Sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta

Mika Aarnio

Haaga-Helia ammattikorkeakoulu

Tradenomin tutkinto

Tutkimustyyppinen opinnäytetyö

2022

Tiivistelmä

Tekijä(t)
Mika Aarnio

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta

Sivu- ja liitesivumäärä
40 + 9

Opinnäytetyössä tarkoituksena oli selvittää, missä tilanteissa vahva sähköinen tunnistaminen oli tarpeellista, kun kuluttaja, kansalainen tai jonkin verkkopalvelun loppukäyttäjä verkkopalvelua käytti. Missä tilanteissa lainsäädäntö edellytti vahvaa sähköistä tunnistamista verkossa olevia sähköisiä palveluita käyttävältä kuluttajalta tai viranomaisen sähköisiä palveluita käyttävältä kansalaiselta? Miten sähköisen palvelun loppukäyttäjä koki palveluun tunnistautumisen ja käytön tapahtuneen sujuvuuden näkökulmasta?

Sähköisiä palveluita ja vahvaa tunnistamista säätelee kansallinen sekä EU-peräinen lainsäädäntö. Lainsäädäntö toimi keskeisenä tietoperustana opinnäytetyössä. Tutkimusaiheeseen vaikuttavan lainsäädännön laajuudesta saa kuvan tutustumalla opinnäytetyön liitteeseen numero 1 (Säädösten lyhenteet). Aihepiiriä koskevaan lainsäädäntöön tutustuttiin enemmän siitä näkökulmasta käsin, että pyrittiin selvittämään regulaation asettamat reunaehdot ja vaatimukset vahvan sähköisen tunnistamisen tilanteille.

Regulaation asettamien reunaehtojen selvittämisen ohella opinnäytetyöprosessin aikana toteutettiin pienimuotoinen Webropol-kyselytutkimus ajalla 24.3.- 8.4.2022. Kyselytutkimuksen avulla haluttiin selvittää, miten kuluttajan näkökulmasta näyttäytyi yksityissektorin ja julkisen sektorin sähköisten asiointipalveluiden käyttäminen tunnistamisprosesseineen. Kyselyyn vastaajilla eniten käytössä ollut sähköinen tunnistamisväline oli suomalaisen pankin myöntämät verkkopankkitunnukset. Kyselyyn vastaajista vain 37 % oli hankkinut itselleen teleoperaattorin mobiilivarmenteen, joka on verkkopankkitunnusten ohella toinen vahvan sähköisen tunnistamisen tunnistamisväline. Digi- ja väestötietoviraston myöntämä kansalaisvarmenne oli huonosti tunnettu ja marginaalisen harvoin käytetty vahvan sähköisen tunnistamisen tunnistusväline.

Loppupäätelminä opinnäytetyössä tuotiin esille se, että sähköisen palveluiden käyttö edellytti yleisen digiosaamisen lisäksi verkkopalvelun loppukäyttäjältä muitakin taitoja, kuten ymmärrystä suomalaisesta pitkälle kehittyneestä julkissektorin ja yksityissektorin palvelujärjestelmästä ja riittävän korkealla tasolla olevaa suomen kielen hallintaa. Puutteita taidoissa oli kaiken ikäisillä. Erityisesti ulkomaalaistaustaisilla henkilöillä oli hankaluuksia ymmärtää digitaalisten palveluiden monimutkaisia tekstisisältöjä ja toiminnallisuuksia. Digitalisaatiokehitys on aiheuttanut sen, että omien tietojen tietoturvanäkökulma on korostunut. Esimerkiksi mielenterveyttä ja sosiaalista osallisuutta edellyttävissä terveyspalveluissa hyödynnettiin paljon etäpalveluita, joita kaikki ihmiset eivät koe tietoturvallisiksi. Myös rahansiirtopalveluiden hoitaminen pelkästään verkossa arvelutti perinteiseen asiointiin tottuneita ihmisiä – erityisesti ikääntynyttä väestöä. Suomalaisia julkisen hallinnon sähköisiä asiointipalveluita on enenevässä määrin tarve käyttää ulkomailla asuvilla ulkomaiden kansalaisilla, joita ei ole rekisteröity Suomessa. He, joilta puuttuu suomalainen henkilötunnus, voi olla mahdotonta saada käyttöönsä suomalaisen pankin tai teleoperaattorin myöntämä vahvan sähköisen tunnistautumisen väline. Yhdenvertaisuuden toteutumiselle edellä mainittu seikka asettaa haasteita.

Asiasanat
sähköinen tunnistaminen, verkkotunnukset, sähköinen asiointi, etäpalvelut, lainsäädäntö

Sisällys

1 Johdanto

Tutkimukseni aihe on sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta. Työni tausta on digitalisaatiokehityksessä ja sähköisten palveluiden läsnäolossa kuluttajien ja kansalaisten jokapäiväisessä elämässä. Tutkimukseni keskiössä on selvittää, missä tilanteissa vahva sähköinen tunnistaminen on tarpeellista, kun kuluttaja, kansalainen tai jonkin verkkopalvelun loppukäyttäjä pyrkii verkkopalvelua käyttämään. Missä tilanteissa lainsäädäntö edellyttää vahvaa sähköistä tunnistamista verkossa olevia sähköisiä palveluita käyttävältä kuluttajalta tai viranomaisen sähköisiä palveluita käyttävältä kansalaiselta? Onko sillä eroa, että käyttääkö kuluttaja julkisen sektorin sähköistä viranomaispalvelua vai käyttääkö hän kaupallista, yksityisen sektorin verkkopalvelua? Miten sähköisen palvelun loppukäyttäjä kokee palveluun tunnistautumisen ja käytön tapahtuneen sujuvan sähköisen asioinnin näkökulmasta? Entä palvelun luotettavuuden ja tietoturvan toteutumisen näkökulmasta?

1.1 Perustelut, miksi asiaa on syytä tutkia

Sähköisten palvelujen määrä, digitaalinen kaupankäynti ja kuluttajien halukkuus käyttää mobiili- ja verkkopalveluita perinteisten ostoskäytäntöjen sijasta on lisääntynyt huomattavasti 2020-luvulla. Sähköisiin palveluihin pääsee käsiksi helposti erilaisilla mobiililaitteilla, jotka käyttävät langattomia verkkoja ns. 24/7-periaatteella eli vuorokauden minä aikana tahansa seitsemänä päivänä viikossa. Covid 19 -epidemia on entisestään lisännyt verkossa tapahtuvaa sähköistä asiointia sekä verkkokaupan suosimista perinteisen paikan päällä liikkeessä tapahtuvan asioinnin kustannuksella. Samanaikaisesti lisääntynyt regulaatio velvoittaa muun muassa julkisen sektorin toimijoilta siihen, että sähköisiä palveluita tulee olla kansalaisten tarjolla perinteisten viranomaisasiointimahdollisuuksien ohella. Laki sähköisestä asioinnista viranomaistoiminnassa (”asiointilaki” 13/2003), laki digitaalisten palveluiden tarjoamisesta (”digipalvelulaki” 306/2019) sekä uusimpana laki julkisen sektorin tiedonhallinnasta (”tiedonhallintalaki” 906/2019) asettavat reunaehtoja sähköisten palvelujen toteuttamiselle sekä asiointimahdollisuuksien monimuotoisuudelle julkisella sektorilla. EU:n jäsenvaltiona Suomi on niin ikään velvoitettu seuraamaan ja noudattamaan eurooppalaista aihepiiriin liittyvää sääntelyä. EU:n maksupalveludirektiivi (ns. EU:n toinen maksupalveludirektiivi, ”PSD 2 -direktiivi”) on vuodesta 2018 lukien velvoittanut erityisesti yksityissektorilla ja verkkokaupankäynnissä toimivia maksupalvelun tarjoajia tunnistamaan asiakkaansa ja käyttämään vahvaa sähköistä tunnistamista tietynlaisessa, esim. luottopalvelujen, maksupalvelujen ja pankkien maksupalvelutoiminnassa. Huomioitavaa lisäksi on se, että sähköinen tunnistaminen tapahtuu Suomessa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (”tunnistuslaki” 617/2009) määräämissä puitteissa. Kansallinen tunnistuslaki täsmentää EU:n ns. eIDAS-asetusta. EU:n

eIDAS-asetuksessa määritellään Euroopan tasolla pohja, vaatimukset ja tunnistamistaso kaikille vahvaa sähköistä tunnistamista tarjoaville tai välittäville toimijoille Euroopassa.

1.2 Tutkimusaiheen rajaus

Opinnäytetyöni aihe on sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta. Nimenomaisesti tutkimusaiheeni koskee suomalaisten palveluntarjoajien tarjoamia sähköisiä palveluita ja vahvaa sähköistä tunnistamista **kuluttajan näkökulmasta, yksittäisen kansalaisen näkökulmasta** tai **verkkopalvelun loppukäyttäjän näkökulmasta.** En esimerkiksi käsittele työssäni julkishallinnon organisaation tai osakeyhtiön puolesta tapahtuvaa edustautumista sähköisissä palveluissa (organisaatiovaltuutukseen perustuva sähköinen tunnistaminen Suomi.fi -palvelussa tai muuhun valtuutukseen, kuten Finnish Authenticator -tunnistuspalveluun, perustuvaan sähköiseen asiointiin organisaation puolesta).

Tutkimusongelmanani on selvittää, millä tavalla toteutettuna verkossa asioivan ihmisen tunnistaminen täyttää vahvan sähköisen tunnistamisen kriteerit? Mitä tämä tarkoittaa kuluttajan näkökulmasta asiaa tarkasteltuna? Tutkimusaiheen tarkastelu perustuu sekä kirjallisuuskatsaustyyppiseen aihepiirin nykytilan ja sitä vahvasti sääntelevän lainsäädännön selvittämiseen, pienimuotoisen kyselytutkimuksen toteuttamiseen sekä omakohtaisten verkkoasiointikokemusteni analysoimiseen sähköisissä viranomaispalveluissa ja yksityissektorin palveluissa. Tutkimukseni ulkopuolelle jäävät niin ikään seikat liittyen digitaaliseen henkilöllisyyteen (kutsutaan myös nimellä ”digitaalinen identiteetti”), tarkemman kuvauksen antaminen Suomen julkishallinnon organisaatioiden e-asiointipalveluiden edellyttämästä Suomi.fi-tunnistuksesta sekä tunnistamisvälineelle asetettavista teknisistä ja turvatekijätyyppisistä vaatimuksista. Syytä on myös mainita, että vaikka tarkastelenkin tutkimusongelmaani kuluttajan näkökulmasta, minulla ei ole mahdollisuutta tässä opinnäytetyössä käydä läpi kuluttajansuojalain (38/1978) laajoja säännöksiä koskien etämyyntiä, etämyyntiin liittyviä kuluttajan oikeuksia tai ko. laissa kuluttajalle suunnatun markkinoinnin ja suoramarkkinoinnin asialliselle toteutukselle säädettyjä vaatimuksia. Nimenomaisesti opinnäytetyöni ulkopuolelle olen myös jättänyt sähköisen viestinnän palveluista annetun lain (917/2014) säännökset koskien sähköistä suoramarkkinointia kuluttajalle sekä sähköisen viestinnän palveluista annetussa laissa käsitellyt tietoyhteiskunnan palveluja koskevat säännökset. Kaikilla edellä mainituilla, opinnäytetyöni ulkopuolelle rajatuilla säädöksillä ja laeilla on liittymäkohdat tutkimusongelmaani. Jos opinnäytetyön pituus tulisi kuitenkin voida pitää noin 40–60 sivuisena, ja aihepiiriltään riittävän rajattuna, on siksi rajausvalintoja tehtävä karkealla kädellä.

Tutkimusaiheeseeni vaikuttavan lainsäädännön laajuudesta saa kuvan tutustumalla opinnäytetyöni liitteeseen numero 1 (Säädösten lyhenteet). Siinä olen esitellyt opinnäytetyössäni käytetyn keskeisen lainsäädännön ja säädösten lyhenteet siten kuin kansallisen lainsäädännön hakemiseen

tarkoitetun Finlex-palvelun viitetiedoissa on niihin viitattu. EU-peräisen lainsäädännön osalta ei vastaavassa EU-oikeuden hakemiseen tarkoitetussa EUR-Lex-palvelussa ollut valitettavasti käytössä samanlaista ”säädösten lyhenteet” -viitetieto-osiota, josta olisi voinut suoraan poimia käyttäväksi vakiintuneet EU-säädösten lyhenteet. Aihepiirin aiempaan tutkimukseen, oikeuskirjallisuuteen ja muuhun lähdeaineistoon perehdyttyäni huomasin kuitenkin myös EU-oikeuden säädöksistä käytetyn tiettyjä, lyhyempiä vakiintuneen kaltaisia lyhenteitä, kuten esimerkiksi ”EU:n PSD 2 -direktiivi” tai ”EU:n toinen maksupalveludirektiivi”. Päädyin EU-oikeuden säädöksiin viittaamisen osalta siihen ratkaisuun, että säädökseen ensimmäisen kerran opinnäytetyössä viitatessani mainitsin säädöksen koko nimen sekä siitä käytetyn lyhenteen. Sitten liitin mielestäni vakiintuneen kaltaiset EU-oikeuden säädösten lyhenteet opinnäytetyöni liitteeseen numero 1 (Säädösten lyhenteet). Edellä esitelty PSD 2 -direktiivi on esimerkiksi koko nimeltään ”Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta”. Luettavamman suomen kielen vuoksi olen käyttänyt tästä säädöksestä jatkossa vain lyhennettä PSD 2 -direktiivi tai EU:n toinen maksupalveludirektiivi. Myös oikeuskirjallisuudessa sekä esimerkiksi suomalaisten pankkien verkkosivuilla, joilla EU:n toisen maksupalveludirektiivin asiakkaan tunnistamisvaatimuksista kuluttajille pyrittiin selkokielellä kertomaan, käytettiin säädöksestä nimeä PSD 2 -direktiivi tai EU:n toinen maksupalveludirektiivi.

2 Tietoperusta

Tutkimukseni keskiössä oleva käsite ”tunnistaminen” tarkoittaa menettelyä, jossa tunnistetaan (yksilöidään) sähköisen verkkopalvelun tai -järjestelmän loppukäyttäjä. Loppukäyttäjällä tarkoitetaan tutkimuksessa henkilöä (ihmistä). Seuraavaksi esitellään tutkimuksessani käytettäviä muita merkittäviä käsitteitä ja termejä sekä niiden taustalla vaikuttavaa oleellista lainsäädäntöä. Tutkimuksessani käytetään paljon erilaisia käsitteitä ja termejä, joihin niin arkikielisessä tekstissä kuin oikeudellisessakin tekstissä viitataan. Arkikielessä ihmiset voivat puhua ”vahvasta sähköisestä tunnistamisesta” tai ”sähköisestä identiteetistä”. Toisaalta myös IT-alalla työskentelevät henkilöt ja ICT-palveluntarjoajat käyttävät puheessaan ja teksteissään samoja käsitteitä. Lainsäätäjän käsitteille antama merkitys on kuitenkin seikkaperäisempi kuin mitä tavalliset ihmiset osana arkielämäänsä käsitteistä puhuvat ja miten niihin arjen tilanteissa viitataan. Tutkimuksessani käsitteitä ja termejä käytetään pääosin siinä merkityksessä kuin lainsäätäjä on ne eri laeissa, yksityiskohtaisesti määritellyt. Tästä johtuen tulen tutkimukseni aluksi esittelemään keskeiset kansalliset lait ja eurooppalaiset säädökset, joissa vahvaa sähköistä tunnistamista, sähköisiä luottamuspalvelutarjoajia, verkkopalvelutarjoajille asetettavia vaatimuksia ja sähköisten palveluiden vaatimuksia on ainakin kuvattu.

2.1 Keskeiset käsitteet

Tutkimuksessani käytetään seuraavaksi esiteltäviä käsitteitä ja termejä siinä merkityksessä kuin lainsäätäjä on ne käsitettä/käsitteitä koskevissa säädöksissä määritellyt.

2.1.1 Verkkopalvelu

Tutkimuksessani verkkopalvelulla tarkoitetaan kaikkia Internetin välityksellä tarjottavia sähköisiä asiointipalveluja, myyntipalveluja, verkkokaupankäynnin alustoja, kulttuurialan palveluja sekä sosiaalisen median palveluja. Verkkopalvelu -käsitettä käytetään tutkimuksessani samassa merkityksessä kuin digitaalisista palveluista annetussa laissa viitataan digitaalisen palvelun käsitteeseen (digipalvelulaki 2 §). Digitaalisten palvelujen tarjoamisesta annetun lain mukaan *digitaalisella palvelulla* tarkoitetaan verkkosivustoa tai mobiilisovellusta sekä niihin liittyviä toiminnallisuuksia (digipalvelulaki 2 §). Tomi Voutilainen on teoksessaan ”Digitaalisten palvelujen sääntely” avannut vielä tarkemmin digipalvelulain tarkoittaman digitaalisen palvelun käsitettä. Voutilaisen (2020), mukaan digitaaliset palvelut ja niiden osiot voidaan jakaa viiteen ryhmään:

- Tietopalvelut ja tiedottamispalvelut, joissa asiakkaalle tarjotaan tietoa palveluntarjoajasta ja sen palveluista;

- Asiakaspalautepalvelu, jossa asiakkaat voivat antaa palautetta palveluista tai osallistua keskusteluun, jolla pyritään kehittämään asiakaspalvelua;

- Tiedonkeruupalvelu, jossa tietojenluovuttaja voi toimittaa viranomaiselle sähköisesti lain edellyttämiä tietoja, esimerkiksi erilaisia ilmoituksia;

- Vireillepanopalvelu / yksisuuntaisen viestinnän mahdollistava palvelu, jossa asiakkaalle tarjotaan mahdollisuus täyttää esimerkiksi hakemuslomake sähköisesti ja lähettää se sähköisiä tiedonsiirtomenetelmiä hyödyntäen viranomaiselle;

- Vuorovaikutteisen sähköisen asioinnin mahdollistavat palvelut, joissa asiakas voi tarkastella viranomaisen järjestelmässä olevia omia tietojaan, täyttää hakemuslomakkeita niin, että osa tiedoista täydentyy lomakkeelle viranomaisen järjestelmästä, jättää hakemuksensa sähköisesti, seurata asiansa käsittelyn etenemistä ja saada päätöksen hakemukseensa sähköisesti. (Voutilainen 2020, 24–29.)

Yleiskielessä käytetään myös *sähköisen palvelun* käsitettä viitattaessa digitaaliseen palveluun tai viitattaessa *verkkopalveluun*. Alan kirjallisuuteen ja verkon eri keskustelupalstoilla käytyyn aihepiirin keskusteluun tutustuttuani olen huomannut, että keskustelupalstakirjoittajat ja alan asiantuntijat viittaavat sähköinen palvelu -käsitteeseen, digitaalinen palvelu -käsitteeseen (tai sen lyhyempään versioon, ”digipalvelu”) sekä verkkopalvelu -käsitteeseen rinnakkain ja usein myös synonyymisesti. Koska jokin linja on valittava, ja koska jokin näistä edellä mainituista, usein samaa tarkoittavista käsitteistä on valittava, olen valinnut tutkimuksessani käytettävän *verkkopalvelu* -käsitettä. Perustelen valintaani sillä, että verkkopalvelu -käsite on yleiskielellä ymmärrettävä käsite (helpommin ymmärrettävä kuin esimerkiksi digitaalinen palvelu -käsite). Ollakseni tarkka ja saadakseni tutkimuksessani käytettävälle avainkäsitteelle mieluummin lainsäätäjän antaman määritelmän kuin itse muotoilemani määritelmän, niin käytän tutkimuksessani verkkopalvelu -käsitettä samassa merkityksessä kuin digitaalinen palvelu -käsitettä käytetään digipalvelulaissa.

2.1.2 Verkkopalvelun tarjoaja

Tutkimuksessani verkkopalveluntarjoajalla viitataan yritykseen tai organisaatioon, joka on verkossa tarjottavien myyntipalvelujen, verkkokaupankäyntialustojen, viranomaisen sähköisten asiointipalvelujen, kulttuurialan palvelujen tai verkossa tarjottavien sosiaalisen median palvelujen takana. Verkkopalvelun tarjoajasta käytetään välillä myös lyhyemmin termiä palveluntarjoaja.

2.1.3 Tunnistaminen

Tunnistaminen on menettely, jossa tunnistetaan verkkopalvelun loppukäyttäjä. Tunnistamisen tarkoitus on erottaa loppukäyttäjät toisistaan käyttäen jotakin tunnistetta. Tunniste voi olla esimerkiksi tietojärjestelmän käyttäjätunnus, Suomessa asuvan henkilön yksilöivä henkilötunnus tai loppukäyttäjän sormenpäistä otettu sormenjälkitunniste (Kyberturvallisuuskeskus 2021a; Voutilainen 2020,

48–56). Vahvalla sähköisellä tunnistamisella voi varmistaa verkkopalvelun loppukäyttäjän henkilöllisyyden sähköisessä asioinnissa. Luotettavana pidetty toimija – kuten suomalainen pankki tai teleoperaattori, joka kuuluu Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ylläpitämään kansalliseen luetteloon hyväksytyistä luottamusverkoston palveluntarjoajista – takaa tunnistautujan henkilöllisyyden. (Kyberturvallisuuskeskus 2021a; Metsola 2018.)

Toisaalta tunnistamista voidaan toteuttaa myös ns. heikkona sähköisenä tunnistamisena tai kevyenä tunnistamisena, jos se nojautuu vain yhteen tunnistamisen tapaan. Tällaisia kevyen tunnistamisen tapoja ovat:

- käyttäjätunnus ja salasana

- pelkkä varmenteellisen sirukortin esittäminen tai pelkkä puhelinsoitto matkapuheli mesta tai matkapuhelimeen tai

- pelkkä biotunnistaminen.

(Kyberturvallisuuskeskus 2021a; Valtionvarainministeriö 2006, 19.)

Tunnistamista kutsutaan vahvaksi, kun sen mahdollistamana voidaan luotettavasti yksilöidä ja todentaa palvelun käyttäjän henkilöllisyys. Vahva tunnistaminen koostuu kolmen eri vaatimuksen yhdistelmästä, joista vähintään kahden on toteuduttava samanaikaisesti, jotta tunnistustapahtuma täyttää vahvan sähköisen tunnistamisen määritelmän (Kyberturvallisuuskeskus 2021a).

Vahva sähköinen tunnistaminen edellyttää:

1) jotain, mitä verkkopalvelun loppukäyttäjä tietää (kuten järjestelmän käyttäjätunnus);

2) jotain, mitä verkkopalvelun loppukäyttäjä omistaa tai mikä on hänen hallussaan (kuten avaintunnuslista tai kertakäyttöisiä tunnuksia generoiva laite, varmenne, sirukortti tai muu väline);

3) jotain, mitä verkkopalvelun loppukäyttäjä fyysisesti omaa (kuten henkilön omat sormenjäljet tai silmän iiristunniste). (Kyberturvallisuuskeskus 2021a; Mitrunen, Salovaara & Viskari 2019, 19–23.)

Vahva sähköinen tunnistaminen perustuu Suomessa kansallisessa väestötietojärjestelmässä sähköisesti ylläpidettäviin henkilöä koskeviin tietoihin, joista tunnistamisen kannalta oleellinen on henkilön yksilöivä ***henkilötunnus***. Kansalaisen sähköiseen identiteettiin voidaan sähköisesti ja henkilötunnusta yhdistämisen avaimena hyödyntäen yhdistää selkeästi todennettavissa olevaa, muista lähteistä peräisin olevaa tietoa. Asiointipalveluille tarjottavassa tunnistuspalvelussa on käytännössä ja yksinkertaistetusti kysymys siitä, että tunnistuspalvelu ilmoittaa käyttäjällä olevaa

tunnistusvälinettä hyödyntäen asiointipalvelulle käyttäjän henkilötunnuksen. (Kyberturvallisuuskeskus 2021a; tunnistuslaki 6–8 §; Voutilainen 2020, 48–51.)

Suomessa vahvan sähköisen tunnistamisen välineinä toimivat tällä hetkellä suomalaisten pankkien myöntämät verkkopankkitunnukset, teleyritysten tarjoamat mobiilivarmenteet, Digi- ja väestötietoviraston myöntämä sähköinen kansalaisvarmenne (yhdistettynä poliisin myöntämään henkilökorttiin) sekä sirullinen, varmenteen sisältävä organisaatiokortti (Kyberturvallisuuskeskus 2021a; tunnistuslaki 8–12 a §).

Organisaatiokortti on organisaatioiden työntekijöille tarkoitettu varmennekortti, jolla voi esimerkiksi kirjautua julkishallinnon sähköisiin asiointipalveluihin ja organisaation omiin tietojärjestelmiin. Korttia voi käyttää myös muun muassa sähköisiin allekirjoituksiin ja toimitilojen kulkutunnisteena. (Kyberturvallisuuskeskus 2021a.)

Suomessa vahvin asema sähköisen tunnistamisen markkinoilla on pitkään ollut pankin myöntämillä verkkopankkitunnisteilla, jotka ovat yli 90 prosentilla väestöstä käytössä (Tuorila 2016, 13–18).

2.1.4 Ensitunnistaminen

Ensitunnistamisella tarkoitetaan tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä. Jäljempänä tässä opinnäytetyössä tarkemmin esiteltävän kansallisen tunnistuslakimme mukaan ensitunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. (Liikenne- ja viestintävirasto, Traficom 2021; tunnistuslaki 2–27 §.) Tunnistusvälineen luotettavuuteen liittyy useita eri osatekijöitä, kuten itse tunnistusväline teknisine ja turvaominaisuuksineen, välineen rekisteröintiprosessi ja ensitunnistamisen tapa. Sähköisen tunnistusvälineen hakijan henkilöllisyyden luotettava todentaminen on yksi tunnistuslain kriittisimmistä velvoitteista ja välttämätön perusta sähköisen tunnistamisen luotettavuudelle (Liikenne- ja viestintävirasto, Traficom 2021). Ensitunnistaminen tulisi siksi voimassa olevan tunnistuslain mukaan tehdä virallisen asiakirjan, kuten passin tai henkilökortin perusteella (Liikenne- ja viestintävirasto, Traficom 2021; tunnistuslaki 2–27 §). Huomioitavaa on se, että ajokortti ei ole kuulunut hyväksyttäviin henkilöllisyyden todistaviin asiakirjoihin enää vuoden 2019 alusta lukien, eikä tunnistusvälineen hakijan henkilöllisyyttä voida siten ensitunnistamisen yhteydessä tarkistaa ajokortista. Huomioitavaa on myös, että ensitunnistamisessa käytettäviksi sallittujen asiakirjojen lista on Suomessa rajattu tunnistuslaissa melko suppeaksi. Se rajoittuu pääsääntöisesti vain Euroopan talousalueen jäsenvaltioiden viranomaisten myöntämiin passeihin tai henkilökortteihin. (Liikenne- ja viestintävirasto, Traficom 2021; tunnistuslaki 17 §.) Todisteeksi tästä käy katkelma tunnistuslain 17 §:stä. Tunnistuslain 17 §:ssä säädetään oletusarvoisesti luotettavista asiakirjoista ja valtioista. Tunnistuslain 17 §:n mukaan ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä

osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa olevat Euroopan talousalueen jäsenvaltioiden sekä Sveitsin tai San Marinon viranomaisen myöntämät passit tai henkilökortit (tunnistuslaki 17 §). Näin ollen lähtökohtaisesti Euroopan alueen ulkopuolelta tulevan henkilön passi tai henkilökortti (esimerkiksi australialaisen henkilön australialainen passi) ei ole Suomessa oletusarvoisesti luotettava asiakirja (eikä Australia näin ollen ole tunnistuslakimme määritelmän mukainen luotettava valtio, siinä missä tunnistuslaki kuvailee Euroopan talousalueen jäsenvaltioiden sekä Sveitsin ja San Marinon olevan luotettavia valtioita). (tunnistuslaki 17 §.)

Kansallisessa tunnistuslaissamme säädetään kuitenkin ***tunnistuspalvelun tarjoajan oikeudesta*** hyväksyä muun valtion passi. Tunnistuslain 17.2 §:n mukaan ***halutessaan tunnistusvälineen tarjoaja voi käyttää*** henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia (tunnistuslaki 17 §). Tunnistusvälineitä tarjoavina tunnistuspalveluvälinetarjoajina toimivat Suomessa käytännössä lähinnä yksityiset pankit ja teleoperaattorit. Tunnistuslain 17.2 §:n mukaan tunnistusväline palveluntarjoajina pankkien ja teleoperaattorien ei kuitenkaan ole mikään pakko käyttää henkilöllisyyden varmentamisessa muun valtion kuin laissa lueteltujen Euroopan alueen valtioiden viranomaisen myöntämää voimassa olevaa passia (tunnistuslaki 17 §). Tunnistuspalvelun tarjoajaa ei tähän siis velvoiteta. Muiden valtioiden passien osalta ***tunnistuspalvelun tarjoajalle annetaan vain itselleen mahdollisuus valita ne valtiot***, joiden viranomaisten myöntämät passit se katsoisi voivansa hyväksyä. Valinta perustuu aina organisaation itse tekemään riskiarvioon, jolloin oletettavaa on, että riskien määrä kasvaa tällaisten, ei-oletusarvoisesti hyväksyttyjen eurooppalaisten valtioiden myöntämien passien osalta. (tunnistuslaki 17 §.)

2.1.5 Tunnistusväline vahvan sähköisen tunnistamisen keskiössä

Tunnistusvälineen hakijan henkilöllisyyden varmentamisen tulisi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, joita ovat valtion myöntämä passi tai henkilökortti, tai toiseen, henkilön käytössä jo olevaan vahvaan sähköiseen tunnistusvälineeseen. Käytännössä viimeksi mainittu tarkoittaa, että esim. mobiilivarmenteen luomisen ja myöntämisen yhteydessä ensitunnistaminen voidaan tehdä sähköisessä palvelussa käyttäen pankkitunnuksia. Tätä sähköisen tunnistusvälineen hyödyntämistä toisen sähköisen tunnistusvälineen luomisprosessissa sanotaan ***ensitunnistamisen ketjuttamiseksi***. (Kyberturvallisuuskeskus 2021a; tunnistuslaki 17 §; Voutilainen 2020, 48–51.)

Suomessa hyväksytään tunnistautumisen välineeksi fyysisessä tunnistamistilanteessa passi ja henkilökortti, jotka molemmat ovat poliisin myöntämiä asiakirjoja. Tunnistamisprosessissa poliisi varmistaa väestötietojärjestelmästä, että kyseinen henkilö on olemassa ja elossa, sekä hakee järjestelmästä passiin tai henkilökorttiin merkittävät tiedot kuten henkilön etu- ja sukunimen. Mikäli henkilö ei aikaisemmin ole saanut passia tai henkilökorttia, tai edellisestä sormenjälkien

ottamisesta on enemmän kuin kuusi vuotta, hänen on tultava asioimaan henkilökohtaisesti poliisin lupapalvelupisteeseen, missä häneltä otetaan sormenjäljet. Lisäksi henkilön on käytävä valokuvaamossa, joka lähettää passikuvan sähköisesti poliisille. (Kyberturvallisuuskeskus 2021a; tunnistuslaki 17 §; Voutilainen 2020, 48–51.)

Liittämällä henkilön kuva passiin tai henkilökorttiin, mahdollistetaan henkilön tunnistus toisaalla tätä dokumenttia käyttäen. Henkilökortin tapauksessa luodaan lisäksi digitaaliset varmenteet, joiden avulla henkilö voi tunnistautua sähköisesti ja luoda sähköisiä allekirjoituksia. Passia tai henkilökorttia käyttämällä henkilö voidaan tunnistaa asiointipisteessä ja myöntää hänelle jokin sähköinen tunnistusväline, esimerkiksi pankkitunnukset. (Mitrunen ym. 2019, 19–23; tunnistuslaki 17 §.)

2.2 Keskeinen lainsäädäntö

Opinnäytetyöni aihepiiriin liittyy olennaisesti aihetta sääntelevä kansallinen ja eurooppalainen lainsäädäntö. Monet opinnäytetyöni käsitteet on myös kuvattu lainsäätäjän toimesta, joten siksi keskeiset lait ja muut säädökset on syytä esitellä tutkimuksessani riittävällä tarkkuudella. Keskeistä tutkimusaiheeni lainsäädäntöä ryhdyin kartoittamaan siten, että hain Internetin hakukoneiden sekä kansallisen lainsäädännön Finlex-palvelun (https://www.finlex.fi/fi/laki/) ja Euroopan unionin lainsäädännön EUR-Lex-palvelun (https://eur-lex.europa.eu/homepage.html?locale=fi) avulla, muun muassa hakusanoilla ”sähköinen tunnistaminen”, ”vahva sähköinen tunnistaminen”, ”sähköiset asiointipalvelut”, ”digitaaliset palvelut” ja ”sähköinen viranomaisasiointi” lainsäädäntöviitteet. Löytämistäni hakutuloksista otin tarkemman tarkastelun kohteeksi ne kansalliset lait ja EU-oikeuden asetukset ja direktiivit, jotka oleellisesti liittyisivät tutkimusongelmaani. Merkittävänä apuvälineenä lainsäädäntöviidakossa toimi Tomi Voutilaisen vuonna 2020 julkaisema teos ”Digitaalisten palveluiden sääntely”. Kyseisen teoksen avulla sain helpommin selkoa siitä, että mitkä lait tai EU-oikeuden asetukset ja direktiivit mitäkin asiaa tai aihepiiriä määrittivät, ja mitkä lakitekstit toisaalta eivät olleet minun tutkimusongelmani kannalta olennaisia lainkaan.

2.2.1 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista

Vaatimukset vahvalle sähköiselle tunnistamiselle on määritelty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (tunnistuslaki, 617/2009). Tunnistuslain 2 §:ssä määritellään, että ***vahvalla sähköisellä tunnistamisella*** tarkoitetaan sellaista henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää eIDAS-asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset (tunnistuslaki 2 §; eIDAS-asetus 8 artikla, 2 kohdan b alakohta). Suomessa kansallisen vahvan tunnistamisen palveluntarjoajien muodostaman luottamusverkoston perusteista on säädetty vuonna 2017 päivitetyllä tunnistuslain muutoksilla. Päivitytyn tunnistuslain mukaan kaikkien markkinaehtoisesti

vahvaa tunnistamista tarjoavien (tunnistusvälineen tarjoajat) tai välittävien (tunnistusvälityspalvelun tarjoajat) toimijoiden on kuuluttava luottamusverkostoon. Luottamusverkoston jäsenten on annettava liikkeelle laskemansa tunnistusväline luottamusverkostossa edelleen välitettäväksi. Suomessa on päätetty, että Liikenne- ja viestintäviraston Traficomin alaisuudessa toimiva Kyberturvallisuuskeskus valvoo Suomen kansallisia luottamuspalveluita tarjoavia palveluntarjoajia, ja myöntää niille tarpeen vaatiessa ja tiettyjen kriteerien täytyttyä ns. hyväksytyn statuksen. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b.) Tunnistuslain 10 §:ssä säädetään uuden markkinoille tulevan tunnistuspalvelun tarjoajan velvollisuudesta ilmoittaa toiminnan aloittamisesta Liikenne- ja viestintävirastolle. Vahvan sähköisen tunnistuspalvelun tarjoajat, jotka ovat tehneet tunnistuslain mukaisen ilmoituksen ja jotka täyttävät lain vaatimukset, muodostavat suoraan lain nojalla sähköisen tunnistamisen luottamusverkoston (tunnistuslaki 10–16 §; Kyberturvallisuuskeskus 2021b). Luottamusverkoston toimintamallin tavoitteena on, että sähköiset asiointipalvelut voivat hankkia sähköistä tunnistamista asiointipalveluunsa keskitetysti tunnistusvälityspalvelulta tarvitsematta tehdä sopimuksia kaikkien tunnistusvälineen tarjoajien kanssa. Mallin toivotaan helpottavan ja lisäävän vahvan tunnistamisen hyödyntämistä asiointipalveluissa. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b; tunnistuslaki 10–16 §.)

Luottamusverkostossa on kaksi erilaista tunnistuspalveluiden tarjoamisen roolia. Tunnistuspalvelun tarjoaja voi tarjota sähköisiä tunnistusvälineitä loppukäyttäjille (välineen tarjoaja) tai se voi välittää tunnistustapahtumia sähköisten palveluiden tarjoajille (tunnistusvälityspalvelu). Tunnistusvälineen tarjoaja voi harjoittaa myös välitystoimintaa eli tunnistuksen tarjontaa asiointipalveluille. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b; tunnistuslaki 10–16 §.)

Liikenne- ja viestintävirasto niin ikään ylläpitää luetteloa Suomeen sijoittuneista vahvaa sähköistä tunnistamista tarjoavista palveluntarjoajista sekä niiden tarjoamista palveluista (tunnistuslaki 12 a §). Hyväksytyt luottamuspalvelut löytyvät kansallisista luotetuista luetteloista (trusted list), jotka ovat päteviä kaikissa EU:n jäsenvaltioissa. Liikenne- ja viestintäviraston ylläpitämä Suomen kansallinen hyväksytty luettelo löytyy verkko-osoitteesta: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.kyberturvallisuuskeskus.fi%2Fsites%2Fdefault%2Ffiles%2Fmedia%2Ffile%2FTunnistuspalvelurekisteri_31052022.XLSX&wdOrigin=BROWSELINK

(Kyberturvallisuuskeskus 2021b). Suomessa hyväksyttyjen sähköisten tunnistus- ja luottamuspalveluntarjoajien luettelossa oli 15.6.2022 haettuna listattu 17 luottamuspalveluntarjoajaa. Näistä 10 oli Suomessa toimivia pankkeja (pankin verkkopankkitunnus/pankin tunnistuspalvelu), näistä 3 oli Suomessa toimivia teleoperaattoreita (teleoperaattorin mobiilivarmenne), näistä 1 oli Suomessa toimiva viranomaistoimija, Digi- ja väestötietovirasto (kansalaisvarmenne, organisaatiovarmenne) ja näistä 3 oli sellaista Suomessa toimivaa ICT-palveluntarjoajaa, jotka eivät itse suoraan

tarjonneet omaa pankkitunnusta tai mobiilivarmennetta, mutta jotka välittivät luotettavasti sähköisessä asioinnissa muiden palveluntarjoajien tunnistusvälineitä eteenpäin ja näin ollen mahdollistivat luottamuksellisen verkkoasioinnin. (Kyberturvallisuuskeskus 2021b.)

2.2.2 EU:n eIDAS-asetus

EU:n eIDAS-asetus eli ”Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta”, on yksinkertaisesti tiivistettynä EU-säädös, joka koskee luotettavuusvaatimuksia ja sähköisen tunnistamisen vaatimuksia (EU:n eIDAS-asetus, EU 2014/910).

Luotettavuusvaatimuksia ja sähköisen tunnistamisen vaatimuksia tarkastellaan suhteessa sähköisissä verkkopalveluissa käytettäviin toimintoihin, joita kutsutaan eIDAS-asetuksessa puolestaan ”luottamuspalveluiksi” (trust services). eIDAS-asetuksen keskeinen idea on se, että sen mahdollistamana tarjotaan sähköisiä tunnistusvälineitä, joilla on mahdollista tunnistautua julkisen hallinnon palveluissa koko EU:ssa. eIDAS-asetus tuli voimaan 1.7.2016 ja se toi muutoksia myös kansalliseen sähköiseen tunnistamiseen. Tunnistus- ja luottamuspalvelulain vaatimuksia muutettiin vastaamaan EU-sääntelyä. Edellä mainitun lisäksi EU:n eIDAS-asetus sääntelee muun muassa sähköistä allekirjoitusta, sähköisiä leimoja, sähköisiä rekisteröityjä jakelupalveluita ja sähköisiä verkkosivuja ja niiden todentamista sekä kaikkiin edellä mainittuihin asioihin liittyviä vaatimuksia kaikissa EU-jäsenvaltioissa. (EU:n eIDAS-asetus.) EU:n eIDAS-asetus tarjoaa EU-jäsenvaltioiden verkkopalveluntarjoajille ja muille palveluntarjoajille mahdollisuuden osoittaa selkeästi, että sen verkkopalveluita varten tarjoama tuote tai toiminto on luotettava. Kansalliset palveluntarjoajat (kuten pankit, teleoperaattorit, ICT-palveluntarjoajat) voivat halutessaan hakea palvelulleen viranomaishyväksyntää. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b; EU:n eIDAS-asetus.)

2.2.3 Laki sähköisestä asioinnista viranomaistoiminnassa

Sähköisestä asioinnista viranomaistoiminnassa annetussa laissa säädetään siitä, että viranomaistoimijoita kannustetaan tarjoamaan kansalaisille tasapuolisia mahdollisuuksia asioida viranomaisessa ja/tai muussa julkishallinnon organisaatiossa ajasta tai paikasta riippumatta (laki sähköisestä asioinnista viranomaistoiminnassa, ”asiointilaki”, 13/2003).

Asiointilain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa sekä edistää digitaalisten tiedonsiirtotapojen hyödyntämistä. Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa (asiointilaki.)

2.2.4 Laki digitaalisten palveluiden tarjoamisesta

Digitaalisten palveluiden tarjoamisesta annetussa laissa todetaan, että viranomaisen on tarjottava jokaiselle mahdollisuus toimittaa asiointitarpeeseensa liittyvät sähköiset viestit ja asiakirjat käyttäen digitaalisia palveluita (digipalvelulaki 5 §). Digipalvelulaissa viranomaisen käsite on laaja, koska lain määritelmäpykälän mukaan viranomaisella tarkoitetaan lähes kaikkia julkishallinnon alalla toimivia tahoja, jotka hoitavat julkista hallintotehtävää – esimerkiksi ammattikorkeakoulu tulkitaan viranomaiseksi digipalvelulain mukaan, koska ammattikorkeakoulu toimii merkittävältä osin julkishallinnon alalla hoitaen julkisia hallintotehtäviä (ammattikorkeakoulun suorittama opiskelijavalinta on esimerkiksi ammattikorkeakoululle uskottu julkinen hallintotehtävä). Digipalvelulain mukaisella viranomaisella tarkoitetaan valtion viranomaisia, valtion liikelaitoksia, hyvinvointialueen ja hyvinvointiyhtymän viranomaisia, kunnallisia viranomaisia, eduskunnan virastoja, tasavallan presidentin kansliaa, itsenäisiä julkisoikeudellisia laitoksia ja Suomen itsenäisyyden juhlarahastoa sekä *”mitä tässä laissa säädetään viranomaisesta, sovelletaan myös ortodoksiseen kirkkoon sekä sen seurakuntiin, yliopistolain tarkoittamiin yliopistoihin, ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin sekä muuhun toimijaan siltä osin kuin se hoitaa julkista hallintotehtävää”*. (digipalvelulaki 2–5 §.)

Digipalvelulain 6 §:n mukaan viranomainen voi vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista ***vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi*** tai ***palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi*** (digipalvelulaki 6 §). Digipalvelulain soveltamisalan piiriin kuuluvalla ammattikorkeakoululla on siis oikeus vaatia opiskelijoiltaan sähköistä tunnistamista ainoastaan, mikäli se on tarpeen jonkin korkeakoulun palvelun käyttöoikeuksien varmistamiseksi tai korkeakoulupalvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi.

Toisaalta digipalvelulain samainen pykälä jatkuu lauseella, jossa todetaan, että jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi, palvelun käyttäjä on tunnistettava hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:n 1 momentin 4 kohdassa tarkoitettua luonnollisen henkilön tunnistuspalvelua, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 momentin 1 kohdassa tarkoitettua vahvaa sähköistä tunnistamista tai painavasta perustellusta syystä muuta vastaavaa tietoturvallista tunnistuspalvelua käyttämällä. (digipalvelulaki 6 §.)

Digipalvelulaki asettaa reunaehdot toisaalta sille, milloin julkishallinnon toimijalla (viranomaisorganisaatiolla tai viranomaisen kaltaisella toimijalla, kuten ammattikorkeakouluorganisaatiolla) on oikeus vaatia loppukäyttäjän sähköistä tunnistamista. Toisaalta laki asettaa reunaehdot myös sille,

milloin verkkopalvelun käyttäjä on tunnistettava sähköisesti. Jälkimmäinen tilanne on käsillä silloin, jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä loppukäyttäjän nähtäväksi tai käytettäväksi. (digipalvelulaki 6 §.)

2.2.5 EU:n toinen maksupalveludirektiivi (PSD 2 -direktiivi)

EU:n maksupalveludirektiivi (Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, eli ns. EU:n toinen maksupalveludirektiivi, lyhyemmin PSD 2 -direktiivi) on julkaisunsa ja sen kansallisen täytäntöönpanon takarajan myötä alkuvuodesta 2018 lukien velvoittanut erityisesti yksityissektorilla ja verkkokaupankäynnissä toimivia maksupalvelun tarjoajia. Maksupalveluntarjoajat ovat lain myötä velvoitettu tunnistamaan asiakkaansa ja käyttämään vahvaa sähköistä tunnistamista tietynlaisessa palvelutoiminnassa, esim. luottopalvelujen, maksupalvelujen ja pankkien maksupalvelutoiminnassa (PSD 2 -direktiivi). PSD 2 -direktiivin tavoitteena on ollut saattaa erilaiset maksupalvelut entistä laajemmin yhtenäisen eurooppalaisen lainsäädännön piiriin. Suomessa PSD 2 -direktiivi on saatettu kansallisesti voimaan kahden eri kansallisen lain täydentämisen myötä: kansallista maksupalvelulakiamme muutettiin lailla 898/2017 ja maksulaitoslakia muutettiin lailla 890/2017 vastaamaan PSD 2 -direktiivin yhteiseurooppalaisia vaatimuksia. Kansallisessa maksupalvelulaissa (”maksupalvelulaki”, 290/2010) on aiemmin esitellyn tunnistuslain ohella määritelty se, mitä ”vahvalla tunnistamisella” tarkoitetaan. Maksupalvelulain 8 §:n 1 momentin 24 kohdan mukaan ***vahvalla tunnistamisella*** tarkoitetaan maksupalvelun loppukäyttäjän sähköistä tunnistamista, jossa suojataan tunnistamistiedon luottamuksellisuutta ja käytetään menettelyä, joka perustuu vähintään kahteen seuraavista kolmesta toisistaan riippumattomasta vaihtoehdosta:

a) johonkin, mitä vain maksupalvelun käyttäjä tietää;

b) johonkin, mitä vain maksupalvelun käyttäjällä on hallussaan;

c) maksupalvelun käyttäjän yksilöivään ominaisuuteen. (maksupalvelulaki 8 §.)

Maksupalvelulain 85 c §:ssä puolessaan on säädetty siitä, missä tilanteissa palveluntarjoajan tulee vaatia vahvaa tunnistamista. Maksupalvelulain 85 c §:n mukaan palveluntarjoajan on käytettävä vahvaa tunnistamista, jos maksaja:

1) käyttää maksutiliään tietoverkon välityksellä;

2) käynnistää sähköisen maksutapahtuman;

3) toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski. (maksupalvelulaki 85c §.)

Jos maksaja puolestaan käynnistää sähköisen maksutapahtuman etäviestimellä (kuten puhelimella), palveluntarjoajan on myös silloin käytettävä vahvaa tunnistamista, johon yhdistetään maksutapahtuman määrä ja maksunsaaja maksupalveluista sisämarkkinoilla ”…”, annettu ns. ensimmäinen EU:n maksupalveludirektiivi (PSD 1), 97 artiklan 2 kohdassa tarkoitetulla tavalla. Palveluntarjoajan on myös riittävin turvatoimenpitein huolehdittava vahvassa tunnistamisessa käytettävien henkilökohtaisten turvatunnusten luottamuksellisuuden ja eheyden suojaamisesta. (maksupalvelulaki 85c §.) Maksupalvelulaissa on niin ikään velvoitettu palveluntarjoaja huolehtimaan riittävästä tietoturvallisuudesta palvelutapahtuman toteuttamiseen liittyen. (PSD 2 -direktiivi; maksupalvelulaki.)

3 Aiemmista tutkimuksista

Yritysten ja eri organisaatioiden verkkosivuilla on tarjolla paljon erilaisia sähköisiä asiointipalveluita, verkkokauppoja tai muutaman klikkauksen päässä kuluttajalle avautuvia sähköisiä tuotteita. On olemassa sosiaalisen median sähköisiä palveluja, joihin rekisteröityminen ei juurikaan vaadi kuluttajan tai verkkopalvelun loppukäyttäjän sähköistä tunnistamista tai tarkempaa identifiointia. Käyttäjän tunnistaminen verkkopalveluun tapahtuu käyttäjätunnuksen ja salasanan avulla. Itse luodun käyttäjätunnuksen ja salasanan turvin on mahdollista rekisteröityä useampiin sosiaalisen median tai esimerkiksi elokuvateattereiden tai lippupalveluiden verkkopalveluihin: riittää, että on hankkinut itselleen jonkin ilmaissähköpostiosoitteen, jonka voi palveluun rekisteröitymisen yhteydessä verkkopalveluun syöttää käyttäjätunnuksenaan. Käyttäjätunnuksen lisäksi loppukäyttäjän tulee itse keksiä itselleen verkkopalveluun käypä, riittävän pitkä ja monimerkkikriteeristön täyttävä salasana. Sähköpostiosoite käyttäjätunnuksena ja salasana -yhdistelmä toimivat useimmissa, esimerkiksi tapahtuma-alan verkkopalveluissa sekä sosiaalisen median palveluissa loppukäyttäjän identiteetin riittävän luotettavana tunnistamisena. Helena Tuorila on tutkinut erityisesti ikäihmisten verkkopalvelujen käyttämistä siitä näkökulmasta, että minkälaisia ongelmallisia kynnyksiä sähköisten palvelujen käyttöön heillä esiintyy. Tutkimuksessaan Tuorila on tuonut esiin sen, että osa ikääntyvistä suomalaisista ei osaa tai halua käyttää tietoteknisiä laitteita lainkaan. (Tuorila 2017, 106.)

Moni Tuorilan tutkittavista oli kokenut lukuisiin eri sähköisiin palveluihin rekisteröitymisen sekä tähän liittyvän käyttäjätunnus- ja salasana -yhdistelmän keksimisen ja muistamisen vaatimuksen ja hallinnoimisen itsellään siten, että käyttäjätunnusta ja salasana -yhdistelmää per sähköinen palvelu ei suositusten mukaan saisi kirjoittaa itselleen minnekään kirjallisesti ylös, vaan ulkomuistista tulisi voida muistaa eri e-palveluihin rekisteröitymiseen liittyvä käyttäjätunnus- ja salasana -yhdistelmä ja tällä tavalla palveluita käyttää, on tavattoman uuvuttavaa ja hankalaa. Tietoturvallisuuden näkökulmasta niin ikään suositellaan sitä, että loppukäyttäjä keksisi aina eri salasana- ja käyttäjätunnus -yhdistelmän per sellainen verkkopalvelu, jonka käyttö ei edellytä vahvaa sähköistä tunnistamista – ja että keksitty salasana olisi riittävän pitkä ja monimerkkikriteeristön täyttävä. Tällöin tekoälyä hyödyntävä hakurobotti tai muu salasanojen murtamiseen käytettävä apuväline ei pystyisi liian helposti keksimään salasanaa. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b; Valtiovarainministeriö 2017, 44, 53–57.)

Myös Marika Nordlund, Lea Stenberg, Kristina Forsberg, Kirsi Alastalo, Jaana Nykänen, Paula Ranta ja Anne Virkkunen ovat suorittamiensa tutkimusten perusteella päätyneet siihen johtopäätökseen, että ikäihmisten keskuudessa Suomessa havaittu sähköisten palveluiden käyttämisen hankalaksi kokeminen, tai se, että ei osaa tai ei halua käyttää sähköisiä palveluita ja niiden käytön edellytyksenä oleva tietoteknisten laitteiden hankkimisen ja hallinnan vaatimus, on varteenotettava

ongelma. Tämä tutkimushavainto merkitsee sitä, että jotta yhdenvertaisuusperiaate voisi toteutua suomalaisessa yhteiskunnassa ei pelkästään voida lähteä toteuttamaan julkisia eikä yksityisiäkään palveluita siten, että niitä on saatavilla ainoastaan sähköisinä palveluina. (Nordlund ym. 2014, 11–12.) Rinnalla tulee yhä säilyttää perinteiset, fyysiseen asiointiin perustuvat palvelut niin yksityisellä kuin julkisella sektorilla. Lisäksi sekä Tuorila että Nordlund ym. toivat havainnoissaan esille sen, että ikäihmisten lisäksi on myös muita suomalaisia tai Suomessa asuvia väestöryhmiä, jotka eivät osaa tai halua käyttää tietoteknisiä laitteita. (Tuorila 2017; Nordlund ym. 2014.) Osa maahanmuuttajataustaisista, eri-ikäisistä henkilöistä esimerkiksi saattaa jäädä digitaalisen palveluyhteiskunnan ulkopuolelle riittämättömien IT-taitojen, IT-laitteiden kalleuden tai puutteellisen suomen tai englannin kielen kielitaidon vuoksi, jota myös vaaditaan digitaalisia palveluita käytettäessä.

Julkishallinnon organisaatioiden verkkosivuilta ja sähköisistä viranomaispalveluista löytyy erilaisia lomakkeita ja sovelluksia, joiden käyttö ei vaadi erillistä tunnistamista, vaan lomakkeet ovat kaikkien verkkosivuilla vierailevien henkilöiden käytössä. Joissakin sähköisen asioinnin tilanteissa lainsäädäntö kuitenkin asettaa selvät vaatimukset sille, kuka voi ja millä tunnistusvälineellä toteutettuna, hoitaa sähköisen asiointinsa viranomaisen kanssa. Vuodesta 2019 lukien kaikkia julkisen sektorin toimijoita velvoittanut digipalvelulaki sekä vuodesta 2018 yksityisen sektorin maksupalvelun palveluntarjoajia velvoittanut päivitetty maksupalvelulaki, johon vuoden 2018 EU:n PSD 2 -direktiivin vaatimukset sisällytettiin, vaativat tietyissä tilanteissa sähköisten palvelujen palveluntarjoajia tunnistamaan vahvasti asiakkaansa ennen kuin heille pääsy asiointipalveluun sallitaan. Valtionhallinnossa tunnistettiin vuonna 2018 tarve selvittää sitä, kuinka tunnistautuminen julkishallinnon sähköisiin palveluihin olisi tarkoituksenmukaisinta Suomessa järjestää ottaen huomioon edellä mainittu regulaatio, kansainvälisen liikkuvuuden lisääntyminen ja toisaalta digitalisaatiokehityksen senhetkinen tilanne. Julkishallinnon sekä yksityisen sektorin tarjoamien ns. välttämättömyyspalvelujen tarjoajien (kuten pankkipalvelujen, sähköntoimituspalvelujen yms.) tulee huomioida palveluita tarjotessaan sekä niiden saavutettavuus että se, että palvelut olisivat tasavertaisesti mahdollisimman laajasti koko väestön saatavilla henkilön iästä tai fyysisistä rajoitteista huolimatta.

Tätä problematiikkaa on analysoitu Valtionvarainministeriön vuonna 2019 julkaisemassa, aihepiiriin liittyvässä tutkimuksessa: ”Sähköinen tunnistaminen: selvitys nykytilasta sekä -kehittämistarpeista” (Mitrunen ym. 2019, 1–50). Kyseisessä selvityksessä tuodaan esille haaste koskien suomalaisen henkilötunnuksen merkittävää asemaa henkilön ensitunnistamisketjun toteuttamisessa. Ja vaikeudet, jotka nousevat esille, kun sähköisissä palveluissa asioi henkilötunnukseton ei-Suomen kansalainen. Mitrusen, Salovaaran & Viskarin 8.3.2019 julkaiseman selvityksen mukaan henkilöllä, jolla ei ole suomalaista henkilötunnusta, ei ole tarjolla luottamusverkoston tunnistusvälineisiin perustuvaa riittävän vahvaa tapaa tunnistautua sähköisiin asiointipalveluihin. Näin ollen kyseisen ryhmän henkilöiden on käytännössä mahdotonta saada suomalaisen pankin tai mobiilioperaattorin

asiakkuutta, eikä heille myöskään voida myöntää suomalaista henkilökorttia. Henkilötunnustuksettomien ihmisten käyttäjäkunta saattaa pudota digitaalisesti järjestettyjen julkishallinnon ja välttämättömyyspalvelujen ulkopuolelle. (Mitrunen ym., 2019, 11–18.)

Kaihlanen ym. on tutkinut haavoittuvien väestöryhmien etäpalvelujen käyttöä COVID- 19- epidemian aikana. Vuonna 2021 julkaistussa tutkimuksessa Kaihlanen tutkimusryhmineen toi löydöksenään esille sen, että julkisten etäpalvelujen edellyttämien digitaitojen puute oli monelle käytön este, iästä riippumatta (Kaihlanen ym. 2021, 1–4). Digipalveluiden käytön suhteen haavoittuvassa asemassa olevina väestön ryhminä etäpalveluiden käyttöä selvittäneet tutkijat listasivat esimerkiksi vähäisen koulutustaustan omaavat suomalaiset nuoret. Tutkijaryhmän mukaan on olemassa merkittävä määrä aivan kantasuomalaisia kouluttamattomia nuoria, jotka kokevat syrjäytyvänsä yhteiskunnan ja palvelujen kaiken aikaa digitalisoituessa. Seikka voi johtua siitä, että digitaalisten palveluiden käyttö edellyttää yleisen digiosaamisen lisäksi myös muita kykyjä, kuten ymmärrystä suomalaisesta pitkälle kehittyneestä julkissektorin palveluvalikoimasta, digitaalisten palveluiden monimutkaisista merkityssisältöistä ja toiminnallisuuksista sekä esimerkiksi virkakielen asianmukaista hallintaa. (Kaihlanen ym. 2021, 1–4.)

Digitaalisen eriarvoisuuden havaitseminen on herättänyt koronaepidemian aikana ja myös epidemian jälkeiseen aikaan siirryttäessä syvää huolta muidenkin tutkijoiden keskuudessa. Pohdintaa on aiheuttanut muun muassa se, miten he, joilla ei ole tasavertaisia tilaisuuksia, kykyjä tai resursseja käyttää digitaalisia palveluja, ovat saaneet koronaepidemian etäpalveluihin siirtymistrendin (tai pakon) aikana tarvitsemansa palvelut. Terveyden ja hyvinvoinninlaitoksen tukemassa, aihepiiriä koskevassa tutkimuksessa on tarkasteltu hyvinvointiyhteiskunnan sähköisiä palveluja saavutettavuuden ja yhdenvertaisuuden toteutumisen näkökulmasta (Virtanen ym. 2022, 2). Virtanen ym. ovat tuoneet esille sen, että voi olla mahdollista, että maahanmuuttajataustainen, Suomeen tullut henkilö voi olla hyvin aktiivinen sosiaalisen median eri kanavien käyttäjä sekä Internetiä sujuvasti käyttävä henkilö. Tästä huolimatta suomalaisen pitkälle kehittyneen julkissektorin palveluvalikoiman, digitaalisten palveluiden monimutkaisten sisältöjen ja toiminnallisuuksien sekä virkakielen ymmärtämisen kanssa ongelmat kuitenkin saattavat käydä maahanmuuttajataustaiselle väestön ryhmälle niin suuriksi, että julkinen asiointipalvelu verkossa voi jäädä toteuttamatta. (Virtanen ym. 2022, 2; myös Heponiemi ym. 2021.)

4 Empiirinen osa

4.1 Tutkimustyyppinen opinnäytetyö

Tutkimustyyppisessä opinnäytetyössäni pyrin selvittämään sitä, missä tilanteissa vahva sähköinen tunnistaminen on tarpeellista, kun kuluttaja, kansalainen tai verkkopalvelun loppukäyttäjä verkkopalvelua käyttää. Missä tilanteissa lainsäädäntö edellyttää vahvaa sähköistä tunnistamista verkossa olevia sähköisiä palveluita käyttävältä kuluttajalta tai viranomaisen sähköisiä palveluita käyttävältä kansalaiselta? Onko sillä eroa, että käyttääkö kuluttaja julkisen sektorin sähköistä viranomaispalvelua vai käyttääkö hän kaupallista, yksityisen sektorin verkkopalvelua? Vastauksia näihin kysymyksiin hain perehtymällä ensin aihepiiriä sääntelevään regulaatioon. Voutilaisen vuonna 2020 julkaisema teos ”Digitaalisten palveluiden sääntely” auttoi minua merkittävästi ottamaan selkoa siitä, että mitkä lait tai EU-oikeuden asetukset ja direktiivit olivat opinnäytetyöni tutkimusongelman kannalta relevantteja (Voutilainen 2020). Löytämiini lakiteksteihin tutustuin (syvällisen perehtymisen sijaan) enemmän siitä näkökulmasta käsin, että pyrin selvittämään regulaation asettamat ***reunaehdot*** ja vaatimukset vahvan sähköisen tunnistamisen tilanteille. Olin enemmän kiinnostunut siitä, että missä tilanteissa yksityisen sektorin sähköisen asioinnin palveluntarjoaja voi edellyttää vahvaa sähköistä tunnistamista. Tai missä tilanteissa puolestaan julkisen sektorin sähköisen asioinnin palveluntarjoaja voi edellyttää palvelun loppukäyttäjältä vahvaa sähköistä tunnistamista? Onko tilanteita, joissa niin yksityisen kuin julkisen sektorinkin palveluntarjoajan tulee nimenomaisesti vaatia palvelun loppukäyttäjältä vahvaa sähköistä tunnistamista ennen kuin hänelle sallitaan pääsy johonkin e-asioinnin palveluun? Opinnäytetyöni toisessa kappaleessa (2 Tietoperusta -> 2.1 Keskeiset käsitteet ja 2.2 Keskeinen lainsäädäntö) olen kuvannut kartoittamani, mielestäni aihepiiriin oleellisesti liittyvän lainsäädännön. Tietoperusta-kappaleessa esitelty lainsäädäntö nähdäkseni ainakin tulisi ottaa huomioon vuonna 2022, jos haluaa selvittää vahvan sähköisen tunnistamisen vaatimuksia ja toteutustapaa verkkopalveluissa kuluttajan näkökulmasta niin yksityisen kuin julkisen sektorin verkkoasioinnin osalta.

Koska en ole koulutukseltani juristi, ja koska myöskään tutkielmani ei ole oikeustieteen alan tutkielma vaan ammattikorkeakoulun ns. IT-tradenomin koulutusohjelman opintojen loppuvaiheen opinnäytetyö, niin on mahdollista, että kartoittamani lainsäädäntöpohja on joiltakin osin puutteellinen. Huomioitavaa on myös se, että regulaatiota tulee kaiken aikaa lisää niin kotoperäisesti (eduskunta säätää uusia kansallisia lakeja) kuin EU-peräisesti (tulee uusi EU:n asetus suoraan sovellettavaksi kaikissa EU-jäsenvaltioissa tai tulee uusi EU:n direktiivi, joka tulee Suomessa saattaa osaksi kansallista oikeusjärjestystä). Opinnäytetyöni Tietoperusta-kappaleessa esiteltyä keskeistä lainsäädäntöä ei ymmärrykseni mukaan voi ainakaan jättää huomioimatta vuonna 2022, mikäli

haluaisi kuvata vallitsevaa nykytilaa koskien vahvan sähköisen tunnistamisen vaatimuksia ja toteutustapaa verkkopalveluissa kuluttajan näkökulmasta.

Regulaation asettamien reunaehtojen selvittämisen jälkeen halusin myös saada tuntuman käytännön tasolla siihen, miten kuluttajan näkökulmasta näyttäytyy yksityissektorin ja julkisen sektorin sähköisten asiointipalveluiden käyttäminen. Niinpä toteutin pienimuotoisen kyselytutkimuksen ja tutustuin myös itse yksittäisenä kuluttajana ja kansalaisena julkisen sektorin sähköisiin asiointipalveluihin sekä esimerkiksi pankin asiakkaana sähköiseen verkkopankkiasiointiin. Pelkän regulaatiopohjan selvittämisen ohella tarvitsin mielestäni eri-ikäisten kuluttajien ja eri väestönryhmien edustajien käytännön tason asiointikokemusnäkökulmaa mukaan tutkimukseeni. Kyselytutkimusaineisto mahdollisti sen, että pystyin kyselyyni saatujen vastausten avulla hakemaan ratkaisua lisätutkimuskysymyksiini. Lisätutkimuskysymyksiäni niin ikään olivat: miten sähköisen palvelun loppukäyttäjä kokee palveluun tunnistautumisen ja käytön tapahtuvan sujuvan sähköisen asioinnin näkökulmasta? Entä palvelun luotettavuuden ja tietoturvan toteutumisen näkökulmasta?

4.2 Kyselytutkimuksen toteutus ja työtapakuvaus

Toteutin ajalla 24.3.2022 - 8.4.2022 pienimuotoisen Webropol-kyselyn otsikolla ”Sähköisten palvelujen käyttö ja niihin liittyvä loppukäyttäjän tunnistaminen”. Julkaisin Webropol-kyselyn linkin siitä kertovan tutkimustiedotteen ohella kolmella eri sähköisellä alustalla, portaalissa tai sosiaalisen median kanavalla, joissa oletin kussakin vierailevan eri-ikäisiä verkkovierailijoita. Valitsemani eri sähköiset alustat olivat: Haaga-Helia ammattikorkeakoulun opiskelijakunta Helgan käyttämä sähköinen Discord-kanava (nuorien aikuisten käyttämä sähköinen alusta), LinkedIn-portaali (työikäisen väestön työnhakuun ja ammatilliseen verkostoitumiseen käyttämä sähköinen alusta) sekä ET-lehden sähköinen keskusteluareena (ikäihmisten keskusteluareenaksi eniten profiloituva sähköinen alusta).

Tarkoituksenani oli tavoittaa eri-ikäisiä verkkopalvelujen käyttäjiä, jotta otanta voisi jokseenkin tasapuolisesti edustaa sähköisten julkishallinnon palveluiden ja yksityisen sektorin palveluiden käyttäjiä Suomessa. Kyselytutkimukseeni annetut vastaukset kerättiin anonyymisti, eri-ikäisiltä, vapaaehtoisilta verkkopalvelujen käyttäjiltä. Pyrin nimenomaisesti siihen, että en keräisi mitään tunnisteellista tietoa eli henkilötietoa sähköiseen kyselyyn osallistujilta. En halunnut saada tietooni esimerkiksi kyselyyn vastaajien sähköpostiosoitetta, heidän ikäänsä, sukupuoltaan, asuinkuntaansa – saati nimitietojaan. Tarkoituksenani oli, että sähköinen kyselyni voisi anonyymisti, henkilötietojen keräämisen ja käsittelyn minimoinnin periaatetta noudattaen, tavoittaa eri-ikäisiä ihmisiä Suomessa. (ks. tarkempi kuvaus kyselyyn vastaajan informointilomakkeesta, Liite 2.) Tutkimusaineiston kerääminen tapahtui Webropol-ohjelmalla tehdyn, pääsääntöisesti strukturoidun eli valmiit vastausvaihtoehdot sisältävän kyselylomakkeen avulla (Liite 3). Kyselylomake sisälsi kysymysten 2–3

ja 5–8 kohdalla valmiit vastausvaihtoehdot (ns. monivalintakysymys), josta vastaajan tuli valita hänen mielestään osuvin vaihtoehto. Kysymysten 1, 4 ja 9 osalta Webropol-kyselylomake sisälsi avoimen tekstikentän muotoisen vastausosion. Vastaaja sai tällöin omin sanoin antaa vastauksensa kysyttyyn kysymykseen. Kyselylomakkeen (Liite 3) avulla saatiin kartoitettua vastauksia keskeisiin tutkimuskysymyksiin kuten, millä sähköisellä tunnistamisvälineellä loppukäyttäjä yksityisen sektorin palveluun tunnistautui tai millainen merkitys palvelun loppukäyttäjälle olisi palvelun sujuvuuden tai toisaalta luotettavuuden ja tietoturvallisuuden tuntu. Kyselylomakkeelle saatiin kolmen eri sähköisen alustan kautta anonyymejä verkkovierailijoiden vastauksia yhteensä 16 kappaletta.

4.3 Menetelmävalinta ja perustelut

Regulaatiopohjan selvityksen jälkeen keräsin niin ikään aineistoa sähköisellä Webropol-kyselylomakkeella. Kyselylomakkeessa oli sekä monivalintakysymyksiä (valmiit vastausvaihtoehdot sisältäviä kysymystyyppejä) että avoin vastaus -tyyppisiä kysymyksiä. Jälkimmäiseen kysymystyyppiin saatuja vastauksia analysoin laadullisin menetelmin. Tämä tarkoittaa sitä, että analysoin saatuja vastauksia jäsentelemällä, tyypittelemällä ja ryhmittelemällä. Aineistoa keräsin pääasiassa kvalitatiivisesti eli laadullisesti. Jossain määrin keräsin aineistoa myös kvantitatiivisesti eli määrällisesti.

Kyselylomakkeella olleet kysymykset koskien sitä, oliko kyselyyn vastaaja hankkinut itselleen teleoperaattorin myöntämän mobiilivarmenteen sähköisen asiointipalveluun tunnistautumisen tunnistautumisvälineeksi tai oliko kyselyyn vastaaja hankkinut itselleen Digi- ja väestötietoviraston myöntämän kansalaisvarmenteen tunnistautumisvälineeksi, edustivat mielestäni määrällisen aineiston keruun puolta. Myös kerätyt vastaukset siihen, että millä tunnistusvälineellä eniten ihmiset ilmoittivat tunnistautuneensa käyttämään julkisen sektorin sähköisen asioinnin palvelua tai yksityisen sektorin sähköisen asioinnin palvelua, edustivat määrällisen aineiston keruun puolta. Keräsin tutkimusaineistoani jossakin määrin sekä laadullisin että määrällisin menetelmin. Tällöin voi pienimuotoisesti puhua jopa opinnäytetyössäni esiintyvästä monimenetelmällisyydestä tai kvantitatiivisen ja kvalitatiivisen tutkimusmenetelmän tosiaan täydentävästä tutkimustavasta (Hirsjärvi, Remes & Sajavaara 2009, 135–137). Tutki ja kirjoita -menetelmäoppaan kirjoittajien mukaan kvalitatiivinen ja kvantitatiivinen tutkimus ovat lähestymistapoja, joita on käytännössä vaikea tarkkarajaisesti erottaa toisistaan. Kvalitatiivinen ja kvantitatiivinen tutkimus onkin järkevämpää mieltää toisiaan täydentävinä lähestymistapoina aineistoon, ei kilpailevina lähestymistapoina. Toisaalta kvalitatiivista ja kvantitatiivista metodia voi ajatella myös siten, että niitä käytetään rinnakkain tutkimusongelmaan pureuduttaessa. (Hirsjärvi ym. 2009, 134–139.) Laadullisen ja määrällisen menetelmän yhdistäminen tai rinnakkaiskäyttö sopi tutkimusongelmani selvittämiseen hyvin. Koin luontevaksi tavaksi yhdistää pääosin kvalitatiiviseen tutkimukseeni myös joitakin elementtejä kvantitatiiviselta menetelmäpuolelta. (Hirsjärvi ym. 2009, 134–139; Helakorpi 1999.)

4.4 Tutkimustuloksista

Hypoteesina kartoittavassa, selittävässä tutkimustyyppisessä opinnäytetyössäni oli se, että suomalaisten pankkien myöntämät verkkopankkitunnukset olisivat ylivoimaisesti käytetyin vahvan sähköisen tunnistamisen tunnistamisväline. Näin vaikka markkinoilla on helposti saatavilla myös esimerkiksi teleoperaattorien myöntämiä mobiilivarmenteita, jotka yhtä lailla soveltuvat vahvan sähköisen tunnistamisen tunnistamisvälineiksi. Suurimmista Suomessa toimivista teleoperaattoreista esimerkiksi Telia Finland Oyj tarjoaa mobiilivarmenteen asiakkailleen ilmaiseksi (kartoitettu tilanne toukokuussa 2022, ks. https://www.telia.fi/kauppa/palvelut/mobiilivarmenne/artikkeli/mobiilivarmenne-auttaa-lakimuutoksessa-newsroom). Muut Suomessa toimivat suuret teleoperaattorit (DNA Oyj ja Elisa Oyj) tarjoavat asiakkailleen mobiilivarmennetta maksullisena lisäpalveluna – tosin hyvin edulliseen hintaan. Sekä DNA:n että Elisan mobiilivarmennepalvelusta henkilöasiakkailtaan veloittama asiakashinta on 1,99 euroa kuukaudessa (kartoitettu tilanne toukokuussa 2022, ks. https://www.dna.fi/mobiilivarmenne, ks. https://elisa.fi/varmenne/).

Kuten jo aiemmin totesin, Suomessa vahvan sähköisen tunnistamisen välineinä kelpaavat tällä hetkellä suomalaisten teleyritysten tarjoamat mobiilivarmenteet, suomalaisten pankkien myöntämät verkkopankkitunnukset, Digi- ja väestötietoviraston myöntämä sähköinen kansalaisvarmenne (yhdistettynä poliisin myöntämään henkilökorttiin) sekä sirullinen, varmenteen sisältävä organisaatiokortti (Kyberturvallisuuskeskus 2021a; tunnistuslaki; Voutilainen 2020, 48–56).

Hypoteesini verkkopankkitunnusten käytön ylivoimaisuudesta tunnistamisvälineenä perustui omakohtaiseen aiempaan verkkoasiointiini. Oman sähköisen asioinnin kokemukseni perustin esimerkiksi Kelan sähköistä verkkopalvelua opiskelijana käyttäessäni (opiskelijan etuudet), Helsingin kaupungin sähköistä verkkopalvelua perheellisenä opiskelijana käyttäessäni (hakiessani esiopetuspaikkaa tyttärelleni Helsingin kaupungin sähköisessä asiointipalvelussa), OmaVero-palvelua käyttäessäni (veronmaksajan näkökulma), pankkiasioita verkossa hoitaessani (pankkipalveluiden asiakas), vakuutusasioita vakuutusyhtiön kanssa hoitaessani (kotivakuutusasiakas) ja kulttuurialan tapahtumiin lippuja ostettaessa (kuluttajan näkökulma ostaessani elokuvalippuja sähköisesti). Pankkien myöntämien verkkopankkitunnusten olemassaolon ”perään kyselemiseen” törmäsi mielestäni lähes joka paikassa verkossa asioidessa.

Verrattuna Digi- ja väestötietoviraston myöntämän sähköisen kansalaisvarmenteen olemassaoloon, niin tämän tunnistusvälineen ”perään kyselemiseen” ei mielestäni suoranaisesti törmännyt verkossa asioidessaan lainkaan. Joskus vain saattoi huomata, että verkkopalveluntarjoaja ei edes tarjonnut verkkoasiointisivullaan mahdollisuutta tunnistautua palveluun vahvasti julkisen palveluntarjoajan, Digi- ja väestötietoviraston, myöntämää sähköistä varmennetta hyödyntäen. Esimerkiksi

käyttämäni vakuutusyhtiön verkkoasiointisivulla oli mahdollista tunnistautua palveluun vahvasti kahdella eri tavalla: suomalaisten pankkien myöntämin verkkopankkitunnistein tai teleoperaattorien myöntämin mobiilivarmentein. Vakuutusyhtiö ei edes tarjonnut verkkoasiointisivullaan mahdollisuutta tunnistautua palveluun vahvasti Digi- ja väestötietoviraston myöntämää sähköistä varmennetta hyödyntäen.

4.5 Webropol-kyselytutkimuksen tulokset – verkkopankkitunnukset suosituimpana vahvan sähköisen tunnistamisen tunnistamisvälineenä

Webropol-kyselyyni vastaajilla eniten käytössä ollut sähköinen tunnistamisväline oli suomalaisen pankin myöntämä verkkopankkitunnus. Webropol-kyselyyn vastaajista 37 % oli hankkinut itselleen teleoperaattorin myöntämän mobiilivarmenteen (63 % kyselyaineiston henkilöistä oli puolestaan sellaisia, joilla ei ollut käytössään mobiilivarmennetta). Webropol-kyselyyn vastaajista 6 % oli hankkinut itselleen Digi- ja väestötietoviraston myöntämän kansalaisvarmenteen (94 % kyselyaineiston henkilöistä oli puolestaan sellaisia, joilla ei ollut käytössään sirulliseen henkilökorttiin sijoitettavaa kansalaisvarmennetta).

Pohdin sitä, että miksi juuri kaupallisen palveluntarjoajan tarjoama sähköisen tunnistamisen väline (suomalaisen pankin tarjoama verkkopankkitunnus) on saavuttanut niin merkittävän aseman suomalaisilla tunnistusvälinemarkkinoilla. Miksi näin on, vaikka sähköisten asiointipalveluiden loppukäyttäjillä olisi mahdollisuus saada käyttöönsä myös julkisen palveluntarjoajan – Digi- ja väestötietoviraston – sähköinen tunnistautumisväline? Suomessa ihmisillä on yleensä vahva usko julkisen sektorin palveluntarjoajien luotettavuuteen, neutraaliuuteen, tasapuolisuuteen, turvallisuuteen ja siihen, että julkinen toimija olisi esimerkiksi suojannut palvelunsa asianmukaisesti. Voisi jopa olettaa, että neutraali, ei-yrityssidonnainen, julkishallinnon toimijan toteuttama sähköinen kansalaisvarmenne, joka sujuvasti sirulliseen, poliisin myöntämään henkilökorttiin sijoitetaan, olisi se tunnistamisväline, jonka suurin osa suomalaisista olisi omaksi ensisijaiseksi sähköiseksi tunnistamisvälineeksi itselleen valinnut. Webropol-kyselyyn vastanneiden henkilöiden vastauksia katsomalla voi kuitenkin päätyä täysin vastakkaiseen lopputulokseen. Jos 94 % kyselyaineiston henkilöistä ei ollut käytössään sirullista henkilökorttiin sijoitettavaa kansalaisvarmennetta, voisi varovaisesti jopa hyvin pienimuotoisenkin kyselytutkimukseni perusteella todeta, että Digi- ja väestötietoviraston myöntämä sähköinen tunnistautumisväline oli hyvin heikosti tunnettu ja hyvin heikosti omaan käyttöön hankittu sähköinen tunnistautumisväline Suomessa.

Toisaalta, voisi myös olettaa, että ”näinä älypuhelimien, älypuhelinsovellusten ja liikkuvan, mobiiliasioinnin aikoina” juuri teleoperaattorin myöntämä mobiilivarmenne, joka kätevästi kulkee siellä mukana, missä älypuhelinkin kulkee ihmisen mukana, olisi hyvin voimakkaaseen suosioon noussut sähköinen tunnistamisväline. Näin ei ole Tuorilan vuonna 2017 julkaiseman tutkimuksensa mukaan

(Tuorila 2017, 106–107). Oman vuonna 2022 toteutetun pienimuotoisen kyselytutkimukseni, suuntaa-antavien vastausten perusteella, on johtopäätös sama.

Webropol-kyselyyni vastanneista henkilöistä 88 % ilmoitti kirjautuneensa edellä mainittuihin julkishallinnon sähköisiin asiointipalveluihin suomalaisen pankin myöntämällä verkkopankkitunnuksella. 13 % vastaajista ilmoitti kirjautuneensa teleoperaattorin mobiilivarmenteella käyttämiinsä julkishallinnon e-palveluihin (monivalintakysymyksissä oli mahdollista rastittaa useampi vaihtoehto vastaukseksi, ks. Liite 3). 6 % vastaajista ilmoitti kirjautuneensa Digi- ja väestötietoviraston kansalaisvarmenteella käyttämiinsä julkishallinnon e-palveluihin (monivalintakysymyksissä oli mahdollista rastittaa useampi vaihtoehto vastaukseksi, ks. Liite 3). Ylipäätään Webropol-kyselyyn vastaajista 37 % oli hankkinut itselleen teleoperaattorin myöntämän mobiilivarmenteen (67 % kyselyaineiston henkilöistä oli puolestaan sellaisia, joilla ei ollut käytössään mobiilivarmennetta).

Teleoperaattorin myöntämä mobiilivarmenne tuli vahvana kakkosena julkisen sektorin sähköisiin palveluihin tunnistautumisen välineenä (pankkien verkkotunnusten ykkössijan jälkeen). Sama tilanne oli yksityisen sektorin verkkoasiointipalveluihin tunnistauduttaessa – erityisesti tilanne korostui yksityisiä pankki-, vakuutus- ja terveydenhoitopalveluissa asioitaessa. Webropol-kyselyn tulosten perusteella arvioituna teleoperaattorin myöntämä mobiilivarmenne tuli vahvana kakkosena yksityisen sektorin sähköisiin palveluihin tunnistautumisen tunnistusvälineenä.

4.6 Webropol-kyselytutkimuksen tulokset suhteessa lainsäädännön vaatimuksiin

Webropol-kyselyyni vastanneiden henkilöiden mukaan julkishallinnonpalveluista eniten käytetyiksi nimettiin sosiaali- ja terveysviranomaisten terveys- ja rokotustietojen sekä sähköisten reseptien Omakanta-palvelu, verohallinnon OmaVero -palvelu sekä Kansaneläkelaitoksen, KELA:n e-asiointipalvelu. Webropol-kyselyyn vastanneista 16 vastaajasta nimesi yksityisen sektorin palveluista eniten käytetyiksi pankkien ja vakuutusyhtiöiden tarjoamat verkkopalvelut sekä suomalaisten teleoperaattorien tarjoamat sähköiset asiointipalvelut koskien puhelinliittymiä ja Internet-liittymiä sekä ns. suoratoistopalvelua. Seuraavaksi eniten Webropol-kyselyyn vastanneet nimesivät käyttäneensä yksityisen sektorin palveluista joko elokuvalippupalvelun tai jonkin tapahtuman, konsertin tai muun musiikki- tai tapahtuma-alan lipunvarauspalvelua. Myös matkustamiseen liittyviä yksityisen sektorin sähköisen asioinnin palveluita (kuten hotellimajoituksen varauspalvelua, juna-, bussi- ja/tai lentolipun varauspalvelua) ilmoitettiin käytetyn viime aikoina. Webropol-kyselyyni vastanneista henkilöstä 63 % ilmoitti kirjautuneensa yksityisen sektorin sähköisiin asiointipalveluihin suomalaisen pankin myöntämällä verkkopankkitunnuksella. Toisaalta mainittava on myös se, että 75 % vastaajista ilmoitti tunnistautuneensa yksityissektorin palveluun pelkällä käyttäjätunnus ja salasana -yhdistelmällä (monivalintakysymyksissä oli mahdollista rastittaa useampi vaihtoehto vastaukseksi, ks. Liite

3). 6 % vastaajista ilmoitti kirjautuneensa teleoperaattorin mobiilivarmenteella yksityisen sektorin e-asiointipalveluun.

Juurikin pankin myöntämillä verkkopankkitunnuksilla tapahtuva vahva sähköinen tunnistaminen toteutettiin lähes kaikkiin aiemmin mainittuihin julkishallinnon eniten vastaajien käyttämiin e-palveluihin (sosiaali- ja terveysviranomaisten ylläpitämä OmaKanta-palvelu, veroviranomaisen ylläpitämä OmaVero-palvelu sekä KELA:n sähköisen asioinnin palvelut). Digipalvelulain velvoitteiden sekä tunnistuslain velvoitteiden valossa tulkittuna tämä on luonteva lopputulos, koska esimerkiksi digipalvelulain 6 §:n mukaan viranomaisen on vaadittava palvelun loppukäyttäjältä vahvaa sähköistä tunnistautumista, jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi (digipalvelulaki 6 §; ks. myös tämän opinnäytetyön kappale 2.2.4). Sosiaali- ja terveysviranomaisten ylläpitämästä OmaKanta-palvelusta, jonne esimerkiksi rokotustiedot, lääkereseptitiedot ja diagnosoidut sairaudet kirjataan, veroviranomaisen ylläpitämästä OmaVero-palvelusta sekä KELA:n sähköisen asioinnin palvelusta, on kaikista mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi. Tällöin palvelun loppukäyttäjä on digipalvelulain vaatimusten mukaan tunnistettava vahvasti.

Pankin myöntämillä verkkopankkitunnuksilla tapahtuva vahva sähköinen tunnistaminen mahdollistettiin myös melkein kaikkiin aiemmin mainittuihin yksityisen sektorin verkkopalveluiden käyttämiseen. Yksityisen sektorinkin toimijan sähköisestä palvelusta voi olla mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi. Digipalvelulain soveltamisalapykälässä (3 §) todetaan, että lakia sovelletaan julkishallinnon toimijoiden lisäksi myös yrityksen, säätiön, yhdistyksen ja muun yhteisön digitaalisiin palveluihin, joiden kehittämisen tai käytön rahoittamiseen osallistuu digipalvelulaissa tarkoitettu viranomainen vähintään puolella kehittämiskustannuksista tai vuotuisista ylläpitokustannuksista (digipalvelulaki 3 §). Lisäksi digipalvelulakia sovelletaan tunnistuspalvelun tarjoajien tunnistuspalveluihin, verkkomaksamisen kokoamis- ja hallinnointipalvelun kautta käytettäviin digitaalisten palvelujen osiin, joilla voidaan hoitaa maksutoimeksiantoja, vesi- ja energiahuollon, liikenteen ja postipalvelujen alalla toimivien organisaatioiden digitaalisiin palveluihin siltä osin kuin niiden tarkoituksena on tarjota vesi- ja energiahuollon, liikenteen ja postipalvelujen alan palvelua yleisölle, luottolaitoksiin, maksulaitoksiin, sijoituspalveluyrityksiin, vakuutusyhtiöihin ja vakuutusyhdistyksiin, siltä osin kuin niiden tarkoituksena on tarjota palvelua yleisölle. (digipalvelulaki 3 §.)

Näin ollen esimerkiksi pankkien, vakuutusyhtiöiden ja sijoituspalveluyritysten on tunnistettava sähköisen palvelunsa loppukäyttäjä vahvasti, jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi. Lähtökohtaisesti pankkien, vakuutusyhtiöiden ja sijoituspalveluyritysten asiakkailleen verkkoon hoidettavaksi mahdollistamat asiat, hakemusten lähettämiset asiakirjaliitteineen ja e-asioinnin kautta käsiteltävät tietosisällöt, eivät ole

julkisia tietosisältöjä. Lähtökohtaisesti edellä mainitut yksityiset palveluntarjoajat saattavat asiakkaidensa saataville sellaista sähköistä palvelua, josta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi. Näin ollen yksityisistä palveluntarjoajista esimerkiksi juuri pankit, vakuutusyhtiöt sekä sijoituspalveluita tarjoavat yritykset, mutta myös laissa luetteloidut vesilaitokset ja sähkölaitokset ovat velvoitettuja kehittämään sähköiset palvelunsa siten, että niissä toteutetaan tarpeen vaatiessa loppukäyttäjän vahva sähköinen tunnistaminen digipalvelulain vaatimukset täyttävällä tavalla.

Toisaalta pitää muistaa huomioida yksityisen sektorin sähköisten palveluiden toteuttamista ja verkkokaupankäyntiä sääntelevä EU:n PSD 2 -direktiivi sekä kansallinen maksupalvelulaki. Kyseiset säädökset velvoittavat erityisesti yksityissektorilla ja verkkokaupan-käynnissä toimivia maksupalvelun tarjoajia tunnistamaan asiakkaansa ja käyttämään vahvaa sähköistä tunnistamista tietynlaisessa, esim. luottopalvelujen, maksupalvelujen ja pankkien maksupalvelutoiminnassa. Maksupalvelulain 85 c §:n mukaan palveluntarjoajan on käytettävä vahvaa tunnistamista, jos maksaja:

1) käyttää maksutiliään tietoverkon välityksellä;

2) käynnistää sähköisen maksutapahtuman;

3) toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski.

Myös jos maksaja käynnistää sähköisen maksutapahtuman etäviestimellä (kuten puhelimella), palveluntarjoajan on käytettävä vahvaa tunnistamista palvelua käyttävään loppukäyttäjään. (maksupalvelulaki 85 c §.) Maksupalvelulain 8 §:n määritelmien mukaan etäviestimellä tarkoitetaan puhelinta, postia, televisiota, tietoverkkoa tai muuta välinettä, jota voidaan käyttää sopimuksen tekemiseen ilman että osapuolet ovat yhtä aikaa läsnä (maksupalvelulaki 8 §).

Webropol-kyselyyn vastaajien mukaan heidän eniten käyttämänsä yksityisen sektorin digitaaliset palvelut olivat pankkipalveluja, teleoperaattorien asiointipalveluja esimerkiksi Internet- tai puhelinliittymäasioiden hoitoon, elokuvalippujen ostopalveluja ja vakuutusyhtiöpalveluja. Myös erilaiset verkkokaupat, kuten Zalandon vaateverkkokauppa, IT-alan laitteisiin ja kodinelektroniikkaan erikoistunut Verkkokauppa.com sekä käytetyn tavaran välittämiseen ja myyntiin profiloitunut Tori.fi -sähköisen kaupankäynnin alusta mainittiin esimerkkeinä käytetyistä yksityissektorin palveluista. Kaikki edellä mainitut e-asioinnin palvelut ovat nähdäkseni sellaisia, joiden toteuttamista PSD 2-direktiivi ja maksupalvelulaki ainakin sääntelevät. Näin on, koska kaikissa edellä luetelluissa palveluissa ja niihin liittyvän maksutapahtuman toteuttamisprosessissa maksaja joko käytti maksutiliään tietoverkon välityksellä, maksaja käynnisti sähköisen maksutapahtuman, maksaja toteutti etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski tai maksaja käynnisti sähköisen maksutapahtuman etäviestimellä (kuten puhelimella). Maksupalvelulain mukaan, mikäli näin on,

palveluntarjoajan on käytettävä vahvaa tunnistamista palvelua käyttävään loppukäyttäjään. (maksupalvelulaki 85 c §.)

4.7 Yhteenvetoa Webropol-kyselytutkimuksen tuloksista

Webropol-kyselyyn vastaajani olivat 44 % täysin samaa mieltä sen väitteen kanssa, että asioiden hoitaminen julkisen sektorin sähköisissä asiointipalveluissa toimi sujuvasti. Webropol-kyselyyn vastaajat olivat puolestaan 56 % jokseenkin samaa mieltä sen väitteen kanssa, että asioiden hoitaminen julkisen sektorin sähköisissä asiointipalveluissa toimi sujuvasti. Yhteenvetona todettakoon, että kaikki kyselytutkimusaineistoni vastaajat (olkoonkin, että heitä oli vain 16 henkilöä), olivat kovin tyytyväisiä asioiden sähköiseen hoitamiseen julkisen sektorin sähköisissä asiointipalveluissa. Sinänsä, mikäli olisi mahdollista laajentaa tuloksen tulkintaa alueelliselle tai jopa valtakunnalliselle tasolle, voisi todeta julkisen sektorin onnistuneen erinomaisesti digitaalisen palveluidensa toteuttamisessa.

Merkittävää eroa ei ollut havaittavissa Webropol-kyselyyn vastaajien keskuudessa siinä, että miten he kokivat julkisen sektorin ja yksityisen sektorin sähköisten asiointipalveluiden toimivan. Webropol-kyselyyn vastaajat olivat 19 % täysin samaa mieltä sen väitteen kanssa, että asioiden hoitaminen yksityisen sektorin sähköisissä asiointipalveluissa toimi sujuvasti. Webropol-kyselyyn vastaajat olivat puolestaan 69 % jokseenkin samaa mieltä sen väitteen kanssa, että asioiden hoitaminen yksityisen sektorin sähköisissä asiointipalveluissa toimi sujuvasti. Vaikuttaa siltä, että myös yksityissektorin toimijat ovat onnistuneet toteuttamaan digitaaliset palvelunsa loppukäyttäjien käyttäjäkokemuksen perusteella arvioituna varsin hyvin.

5 Pohdinta

5.1 Sähköisten palveluiden tila ja yhdenvertaisuuden toteutuminen Suomessa

Webropol-kyselyn tuloksia peilatessani kokonaisvaltaisesti opinnäytetyön tietoperustaan ja aiempaan aihepiiristä tehtyyn tutkimukseen, vahvistaa myös itse keräämäni aineisto käsitystä siitä, että sähköisten tunnistamisvälineiden tasapuolisella saatavuudella on merkittävä vaikutus hyvinvointiyhteiskunnan toimivuuteen ja yhdenvertaisuuden toteutumiseen. Virtanen ym. (2022) ovat todenneet, että suomalaisessa yhteiskunnassa elää tällä merkittävä joukko ihmisiä, joiden digitaalisten palvelun käytön taito on puutteellinen tai jotka ovat digitaalisten palveluiden käytön ulkopuolella jonkin muun syyn vuoksi – esimerkiksi sen vuoksi, että heiltä puuttuu vahvan sähköisen tunnistamisen tunnistamisväline. Edellä mainitut tutkijat ovat vuoden 2022 alkupuoliskolla julkaistussa Terveyden ja hyvinvoinnin laitoksen julkaisussa *”Päätösten tueksi 1/2022, Hyvinvointiyhteiskunnan digitaaliset palvelut yhdenvertaisiksi”* todenneet, että suuri osa haavoittuvassa asemassa olevista yhteiskunnan asukkaista (ikääntyneistä, mielenterveyskuntoutujista, maahanmuuttajista yms.) osaa kyllä operoida sujuvasti Internetissä ja erilaisilla sosiaalisen median kanavilla, mutta ei kuitenkaan kykene asioimaan hyvinvointiyhteiskunnan digitaalisissa palveluissa. (Virtanen ym. 2022, 1–2.)

Edellä viitattujen tutkijoiden mukaan havainto johtuu siitä, että sähköisen palvelualustan käyttö edellyttää yleisen ICT-osaamisen lisäksi muitakin taitoja, kuten ymmärrystä suomalaisesta pitkälle kehittyneestä julkissektorin ja yksityissektorin järjestelmästä ja virkakielestä. Osaamisvajetta on kaiken ikäisillä ja nimenomaisesti vähän koulutetuilla sekä niillä ulkomaalaistaustaisilla, jotka tutustuvat vielä suomen kieleen. Usean asiointia hankaloittaa heikentynyt oppimiseen liittyvä toimintakyky, jolloin sähköisten palveluiden visaisia tekstisisältöjä ja toiminnallisuuksia on haastavaa sisäistää. Moni ei omaa tarvittavia päätelaitteita, ja esimerkiksi pelkällä mobiililaitteella palveluiden käyttö voi tuntua hankalalta. On myös yhä joitakin palveluita, joita ei voi käyttää mobiililaitteella, vaan e-palvelun käyttö vaatii joko kannettavaa tietokonetta tai niin sanottua pöytäkonetta. Suomalaisessa yhteiskunnassa elää merkittävä joukko ihmisiä, joiden tuki digitaalisten hyvinvointiyhteiskunnan palveluiden käyttöön saattaa myös olla omien lasten, lastenlasten, muiden omaisten tai kolmannen sektorin järjestöjen varassa. (Virtanen ym. 2022, 1–2; Tuorila 2016, 13–18; 2017, 106–107; Heponiemi 2021.) Oman aineistoni vastaajien avoimista vastauksista heijastui samansuuntainen viesti, että digitaalisten palveluiden käyttö edellyttää digiosaamisen lisäksi muitakin taitoja – ymmärrystä esimerkiksi tietoturvasta, ja että kaikilla vastaajilla ei tieto-taitotaso tässä suhteessa ole välttämättä kovin hyvällä tasolla. Koettiin myös, että pitäisi ehtiä parantamaan omia e-palvelujen käyttötaitoja, ja toisaalta jotkut kokivat rasitteena sen, että ylipäätään moisia asioita vielä ikäihmisenkin pitäisi ryhtyä opettelemaan.

Huoli henkilökohtaisten tietojen tietoturvasta on kasvanut digitaalisuuden myötä. Esimerkiksi mielenterveyttä ja sosiaalista osallisuutta edistävissä palveluissa hyödynnetään nykyään yllättävän paljon ns. chat-palveluita, joita kaikki ihmiset eivät koe tietoturvallisiksi. Myös rahansiirtoihin liittyvien palveluiden hoitaminen pelkästään verkossa (verkkokauppa-alustat, pankkipalvelut verkossa, vakuutusyhtiöpalvelut verkossa yms.) arveluttavat perinteiseen, kasvokkain tapahtuneeseen asiointiin tottuneita ihmisiä – erityisesti ikääntynyttä väestöä. Oman aineistoni vastaajat mainitsivat avointen tekstikenttien vastausosioissa heidän asiointikokemukseensa oleellisesti vaikuttavina seikkoina juurikin sen, että kuinka tietoturvallisena ja luotettavana he kunkin verkkopalvelun ja sen takana toimivan tahon arvioivat, ja toisaalta, kuinka sujuvasti he tarpeen vaatiessa voivat muuttaa asiointitapansa tietyn, asiointitapahtuman osalta perinteiseksi kasvokkain tapahtuvaa asiointimuotoon. Näin, mikäli esimerkiksi verkkokaupan käyttäminen rahansiirtoihin liittyvien palveluiden osalta tai esimerkiksi chat-palvelutyyppinen terveysasioiden hoitaminen verkossa koetiin ei-riittävän-luotettavalla tavalla tai ei-riittävän-turvallisella tavalla toteutetuksi loppukäyttäjän näkökulmasta. Hiljattain vuoden 2020 lokakuussa tietomurron kohteeksi joutunut psykoterapiakeskus Vastaamon sähköinen palvelu, ja sen seurauksena aiheutunut laajamittainen, kymmeniä tuhansia ihmisiä koskenut tietosuoja- ja tietoturvapoikkeamatapaus, oli ja yhä on entisestään omiaan lisäämään kaiken ikäisten ihmisten arvostusta riittävän tietoturvallisia ja luotettavia sähköisiä palveluita kohtaan. Toisaalta psykoterapiakeskus Vastaamon ikävä tapaus osoitti myös sen, että joitakin asiointipalveluita – erityisesti terveyden- ja sosiaalihuollon palveluita yhä halutaan mieluummin hoitaa kasvokkaisessa, perinteissä asiointimuodossa kuin pelkän ICT-teknologian avulla.

Kolmantena seikkana nostan esiin sen, että ei kaikilla myöskään ole mahdollisuutta käyttää digitaalista palvelua omassa rauhassa. Tämä vaikuttaa tietosuojan toteutumiseen palvelun käytön yhteydessä. Terveydenhuollon digitaalisia ja etäpalveluja toteutettaessa Valvira (Sosiaali- ja terveysalan lupa- ja valvontavirasto) on esimerkiksi todennut ja julkisilla verkkosivuillaan (www.valvira.fi) asian ohjeistanut siten, että terveydenhuollon ammattilaisen tulee suorittaa yksilöllinen arviointi per potilas siitä, että onko potilaalla riittävät mahdollisuudet käyttää digitaalista terveydenhuollon etäpalvelua (esimerkiksi huomioon ottaen hänellä olevat ICT-laitteet, hänen mahdollisuus käyttää esim. digitaalista lääkärin etävastaanottovideopalvelua rauhassa, huomioon ottaen potilaan ICT-taitojen taso. (Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016.) Nimenomaan koronaepidemian aikana sai ihan Helsingin Sanomista, Ilta-Sanomista ja muista yleisimmistä Suomessa säännöllisesti ilmestyvistä sanoma- ja aikakausilehdistä lukea siitä, että miten erityisesti ikääntyneempi väestö oli päästä pyörällään siitä, minkälaisia terveydenhuollon ja kotisairaanhoidon etä- ja digipalveluita heille tarjottiinkaan ja minkälaisia taitoja siirtyä sähköisten palveluiden käyttäjiksi heiltä yhtäkkisesti vaadittiin, kun pyrittiin välttämään lähikontakteja eri ihmisten kesken. Vaikka

terveydenhuollossa ja jopa kotisairaanhoidossa on tapahtunut merkittävää digitalisaatiokehitystä viime vuosina (esim. sensorirannekkein tapahtuva terveysdatan mittaaminen potilaalta), ja kyvykkyyttä siirtää palveluja digitaalisesti toteutettaviksi, ei kuitenkaan kaikkia terveys- ja sosiaalipalveluja voi tarjota etänä tai ICT-teknologian välityksellä jatkossakaan. Monelle ikääntyneelle tai vaikka vaikeasti vammautuneelle henkilölle muutaman kerran viikossa tapahtuva kotisairaanhoidon käynti omaan kotiin kasvokkain toteutettuna saattaa olla ainoa mahdollisuus toisen ihmisen kanssa keskusteluun. Kasvokkain tapahtuvaa vuorovaikutusta ja tavanomaisen keskustelumahdollisuuden tarjoamista pitää arvostaa jatkossakin.

Valvira on määrittänyt etäpalvelut palveluiksi, “joissa potilaan tutkiminen, diagnostiikka, tarkkailu, seuranta, hoitaminen, hoitoon liittyvät päätökset tai suositukset perustuvat esimerkiksi videon välityksellä verkossa tai älypuhelimella välitettyihin tietoihin ja dokumentteihin” (Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016). Etäpalvelussa hyödynnetään jotakin ICT-teknologiaa, kuten potilaan matkapuhelinta, tietokonetta, sensorilaitetta, älykelloa, älyranneketta, näiden yhdistelmiä tai näihin teknologioihin rakennettuja sovelluksia tavoitteelliseen asiakkaan ja ammattilaisen yhteistyöhön. Etäpalvelut rinnastetaan monilta osin perinteisiin vastaanottokäynteihin. Valviran mukaan teknologian kehittyessä terveydenhuollon palveluita voidaan tuottaa uusilla tavoilla. Huomioitavaa kuitenkin Valviran mukaan tässä on se, että terveydenhuollon ammattilaisen tulisi pohtia aina kunkin asiakkaan kohdalla juuri kyseisen asiakkaan soveltuvuutta käyttämään etäpalveluja. Tätä yksilöllistä pohdintatilannetta helpottamaan Valvira on julkaissut terveydenhuollon ammattilaisille digitaalisten ja etäterveydenhuoltopalvelujen antamista koskevat ohjeet ”Potilaille annettavat terveydenhuollon etäpalvelut”. (Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016.) Terveydenhuollon ammattihenkilön tulee arvioida yksilöllisesti, soveltuuko potilas hoidettavaksi etäyhteyden välityksellä. Potilaan tunnistaminen etäyhteydellä tapahtuvaan terveydenhoidon palveluun on perustuttava luotettavaan menetelmään, jollaisena pidetään muun muassa sitä vahvan tunnistamisen prosessia, josta säädetään tunnistuslaissa (Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016). Voimassa oleva lainsäädäntö ei kuitenkaan vielä huomioi etäpalveluja kattavasti. Nähdäkseni tarpeen olisi antaa yksityiskohtaiset säännöt koskien ainakin etäterveys- ja sosiaalipalvelujen tarjoamiselle asetettavia tietoturva- ja tietosuojavaatimuksia sekä määritellä ne etäterveys- ja etäsosiaalipalvelujen tarjoamisen tilanteet, joissa vaaditaan vahvaa sähköistä tunnistamista. Yksittäisellä terveydenhoidon ja sosiaalihuollon ammattilaisella on toistaiseksi ja tulevaisuudessa vaativa vastuu arvioida, millaisiin terveydenhoidon tai sosiaalihuollon tilanteisiin ja minkä tyyppiselle asiakkaalle digitaalisuus parhaiten soveltuu. Vai soveltuuko lainkaan. (Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016.)

Neljänneksi, kaikki ihmiset eivät arvosta digitaalisia palveluja tai eivät oikein koe niiden tuovan mitään lisäarvoa itselleen. Osa ihmisistä koki (aineistoni avointen vastausten analysoinnin perusteella esitettynä) digitaalisuuden jopa ikävänä ja itseään rasittavana asiana. Erityisesti ikääntynyt väestö haikaili perinteisten, vuorovaikutuksellisten asiointitilanteiden perään (vanhojen hyvien aikojen perään, kuten eräs avoimeen vastausosioon kirjoittanut Webropol-kyselyyni vastaaja asian ilmaisi toteamuksellaan: ”Verovirastoonkin sai mennä ihan paikan päälle asioimaan virkailijan kanssa”). Nykyinen digitaalisen palveluiden runsas toteuttamistapa edellyttää asiakkaalta itseltään suurta omaa kiinnostusta ja kykeneväisyyttä opetella digitaalisten palveluiden käyttö tunnistautumisprosesseineen ja esimerkiksi verkkopankissa tapahtuvine kaksinkertaisine maksuvahvistuksineen. Monien ikäihmisten elämäntilanne on vaikea, muisti reistailee, terveys muutoin huono, tai suomen kielen taito tai digitaidot niin heikkoja, ettei vaadittua itsenäistä digitaalisten palveluiden käytön opettelumahdollisuutta ole. Nämä digitaalisissa palveluissa koetut haasteet voivat pudottaa asiakkaita pois palveluista kokonaan (vaikka tarve saada terveys- tai mielenterveyspalvelua yhä olisi olemassa). Sähköisessä asioinnissa kohdatut ongelmat ja koko e-asioinnin pelkäksi rasitteeksi kokeminen voivat entisestään voimistaa digitaalista ja sosiaalista syrjäytymistä Suomessa.

Siksi tuonkin tässä yhteydessä kehittämisehdotuksena IT-alalla työskenteleville palveluiden toteuttajille ja toisaalta myös eri alojen ”palvelu-päätöksentekijöille” ja palvelumuotoilijoille sen, että vaikka kuinka kehitettäisiin hienoja ja sujuvasti käytettäviä sähköisiä palveluita, erityisesti välttämättömyyspalveluiden toteuttamisen osalta on tärkeää säilyttää rinnalla perinteiset, paikan päällä organisaatiossa saatavilla olevat palvelut. Sähköisten palveluiden kustannuksella ei siis saa unohtaa perinteisten palvelumuotojen tärkeyttä monelle asiakkaalle ja väestöryhmän edustajalle. Toisaalta digitaalisen syrjäytymisen uhkassa oleville henkilöille tulisi tarjota entistä enemmän matalan kynnyksen digiklinikoita, ikäihmisten digiklinikoita, maahanmuuttajille suunnattuja, eri kielillä toteutettuja digiklinikoita ja muita digitaalisten palveluita käytön opettelun tilaisuuksia. Näin, koska mikään ei viittaa siihen, että digitaalisuus olisi vähenemässä palvelujen toteutuksessa tulevaisuudessa.

5.2 Kyselytutkimusaineiston luotettavuudesta ja eettisyydestä

Tutkimustyyppisen opinnäytetyön johtopäätös- ja pohdintaosiossa keskeinen sisältö on luotettavuus- ja eettisyyspohdinta. Luotettavuuteen ja otannan kattavuuteen minun tutkimuksessani vaikutti se, että julkaisin Webropol-kyselylomakkeeni linkin kolmella eri sähköisen areenan ilmoitustaululla siten, että pyrin aidosti houkuttelemaan vapaaehtoisia ihmisiä vastaamaan sähköisten palveluiden käyttöä ja loppukäyttäjän vahvaa tunnistamista koskevaan kyselyyn. Mielestäni sellainen sähköisten Webropol-kyselyiden toteutustapa, jossa etukäteen etsitään tietoon esimerkiksi jonkin organisaation kaikkien opiskelijoiden tai organisaation kaikkien työntekijöiden sähköpostiosoitteet, ja sitten lähetetään heille ns. massajakelusähköposti, jossa pyydetään anonyymisti vapaaehtoisia

organisaation opiskelijoita tai työntekijöitä vastaamaan sähköiseen Webropol-kyselyyn, ei ole eettisesti kestävä sähköisten kyselyn toteutustapa (sähköpostiosoite monesti paljastaa kyselyyn vastaajan henkilöllisyyden, tällöin myöskään anonyymisyyslupaus ei toteudu). Toteutustapa ei nähdäkseni ole EU:n yleisen tietosuoja-asetuksen henkilötietojen käsittelyn minimoinnin periaatetta kunnioittava sähköisen kyselyn toteuttamistapa. Sähköpostiosoite on henkilötieto (Tietosuojavaltuutetun toimisto s.a. a). Organisaation kaikkien opiskelijoiden tai kaikkien työntekijöiden sähköpostiosoitteiden käyttäminen osana opinnäytetyöhön liittyvän sähköisen kyselyn levittämistä, on henkilötietojen käsittelyä. Henkilötietojen käsittelylle tulee aina olla laillinen perusta (Tietosuojavaltuutetun toimisto s.a. b.) Sillä ei ole väliä, kuinka kauan tai kuinka pitkään henkilötietoja käsitellään. Jo henkilötietojen muutaman sekunnin mittainen katselu on henkilötietojen käsittelyä (Tietosuojavaltuutetun toimisto s.a. a; Tietosuojavaltuutetun toimisto s.a. b; Tietosuojavaltuutetun toimisto s.a. c.)

5.3 Kyselytutkimuksen toteutustavan tietosuojaperiaatteista

Nähdäkseni opinnäytetyöhön liittyvän sähköisen kyselyn tapauksessa ainoa minulle soveltuva, henkilötietojen käsittelyn oikeusperuste olisi ollut rekisteröidyltä (sähköpostiosoitteen haltijalta) saatu suostumus (Tietosuojavaltuutetun toimisto s.a. b). Mielestäni minun olisi ollut lähes mahdotonta ja äärimmäisen työlästä ryhtyä pyytämään opinnäytetyöhöni liittyvää sähköisen kyselyn levittämistä sähköpostitse varten ensin suostumusta kaikilta esim. Haaga-Helia ammattikorkeakoulun opiskelijoilta siihen, että saisin käyttää hyödykseni heidän oppilaitoksensa tarjoamaa sähköpostiosoitetta. Halusin toteuttaa aidosti anonyymin sähköisen kyselyn, jossa en edes Webropol-kyselylinkin levittämisen vaiheessa joutuisi keräämään itselleni organisaation kymmenien ihmisten sähköpostiosoitteita tietooni. Siksi päädyin julkaisemaan kyselyni täysin anonyymisti kolmella eri sähköisellä ilmoitustaululla siten, että en joutuisi hyödyntämään kenenkään sähköpostiosoitetta osana sähköisen kyselyn tiedottamisvaihetta. Valitsemani eri sähköiset alustat ja niiden ilmoitustaulut (dashboard) olivat: Haaga-Helia ammattikorkeakoulun opiskelijakunta Helgan käyttämän Discord-kanavan sähköinen ilmoitustaulu, LinkedIn-portaalin sähköinen ilmoitustaulu sekä ET-lehden sähköisen keskusteluareenan ilmoitustaulu.

Tarkoituksenani edellä mainitulla tavalla julkaistussa Webropol-kyselyssä oli tavoittaa eri-ikäisiä verkkopalvelujen käyttäjiä eri sähköisiltä kanavilta, jotta otanta edustaisi jokseenkin tasapuolisesti eri-ikäisiä sähköisten julkishallinnonpalveluiden ja yksityisen sektorin sähköisten asiointipalveluiden käyttäjiä Suomessa. Eri-ikäisten ja eri sähköisiä areenoita käyttävien palveluiden loppukäyttäjien tavoittaminen lisäisi kattavampaa ja luotettavampaa kuvaa sähköisten palveluiden käytöstä ja loppukäyttäjän vahvasta tunnistamisesta palvelun käytön yhteydessä. Haaste, joka liittyy edellä kuvattuun vastausten anonyymiin keruutapaan, on se, että sähköisillä alustoilla vapaasti levitettävien (”lumipallo-otanta” -tyyppisten) vastauslomakelinkkien takia palautusprosenttia ei voi määrittää,

koska kehikkoperusjoukkoa ei ole. Usein vastausmäärä saattaa myös jäädä toivottua vähäisemmäksi. Näin kävi valitettavasti myös minun sähköisen Webropol-kyselyni osalta.

Ajalla 24.3.2022 – 8.4.2022 avoinna ollut Webropol-kyselytutkimukseni saavutti niin ikään vain 16 kyselyyn vastaajan täyden vastauksen. Näin kävi, vaikka yritinkin tiedottaa ja viestittää parhaan kykyni mukaan Webropol-kyselyni olemassaolosta ja siitä, että mitään vastaajien henkilötietoja ei kerättäisi tai käsiteltäisi kyselyyn vastaamisen lomassa (ei edes sähköpostiosoitteitaan käsiteltäisi kyselyn toteuttamisen yhteydessä).

Olisin toivonut suurempaa kyselyyn vastaajien määrää. Lopputuloksen selvittyä huhtikuussa 2022, tuli minun vain huomioida kyselytutkimukseeni osallistujien kohtalaisen pieni määrä siinä, että aineiston pienuuden vuoksi sen perusteella ei tullut tehdä liian pitkälle meneviä johtopäätöksiä tai yleistyksiä. Kyselytutkimukseeni saatuihin vastauksiin suhtauduin siksi enemmän suuntaa-antavana aineistona vastaajien pienen osallistujamäärän vuoksi. Pelkästään itse keräämäni aineiston perusteella en edellä mainitusta syystä johtuen ole tehnyt laajempaa tulkintaa tutkimusongelmani kannalta keskeisistä asioista. Olenkin hyödyntänyt oman aineiston ohella ammattitutkijoiden aihepiiristä tekemää aiempaa tutkimusta johtopäätöksiä opinnäytetyöni asianmukaiseen kappaleeseen kirjoittaessani.

5.4 Yhteenvetoa ja jatkoselvityksille avautuvia tutkimuskysymyksiä

Suomalaisen pankin myöntämät verkkopankkitunnukset – ja jossakin määrin myös mobiilivarmenne – avaavat oven erityisesti julkisen sektorin, mutta hyvin pitkälti myös yksityisen sektorin mahdollistamien sähköisten palveluiden käytölle. Jopa elokuvalippujen ostamiseen saattaa tarvita loppuviimeinen pankin verkkopankkitunnukset ja/tai teleoperaattorin myöntämän mobiilivarmenteen, jotta lippujen ostotapahtuman sai suoritettua asianmukaisesti loppuun. Tämä kävi ilmi tutkimuksessani.

Voisi olla melkein opinnäytetyön veroinen jatkotutkimusaihe selvittää sitä, miten laaja yhä on sen henkilötunnustuksettomien suomalaisten verkkopalveluiden potentiaalisen käyttäjäkunnan osuus, joka putoaa suomalaisten julkishallinnon ja yksityisen sektorien tarjoamien sähköisten palveluiden ulkopuolelle, koska heillä ei ole mahdollisuutta saada suomalaisen pankin myöntämiä verkkopankkitunnuksia ja/tai Suomeen rekisteröityneen mobiilioperaattorin myöntämää mobiilivarmennetta. Myös sitä tulisi samalla selvittää, että kuinka laaja on ilman suomalaista henkilöllisyystodistusta olevien suomalaisten verkkopalveluiden potentiaalisen käyttäjäkunnan osuus. Ja mitä vaikutuksia tilanteella on ihmisten yhdenvertaisuuden toteutumiselle yhteiskunnassamme. Lisämausteen tähän potentiaaliseen jatkotutkimusasetelmaan tuo se, että vahvat sähköiset tunnistamisvälineet ovat Suomessa yksityisen sektorin hallussa. Yksityisen sektorin asiakasvalinta tällä hetkellä nähdäkseni ohjaa sitä, ketkä saavat mahdollisuuden sähköiseen asiointiin maassamme. Tunnistamisvälineiden

myöntäminen perustuu pitkälti Suomessa pankkien omaan asiakasvalintaan. Minulla on ollut onnea, kun oma suomalainen pankkini on kelpuuttanut minut asiakkaakseen – ja on päättänyt myöntää minulle myös vahvan sähköisen tunnistamisen tunnistusvälineen – verkkopankkitunnukset. Tunnistusvälinetarjoajina suurimmat suomalaiset pankit (kuten Osuuspankki, Nordea, Danske Bank, Handelsbanken, Ålandsbanken, S-Pankki, Aktia, POP Pankki ja Säästöpankki) sekä suurimmat suomalaiset teleoperaattorit (kuten Elisa Oyj, Telia Finland Oyj ja DNA Oyj) käyttävät merkittävää valtaa päättäessään siitä, mitkä ei-Euroopan alueen valtiot ja kyseisten valtioiden myöntämät passit ne suostuvat hyväksymään ensitunnistusprosessissa omaan riskiarviointiinsa perustuen sellaisiksi passeiksi, jotka voidaan kelpuuttaa henkilöllisyyden varmentamisprosessissa asianmukaisesti ja henkilöllisyyden riittävän luotettavasti todentaviksi passeiksi.

Onko kansallinen tunnistuslakimme kaikkia suomalaisen julkishallinnon digitaalisia palveluita käyttäviä henkilöitä kohtaan tasapuolinen ja yhdenvertainen, jos lainsäädännössä rajataan ensitunnistamisessa käytettäviksi sallittujen asiakirjojen lista melko suppeaksi rajoittuen pääsääntöisesti vain Euroopan talousalueen jäsenvaltioiden viranomaisten myöntämiin passeihin ja henkilökortteihin? Ensitunnistamisen asianmukainen toteuttaminen on puolestaan olennainen osa prosessia saada sähköinen vahva tunnistamisväline, kuten suomalaisen pankin myöntämät verkkopankkitunnukset, käyttöön.

Suomen kansalaisten lisäksi myös Suomessa asioivien ulkomaalaisten henkilöiden tunnistamisen ja heille verkkoasioinnin mahdollistaminen tulisi olla mahdollista. Tämä asettaa erityisen haasteen, koska globaalia, EU-alueen rajat ylittävää, luotettavaa ja riittävän tietoturvallista, vahvaa sähköisen tunnistamisen tapaa tai välinettä ei oikein ole vielä olemassa. Tilanne voi tulla eteen niin sanotuissa kansainvälisen etätunnistamisen tilanteissa, joissa sähköisen tunnistamisen tason pitäisi lisäksi olla korkea. Näin voi olla esimerkiksi tilanteessa, jossa kiinalainen henkilö hakee työperusteista oleskelulupaa Suomeen ennakkoon ja tällaisen henkilön asioidessa Suomen maahanmuuttoviranomaisen kanssa etukäteen, etänä, verkossa. Edes eIDAS-asetus (ks. kappale 2.2.2) ei helpota tilannetta, koska eIDAS-asetuksella on velvoitettu vain EU-alueen sisäpuoliset toimijat vastavuoroiseen eurooppalaisten vahvojen tunnistamisvälineiden tunnustamiseen. Esim. EU-alueella toimivan italialaisen pankin myöntämä vahva sähköinen tunnistamisväline (italialaisen pankin myöntämä verkkopankkitunniste) tulee eIDAS-asetuksen ja kansallisen tunnistuslakimme velvoittavuuden myötä vastavuoroisesti tunnustaa Suomen viranomaisen toimesta kelvolliseksi vahvan tunnistamisen tunnistamisvälineeksi. Vain EU-jäsenvaltioita velvoittavan eIDAS-asetuksen rajoittuneisuus tulee esille siinä, että se ei velvoita Suomen viranomaista vastavuoroisesti tunnustamaan kiinalaisen pankin myöntämää vahvan tunnistamisen verkkopankkitunnusta tunnistamisvälineeksi. Myös se on haaste, että suomalaista henkilötunnusta, joka oleellisesti liittyy Suomessa henkilön ensitunnistamisketjun toteuttamiseen, ei välttämättä ole kaikilla ei-Suomen kansalaisilla. Äsken

esimerkiksi otetun tapauksen kiinalaisella henkilöllä (tilanne, jossa kiinalainen henkilö hakee työperusteista oleskelulupaa Suomeen maahanmuuttovirastolta etukäteen, etänä, verkossa) ei ole mahdollisuutta myöskään tunnistautua suomalaisessa maahanmuuttoviranomaisessa siten, että hän antaisi Suomen viranomaiselle tietoon henkilötunnuksensa, ja sitä kautta pyrkisi saamaan henkilöllisyytensä tunnistamisprosessin vireille saadakseen työluvan Suomeen.

Suomalaisia julkisen hallinnon sähköisiä asiointipalveluita on enenevässä määrin tarve käyttää ulkomailla asuvilla ulkomaiden kansalaisilla, joita ei ole rekisteröity Suomessa. Työperusteisen oleskeluluvan hakutilanteessa Suomen maahanmuuttovirastolta havaitun vahvan kansainvälisen etätunnistautumisen problematiikan lisäksi sama haaste toistuu opiskeluperusteisen oleskeluluvan hakutilanteessa. Vahvaa kansainvälistä verkossa tapahtuvaa sähköistä etätunnistautumista saatettaisiin myös tarvita tilanteessa, jossa esimerkiksi intialainen IT-alasta kiinnostunut henkilö hakee opiskeluperusteista oleskelulupaa Suomeen ennakkoon, etänä ja verkossa. Valtakunnallisista Suomessa ilmestyvistä sanomalehdistä on ainakin vuodesta 2019 lukien saatu lukea siitä, miten suomalaiset ammattikorkeakoulut yhteistyössä IT-alan tai koulutusalan yritysten kanssa ovat pyrkineet erilaisten AMK-koodari-hankkeiden mahdollistamana tai kansainvälisten opintopolku -hankkeiden mahdollistamana. Ks. esim. https://www.metropolia.fi/fi/opiskelu-metropoliassa/osaamisen-tayden-taminen/amkoodari, sekä ks. esim. Viope Education Oy ja Haaga-Helia Ammattikorkeakoulun tekemä yhteistyö kansainvälisten opintopolkujen toteuttamisessa: https://www.viope.com/palve-lumme, https://www.viope.com/viope-1. Näissä hankkeissa ja toiminnoissa ideana on ollut houkutella aasialaisia, vähäisen IT-alan koulutuksen tai pelkän kiinnostuksen IT-alaa kohtaan omaavia henkilöitä saapumaan Suomeen suorittamaan soveltuva IT-alan AMK-tutkinto, jolla sitten henkilön valmistuttua paikattaisiin Suomessa vallitsevaa koodaripulaa. Suomesta opiskeluperusteista oleskelulupaa ennakkoon hakevan, ei-Suomen kansalaisen tilanne, kun hänen asiaansa hoidetaan suomalaisen korkeakoulun opiskelija- ja hakijapalveluissa ja maahanmuuttovirastossa yhtä aikaa, kohtaa väistämättä jossakin vaiheessa kansainvälisen vahvan sähköisen tunnistautumisen problematiikan (tai lähinnä sen, ettei täysin luotettavaa, vastavuoroisesti eri valtioiden tunnustamaa ja tietoturvallista sellaista oikein ole olemassa).

Suomen kansalaisten lisäksi myös Suomessa asioivilla ulkomaalaisilla henkilöillä tulisi olla tasavertaiset mahdollisuudet käyttää sähköisiä julkisen sektorin ja yksityissektorin sähköisiä palveluita. Niiden Suomessa asuvien tai suomalaisia verkkopalveluita käyttävien henkilöiden asema, joille ei ole syystä tai toisesta myönnetty suomalaista henkilöllisyystodistusta sekä heiden, joille ei ole syystä tai toisesta myönnetty suomalaista henkilötunnusta, asema on hyvin haastava suhteessa sähköisten palveluiden käyttämiseen. Suomalainen henkilöllisyystodistus ja toisaalta suomalainen henkilötunnus ovat avainasemassa siihen, että henkilö voi saada suomalaisen pankin myöntämät

verkkopankkitunnukset ja/tai Suomeen rekisteröityneen mobiilioperaattorin myöntämän mobiilivarmenteen.

Opinnäytetyöni aihepiirin aiempaa tutkimusta esitellessäni (ks. kappale 3 ”Aiemmasta tutkimuksesta”) toin esiin raportin ”Sähköinen tunnistaminen: selvitys nykytilasta sekä – kehittämistarpeista”, joka on julkaistu 8.3.2019 eli reilu 3 vuotta sitten. Siinä raportin kirjoittajat totesivat, että niiden Suomessa asuvien tai suomalaisia verkkopalveluita käyttävien henkilöiden asema, joille ei ole syystä tai toisesta myönnetty suomalaista henkilöllisyystodistusta sekä heiden, joille ei ole syystä tai toisesta myönnetty suomalaista henkilötunnusta, asema on hyvin haastava suhteessa sähköisten palveluiden käyttämiseen. Käytännössä raportin kirjoittajat totesivat jo vuonna 2019, että ko. väestön osa putoaa digitaalisten, vahvaa sähköistä tunnistamista edellyttävien palveluiden käytön ulkopuolelle. Haluan opinnäytetyöni loppuosiossa tuoda esille, että mitä on tapahtunut tämän asian saralla (lähinnä epäkohdan poistamisen eteen tehdyt toimenpiteet) viimeisen kolmen vuoden aikana kesäkuuhun 2022 mennessä. Uusimpana positiivisena asiana todettakoon, että Digi- ja väestötietovirasto on toteuttanut henkilötunnuksettomille ulkomaan kansalaisille ns. Finnish Authenticator -tunnistuspalvelun. Finnish Authenticator -tunnistuspalvelu löytyy Digi- ja väestötietoviraston verkkosivuilta (Digi- ja väestötietovirasto a) sekä Suomi.fi -yhteisverkkopalveluportaalin kautta haettuna verkko-osoitteesta: https://www.suomi.fi/ohjeet-ja-tuki/tietoa-tunnistuksesta/finnish-authenticator-tunnistuspalvelu.

Finnish Authenticator -tunnistuspalvelulla tunnistautuminen on tarkoitettu yritysten ja yhteisöjen ulkomaalaisille edustajille, joilla ei ole suomalaista henkilötunnusta eikä tunnistusvälinettä. Sovellusta voi käyttää asiointipalveluun kirjautumiseen niissä Suomen julkishallinnon asiointipalveluissa, jotka ovat ottaneet käyttöön Finnish Authenticator -tunnistuspalvelun. Ulkomaista yritystä edustavan on haettava myös tarvittavat Suomi.fi-valtuudet virkailijavaltuuttamispalvelun kautta. Finnish Authenticator -tunnistuspalvelussa ulkomaalainen rekisteröi itselleen ulkomaalaisen tunnisteen (UID) ja todentaa henkilöllisyytensä Finnish Authenticator -sovelluksen avulla. Tämän ensitunnistuksen yhteydessä käyttäjä ottaa kuvan itsestään sekä passistaan tai kansallisesta henkilöllisyystodistuksestaan. Tunnistuspalvelu vahvistaa henkilöllisyyden, jos itsestä otettu kuva ja henkilöasiakirjan tiedot vastaavat toisiaan. (Digi- ja väestötietovirasto s.a. a; Digi- ja väestötietovirasto s.a. b.)

Huomioon otettavaa on, että Finnish Auhtenticator -tunnistuspalvelun FinnAuth-tunnusta (UID-tunnusta) ei kuitenkaan voi ulkomaalainen, henkilötunnukseton henkilö käyttää mihinkään omaan, henkilökohtaiseen asiointiin, vaan ainoastaan yritysten ja yhteisöjen puolesta asiointiin (Digi- ja väestötietovirasto s.a. a). Finnish Authenticator -tunnistuspalvelun toteutustapa ei myöskään vastaa eIDAS-asetuksessa, PSD 2 -direktiivissä eikä kansallisessa tunnistuslaissa vahvalle sähköiselle tunnistamiselle asetettuja vaatimuksia. (Digi- ja väestötietovirasto s.a. a; Digi- ja väestötietovirasto s.a. b.) Tällä saralla epäkohtaa ei siis ole onnistuttu vielä poistamaan kokonaan. Yrityksen tai

organisaation puolesta asiointiin ulkomaalaisten, henkilötunnuksettomien ja ei-vahvaa-tunnistusvälinettä-omaavien henkilöiden osalta on tapahtunut kiitettävästi parannusta.

Hyvä jatkotutkimuksen ja jatkokehittämisen aihe IT-alan asiantuntijalle ja miksei myös esimerkiksi palvelumuotoilijalle voisi olla tämä: miten ratkaista globaali, EU-alueen rajat ylittävä, luotettava ja riittävän tietoturvallinen, vahvan sähköisen tunnistamisen tapa tai toteuttaa edellä mainittuun haastavaan tilanteeseen soveltuva vahva sähköinen tunnistamisväline, jonka kaikki maailman eri valtiot vastavuoroisesti tunnustaisivat kelvolliseksi tunnistusvälineeksi eri maailman valtiossa.

Lähteet

Digi- ja väestötietovirasto s.a. a. Digi- ja väestötietoviraston Finnish Authenticator -tunnistuspalvelu. Luettavissa: https://dvv.fi/finnish-authenticator. Luettu 15.6.2022.

Digi- ja väestötietovirasto s.a. b. Digi- ja väestötietoviraston Suomi.fi -yhteisverkkopalveluportaali. Suomi.fi -verkkopalvelu sisältää muun muassa Suomi.fi -tunnistuspalvelun julkisen sektorin vahvan sähköisen tunnistamisen palveluihin. Luettavissa: https://www.suomi.fi/ohjeet-ja-tuki/yleiset-ohjeet. Luettu 15.6.2022.

EUR-Lex-palvelu s.a. Euroopan unionin lainsäädännön EUR-Lex-palvelu. Luettavissa: https://eur-lex.europa.eu/homepage.html?locale=fi. Luettu: 14.4.2022.

Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta. Luettavissa EUR-Lex-palvelussa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32014R0910&from=FI. Luettu 14.6.2022.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Luettavissa EUR-Lex-palvelussa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI. Luettu 14.6.2022.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta. Luettavissa EUR-Lex-palvelussa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32015L2366&from=FI. Luettu 14.6.2022.

Finlex-palvelu s.a. Suomen kansallisen lainsäädännön Finlex-palvelu. Luettavissa: https://www.finlex.fi/fi/laki/. Luettu 11.4.2022.

Helakorpi, S. 1999. Opinnäytetyö ja tutkimustoiminta ammattikorkeakoulussa. Hämeenlinna: Hämeen ammattikorkeakoulu, Opettajakorkeakoulun julkaisuja D: 188.

Heponiemi, T., Gluschkoff, K., Leemann, L., Manderbacka, K., Aalto, A-M. & Hyppönen, H. 2021. Digital inequality in Finland: access, skills and attitudes as social impact mediators. New Media & Society. Julkaistu 28.7.2021. Luettavissa: https://journals.sagepub.com/doi/10.1177/14614448211023007. Luettu 7.6.2022.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Tammi. Helsinki.

Kaihlanen, A-M., Virtanen, L., Valkonen, P., Kilpinen, J., Hietapakka, L., Buchert, U., Hörhammer, I., Isola, A-M., Laukka, E., Kouvonen, A., Kujala, S.& Heponiemi, T. 2021. Haavoittuvat ryhmät etäpalvelujen käyttäjinä: kokemuksia COVID- 19- epidemian ajalta. Tutkimuksesta tiiviisti: 2021_033, THL. Luettavissa: https://www.julkari.fi/bitstream/handle/10024/142805/URN_ISBN_978-952-343-687-9.pdf?sequence=1&isAllowed=y. Luettu 10.6.2022.

Kyberturvallisuuskeskus 2021a. Sähköinen tunnistaminen. WWW-dokumentti. Päivitetty 11.3.2022. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen. Luettu 27.5.2022.

Kyberturvallisuuskeskus 2021b. Kyberturvallisuuskeskuksen ylläpitämä hyväksytty luettelo kansallisista luottamuspalveluista. Diaarinumero: 783/620/2017. Tunnistuspalvelut -välilehti. Päivitetty 12.4.2022. Luettavissa: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.kyberturvallisuuskeskus.fi%2Fsites%2Fdefault%2Ffiles%2Fmedia%2Ffile%2FTunnistuspalvelurekisteri_31052022.XLSX&wdOrigin=BROWSELINK. Luettu 15.6.2022.

Laki digitaalisten palvelujen tarjoamisesta 306/2019. Luettavissa Finlex-palvelussa: https://www.finlex.fi/fi/laki/ajantasa/2019/20190306. Luettu 14.6.2022.

Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003. Luettavissa Finlex-palvelussa: https://www.finlex.fi/fi/laki/ajantasa/2003/20030013. Luettu 14.6.2022.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009. Luettavissa Finlex-palvelussa: https://www.finlex.fi/fi/laki/ajantasa/2009/20090617. Luettu 14.6.2022.

Liikenne- ja viestintävirasto Traficom 2021. Tulkintamuistio ensitunnistamisessa hyväksyttävistä asiakirjoista ja asiakirjojen tutkinnasta. Diaarinumero Traficom/10078/09.02.00/2021. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Traficomin_tulkintamuistio_ensitunnistamisesta_21_10_2021.pdf. Luettu 14.6.2022.

Maksulaitoslaki 297/2010. Luettavissa Finlex-palvelussa: https://www.finlex.fi/fi/laki/ajantasa/2010/20100297. Luettu 14.6.2022.

Maksupalvelulaki 290/2010. Luettavissa Finlex-palvelussa: https://www.finlex.fi/fi/laki/ajantasa/2010/20100290. Luettu 14.6.2022.

Metsola, A. 2018. Mitä vahva sähköinen tunnistaminen tarkoittaa? FiCom ry:n WWW-dokumentti. Julkaistu 10.10.2018. Luettavissa: https://www.ficom.fi/ajankohtaista/uutiset/mita-vahva-sahkoinen-tunnistaminen-tarkoittaa/. Luettu 15.9.2021.

Mitrunen, J., Salovaara, T. & Viskari, J. 2019. Sähköinen tunnistaminen: Selvitys nykytilasta sekä -kehittämistarpeista. Valtiovarainministeriön julkaisuja 2019: 20. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161432/20_2019_Sahkoinen%20tunnistaminen.pdf?sequence=1&isAllowed=y. Luettu 5.10.2021.

Nordlund, M., Stenberg, L., Forsberg, K., Alastalo, K., Nykänen, J., Ranta, P., & Virkkunen, A. 2014: Ikäteknologian monimuotoinen maailma. Vanhustyön keskusliitto: Vanhus- ja lähimmäispalvelun liitto. Helsinki.

Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto, Valvira 2016. Potilaille annettavat terveydenhuollon etäpalvelut 2016 -ohje. Päivitetty 8.2.2022. Luettavissa: https://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/potilaille-annettavat-terveydenhuollon-etapalvelut. Luettu 17.6.2022.

Tietosuojavaltuutetun toimisto s.a. a. Henkilötietojen käsittelyn oikeusperusteet. Luettavissa: https://tietosuoja.fi/kasittelyperusteet. Luettu 7.6.2022.

Tietosuojavaltuutetun toimisto s.a. b. Mikä on henkilötieto? Luettavissa: https://tietosuoja.fi/mika-on-henkilotieto. Luettu 7.6.2022.

Tietosuojavaltuutetun toimisto s.a. c. Ohjeet organisaatioille henkilötietojen käsittelystä. Luettavissa: https://tietosuoja.fi/henkilotietojen-kasittely. Luettu 7.6.2022.

Tuorila, H. 2016: Sähköisten palveluiden käyttämättömyyden seuraukset välttämättömyyspalveluissa. Kilpailu- ja kuluttajavirasto. Kilpailu- ja kuluttajaviraston selvityksiä 6/2016. Luettavissa: https://www.kkv.fi/uploads/sites/2/2021/11/2016-kkv-selvityksia-6-2016-sahkoisten-palvelujen-kayttamattomyys.pdf. Luettu 7.6.2022.

Tuorila, H. 2017: Sähköisten tunnistamisvälineiden saavutettavuuden vaikutus palveluyhteiskunnan digitalisaatioon. Julkari. STM:n hallinnonalan avoin julkaisuarkisto. Luettavissa: https://www.julkari.fi/bitstream/handle/10024/134737/YP1701_Tuorila.pdf?sequence=1&isAllowed=y. Luettu 7.6.2022.

Valtiovarainministeriö 2006. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI.

Tunnistaminen julkishallinnon verkkopalvelussa. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_12_2006.pdf. Luettu 15.5.2022.

Valtiovarainministeriö 2017. Sähköisen asioinnin tietoturvallisuus -ohje. Valtiovarainministeriön julkaisuja 25/2017. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_25_2017.pdf. Luettu 7.6.2022.

Virtanen, L., Kaihlanen A-M., Kouvonen A., Safarov N., Laukka E., Valkonen P. & Heponiemi T. 2022: Hyvinvointiyhteiskunnan digitaaliset palvelut yhdenvertaisiksi. 9 kriittistä toimenpidettä haavoittumassa asemassa olevien huomioimiseksi. Päätösten tueksi 1/2022. Terveyden ja hyvinvoinnin laitos, THL. Luettavissa: https://www.julkari.fi/bitstream/handle/10024/143708/URN_ISBN_978-952-343-811-8.pdf?sequence=1. Luettu 10.6.2022.

Voutilainen, T. 2020: Digitaalisten palvelujen sääntely. Alma Talent. Helsinki.

Liitteet

Liite 1. Säädösten lyhenteet

Liite 2. Kyselyyn vastaajan informointilomake, opinnäytetyöhön liittyvä sähköinen kysely

Liite 3. Kyselylomake (Webropol-kysely)

Liite 1. Säädösten lyhenteet

Säädöksen (lain) lyhenne	Säädöksen (lain) koko nimi
e-IDAS-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 1999/93/EY kumoamisesta
EU:n yleinen tietosuoja-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta
PSD 2 -direktiivi / EU:n toinen maksupalveludirektiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta
digipalvelulaki	Laki digitaalisten palvelujen tarjoamisesta 306/2019
asiointilaki	Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003
tunnistuslaki	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009
maksulaitoslaki	Maksulaitoslaki 297/2010
maksupalvelulaki	Maksupalvelulaki 290/2010

lähde: Finlex-palvelu ja EUR-Lex-palvelu opinnäytetyössä käytetyn keskeisen lainsäädännön osalta (säädösten lyhenteet niin kuin Finlex-palvelun viitetiedoissa on esitetty)

Liite 2. Kyselyyn vastaajan informointilomake, opinnäytetyöhön liittyvä sähköinen kysely

TIEDOTE SÄHKÖISEN KYSELYN TARKOITUKSESTA

Pyyntö osallistua ja vastata sähköiseen kyselyyn

Sinua pyydetään osallistumaan ja vastaamaan sähköiseen kyselyyn, jossa tutkitaan sähköisten palvelujen käyttöä ja niihin liittyvää loppukäyttäjän tunnistamista. Kyselyssä on yhdeksän kysymystä. Kyselyyn vastaaminen kestää noin 8 minuuttia. Kyselyyn vastaaminen on vapaaehtoista. Kysymyksissä ei pyydetä sinua laittamaan vastausosioon itsestäsi mitään tunnisteellista tietoa (kuten etunimeä, sukunimeä, sähköpostiosoitetta, kotikaupunkia yms.).

Tämä tiedote kuvaa sähköistä kyselyä ja kyselyyn vastaajan osuutta siinä. Jatkamalla varsinaiseen sähköiseen kyselyyn seuraavan linkin kautta < linkki varsinaiselle kyselylomakkeelle (webropol-kysely) >, ja ryhtymällä vastaamaan siinä oleviin kuuteen kysymykseen, annat suostumuksesi kyselyyn osallistumisesta.

Vapaaehtoisuus

Kyselyyn osallistuminen on täysin vapaaehtoista. Voit myös keskeyttää sähköiseen kyselyyn vastaamisen koska tahansa syytä ilmoittamatta.

Sähköisen kyselyn tarkoitus

Tämän sähköisen kyselyn tarkoituksena on tutkia sähköisten palvelujen käyttöä ja niihin liittyvää loppukäyttäjän tunnistamista kuluttajan näkökulmasta. Kysely toteutetaan osana aineiston keruuta Haaga-Helia ammattikorkeakoulun opinnäytetyötä varten. Opinnäytetyöhön liittyvän kyselytutkimuksen avulla voidaan saavuttaa aihepiiristä tärkeää tietoa, jota analysoidaan ja hyödynnetään opinnäytetyössä, opinnäytetyön tekijän toimesta.

Sähköisen kyselyn toteuttaja

Kysely toteutetaan osana aineiston keruuta Haaga-Helia ammattikorkeakoulun opiskelijan, Mika Aarnion, Tietojenkäsittelyn koulutusohjelman opinnäytetyötä varten. Opinnäytetyön nimi on ”Sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta”. Opinnäytetyö on kokonaisuudessaan tarkoituksena toteuttaa ja saada valmiiksi vuoden 2022 aikana.

Sähköisen kyselyn mahdolliset hyödyt

Opinnäytetyöhön liittyvän kyselytutkimuksen avulla voidaan saavuttaa aihepiiristä tärkeää tietoa, jota analysoidaan ja hyödynnetään opinnäytetyössä.

Sähköisen kyselyn tuloksista tiedottaminen

Vastausten perusteella tehtävästä analyysistä sekä sen tuloksista kerrotaan opinnäytetyössä. Kysymyksessä on niin ikään Haaga-Helia ammattikorkeakoulun Tietojenkäsittelyn koulutusohjelmaan vuonna 2022 tehtävä opinnäytetyö, joka julkaistaan avoimesti sähköisessä opinnäytetöiden ns. Theseus-tietokannassa.

Mitä kyselyvastauksille tapahtuu sähköisen kyselyn päätyttyä?

Varsinainen kyselytutkimusaineisto säilytetään vain vuoden 2022 ajan Webropol-ohjelmistossa. Vuoden 2022 aikana sen analysoija, opinnäytetyön tekijä, Mika Aarnio hyödyntää sitä opinnäytetyössään. Kun opinnäytetyö saadaan valmiiksi ja jätetään Haaga-Helia ammattikorkeakoululle arvioitavaksi, niin tällöin kyselyyn saatujen vastausten käsittely loppuu. Kun vuoden 2022 aikana opinnäytetyön tekijä tullee saamaan opinnäytetyöstään arvosanan Haaga-Helia ammattikorkeakoululta, ja mikäli hän ei hae muutosta saamaansa opinnäytetyön arvosanaan Haaga-Helia

ammattikorkeakoululta, niin tämän jälkeen sähköisen kyselyyn annetut vastaukset tuhotaan lopullisesti Webropol-ohjelmistosta opinnäytetyön tekijän toimesta.

Lisätiedot

Pyydän sinua tarvittaessa esittämään sähköiseen kyselyyn liittyviä kysymyksiä sekä mahdollisia opinnäytetyökokonaisuuteen liittyviä kysymyksiä ensisijaisesti opinnäytetyöstä vastaavalle henkilölle, Haaga-Helia ammattikorkeakoulun opiskelija Mika Aarniolle ja/tai tarvittaessa tämän opinnäytetyöohjaajalle.

Sähköisen kyselyn toteuttaja / opinnäytetyötekijä, Haaga-Helia ammattikorkeakoulu

Nimi: Mika Aarnio

Sähköposti: mika.aarnio@myy.haaga-helia.fi

Opinnäytetyön ohjaaja / Haaga-Helia ammattikorkeakoulu

Nimi: Elina Ulpovaara

Titteli: Lehtori

Organisaatio: Haaga-Helia ammattikorkeakoulu Oy

Sähköposti: elina.ulpovaara@haaga-helia.fi

Liite 3. Kyselylomake (Webropol-kysely)

Sähköisten palvelujen käyttö ja niihin liittyvä loppukäyttäjän tunnistaminen

Pakolliset kysymykset merkitty tähdellä (*)

TIEDOTE SÄHKÖISEN KYSELYN TARKOITUKSESTA

Sinua pyydetään osallistumaan ja vastaamaan sähköiseen kyselyyn, jossa tutkitaan sähköisten palvelujen käyttöä ja niihin liittyvää loppukäyttäjän tunnistamista.
Kyselyssä on yhdeksän kysymystä. Kyselyyn vastaaminen kestää noin 8 minuuttia.
Kyselyyn vastaaminen on vapaaehtoista. Kysymyksissä ei pyydetä sinua laittamaan vastausosioon itsestäsi mitään tunnisteellista tietoa (kuten etunimeä, sukunimeä, sähköpostiosoitetta, kotikaupunkia yms.).

Vapaaehtoisuus
Kyselyyn osallistuminen on täysin vapaaehtoista.
Voit myös keskeyttää sähköiseen kyselyyn vastaamisen koska tahansa syytä ilmoittamatta.

Sähköisen kyselyn tarkoitus
Tämän sähköisen kyselyn tarkoituksena on tutkia sähköisten palvelujen käyttöä ja niihin liittyvää loppukäyttäjän tunnistamista kuluttajan näkökulmasta. Kysely toteutetaan osana aineiston keruuta Haaga-Helia Ammattikorkeakoulun opinnäytetyötä varten. Opinnäytetyöhön liittyvän kyselytutkimuksen avulla voidaan saavuttaa aihepiiristä tärkeää tietoa, jota analysoidaan ja hyödynnetään opinnäytetyössä, opinnäytetyön tekijän toimesta.

Sähköisen kyselyn toteuttaja
Kysely toteutetaan osana aineiston keruuta Haaga-Helia Ammattikorkeakoulun opiskelijan, Mika Aarnion, Tietojenkäsittelyn koulutusohjelman opinnäytetyötä varten. Opinnäytetyön nimi on ”Sähköiset palvelut ja vahva tunnistaminen kuluttajan näkökulmasta”. Opinnäytetyö on kokonaisuudessaan tarkoituksena toteuttaa ja saada valmiiksi vuoden 2022 aikana.

Sähköisen kyselyn mahdolliset hyödyt
Opinnäytetyöhön liittyvän kyselytutkimuksen avulla voidaan saavuttaa aihepiiristä tärkeää tietoa, jota analysoidaan ja hyödynnetään opinnäytetyössä.

Sähköisen kyselyn tuloksista tiedottaminen
Vastausten perusteella tehtävästä analyysistä sekä sen tuloksista kerrotaan opinnäytetyössä.

Kysymyksessä on niin ikään Haaga-Helia Ammattikorkeakoulun Tietojenkäsittelyn koulutusohjelmaan vuonna 2022 tehtävä opinnäytetyö, joka julkaistaan avoimesti sähköisessä opinnäytetöiden ns. Theseus-tietokannassa.

Mitä kyselyvastauksille tapahtuu sähköisen kyselyn päätyttyä?
Varsinainen kyselytutkimusaineisto säilytetään vain vuoden 2022 ajan Webropol-ohjelmistossa. Vuoden 2022 aikana sen analysoija, opinnäytetyön tekijä, Mika Aarnio hyödyntää sitä opinnäytetyössään. Kun opinnäytetyö saadaan valmiiksi ja jätetään Haaga-Helia Ammattikorkeakoululle arvioitavaksi, niin tällöin kyselyyn saatujen vastausten käsittely loppuu. Kun vuoden 2022 aikana opinnäytetyön tekijä tullee saamaan opinnäytetyöstään arvosanan Haaga-Helia Ammattikorkeakoululta, ja mikäli hän ei hae muutosta saamaansa opinnäytetyön arvosanaan Haaga-Helia Ammattikorkeakoululta, niin tämän jälkeen sähköisen kyselyyn annetut vastaukset tuhotaan lopullisesti Webropol-ohjelmistosta opinnäytetyön tekijän toimesta.

Lisätiedot

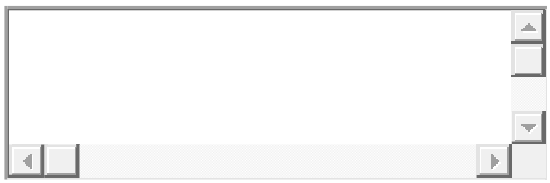
Pyydän sinua tarvittaessa esittämään sähköiseen kyselyyn liittyviä kysymyksiä sekä mahdollisia opinnäytetyökokonaisuuteen liittyviä kysymyksiä ensisijaisesti opinnäytetyöstä vastaavalle henkilölle, Haaga-Helia Ammattikorkeakoulun opiskelija Mika Aarniolle ja/tai tarvittaessa tämän opinnäytetyöohjaajalle.

Sähköisen kyselyn toteuttaja / opinnäytetyötekijä, Haaga-Helia Ammattikorkeakoulu
Nimi: Mika Aarnio
Sähköposti: mika.aarnio@myy.haaga-helia.fi

Opinnäytetyön ohjaaja / Haaga-Helia Ammattikorkeakoulu
Nimi: Elina Ulpovaara
Titteli: Lehtori
Organisaatio: Haaga-Helia Ammattikorkeakoulu Oy
Sähköposti: elina.ulpovaara@haaga-helia.fi

1. Mitä sähköisiä viranomaispalveluita olet viime aikoina käyttänyt?

***Sähköisillä viranomaispalveluilla tarkoitetaan tässä laajasti ymmärrettynä kaikkia Suomen julkisen sektorin sähköisiä asiointipalveluita kuten Kansaneläkelaitoksen (KELA) sähköisiä hakemusten käsittelypalveluita ja KELA:n muita e-asiointipalveluita esimerkiksi opiskelijaetuuksiin liittyen, sosiaali- ja terveysviranomaisten terveys- ja rokotustietojen sekä sähköisten reseptien Omakanta-palvelua, verohallinnon OmaVero -palvelua esimerkiksi veroilmoituksen hoitamista varten tai muutosverokortin tilaamista varten, poliisin sähköistä asiointipalvelua yms. **



2. Millä sähköisellä tunnistusvälineellä /-tavalla kirjauduit käyttämiisi julkisen sektorin sähköisiin viranomaispalveluihin? *

☐ **Suomalaisen pankin myöntämällä verkkopankkitunnuksella?**

☐ **Teleoperaattorin myöntämällä mobiilivarmenteella?**

☐ **Digi- ja väestötietoviraston kansalaisvarmenteella (joka on mahdollista saada poliisin myöntämään sirulliseen henkilökorttiin)?**

☐ **Pelkällä käyttäjätunnus + salasana -yhdistelmällä? (toisin sanoen tilanne, jossa ei vaadittu sinulta palvelun käyttämisen edellytyksenä vahvaa sähköistä tunnistautumista)?**

☐ **Joku muu, mikä?**

3. Mitä mieltä olet seuraavista väittämistä:

Asioiden hoitaminen julkisen sektorin sähköisissä asiointipalveluissa toimii sujuvasti. *

- **Täysin samaa mieltä**
- **Jokseenkin samaa mieltä**
- **Ei samaa eikä eri mieltä**
- **Jokseenkin eri mieltä**
- **Täysin eri mieltä**

4. Mitä sähköisiä yksityissektorin palveluita olet viime aikoina käyttänyt?

Sähköisillä yksityissektorin palveluilla tarkoitetaan tässä laajasti ymmärrettynä kaikkia suomalaisia kaupallisia, yksityisen sektorin palveluita kuten suomalaisten pankkien tarjoamia verkkopankkipalveluita, suomalaisten teleoperaattorien tarjoamia sähköisiä asiointipalveluita, elokuvalippujen ja muiden kulttuurialan tapahtumien lippujen välitys- ja ostopalveluita, kaupallisten toimijoiden verkkokauppapalveluita yms. *

5. Millä sähköisellä tunnistusvälineellä /-tavalla kirjauduit käyttämiisi kaupallisiin, yksityissektorin sähköisiin palveluihin? *

- **Suomalaisen pankin myöntämällä verkkopankkitunnuksella?**
- **Teleoperaattorin myöntämällä mobiilivarmenteella?**
- **Digi- ja väestötietoviraston kansalaisvarmenteella (joka on mahdollista saada poliisin myöntämään sirulliseen henkilökorttiin)?**

☐ **Pelkällä käyttäjätunnus + salasana -yhdistelmällä? (toisin sanoen tilanne, jossa ei vaadittu sinulta palvelun käyttämisen edellytyksenä vahvaa sähköistä tunnistautumista)?**

☐ **Joku muu vaihtoehto, mikä?**

6. Mitä mieltä olet seuraavista väittämistä:

Asioiden hoitaminen yksityisen sektorin sähköisissä asiointipalveluissa toimii sujuvasti. *

○ **Täysin samaa mieltä**

○ **Jokseenkin samaa mieltä**

○ **Ei samaa eikä eri mieltä**

○ **Jokseenkin eri mieltä**

○ **Täysin eri mieltä**

7. Onko sinulla hankittuna teleoperaattorin myöntämä mobiilivarmenne? *

○ **Kyllä**

○ **Ei**

8. Onko sinulla hankittuna Digi- ja väestötietoviraston kansalaisvarmenne? *

○ **Kyllä**

○ **Ei**

9. Miten koet sähköisten asiointipalveluiden loppukäyttäjänä palveluiden luottamuksellisuuden ja tietoturvan toteutuva