa suotavana, mutta esille tuodaan huoli kasvavista kuluista sekä ainakin tässä vaiheessa epäselvistä vaatimuksista. Viestintävirasto tuo myös esille mahdollisuuden, että eIDAS-asetuksen mukaisesti ilmoitettua korkean tason tunnistusvälinettä haetaan ei-ilmoitetulla tunnistusvälineellä, jonka auditointi suoritetaan sisäisen tarkastuslaitoksen toimesta. Tällainen tilanne ei edistäisi tietoturvaa.[151] Ulkopuolisten vaatimustenmukaisuuden tarkastuslaitosten tarkastukset saattavat kasvattaa luottamusta sähköiseen tunnistamiseen jos se markkinoidaan loppukäyttäjille tehokkaasti.

6.3.4 Luottamuspalvelut

Koska luottamuspalveluja, eli sähköisiä allekirjoituksia, leimoja, aikaleimoja ja verkkotunnusten varmenteita säädellään vastaisuudessa eIDAS-asetuksella, ehdotetaan tunnistuslaista kumottavaksi sähköisiä allekirjoituksia koskeva sääntely. Vastuukysymykset ratkaistaan kuitenkin edelleen kansallisen lainsäädännön mukaisesti, josta syystä lakiin ehdotetaan lisättäväksi uusi 4 a luku, jonka sisältämien säännösten avulla hyväksytyllä varmenteella varmennettavan kehittyneen sähköisen allekirjoittamisen vastuut jakautuvat kuten nytkin. Myös sähköiset leimat on teknisen samankaltaisuuden vuoksi otettu sääntelyn piiriin.[152]

Muutos ehkäisisi päällekkäistä sääntelyä ja yhdessä eIDAS-asetuksen kanssa helpottaisi muihin jäsenvaltioihin sijoittuneiden luottamuspalveluiden tarjoajien pääsyä Suomen markkinoille sääntelyn ollessa samanlaista. Toisaalta hakijoiden henkilötiedot on joka tapauksessa tarkastettava kansallisista rekistereistä, joten suurta muutosta markkinatilanteessa tuskin tapahtuu, ja loppukäyttäjän näkökulmasta hyödyt jäänevät pieniksi.

Vaikka esitetty 4 a luku onkin otsikoitu *"Luottamuspalveluita koskevia säännöksiä,"* sen kolmesta pykälästä kaksi ensimmäistä koskivat vielä luonnosvaiheessa vain sähköisiä allekirjoituksia. Viimeisessä, ehdotetussa 41 §:ssä todetaan, että luottamuspalvelun tarjoajan vastuusta säädetään eIDAS-asetuksessa, ja muilta osin noudatetaan vahingonkorvauslakia. eIDAS-asetuksen 13. artiklan säännökset ovat kuitenkin hyvin yleisellä tasolla, kuten jo aiemmin on kuvattu. Lopullisessa hallituksen esityksessä tunnistusla-

---

[150] Viestintävirasto 7 B/2009 M, 2 §, 4–5 §; Viestintävirasto MPS 7, kohta 3.5 5 § Vuosiraportti

[151] Viestintävirasto 2016, s. 11–13; myös mm. Elinkeinoelämän keskusliitto 2016; Nordea 2016; OP Osuuskunta 2016

[152] HE 74/2016 vp, s. 8, 40–41; LVM 2016, s. 31

kiin ehdotetaankin tarkemmin säädeltäväksi myös sähköisten leimojen luvaton käyttö, sillä ne vastaavat teknisesti sähköisiä allekirjoituksia.

Kuvitellaan tilanne, jossa hyväksytty luottamuspalvelun tarjoaja on myöntänyt sähköisen leiman A Oy:lle. Työntekijä X, joka on käyttänyt leimaa työssään, irtisanotaan, jolloin hän vie sähköisen leiman luomisvälineen mukanaan. Ennen kuin A Oy:ssä huomataan luomisvälineen kadonneen, on X tehnyt toimeksiantoja yrityksen nimissä. A Oy ilmoittaa luottamuspalvelun tarjoajalle luomisvälineen kadonneen, mutta ennen kuin varmenne ehditään peruuttaa, ehtii X tehdä vielä yhden toimeksiannon.

X on luonnollisesti vahingonkorvausvelvollinen, sillä vahinko on aiheutunut X:n tahallisuudesta, ja petos on rangaistava teko (vahingonkorvauslaki 2:1 §, 5:1 §; RL 36:1 §). Asiassa tulee tarkastella myös A Oy:n sekä luottamuspalvelun tarjoajan vahingonkorvausvastuuta suhteessa vahinkoa kärsineisiin petollisten toimeksiantojen vastapuoliin. Kun sähköisen allekirjoittamisen vastuuta sääntelevä ehdotettu 40 § koskee myös sähköisiä leimoja, tulisivat aiheutuneet vahingot A Oy:n korvattavaksi siihen asti, kunnes varmenteen peruutuspyyntö on saapunut luottamuspalvelun tarjoajalle. Luottamuspalvelun tarjoaja olisi vastuussa viimeisestä petollisesta toimeksiannosta aiheutuneista vahingoista.

Jos näin ei kuitenkaan olisi esitetty, määräytyisi vastuu vahingoista eIDAS-asetuksen 13 artiklan ja vahingonkorvauslain mukaan. Koska kyseessä on hyväksytty luottamuspalvelun tarjoaja, on sen pystyttävä näyttämään, ettei viimeisen toimeksiannon onnistuminen ole johtunut sen huolimattomuudesta. Todennäköisesti luottamuspalvelun tarjoaja olisi ollut vahingonkorvausvelvollinen viimeisestä toimeksiannosta aiheutuneesta vahingosta, koska varmenteen peruutuspyyntö oli saapunut sille jo ennen toimeksiannon tekemistä.

A Oy:n vastuu aiheutuneista vahingoista olisi kuitenkin määräytynyt täysin vahingonkorvauslain mukaan. Tulkittavaksi olisi tullut, ovatko vahingot aiheutuneet A Oy:n tuottamuksesta, kun se on mahdollisesti toiminut huolimattomasti X:n viedessä sähköisen leiman luomisvälineen mukanaan. Todennäköisesti vahingon olisi katsottu tapahtuneen A:n tuottamuksesta, mutta korvausta ei tuomittaisi puhtaasta varallisuuteen kohdistuvasta vahingosta erittäin painavien syiden puuttuessa.

Sama pohdinta tulisi käydä myös, jos A Oy:n tiloihin murtauduttaisiin ja rikolliset käyttäisivät sähköistä leimaa ennen kuin leiman luomistietojen huomattaisiin joutuneen sivullisen haltuun. Sähköisiin luottamuspalveluihin kohdistuvan luottamuksen ylläpitämiseksi ehdotettu tunnistuslain 40 § on kuitenkin ulotettu koskemaan myös sähköisiä leimoja ja muita varmennepohjaisia luottamuspalveluita, jolloin vastuita koskeva oikeustila tulee olemaan selkeämpi.

7 MUUTOSTEN MAHDOLLISET VAIKUTUKSET PALVELUIDEN KÄYTTÖÖN

Tässä luvussa aiemmin kuvattuja muutoksia sähköistä tunnistamista koskevassa lainsäädännössä tarkastellaan UTAUT2-mallin[153] perusteella löydettyjen sähköisen asioinnin käytön ajureiden näkökulmasta. UTAUT2-mallin ajureista tarkasteltavaksi tulevat aikaisemmin esitetyn mukaisesti odotettu hyöty (*performance expectancy*), odotettu vaiva (*effort expectancy*), sosiaalinen paine (*social* influence) sekä vastine rahalle (*price value*).

Kansallisella vahvan sähköisen tunnistamisen luottamusverkostolla tulee olemaan suuri vaikutus tunnistamisen järjestämiseen etenkin tunnistamista vaativien palvelujen tarjoajien näkökulmasta. Odotettavissa on, että vaiva pienenee, kun sopimuksen voi tehdä yhden tunnistuksenvälityspalvelun tarjoajan kanssa niin, että kaikkien vahvojen sähköisten tunnistusvälineiden käyttäjät voivat kirjautua palveluun. Vaiva pienentynee myös teknisellä puolella, kun palveluntarjoajan on toteutettava vain yksi tekninen rajapinta tunnistamista varten.

Mahdollisuus sopia vain yhden tunnistuksenvälityspalvelun käyttämisestä vaikuttanee myös koettuun vastineeseen rahalle, kun palveluntarjoajan ei tarvitse maksaa kuukausimaksua jokaiselle tunnistuspalvelun tarjoajalle kuten tällä hetkellä. Vaikka transaktiokohtainen maksu nousisikin tunnistuksenvälityspalvelun tarjoajan keräämän maksun takia, pidän todennäköisenä, että vahvan sähköisen tunnistamisen mahdollistaminen tulee kannattavaksi aiempaa pienemmillä transaktiomäärillä, jolloin kiinteiden kustannusten rooli korostuu. Lopullinen vaikutus riippuu tietysti käyttöön tulevista hinnoittelumalleista, joista kaupalliset toimijat voivat vapaasti päättää.

Mikäli yllä olevien vaikutusten oletetaan toteutuvan, näkyy luottamusverkosto loppukäyttäjälle vahvan sähköisen tunnistamisen mahdollisuutena yhä useammassa asiointipalvelussa, korottaen tunnistusvälineen hankkimisesta saatavaa odotettua hyötyä. Vahvan sähköisen tunnistamisen yleistyminen voi vaikuttaa myös yksittäisen henkilön kokemaan sosiaaliseen paineeseen käyttää sähköisen tunnistamisen menetelmiä.

Henkilötietojen tarkastamisvelvollisuus väestötietojärjestelmästä ei vaikuttane merkittävästi sähköisen tunnistamisen suosioon, sillä vakiintunut käytäntö on jo aiemmin ollut henkilöllisyyden varmentaminen viranomaisrekisteristä. Ulkomaiden kansalaisten kohdalla odotettu vaiva kuitenkin kasvaa, kun tiedot pitää saada merkittyä väestötietojärjestelmään ennen tunnistusvälineen hakemista tai viimeistään hakemisen yhteydessä. Vaikutus pienenee, mikäli tunnistusvälineiden tarjoajat pitävät tunnistusvälineet voi-

---

[153] Unified Theory of Acceptance and Use of Technology 2 (Venkatesh, Thong & Xu 2012), ks. Kuvio 2, s. 14

massa sopimusperusteisesti, muina kuin vahvoina sähköisen tunnistamisen välineinä. Tämä kuitenkin edellyttää aina sopimusta tunnistuspalvelun tarjoajan ja tunnistamista vaativan palvelun tarjoajan välillä, eikä välineellä voi tunnistautua luottamusverkoston kautta tai hakea uutta tunnistusvälinettä, sillä nämä ovat mahdollisia vain tunnistuslain tarkoittamilla vahvoilla tunnistusvälineillä.[154]

Myös eIDAS-asetuksen säännökset unionin sisärajat ylittävästä tunnistamisesta pienentävät ulkomaalaisiin kohdistuvia vaikutuksia, kun heidän on tulevaisuudessa mahdollista käyttää oman kotivaltionsa ilmoittamia vahvan sähköisen tunnistamisen välineitä viranomaisten asiointipalveluissa. UTAUT2-mallin mukaisesti vaikutukset kohdistuvat tunnistusvälineestä saatavaa odotettua hyötyä nostavasti ja vaivaa pienentävästi niillä, jotka asioivat ulkomaisten viranomaisten kanssa. Muiden osalta rajat ylittävän tunnistamisen mahdollisuus on merkityksetön. Jos rajat ylittävää tunnistamista hyödyntävällä henkilöllä on ollut vieraan jäsenvaltion hyväksymä tunnistusväline, jonka tämä voi muutoksen jälkeen sulkea, pienentää asetus myös loppukäyttäjän maksuja.

Rajat ylittävä tunnistaminen on eIDAS-asetuksessa mahdollistettu myös yksityisille yrityksille, jotka toimivat palveluntarjoajina. Tämä saattaa yhdessä tietoturvallisuuden varmuustasojen kanssa vaikuttaa useissa valtioissa toimivien palveluntarjoajien hallinnointitaakkaan ja helpottaa monikansallisten asiointipalvelujen rakentamista, mutta asiasta on vaikea antaa arviota ilman tarkempaa tutkimusta.

Mahdollisuus hakea vahvaa sähköistä tunnistusvälinettä olemassa olevalla vahvalla sähköisen tunnistamisen välineellä pienentää tunnistusvälineen hakemisen odotettua vaivaa. Uusien ja erilaisten tunnistusvälineiden kokeileminen helpottuu ja toisaalta tunnistuspalvelun tarjoajan vaihtaminenkin onnistuu ilman henkilökohtaista asiointia tunnistuspalvelun tarjoajan toimipisteessä, mikä saattaa vaikuttaa tunnistuspalveluiden tarjoajien hinnoitteluun. Toisaalta muutos helpottaa identiteettivarkaudessa, kun uusia tunnistusvälineitä voi hakea rajattomasti sen jälkeen, kun rikollinen on saanut yhden välineen haltuunsa.

Esitetty hallinnon sähköisen asioinnin tukipalvelujen keskittäminen VRK:lle sekä tunnistus.fi- ja Vetuma-portaalien korvaaminen aiheuttaa aluksi työtä viranomaispalveluntarjoajille, mutta tunnistuspalveluiden kustannusten kohdistaminen yhteiseen budjettiin pienentää yksittäisen viraston kustannuspaikalle kohdistuvaa vaikutusta ja tekee näin sähköisen tunnistamisen käyttämisestä houkuttelevampaa. Yksittäisen palveluntarjoajan kannalta kustannustehokkuus siis kasvaa, vaikka koko julkishallinnon osalta kustannukset eivät muuttuisikaan.

Loppukäyttäjän kannalta julkishallinnon sisäisellä kustannusten jakautumisella ei ole merkitystä, eikä käyttäjän kokemus tunnistamisessa juuri muutu nykyistenkin tunnista-

---

[154] HE 272/2014 vp, s. 18–19

misportaalien ollessa helppokäyttöisiä. Kertakirjautumispalvelu voi kuitenkin helpottaa käyttäjän siirtymistä yhden viranomaisen asiointipalvelusta toiseen, mikä vaikuttaa helppokäyttöisyyteen. Julkishallinnon kannalta kertakirjautuminen tuo säästöjä kirjautumiskertojen pienentyessä, mikäli tunnistuspalveluiden tarjoajien transaktiokohtainen hinta ei muutu.

Suunniteltu rooli- ja valtuushallintapalvelu, joka mahdollistaisi aluksi laillisen edustusoikeuden tarkistamisen ja myöhemmin laajentuisi myös henkilöiden toisilleen antamiin valtakirjoihin, vaikuttaisi sekä palveluntarjoajiin sekä loppukäyttäjiin. Erityisesti viranomaispalveluiden odotettavissa oleva hyöty kasvaisi, kun jonkin henkilön laillinen huoltaja voisi asioida sähköisesti tämän puolesta. Sama hyöty näkyisi luonnollisesti myös loppukäyttäjänä olevan huoltajan puolella. Suunnitelma tarjota palvelua myös yksityisille yrityksille kasvattaa järjestelystä saatavaa odotettua hyötyä entisestään, kun vaikkapa henkilön valtuus toimia sairaan vanhempansa puolesta voidaan todeta viranomaisen ylläpitämästä rekisteristä.

Esitetty henkilökorttilaki vaikuttaisi täysin sähköisen hakemusmenettelyn ja sairausvakuutustietojen poistamisen kautta. Täysin sähköinen hakemusmenettely pienentäisi hakijan kokemaa vaivaa, kun henkilökorttia varten ei tarvitsisi käydä poliisiasemalla henkilökohtaisesti. Toisaalta sairausvakuutustietojen sisällyttämisen mahdollisuuden poistaminen pienentää kortista saatavaa hyötyä, kun Kela-korttia on jälleen kannettava mukana. Mahdollinen hinnan aleneminen kuitenkin kompensoisi pienentynyttä hyötyä, mutta hallituksen esitys ei ota kantaa henkilökortin hinnan muutokseen.

Oikeushenkilöiden tunnistusvälineiden ja sähköisten leimojen osalta on vaikea arvioida vaikutuksia. Ainakin lyhyellä tähtäimellä odotettu helppokäyttöisyys pienenee huomattavasti, kun oikeushenkilöiden kehittyneiden sähköisten allekirjoitusten luominen poistuu. Aihe vaatisikin tarkempaa tutkimusta, jotta suosituksia toimenpiteistä käytön helpottamiseksi ja saatavien hyötyjen kasvattamiseksi voisi tehdä.

8 LOPUKSI

Sähköisen asioinnin odotetaan edelleen kasvavan. Yllä esitetyt lakimuutosten mahdolliset vaikutukset perustuvat kuitenkin vain yhteen teoreettiseen malliin. Tulokset tulisikin tarkistaa empiirisellä tutkimuksella, esimerkiksi tilastoihin ja haastatteluihin perustuvalla tutkimuksella nyt ja muutaman vuoden kuluttua, kun muutokset alkavat oletettavasti vaikuttaa tarjolla oleviin palveluihin. Myös muita teoreettisia malleja käyttämällä voitaisiin saada tuloksia, jotka joko tukevat tai kumoavat yllä mainittuja päätelmiä.

EIDAS-asetus yhtenäistää säädöskenttää EU:n sisällä erityisesti luottamuspalveluiden osalta. Oikeushenkilön vahvan sähköisen tunnistamisen osalta on kuitenkin edelleen epäselvää, kuinka palvelu käytännössä järjestettäisiin, eikä varmuustasoasetuksen suositus oikeushenkilön tunnistusvälineen kytkemisestä luonnolliseen henkilöön selvennä tilannetta. Samat ongelmat tulevat näkyviin myös kansallisessa tunnistuslaissa, jota ehdotetaan yhtenäistettäväksi eIDAS-asetuksen kanssa. Vaikka lain onkin hyvä olla teknologianeutraali, ei tulisi säätää vaatimuksia, joille ei ole olemassa toteuttamistapaa. Mahdollisen teknisen toteutustavan voisi yrittää löytää tietojärjestelmä- tai tietojenkäsittelytiedettä ja oikeustiedettä yhdistävällä tutkimuksella.

Myös kansalaisvarmenteen sisällyttämistä henkilökortille tulisi arvioida kriittisesti. Vaadittavan infrastruktuurin ylläpitäminen ja kehittäminen on kuitenkin maksullista, mutta käyttö ei ole kovin yleistä. Kun henkilökorttia ei olla säätämässä kaikille pakolliseksi, ja toisaalta perustuslakivaliokunta on katsonut, ettei vahvan sähköisen tunnistamisen ja laatuvarmenteiden myöntämistä ole pidettävä julkisena hallintotehtävänä, tulisikin selvittää Iso-Britannian mallin mukaiseen järjestelmään siirtymistä.[155] Tällöin valtio kilpailuttaisi tunnistuspalveluntarjoajat, ja kansalainen voisi kilpailutuksessa menestyneistä vaihtoehdoista valita mieluisen.

Kansallinen tunnistuspalvelun tarjoajien luottamusverkosto tulee avaamaan liiketoimintamahdollisuuksia tunnistamisen välityspalveluille, hieman samoin kuin verkkomaksaminen on jo nykyisin mahdollista kanavoida maksupalveluntarjoajan kautta.[156] Tällöin yksittäisen asiointipalvelun tarjoajan ei tarvitse tehdä sopimusta kuin yhden tunnistuspalveluntarjoajan kanssa, mikä mahdollistaa kaikkien luottamusverkostoon liitettyjen tunnistusvälineiden käyttäjien kirjautumisen palveluunsa. Odotettavissa onkin vahvan sähköisen tunnistamisen leviäminen yhä pienempiin palveluihin.

Uusin esitetty muutos tunnistuslakiin, HE 74/2016, vaikuttaa kuitenkin hätäisesti valmistellulta oikeushenkilöiden tunnistusvälineiden ja sähköisten leimojen osalta. Erityisesti väärinkäyttötilanteissa vastuun jakautuminen eri osapuolien välillä on epäselvää,

---

[155] PeVL 16/2009 vp, Valiokunnan kannanotot > Perustelut > Perustuslain 124 §

[156] Esimerkiksi Paytrail, Checkout Finland ja Klarna tarjoavat tällaista palvelua

ellei tilanteita ole erikseen huomioitu tunnistusvälineen tarjoajan ja haltijan välisellä sopimuksella. Esimerkiksi oikeushenkilön tunnistusvälineen luovuttaminen toiselle voidaan vielä määritellä usealla tavalla. On myös huomioitava, että uusi henkilökorttilaki, hallinnon sähköisen asioinnin yhteisiä tukipalveluja koskeva laki sekä tunnistuslain muutos ovat kaikki vielä luonnoksia, jotka odottavat vielä valiokuntakäsittelyjä ja eduskunnan vastausta.

Kaikkiaan esitetyt muutokset kuitenkin kannustavat sähköisten tunnistus- ja allekirjoituspalveluiden käyttöönottoon UTAUT2-mallin kautta tarkasteltuna. Ulkomaalaisten osalta tarkastelu on kuitenkin vaikeampaa, sillä Suomalaisen tunnistusvälineen hakeminen on hankalampaa vuoden 2016 alusta alkaen. Toisaalta EU-kansalaisten mahdollisuudet tunnistautua viranomaisten asiointipalveluihin minkä tahansa jäsenvaltion hyväksymällä tunnistusvälineellä tulee olemaan mahdollista. Rajat ylittävä vahva sähköinen tunnistaminen on lain tasolla mahdollista myös yrityksille, mutta palvelun kustannukset ja järjestämistapa ovat tässä vaiheessa vielä epäselviä.

LÄHTEET

Artikkelit ja kirjallisuus

Anderson, Keith B. – Durbin, Erik – Salinger, Michael A. (2008) Identity theft. *Journal of Economic Perspectives* Vol 22 (2), ss. 171–192.

Arenas-Gaitán, Jorge – Peral-Peral, Begoña – Ramón-Jerónimo, Maria Angeles (2015) Elderly and internet banking: an application of UTAUT2. *Journal of Internet Banking and Commerce* Vol. 20 (1), s. 1–23.

Davis, Fred D – Bagozzi, Richard P – Warshaw, Paul R (1989) User acceptance of computer technology: a comparison of two theoretical models. *Management Science* Vol. 35 (8), 2. 982–1003.

Gilbert, David – Balestrini, Pierre – Littleboy, Darren (2004) Barriers and benefits in the adoption of e-government, *International Journal of Public Sector Management*, vol. 17 (4), s. 286–301.

Halilovic, Semina – Cicic, Muris (2013) Understanding determinants of information systems users' behaviour: a comparison of two models in the context of integrated accounting and budgeting software. *Behaviour & Information Technology* Vol. 32 (12), s. 1280–1291.

Hung, Shin-Yuan – Chang, Chia-Ming – Yu, Ting-Jing (2006) Determinants of user acceptance of the e-Government services: the case of online tax filing and payment system. *Government information quarterly* Vol 23 (1), s. 97–122.

Koski, Niina (2002) Asiakkaan kokemat hyödyt sähköisessä pankkiasioinnissa: uudet vs. vanhat käyttäjät *teoksessa Kuusela, Hannu – Rintamäki, Timo (2002) Arvoa tuottava asiointikokemus: hyödyt ja uhraukset sähköisen asioinnin kehittämisessä. Tampere University Press*, s. 87–102.

Koski, Nina – Villberg, Katariina (2002) Sähköisen pankkiasioinnin hyödyt *teoksessa Kuusela, Hannu – Rintamäki, Timo (2002) Arvoa tuottava asiointikokemus – Hyödyt ja uhraukset henkilökohtaisen ja sähköisen asioinnin kehittämisessä. Tampere University Press*, s. 63–73.

Lee, Jooho – Kim, Hyun Joon – Ahn, Michael J (2011) The willingness of e-Government service adoption by business users: The role of offline service quality and trust in technology. *Government information quarterly* Vol 28 (2), s. 222–230.

Peczenik, Aleksander (1995) Juridikens teori och metod. Norstedts Juridik, Tukholma.

Pikkarainen, Tero – Pikkarainen, Kari – Karjaluoto, Heikki – Pahnila, Seppo (2004) Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research* Vol 14 (3), s. 224–235.

Ponka, Ilja (2013) Sähköinen tunnistaminen ja allekirjoitus Suomen velvoiteoikeudessa. Väitöskirja, Helsingin yliopiston oikeustieteellinen tiedekunta. Unigrafia Oy, Helsinki.

Rondan-Cataluña, Francisco Javier – Arenas-Gaitán, Jorge – Ramírez-Correa, Patricio Esteban (2015) A comparison of the different versions of popular technology acceptance models. A non-linear perspective. *Kybernetes* Vol 44 (5), s. 788–805.

Ståhlberg, Pauli – Karhu, Juha (2013) Suomen vahingonkorvausoikeus. 6., uudistettu painos. Talentum Media Oy.

Venkatesh, Viswanath – Morris, Michael G – Davis, Gordon B – Davis, Fred D (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly* Vol 27 (3), s. 425–478.

Venkatesh, Viswanath – Thong, James Y L – Xu, Xin (2012) Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly* Vol 36 (1), s. 157–178.

Villberg, Katariina (2002) Pankkipalvelut verkossa – asiakkaan kokemat utilitaristiset ja hedonistiset hyödyt *teoksessa Kuusela, Hannu – Rintamäki, Timo (2002) Arvoa tuottava asiointikokemus: hyödyt ja uhraukset sähköisen asioinnin kehittämisessä. Tampere University Press*, s. 74–86.

Voutilainen, Tomi (2009) ICT-oikeus sähköisessä hallinnossa. ICT-oikeudelliset periaatteet ja sähköinen hallintomeettely. Väitöskirja, Joensuun yliopisto. Edita Publishing Oy, Helsinki.

Julkislähteet

Cabinet Office (2013) CESG Good Practice Guide No. 46: Organisation Identity. Issue No: 1.0, October 2013. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271278/Good_practice_guide_organisation_identity.pdf>, haettu 3.5.2016.

Estonian Digital Signatures Act, RT I 2000, 26, 150. <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/508072014007/consolide>, haettu 17.5.2016.

Estonian Identity Documents Act, RT I 1999, 25, 365. <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/511042016001/consolide>, haettu 2.5.2016.

Euroopan komissio (2014) Delivering on the European advantage? How European governments can and should benefit from innovative public services. eGovernment benchmark. Insight report. Publications Office of the European Union, Luxembourg.

Euroopan komissio (2016) Questions & answers on trust services under eIDAS. Published on 29/02/2016. <https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas>, haettu 26.3.2016.

Eurostat (2016) http://ec.europa.eu/eurostat/web/information-society/data/database, Policy indicators > Benchmarking digital Europe:: key performance indicators > Public services - individuals (isoc_bdek_ps), haettu 24.1.2016.

Government Digital Service (2016) Guidance: GOV.UK Verify. Published 6 April 2016. <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>, haettu 2.5.2016.

Hallituksen julkaisusarja 10/2015. Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen strateginen ohjelma. 29.5.2015. Valtioneuvoston kanslia.

HE 96/1998 vp Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 36/2009 vp Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi.

HE 169/2009 vp Hallituksen esitys eduskunnalle maksupalvelulaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 230/2014 vp Hallituksen esitys eduskunnalle eräiden hallintoasioiden muutoksenhakusäännösten tarkistamisesta.

HE 41/2016 vp Hallituksen esitys eduskunnalle henkilökorttilaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 59/2016 vp Hallituksen esitys eduskunnalle laeiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain muuttamisesta.

HE 74/2016 vp Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi.

Henkilökortin käyttöehdot (2011) Henkilökortin käyttöehdot. Poliisihallitus. Väestörekisterikeskus. Ohje. 8.4.2011. <http://www.fineid.fi/default.aspx?id=0&docid=5024&action=Publish>, haettu 24.3.2015.

KK 358/2013 vp Kirjallinen kysymys sähköisestä tunnistautumisesta peruspalvelujen ja kansalaisoikeuksien näkökulmasta. Tarkistettu versio 2.0. Ritva Elomaa (ps), 26.4.2013, sekä hallinto- ja kuntaministeri Henna Virkkusen vastaus 24.5.2013.

KK 262/2016 vp Kirjallinen kysymys mobiilitunnistautumisesta viranomaispalveluihin prepaid-liittymällä. Ritva Elomaa (ps), 4.5.2016.

LVM (2016) Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä laeiksi eräiden siihen liittyvien lakien muuttamisesta. Luonnos 19.1.2016. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=191831>, haettu 25.3.2016.

LVMa 439/2015 liikenne- ja viestintäministeriön asetus tarkoituksenmukaisen internetyhteyden vähimmäisnopeudesta yleispalvelussa (439/2015).

OECD (2007) OECD recommendation on electronic authentication and OECD guidance for electronic authentication. June 2007. <http://www.oecd.org/internet/ieconomy/38921342.pdf>, haettu 18.2.2015.

PeVL 16/2009 vp Perustuslakivaliokunnan lausunto 16/2009 vp. Tarkistettu versio 2.0. Hallituksen esitys laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi.

Poliisihallitus (2016) Poliisihallituksen lausunto muutosehdotukseen koskien lakia vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. 22.02.2016. POL-2016-1416. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=195580>, haettu 25.3.2016.

Työ- ja elinkeinoministeriö (2016) Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä laeiksi eräiden siihen liittyvien lakien muuttamisesta; työ- ja elinkeinoministeriön lausunto. 25.02.2016. TEM/198/03.01.08/2016.

UK Identity Cards Act 2006, 2006 Chapter 15. <http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf>, haettu 2.5.2016.

Valtioneuvoston kanslia (2005) Kuntien ja valtion tietohallinnon yhteisten menettelytapojen ja koordinoinnin kehittäminen – Kehittämistyöryhmän loppuraportti. Valtioneuvoston kanslian julkaisuja 10/2005.

Valtiovarainministeriö (2015) Palveluväylä. <http://vm.fi/palveluvayla>, haettu 3.4.2015.

Verohallinto (2016) Lausunto hallituksen esitysluonnoksesta vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta. A4/000001/2016. 22.2.2016. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=195439>, haettu 25.3.2016.

Viestintävirasto (2014) Rekisteri laatuvarmenteita tarjoavista varmentajista. Julkaistu 19.08.2014. <https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus/rekisterilaatuvarmenteitatarjoavistavarmentajista.html>, haettu 13.1.2016.

Viestintävirasto (2015) Rekisteri tunnistuspalvelun tarjoajista. Julkaistu 13.11.2015. <https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus/rekisteritunnistamispalveluntarjoajista/rekisteritunnistamispalvelujentarjoajista.html>, haettu 13.1.2016.

Viestintävirasto (2016a) Viestintäviraston tekniset määräykset työryhmä 1/2016. Viestintävirasto 8.3.2016. <https://www.viestintavirasto.fi/attachments/esitykset/Kalvot_8.3.2016_Viestintaviraston_tekniset_maaraykset_tyoryhma.pdf>, haettu 16.5.2016.

Viestintävirasto (2016b) Viestintäviraston lausuntopyyntö luonnoksesta määräykseksi 72 sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. 13.5.2016, Dnro 81/060/2016.

Viestintävirasto 7 B/2009 M. Määräys tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle. Annettu Helsingissä 27 päivänä elokuuta 2009.

Viestintävirasto MPS 7. Määräyksen 7 perustelut ja soveltaminen. Tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle. 1.9.2009.

Viestintävirasto MPS 72 luonnos. Määräyksen 72 perustelut ja soveltaminen. Sähköinen tunnistaminen ja sähköiset luottamuspalvelut. 13.5.2016.

VNa 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta.

VTV (2016) Digitaalisten asiointipelveluiden kehittäminen ja tuotanto. Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 6/2016, Dnro 235/54/2014.

SopS 17/1954 Asetus Suomen, Tanskan, Norjan ja Ruotsin kansalaisten vapauttamisesta velvollisuudesta omata passi sekä oleskelulupa muussa pohjoismaassa kuin kotimaassa oleskellessaan tehdyn pöytäkirjan voimaansaattamisesta.

Muut lähteet

BBC News (2010) Identity cards scheme will be axed 'within 100 days'. 27.5.2010. <http://news.bbc.co.uk/2/hi/8707355.stm>, haettu 2.5.2016.

Cabinet Office (2014) Identity Assurance Programme Market Briefing Event, 30th October 2014. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371500/Market_Engagement_Day_30_October_2014_FINAL.pdf>, haettu 3.5.2016.

Danske Bank (2012) Tunnistuspalvelun sopimusehdot. Voimassa 15.11.2012. <https://www.danskebank.fi/PDF/fi/Yritysasiakkaat/Verkkopalvelut/TUPASTUNNISTUSPALVELUSOPIMUSEHDOTFI.pdf>, haettu 12.1.2016.

Danske Bank (2013) Sähköisen asioinnin ehdot – verkkopankki ja puhelinpalvelu. <http://www.danskebank.fi/PDF/fi/Henkiloasiakkaat/Verkkopalvelut/SAHKOISENASIOINNINEHDOTFI.pdf>, haettu 26.3.2015.

eIDAS expert group (2016) Guidance for the application of the levels of assurance which support the eIDAS Regulation. <https://www.viestintavirasto.fi/attachments/suositukset/LOA_Guidance.pdf>, haettu 26.3.2016.

Elinkeinoelämän keskusliitto (2016) Lausunto 24.2.2016. HE vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä eräiden siihen liittyvien lakien muuttamisesta. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=195747>, haettu 26.3.2016.

FiCom (2011) Mobiiliasiointivarmenne – Varmennepolitiikka – operaattoreiden mobiiliasiointivarmenteita varten. Versio 1.1. Voimassa 15.4.2011 lähtien. <http://www.mobiilivarmenne.fi/documents/Mobiiliasiointivarmenne-Varmennepolitiikka.pdf >, haettu 17.2.2015.

Finanssialan keskusliitto (2013a) Pankkien TUPAS-tunnistuspalvelu palveluntarjoajille. Palvelukuvaus ja palveluntarjoajan ohje. Versio 2.4. 2.12.2013. <https://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas_varmennepalvelu_V_2.4.pdf>, haettu 15.2.2015.

Finanssialan keskusliitto (2013b) Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet. V2.0c 2.12.2013. <https://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas_tunnistusperiaatteet_v20c_FI.pdf>, haettu 15.2.2015.

Finanssialan keskusliitto (2015) Säästäminen, luotonkäyttö ja maksutavat. Tekstiraportti. 9.10.2015. <https://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/FK-Julkaisu-Saastaminen_luotonkaytto_ja_maksutavat_2015.pdf>, haettu 12.1.2016.

Hughes, Janet (2014a) What is identity assurance? Government Digital Service Blog, 23.1.2014. <https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/>, haettu 3.5.2016.

Hughes, Janet (2014b) How does a certified company establish that it's really you? GOV.UK Verify Blog, 21.11.2014. Government Digital Service. <https://identityassurance.blog.gov.uk/2014/11/21/how-does-a-certified-company-establish-that-its-really-you/>, haettu 3.5.2016.

KaPA (2014) Palveluväylän kehitysympäristö <https://confluence.csc.fi/pages/viewpage.action?pageId=37816865>, haettu 3.4.2015.

Nordea (2015a) Pankkitunnuksilla käytettävien palvelujen yleiset sopimusehdot 02.2015. <http://www.nordea.fi/sitemod/upload/root/content/nordea_fi_fi/henkiloasiakkaat/internetpalvelut/pdf/MMST960DL_0215.pdf>, haettu 26.3.2015.

Nordea (2015b) E-tunnistesopimusehdot 10.2015 <http://www.nordea.fi/Images/58-86171/e-tunniste-sopimusehdot.pdf>, haettu 12.1.2016.

Nordea (2016) Lausunto vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä eräiden siihen liittyvien lakien muuttamisesta. 22.02.2016. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=195600>, haettu 26.3.2016.

OP (2013) Tupas-tunnistuspalvelu – käyttöehdot. Käytössä 19.6.2013 alkaen. <https://www.op.fi/media/liitteet?cid=151692667&srcpl=4>, haettu 12.1.2016.

OP (2014) Osuuspankin verkkopalvelutunnusten ja OP-verkkopalveluiden yleiset ehdot. <https://www.op.fi/media/liitteet?cid=151246258&srcpl=3>, haettu 26.3.2015.

OP Osuuskunta (2016) LVM lausuntopyyntö LVM/2005/03/2015 (vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä eräiden siihen liittyvien lakien muuttamisesta). 22.2.2016. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=195604>, haettu 26.3.2016.

Ralph, Livia (toim) (2016) Digital identity across borders: Opening a bank account in another EU country. Project report, February 2016. Open Identity Exchange. <http://oixuk.org/wp-content/uploads/2016/02/Digital-Identity-Across-Borders-FINAL-Feb2016-2.pdf>, haettu 2.5.2016.

Simola, Kreetta (2015) Sähköisen tunnistamisen luottamusverkosto. KaPA-info29.9.2015: Tunnistus, roolit ja valtuudet. Liikenne- ja viestintäministeriö <http://vm.fi/documents/10623/1789537/KaPA-20150929-Luottamusverkoston-kuulumisia-Kreetta-Simola.pdf/2ef586bc-eb05-4360-8506-ca12b23a968b>, haettu 20.3.2016.

Sonera (2016) Sonera ID:n tunnistusperiaatteet <https://www.sonera.fi/asiakastuki/ohjeet/Sonera-ID:n-tunnistusperiaatteet?id=1242>, haettu 15.1.2016.

Suomi.fi (2015) Verkkotunnistaminen ja -maksaminen Vetuma – Työhuone. <http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_maksaminen_vetuma/>, haettu 11.3.2015.

Tunnistus.fi (2015) <https://www.tunnistus.fi/>, haettu 11.3.2015.

Walker, Robin – Rea, Sam (2014) Identity assurance in the European Union. GOV.UK Verify Blog, 17.11.2014. Government Digital Service. <https://identityassurance.blog.gov.uk/2014/11/17/identity-assurance-in-the-european-union/>, haettu 2.5.2016.

Oikeustapaukset ja ratkaisusuositukset

Korkein oikeus

KKO 1994:82

KKO 2006:81

Hallinto-oikeudet

Itä-Suomen HAO 17.06.2015 15/0193/4

Hovioikeudet

Helsingin HO 2007:2

Kouvolan HO 2012:3

Kouvolan HO 2012:4

Eduskunnan apulaisoikeusasiamiehen päätökset

AOA 4653/4/14

AOA 3666/4/10

Vakuutus- ja rahoitusneuvonta FINE:n pankkilautakunnan ratkaisusuositukset

PKL 59/11

PKL 20/13

PKL 10/14

PKL 32/15