



ARVIOMUISTIO

Valtiovarainministeriö
Julkisen hallinnon tieto- ja viestintätekniinen osasto
18.03.2021

Arviomuistio digitaalisen henkilöllisyyden kehityksestä

Sisällys

I OSA: JOHDANTO JA HANKKEEN TAUSTA	5
1. Johdanto	5
2. Digitaalisen henkilöllisyyden hanke ja sen tavoitteet	10
II OSA: DIGITAALISEN HENKILÖLLISYYDEN NYKYTILA JA TULEVAISUUS	12
3. Nykytilan kuvaus	12
3.1. Henkilöllisyyttä osoittavat asiakirjat	13
3.1.1. Henkilökortti	13
3.1.2. Passi	15
3.2. Vahva sähköinen tunnistaminen	18
3.2.1. Sähköinen tunnistaminen	18
3.2.2. Vahvat sähköiset tunnistuspalvelut	18
3.2.3. Tunnistusmenetelmät	18
3.2.4. Varmenne	19
3.2.5. Luottamusverkosto	19
4. Nykytilan arvio	20
5. Tavoiteltavan toimintamallin kuvaus	27
5.1. Digitaalisen identiteetin muodostaminen ja myöntäminen	28
5.1.1. Ydinidentiteetti ja asiayhteydellinen identiteetti	29
5.2. Ratkaisut, jotka mahdollistavat digitaalisen henkilöllisyyden osoittamisen käytiasioinnissa	30
5.3. Ratkaisut, jotka mahdollistavat muiden viranomaistietojen, kuten lupien tai vahvistettujen rekisteritietojen esittämisen	32
5.4. Digitaalisen henkilöllisyyden osoittaminen asiointipalveluissa sähköisesti	32
5.5. Alustavat arviot tavoitetilan vaikutuksista nykyiseen toimintaympäristöön ja vaikutusarvioinnin suunnitelmat	35
5.5.1. Esimerkki tulevaisuuden tavoitetilasta	38
5.6. Vaihtoehtoisten toimintamallien tarkastelu	40
III OSA: Tavoiteltavan toimintamallin keskeiset oikeudelliset kysymykset	42
6. Hankkeen taustalla vaikuttavan lainsäädännön nykytila	42
6.1. Perus- ja ihmisoikeudet	42
6.1.1. Perusoikeuksien kohderyhmä ja turvaaminen	42
6.1.2. Perusoikeudet sähköisessä asiointinnissa	43
6.1.3. Perus- ja ihmisoikeusnäkökulma ja identiteetti	46
6.2. Julkisen vallan käyttö, julkinen tehtävä ja julkinen hallintotehtävä	48
6.3. Yhdenvertaisuus ja henkilön aseman perusteella huomioitavat erityiskysymykset	51
6.3.1. Yhdenvertaisuuslaki ja tasa-arvo	51

6.3.2.	Vajaavaltaisia henkilöitä koskevat erityiskysymykset	54
6.3.3.	Vammaisia henkilöitä koskevat erityiskysymykset.....	56
6.3.4.	Työntekijöitä koskevat erityiskysymykset	57
6.3.5.	Ulkomaan kansalaisia koskevat erityiskysymykset.....	58
6.4.	Sähköistä asiointia koskeva EU-sääntely.....	60
6.4.1.	Single Digital Gateway	60
6.4.2.	Palveludirektiivi	60
6.4.3.	Direktiivi digitaalisten välineiden ja prosessien käytöstä yhtiöoikeuden alalla.....	61
6.5.	Luottamusverkostoa ja sähköistä tunnistamista koskeva sääntely	61
6.5.1.	Tunnistusmarkkinoiden sääntely.....	61
6.5.2.	eIDAS-asetus ja sen täytäntöönpano.....	63
6.5.3.	PSD2	66
6.6.	Valtion identiteetinhallintaa ja tunnistusvälineitä koskeva sääntely.....	67
6.6.1.	Väestötietojärjestelmä ja sen sisältämät tunnisteet	67
6.6.2.	Digi- ja väestötietoviraston varmennetoiminta ja kansalaisvarmenne.....	68
6.7.	Julkisen sektorin sähköiset palvelut, tunnistaminen ja tiedonhallinta.....	69
6.7.1.	Velvollisuus järjestää sähköisiä palveluita.....	69
6.7.2.	Henkilöllisyyden osoittaminen sähköisissä julkisissa palveluissa	71
6.7.3.	Tiedonhallinta	72
6.8.	Henkilöllisyysasiakirjojen sääntely	74
6.8.1.	Henkilöllisyysasiakirjojen sääntelystä yleisesti	74
6.8.2.	Henkilökortin sääntely.....	75
7.	Toimintamallin kilpailu- ja valtiontukioikeudelliset näkökohdat.....	76
7.1.	Yleisesti kilpailu- ja valtiontukisääntelystä	76
7.1.1.	Soveltamisala ja taloudellisen toiminnan käsite.....	76
7.1.2.	Kilpailuneutraliteetti.....	78
7.1.3.	Kielletty valtiontuki	79
7.2.	Toiminnallinen ratkaisu kilpailu- ja valtiontukioikeudellisesta näkökulmasta	82
7.2.1.	Toiminnallisen ratkaisun elementit	82
7.2.2.	Digitaalisen identiteetin muodostaminen.....	83
7.2.3.	Sovellus, josta identiteetin voi todentaa käytäntöasiointissa.....	86
7.2.4.	Mahdollisuus esittää muita lupia/attribuutteja sovelluksessa	87
7.2.5.	Sovelluksen etäkäyttö: tunnistuspalvelu julkisen sektorin asiointipalveluihin	88
7.3.	Yhteenvedo ja selvitetävät kysymykset.....	97
8.	Muut hankkeen etenemisen kannalta olennaiset oikeudelliset kysymykset.....	98
8.1.	Henkilöllisyysasiakirjat ja digitaalinen identiteetti.....	98

8.2. Vahva sähköinen tunnistaminen ja digitaalinen identiteetti.....	100
8.2.1. Valtion ratkaisun suhde vahvaan sähköiseen tunnistamiseen.....	100
8.2.2. Digitaalisen identiteetin hyödyntäminen sähköisessä asiointissa	103
8.3. eIDAS ja digitaalinen identiteetti	104
8.4. Tiedonhallinta	105
IV OSA: YHTEENVETO	108

I OSA: JOHDANTO JA HANKKEEN TAUSTA

1. Johdanto

Tässä muistiossa käsitellään niitä keskeisimpiä ratkaisuja, joita Digitaalisen henkilöllisyyden ja sen hyödyntämistapojen kehittämishankkeessa on suunniteltu toteutettavan digitaalisen henkilöllisyyden ja siihen liittyvien käyntiasioinnin ja sähköisen asioinnin ratkaisujen osalta. Konkreettinen juridinen tarkastelu on kuitenkin sähköisen asioinnin osalta toistaiseksi rajattu ratkaisuihin, jotka mahdollistavat digitaalisen henkilöllisyyden hyödyntämisen julkisen sektorin palveluissa. Hankkeen tavoitteet ja erityisesti visiot sähköisen asioinnin tulevaisuudesta ja siihen liittyvästä EU-kehityksestä edellyttävät uusia avauksia myös yksityisen sektorin palveluihin. Muistiossa todetaan, että raja yksityisen ja julkisen sektorin asioinnin välillä on osin vaikeasti hahmotettavissa ja tulee jatkossa edelleen hämärtymään. Nämä muutokset vaativat uusia toimintamalleja ja -tapoja myös digitaalisen identiteetin kansalliseen lainsäädäntöön, toteutukseen ja hyödyntämiseen.

Sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annettu EU-asetus (myöhemmin eIDAS-asetus) tuli voimaan 17.9.2014 ja sitä on sovellettu 1.7.2016 alkaen. Asetuksen 49 artiklan ensimmäisen kohdan mukaan Euroopan komissio järjesti julkisen kuulemisen kesällä 2020 asetuksen soveltamisen uudelleenarvioimiseksi ja raportoimiseksi Euroopan parlamentille ja neuvostolle. Komissio on tämän hetken tietojen valossa esittämässä parlamentille huhtikuussa 2021 ehdotuksensa EU:n sähköistä tunnistamista ja luottamuspalveluita määrittävän asetuksen muutoksista ja eurooppalaisen digitaalisen identiteetin kehikon luomisesta. Julkisen kuulemisen tulosten perusteella voidaan päätellä, että nykyisen eIDAS-asetuksen toimeenpano ei ole täyttänyt sille asetettuja odotuksia. Rajat ylittävän sähköisen tunnistaminen ei mahdollista kuin osassa jäsenvaltioita ja tapahtumamäärät ovat jääneet hyvin vaatimattomiksi. Komission puheenjohtaja Von der Leyen nostikin 16.9.2020 pitämässään linjapuheessa esille tarpeen synnyttää eurooppalainen vaihtoehto suurille digitaalisille alustoille, vaihtoehto joka olisi eurooppalaisten kontrolloitavissa, ja jossa kansalainen voisi itse päättää, miten häneen liittyviä tietoja käytetään.

Euroopan komission tiedonannossa Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle ja Euroopan alueiden komitealle Digitaalisesta finanssistrategiasta (Digital Finance Strategy for the EU, 24.9.2020) komissio kuvaa tarpeen luoda vuoteen 2024 mennessä yhteinen eurooppalainen lainsäädännöllinen kehikko digitaaliselle identiteetille. Lainsäädännöllinen kehikko mahdollistaisi finanssisektorille asiakkaaksi ottamisen entistä

nopeammin ja sujuvammin. Komissio edellyttäisi, että asiakkaan tunnistamisessa tukeuduttaisiin uudistettuun eIDAS-sääntelyyn. Ratkaisun tulisi mahdollistaa finanssipalveluiden asiakkaille mahdollisuuden jakaa omalla suostumuksellaan omia tietojaan.

Eurooppa-neuvoston päätelmissä (2.10.2020) nostetaan esille tarvetta kehittää Euroopan Unionin laajuista turvallista sähköisen tunnistamisen kehikkoa, joka mahdollistaisi ihmisille hallita omaa digitaalista identiteettiään ja joka mahdollistaisi pääsyn julkisen ja yksityisen sektorin palveluihin ja rajat ylittäviin palveluihin. Neuvosto pyytää komissiota antamaan ehdotuksen eurooppalaisesta digitaalisesta identiteetistä vuoden 2021 puoliväliin mennessä.

Komission odotetaan ehdottavan eIDAS-asetukseen täsmennyksiä, lisää velvoittavuutta jäsenvaltioihin tukea rajat ylittävää tunnistamiseen edellytyksiä ja vahvistuksia yksityisen sektorin asemaa osallistua ratkaisujen toteuttamiseen. Ennakkotietojen mukaan komissio tulisi ehdottamaan yhteistä eurooppalaista sääntelyä uuden tyyppisille luottamuspalveluille. Kyseiset luottamuspalvelut voisivat välittää Euroopan Unionin alueella varmennettuja henkilötietoja jäsenvaltioissa ja jäsenvaltioiden välillä. Uudet Euroopan Unionin luottamuspalvelut nojaisivat käyttäjän hallussa olevan digitaalisen mobiililompakon konseptiin. Yksittäisen jäsenvaltion tulisi tuottaa digitaaliseen lompakkoon viranomaisen (pohjoismaissa tyypillisesti väestötietoviranomainen) henkilön ydinidentiteetin, siihen liittyvän digitaalisen todisteen (kredentiaali). Näitä käyttäjän hallussa olevia ydinidentiteettiin liitettyjä henkilötietoja tulisi jäsenvaltioiden hyväksyä omissa digitaalisissa palveluissaan hyödynnettäviksi.

Suorien eIDAS-sääntelymuutosten lisäksi komissio tulee ehdottamaan eurooppalaisen digitaalisen identiteetin kehikon EUid:n synnyttämisestä EU-jäsenvaltioiden välille. Ennakkotietojen perusteella EUid tukeutuisi jäsenvaltioiden kansallisten digitaalisen identiteetin hallintajärjestelmien varaan tavoitteena synnyttää yhteentoimiva toimintamalli, jossa EU-kansalainen voisi luovuttaa rajat ylittävissä palveluissa digitaalisen mobiililompakon avulla häneen itseensä liittyviä tietoja toisen jäsenvaltion palveluihin. Eurooppalainen digitaalinen identiteetti velvoitettaisiin hyväksymään jäsenvaltioiden sekä julkisissa, että yksityisissä palveluissa. EU-kansalaisille EUid:n käyttöönotto olisi vapaaehtoista.

Digitaalisen henkilöllisyyden ja sähköisen asioinnin maailma on kehittymässä suuntaan, jossa henkilö itse kontrolloi häneen liittyvien tietojen jakamista kolmansille osapuolille (mobiilipohjaisten) identiteetilompakoiden avulla. Kansalaiseen liittyvän tiedon pitää siirtyä entistä sujuvammin asiointipalvelujen

välillä, ja tähän liittyvät oleellisesti itse henkilön identiteettiin liittyvät muut tiedot, joiden tulisi olla varmennettavissa sähköisesti samalla tavoin kuin henkilön henkilötunnus (osa ydinidentiteettiä) on nykyisin. Yksittäisten ydinidentiteettiä tarkemmin kuvaavien attribuuttien alkuperä, eheys ja ajantasaisuus (aikaleima) eivät ole tänä päivänä selvitettävissä. Esimerkiksi nykyisen sähköisen asiointin yhteydessä ei ole teknisesti mahdollista kertoa pelkkää osoitetietoa luotettavasti paljastamatta henkilöllisyyttään. On ensin todistettava henkilöllisyys (henkilötunnus) asiointipalvelulle, jonka jälkeen palvelu hakee tarvitsemansa osoitetiedon kolmannen osapuolen rekisteristä henkilötunnuksen avulla. Mikäli henkilötunnusta ei ole, palvelun käyttö ei ole mahdollista.

Digitaalisia palveluita käytetään yhä enemmän, ja asiointi on siirtymässä monilla toimialoilla pääasiallisesti digitaaliseksi. Palveluiden kehittyminen edellyttää myös digitaalisen henkilöllisyyden kehittämistä siten, että se vastaa moderneja teknologioita hyödyntävien palveluiden vaatimuksiin. Jotta taataan turvallisuus ja luotettavuus palveluissa, tulee digitaalisen identiteetin perustua valtion takaamaan ydinidentiteettiin, joka tarjotaan yhdenvertaisesti ja saavutettavasti kaikille yhteiskunnan palveluja hyödyntäville.

Siirryttäessä yhä enemmän digitaaliseen toimintamalliin on huomioitava, että yhteiskunnan painopiste muuttuu. Digitaaliset palvelukanavat tulevat käytetyimmiksi ja kansalaisyhteiskunta siirtyy verkkoon. Näissä olosuhteissa nousee esille myös kysymys siitä, kenellä on pääsy palveluihin ja kuka voi ottaa osaa tähän digitaaliseen yhteiskuntaan. Tällöin on myös kiinnitettävä enemmän huomiota siihen, miten luonnolliset henkilöt voivat käyttää digitaalista henkilöllisyyttä digitaalisissa palveluissa. Tarkasteltaessa yksilön perusoikeuksia vasten digitaalisen yhteiskunnan rakenteita voidaan kysyä, olisiko yksilölle turvattava mahdollisuudet ja välineet sähköiseen asiointiin julkisen vallan toimesta, osallistumisoikeuksien, hyvän hallinnon ja yhdenvertaisuuden nimissä.

Tähän kehitykseen ja näihin tarpeisiin vastaamiseksi valtiovarainministeriössä on tunnistettu tarve kehittää digitaalisen henkilöllisyyden saamisen, käytön ja hallinnoinnin toimintatapoja kokonaisuutena. Vastaavia tarpeita on tunnistettu myös keskeisten markkinatoimijoiden keskuudessa. Mm. Findy-yhteisö on esittänyt digitaalisen identiteetin tulevaisuuden ratkaisuksi kryptografisesti vahvistettuja väittämiä. Nämä väittämät toimivat etukäteen loppukäyttäjälle myönnettyinä todisteina (kredentiaaleina), joita käyttäjä voi osoittaa sähköisessä asiointitilanteessa hajautetun identiteettiverkon välityksellä.

Nykyisestä sähköisen kirjautumisen kehittämisestä tulisi siirtyä tarkastelemaan koko digitaalisen henkilöllisyyden ketjua rekisteri-identiteetistä asiointitapahtumaan. Asiointitapahtuman luonne ei aina vaadi kirjautumista palveluun vahvasti tunnistautuen, vaan se voi olla esimerkiksi pelkän iän osoittaminen ja todistaminen sähköisesti. Ekosysteemin on siis muututtava tukemaan henkilöllisyyttä määrittävän vahvistetun tiedon myöntämistä ja osoittamista esimerkiksi puhelinsovelluksen avulla sekä käyntiasioinnissa, että sähköisessä asioinnissa. Ekosysteemin tulee tukea eri tasoisia digitaalisen henkilöllisyyden ja henkilötietojen osoittamisen menetelmiä rekisteri-identiteetin ja siitä luotavan digitaalisen todisteen luotettavuustasosta riippuen. Asiointipalveluilla voi olla tarve mahdollistaa myös alempia luotettavuustasoja tai toisaalta rajata palvelua tasojen perusteella (esim. passin hakeminen poliisilta sähköisesti). Ekosysteemin sekä asiointipalvelujen tulee jatkossa tukea myös alaikäisten ja ulkomaalaisten digitaalisen henkilöllisyyden osoittamisen menetelmiä palvelusta riippuen.

Pääministeri Marinin hallitusohjelmassa on asetettu tavoitteeksi, että Suomi tunnetaan edelläkävijänä, jossa digitalisaation ja teknisen kehityksen tuomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen. Tavoitteena on nostaa julkisen sektorin teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä. Hallitusohjelman mukaan tavoitteena on edistää Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen sekä edistää toimivien tunnistusratkaisujen kehittymistä. Hallitusohjelmassa on lisäksi nostettu esiin henkilön mahdollisuudet hallita omia julkisissa palveluissa olevia tietojaan sekä riittävät tukipalvelut sähköisten julkisten palveluiden käyttöön yhdenvertaisuuden varmistamiseksi.

Valtiovarainministeriö on 8.10.2020 asettanut hankkeen digitaalisen henkilöllisyyden ja sen hyödyntämistapojen kehittämiseksi. Tässä muistiossa kuvataan Digitaalisen henkilöllisyyden kehittämisen hankkeen tavoitteet ja ne tarvittavat toimenpiteet, joilla henkilöön liittyvät tai henkilöllisyyttä kuvaavat tiedot voitaisiin tuoda tehokkaammin henkilön itsensä hallinnoitaviksi ja samalla mahdollistaa monipuolisempien, turvallisempien ja valtion rajat ylittävien sähköisten palvelujen kehittäminen. Hankkeessa toteutettavat ratkaisut suunnitellaan lähtökohtaisesti siten, että ne ovat teknisesti hyödynnettävissä myös yksityisen sektorin käyttöön. Tavoiteltavan toimintamallin kuvaus pyrkii avaamaan mahdollisia yksityisen sektorin hyödyntämistapoja tulevaisuuden ekosysteemissä, mutta arviomuistion juridinen tarkastelu on tehty julkisen sektorin palveluiden kannalta. Hanke ei lähtökohtaisesti muuta julkisen hallinnon mahdollisuuksia hyödyntää luottamusverkoston vahvan sähköisen tunnistamisen palveluita.

Arviomuistion tavoitteena on kartoittaa olemassa olevaa lainsäädäntöä sekä arvioida niitä keskeisiä oikeudellisia kysymyksiä, jotka vaikuttavat valtion mahdollisuuksiin tuottaa uusia ratkaisuja digitaalisen henkilöllisyyden ja sähköisen tunnistamisen toimintakentälle. Lisäksi muistiossa pyritään kartoittamaan sellaisia oikeudellisia kysymyksiä, jotka ovat keskeisiä mahdolliselle hallituksen esityksen perusvalmistelulle ja edellyttävät laajempaa vuoropuhelua ennen perusvalmistelun asettamista.

Hankkeen taustalla on pidempiaikainen kehitys henkilöllisyyden ja digitaalisten palvelujen alalla. Henkilön virallisen identiteetin hallinnoimista ja käyttöä koskevia selvityksiä on toteutettu viimeisen vuosikymmenen aikana eri hankkeissa. Kattavimpana selvityksenä voidaan pitää sisäministeriön joulukuussa 2010 julkaistua identiteettiohjelman loppuraporttia¹, jossa kuvataan tuolloin viranomaisen tuottaman identiteetin luomiseen, hallinointiin ja käyttöön kohdistuneita kehitystarpeita. Osa raportin ehdotuksista on toteutunut sen julkaisun jälkeen. Valtiovarainministeriön asettama henkilötunnuksen uudistamista pohtinut työryhmä käsitteli huhtikuussa 2020 julkaisemassaan loppuraportissa² henkilön yksilöimistä varten tarvittavien rekisteröintitietojen ja -menettelyiden muutostarpeita. Digitaalisissa palveluissa tapahtuvaa henkilöllisyyden osoittamista, todentamista ja tunnistamista on kuvattu myös useissa sähköistä tunnistamista koskevissa hallituksen esityksissä.

Valtiovarainministeriö pyysi syksyllä 2018 Väestörekisterikeskukselta esiselvitystä sähköisen tunnistamisen vaihtoehdoista, jotka vastaisivat nykymalliin liittyviin ongelmakohtiin suhteessa digitaalisen identiteetin tulevaisuuden oletettuihin käyttötapoihin. Selvityksen tavoitteena oli löytää yksi tai useampi vaihtoehtoinen sähköisen tunnistamisen ja digitaalisen identiteetin hallinnan malli, joka olisi

- laajasti koko väestön saatavilla,
- syrjimättömästi ja esteettömästi kansalaisten käytettävissä,
- helppokäyttöinen, käyttäjälähtöinen ja hyödynnettävissä myös mobiiliasioinnissa sekä
- soveltuvin osin käytettävissä myös ulkomaalaisten tunnistamiseen.

Selvitystyötä arvioi valtiovarainministeriön asettama ohjausryhmä, joka ei ollut päätelmissään yksimielinen. Eriävän mielipiteen jättivät liikenne- ja

¹Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. (Sisäasiainministeriön julkaisu 32/2010) https://api.hankeikkuna.fi/asiakirjat/638e97d1-bb6f-49c4-9cda-238118560a7c/4db67488-da3b-42b0-932b-583cd6fe98ba/JULKAISU_20110126101755.pdf

²HETU-uudistuksen loppuraportti (Valtiovarainministeriön julkaisu – 2020:20): <http://julkaisut.valtioneuvosto.fi/handle/10024/162162>

viestintäministeriö, Kilpailu- ja kuluttajavirasto ja Liikenne- ja viestintävirasto Traficom.

Hanketta edeltävän virkamiesvalmistelun pohjalta on pidetty tarpeellisena, että hankkeen aikana kehitetään toimintamalli ja tuotetaan tarvittavat ratkaisut, joiden avulla valtion takaama digitaalinen henkilöllisyys voidaan tarjota digitaalisena henkilöllisyystodistuksena ns. mobiilihenkilökorttina yksilön käyttöön erilaisissa asiointitilanteissa. Lisäksi hankkeen tavoitteena on laajentaa yhteistyössä henkilötunnuksen uudistamisen hankkeen sekä ulkomaalaislainsäädännön ja lupamenettelyjen kehittämishankkeen kanssa ydinidentiteetin kohderyhmää niistä henkilöistä, jotka tällä hetkellä rekisteröidään väestötietojärjestelmään. Toimintamalli edellyttää poliisin toteuttaman henkilön rekisteröintiprosessin sekä valtion identiteetin hallinnan kehittämistä tukemaan digitaalisen henkilöllisyyden muodostumista ja elinkaarta. Tätä yleistä tehtävänasettelua tarkennetaan hankkeessa tehtävien selvitysten mukaisesti.

2. Digitaalisen henkilöllisyyden hanke ja sen tavoitteet

Hankkeen asettamispäätöksen mukaisesti digitaalisen henkilöllisyyden hankkeen tavoitteena on:

1. tuottaa yhdenvertaiset edellytykset ja mahdollisuudet jokaiselle hyödyntää digitaalista henkilöllisyyttä yhteiskunnan palveluissa ja luoda mahdollisuuksia laajentaa viranomaisen vahvistamien henkilötietojen joukkoa, joka asiointissa voidaan välittää toiselle osapuolelle,
2. varmistaa edellytykset yksilökeskeisesti ihmiseen itseensä liittyvien henkilötietojen jakamisen (Self Sovereign Identity) syntymiselle ja kehitykselle tulevaisuudessa siten, että digitaalisen henkilöllisyyden ratkaisujen perustana voisi toimia valtion takaama ydinidentiteetti,
3. mahdollistaa jokaiselle tarvitsevalle tunnistautuminen julkishallinnon palveluihin sähköisesti myös työtehtävien hoitamista varten,
4. varmistaa julkisen hallinnon vahvan sähköisen tunnistamisen kustannusten hallittavuus ja ennakoitavuus sekä
5. tuottaa edellytykset ulkomaalaisen henkilön rekisteröinnille ja sähköiselle tunnistautumiselle Suomeen ja mahdollistaa Suomesta rajat ylittävä sähköinen tunnistaminen Euroopan parlamentin ja neuvoston sähköisestä tunnistamisesta

ja sähköisiin transaktioihin liittyvistä luottamuspalveluista annetun asetuksen (EU) N:o 910/2014 mukaisesti huomioiden Euroopan Unionin regulaatioon kohdistuvat muutokset.

Hanke koostuu kahdesta työpaketista. Näihin kokonaisuuksiin liittyviä tehtäviä toteutetaan soveltuvien osin rinnakkain.

Hankkeen 1. työpaketissa:

- selvitetään mobiilihenkilökortin edellytykset ja toimintamallit henkilöllisyyden osoittamiseen fyysisen asioinnin lisäksi myös digitaalisessa toimintaympäristössä,
- tuotetaan valtiovarainministeriön, liikenne- ja viestintäministeriön, kilpailu- ja kuluttajaviraston sekä liikenne- ja viestintäviraston yhteistyönä selvitys tunnistus- ja identiteettipalveluiden nykytilasta ja tarpeista,
- laaditaan nykytilaa ja tulevaisuutta kartoittavien selvityksen sekä oikeudellisen arvion pohjalta tarkennettu ehdotus hankkeessa tavoiteltavan ratkaisun ja toimintamallin päälinjoista sekä
- laaditaan alustava arvio hankkeen edellyttämistä lainsäädäntömuutoksista.

Hankkeen työpaketin 1 selvitysten tulokset sekä linjaukset on koottu tähän arviomuistioon. Lausuntokierroksen perusteella tarkennetaan työpaketin 2 tehtäviä ja toteutussuunnitelmaa.

Hankkeen 2. työpaketissa:

- kehitetään toimintamallit julkisen vallan tehtäviksi digitaalisen henkilöllisyyden mobiilihenkilökortin luomisessa, hallinnoimisessa ja hyödyntämisessä,
- toteutetaan sellaiset muutokset jotka ovat tarpeen digitaalisen henkilöllisyyden kohderyhmän laajentamiseksi,
- toteutetaan digitaalisen henkilöllisyyden ja mahdollisen digitaalisen todistuksen (kredentiaalin) luomiseksi tarvittavat järjestelmäratkaisut,
- varmistetaan digitaalisen henkilöllisyyden ja digitaalisen todistuksen kehityksessä yksityisen sektorin mahdollisuus tuottaa ja kehittää valtion ydinidentiteettiä perustuvia digitaalisia välineitä ja palveluita,
- toteutetaan valtion takaaman digitaalisen henkilöllisyyden osoittamisen ratkaisu yhdenvertaisesti kaikille henkilöryhmille älypuhelinsovelluksena sekä vaihtoehtoisena välineenä sähköiseen asiointiin niille, jotka eivät kykene älypuhelin käyttöön,

- yhteistyössä sisäministeriön ja poliisihallituksen kanssa kehitetään henkilökortin myöntämisen ja hyödyntämisen toimintatapoja tukemaan digitaalisen henkilöllisyyden luomista ja osoittamista sekä tuotetaan fyysiselle henkilökortille rinnakkainen mobiilihenkilökortti,
- varaudutaan mobiilihenkilökortin kehityksessä edelleen siihen, että sovellukseen voidaan viedä muitakin valtionhallinnossa suoraan henkilölle myönnettäviä lupia ja tietoja sekä
- valmistellaan kehitettävien ratkaisujen ja toimintamallien mahdollisesti edellyttämät lainsäädäntömuutokset hallituksen esityksen muotoon.

Hanke toteutetaan 8.10.2020 - 30.6.2023 välisenä aikana.

II OSA: DIGITAALISEN HENKILÖLLISYYDEN NYKYTILA JA TULEVAISUUS

3. Nykytilan kuvaus

Nykytilassa henkilöllisyyden osoittamisen tavat ja menetelmät vaihtelevat asiointiyhteydestä riippuen. Henkilöllisyyden voi osoittaa käyntiasioinnissa poliisiin (tai Suomen edustuston) myöntämällä passilla tai henkilökortilla. Suomen kansalaisista noin 4,2 miljoonalla (noin 75% kansalaisista) on voimassa oleva passi tai henkilökortti. Joissakin arjen käyntiasiointitilanteissa myös ajokortti kelpaa osoittamaan henkilöllisyyden, apteekissa riittää usein pelkkä Kela-kortti, jolla osoitetaan tarvittavat sairausvakuutustiedot ja esimerkiksi kirjastossa kirjastokortti.

Vuoden 2019 alusta tuli voimaan lakimuutos, jonka seurauksena ajokortti ei käy enää henkilöllisyystodistuksena vahvaa sähköistä tunnistamisvälinettä (pankkitunnukset, mobiilivarmenne, kansalaisvarmenne) haettaessa eikä välttämättä esimerkiksi pankissa asioita hoitaessa. Ajokortti ei myöskään sovellu henkilöllisyyden osoittamiseen uutta henkilökorttia tai passia noudettaessa. Terveystieteiden ja useiden valtion virastojen työntekijöiden ammatti- ja virkakorttien saaminen edellyttää työntekijän tunnistamista passista tai henkilökortista.

Käytännössä ajokortti on hyväksytty henkilöllisyyden osoittamiseen monissa kaupoissa ja ravintoloissa sekä muissa kuluttajapalveluissa. Ajokorttia on käytetty henkilöllisyyden osoittamiseen esimerkiksi paketteja noudettaessa, iän tarkistamiseksi erilaisia ikärajoitettuja tuotteita ostettaessa, lääkärikäynnille ilmoittauduttaessa, kanta-asiakaskorttina siihen sisältyvän viivakoodin perusteella sekä ajo-oikeuden osoittamiseen esimerkiksi autoa vuokrattaessa tai

yhteiskäyttöautoa käyttöönotettaessa. Ajokortista voidaan käytännössä todeta, että henkilölle on ajokortin myöntöhetkellä myönnetty ajo-oikeus tiettyihin ajoneuvoluokkiin ja sen myöntämisprosessissa henkilön henkilöllisyys on tarkastettu voimassaolevasta passista tai henkilökortista. Erilaisia oikeuksia voidaan osoittaa muilla tavoilla, esimerkiksi kirjastokortilla lainausoikeus, kalastusluvalla kalastusoikeus jne. Näissä tilanteissa ei varsinaisesti osoiteta henkilöllisyyttä, ellei sitä erikseen asiointiyhteydessä pyydetä. Henkilöllisyys on voitu todentaa esimerkiksi lupaa myönnettäessä tai lupa on myönnetty hakijan antamien tietojen perusteella.

Henkilöllisyyden osoittaminen sähköisessä asiointissa voidaan tehdä joko ns. virallisilla henkilöllisyyden osoittavilla menetelmillä (vahva sähköinen tunnistaminen) tai muilla tavoilla (esimerkiksi Google- tai Facebook-tunnistus, käyttäjätunnus ja salasana, sähköpostivarmistus tms.), jotka mielletään yleisesti riittävän luotettaviksi, mutta joissa ei välttämättä ole varmistettu käyttäjän henkilöllisyyttä luotettavasti virallisia menetelmiä hyödyntäen.

3.1. Henkilöllisyyttä osoittavat asiakirjat

3.1.1. Henkilökortti

Henkilökortilla tarkoitetaan Suomen kansalaiselle myönnettävää henkilökorttia, ulkomaalaisen henkilökorttia sekä alaikäisen henkilökorttia, joista säädetään henkilökorttilaissa (25.8.2016/663).

Henkilökorttia haetaan poliisilta. Hakemus voidaan panna vireille sähköisesti. Hakijan tulee saapua henkilökohtaisesti viranomaisen luokse hakemuksen täydentämistä ja tunnistamista varten.

Ulkomailla oleskeleva Suomen kansalainen voi hakea henkilökorttia Suomen suurlähetystöltä, lähetetyn virkamiehen johtamalta konsulaatilta ja sellaiselta muulta Suomen edustustolta, jossa myönnetään passeja ja jossa palvelevan nimetyn Suomen kansalaisen ulkoasiainministeriö on oikeuttanut myöntämään henkilökortteja (Suomen edustusto). Hakijan on oltava henkilökohtaisesti läsnä haettaessa henkilökorttia Suomen edustustolta eikä hakemusta voida panna vireille sähköisesti. Alaikäisen henkilökorttia ja väliaikaista henkilökorttia ei voida hakea Suomen edustustolta.

Henkilökortin kevennetty hakumenettely

Hakijan ei tarvitse saapua henkilökohtaisesti viranomaisen luokse henkilökorttia sähköisesti haettaessa, jos:

1) hakijalle on henkilökorttihakemusta edeltävän kuuden vuoden aikana myönnetty Suomen kansalaisen henkilökortti tai passi, jota haettaessa hakija on henkilökohtaisesti asioinut viranomaisen luona;

2) hakija on 1 kohdassa tarkoitettua asiakirjaa myönnettäessä ollut yli 12-vuotias; ja

3) hakijalta on henkilökorttihakemusta edeltävän kuuden vuoden aikana otettu nimikirjoitusnäyte henkilökorttia tai passia varten eikä hakijan suku- tai etunimi ole tämän jälkeen muuttunut.

Hakijan ei tarvitse saapua henkilökohtaisesti viranomaisen luokse ulkomaalaisen henkilökorttia sähköisesti haettaessa, jos:

1) hakijalle on henkilökorttihakemusta edeltävän kuuden vuoden aikana myönnetty ulkomaalaisen henkilökortti, jota haettaessa hakija on henkilökohtaisesti asioinut viranomaisen luona;

2) hakija on 1 kohdassa tarkoitettua asiakirjaa myönnettäessä ollut yli 12-vuotias; ja

3) hakijalta on henkilökorttihakemusta edeltävän kuuden vuoden aikana otettu nimikirjoitusnäyte ulkomaalaisen henkilökorttia varten eikä hakijan suku- tai etunimi ole tämän jälkeen muuttunut.

Henkilökortin kevennetyssä hakumenettelyssä hakijan ei edellä mainittujen edellytysten täytyessä tarvitse tulla poliisiasemalle, vaan hän voi tehdä hakemuksen kokonaan poliisin sähköisellä asiointialustalla, kunhan liittää hakemukseensa uuden passikuvansa. Hakijan tunnistaminen poliisin asiointipalveluun perustuu vahvaan sähköiseen tunnistamiseen. Tunnistusvälineinä käytetään verkkopankkitunnuksia, henkilökortin kansalaisvarmennetta ja mobiilivarmenteita. Lisäksi toimitettua kasvokuvaa verrataan hakijan aiempiin kasvokuviin sekä koneellisesti että virkamiehen toimesta. Henkilökohtainen läsnäolo ensimmäistä kertaa henkilökorttia haettaessa, vahva sähköinen tunnistaminen ja kasvokuvien vertaaminen yhdessä luovat pohjan, jonka nojalla biometristen tunnisteiden yhtäpitävyys hakijan henkilöllisyyden kanssa voidaan todeta.

Hakijan tulee kuitenkin saapua henkilökohtaisesti viranomaisen luokse, jos se on hakijan tunnistamiseksi, uuden nimikirjoitusnäytteen antamiseksi tai muusta erityisestä syystä tarpeen.

Kevennettyä hakumenettelyä ei sovelleta haettaessa henkilökorttia Suomen edustustolta eikä haettaessa alaikäisen henkilökorttia tai väliaikaista henkilökorttia.

Henkilökortin myöntämisen edellytyksenä on, että hakija on tunnistettu ja hänen henkilöllisyytensä on luotettavasti todennettu. Hakijan on henkilökorttia hakiessaan esitettävä voimassa oleva henkilöllisyyttä osoittava asiakirja. Jos hakijalla ei ole esittää tällaista asiakirjaa, henkilökortin myöntävä viranomainen tunnistaa hakijan ja todentaa tämän henkilöllisyyden.

Hakemukseen on liitettävä hakijan kasvokuva, josta hakija on hyvin tunnistettavissa.

Jos ulkomaalaisen henkilökorttia hakevalla ei ole esittää voimassa olevaa henkilöllisyyttä osoittavaa asiakirjaa, hänen tulee esittää voimassa oleva oleskelulupakortti tai oleskelukortti. Hakemuksen vastaanottava viranomainen saa tällöin ottaa hakijalta sormenjäljet ja verrata niitä oleskelulupakortin tai oleskelukortin tekniseen osaan talletettuihin sormenjälkiin hakijan henkilöllisyyden todentamiseksi. Vertaamista varten otettuja sormenjälkitietoja voidaan käyttää vain vertaamisen ajan, ja ne on hävitettävä välittömästi sen jälkeen.

Alaikäiselle hakijalle voidaan myöntää henkilökortti, jos huoltajat siihen suostuvat. Jos joltakin huoltajalta ei matkan, sairauden tai muun vastaavan syyn vuoksi voida saada suostumusta ja jos ratkaisun viivästyminen aiheutuisi kohtuutonta haittaa, henkilökortti voidaan myöntää ilman tämän suostumusta. Alaikäiselle hakijalle voidaan ilman huoltajien suostumusta myöntää alaikäisen henkilökortti.

Poliisin ja Suomen edustuston myöntämät henkilökortit ovat sirullisia, lukuun ottamatta alaikäisille ilman huoltajan suostumusta myönnettävää ja väliaikaista korttia. Sirulliseen henkilökorttiin sisältyy väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 61 §:n 3 momentissa tarkoitettu Digi- ja väestötietoviraston myöntämä kansalaisvarmenne. (29.11.2019/1167). Varmenne mahdollistaa henkilön luotettavan tunnistamisen sähköisessä asiointissa.

3.1.2. Passi

Passilla tarkoitetaan Suomen kansalaiselle myönnettävää passia, diplomaattipassia ja virkapassia, joista säädetään passilaissa (21.7.2006/671).

Passia haetaan poliisilta. Hakemus voidaan panna vireille sähköisesti. Hakijan tulee saapua henkilökohtaisesti viranomaisen luokse hakemuksen täydentämistä varten.

Ulkomailla oleskeleva Suomen kansalainen voi hakea passia Suomen suurlähetystöltä tai lähetetyn virkamiehen johtamalta konsulaatilta taikka sellaiselta muulta Suomen edustustolta, jossa palvelevan nimetyn Suomen kansalaisen ulkoministeriö on oikeuttanut myöntämään passeja. Hakijan on oltava henkilökohtaisesti läsnä passia haettaessa. Hakemusta ei voida panna vireille sähköisesti.

Diplomaattipassia ja virkapassia haetaan ulkoministeriöltä. Hakemuksen voi erityisistä syistä jättää myös poliisille tai Suomen edustustoon. Hakijan on oltava henkilökohtaisesti läsnä diplomaattipassia ja virkapassia haettaessa. Hakemusta ei voida panna vireille sähköisesti.

Hakemukseen on liitettävä hakijan tuore kasvokuva, josta hakija on hyvin tunnistettavissa. Hakijan on esitettävä tunnistamisasiakirjana voimassa oleva henkilöllisyyttä osoittava asiakirja. Jos hakijalla ei ole esittää tunnistamisasiakirjaa, passin myöntävä viranomainen suorittaa tunnistamisen.

Sähköinen asiointi edellyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) tarkoitettua tunnistusvälinettä.

Passin kevennetty hakumenettely

Jos hakija hakee uutta passia poliisilta sähköisesti kuuden vuoden kuluessa aiemman passin myöntämisestä ja aiempaa passia varten on otettu sormenjäljet ja annettu nimikirjoitusnäyte, passia haettaessa ei edellytetä hakijan henkilökohtaista läsnäoloa. Menettelyä kutsutaan passin kevennetyksi hakumenettelyksi. Passin kevennetyssä hakumenettelyssä hakijan henkilöllisyyden todentamiseen sovelletaan samoja käytäntöjä kuin henkilökortin kevennetyssä hakumenettelyssä: henkilökohtainen läsnäolo ensimmäistä kertaa passia haettaessa, vahva sähköinen tunnistaminen ja kasvokuvien vertaaminen yhdessä luovat pohjan, jonka nojalla biometrinen tunnistaminen yhtäpitävyys hakijan henkilöllisyyden kanssa voidaan todeta.

Hakijan tulee kuitenkin saapua henkilökohtaisesti viranomaisen luokse uutta passia sähköisesti haettaessa, jos se on hakijan tunnistamiseksi, uusien sormenjälkien ottamiseksi, uuden nimikirjoitusnäytteen antamiseksi tai muusta erityisestä syystä tarpeen.

Kevennettyä hakumenettelyä ei sovelleta haettaessa uutta passia Suomen suurlähetystöltä tai lähetetyn virkamiehen johtamalta konsulaatilta taikka sellaiselta muulta Suomen edustustolta, jossa palvelevan nimetyn Suomen kansalaisen ulkoasiainministeriö on oikeuttanut myöntämään passeja, eikä haettaessa uutta diplomaattipassia, virkapassia, merimiespassia tai ulkomaalaislain (301/2004) 8 luvussa tarkoitettua ulkomaalaiselle myönnettävää matkustusasiakirjaa.

Alaikäisen passihakemukseen tulee liittää hänen huoltajiensa suostumus. Huoltaja voi antaa suostumuksensa passin kelpoisuusalueen tai voimassaoloajan osalta rajoitettuna. Jos alaikäinen on otettu Suomessa sosiaalilautakunnan huostaan, antaa suostumuksen sosiaalihuoltolain (710/1982) 6 §:n 1 momentissa tarkoitettu toimielin.

Poliisihallituksella on oikeus antaa passin myöntäville viranomaisille määräyksiä tunnistamisen suorittamisesta.

Passin myöntävä viranomainen tarkastaa hakijan henkilötiedot väestötietojärjestelmästä, ja tiedot merkitään passiin väestötietojärjestelmän tietojen mukaisesti.

Passissa on jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista annetussa neuvoston asetuksessa (EY) N:o 2252/2004 (EU:n passiasetus) tarkoitettu tekninen osa. Tekniseen osaan talletetaan passinhaltijan kasvokuva sekä sormenjäljet tarvittavine lisätietoineen siten kuin EU:n passiasetuksessa säädetään.

Poliisihallitus huolehtii siitä, että passin tekniseen osaan talletetut tiedot suojataan EU:n passiasetuksen ja sen soveltamiseksi annettujen säännösten mukaisesti tehokkaasti tunkeutumista, luvaton lukemista, muuttamista, käyttöä ja muuta luvaton käsittelyä vastaan.

Tekniseen osaan talletettujen tietojen aitouden ja eheyden varmistamiseen liittyvät sekä sormenjälkien lukemisessa tarvittavat varmenteet luo Digi- ja väestötietovirasto.

Poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista säädetään tarkemmin valtioneuvoston asetuksella 1167/2016.

3.2. Vahva sähköinen tunnistaminen

3.2.1. Sähköinen tunnistaminen

Vahvan sähköisen tunnistamisen avulla kuluttajat voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa ja sähköisten asiointipalveluiden tarjoajat voivat tunnistaa asiakkaansa. Tunnistuspalveluiden vaatimuksista säädetään laissa. Suomeen sijoittuneiden palvelun tarjoajien on ennen toimintansa aloittamista tehtävä kirjallinen ilmoitus Liikenne- ja viestintävirastolle (Traficom). Viraston Kyberturvallisuuskeskus valvoo vaatimusten noudattamista, antaa lakia tarkentavia määräyksiä ja ylläpitää julkista rekisteriä vaatimukset täyttävistä tunnistuspalvelun tarjoajista.

3.2.2. Vahvat sähköiset tunnistuspalvelut

Suomessa on kahdenlaisia vahvan sähköisen tunnistamisen palveluntarjoajia

- Tunnistusvälineen tarjoaja tarjoaa tunnistusvälineitä käyttäjille
- Tunnistusvälityspalvelu myy tunnistuspalvelua asiointipalveluille
- Sama palveluntarjoaja voi halutessaan toimia sekä välineen että välityspalvelun tarjoajana.

Vahva sähköinen tunnistuspalvelu voi olla varmuustasoltaan joko korotettu tai korkea.

Vahvoja sähköisiä tunnistuspalveluita ovat

- pankkien verkkopankkitunnukset
- teleyritysten mobiilivarmenteet
- Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla ja eräät muut tunnistusvarmenteet
- erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut

3.2.3. Tunnistusmenetelmät

Vahva sähköinen tunnistus voi perustua teknisesti eri menetelmiin. Yhteistä menetelmille on se, että niissä on käytettävä vähintään kahta seuraavista todentamistekijöistä ja dynaamista todentamismekanismia:

- tiedossa oloon perustuva todentamistekijä, jonka henkilön on osoitettava olevan tiedossaan (esim. salasana, PIN-koodi)
- hallussapitoon perustuva todentamistekijä, jonka henkilön on osoitettava olevan hallussaan (esim. tunnuslukulaite, mobiilisovellus, tunnuslukulista)
- luontainen todentamistekijä, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen (esim. sormenjälki, iiris)

Dynaamisella todentamisella tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa.

3.2.4. Varmenne

Osa vahvan sähköisen tunnistamisen menetelmistä perustuu varmenteisiin. Yleisesti varmenteita tarvitaan tietoverkkojen kautta tapahtuvassa tunnistamisessa, salauksessa ja sähköisen allekirjoituksen tekemisessä. Varmenne on luotettavan organisaation sähköisesti allekirjoittama todistus, joka todentaa varmenteen omistajan henkilöllisyyden. Varmenne sisältää julkisen avaimen, jolla varmenteen omistajan voi tunnistaa. Julkisen avaimen lisäksi varmenne sisältää muita tietoja, kuten

- henkilön tai organisaation nimen,
- varmenteen myöntämispäivän,
- viimeisen voimassaolopäivän tai
- yksilöllisen sarjanumeron.

Tunnistamisessa käytettävän varmenteen tietosisällöstä on säädetty tunnistus- ja luottamuspalvelulaissa.

3.2.5. Luottamusverkosto

Vahvan sähköisen tunnistuspalvelun tarjoajat, jotka ovat tehneet tunnistus- ja luottamuspalvelulain (617/2009) mukaisen ilmoituksen ja jotka täyttävät lain vaatimukset, muodostavat suoraan lain nojalla 1.5.2017 alkaen sähköisen tunnistamisen luottamusverkoston.

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.

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.

Luottamusverkoston toimintamallin mukaan tunnistusvälineen tarjoajalla on velvoite antaa tunnistusväline välitettäväksi kaikille rekisteröidyille tunnistusvälityspalveluille laissa säädetyllä hinnalla. Toisin sanoen tunnistusvälineen tarjoajan tulee mahdollistaa se, että tunnistusvälityspalvelu tarjoaa luottavalle osapuolelle eli sähköisen asiointipalvelun tarjoajalle mahdollisuuden tunnistaa asiakkaansa vahvalla sähköisellä tunnistusvälineellä. Välitys perustuu kahdenvälisiin sopimuksiin.

4. Nykytilan arvio

Sähköisen tunnistamisen markkinan ja käytön nykyistä tilaa kuluttajien ja yritysten näkökulmasta kartoitettiin toteuttamalla valtiovarainministeriön toimeksiannosta kolme erillistä markkinaselvitystä. Näistä kaksi oli suunnattu kuluttajille ja yksi sähköistä tunnistamista hyödyntäville yrityksille. Edellä mainittujen selvitysten lisäksi Kilpailu- ja kuluttajavirasto sekä Liikenne- ja viestintävirasto ovat tehneet omat selvitykset sähköisen tunnistamisen markkinasta, mutta näiden selvitysten tuloksia ei ollut käytettävissä tämän muistion valmistelussa. Tästä syystä nykytilan arvio on puutteellinen ja yksipuolinen. Nykytilan arvioissa ei ole kattavasti kuvattu eikä arvioitu sähköisen tunnistamisen markkinaa, sen kilpailutilannetta, tunnistuspalveluja tuottavien yritysten tulevaisuuden arvioita tai julkisen sektorin osuutta ostajana vahvan sähköisen tunnistamisen palvelumarkkinasta. Näitä kokonaisuuksia arvioidaan tarkemmin liikenne- ja viestintäviraston sekä Kilpailu- ja kuluttajaviraston selvityksissä.

Yleisen kuluttajatutkimuksen aiheena oli kuluttajien käyttämät vahvan sähköisen tunnistamisen tavat ja välineet ja käyttö. Tiedonkeruu toteutettiin puhelinhaastatteluna ja siihen tehtiin yhteensä 2003 haastattelua. Haastateltavat poimittiin kiintiöidysti väestötietojärjestelmään kirjatusta yli 15-vuotiaista. Kiintiöinnillä varmistettiin väestöedustavuus ja aineisto on painotettu iän, sukupuolen ja suuralueen mukaan väestöä vastaavaksi. Tutkimuksen tiedot kerättiin 30.10.-9.12.2020.

Puhelinhaastatteluna toteutetun kuluttajakyselyn lisäksi toteutettiin Vammaisfoorumin jäsenilleen jakamana avoin verkkokysely, jolla pyrittiin tavoittamaan erityisesti kuluttajia, joilla on mahdollisesti jokin toimintarajoite. Verkkokyselyn kysymykset olivat vastaavat puhelinhaastatteluna suoritettua kuluttajatutkimuksen kanssa. Vammaisfoorumin kautta jaettuun verkkokyselyyn saatiin 96 vastausta. Vastaajien taustoista ei ole muuta tietoa, kuin mitä he ovat kyselyn yhteydessä antaneet eikä vastaajia ole rajattu tai painotettu iän, sukupuolen tai asuinalueen mukaan.

Yritysten käyttämiä vahvan sähköisen tunnistamisen tapoja ja menetelmiä selvitettiin Suomessa toimiville yrityksille tehdyillä puhelinhaastatteluilla. Tiedonkeruun kohteena oli yhteensä 501 eri yritystä. Yritysten yhteystietolähteenä käytetty Bisnoden Selector-palvelua. Tiedonkeruussa käytettiin kiintiöintiä, jotta aineistoon saatiin yrityksiä eri koko luokista ja toimialoilta. Aineistoa ei ole painotettu. Tutkimuksen tieto kerättiin 11.11.-2.12.2020.

Nykytilassa kuluttajalla on käytännössä varsin rajattu valinnanvapaus sähköisen tunnistamisen palvelujen osalta. Tämä johtuu siitä, että sähköinen tunnistaminen on sidottu muuhun asiakkuuteen, kuten pankki- tai mobiilipalveluasiakkuuteen. Tällöin uuden tunnistusvälineen hankinta tarkoittaa myös uuden asiakkuussuhteen perustamista tai voimassaolevan asiakkuuden siirtämistä toiselle palveluntarjoajalle. Lähtökohtaisesti kuluttajan on siis tyydyttävä niihin tunnistusratkaisuihin, mitä hänen käyttämänsä pankki- tai mobiilipalveluntarjoaja tarjoaa hänen käytettäväksi. Kuluttajan mahdollisuudet vaikuttaa siihen, mitä tunnistusratkaisua hän käyttää sähköiseen palveluun tunnistautuessa ovat tosiasiallisesti hyvin rajalliset. Tämän lisäksi pankkipalveluissa, erityisesti verkko-ostoissa tehtävät maksunvahvistukset, edellyttävät pääsääntöisesti maksuvälineen myöntäneen rahoituslaitoksen käyttämää tunnistusmenetelmää. Tästä johtuen kuluttaja voi käyttää oman pankkinsa tunnistusvälinettä pääasiallisena tunnistuspalvelunaan, mutta ei esimerkiksi mobiilivarmennetta, vaan käytännössä hän joutuu käyttämään vähintään maksuvälineen myöntäneen pankin tunnistuspalvelua verkko-ostoja tehdessään.

Sähköisen tunnistamisen palveluja ja niiden yhteentoimivuutta säädellään vahvan sähköisen tunnistamisen lainsäädännön kautta. Julkisen hallinnon sähköisissä palveluissa käytetään paljon vahvaa sähköistä tunnistusta ja käytännössä lähes kaikki julkisen sektorin sähköiset palvelut hyväksyvät kaikki vahvaa sähköistä tunnistamista tarjoavat palveluntarjoajat tunnistusmenetelmäksi. Yksityisen ja kolmannen sektorin palveluissa suurelta

osin sähköisissä palveluissa tarjotaan kuluttajille ainoastaan heikkoa tunnistusta palveluun tunnistautumiseksi. Yksityisen ja kolmannen sektorin sähköisissä palveluissa on kuitenkin viime vuosina otettu entistä laajemmin käyttöön vahva sähköinen tunnistus joko ainoana vaihtoehtona tai rinnakkaisena vaihtoehtona jollekin heikolle tunnistusratkaisulle. Pääasiallinen syy tähän on ollut lainsäädäntömuutokset, jotka vaativat sähköisen palvelun tarjoajaa tekemään tunnistautumisen vahvalla tunnistuksella. Myös viime vuosina esille tulleet tietomurrot ja tietosuojaloukkaukset ovat lisänneet vahvan tunnistuksen käyttöä.

Kuluttajakyselyissä selvitettiin, onko vastaajalla käytössä internet-yhteys ja mitä laitteita hänellä on internetin selaamiseen sekä sähköisten palvelujen käyttöön. Kaikista vastaajista 96%:lla oli käytössä internet-yhteys. Yli 75-vuotiailla vastaajilla internet-yhteys oli 72 %:lla vastaajista, muilla ikäryhmillä internet-yhteys oli 91-100 % vastaajilla. Molemmissa kuluttajakyselyissä tietokone oli yli 91 %:lla vastanneista (vammaisjärjestöjen jäsenille suunnattuun kyselyyn vastanneilla 95%), tabletti 59 %:lla vastanneista (vammaisjärjestöjen jäsenille suunnattuun kyselyyn vastanneilla 68%) ja älypuhelin 93 %:lla vastanneista (vammaisjärjestöjen jäsenille suunnattuun kyselyyn vastanneilla 94%). Puhelinhaastatteluun vastanneiden kuluttajien käytettävissä olevien laitteiden ikäryhmittäin tehtävä tarkastelu osoittaa, että 15-24 –vuotiailla vastaajilla älypuhelin oli 100 %:lla vastaajista, 25-34 –vuotiailla 99 %:lla vastaajista ja vastaavasti 75-80 –vuotiaista vastaajista älypuhelin oli 59 %:lla vastaajista. Huomattavaa on, että ikäluokissa 65-74 –vuotiaista vastaajista 6 % ja 75-80 –vuotiaista vastaajista 17 % eivät omista tietokonetta, tablettia tai älypuhelinlaitea.

Kuluttajilta, joilla on käytössään internet-yhteys, kysyttiin mikä on yleisin laite (oma tai julkisesti käytettävä), jolla yleisimmin selaatte internettiä ja käytätte sähköisiä palveluja kuten verkkopankkia ja julkishallinnon sähköisiä palveluja. Kaikista vastaajista yleisin laite oli puhelin 53 %:lla vastaajista, tietokone 38 %:lla vastaajista ja tabletti 9 %:lla vastaajista. Ikäryhmittäin vastauksia tarkasteltaessa voidaan todeta, että puhelin on yleisin laite internetin selaamiseen ja sähköisten palvelujen käyttöön alle 44-vuotiaille vastaajille. Yli 55-vuotiailla vastaajilla yleisimmin käytetty laite on tietokone.

Kuluttajilla pankkitunnusten levinneisyys ja käyttö ovat hyvin korkealla tasolla: 90% kaikista kuluttajatutkimusten vastaajista käyttää pääasiallisesti verkkopankkitunnuksia vahvaan sähköiseen tunnistamiseen. Pääasiallinen käyttökohde on pankki- tai maksupalvelujen käyttö verkossa. Mobiilivarmennetta käyttäen on edelleen varsin vähäistä: 8% kaikista vastaajista käyttää yleisimmin mobiilivarmennetta sähköisen tunnistamisen menetelmänä.

Kaikista vastaajista pankin myöntämä verkkopankkitunnus on 98 %:lla vastaajista, teleyrityksen (DNA:n, Elisan tai Telian) myöntämä mobiilivarmenne 22 %:lla vastaajista, kansalaisvarmenne 6 %:lla vastaajista ja työnantajan työntekijälle myöntämä organisaatiovarmenne 7 %:lla vastaajista. Kaikista kuluttajakyselyiden vastaajista noin 1 %:lla ei ole mitään edellä mainittua tunnistusvälinettä käytössään.

Kuluttajilta kysyttiin myös, mitä tunnistusvälinettä he käyttävät yleisimmin. Pankin myöntämä verkkopankkitunnusta käyttää yleisimmin 90 % kaikista vastanneista niin puhelinhaastatteluna kuin verkkokyselynä tehdyssä kyselyssä. Teleyrityksen (DNA:n, Elisan tai Telian) myöntämää mobiilivarmennetta käyttää yleisimmin 8 % puhelinhaastatteluun vastanneista ja 14% verkkokyselyyn vastanneista kuluttajista. Kansalaisvarmennetta (poliisin myöntämä henkilökortti ja siinä käyttöön otettu kansalaisvarmenne) käyttää yleisimmin vain yksittäisiä kuluttajia. Organisaatio-varmennetta (työnantajan työntekijälle myöntämä kortti ja siinä käyttöön otettu organisaatiovarmenne) käyttää yleisimmin joitakin kuluttajia, enemmän kuin kansalaisvarmennetta.

Kyselyissä selvitettiin myös, onko kuluttaja ottanut tai onko aikeissa ottaa käyttöön uuden tai uusia tunnistusvälineitä. Suurin osa vastaajista (88%) ei ole ottanut eikä ole aikeissa ottaa uutta tunnistusvälinettä käyttöönsä. Niistä vastaajista, jotka olivat ottaneet uuden tunnistusvälineen käyttöönsä, 35 % kertoi syyksi uuden välineen helppokäyttöisyyden.

Kyselyssä selvitettiin myös, mihin palveluihin kuluttajat sähköisillä tunnistusvälineillä tunnistautuvat yleisimmin. Lähes jokainen (99% vastanneista) vastannut oli käyttänyt sähköistä tunnistautumista hoitaakseen pankkiasioitaan ja 87% vastanneista käytti sähköistä tunnistautumista kaikista yleisimmin verkkopankkiin kirjautumiseen.

Suuri osa vastanneista (87 % vastanneista) oli myös käyttänyt sähköistä tunnistautumista asioidakseen julkisen hallinnon sähköisissä palveluissa. Vastaajista 4 % ilmoitti käyttävänsä sähköistä tunnistautumista eniten julkisen hallinnon sähköisiin palveluihin.

Kyselyyn vastanneista 71 % oli käyttänyt sähköistä tunnistautumista verkkokaupassa verkko-ostoksen hyväksymiseksi ja luottokorttimaksun vahvistamiseksi. Vastanneista 4% kertoi, että verkkokaupassa verkko-ostoksen hyväksymiseksi ja luottokorttimaksun vahvistamiseksi oli heidän yleisin palvelu, jossa käyttävät sähköistä tunnistautumista. Tämän osalta on huomioitava, että kyselyn toteutusaikana syksyllä 2020 ei vielä tarvinnut

käyttää sähköistä tunnistautumista verkkomaksun vahvistamiseen. Toisen maksupalveludirektiivin (PSD2) siirtymäaika päättyi 31.12.2020 ja vahvan tunnistamisen vaatimus koskee 1.1.2021 alkaen kaikkea sähköisesti tapahtuvaa maksamista.

Yksityisten yritysten sähköisiin palveluihin (esim. vakuutusyhtiöiden, terveyspalveluyritysten ja sähköyritysten sähköiset palvelut) sähköistä tunnistautumista oli käyttänyt 56 % vastaajista, kolmannen sektorin toimijoiden esimerkiksi järjestöjen sähköisiin palveluihin (esim. työttömyyskassan ja ammattiliittojen sähköiset palvelut) 23 % vastaajista ja työtehtävien hoitamiseksi 22 % vastaajista. Noin puolet kyselyihin vastanneista kuluttajista oli käyttänyt sähköistä tunnistusvälinettä sähköisen allekirjoituksen tekemiseen.

Kuluttajilta kysyttiin myös mieluisinta sähköisen tunnistamisen tunnistusvälinettä. Älypuhelimeen tai tablettiin asennettu tunnuslukusovellus oli mieluisin 34 %:lle vastaajista. Tunnuslukulista (tunnistautuminen käyttäen paperista tai muovista tunnuslukulistaa) oli mieluisin tunnistusväline 22 %:lle vastaajista. Älypuhelimien tai tabletin sormenjälkitunnistus oli mieluisin 22 %:lle vastaajista. Tunnuslukulaite oli mieluisin tunnistusväline 6 %:lle vastaajista.

Kuluttajakyselyissä selvitettiin myös vastaajien halukkuutta ottaa käyttöön ja käyttää valtion tarjoamaa älypuhelimella ja/tai muistitikulla käytettävää vahvaa sähköistä tunnistusvälinettä. Puhelinhaastatteluun vastanneista 32 % oli kiinnostunut, jos käyttö on ilmaista; 30 %, jos se olisi helppokäyttöinen; 23 %, jos sitä voisi käyttää myös muissa kuin julkishallinnon sähköisissä palveluissa; 9 % jos sitä voisi käyttää työtehtävien hoitamiseen. Vastanneista 49 % ei ollut kiinnostunut valtion tarjoaman tunnistusvälineen käyttöönnotosta.

Kyselytutkimuksen mukaan 88 prosenttia vastanneista käyttäisi vahvaa sähköistä tunnistusvälinettä sähköiseen palveluun tunnistautuessa, jos heillä olisi mahdollisuus valita tunnistusmenetelmä. Ennen kaikkea vastaajat perustelivat vahvan sähköisen tunnistusvälineen käyttämistä sillä, että se on turvallinen käyttää (60 %), sitä on helpompi käyttää (29 %) ja heidän ei tarvitse muistaa kuin yksi käyttäjätunnus ja salasana tunnistautuessaan eri palveluihin (19 %).

Vastanneista 7 prosenttia taas käyttäisi muuta kuin vahvaa sähköistä tunnistusvälinettä eli niin sanottua heikkoa tunnistusvälinettä ja 4 prosenttia ei osannut sanoa. Vastanneista heikkoa tunnistusvälinettä mieluummin käyttävät perustelivat valintaansa ennen kaikkea sillä, että heikkoa tunnistusvälinettä on helpompi (52 %) ja nopeampi (16 %) käyttää ja että se on turvallisempi käyttää

(16 %). Perusteina olivat myös se, että tarvitsee muistaa vain yksi käyttäjätunnus ja salasana (9 %) ja se että välinettä voi käyttää ilman tunnuslukulistaa, -sovellusta tai laitetta tai matkapuhelinta (8%). Vastausten osalta on syytä huomioida, että vastaajajoukko, joka käyttäisi mieluummin heikkoa tunnistusvälinettä, oli pieni, jolloin vastausten perusteella ei voida tehdä kaikkia kansalaisia koskevia johtopäätöksiä perusteita heikon tunnistusvälineen käyttämiseksi. Vastauksista voidaan kuitenkin saada jonkinlaista näkemystä perusteista, miksi osa kansalaisista valitsisi mieluiten heikon tunnistusvälineen.

Vastanneista 95 prosenttia vahvan sähköisen tunnistusvälineen omistajista pitivät sen käyttämistä vähintäänkin helppona, vaikka osa (15 %) olikin kokenut joitakin haasteita sen käyttämisessä. 5 prosenttia piti vahvan sähköisen tunnistusvälineen käyttämistä haastavana. Kysyttäessä, mitä ongelmia vastaajat kokivat vahvan sähköisen tunnistusvälineen käyttämisessä, korostuivat vastauksessa lähinnä muut kuin itse tunnistusvälineeseen liittyvät ongelmat, kuten palvelun käyttöön liittyvät yhteysongelmat ja -häiriöt (12 %) sekä yleinen tietoteknisten laitteiden hankala käytettävyys (8%). Jossain määrin koetut ongelmat liittyivät myös itse tunnistusvälineen käyttämiseen ja häiriöihin niissä sekä annettuihin ohjeisiin välineen käyttämiseksi. Kyselytutkimuksen perusteella suurin osa kansalaisista selkeästi käyttäisivät vahvaa sähköistä tunnistusvälinettä tunnistautumisessa, jos vain palveluntarjoaja mahdollistaisi sen sähköisessä palvelussaan. Kansalaisten näkökulmasta vahvalle edulliselle ja helppokäyttöiselle sähköiselle tunnistukselle näyttäisi olevan jonkinlainen tarve. Nykyinen tarjonta tai käyttömahdollisuudet eivät kuitenkaan täysin vastaa tarvetta, jos 52% vastaajista pitää heikkoja tunnistusvälineitä helpompina käyttää.

Heikkoja tunnistusvälineitä käytetään ennen kaikkea siitä syystä, ettei vahvaa sähköistä tunnistusvälinettä ole mahdollista käyttää sähköisessä palvelussa. Olennaiseksi kysymykseksi nouseekin, onko palveluissa mahdollista käyttää vahvaa sähköistä tunnistamista. Yrityksille tehdyn kyselyn vastausten perusteella yrityksen tarjoavat omien palvelujensa kirjautumismenetelmänä pääsääntöisesti muuta kuin vahvaa sähköistä tunnistamista. Kyselyn vastausten perusteella noin 60% asiakkaiden ensirekisteröinnistä varmistetaan muulla kuin vahvalla sähköisellä tunnistamisella.

Vahvaa sähköistä tunnistamista käytettäisiin todennäköisesti enemmän, jos sitä olisi mahdollista käyttää useammassa asiointipalvelussa. Yhtenä syynä siihen, ettei vahva sähköinen tunnistus ole käytettävissä useammassa asiointipalvelussa voidaan oletetusti pitää vahvan sähköisen tunnistamisen kustannusta asiointipalvelun tuottajalle. Kuluttajakyselyjen perusteella voidaan todeta, että

mitä vanhemmasta ikäluokasta on kyse, sitä suurempi vastustus kuluttajalla on muuttaa nykyisiä toimintatapoja tai käyttämiään tunnistusmenetelmiä.

Yleisesti ottaen kuluttaja- ja yrityskyselyjen tulokset heijastavat vahvan sähköisen tunnistamisen markkinoiden ja käytön nykyistä tilaa, eikä tuloksista voi vetää täysin aukottomia johtopäätöksiä kuluttajien tai yritysten näkökulmasta sähköiseen tunnistamiseen kohdistuvista tulevaisuuden kehittämistarpeista. Tehtyjen selvitysten perusteella ei voi arvioida suoraan kuluttajien intoa ottaa käyttöön valtion uutta menetelmää osoittaa henkilöllisyys digitaalisen palvelun avulla. Tällaisesta palvelusta tai toimintamallista ei ole kenelläkään kokemusta ja voidaan perustellusti arvioida. Lisäksi käyttötarvearviota on vaikea tehdä, koska uudenlaisen menetelmän hyödyntämismahdollisuudet todennäköisesti poikkeavat laajasti nykyisestä sähköisen tunnistamisen käyttölaajuudesta.

Erityisesti erilaiset mobiilisovelluspohjaiset tunnistusratkaisut ovat vähentäneet itse tunnistusvälineisiin aiemmin liittyneitä esteettömyysaasteita, mutta edelleen kuluttajat kohtaavat edelleen jonkin verran vaikeuksia esimerkiksi ruudunlukuohjelmalla tunnistussovelluksia käytettäessä. Suurimpia esteitä sähköisen tunnistamisen käytölle digitaalisissa palveluissa näyttäisi olevan varsinaisten asiointipalvelujen vaikeakäyttöisyys. Toisaalta osa käyttäjistä on toisaalta edelleen sähköisen tunnistamisen käyttömahdollisuuksien ulkopuolella. Nämä voivat johtua esimerkiksi ulkomaalaisen osalta puuttuvasta henkilötunnuksesta tai toimintarajoitteisella käyttäjällä avustajan käytöstä, joissakin tapauksissa myös tunnistusmenetelmään liittyvästä käyttöesteestä. Yksittäistapauksissa tunnistusvälineisiin ja –palveluihin liittyviä saatavuus- ja käyttöesteitä on ratkottu yhdenvertaisuuslain (1325/2014) 15 §:ssä säädetyn kohtuullisten mukautusten perusteella. Ulkomaalaisten henkilöiden rekisteröintiin ja henkilötunnuksen saamiseen liittyviin haasteisiin paneudutaan henkilötunnuksen uudistamista pohtivan työryhmän työssä. Digitaalisen henkilöllisyyden hankkeessa tarkastellaan ulkomaalaisten henkilöiden mahdollisuuksia saada käyttöönsä digitaalinen identiteetti ja hyödyntää sitä asiointissa, mutta tämä on kytköksissä henkilötunnuksen uudistushankkeessa mahdollisesti valmisteltaviin muutoksiin henkilöiden kirjaamisesta väestötietojärjestelmään. Hankkeessa on tarkoitus edistää yleisesti myös toimintarajoitteisten kuluttajien digitaalisen identiteetin saanti- ja käyttömahdollisuuksia.

Nykytilan osalta ei myöskään arvioitu nykyisen toiminnan kustannusrakennetta sähköisen tunnistuspalvelujen tuottajien tai sähköisten asiointipalvelujen tarjoajien näkökulmasta. Tällä hetkellä Liikenne- ja viestintävirasto perii tunnistuspalvelun rekisteröinnistä 5000 euron rekisteröimismaksun. Lisäksi

tunnistuspalvelun tarjoajan tai yhteenliittymän on suoritettava Liikenne- ja viestintävirastolle vuosittain yhteensä 14 000 euron valvontamaksu kaikkien tarjoamiensa tunnistuspalveluiden valvonnasta. Aloittavan tunnistuspalvelun rekisteröinti- ja valvontamaksut ovat siis ensimmäisenä toimintavuotena 19 000 euroa. Lain vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009) 12 c §:ssä säädetään yhden tunnistustapahtuman enimmäishinta 3 sentiksi, joten pelkkien viranomaismaksujen kattaminen vaatii tunnistuspalvelun tarjoajalta ensimmäisenä vuotena 633 333 laskutettavaa tunnistustapahtumaa. Seuraavina vuosina valvontamaksun kattaminen vaatii 466 666 laskutettavaa tunnistustapahtumaa. Tällä hetkellä tunnistuspalvelurekisterissä on 16 tunnistuspalvelu- tai tunnistuksenvälityspalvelua. Näiden vuosittaisten valvontamaksujen kattaminen vaatii noin 7 466 666 laskutettavaa tunnistustapahtumaa. Tämä vastaa noin koko julkisen sektorin yhden kuukauden laskutettavien tunnistustapahtumaostojen määrää.

Julkisen hallinnon sähköisiin asiointipalveluihin tehtävien tunnistustapahtuminen ja niiden välittämiseen tarvittavien palvelujen vuosikustannukset ovat noin 7,4 miljoonaa euroa vuodessa sekä 8,3 henkilötyövuotta. Karkeasti arvioiden julkisen sektorin markkinoilta ostettavan vahvan sähköisen tunnistamisen kustannukset ovat vuositasolla noin 8 miljoonaa euroa.

Julkisen hallinnon sähköisiin palveluihin tarvittava käyttäjän identifiointikustannus vuositasolla on jo ylittänyt valtion oman tunnistuspalvelun tuottamisen ja ylläpitämisen kustannukset. Valtion oma tunnistuspalvelu muut poissulkevana ei sinänsä ole kuitenkaan ensisijainen vaihtoehto, koska kansalaiselle syntyisi tällöin tarve opetella useita tunnistusratkaisuja. Vaihtoehtoiksi on jäänyt vain regulaatiolla pakottaa tuottamaan tunnistaminen yksityisistä palveluista halvemmalla. Tämä ei taas sovi markkinaehtoisien ekosysteemien kehittämisen periaatteisiin eikä kannusta kilpailuun kehittämällä palveluita.

5. Tavoiteltavan toimintamallin kuvaus

Nykyinen sähköisen tunnistamisen toimintaympäristö on perusrakenteiltaan määritelty ja säännelty pitkälti 2010-luvun taitteessa. Sähköisen tunnistamisen kokonaisuus on toiminut sille määriteltyjen tehtävien osalta pääsääntöisesti kohtalaisesti. Tämä on toisaalta vaatinut myös voimakasta ohjausta lainsäädännön tasolla esimerkiksi yhteentoimivuuden osalta luottamusverkostosäätelyllä ja valtion merkittävää roolia ostajana sähköisen tunnistamisen palveluille. Näistä lähtökohdista nykyinen malli on kyennyt

vastaamaan välttävästi nykyisiin käyttötarpeisiin, mutta vahvan sähköisen tunnistamisen käytön hyödyntämisen laajentuminen yhteiskunnan eri toimintasektoreille on edelleen alhainen sille jo 2010-luvun alussa asetettuihin tavoitteisiin nähden.

Nykytilan arvio ei kuitenkaan välttämättä kerro siitä, kuinka hyvin nykyinen järjestelmä vastaa arvioituihin lähitulevaisuuden käyttötarpeisiin. Digitaalinen identiteetti, siihen liittyvät tiedot ja niiden käyttö ovat digitalisaation myötä nousseet erittäin keskeiseksi tekijäksi digitaalisen yhteiskunnan palvelujen käytön kehittymisen näkökulmasta. Tämä vaatii perustavaa laatua olevia muutoksia nykyiseen sähköistä tunnistamista, henkilöllisyyden saamista ja osoittamista sekä henkilötietojen käyttöä koskevaan säätelyyn.

5.1. Digitaalisen identiteetin muodostaminen ja myöntäminen

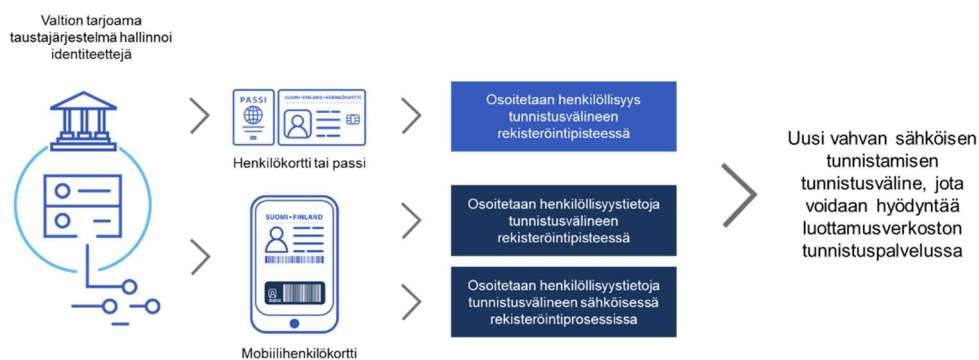
Digitaalisen henkilöllisyyden hankkeen yksi kehityskohde on laajentaa käyttäjäryhmiä, joilla olisi mahdollisuus osoittaa henkilöllisyytensä sähköisesti asioissa. Tähän tavoitteeseen liittyy kiinteästi väestötietojärjestelmän ja henkilötunnusjärjestelmän kehittäminen, jota toteutetaan valtionvarainministeriön 1.12.2020 asettamassa Henkilötunnuksen uudistamisen ja valtion takaaman identiteetin hallinnoimisen hankkeessa. Yhdessä nämä kaksi hanketta pyrkivät laajentamaan väestötietojärjestelmän tietosisältöä ja sille asetettua säätelyä siten, että henkilötunnuksen saaminen helpottuisi ja sen osoittamiseksi tarjottaisiin digitaalinen sovellus. Yhtenä tavoitteena tällä on mahdollistaa ulkomaalaisille henkilöille nykyistä helpommin asiointi viranomaisessa.

Kansalaisen ensitunnistaminen, ydinidentiteetin rekisteröinti ja sen elinkaaren hallinta on säädetty Digi- ja väestötietoviraston ja osin poliisin tehtäväksi. Digitaalisen henkilöllisyyden hankkeessa on kyse viranomaisen perusrekistereihin kirjattavista luotettavista henkilötiedoista, tunnisteista ja metatiedoista, ja niiden tarjoamisesta viranomaisten ja yksityisen sektorin käyttöön digitaalisen identiteetin muodossa henkilön itsensä hallinnoimana.

Digitaalisen identiteetin ja sähköisen asioinnin maailma on kehittymässä suuntaan, jossa henkilö itse suoraan kontrolloi häneen liittyvien tietojen jakamista kolmansille osapuolille (mobiilipohjaisten) identiteettilompakoiden avulla. Fyysisen maailman vastaava vertailukohde on lompakko, jonka sisällä ihminen säilyttää muovikortteina erilaisia todistuksia ja lupia. Sähköisessä tunnistamisessa pitkään käytössä ollut toimintamalli, jossa henkilön ja asiointipalvelun välissä on toiminut luotettu osapuoli ns. tunnistuspalvelun tarjoaja, on merkittävien muutosten edessä.

Valtio tunnistaa käyttäjän fyysisesti poliisilaitoksella joka tapauksessa esimerkiksi passia tai henkilökorttia haettaessa. Nykyisessä mallissa henkilö tulee tunnistaa uudelleen sähköistä tunnistusvälinettä myönnettäessä. Valtion luodessa suoraan digitaalisen ydinidentiteetin, jonka avulla voidaan ottaa käyttöön myös muita välineitä, luotaisiin edellytyksiä vähentää tarvetta eri toimijoiden tekemälle kalliille fyysisen ensitunnistamisen prosessille.

Ratkaisulla voidaan nähdä myönteisiä vaikutuksia nykyiseen tunnistuspalvelujen hinnoitteluun. Hinnoittelun taustalla yhtenä merkittävänä yksittäisenä kustannustekijänä on VTJ-kysely ensitunnistamisen yhteydessä. Tämä jäisi suunnitellussa mallissa osittain tarpeettomaksi, koska valtion digitaalisen henkilöllisyyden ratkaisussa valtion vahvistamat, ajantasaiset henkilötiedot siirtyisivät käyttäjän hallinnoimina väestötietojärjestelmästä tunnistusvälineen myöntäjälle tai asiointipalvelulle.



5.1.1. Ydinidentiteetti ja asiayhteydellinen identiteetti

Tässä arviomuistiossa käsitellään pääsääntöisesti vain luonnollisten henkilöiden identiteettiä, mutta myös yrityksillä, rakennuksilla, laitteilla ja jopa aineettomilla asioilla voi olla ja tulevaisuudessa on yksilöivä identiteetti. Henkilöön keskeisesti liittyvät henkilötiedot, jotka luotettavasti auttavat yksilöimään ja tunnistamaan henkilön, voidaan karkeasti jaotella yksilöivän tiedon vahvistajan ja rekisteröijän mukaan kahteen toisiaan muistuttavaan pääryhmään: ydinidentiteettiin ja asiayhteyteen liittyvään identiteettiin.

Henkilön **ydinidentiteetti** on joukko keskeisiä väestötietojärjestelmään tallennettuja tietoja, jotka luovat perustan henkilön luotettavaan yksilöintiin Suomessa. Näitä tietoja ovat esim. henkilötunnus, etunimi, sukunimi ja syntymäaika. Digi- ja väestötietoviraston ylläpitämää henkilön ydinidentiteettiä hyödynnetään laajalti koko yhteiskunnassa. Hankkeessa tavoitteena on, että

henkilön haltuun saatettu ydinidentiteetti olisi jatkossa entistä laajemmin hyödynnettävissä erilaisissa asiointitilanteissa, mukaan lukien sähköisessä tunnistamisessa.

Asiayhteydellinen identiteetti on identiteetti, joka on perustettu ja jota käytetään ensisijaisesti tiettyyn tarkoitukseen tietyssä asiakkuuteen liittyvässä kontekstissa ja mahdollisesti myös asioinneissa pääsääntöisesti sopimusperusteisesti. Esimerkiksi pankki- ja vakuutuspalveluissa asiakas voi hoitaa sähköisesti laskujen maksamisen ja vakuutuskorvauksen hakemisen hyödyntäen pankin asiakkaistaan ylläpitämää identiteettiä ja tämän avulla sekä tätä varten luotua tunnistusvälinettä. Identiteettiä hallitaan pankin asiakastietokannassa. Käyttöyhteydestä riippuen asiayhteydellinen identiteetti voi olla asiakassuhteen syntymishetkellä tarkistettu ja sidottu väestötietojärjestelmän ydinidentiteettiin, mutta sitä hallitaan palvelutarjoajan asiakastietojärjestelmässä tai muualla.

5.2. Ratkaisut, jotka mahdollistavat digitaalisen henkilöllisyyden osoittamisen käyntiasioinnissa

Hankkeen keskeinen tavoite on luoda viranomaisen hallinnoiman ydinidentiteettitiedon (väestötietojärjestelmä) henkilöön liittämistä digitaalinen todistus. Henkilön liittäminen ydinidentiteettiin tapahtuu poliisin tehdessä henkilöllisyyden tarkistuksen passin tai henkilökortin hakemisen yhteydessä. Tämä kokonaisuus muodostaisi henkilön valtion takaaman digitaalisen henkilöllisyyden. Ydinidentiteettitiedon ja henkilön yhdistämisen voi tehdä virallisten henkilöllisyystodistusten osalta vain viranomaisen. Digitaaliseen identiteettiin liittyy olennaisesti menetelmä, jonne identiteetin osoittava digitaalinen todiste voidaan tallentaa ja mistä sitä voidaan käyttää. Tällaista palvelua kutsutaan digitaaliseksi lompakoksi.

Digitaalinen ydinidentiteetti kytkettäisiin henkilön digitaalisen henkilöllisyyden tallennusmenetelmään, digitaaliseen lompakkoon samalla, kun henkilölle myönnetään henkilökortti tai passi tai kun henkilö uusii näitä. Samalla henkilölle muodostuu valtion tuottamaan digitaaliseen lompakkoon digitaalinen henkilökortti (mobiilihenkilökortti), joka mahdollistaa henkilöllisyyden osoittamisen digitaalisesti sekä julkisen sektorin että yksityisen sektorin käyntiasiointipalveluissa. Digitaalisen henkilöllisyyden hanke toteuttaa ratkaisun henkilöllisyyden tarkastamista varten sekä mobiilisovelluksena että erillisenä standardirajapintana, mikäli tarkastustoiminnallisuus halutaan integroida esimerkiksi olemassa oleviin asiakasjärjestelmiin (kassajärjestelmät tms.). Määrittelytyössä tarvitaan hankkeen ja sen julkisen sekä yksityisen sektorin sidosryhmien läheistä yhteistyötä.

Mobiilihenkilökortin voi tallentaa vain valtion tuottamaan digitaaliseen lompakkoon, mutta tarkoituksena on, että digitaalisen todistuksen ydinidentiteetin ja henkilön liitoksesta voisi tulevaisuudessa tallentaa valtion tuottaman digitaalisen lompakon lisäksi muihinkin lainsäädännössä asetetut vaatimukset täyttäviin digitaalisiin lompakoihin. Jotta tämä olisi tulevaisuudessa mahdollista, ja jotta ratkaisut olisivat lähtökohtaisesti yhteensopivia, tarvitaan läheistä yhteistyötä hankkeen ja muiden potentiaalisten digitaalisen lompakon tarjoajien välillä jo lausuntokierroksen aikana.

Tässä arviomuistiossa myöhempi juridinen tarkastelu on tehty mobiilihenkilökortin ja valtion tuottaman digitaalisen lompakon kannalta.

Kun ydinidentiteetti tuotetaan digitaalisena todisteena mobiilisovelluksella osoitettavaksi, sähköinen henkilöllisyyden osoittaminen ja käyntiasioinnissa henkilöllisyyden osoittaminen eivät enää ole tekniikaltaan irrallisia ratkaisuja. Sähköinen asiointi ja käyntiasointi voivat käyttää samaa teknologiaa sekä rekisteröinnin ja myöntämisen prosesseja. Käyntiasioinnissa henkilöllisyyden osoittamiseen ei ole syntynyt markkinaehtoisesti kehittyvää markkinaa, joten sen toteuttaminen hankkeessa on luontevasti valtion tehtävän laajentamista digitalisaation keinoin. Tarvitaan vain kyky myöntää oma sovellus ja siihen ydinidentiteetin todiste.



Tavoiteltavassa toimintamallissa ydinidentiteetti ja sen osoittava digitaalinen todiste on erotettu siitä välineestä, jonka kautta ydinidentiteetin osoittavaa digitaalista todistetta käytetään. Viranomaisen keskeinen rooli on tuottaa ydinidentiteetti (henkilön kirjaaminen väestötietojärjestelmään) ja digitaalinen todiste, joka osoittaa, että väestötietojärjestelmään luotu ydinidentiteetti on

liitetty luonnolliseen henkilöön. Fyysisessä maailmassa tämä todiste on passi tai henkilökortti.

Ydinidentiteetin osoittavan digitaalisen todisteen käyttäminen vaatii digitaalisen tallennustavan eli digitaalisen lompakon aivan kuten passi muodostaa samoista tiedoista fyysisen tallennustavan. Tavoitteena oleva asiakkuusriippumaton digitaalinen identiteetti ja sen osoittamisen menetelmä edellyttää, että viranomaisella on velvollisuus tuottaa ja tarjota käyttäjälle digitaalinen tallennusmenetelmä, jolla digitaalista identiteettiä voi käyttää ja siihen liitettyjä varmennettuja viranomaistietoja (väittämiä) voi välittää digitaalisiin palveluihin.

5.3. Ratkaisut, jotka mahdollistavat muiden viranomaistietojen, kuten lupien tai vahvistettujen rekisteritietojen esittämisen

Usein sähköisissä palvelukokonaisuuksissa tarvitaan asiointitapahtuman sujuvaan käsittelyyn yhdistelmä yksittäisiä tietoja sekä yksityisen että julkisen puolen palveluista ja rekistereistä. Jos tarvittavat tiedot ovat valmiiksi vahvistettuina väittämänä loppukäyttäjän kontrollissa ja hän voi osoittaa niitä kulloisenkin asiointitapahtuman edellyttämällä tavalla, palvelun kehittäminen yksinkertaistuu ja itse asiointi nopeutuu. Nykyisessä keskitettyjen tietovarantojen toimintaympäristössä tietojen kerääminen eri rekistereistä vaatii aina palvelujen välisiä järjestelmäintegraatioita. Tämä on kallista ja hidasta toteuttaa, eikä aina välttämättä ole edes mahdollista. Nykyisessä toimintamallissa yksittäisten tietottribuuttien oikeellisuuden tarkistaminen on vaikeaa tai mahdotonta varsinaiselle asiointipalvelulle (kolmas osapuoli). Henkilötiedon yksittäisten attribuuttien osoittaminen on lopulta laajempi kokonaisuus kuin tunnistaminen, eikä sitä pitäisi lähteä ratkaisemaan nykyisen tunnistamisen lainalaisuuksista johtamalla.

5.4. Digitaalisen henkilöllisyyden osoittaminen asiointipalveluissa sähköisesti

Valtion tuottama ydinidentiteetti ja sen osoittava digitaalisen todisteen tallennusmenetelmä (mobiilihenkilökortti) mahdollistavat henkilöllisyyden osoittamisen käynti- ja sähköisessä asioinnissa käytännössä kaikille, jotka voivat saada suomalaisen passin tai henkilökortin (ml. alaikäisen ja ulkomaalaisen henkilökortti), ja joilla on mahdollisuus käyttää älypuhelinta. Valtion takaama digitaalinen todiste tarjotaan myös ns. vaihtoehtoisena välineenä (esim. USB-tikku) niille, joilla ei ole mahdollisuutta tai halua käyttää älypuhelinta. Tämä edistää yhdenvertaisia mahdollisuuksia asioida sähköisesti viranomaisissa tai yksityisten palveluntarjoajien palveluissa, kun sähköinen

asiointi on muuttunut poikkeuksesta pääsääntöiseksi asiointitavaksi usean viranomaisen palveluissa 2010-luvun aikana. Korona-pandemia on voimistanut muutosta korostaen entisestään sähköisen asioinnin toimintaedellytysten turvaamiseen kriittisyyttä. Sähköiselle asiointille ei välttämättä enää löydy vastaavaa käyntiasiointivaihtoehtoa lainkaan.

Ydinidentiteetin ja sen osoittavan digitaalisen todisteen pitää olla käytettävissä sähköiseen asiointiin myös ilman passin tai henkilökortin hakemista ja myöntämistä, jolloin täytyy arvioida poliisin olemassa olevan passi- ja henkilökorttiprosessin kehittämistä tai luoda kokonaan uusi rekisteröimisprosessi ydinidentiteetin ja luonnollisen henkilön liittämiseksi.

Hankkeen tavoitteiden mukaisesti valtion tuottaman ydinidentiteetin ja sen osoittavan digitaalisen todisteen voi jatkossa saada myös henkilö, jolla ei ole mahdollisuutta saada suomalaista passia tai henkilökorttia. Tällöin ratkaisu on käytössä sähköisessä asiointissa myös esimerkiksi ulkomaalaisilla, jotka ovat tulossa Suomeen opiskelemaan tai asioivat suomalaisissa asiointipalveluissa työnsä johdosta. Ydinidentiteetin rekisteröinti ja luonnollisen henkilön liittäminen digitaalisesti todisteeksi tapahtuu tässä tapauksessa erillisen rekisteröintiprosessin kautta. Tämän rekisteröintiprosessin tuottaminen tehdään yhteistyössä Henkilötunnuksen uudistamisen ja valtion takaaman identiteetin hallinnoimisen hankkeen kanssa. Prosessissa syntyvää digitaalista todistetta hyödynnetään tässä hankkeessa toteutettavaan ratkaisuun. Digitaalisen todisteen ydinidentiteetin ja luonnollisen henkilön liitoksesta voisi tulevaisuudessa tallentaa valtion tuottaman digitaalisen lompakon lisäksi muihinkin lainsäädännössä asetetut vaatimukset täyttäviin digitaalisiin lompakoihin. Jotta tämä olisi tulevaisuudessa mahdollista, ja jotta ratkaisut olisivat lähtökohtaisesti yhteensopivia, tarvitaan läheistä yhteistyötä hankkeen ja muiden potentiaalisten digitaalisen lompakon tarjoajien välillä jo lausuntokierroksen aikana.

Digitaalisen henkilöllisyyden osoittaminen mahdollistetaan sähköisesti myös puhelinasiointissa.

Tulevaisuuden tavoitetilassa kansalaisen ydinidentiteetin säilyttävä ja kontrolloiva identiteetilompakko on “kontrollipiste”, koska kaikki henkilön transaktiot tapahtuvat lompakko-operaattoreiden tarjoaman digitaalisen lompakon kautta. Viranomaisen tuottama digitaalinen tallennusmenetelmä ydinidentiteetin osoittavalla digitaaliselle todisteelle ei kuitenkaan ole ainoa menetelmä, mutta se on ainoa menetelmä, johon digitaalisen henkilökortin (mobiilihenkilökortti) voi tallentaa.

Digitaalinen todistusta voitaisiin hyödyntää turvallisissa henkilöllisyyden osoittamista vaativissa ratkaisuisissa, ja tuon digitaalisen todisteen käyttöä varten henkilöllä on oltava hallinnassaan siihen liitetty salaisuus – esimerkiksi salainen avain. Avainta hallitaan ensin valtion tarjoamalla välineellä ja varaudutaan jo hanketta toteuttaessa siihen, että todiste voidaan tulevaisuudessa myöntöhetkellä kytkeä esimerkiksi markkinatoimijan tarjoamaan siihen tarkoitukseen suunniteltuun ja auditoituun välineeseen.

Tämä mahdollistaisi nykyistä toimintamallia paremmin kilpailun yhtäältä digitaalisen identiteetin ja henkilön liitoksen osoittavien tuotteiden välillä sekä toisaalta sähköisten, luottamusta vaativien, lisäarvopalveluiden välillä. Valtion tuottama digitaalinen identiteetti digitaalisena todistena ja välineenä voisi myös mahdollistaa digitaalisten palveluiden innovaatiota sellaisille toimijoille, jotka eivät ole kiinnostuneita ylläpitämään laajoja asiakkuuteen perustuvia identiteettirekistereitä.

Sähköisen henkilöllisyyden osoittamisen metodista tai liikkeellelaskijasta riippumatta osoitettu tieto on pystyttävä asiointipalvelussa tarkistamaan myöntäjältä ja loppukäyttäjän on ymmärrettävä ja hyväksyttävä, mitkä osapuolet transaktiossa käsittelevät käyttäjän henkilöllisyyttä osoittavaa dataa. Nykyinen vahva sähköinen tunnistaminen voidaan nähdä tuon laajemman määritelmän osajoukkona. Mikäli uudistettu ekosysteemi vaatii uusia rajapintoja tai toiminnallisuuksia, niillä voidaan aina toteuttaa myös vanhan ekosysteemin rajatumpi sähköinen tunnistustoiminto ja markkinaehtoiset tunnistuspalvelut ja välityspalvelut konvertoivat tarvittaessa uuden ja vanhan metodin välillä. Asiointipalvelun ei tarvitsisi tehdä muutoksia, mikäli se ei uusia ominaisuuksia ja mahdollisuuksia tarvitse.

Digitaalisen identiteetin ja välineiden kehityksessä on myös huomioitava mahdollinen digitaalisen ja fyysisen asioinnin yhdistyminen. Nykyisessä toimintaympäristössä digitaalinen ja fyysinen asiointi ovat suurelta osin toisistaan erillisiä ja irrallisia. Tulevaisuudessa on todennäköistä, että nämä yhdistyvät siten, että fyysisessä asiointissa henkilö voi todentaa olevansa väittämänsä henkilö hyödyntäen digitaalista henkilöllisyyden todentamisen menetelmää. Tällöin esimerkiksi asiointitilanteessa, joissa nykyisin vaaditaan virallinen henkilöllisyystodistus, henkilö voisi todentaa henkilöllisyytensä digitaalista palvelua käyttäen joko suoraan todentamista vaativaan palveluun tai näyttämällä henkilön hallussa olevaa digitaalista henkilöllisyystodistusta sitä pyytävälle. Henkilö voi asioidessaan myöskin tarvita mahdollisuutta tunnistautua laitteelle, todistaa omaavansa oikeuden avata sähköisen lukon tai osoittaa edustavansa jotakin yritystä. Myös näitä kysymyksiä olisi arvioitava suunniteltaessa digitaaliseen identiteettiin pohjautuvia välineitä ja palveluita.

Ydinidentiteetin osoittavan digitaalisen todisteen voisi tulevaisuudessa tallentaa myös muuhun käyttäjän käytössä olevaan digitaaliseen lompakkoon. Tavoitella todennäköisesti edellyttää ainakin digitaalisten lompakkojen osalta uutta säätelyä, jolla varmistetaan niiden luotettavuus, turvallisuus, yhteentoimivuus ydinidentiteetin digitaalisen todisteen tallennus- ja käyttömenetelmänä sekä säädellään vastuuperiaatteet. Tämä muuttaa nykyisen vahvan sähköisen tunnistamisen säätelyn kohdetta, koska identiteetin tallentavalla lompakkopalvelulla ja sinne tallennetulla ydinidentiteetin digitaalisella todisteella ja muilla varmistetuilla tiedoilla voi olla eri vastuuorganisaatiot. Tässä arviomuistiossa myöhempi juridinen tarkastelu on tehty valtion tuottaman digitaalisen lompakon kannalta.

Viranomaisilla on rekistereissään tietoja, joista se tuottaa erilaisia fyysisiä todisteita kansalaisille – ajo-oikeudesta, opintasuorituksista tai vaikkapa ase- ja hallussapito-oikeudesta. Näitä tietoja voidaan tuottaa digitaalisina todisteina ja myöntää kansalaisen osoitettavaksi eteenpäin asiointitilanteissa. Myös yksityisillä toimijoilla, muillakin kuin tunnistus- tai välityspalveluilla, on tietoja henkilöstä, joita asiointipalvelut voivat tarvita tuottaakseen parempia digitaalisia palveluita yhden luukun periaatteella.



5.5. Alustavat arviot tavoitetilan vaikutuksista nykyiseen toimintaympäristöön ja vaikutusarvioinnin suunnitelmat

Digitaalisen henkilöllisyyden hanke tuottaa henkilöllisyyden ja siihen liittyvien tietojen osoittamisen menetelmän loppukäyttäjälle, kansalaiselle. Hankkeen tuottaman kokonaisuuden kautta henkilöllisyyttä osoittaa asiointipalvelulle henkilö itse. Henkilö voi käyttää menetelmää myös yksityisen sektorin asiointipalveluissa halutessaan. Tällöin asiointipalvelulla on oltava valmius ottaa vastaan osoitettu henkilöllisyystieto, ja tarkastaa tiedon ajantasaisuus ja oikeellisuus hankkeessa tuotettavan avoimen rajapinnan kautta.

Henkilöllisyystiedon tarkastaminen on mahdollistettu kaikille toimijoille, sillä tarkastusrajapinta on avoin aivan kuten nykyisessä kansalaisvarmenteessa. Digitaalisen henkilöllisyyden hanke tuottaa asiointipalveluiden vaatiman henkilöllisyyden tarkastamisen rajapintaosuuden, mutta tämän käyttö riippuu yksityisen sektorin asiointipalveluista. Käyttöönottoon on ainakin kaksi erilaista tapaa. Joko asiointipalvelut toteuttavat henkilöllisyyden tarkastamisen itse, jolloin niiden olisi otettava käyttöön luottamusverkoston ulkopuolinen menetelmä ja rajapinnat tai joku yksityinen palveluntarjoaja toteuttaa välityspalvelun, joka toteuttaa tarkastuksen asiointipalvelun puolesta. Tämä vastaa nykyistä luottamusverkostotoimintaa. Valtio ei siis päättä siitä, voivatko yksityiset käyttää hankkeessa syntyviä palveluita, mutta antaa siihen mahdollisuuden. Tämä vastaa nykyistä passin tai henkilökortin esittämisen logiikkaa, jossa viranomaisella ei ole tietoa siitä, missä henkilö milloinkin henkilöllisyysasiakirjaansa näyttää ja osoittaa siten henkilöllisyytensä.

Nykyisen luottamusverkoston toimijat pystyvät hyödyntämään valtion tuottamaa henkilöllisyyden osoittamisen menetelmää omissa palveluissaan oman tunnistusvälineensä rinnalla tai kokonaan nojautuen henkilön itsensä osoittamaan henkilöllisyyteen. Julkisen hallinnon palveluihin mahdollistetaan pääsy luottamusverkoston vahvan sähköisen tunnistamisen palveluilla myös jatkossa.

Ehdotetuilla muutoksilla voi olla merkittäviä vaikutuksia nykyiseen sähköisen tunnistamisen toimintakenttään. Valtion rooli ydinidentiteetin tuottajana ei muuttuisi nykyisestä eli valtio tuottaisi ja tarjoaisi jatkossakin ydinidentiteetin kuten nykyisin. Valtio tarjoaa jo nyt myös menetelmän ydinidentiteetin osoittamiseksi myös digitaalisessa palvelukanavassa (henkilökortin sirulla oleva varmenne). Näiden lisäksi tulisi tarjolle uusi tapa osoittaa henkilöllisyys digitaalista menetelmää hyödyntäen käynti-, puhelin- ja digitaalisessa asiointinnissa.

Merkittävin muutos, joka esitetystä toimintamallista tulisi liittyä ydinidentiteettiin liitetyn digitaalisen todisteen myöntämisen irrottaminen tunnistusvälineestä. Tällöin markkina siirtyy digitaalisen identiteetin myöntämisestä ja saamisesta niihin menetelmiin, joihin sen voi tallentaa tai joiden kautta sitä voi käyttää. Valtion tuottama digitaaliseen identiteettiin liitetty digitaalinen todiste on tarkoitus toteuttaa niin, että todisteen myöntävä viranomainen voi seurata vain mihin digitaaliseen lompakkoon todiste yhdistetään, mutta viranomainen ei voi seurata, missä identiteettiä käytetään. Lompakon myöntäjällä ei myöskään ole välttämättä tietoa, missä palvelussa identiteettiä käytetään, koska lompakko ja identiteetti ovat toisistaan loogisesti

irrationaaliset. Sähköistä tunnistusta pyytävä asiointipalvelu kysyy tunnistusta varten tarvittavat tiedot identiteetin digitaaliselta todisteelta ja lompakon kautta kuluttaja voi hallita, mihin palveluun hän digitaalisen identiteetin tietoja välittää. Lompakkopalvelun tuottajat voivat toki tarjota erilaisia hallinnan tasoja, mitä tietoja ja kuinka paljon lompakkopalvelun tarjoaja tietää käyttäjän digitaalisesta elämästä. Tämä on todennäköisesti myös yksi markkinoille tulevista kilpailutekijöistä pelkän hinnan lisäksi.

Tavoitetilassa sähköisen tunnistuksen laskutusta ei voida rakentaa tunnistamistapahtumien varaan, koska mallissa ei ole enää keskitettyä pistettä, joka seuraisi henkilön identiteeteillä tekemiä tunnistustapahtumia tai niistä välittämiä tietoja. Tämä johtaa siihen, että kuluttaja on käytännössä ainoa laskutuskohte ja sähköisen tunnistamisen markkina muuttuu sähköisen lompakon ja varmennettujen väittämien markkinaksi. Molemmissa asiakas on kansalainen, ei asiointipalvelu. Tunnistuspalveluita tarvitaan edelleen, koska asiointipalvelut ulkoistavat asiakkailta tulevien väittämien tarkistuspalveluita, mikäli eivät halua toteuttaa tätä toiminnallisuutta itse.

Tavoitetilassa sähköisen tunnistamisen sääntely kohdistuisi ensisijaisesti lompakko-operaattoritoimintaan, siten että lompakoiden tarjoajien välille luodaan pelisäännöt kilpailulle markkinalle. Digitaalisen henkilöllisyyden hankkeen keskeinen tavoite on pitää valtion ydinidentiteetti kansalaisen perusoikeutena missä tahansa turvalliseksi määritellyssä lompakossa. Sääntelyä tulisi arvioida suhteessa siihen, miten se olisi edistää mahdollisimman hyvin loppukäyttäjän valinnanvapautta erilaisten luottamusinfrastruktuurin tai lompakontarjoajan tai näiden määrän suhteen. Valtion tuottama ydinidentiteetti ja sen digitaalinen todiste tulisi olisi sääntelyllä ns. pakollinen jokaiseen luvanvaraiseen lompakkopalveluun hyväksyttävä identiteetti. Valtion tuottama ydinidentiteetti ei estä muiden, asiakassuhteeseen liittyvien identiteettien tuottamista ja niiden liittämistä identiteettilompakoihin. Näiden identiteettien osalta jokainen toimija joutuu arvioimaan tarvetta omasta näkökulmastaan palvelutarve- ja sopimusperustaisesti.

Tavoitetilassa sähköisessä tunnistamisessa olisi todennäköisesti jossakin määrin nykyisestä poikkeavat hinnoittelu- ja liiketoimintamallit. Pankin tai mobiilioperaattorin välineessä voi olla valtion ydinidentiteetin todiste tai valtion välineessä voi olla pankin tai mobiilioperaattorin identiteetin todiste. Myös kolmansia osapuolia voi ilmoittautua myöntämään henkilöstä vahvistettuja tietoja, joita käytetään asiointitapahtuman sujuvampaan tuottamiseen. Varsinainen vaikutustenarviointi tehdään mahdollisen hallituksen esityksen valmistelun yhteydessä. Arviomuistion lausuntopalautetta hyödynnetään vaikutustenarvioinnin suunnittelussa ja valmistelussa.

5.5.1. Esimerkki tulevaisuuden tavoitetilasta

Toimija (pankki, mobiilioperaattori, Digi- ja väestötietovirasto tai joku muu) kehittää digitaalisen lompakon, jonka ulkoinen tarkastuslaitos auditoi ja Liikenne- ja viestintävirasto Traficom hyväksyy ydinidentiteetin digitaalisen todisteen tallennusmenetelmäksi. Sovelluskauppa tarjoaa tämän tyhjän digitaalisen lompakon loppukäyttäjälle. Käyttäjä lataa puhelimeensa lompakkosovelluksen. Lompakkoon kirjoitetaan varmennettuina todisteina (myönnetään) väestötietojärjestelmän ylläpitämiä ja varmennepalvelun allekirjoittamia (varmentamia) tietoja (esimerkiksi henkilötunnus, nimi, syntymäaika, sukupuoli tai kansalaisuus) samassa yhteydessä, kun henkilö käy fyysisesti poliisiasemalla tunnistautumassa (liitos luonnolliseen henkilöön, kasvokuva).

Tämän jälkeen henkilön mobiililompakkoon on tallennettu digitaalisesti allekirjoitettuja varmennettuja häneen liittyviä viranomaistietoja, joita henkilö itse voi jakaa asiointipalvelulle niin halutessaan. Tietoja voi jakaa vain yhden kerrallaan tai useita yhtä aikaa, asiointitarpeesta riippuen.

Mikäli henkilöllä on voimassa oleva henkilökortti tai passi, fyysinen tunnistautuminen on poliisiasemalla jo tehty, jolloin varmennettujen tietojen vienti lompakkoon voidaan tehdä vahvaa sähköistä tunnistautumista käyttäen. Mikäli varmennettuihin tietoihin tulee muutoksia, digitaalinen lompakko huolehtii niiden ajantasaisuudesta.

Esimerkissä ei tunnistauduta asiointipalvelulle (identifioiduta) nykyisin säädellyllä tavalla, vaan ”tunnistautuminen” tapahtuu lompakolle, jonka kautta asiointipalvelulle osoitetaan ainoastaan välttämättömät tiedot kyseisen asioinnin hoitamiseksi. Eri lompakot voivat käyttää erilaisia hyväksymismenetelmiä, esimerkiksi sormenjäljellä, PIN-koodilla tai kasvontunnistuksella. Käyttäjä voi valita itselleen parhaiten sopivan lompakon tai lompakoita, joita haluaa käyttää.

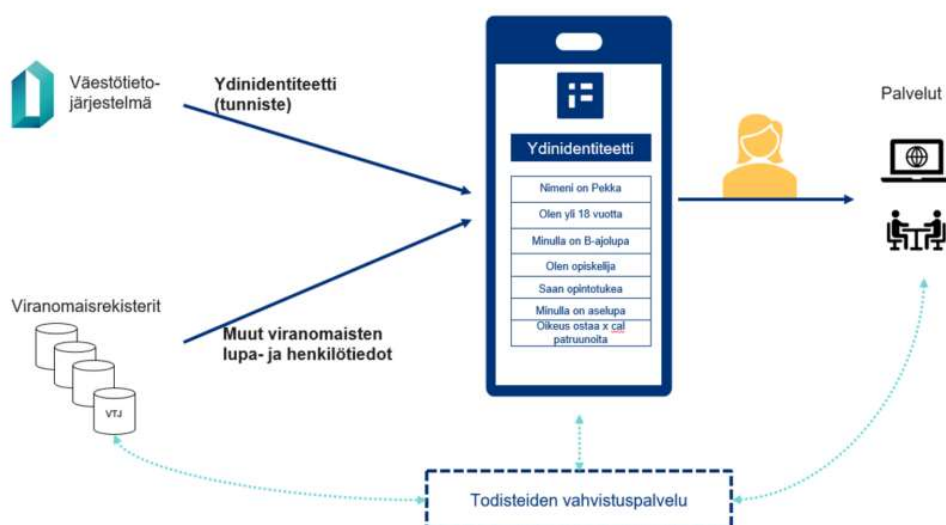
Esimerkissä henkilön hallinta omista tiedoistaan lisääntyy, koska viranomaisen vahvistama tieto voidaan jakaa asiointipalvelulle vain henkilön itsensä suostumuksella. Olennaista on, että henkilö voi jakaa lompakon kautta tietoa riippumatta siitä, mihin rekisteriin henkilöön liitetty tieto on alun perin tallennettu. Asiointipalveluiden kehittäminen ja datan hyödyntäminen taas helpottuvat, koska henkilöön liitettyjä tietoja ei tarvitse hakea erilaisista

rekistereistä integroitumalla moneen eri tiedon lähteeseen (rekisteriin tai asiakastietokantaan).

Tavoitetilassa viranomaisten oikeus saada asiointia varten tarpeelliset tiedot toiselta viranomaiselta ei muuttuisi. Tavoitetilassa henkilöön liittyviä vahvistettuja tietoja (kredentiaaleja) voi tulla loppukäyttäjälle muiltakin myöntäjiltä kuin viranomaisilta (esim. DVV, poliisi, Traficom, Kela, Vero), jos asiakastietoa hallinnoiva organisaatio sen hyväksyy. Lompakko toimii siis ajan myötä fyysisen lompakon tapaan kerryttäen henkilöstä eri lähteistä liikkeelle laskettua tietoa.

Henkilö voi osoittaa omia tietojaan asioidessaan viranomaisten kanssa tai vaikkapa tilatessaan tuotteita verkkokaupasta, halliten kuitenkin itse jakamansa tiedon määrää. Vastaanottaja voi todentaa tiedon oikeellisuuden tarkastamalla vahvistetun tiedon (kredentiaalain) tilan eritavoin. Yksi mahdollisuus voi olla esimerkiksi yhteinen luottamusinfrastruktuuri, joka yhdistää tiedon tuottajat, sen hyödyntäjät ja tiedon kohteen. Tällaisessa toimintaympäristössä olennaista olisi mahdollistaa tiedon oikeellisuuden varmistus ilman teknistä yhteyttä tiedon myöntäjään tai sen tietojärjestelmään.

Tavoitetilan esimerkki ei välttämättä edellytä vanhan toimintamallin täydellistä purkamista, mutta uusia ominaisuuksia ei saada toteutettua vain vanhaa uudistamalla.



Tavoitetilassa valtiolla on kolme erilaista roolia:

1. Valtio ylläpitää erilaisia rekistereitä ja niihin liittyviä henkilötietoja, joita voitaisiin tuoda henkilön identiteettilompakkoon. Kaikki tieto ei ole ydinidentiteettitietoa. Lompakkoon myönnetty tieto on osoitettavissa myös yksityisille palveluille tai yksityisellä lompakolla.
2. Valtio digitalisoi asiointipalveluitaan ja toimii asiointipalveluna henkilön osoittaman tiedon kysyjänä ja tarkistajana. Julkisessa hallinnossa tarvitaan myös yksityisten myöntämiä ja vahvistamia tietoja henkilöstä. Esimerkiksi oikeat pankkitilitiedot olisi merkittävä toiminnallinen tehostustoimi etuuskäsittelyssä.
3. Valtio käyttää julkista valtaa ja ohjaa säätelyllä toimintaa pitääkseen sen yhdenvertaisena, saavutettavana, luotettavana ja turvallisena sekä sitovia kansainvälistä säätelyä ja muita sitoumuksia vastaavana.

5.6. Vaihtoehtoisten toimintamallien tarkastelu

Toimintamallia valmisteltaessa on arvioitu myös nykyisen sähköisen tunnistamisen markkinan toimivuutta suhteessa ehdotettuun tavoitetilään. Vahvan sähköisen tunnistamisen nykyinen toimintamalli pohjautuu markkinaehtoiseen toimintaan, jossa identiteetinhallinta on sähköistä tunnistamista palveluna tarjoavien yritysten hallinnassa. Tämä on ollut selkeä säätelypoliittinen linja vuodesta 2009 alkaen. Tässä arviomuistiossa ehdotettu digitaalisen identiteetinhallinnan toimintamalli lähtee ajatuksesta, jossa identiteetinhallintapiste voi siirtyä ihmiselle itselleen tunnistuspalvelua tuottavalta organisaatiolta. Tätä muutosta ei ole mahdollista toteuttaa nykyisen sähköisen tunnistamisen toimintamallin kautta.

Yhtenä vaihtoehtona on esitetty nykyjärjestelmän kehittäminen, jossa valtio säilyisi merkittävänä ostajana tunnistusmarkkinoilla ja tunnistuspalveluntarjoajat olisivat lähinnä nykyiset toimijat. Tällöin valtio joutuisi hyödyntämään nykyistä huomattavasti voimakkaammin asemaansa merkittävänä ostajana tunnistusmarkkinoilla kilpailuttaessaan tunnistautumista sen sähköisiin julkisiin palveluihin. Käytännössä tämä tarkoittaisi valtion yksipuolista ilmoitusta enimmäiskustannuksista, joita se suostuu sähköisestä tunnistamisesta julkisen hallinnon digitaalisiin palveluihin yhteensä maksamaan. Kustannustaso rajautuisi käytännössä nykyiseen määrärahasoon (noin 5-6 miljoonaa euroa/vuosi), joka sähköisen tunnistamisen ostokustannuksiin on varattu. Samalla tämä tarkoittaisi joko valtion näkökulmasta käyttäjäkohtaisen kiinteähintaisen kokonaiskustannuksen vaatimusta ja tunnistuspalvelujen tulisi keskenään sopia maksetun kokonaissumman jakautumisesta eri palveluntarjoajien kesken tai kokonaiskustannusten leikkuria, jolloin vuosittaisen

enimmäismäärän ylityttyä valtion ei enää korvaisi mitään sähköisen tunnistuksen käytöstä palvelun tarjoajille. Harkittavaksi tulisi myös digipalvelulain 6§:n perusteella vahvan sähköisen tunnistamisen käytön rajoittaminen vain niihin palveluihin, joissa sen käyttö on välttämätöntä. Näiden toimenpiteiden kautta ei saavutettaisi mitään etuja sähköisen tunnistamisen käytön yleistymiselle yksityisen sektorin palveluissa, vaan todennäköisesti kustannuspaine niiden osalta kasvaisi entisestään.

Yhtenä arviointikohteena on esitetty myös mahdollisuutta laskea VTJ-kyselyn maksua tai jopa mahdollistaa sen antamista ilmaiseksi tunnistuspalvelutarjoajille. Nykyisellään VTJ-kyselyt muodostavat merkittävän yksittäisen tunnistuspalvelujen kustannuskomponentin. VTJ-kyselyn maksuttomuus todennäköisesti alentaisi tunnistuspalvelujen hintaa. Tästä ei kuitenkaan ole varmuutta, että alentunut viranomaiskustannus siirtyisi sellaisenaan kuluttaja- tai yrityspalvelujen hinnoitteluun. Jos nykyistä sähköisen tunnistamisen toimintamallia halutaan jatkaa, ehdotus on perusteltu, jos siihen yhdistetään myös valtion näkökulmasta rajattu kustannustaso. Tässä arviomuistiossa esitetty tavoitetila siirtäisi VTJ-tiedon kuluttajan välitettäväksi, jolloin tieto olisi käytettävissä suoraan myös sähköisen tunnistamisen toimijoille.

Sähköisen ensitunnistamisen sääntely on ollut yksi keskeisiä haasteita nykyisen sähköisen tunnistamisen markkinoiden toimivuuden kannalta. Yhtenä nykyjärjestelmän kehittämiskohteena on esitetty, että tunnistamisen markkinasääntely säilyisi ennallaan, mutta valtio ottaisi suuremman roolin nimenomaisesti ensitunnistamisessa ja sen antamisesta tunnistustoimijoiden käyttöön. Käytännössä tämä tarkoittaisi joko tässä arviomuistiossa esitetyn digitaalisen henkilökortin toteutusta tai valtion toteuttamaa digitaalisen tunne asiakkaasi –palvelua (eKYC-palvelun), johon liittyvät vastuukysymykset olisivat valtion näkökulmasta hankalia.

Käytännössä esitetyn tavoitetilan toteuttaminen nykyisen sähköisen tunnistamisen toimintamallin kautta on hyvin vaikeaa tai mahdotonta ilman merkittävää puuttumista nykyiseen markkinasääntelyyn. Identiteetin hallinnan kontrollin siirtyminen tunnistuspalvelulta tunnistettavalle henkilölle muuttaa perustavalla tavalla niitä (liike)toiminnan rakenteita, joiden perusteella nykyinen lainsäädäntö on rakennettu. Tämä ei kuitenkaan poista sääntelyn markkinaehtoisuutta, mutta muuttaa markkinan kohteena olevan toiminnan nykyisestä.

III OSA: Tavoiteltavan toimintamallin keskeiset oikeudelliset kysymykset

6. Hankkeen taustalla vaikuttavan lainsäädännön nykytila

6.1. Perus- ja ihmisoikeudet

6.1.1. Perusoikeuksien kohderyhmä ja turvaaminen

Perusoikeudet kuuluvat pääsääntöisesti kaikille Suomen oikeudenkäyttöpiirissä oleville ihmisille. Joitakin vuosikymmeniä sitten katsottiin vielä, että perusoikeudet on pääsääntöisesti tarkoitettu kansalaisille³. Perusoikeusuudistuksen yhteydessä perustuslakia edeltäneen hallitusmuodon otsikointia kuitenkin muutettiin tarkoituksenmukaisesti laajentavalla tavalla. Nimike "Suomen kansalaisten yleiset oikeudet ja oikeusturva" ehdotettiin korvattavaksi nykyaikaista valtiosääntöoikeudellista kielenkäyttöä vastaavalla ja henkilöllisen soveltamisalan laajentamisen pääsääntöisesti kaikkiin Suomen oikeudenkäyttöpiirissä oleviin ihmisiin osoittavalla nimikkeellä "Perusoikeudet" (HE 309/1993 vp) Tässä hyvin laajassa kohderyhmässä perusoikeudet suojaavat henkilöä tämän syntymästä kuolemaan, vaikkakin joidenkin perusoikeuksien käyttämiselle on asetettu ikärajoituksia⁴.

Perusoikeuksilla voi olla erilaisia vaikutuksia. Säännös sisältää tavallisesti veloitteen olla loukkaamatta oikeuden sisältöä ja erityisesti perusoikeuden ydinsisällön tulee olla loukkaamaton. Osa perusoikeussäännöksistä voivat antaa henkilöille subjektiivisia oikeuksia, kun taas osa on kirjoitettu väljempään muotoon.⁵ Perusoikeuksien vaikuttavuuden näkökulmasta on kuitenkin tärkeää huomata perustuslain 22 §:n asettava velvoite: julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen.

Perusoikeussäännökset sitovat julkista valtaa sen kaikessa toiminnassa, niin lainsäädännössä, hallinnossa kuin lainkäytössä. Perusoikeuksien käytännön toteutumisen kannalta ei ole kuitenkaan riittävää, että julkinen valta pidättäytyy itse puuttumasta perusoikeuksiin. Usein perusoikeuksien tosiasiallinen toteutuminen edellyttää julkisen vallan aktiivisia toimenpiteitä, esimerkiksi yksilön perusoikeuksien suojaamiseksi ulkopuolisilta loukkauksilta tai

³ Husa, Jaakko – Pohjolainen, Teuvo: Julkisen vallan oikeudelliset perusteet: Johdatus julkisoikeuteen (2014) (Alma Verkkokirjajhyly 29.5.2020 13:25:5), s. 139.

⁴ Husa – Pohjolainen, s. 139.

⁵ Husa – Pohjolainen, s. 139.

tosiasiallisten edellytysten luomiseksi perusoikeuksien käyttämiselle. Julkisen vallan velvoite turvata perusoikeuksien ja ihmisoikeuksien toteutuminen korostaa pyrkimystä perusoikeuksien aineelliseen turvaamiseen muodollisen, menettelyvaatimuksiin liittyvän perusoikeusturvan rinnalla. (HE 309/1993 vp, s. 75)

Turvaamisvelvollisuus ulottuu perusoikeuksien ohella myös Suomea velvoittavissa kansainvälisissä sopimuksissa turvattuihin ihmisoikeuksiin. Säännös vastaa ihmisoikeussopimusten lähtökohtia ja niiden kansainvälisissä valvontaelimissä saamaa tulkintaa. Esimerkiksi Euroopan ihmisoikeussopimus edellyttää, että sopimusvaltiot takaavat jokaiselle oikeudenkäyttöpiiriinsä kuuluvalla sopimuksen turvaamat oikeudet (1 artikla). Takaamisella tarkoitetaan myös valtion tehokkaita positiivisia toimenpiteitä oikeuksien turvaamiseksi käytännössä. (HE 309/1993 vp, s. 75)

Julkiselle vallalle asetettu perusoikeuksien ja ihmisoikeuksien toteutumisen turvaamisvelvollisuus koskee myös oikeuksien toteutumista yksityisten keskinäisissä suhteissa. Käytännössä velvoite kohdistuu lähinnä lainsäätäjään, jonka tehtävänä on täsmentää yleisellä tasolla ilmaistua perusoikeutta niin, että sen vaikutus ulottuu myös yksityisiin suhteisiin. Tällä tavoin vaikuttaa esimerkiksi naisten ja miesten tasa-arvoa edistävän lainsäädännön ylläpitäminen. (HE 309/1993 vp, s. 75)

Perustuslaissa ei ole määritelty niitä keinoja, joilla julkisen vallan tulee turvaamisvelvollisuutensa toteuttaa. Keinovalinta jää kussakin tapauksessa erikseen harkittavaksi. Valittavat keinot saattavat myös vaihdella huomattavasti. Keskeisiin keinoihin kuuluvat perusoikeuden käyttöä turvaavan ja täsmentävän lainsäädännön säätäminen sekä taloudellisten voimavarojen kohdentaminen. (HE 309/1993 vp, s. 75)

Säännös perusoikeuksien turvaamisesta on kaikkia perusoikeuksia ja Suomea sitovissa kansainvälisissä ihmisoikeussopimuksissa turvattuja ihmisoikeuksia koskeva yleissäännös. Sen ohella on useissa perustuslain säännöksissä sitä täsmentäviä erityissäännöksiä. (HE 309/1993 vp, s. 75)

6.1.2. Perusoikeudet sähköisessä asiointissa

Perustuslain 21 §:n 2 momentin mukaan käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla. Kuten sanamuodosta käy ilmi, momentin luettelo hyvän hallinnon takeista ei ole tyhjentävä. Hyvään hallintoon kuuluu myös ”sellaisten menettelymuotojen

turvaaminen, jotka mahdollistavat osallistumisen ja vaikuttamisen itseä ja elinympäristöä koskevaan viranomaisen päätöksentekoon”⁶. Tätä tukevat perustuslain 2 §:n 2 momentti ja perustuslain 14 §:n 4 momentti. Perustuslain 2 §:n 2 momentin mukaan kansanvaltaan sisältyy yksilön oikeus osallistua ja vaikuttaa yhteiskunnan ja elinympäristönsä kehittämiseen.

Perustuslain 14 §:n 4 momentin mukaan julkisen vallan tehtävänä on edistää yksilön mahdollisuuksia osallistua yhteiskunnalliseen toimintaan ja vaikuttaa häntä itseään koskevaan päätöksentekoon. Tämä säännös on sisältynyt jo aiemman hallitusmuodon 11 §:ään (HE 1/1998 vp, s. 79). Säännös sisältää julkiseen valtaan kohdistuvan perustuslaillisen toimeksiannon edistää yksilön mahdollisuuksia osallistua muulla kuin perinteisillä vaalioikeuksilla yhteiskunnalliseen toimintaan ja vaikuttaa itseään koskevaan päätöksentekoon. Säännös ei täsmennä niitä keinoja, joilla julkisen vallan tulisi edistämismahdollisuutensa täyttää. Esimerkkeinä vanhan hallitusmuodon perusteluissa on kuitenkin annettu erilaisia osallistumisjärjestelmiä koskevan lainsäädännön kehittäminen. Yksilön vaikuttamismahdollisuudet voisivat toetua esimerkiksi vapaana kansalaistoimintana tai tätä tarkoitusta varten luotujen nimenomaisten mekanismien kautta. Säännös ei rajaa vaikuttamismahdollisuuksia iän perusteella vaan säännös edellyttää, että myös lapsille turvataan mahdollisuus vaikuttaa itseään koskeviin asioihin heidän kehitystään vastaavasti. (HE 309/1993 vp, s. 62)

Nyky-yhteiskunnassa digitaalisten palvelujen on katsottu mahdollistavan myös osallistumisoikeuksien toteuttamisen elinympäristöä koskevaan päätöksentekoon. Digitaalisissa palveluissa luodaan mahdollisuuksia osallistua yhteiskunnalliseen toimintaan ja vaikuttaa itseään koskevaan päätöksentekoon (HE 60/2018 vp, s. 5.) Julkisen sektorin digitaalisten palvelujen yhdenmukaisilla vaatimuksilla palvelujen tarjoamiseksi sekä palvelujen saavutettavuudella edistetään myös yleisemmin perustuslain 21 §:ssä säädettyjen hyvän hallinnon takeiden toteuttamista. Hyvään hallintoon kuuluu jokaisen oikeus saada viranomaisilta asianmukaisia palveluita. Digitaaliset palvelut ovat osa viranomaisten palveluvalikoimaa, ja palvelujen saavutettavuus kaikille on osa hyvän hallinnon toteuttamista. (HE 60/2018 vp, s. 6) Digitaalisten palveluiden on katsottu edistävän useampien perusoikeuksien toteutumista ja niitä kehittämällä voidaan edistää yhdenvertaisuutta sekä hyvän hallinnon toteuttamista yhteiskunnassa. (HE 60/2018 vp, s. 5)

Perustuslain 6 §:n mukaan ihmiset ovat yhdenvertaisia lain edessä. Ketään ei saa ilman hyväksyttävää perustetta asettaa eri asemaan sukupuolen, iän,

⁶ Mäenpää, Olli: Yleinen hallinto-oikeus, s. 95 (Alma Verkkokirjajhyly 8.5.2020 15:23:18).

alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella. Lapsia on kohdeltava tasa-arvoisesti yksilöinä, ja heidän tulee saada vaikuttaa itseään koskeviin asioihin kehitystään vastaavasti.

Yhdenvertaisuudesta johtuvia velvoitteita tarkennetaan yhdenvertaisuuslaissa (1325/2014), jota sovelletaan sekä julkisessa että yksityisessä toiminnassa. Yhdenvertaisuuslaki on yleislaki, joka koskee yhdenvertaisuuden edistämistä yleisellä tasolla ja syrjintään puuttumista yksittäistapauksissa. Yhdenvertaisuuslain 1 §:n mukaan lain tarkoituksena on edistää yhdenvertaisuutta ja ehkäistä syrjintää sekä tehostaa syrjinnän kohteeksi joutuneen oikeusturvaa saattamalla eri perusteilla ja eri elämänalueilla tapahtuva syrjintä mahdollisimman samanlaisten oikeussuojakeinojen ja seuraamusten piiriin. Yhdenvertaisuuslain 5 §:n 1 momentin mukaan viranomaisen on arvioitava yhdenvertaisuuden toteutumista toiminnassaan ja ryhdyttävä tarvittaviin toimenpiteisiin yhdenvertaisuuden toteutumisen edistämiseksi. Edistämistoimenpiteiden on oltava viranomaisen toimintaympäristö, voimavarat ja muut olosuhteet huomioon ottaen tehokkaita, tarkoituksenmukaisia ja oikeasuhtaisia.

Digitaalisilla palveluilla voidaan edistää yhdenvertaisuutta. (HE 60/2018 vp, s. 5.) Vuonna 2019 voimaan tulleella digipalvelulalla on saavutettavuusvaatimusten keinoin edistetty jokaisen mahdollisuuksia asioida itsenäisesti ilman avustajaa digitaalisten palvelujen avulla viranomaisten ja muiden palveluntarjoajien kanssa. Voimassa oleva sääntely ei edelleenkään mahdollista kaikissa tilanteissa jokaiselle mahdollisuuksia asioida tai saada tietoja viranomaisen toiminnasta digitaalisia palveluja käyttämällä (HE 60/2018 vp, s. 92).⁷

Toistaiseksi lainsäädännössä sähköistä asiointia on arvioitu ensisijaisesti siitä lähtökohdasta, että palveluita on käytettävissä ja olennaista on, miten yksilöiden oikeudet toteutetaan tässä uudessa digitaalisessa ympäristössä. Fyysiset palvelukanavat ovat edelleen olleet toiminnan lähtökohtana ja ne varmistavat viime kädessä, että yksilöiden oikeudet ja velvollisuudet toteutuvat. Tässä kontekstissa pääsy digitaalisiin palveluihin ei itsessään ole ollut perusoikeuskysymys vaan huomio on keskittynyt siihen, vaarantavatko uudet toimintamallit yksilön oikeuksia.

Siirryttäessä yhä enemmän digitaaliseen toimintamalliin on kuitenkin huomioitava, että yhteiskunnan painopiste muuttuu. Digitaaliset palvelukanavat

⁷ Huomattava, että sääntely tulee sovellettavaksi porrastetusti vuoteen 2022 mennessä.

tulevat käytetyimmiksi ja kansalaisyhteiskunta siirtyy verkkoon. Näissä olosuhteissa nousee esille myös kysymys siitä, kenellä on pääsy palveluihin ja kuka voi ottaa osaa tähän digitaaliseen yhteiskuntaan. Tällöin on myös kiinnitettävä enemmän huomiota siihen, miten luonnolliset henkilöt voivat käyttää digitaalista henkilöllisyyttä digitaalisissa palveluissa. Tarkasteltaessa yksilön perusoikeuksia vasten digitaalisen yhteiskunnan rakenteita voidaan kysyä, olisiko yksilölle turvattava mahdollisuudet ja välineet sähköiseen asiointiin julkisen vallan toimesta, osallistumisoikeuksien, hyvän hallinnon ja yhdenvertaisuuden nimissä.

Digitaalisten palvelujen käyttöoikeutta on arvioitu esimerkiksi laissa luottolaitostoiminnasta (610/2014), jolla toimeenpantiin Euroopan parlamentin ja neuvoston direktiivi 2014/92/EU, annettu 23 päivänä heinäkuuta 2014, maksutileihin liittyvien maksujen vertailukelpoisuudesta, maksutilien siirtämisestä ja mahdollisuudesta käyttää perusmaksutilejä (perusmaksutilidirektiivi). Perusmaksutilidirektiivin 15 artiklassa säädetään syrjimättömyydestä. Jäsenvaltioiden on varmistettava, etteivät luottolaitokset syrji EU:ssa laillisesti asuvia kuluttajia heidän kansalaisuutensa tai asuinpaikkansa tai minkään muun perusoikeuskirjan 21 artiklassa tarkoitetun syyn vuoksi, kun nämä kuluttajat hakevat tai käyttävät maksutiliä EU:ssa. Perusmaksutilin haltijana olemiseen sovellettavat ehdot eivät myöskään saa olla millään tavoin syrjiviä. Kuluttajien tulee saada myös perusmaksutilin käyttämiseksi tarvittavat välineet syrjimättömästi ml. verkkopankkipalvelujen käyttämiseksi tarvittavat välineet.

6.1.3. Perus- ja ihmisoikeusnäkökulma ja identiteetti

Oikeus identiteettiin tai henkilöllisyyteen johtuu yleensä muista suojatuista oikeuksista tai sisältyy niihin. Lapsen oikeuksien sopimuksessa on kuitenkin erikseen määrätty lapsen oikeudesta henkilöllisyyteen. Sopimuksen 8 artiklan mukaan:

1. Sopimusvaltiot sitoutuvat kunnioittamaan lapsen oikeutta säilyttää henkilöllisyytensä, myös kansalaisuutensa, nimensä ja sukulaissuhteensa niin kuin lainsäädännössä niistä määrätään ilman, että niihin puututaan laittomasti.
2. Milloin lapselta on laittomasti riistetty hänen henkilöllisyytensä osittain tai kokonaan, sopimusvaltioiden on annettava hänelle asianmukaista apua ja suojelua pyrkimyksensä nopeasti palauttaa lapselle hänen henkilöllisyytensä.

Vaikka kyse on lapsen oikeuksista, ei voida ajatella, että oikeus henkilöllisyyteen lakkaisi henkilön aikuistuesssa. Lapsen oikeuksien sopimus takaa lapselle pysyvän henkilöllisyyden. Sen ylläpitäminen on olennaista myös aikuisen oikeuksien näkökulmasta ja omalta osaltaan varmistaa vielä syntymättömien lasten identiteetin eheyden.

Euroopan ihmisoikeustuomioistuin on käsitellyt identiteettiin liittyviä kysymyksiä Euroopan ihmisoikeussopimuksen (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi SopS 85-86/1998) 8 artiklan näkökulmasta. Sopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhelämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalisen suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Euroopan ihmisoikeustuomioistuin on katsonut, että henkilön identiteettiä koskevat kysymykset kuuluvat yksityiselämän käsitteen keskeiseen ytimeen⁸ ja oikeus identiteettiin on keskeinen osa yksityiselämän käsitettä⁹. Vaikka 8 artikla ei sisällä suoraa viittausta henkilön nimiin, tuomioistuin on katsonut, että ne kuuluvat henkilön yksityiselämän piiriin, sillä nimi toimii henkilön identifioinnin välineenä ja muodostaa yhteyden perheeseen.¹⁰ Tapauksissa on kuitenkin ollut kyse siitä, onko valtion toiminta puuttunut sopimuksen vastaisesti tähän yksityisen elämän piiriin, esimerkiksi kieltäydyttäessä tietyn nimen rekisteröinnistä, ei henkilön oikeudesta tällaiseen yksilöivään tietoon.¹¹ Henkilötietojen rekisteröinti on myös tullut 8 artiklan piiriin erityisesti transseksuaalien muutetun sukupuolen rekisteröinnissä väestötietojärjestelmään¹². Tuomioistuin on useassa tapauksessa katsonut, että henkilö voi vedota 8 artiklaan ja yksityiselämän piiriin loukkaukseen tapauksissa, joissa hänen sukupuolen muutostaan ei tunnusteta juridisesti¹³. Suomalaista väestötietojärjestelmää koskeneessa tapauksessa tunnustettiin, että kysymys henkilötunnukseen sisältyvän sukupuolitiedon muuttamisesta oli

⁸ Heikkilä, Satu – Hirvelä Päivi: Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 642. (Alma Verkkokirjahylly 7.5.2020 09:36:37)

⁹ *Menesson v. France*, no. 65192/11, 26.6.2014.

¹⁰ *Guillot v. France*, no. 22500/93, 24.10.1996, para 19; *Stjerna v. Finland*, no. 18131/91, 25.11.1994, para 37; *Johansson v. Finland*, no. 10163/02, 6.9.2007, para 28.

¹¹ *Guillot v. France*, no. 22500/93, 24.10.1996; *Stjerna v. Finland*, no. 18131/91, 25.11.1994; *Johansson v. Finland*, no. 10163/02, 6.9.2007.

¹² Heikkilä – Hirvelä, s. 642.

¹³ *Hämäläinen v. Finland* [GC], no. 37359/09, 16.7.2014, para 59.

hakijan yksityiselämän suojan piirissä¹⁴. Identiteetin piiriin on katsottu kuuluvan myös henkilön etninen alkuperä ja väestötietojärjestelmään merkitty vakituinen asuinpaikka.¹⁵

Henkilön identiteettiin liittyviä ihmisoikeus- ja perusoikeuskysymyksiä käsitellään yleisesti henkilön ominaispiireisiin, perhesuhteisiin ja henkilökohtaisiin valintoihin liittyvien kysymysten kautta. Esimerkiksi voidaan tarkastella henkilön oikeutta siihen, että hänen tosiasialliset ihmissuhteensa tunnustetaan osaksi valtion vahvistamaa ja ylläpitämää identiteettiä. Vähemmän on kuitenkin analysoitu sitä, mikä on henkilön oikeus itse identiteettiin. Tämä voi osin johtua siitä, että henkilön yksilöiminen on kehittyneelle yhteiskuntarakenteelle niin välttämätöntä, että oikeus lähtökohtaisesti toteutuu.

Siirryttäessä yhä enemmän sähköisiin palveluihin tämä kysymys perustavanlaatuisesta oikeudesta identiteettiin tulee uudelleen ajankohtaiseksi. Arvioitaessa valtion toimintamahdollisuuksia tai –velvoitteita digitaalisen identiteetin piirissä on huomioitava myös identiteetin ihmisoikeusnäkökulmat sekä perustuslain 22 §:ssä säädetty julkisen vallan velvollisuus turvata perusoikeuksien ja ihmisoikeuksien toteutuminen. On kysyttävä, onko yksilöllä oikeus luotettavaan ja pysyvään digitaaliseen identiteettiin, joka mahdollistaa toiminnan digitaalisessa yhteiskunnassa.

6.2. Julkisen vallan käyttö, julkinen tehtävä ja julkinen hallintotehtävä

Perustuslain 2 §:ssä säädetään, että julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Julkisen vallan käyttäjällä tulisi aina olla viime kädessä eduskunnan säätämään lakiin palautettavissa oleva toimivaltaperuste. Esimerkiksi viranomaisilla ei siten voisi olla sellaista julkisen vallan käyttämistä tarkoittavaa toimivaltaa, jolla ei olisi nimenomaista tukea oikeusjärjestyksessä. (HE 1/1998 vp, s. 74)

Julkisen vallan käsite on laajempi kuin valtiiovallan käsite. Julkisen vallan käyttöä ei ole palautettavissa yksinomaan valtion toiminnaksi. Suomessa esimerkiksi kunnat, kuntayhtymät ja välillisen julkishallinnon organisaatiot, kuten Kansaneläkelaitos ja julkisoikeudelliset yhdistykset käyttävät merkittävää julkista valtaa. Annettaessa julkista valtaa valtiokoneiston ulkopuolelle on kuitenkin varmistettava oikeusvaltioperiaatteen ulottuminen myös tähän toimintaan. (HE 1/1998 vp, s. 74)

¹⁴ *Hämäläinen v. Finland* [GC], no. 37359/09, 16.7.2014, para 64.

¹⁵ Heikkilä – Hirvelä, s. 642.

Julkisen vallan käytön piiriin luetaan sellaiset norminanto-, lainkäyttö- ja hallintopäätökset, jotka tehdään yksipuolisesti ja joiden vaikutus ulottuu yksityisiin oikeussubjekteihin. Toisena keskeisenä julkisen vallan käytön muotona voidaan pitää välitöntä voimakeinojen käyttämistä ulkopuolisiin nähden. Julkisen vallan käytön ydinalueeseen kuuluvat esimerkiksi poliisitoimi, tuomioistuinlaitoksen lainkäyttötoiminta, ulosottotoimi ja verotus sekä viranomaisen oikeus määrätä ulkopuolisille virallisia seuraamuksia (esim. uhkasakko). Julkisen vallan alaa ei voida kuitenkaan tyhjentävästi määritellä, vaan sitä voidaan tarpeen mukaan ja perustuslain sallimissa rajoissa lainsäädännöllä laajentaa tai supistaa. Julkisen vallan väärinkäyttöä vastaan on perustuslaissa luotu useita takeita. Keskeinen merkitys on tältä osin erityisesti julkisen vallan käyttämiselle asetettavia vaatimuksia. (HE 1/1998 vp, s. 74)

Hallintolain 2 §:n 3 momentin mukaan hallintolakia sovelletaan valtion liikelaitoksissa, julkisoikeudellisissa yhdistyksissä sekä yksityisissä niiden hoitaessa julkisia hallintotehtäviä. Hallintolain perustelujen mukaan julkisiin hallintotehtäviin liittyy usein oikeus käyttää julkista valtaa eli hallintopäätösten tekemistä sekä asian ratkaisemista välittömästi palvelevia valmistelu- ja täytäntöönpanotoimia. Julkisen vallan käyttämistä on myös yksityisiin kohdistuvien käskyjen ja kieltojen antaminen. Keskeistä on myös, että tehtävä perustuu lailla tai lain nojalla annettuun julkiseen toimeksiantoon. Hallintolaissa tarkoitettu julkisen hallintotehtävän käsite kattaa myös merkittävän julkisen vallan käytön, esimerkiksi voimakeinojen käyttämisen tai muun puuttumisen yksilön perusoikeuksiin. (HE 72/2002 vp, s. 48)

Julkishallinnon keskeiset tehtävät voidaan ryhmitellä neljään sisällöltään ja luonteeltaan erilaiseen pääryhmään:

1. Hallinnollinen sääntely ja valvonta
2. Julkisten palvelujen tuottaminen ja järjestäminen
3. Hallinnon ylläpito ja johtaminen
4. Viranomaisen taloudellinen toiminta.

Ryhmittely ei kuitenkaan ole täysin tarkkarajainen, vaan usein palvelujen tuottamiseen liittyy eri pääryhmien mukaista toimintaa. Julkishallinnon tehtävien perusrahoitus perustuu verotukseen ja budjettivaroihin, sillä tehtävien päätarkoitus on yleisen edun toteuttaminen, ei voiton tuottaminen.¹⁶

¹⁶ Mäenpää: Yleinen hallinto-oikeus, s. 35

Julkisen hallintotehtävän käsite saa sisältönsä perustuslain (731/1999) 124 §:stä.¹⁷ Perustuslaissa säädetään julkisen hallintotehtävän antamisesta muulle kuin viranomaiselle. Julkisella hallintotehtävällä perustuslaissa tarkoitetaan verraten laajaa hallinnollisten tehtävien kokonaisuutta, johon kuuluu esimerkiksi lakien toimeenpanoon sekä yksityisten henkilöiden ja yhteisöjen oikeuksia, velvollisuuksia ja etuja koskevaan päätöksentekoon liittyviä tehtäviä. (HE 1/1998 vp, s. 179) Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. Kyseinen pykälä edellyttää, että siirrettäessä julkinen hallintotehtävä viranomaiskoneiston ulkopuoliselle taholle huolehditaan säännösperusteisesti perusoikeuksien, oikeusturvan ja hyvän hallinnon vaatimusten turvaamisesta tässä toiminnassa. (HE 72/2002 vp, s. 49)

Julkisen hallintotehtävän käsite on keskeinen myös tarkasteltaessa valtionhallinnon mahdollisuuksia tuottaa digitaalisen henkilöllisyyden ratkaisuja ja tähän liittyviä tunnistuspalveluita. Kansallisesti kysymystä on tunnistuspalvelujen osalta tarkasteltu erityisesti tunnistuslain yhteydessä. Perustuslakivaliokunta on katsonut liiketaloudellisten palvelujen luonteen tunnistamismarkkinoilla siinä määrin etäännyneen julkiseen hallintotehtävään liitettävistä ominaispiirteistä, että toimintaa ei pidetä julkisen hallintotehtävän hoitamisena. Valokunta kuitenkin korosti vahvan sähköisen tunnistamisen välineillä ja varmennetoiminnalla olevan merkitystä erilaisissa oikeustoimissa osapuolten aseman kannalta ja siten luottamusverkostoa koskevan sääntelyn olevan tarpeen (PeVL 16/2009). Perustuslakivaliokunta on sittemmin viitannut aiempaan kantaansa siitä, että sähköisen tunnistamisen välineiden tarjoamista ei tulisi pitää julkisena hallintotehtävänä (PeVL 74/2018 vp).

Ennen vuonna 2009 annettua kannanottoa perustuslakivaliokunta oli katsonut varmennetoiminnan sellaisenaan olevan perustuslain 124 §:n mukaista toimintaa, muttei pitänyt ongelmallisena sitä, että muutkin kuin viranomaiset voivat lain nojalla sitä harjoittaa (PeVL 2/2002). Tuolloin valiokunta katsoi, että varmennetoiminnalla on merkitystä sähköisen liiketoiminnan ja muun asioinnin osapuolten oikeusaseman kannalta ja siten se on rinnastettavissa viranomaisen myöntämään henkilötodistukseen. Tehtävässä ei aiemminkaan katsottu olevan ensisijaisesti kysymys yksilön etua tai oikeutta koskevasta päätöksenteosta (PeVL 2/2002 vp).

¹⁷ Niemivuo, Matti – Keravuori-Rusanen, Marietta – Kuusikko, Kirsi: Hallintolaki (2010), s. 110.

On huomattava, että perustuslakivaliokunnan kannanotot ovat keskittyneet siihen, onko ehdotettu sähköisten allekirjoitusten ja sittemmin luottamusverkoston sääntely yhdenmukainen perustuslain 124 §:n kanssa ja voidaanko toimintaa ehdotetun sääntelyn perusteella harjoittaa yksityisellä sektorilla perustuslain estämättä. Valiokunta ei ole ottanut kantaa siihen mahdollisuuteen, että jonkin erikseen säännellyn tunnistuspalvelun tuottaminen olisi julkinen hallintotehtävä tai sisältäisi julkisen vallan käyttöä.

Lisäksi on huomattava, että Digi- ja väestötietoviraston (DVV) kansalaisvarmenteita koskeva palveluntarjonta on katsottu julkisen vallan käytöksi. Vaikka vahvan sähköisen tunnistamisen palvelun ja varmenteiden tarjonta on katsottu yksityiseksi palveluntarjonnaksi, joihin ei ole tarvetta liittää perustuslain 124 §:n mukaista julkisen vallan käyttöä, ei kansalaisvarmenteen tuottamista ole rajattu julkisen hallintotehtävän ulkopuolelle. Kansalaisvarmenteen tuottamisesta säädetään erikseen siten, että se on DVV:n viranomaistoimintaa. (HE 36/2009 vp, s.87)

6.3. Yhdenvertaisuus ja henkilön aseman perusteella huomioitavat erityiskysymykset

6.3.1. Yhdenvertaisuuslaki ja tasa-arvo

Yhdenvertaisuuslain tarkoituksena on edistää yhdenvertaisuutta ja ehkäistä syrjintää. Yhdenvertaisuuden edistämiseksi viitataan yhdenvertaisuuden toteutumiseen käytännössä ja siten toimenpiteisiin, joilla pyritään ihmisten yhdenvertaisen kohtelun toteuttamiseen ja muihin verrattuna heikommassa asemassa olevien aseman parantamiseen tosiasiallisen yhdenvertaisuuden saavuttamiseksi. Lakia sovelletaan sen 2 §:n mukaan kaikessa julkisessa ja yksityisessä toiminnassa. Lakia ei kuitenkaan sovelleta yksityis- eikä perhe-elämän piiriin kuuluvaan toimintaan eikä uskonnonharjoitukseen. Lisäksi osaa sen säännöksistä sovelletaan vain tiettyihin toimijoihin, esimerkiksi viranomaisiin ja työnantajiin. Lisäksi on huomattava, että sukupuoleen perustuvan syrjinnän kiellosta ja sukupuolten välisen tasa-arvon edistämisestä säädetään naisten ja miesten välisestä tasa-arvosta annetussa laissa. Yhdenvertaisuuslakia voidaan kuitenkin tasa-arvolain lisäksi soveltaa tilanteisiin, joissa on kysymys paitsi sukupuoleen perustuvasta myös yhdenvertaisuuslaissa kiellettävästä syrjinnästä (*moniperusteinen syrjintä*).

Viranomaisella on yhdenvertaisuuslain 5 §:n mukaan velvollisuus edistää yhdenvertaisuutta. Viranomaisen tulisi esimerkiksi arvioida sitä, miten yhdenvertaisuusnäkökulma on otettu huomioon viranomaisen tehtäviin kuuluvien toimintojen järjestämisessä samoin kuin siihen, miten sen toiminta on tosiasiallisesti vaikuttanut syrjinnän vaarassa olevien ryhmien asemaan.

Viranomaisen tulisi toimialallaan arvioida yhdenvertaisuuden toteutumista esimerkiksi asioiden valmistelussa, päätöksenteossa, hallintotoiminnassa ja -tavoissa, ja tiedotuksessa. Laajoissa tai muutoin merkitykseltään tärkeissä hankkeissa olisi arvioitava, vaikuttaako hanke syrjinnän vaarassa olevien ryhmien oikeuksiin, velvollisuuksiin tai asemaan. Viranomaisen olisi arvioinnin lisäksi ryhdyttävä tarvittaviin toimenpiteisiin yhdenvertaisuuden toteutumisen edistämiseksi. Tarvittavilla toimenpiteillä viitataan sellaisiin käytännöllisiin keinoihin yhdenvertaisuuden toteutumisen edistämiseksi, joihin arvioinnissa havaitut kehittämiskohteet ja mahdolliset ongelmat antavat aiheita. Edistämisessä olisi usein kyse toimenpiteistä, joilla julkiset palvelut pyritään järjestämään syrjinnän vaarassa olevien ryhmien tarpeet paremmin huomioon ottavalla tavalla. Esimerkiksi sähköisiä palveluita suunniteltaessa ja käyttöön otettaessa tulisi varmistaa palveluiden soveltuvuus vanhuksille. (HE 19/2014 vp)

Syrjinnän kiellosta säädetään lain 8 §:ssä. Ketään ei saa syrjiä iän, alkuperän, kansalaisuuden, kielen, uskonnon, vakaumuksen, mielipiteen, poliittisen toiminnan, ammattiyhdistystoiminnan, perhesuhteiden, terveydentilan, vammaisuuden, seksuaalisen suuntautumisen tai muun henkilöön liittyvän syyn perusteella. Syrjintä on kielletty riippumatta siitä, perustuuko se henkilöä itseään vai jotakuta toista koskevaan tosiseikkaan tai oletukseen. Syrjintäperusteiden luettelo ei ole tyhjentävä.

Syrjintä on välitöntä, jos jotakuta oikeudettomasti kohdellaan henkilöön liittyvän syyn perusteella epäsuotuisammin kuin jotakuta muuta on kohdeltu, kohdellaan tai kohdeltaisiin vertailukelpoisessa tilanteessa. Epäsuotuisalla kohtelulla viitattaisiin sellaiseen menettelyyn, joko tekoon tai laiminlyöntiin, jolla menettelyn kohde asetetaan muihin nähden huonompaan asemaan. Kyse voi siten olla esimerkiksi rajoitusten, vaatimusten, rasitteiden tai velvoitteiden asettamisesta vain tietyille henkilöille tai henkilöryhmälle samoin kuin esimerkiksi jonkin yleisesti saatavilla olevan etuuden, palvelun tai oikeuden epäämistä tai rajoittamisesta.

Syrjintä on välillistä, jos näennäisesti yhdenvertainen sääntö, peruste tai käytäntö saattaa jonkun muita epäedullisempaan asemaan henkilöön liittyvän syyn perusteella, paitsi jos sääntö, peruste tai käytäntö perustuu lakiin taikka sillä muutoin on hyväksyttävä tavoite ja tavoitteen saavuttamiseksi käytetyt keinot ovat asianmukaisia ja tarpeellisia. Sääntö, peruste tai käytäntö ei olisi syrjivä, jos se perustuu lakiin tai sillä muutoin on hyväksyttävä tavoite ja tavoitteen saavuttamiseksi käytetyt keinot ovat asianmukaisia ja tarpeellisia. Syrjintää ei ole sellainen oikeasuhtainen erilainen kohtelu, jonka tarkoituksena

on tosiasiallisen yhdenvertaisuuden edistäminen taikka syrjinnästä johtuvien haittojen ehkäiseminen tai poistaminen (HE 19/2014 vp)

Erilainen kohtelu voi 10 §:n mukaan olla oikeutettua, jos se perustuu joko lakiin tai muuhun hyväksyttävään perusteeseen. Lainsäädännölle on ominaista, että se kohtelee hyväksyttävien yhteiskunnallisten päämäärien vuoksi ihmisiä eri tavoin pyrittäessä esimerkiksi eri ryhmien tarpeita vastaavaan ja kulloisenkin yhteiskuntakehityksen vaatimaan sääntelyyn. Lainsäädäntöön perustuvien erilaisten erotteluiden hyväksyttävyyys perustuslain 6 §:n 2 momentin kannalta arvioidaan jo lakeja säädettäessä. (HE 19/2014 vp) Yllä kuvatusti lailla säätäminen ei luonnollisesti poista tai kevennä viranomaisen velvollisuutta huolehtia yhdenvertaisuuden toteutumisesta. Lakia säädettäessä olisi tarkasti arvioitava vaikuttaako hanke syrjinnän vaarassa olevien ryhmien oikeuksiin, velvollisuuksiin tai asemaan ja huomioitava viranomaisen velvollisuus toiminnassaan edistää yhdenvertaisuuden toteutumista.

Yhdenvertaisuuslaki sisältää myös erityisen säännöksen vammaisten ihmisten yhdenvertaisuuden edellyttämistä kohtuullisista mukautuksista. Viranomaisen sekä tavaroiden tai palvelujen tarjoajan on tehtävä asianmukaiset ja kulloisessakin tilanteessa tarvittavat kohtuulliset mukautukset, jotta vammaisen henkilö voi yhdenvertaisesti muiden kanssa asioida viranomaisissa sekä saada koulutusta, työtä ja yleisesti tarjolla olevia tavaroita ja palveluita samoin kuin suoriutua työtehtävistä ja edetä työuralla. Kohtuullisilla mukautuksilla tarkoitetaan YK:n vammaisyleissopimuksen mukaan tarvittaessa yksittäistapauksissa toteutettavia tarpeellisia ja asianmukaisia muutoksia ja järjestelyjä, joilla ei aiheuteta suhteetonta tai kohtuutonta rasitetta, ja joilla varmistetaan vammaisten ihmisten mahdollisuus nauttia tai käyttää kaikkia ihmisoikeuksia ja perusvapauksia yhdenvertaisesti muiden kanssa. Yhdenvertaisuuslaki ei edellytä, että olosuhteet, joissa esimerkiksi palveluja tarjotaan, ovat kohtuullisten mukautusten tekemisen jälkeen vammaisille ihmisille täsmälleen samanlaiset kuin muille asiakkaille. Olennaista on, että palvelut tulevat mukautuksilla vammaisten ihmisten saataville. Kohtuulliset mukautukset on käsitteellisesti erotettava yleis- ja pysyväisluonteisista esteettömyystoimenpiteistä.

Naisten ja miesten välisestä tasa-arvosta annetun lain (609/1986) tarkoituksena on estää sukupuoleen perustuva syrjintä ja edistää naisten ja miesten välistä tasa-arvoa sekä tässä tarkoituksessa parantaa naisten asemaa erityisesti työelämässä. Lain tarkoituksena on myös estää sukupuoli-identiteettiin tai sukupuolen ilmaisuun perustuva syrjintä.

Lain 6 c §:n mukaan viranomaisten tulee ennaltaehkäistä sukupuoli-identiteettiin tai sukupuolen ilmaisuun perustuvaa syrjintää tavoitteellisesti ja suunnitelmallisesti. Välitön ja välillinen syrjintä sukupuolen perusteella on kielletty. Syrjinnällä tarkoitetaan naisten ja miesten asettamista eri asemaan sukupuolen perusteella; eri asemaan asettamista raskaudesta tai synnytyksestä johtuvasta syystä; sekä eri asemaan asettamista sukupuoli-identiteetin tai sukupuolen ilmaisun perusteella.

Yhdenvertaisuus ja tasa-arvokysymykset on huomioitava kehitettäessä digitaalista henkilöllisyyttä sekä identiteettiratkaisuun liittyvää tunnistusvälinettä. Henkilön asema voi muodostaa tilanteen, jossa yleisesti järjestetyt palveluratkaisut eivät kata kaikkien loppukäyttäjien tarpeita. Tällaisia henkilön aseman perusteella huomioitavia erityiskysymyksiä ovat esimerkiksi vajaavaltaisiin, vammaisuuteen, työntekijöihin sekä ulkomaan kansalaisiin liittyvät kysymykset.

6.3.2. Vajaavaltaisia henkilöitä koskevat erityiskysymykset

Vajaavaltainen on määritelty laissa holhustoimesta (442/1999, jäljempänä holhustoimilaki). Lain mukaisesti vajaavaltaisella tarkoitetaan alle 18-vuotiasta henkilöä (alaikäinen) ja sellaista 18 vuotta täyttänyttä henkilöä (täysiikäinen), joka on julistettu vajaavaltaiseksi. Yleensä hallintomenettelykelpoisuus puuttuu vajaavaltaiselta ja hänen puolestaan puhevaltaa käyttää huoltaja, edunvalvoja tai muu laillinen edustaja. Vajaavaltaisella on kuitenkin oikeus käyttää yksinään puhevaltaa asiassa, joka koskee hänen valitsemaansa tuloa tai varallisuutta (Hallintolain 14.1 §). Täysiikäinen vajaavaltainen käyttää itse yksin puhevaltaa henkilöään koskevassa asiassa, jos hän kykenee ymmärtämään asian merkityksen (Hallintolain 14.2 §). Kun asia koskee viisitoista vuotta täyttänyttä alaikäistä, hänellä ja hänen huoltajallaan tai muulla laillisella edustajallaan on kummallakin oikeus erikseen käyttää puhevaltaa asiassa, joka koskee alaikäisen henkilöä taikka henkilökohtaista etua tai oikeutta (Hallintolain 14.3 §). Tällaisia asioita voivat olla muun muassa alaikäisen oppivelvollisuutta sekä terveydenhoitoa koskevat asiat.¹⁸

Henkilöä voi edustaa myös edunvalvoja, jonka asemasta on säädetty muun muassa holhustoimilaissa, edunvalvontavaltuutuksesta annetussa laissa (648/2007) sekä hallintolain 15 §:ssä. Edunvalvontavaltuutuksella valtuutettu (kuten edunvalvoja) voidaan oikeuttaa edustamaan valtuuttajaa tämän omaisuutta koskevissa ja muissa taloudellisissa asioissa.

¹⁸ Mäenpää Olli: Hallintolaki ja hyvän hallinnon takeet, 2008, s. 122

Edunvalvonnan osalta voidaan pitää sähköisen asioinnin ongelmana tilanteita, joissa sekä päämiehellä että edunvalvojalla on puhevalta. Näissä tilanteissa sähköisen asioinnin käytön edellytykset voivat olla toiminnallisuuksiltaan haasteellisia, jos jonkin toimenpiteen suorittamiseen tarvitaan sähköisessä asiointipalvelussa sekä päämiehen että edunvalvojan hyväksyntää. Tällaisissa tilanteissa sekä edunvalvoja että päämies joutuvat tekemään esimerkiksi hyväksymistoimenpiteen sähköisessä asiointipalvelussa erikseen.¹⁹ Edunvalvonnassa olevalla henkilöllä ei välttämättä ole mahdollista saada omia henkilökohtaisia tunnistusvälineitä, jolloin sellaiset tilanteet, joissa hän voisi toimia itse omassa asiassaan viranomaisessa ei käytännössä ole mahdollista sähköisissä asiointipalveluissa.

Alaikäisen oikeus vaikuttaa itseään koskeviin asioihin johtaa perustuslain 6 §:n 3 momentista, jonka mukaan lapsia on kohdeltava tasa-arvoisesti yksilöinä ja heidän tulee saada vaikuttaa itseään koskeviin asioihin kehitystään vastaavasti. Esimerkiksi lastensuojelulain (417/2007) 20-21 §:n mukaan lapsen toivomukset ja mielipide on otettava huomioon lapsen iän ja kehitystason edellyttämällä tavalla. 12 vuotta täyttänyt lapsi voi käyttää huoltajan tai muun laillisen edustajan ohella erikseen puhevaltaansa itseään koskevassa lastensuojeluasiassa. Tuotettaessa sähköisiä palveluita tulisi myös huomioida alaikäisen mahdollisuus hoitaa itsenäisesti itseään koskevia asioita.

Vahvan sähköisen tunnistuspalvelun tarjoajat tarjoavat erilaisiin riskiarvioihin perustuen tunnistusvälineitä alaikäisille. Osa välineiden tarjoajista ovat määrittäneet alaikärajoja, jota nuoremmille henkilöille ei anneta, vaikka käytettävissä olisi huoltajan antama suostumus tunnistusvälineen hankintaan. Pääsääntöisesti vahvaa sähköistä tunnistamista edellyttävissä asioissa alaikäistä edustaa eli digitaalista palvelua käyttää tämän puolesta huoltaja.²⁰

Digipalvelulaissa on säädetty tilanteista, joissa vahvaa sähköistä tunnistusvälinettä tulisi käyttää. Laissa on vahvan sähköisen tunnistamisen käyttövelvoite, joka ulottuu myös oppilashuoltoon liittyviin digitaalisiin palveluihin, vaikuttaa lasten asemaan käyttää kyseisiä palveluita. Oppilashuoltoon liittyvät palvelut ja niiden käyttömahdollisuudet ovat kuitenkin oppilaan oikeuksien toteutumisen kannalta merkittäviä. Digitaalisten palvelujen käyttö lisää lasten ja erityisesti nuorten mahdollisuuksia saada itseään koskevia tietoja ja osallistua itseä koskevaan päätöksentekoon. (HE 60/2018 vp, s.38)

¹⁹ Voutilainen Tomi: Sähköisen identiteetin käytöstä julkisessa hallinnossa, Edilex 2008/8, s.9.

²⁰ Sähköinen tunnistaminen - Selvitys nykytilasta sekä kehittämistarpeista, Valtiovarainministeriön julkaisuja 2019:20, s. 28.

6.3.3. Vammaisia henkilöitä koskevat erityiskysymykset

Yhdenvertaisuuslain 8 § kieltää henkilön syrjinnän vammaisuuden perusteella. Vammaisuudelle ei ole olemassa yksiselitteistä oikeudellista määritelmää, vaan sille on eri laeissa annettu erilaisia määritelmiä. YK:n vammaisten henkilöiden oikeuksien yleissopimuksen 1 artiklan mukaan vammaisiin henkilöihin kuuluvat ne, joilla on sellainen pitkäaikainen ruumiillinen, henkinen, älyllinen tai aisteihin liittyvä vamma, joka vuorovaikutuksessa erilaisten esteiden kanssa voi estää heidän täysimääräisen ja tehokkaan osallistumisensa yhteiskuntaan yhdenvertaisesti muiden kanssa. Vammaisuus voi olla syntyperäistä, taikka se voi johtua esimerkiksi tapaturmasta tai onnettomuudesta. (HE 19/2014 vp)

Yhdenvertaisuus ei kuitenkaan tarkoita sitä, että kaikille tarjota palvelua samalla tavalla, vaan kaikille tarjotaan mahdollisuudet saada samanlaista palvelua erilaisin keinoin. Saavutettavien digitaalisten palvelujen avulla pystytään merkittävästi edistämään varsinkin erityisryhmiin kuuluvien henkilöiden itsemääräämisoikeuden toteutumista ja parantamaan heidän toimintaedellytyksiä viranomaisasioinnissa. (HE 60/2018 vp, s. 7)

Hallintolain säännöksen perusteluiden (HE 72/2002 vp, s. 57) mukaan julkisia palveluja järjestettäessä tulee kiinnittää huomiota palvelujen riittävyteen ja saatavuuteen sekä hallinnossa asioivan valinnanvapauteen. Palvelujen saatavuutta ei tulisi rajoittaa ilman asiallisesti hyväksyttäviä perusteita. Myös hallinnossa asioivan itsemääräämisoikeutta ja toimintaedellytyksiä viranomaisasioinnissa olisi mahdollisuuksien mukaan pyrittävä edistämään.

Saavutettavuusdirektiivituli voimaan 22 päivänä joulukuuta 2016 ja se saatettiin voimaan digipalvelulain nojalla. Direktiivin tavoitteena on edistää saavutettavuuden sisämarkkinoita yhdenmukaistamalla julkisen sektorin elinten verkkosivustojen ja mobiilisovellusten saavutettavuusvaatimuksia sekä parantaa julkisen sektorin elinten palvelujen ja mobiilisovellusten saavutettavuutta käyttäjien, erityisesti vammaisten henkilöiden, parissa. Direktiivissä on jäsenvaltioita velvoittavat säännökset, joilla varmistetaan, että julkisen sektorin elinten verkkosivustot ja mobiilisovellukset täyttävät direktiivissä säädetyt saavutettavuusvaatimukset. Verkkosivustolla tarkoitetaan käytännössä tietoverkon yli erilaisilla päätelaitteilla käytettävää palvelua, joka voi sisältää myös siirtymiä toiseen palveluun, esimerkiksi käyttäjän tunnistamista varten (HE 60/2018, vp s.13).

Digipalvelulain valmistelussa on arvioitu, että erityisesti niiden organisaatioiden, joiden asiointiprosessit ovat sidoksissa julkiseen hallintoon laajemmissa palvelukokonaisuuksissa, verkkosivustoihin tulisi soveltaa samoja

vaatimuksia kuin julkisen sektorin organisaatioihin. Tämä on tärkeää, jotta erityisesti vammaiset ja muut erityisryhmiin kuuluvat henkilöt voisivat hoitaa asiointinsa mahdollisimman itsenäisesti ilman, että organisaatioihin sovellettavat erilaiset vaatimukset estäisivät tosiasiaissa palvelujen käytön. (HE 60/2018, vp s.28)

Digipalvelulain saavutettavuusvaatimuksia sovelletaan tunnustuslain 12 §:ssä tarkoitettuun rekisteriin merkittyjen tunnustuspalvelun tarjoajien tunnustuspalveluihin julkisen sektorin palveluissa, joissa edellytetään sähköistä tunnistamista tai osana prosessia maksamista, ei voida toteuttaa kokonaisprosessina saavutettavaa, jos lainsäädännöllä ei voida varmistaa, että kaikkiin palveluprosessin osiin sovelletaan samoja saavutettavuusvaatimuksia (HE 60/2018 vp, s. 23).

Käytännössä siis nykysäätelyn mukaisesti yksityisten toimijoiden tunnistusvälineiden tulee täyttää saavutettavuusvaatimukset ja luottolaitoslain mukaan sähköisen tunnistamisen palveluita tarjotessaan talletuspankin tulee kohdella kaikkia asiakkaita yhdenvertaisesti ja syrjimättömästi. Talletuspankki saa kieltäytyä perusmaksutilin avaamisesta ja perusmaksutiliin liittyvien maksupalveluiden tarjoamisesta vain rahanpesun ja terrorismin rahoittamisen estämisestä annetusta laista (444/2017) tai eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämistä annetusta laista (659/1967) johtuvasta syystä.

6.3.4. Työntekijöitä koskevat erityiskysymykset

Yhtenä kokonaisuutena digitaalisen henkilöllisyyden hallinnassa on arvioitava myös niitä luonnollisia henkilöitä, jotka työntekijän ominaisuudessa tunnistautuvat organisaation puolesta sähköisiin asiointipalveluihin. Kun henkilö toimii yrityksen tai yhteisön palvelussa tai sen lukuun, on hän aina tiettyssä roolissa, jonka perusteella hänellä on käyttövaltuus asiointiin. Käyttöoikeus määrittää esimerkiksi tietojärjestelmiin, josta henkilön oikeus asiointiin voidaan tarkistaa. Henkilön kelpoisuus voi määräytyä myös oikeushenkilön virallisessa asemassa (orgaaniasema) toimimisen perusteella, jolloin hänellä on oikeus toimia oikeushenkilön edustajana ja käyttää sen puolesta puhevaltaa viranomaisissa.²¹

Julkishallinnon sähköisiä asiointipalveluja ei ole rajattu koskemaan ainoastaan luonnollisten henkilöiden palveluja, vaan palveluja tarjotaan yhtä lailla yrityksille yhä enenevässä määrin. Suomi.fi-tunnistuksen kautta jokaisen

²¹ Voutilainen (2008), s. 9-10.

tunnistautujan on kuitenkin käytettävä joko henkilökohtaisia pankkitunnuksiaan taikka henkilökorttia. Mikäli työnantaja ei tarjoa esimerkiksi organisaatiokorttia työntekijöiden tunnistamiseksi, tulee työntekijöiden käyttää omia henkilökohtaisia pankkitunnuksiaan taikka mobiilivarmennetta tunnistautuessaan organisaation puolesta sähköisiin palveluihin. Käytännössä henkilön edustaessa organisaatiota, ei hän voi kieltäytyä tunnistautumasta omilla henkilökohtaisilla tunnistusvälineillään, mikäli hän haluaa tosiasiallisesti hoitaa työtehtäviään.

Digi- ja väestötietovirasto on tuottanut KATSO -palvelua tukipalvelulain nojalla, jossa erillisellä KATSO -tunnisteella viranomainen tai muu julkista tehtävää hoitava voi julkista tehtävää hoitaessaan tunnistaa organisaation ja sitä edustavan henkilön. KATSO -palvelu on kuitenkin päättynyt ja se on korvattu asiointivaltuuspalvelulla sekä tunnistuspalvelulla. Näiden osalta jatkossa kaikki yrityksen puolesta asioivat luonnolliset henkilöt tarvitsevat julkishallinnon sähköisiin asiointipalveluihin tunnistautumiseen joko varmennekorttia, mobiilivarmennetta taikka henkilökohtaisia pankkitunnuksia. Organisaation edustajalle ei siten jää mahdollisuutta tunnistautua julkishallinnon asiointipalveluihin muutoin kuin käyttämällä omia henkilökohtaisia tunnistusvälineitään, ellei organisaatiossa hyödynnetä organisaatiovarmennekortteja.

6.3.5. Ulkomaan kansalaisia koskevat erityiskysymykset

Henkilötunnuksen uudistamista pohtineen työryhmän loppuraportista²² käy ilmi, että yhteiskunnassa on esimerkiksi kansainvälisen muuttoliikkeen vuoksi paljon henkilöitä, jotka pitää yksilöidä, mutta joilla ei ole henkilötunnusta. Samaan aikaan teknologinen kehitys on mahdollistanut asioinnin ilman henkilökohtaista käyntiä fyysisessä toimipisteessä, jolloin erityisesti ulkomailla asuvien suomalaisten ja myös ulkomaalaisten henkilöiden yksilöinti tulisi olla mahdollista digitaalisessa asiointiprosessissa. Työryhmän ehdotuksilla on näin ollen yhteys myös sähköisen tunnistamisen kehittymiseen.

Maahantulovaiheen sujuvuus on olennainen osa kansainvälisten osaajien houkuttelua. Työn hakeminen ulkomailta käsin on haasteellista, sillä esimerkiksi Työmarkkinatori -palvelun käyttö edellyttää vahvaa tunnistautumista. Maassa jo oleskelevien ulkomaalaisten tunnistautumiseen liittyvät haasteet on niin ikään oleellista huomioida digitaalisen tunnistautumisen vaihtoehtoja selvitettyä. Tältä osin on kuitenkin huomioitava myös se, miltä osin ongelmia voitaisiin lieventää tarkastelemalla

²² HETU-uudistuksen loppuraportti (Valtiovarainministeriön julkaisu – 2020:20), <http://julkaisut.valtioneuvosto.fi/handle/10024/162162>

uudelleen sähköinen tunnistamisen välttämättömyyttä ulkomaalaisille tarjottavissa palveluissa.

Digi- ja väestötietovirasto tarjoaa ulkomaan kansalaisen tunnistuspalvelua ja tunnistusvälinettä ulkomaan kansalaisen tunnistamiseksi. Palvelun avulla voidaan tietyllä varmuustasolla tunnistaa sellaisia ulkomaan kansalaisia, joilla ei ole suomalaista henkilötunnusta ja jotka eivät siksi voisi saada tunnistuslain mukaista vahvan sähköisen tunnistamisen välinettä. Lisäksi edellytyksenä on, ettei ulkomaan kansalainen voi saada myöskään eIDAS-asetuksen mukaista ulkomaista vastavuoroisesti hyväksyttävää tunnistusvälinettä. Tunnistuspalvelulla ei korvata vahvan tunnistamisen palveluja, joiden hyödyntäminen hallinnon asiointissa on edelleen pääsääntö. Kyseinen palvelu ei ole korotetun tai korkean tason tunnistusväline, joten sen avulla voidaan tunnistautua asiointipalveluihin, joissa voidaan käyttää muitakin tunnistusmenetelmää kuin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa tarkoitettua vahvaa sähköistä tunnistamista. Palvelua käyttäviä loppukäyttäjiä ei myöskään merkitä väestötietojärjestelmään, vaan DVV ylläpitää erillistä ulkomaan kansalaisten tunnistusvälineiden rekisteriä.

eIDAS-asetus ei itsessään ratkaise EU-jäsenvaltioiden välistä kansalaisten tunnistamisen haastetta. Vastavuoroinen tunnistaminen edellyttää myös sitä, että asiointipalveluja tarjoavat organisaatiot mahdollistavat EU-kansalaisen vahvan sähköisen eIDAS-tunnistamisen asiointipalvelussaan. Vaikka toisen jäsenvaltion kansalainen pystyisi tunnistautumaan jäsenmaiden solmupisteiden kautta asiointipalveluun, ei asiointi kuitenkaan onnistu palvelussa, mikäli käyttäjäorganisaatio ei ole tehnyt tarvittavia teknisiä muutoksia. Erityisesti henkilötunnuksen puuttuminen aiheuttaa haasteita tunnistauduttaessa toisesta jäsenvaltiosta peräisin olevalla sähköisen tunnistamisen menetelmällä kansallisiin asiointipalveluihin (HE 32/2019 vp, s. 10).

On myös huomiotava maahanmuuttajat, joilla ei ole henkilötunnusta. Maahanmuuttajat voivat saada vahvan sähköisen tunnistusvälineen vasta, kun henkilölle on myönnetty suomalainen henkilötunnus. Henkilötunnuksen voi saada Maahanmuuttoviraston oleskeluluvan myöntämisen prosessissa ulkomaalaislain (301/2004) mukaisesti.

Kun päätös oleskeluluvan myöntämisestä on tehty, ulkomaisella henkilöllä on mahdollisuus saada ulkomaalaisen henkilökortti, jota voidaan käyttää henkilöllisyyden osoittamiseen Suomen kansalaiselle myönnettyä henkilökorttia vastaavalla tavalla. Nämä yhdistettynä turvapaikanhakuprosessin nopeuteen parantavat turvapaikanhakijoiden pääsyä maksu- ja

pankkipalveluiden piiriin ja sitä kautta edistävät tunnistusvälineiden saamista. (HE 123/2016 vp, s.11)

6.4. Sähköistä asiointia koskeva EU-sääntely

6.4.1. Single Digital Gateway

Yhteisestä digitaalisesta palveluväylästä (Single Digital Gateway SDG) annetun asetuksen ((EU) 2018/1724) mukaan tietyt asiointipalvelut tulisi olla saatavilla digitaalisen palveluväylän kautta kaikille EU-käyttäjille vuoden 2023 loppuun mennessä. Digitaaliseen palveluväylään tulisi jatkossa liittää myös muita asetuksen soveltamisalaan kuuluvia asiointipalveluita, jos ne ovat kansallisesti käytettävissä sähköisesti. Näin ollen SDG-asetuksen velvoitteet sähköiselle asiointille tulisi huomioida valtionhallinnossa laajasti, koska useimpien sähköisen asiointipalveluiden tulisi olla myös muiden kuin suomalaisten asiakkaiden käytettävissä. Digitaalisen palveluväylän toimeenpano edellyttääkin useilta viranomaisilta heidän sähköisten asiointipalveluidensa kehittämistä, niin että ne ovat asioitavissa myös rajat ylittävästi. Lisäksi Suomessa tulisi olla käytettävissä sellainen tunnistratkaisu, jonka avulla asiakkaan digitaalinen henkilöllisyys voidaan tunnistaa vahvasti. Rajat ylittävä sähköinen tunnistautuminen on siis SDG-asetuksen toimeenpanon kannalta keskeistä. Sähköisen tunnistamisen ratkaisut eivät kuitenkaan kuulu SDG-asetuksen piiriin, vaan SDG-asetus lähtee siitä, että käytössä olisi jo jokin toimiva tunnistautumistratkaisu myös rajat ylittäville käyttäjille.

6.4.2. Palveludirektiivi

Palveludirektiivin (2006/123/EY) mukaan yritystoiminnan aloittamiseen ja harjoittamiseen liittyvät lupamenettelyt tulisi voida hoitaa etäältä ja sähköisesti koko EU:n alueella. Muista jäsenvaltioista peräisin olevien palveluntarjoajien olisi lähtökohtaisesti pystyttävä toimimaan kansallisten välineidensä avulla muiden jäsenvaltioiden viranomaisten kanssa. Käytännössä tämä palveludirektiivin velvoite on kuitenkin toteutunut heikosti. Suurimmat haasteet ovat liittyneet rajat ylittävään sähköiseen tunnistautumiseen. Myös komissio on kiinnittänyt asiaan huomiota ja lähettänyt kaikille jäsenvaltioille, mukaan lukien Suomelle, virallisen huomautuksen (2018/2385) keskitettyjen asiointipisteiden puutteellisesta toiminnasta. Komissio on nostanut Suomelle lähettämässään huomautuksessa esille muun muassa puutteita, jotka liittyvät rajat ylittävien käyttäjien sähköiseen asiointiin kuten sen, että Suomen on varmistettava, että jäsenvaltioiden eIDAS-asetuksen mukaisesti ilmoittamat sähköisen tunnistamisen menetelmät tunnistetaan ja niiden avulla on mahdollista hoitaa sähköiset menettelyt. Suomi on todennut vastauksessaan komissiolle muun

muassa sen, että sähköisiä menettelyjä kehitetään kansallisesti erillisillä lainsäädäntöhankkeilla ja kehittämissuunnitelmoilla, joilla on itsenäiset toteutusaikataulut sekä kertonut eIDAS-asetuksen kansallisen toimeenpanon aikataulusta.

6.4.3. Direktiivi digitaalisten välineiden ja prosessien käytöstä yhtiöoikeuden alalla

Digitaalisten välineiden ja prosessien käytöstä yhtiöoikeuden alalla annettu direktiivi (2019/1151), digitalisaatiodirektiivi, edellyttää muun ohessa, että osakeyhtiö tulee pääsääntöisesti voida perustaa ja sivuliike rekisteröidä sähköisesti ja rajat ylittävästi ilman fyysistä läsnäoloa Suomessa. Direktiivi tulee muutamaa poikkeusta lukuun ottamatta olla täytäntöönpanttu 1.8.2021 mennessä. Direktiivi kuitenkin mahdollistaa määräajan pidentämisen vuodella, jos sille on osoitettavissa objektiiviset perusteet. Selvää on myös, että jos Suomi ei ole notifioinut omaa tunnistamisratkaisua, estyy vastaava asiointi Suomesta ulospäin.

Tunnistamisratkaisun osalta digitalisaatiodirektiivissä edellytetään, että jäsenvaltioiden on varmistettava, että hakijat, jotka ovat unionin kansalaisia, voivat käyttää sähköisissä menettelyissä a) jäsenvaltion itse hyväksymän sähköisen tunnistamisen järjestelmän puitteissa käyttöön otettua sähköisen tunnistamisen menetelmää; b) toisessa jäsenvaltiossa käyttöön otettu sähköisen tunnistamisen menetelmää, joka on tunnustettu rajat ylittävää todentamista varten asetuksen (EU) N:o 910/2014 6 artiklan mukaisesti.

Valmistelussa onkin keskeistä huomioida, että EU-säädökset velvoittavat Suomea jäsenvaltiona, ja niiden noudattamatta jättäminen voi johtaa rikkomusmenettelyn aloittamiseen.

6.5. Luottamusverkostoa ja sähköistä tunnistamista koskeva sääntely

6.5.1. Tunnistusmarkkinoiden sääntely

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, jäljempänä tunnistuslaki) säätelee luottamusverkostosta ja sen toimintaa. Tunnistuslaissa säädetään sen 1 §:n mukaan vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta tunnistuspalveluita käyttäville palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille.

Tunnistuslain 10 §:ssä säädetään tunnistuspalvelun tarjoajan velvollisuudesta ilmoittaa toiminnan aloittamisesta Liikenne- ja viestintävirastolle (Traficom). Luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajat, jotka ovat tehneet

lain 10 §:n mukaisen ilmoituksen Liikenne- ja viestintävirastoon (Traficom). Luottamusverkoston jäsenten on annettava liikkeelle laskemansa tunnistusväline luottamusverkostossa edelleen välitettäväksi. Laissa säädetään toimijoiden ilmoitusvelvollisuudesta, käyttöoikeuden toimitusehdoista ja myös käyttöoikeudesta perittävästä korvauksesta. Tunnistuspalvelua on mahdollista tarjota myös tekemättä ilmoitusta Traficomille, mutta tällöin tunnistuspalvelun tarjoajalla ei ole vahvan sähköisen tunnistuspalvelun tarjoajan asemaa. (HE 272/2014 vp, s. 19) Tunnistuslain sääntelyllä varmistetaan lisäksi sähköisen asioinnin turvallisuutta tunnistauduttaessa asiointipalveluihin.

Tunnistuslain 2 §:n 1 kohdan mukaan vahvalla sähköisellä tunnistamisella tarkoitetaan sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset. Tunnistuslaki ei siten säätele matalan tason tunnistusvälineitä.

Traficom ylläpitää rekisteriä vahvan sähköisen tunnistuspalvelun tarjoajista. Tunnistuslain esitöiden mukaan rekisteri on järjestelylle hyvin keskeinen: sekä kuluttaja että tunnistuspalvelua hankkiva palveluntarjoaja voivat sen avulla luottaa tunnistuspalvelun tarjoajaan. Kun väline on tarjottu luottamusverkostoon välitettäväksi, ei erillisiä sopimuksia välineen toiminnasta tai tietoturvasta tarvita, sillä rekisterissä olevien tunnistusvälineiden tiedetään olevan vaatimusten mukaisia. Tunnistuslain 29 § edellyttää, että tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulle arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.

Luottamusverkoston jäsenille on tunnistuslaissa asetettu tiettyjä velvoitteita. Tunnistusvälineen tarjoajan on 12 a §:n mukaisesti laadittava tunnistuspalvelunsa käyttöoikeuden toimitusehdot ja käytettävä niitä tehdessään sopimuksia tunnistusvälityspalveluiden tarjoajien kanssa. Käyttöoikeuden ehtojen on oltava tunnistuslain mukaisia sekä kohtuullisia ja syrjimättömiä. Tunnistusvälineen tarjoaja voi kieltäytyä sopimuksen tekemisestä ainoastaan, jos tunnistusvälityspalvelun tarjoaja toimii vastoin tunnistuslakia tai sen nojalla annettuja säännöksiä tai määräyksiä taikka kieltäytymiselle on muu painava peruste. Tunnistusvälineen tarjoajan on myös mahdollistettava lain 17 §:n 4 momentin mukaan se, että toinen tunnistusvälineen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnistamiseen haettaessa

vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Tällä menettelyllä tarkoitetaan lain mukaisesti ensitunnistamisen ketjuttamista (HE 264/2018 vp, s. 31-32).

Luottamusverkoston vastuukysymyksistä on säännelty tunnistuslaissa sekä vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta annetussa valtioneuvoston asetuksessa (169/2016). Tunnistuslain 12 d §:n mukaisesti se tunnistuspalvelun tarjoaja, joka tahallaan tai huolimattomasti toimii luottamusverkostoa koskevan sääntelyn vastaisesti taikka ensitunnistuksesta säädettyjen velvollisuuksien vastaisesti, on velvollinen korvaamaan toiselle tunnistuspalvelun tarjoajalle aiheuttamansa vahingon. Vahingonkorvaus käsittää korvauksen kuluista, hinnanerosta sekä muusta välittömästä taloudellisesta vahingosta.

Vahvan sähköisen tunnistamisen palvelun ja varmenteiden tarjonta katsotaan tällä hetkellä yksityiseksi palveluntarjonnaksi, johon ei liity julkisen vallan käyttöä tai julkista hallintotehtävää perustuslain 124 §:n tarkoittamalla tavalla. (PeVL 16/2009 vp, s. 2-3) Luottamusverkostossa on kyse yksityisistä palveluntarjoajista koostuvan markkinan sääntelystä. (HE 36/2009 vp, s. 87) Markkinaehtoisten toimijoiden varaan rakentuvalla järjestelyllä pyritään teknologianeutraaliin tunnistuspalveluiden kehittämiseen. Digi- ja väestötietoviraston (DVV) tuottamia tunnistuspalveluita säännellään laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009), laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) sekä henkilökorttilaissa. Luottamusverkostosta säädettyä viranomaisen tarjoama henkilökorttiin liitetty kansalaisvarmenne ei ollut saavuttanut sähköisten tunnistamisvälineiden markkinoilla merkittävää markkina-asemaa. (HE 74/2016 vp, s. 8). DVV:n tuottamat tunnistuspalvelut ovat kuitenkin tällä hetkellä yhtä lailla osa markkinaehtoista luottamusverkostotoimintaa.

6.5.2. eIDAS-asetus ja sen täytäntöönpano

Sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annettu Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 (jäljempänä eIDAS-asetus) tuli voimaan 17.9.2014 ja sitä on sovellettu 1.7.2016 alkaen. Asetuksessa perustettiin sähköisen tunnistamisen yhteentoimivuusjärjestelmä, jonka tavoitteena on mahdollistaa tulevaisuudessa se, että toisessa jäsenvaltiossa myönnettyillä sähköisillä tunnistamisvälineillä voidaan tunnistautua toisen jäsenvaltioiden julkisiin tai yksityisiin sähköistä tunnistamista vaativiin palveluihin. eIDAS-

asetus toi muutoksia myös kansalliseen sähköiseen tunnistamiseen, jolloin tunnistuslain vaatimuksia muutettiin vastaamaan EU-sääntelyä.

eIDAS-asetuksen tarkoituksena on lisätä luottamusta sähköisiin transaktioihin sisämarkkinoilla sekä parantaa julkisten ja yksityisten verkkopalvelujen, sähköisen liiketoiminnan ja sähköisen kaupankäynnin toimivuutta unionissa. Asetuksen 6 artiklassa säädetään sähköisen tunnistamisen menetelmien vastavuoroisesta tunnustamisesta. Kun julkisen sektorin elimen yhdessä jäsenvaltiossa tarjoaman verkkopalvelun käyttö edellyttää kansallisen oikeuden nojalla tai kansallisessa hallinnollisessa käytännössä sähköistä tunnistamista, toisessa jäsenvaltiossa myönnettyt verkkopalvelujen käyttöön tarvittavat sähköisen tunnistamisen menetelmät on tunnustettava ensimmäisessä jäsenvaltiossa kyseisen verkkopalvelun osalta rajat ylittävää todentamista varten. Vastavuoroinen tunnistaminen kuitenkin edellyttää, että sähköisen tunnistamisen menetelmä on myönnetty komission 9 artiklan mukaisesti julkaisemaan luetteloon sisältyvän sähköisen tunnistamisen järjestelmän puitteissa.

Jos tunnistusvälineen tarjoaja haluaa notifioida tunnistusmenetelmänsä EU:n komissiolle, Liikenne- ja viestintävirasto tekee notifiointin yhteistyössä tunnistuspalvelun tarjoajan kanssa. Tästä säädetään tunnistuslain 42 a §:ssä, jonka mukaan viraston tehtävänä on ilmoittaa sähköisen tunnistamisen järjestelmiä Euroopan komissiolle. Tunnistuksenvälityspalveluita ei notifioida, mutta tieto niistä harkitaan sisällytettäväksi ainakin yleisellä tasolla menetelmän notifiointiin. Notifiointissa annettavista tiedoista säädetään komission täytäntöönpanopäätöksessä olosuhteiden, muutoseikkojen ja menettelyjen määrittelemisestä eIDAS-asetuksen 9 artiklan 5 kohdan mukaisesti. Notifiointiin liittyy mahdollinen ETA-alueen jäsenvaltioiden edustajien tekemä vertaisarviointi, joka kestää kokonaisuudessaan noin kuusi kuukautta. Vertaisarvioinnin puitteista säädetään komission täytäntöönpanopäätöksessä (EU) 2015/296 menettelyä koskevien järjestelyjen vahvistamisesta sähköiseen tunnistamiseen liittyvää jäsenvaltioiden välistä yhteistyötä varten eIDAS-asetuksen 12 artiklan 7 kohdan mukaisesti.²³

eIDAS-asetuksen mukainen vastavuoroinen tunnistaminen ei ole edennyt toivotulla nopeudella. Asetus on tullut voimaan vuonna 2016, mutta jäsenvaltioiden välillä ei vielä täysimääräisesti toteudu rajat ylittävää tunnistamista. Alkuvuoteen 2021 mennessä Tsekki, Viro, Italia, Alankomaat, Tanska, Espanja, Latvia, Saksa, Slovakia, Kroatia, Belgia, Luxemburg, Liettua, Portugali sekä Belgia ovat ilmoittaneet komissiolle omat sähköisen

²³ ks. traficom sivut

tunnistamisen järjestelmänsä. Lisäksi useat muut jäsenvaltiot ovat aloittaneet ilmoittamisprosessin. Helmikuussa 2021 Suomen solmupisteen kautta voivat Italian, Saksan, Viron sekä Espanjan kansalaiset tunnistautua kansallisiin asiointipalveluihin. Vaikka vastavuoroinen tunnistaminen toteutuisi asetuksen mukaisesti, ei asiointi kuitenkaan onnistu asiointipalvelussa, mikäli palvelun tarjoaja ei ole tehnyt tarvittavia teknisiä muutoksia. Erityisesti henkilötunnuksen puuttuminen aiheuttaa haasteita tunnistauduttaessa rajat ylittävällä tunnistusvälineellä kansallisiin asiointipalveluihin. (HE 32/2019 vp, s. 9-10) eIDAS-tunnistusvälineiden henkilön yksilöivät tiedot voivat poiketa huomattavasti kansallisesta henkilötunnuksesta ja se taas voi estää rajat ylittävän asioinnin.

Digi- ja väestötietovirasto tuottaa eIDAS-asetuksen mukaista kansallista solmupistettä tunnistuslain 42 c §:n nojalla. Solmupisteen kautta rajat ylittävä tunnistaminen toteutetaan välittämällä tunnistustapahtumat Suomi.fi-tunnistuksen kautta. Suomi.fi-tunnistus on tarkoitettu viranomaisten sekä muiden julkista hallintotohtävää hoitavien digitaalisiin palveluihin, joten yksityiset toimijat eivät tällä hetkellä voi hyödyntää rajat ylittävää tunnistusta. eIDAS-asetus jättää jäsenvaltioille mahdollisuuden päättää siitä, ottavatko ne yksityisen sektorin mukaan rajat ylittävään tunnistamiseen. Kuitenkin jäsenvaltioiden olisi kannustettava yksityistä sektoria käyttämään vapaaehtoisesti vastavuoroinen tunnistamisen menetelmiä tunnistamistarkoituksiin, kun se on tarpeen verkkopalveluissa.²⁴

eIDAS-asetuksen 49 artiklan ensimmäisen kohdan mukaan Euroopan komissio järjesti julkisen kuulemisen kesällä 2020 asetuksen soveltamisen uudelleenarvioimiseksi ja raportoimiseksi Euroopan parlamentille ja neuvostolle. Komissio on tämän hetken tietojen valossa esittämässä parlamentille huhtikuussa 2021 ehdotuksensa EU:n sähköistä tunnistamista ja luottamuspalveluita määrittävän asetuksen muutoksista ja eurooppalaisen digitaalisen identiteetin kehikon luomisesta. Komission odotetaan ehdottavan eIDAS-asetukseen täsmennyksiä, lisää velvoittavuutta jäsenvaltioihin tukea rajat ylittävään tunnistamiseen edellytyksiä ja vahvistuksia yksityisen sektorin asemaa osallistua ratkaisujen toteuttamiseen. Ennakkotietojen mukaan komissio tulisi ehdottamaan yhteistä eurooppalaista sääntelyä uuden tyyppisille luottamuspalveluille, joita varten yksittäisen jäsenvaltion tulisi tuottaa digitaaliseen lompakkoon viranomaisen henkilön ydinidentiteetin ja siihen liittyvän digitaalisen todisteen (kredentiaali). EIDAS-asetuksen uudelleenarviontia on käsitelty laajemmin edellä osassa 1.

²⁴ eIDAS-asetus, johdanto-osan perustelukappaleet 13-17

6.5.3. PSD2

Lyhenne PSD2 viittaa sanoihin Payment Services Directive 2, tarkemmin 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 (jäljempänä PSD2). Direktiivi implementoitiin osaksi maksupalvelulakia (290/2010). Direktiivi asetti uusia vaatimuksia maksupalveluille sekä vahvan sähköisen tunnistamisen vaatimuksille maksupalvelujen yhteydessä.

Direktiivi korostaa sähköisten maksujen turvallisuutta käyttäjien suojelemiseksi ja vakaan ympäristön luomiseksi sähköiselle kaupankäynnille. Direktiivi velvoittaa toteuttamaan sähköisesti tarjotut maksupalvelut siten, että käytettävissä olevilla teknologioilla voidaan taata käyttäjän turvallinen tunnistaminen ja vähentää mahdollisimman paljon petoksen riskiä. Käytännössä turvatoimien on oltava maksupalveluun liittyvän riskin tason mukaiset. Turvallinen tunnistaminen toteutuu tyypillisesti käyttäen erilaisia salausjärjestelmiä, jotka perustuvat maksajan henkilökohtaisiin laitteisiin. On katsottu, että toimenpiteet, joihin kuuluu tyypillisesti salausjärjestelmiä ja joissa voidaan käyttää tunnistamiskoodeja, voivat lisätä maksutapahtumien turvallisuutta.²⁵

Palveluntarjoajan on käytettävä vahvaa tunnistamista, jos maksaja käyttää maksutiliään tietoverkon välityksellä, käynnistää sähköisen maksutapahtuman tai toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski. Lisäksi vahvaan tunnistamiseen liittyisi direktiivin mukaisia lisävaatimuksia silloin, kun maksaja käynnistää sähköisen maksutapahtuman etäviestimellä, esimerkiksi verkkopankissa. (HE 132/2017 vp, s. 20)

Maksupalvelulain 8 §:n mukaan henkilön vahva tunnistaminen on tehtävä kahden tekijän varmennuksella, mikä tarkoittaa, että vahvan tunnistamisen on perustuttava 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.

²⁵ PSD2, johdanto-osan perustelukappaleet 95-96.

6.6. Valtion identiteetin hallintaa ja tunnistusvälineitä koskeva sääntely

6.6.1. Väestötietojärjestelmä ja sen sisältämät tunnisteet

Väestötietojärjestelmästä ja sen ylläpidosta säädetään laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista, jäljempänä väestötietolaki. Väestötietojärjestelmä on perusrekisteri, jossa ylläpidetään ajantasaiset henkilötiedot Suomen kansalaisista ja Suomessa vakinaisesti tai tilapäisesti asuvista ulkomaalaisista henkilöistä. Perusrekisterijärjestelmä on luotu palvelemaan koko yhteiskuntaa ja sen tietohuoltoa. (HE 89/2008 vp, s. 54 ja 64) Sekä luonnollisten henkilöiden että oikeushenkilöiden olemassa olon virallisuus pohjautuu rekisteröintiin, jonka perusteella henkilöt yksilöidään. Perusrekisterit muodostavat yhteiskunnan perustietovarantojärjestelmän.²⁶

Perusrekistereille on ominaista, että niistä säädetään laissa tai asetuksessa. Niiden tietoihin liittyy myös niin sanottu julkinen luotettavuus tai muu vastaava tietojen luotettavuuden takaava ominaisuus. Perusrekisterin luotettavuudella tarkoitetaan sitä, että tiedot katsotaan lähtökohtaisesti eheiksi eli luotettaviksi ja ajantasaisiksi, jollei asiasta esitetä vastanäyttöä.

Väestötietolain 18 §:ssä säädetään niistä järjestelmän tiedoista, joiden katsotaan olevan julkisesti luotettavia. Pykälän mukaan pidetään väestötietojärjestelmään talletettuja 13 §:n 1 momentin 1-21 kohdissa tarkoitettuja henkilötietoja julkisesti luotettavina tietoina, jollei osoiteta, että tieto on virheellinen tai puutteellinen. Muita kuin 13 §:ssä tarkoitettuja järjestelmään talletettuja tietoja julkinen luotettavuus ei koske ja niitä saa käyttää henkilöä koskevassa päätöksenteossa vain, jos hänelle annetaan päätöksenteon yhteydessä nimenomainen selvitys tietojen sisällöstä ja käytöstä (HE 89/2008 vp, s. 83). 13 §:n tietoihin sisältyy muun muassa tekninen tunnistetieto ja sähköinen asiointitunnus.

Väestötietojärjestelmä perustuu niin kutsutun kertarekisteröinnin periaatteelle, jonka mukaan rekisteröitävät tiedot tulee rekisteröidä vain kerran, jolloin tietojen päällekkäistä rekisteröintiä tietojärjestelmiin eri asiayhteyksissä vältettäisiin. Muut toimijat päivittävät omiin rekistereihinsä tietonsa väestötietojärjestelmästä.²⁷ Väestötietojärjestelmän sisältämät olennaiset

²⁶ Voutilainen Tomi: ICT-oikeus sähköisessä hallinnossa, 2009, s. 90.

²⁷ Voutilainen (2009), s. 90

henkilöä identifioivat tunnisteet ovat henkilötunnus, sähköinen asiointitunnus sekä ulkomaan kansalaista koskeva rekisterimerkintä.

Sähköinen asiointitunnus liittyy varmenteen myöntämiseen. Väestötietolain 63 §:n mukaan, kun henkilön tiedot talletetaan ensimmäisen kerran väestötietojärjestelmään, hänelle annetaan sähköisen asiointitunnuksen antamisessa tarvittava yksilöllinen tekninen tunnistetieto. Tekninen tunnistetieto muutetaan yksilölliseksi asiointitunnukseksi, kun henkilölle myönnetään ensimmäisen kerran kansalaisvarmenne tai muu DVV:n myöntämä varmenne. Tekninen tunnistetieto ja sähköinen asiointitunnus muodostuvat kahdeksasta satunnaisesti valitusta numerosta sekä tarkastusmerkistä, eivätkä sisällä henkilöön liittyviä tunnistetietoja.

6.6.2. Digi- ja väestötietoviraston varmennetoiminta ja kansalaisvarmenne

Digi- ja väestötietovirasto tuottaa väestötietolain mukaisesti varmennetun sähköisen asioinnin palveluita. DVV tuottaa henkilövarmenteita kansalaisille, organisaatioille sekä sosiaali- ja terveydenhuoltosektorille. Henkilövarmenteita käytetään tietoverkkojen kautta tapahtuvassa tunnistamisessa, salauksessa ja sähköisen allekirjoituksen tekemisessä. DVV:n myöntämät tunnistus- ja allekirjoitusvarmenteet täyttävät sekä eIDAS-asetuksen että tunnistuspalvelulain mukaiset vaatimukset. DVV toimii korkean tason vaatimukset täyttävänä tunnistuspalvelun tarjoajana tuottaessaan varmennepohjaista tunnistusvälineitä. DVV:n tuottamat varmennepalvelut ovat osa luottamusverkostoa ja tällä hetkellä kansallisesti ainoana korkean tason tunnistusvälineen tarjoaja. Muut luottamusverkostossa olevat tunnistuspalvelun tarjoajat tuottavat korotetun tason tunnistuspalveluita. Pääsääntöisesti korotetun tason tunnistusväline riittää tunnistauduttaessa sähköisiin asiointipalveluihin.

DVV:n varmennepalvelu koostuu varmennejärjestelmästä, jossa varmentajan toimesta luodaan varmenteet ja allekirjoitetaan suljettujen varmenteiden sulkulistat, voimassaolevien varmenteiden varmennehakemistosta, neuvontapalvelusta, suljettavien varmenteiden sulkupalvelusta sekä suljettujen varmenteiden sulkulistapalvelusta. Varmenteiden ja toimikorttien hallinnointi tapahtuu varmennetietojärjestelmässä. DVV:lle kuuluvat tehtävät on pykälässä jaettu kahteen osaan, joista ensimmäinen koskee viranomaistehtäviä eli viraston hoidettavaksi säädettyä kansalaisvarmennetta koskevaa tehtäväkokonaisuutta sekä toinen osa niitä tehtäviä ja palveluita, joita DVV:n on mahdollista tarjota esimerkiksi liiketaloudellisina palveluina. Kansalaisvarmennetta lukuun ottamatta DVV:llä ei ole minkäänlaista monopoliasemaa tai yksinoikeutta siinä varmennepalvelujen ja suoritteiden tuottamiseen. (HE 89/2008 vp, s. 53) DVV:n lakisääteisenä tehtävänä on kuitenkin lisäksi tuottaa sosiaali- ja

terveydenhuollon varmennepalvelut (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ja laki sähköisestä lääkemääräyksestä).

Kansalaisvarmenteella tarkoitetaan DVV:n luonnolliselle henkilölle myöntämää varmennetta, joka sisältyy henkilökorttilaissa (663/2016) tarkoitettuun henkilökorttiin tai muuhun viranomaisen asiakirjaan tai tekniseen alustaan, ja jota käytetään henkilön todentamista, sähköisen allekirjoituksen tekemistä sekä asiakirjojen ja viestien salausta varten. Kansalaisvarmenteella tarkoitetaan myös muuhun viranomaisen asiakirjaan tai tekniseen alustaan sisältyvää DVV:n myöntämää varmennetta, jota käytetään edellä mainittuun tarkoitukseen. Väestötietolaissa säännellään tarkemmin DVV:n varmennetoimintaan liittyviä menettelyitä ja tietojen käsittelyä.

Kansalaisvarmenne on julkisoikeudellinen suorite tuotettaessa varmennetta viralliselle henkilökortille. Muille alustoille tuotettaessa kansalaisvarmenne ei ole julkisoikeudellinen suorite, koska periaatteessa loppukäyttäjä voi itse valita markkinoilla olevan kortti- tai muun tallennealustan yksityisiltä markkinoilta.²⁸ Henkilön yksilöintitietona käytetään kansalaisvarmenteella tapahtuvassa tunnistuksessa sähköistä asiointitunnusta (SATU).

6.7. Julkisen sektorin sähköiset palvelut, tunnistaminen ja tiedonhallinta

6.7.1. Velvollisuus järjestää sähköisiä palveluita

Julkisen sektorin palvelujen järjestäminen pohjautuu ensisijaisesti hallintolakiin ja siinä säädettyyn. Hallintolain 7 §:n palveluperiaatteen mukaisesti asiointi ja asian käsittely viranomaisessa on pyrittävä järjestämään siten, että hallinnossa asioiva saa asianmukaisesti hallinnon palveluita ja viranomainen voi suorittaa tehtävänsä tuloksellisesti. Palveluperiaate ja viranomaisen tehtävien tuloksellinen hoitaminen merkitsevät sitä, että asiointi tulee voida tapahtua sekä hallinnossa asioivan, että viranomaisen kannalta mahdollisimman nopeasti, joustavasti ja yksinkertaisesti sekä kustannuksia säästäen. Asiointi on pyrittävä järjestämään siten, että hallinnossa asioiva voi helposti muodostaa kokonaiskäsityksen asiansa hoitamiseen tarvittavan palvelun sisällöstä ja siihen liittyvistä toimista. (HE 72/2002 vp, s.57)

Viranomaisen velvollisuudesta tarjota palvelujaan digitaalisesti on säädetty digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019, jäljempänä digipalvelulaki). Lain esitöiden mukaan digipalvelulaki on hallintolakia ja muita hallinnon yleislakeja täydentävä erityislaki, jossa määritellään

²⁸ Valtiontalouden tarkastusviraston toiminnantarkastuskertomus 161/2008, s. 30.

digitaalisille palveluille asetettavat erityiset vaatimukset ja pyritään turvaamaan kaikille yhtäläinen mahdollisuus asiansa hoitamiseen palvelun laadusta riippumatta sekä vastaamaan mahdollisimman hyvin yhteiskunnallisten erityisryhmien tarpeisiin palvelujen saamisessa.

Digipalvelulain 2 luvun 5 §:n mukaan viranomaisen on tarjottava jokaiselle mahdollisuus toimittaa asiointitarpeeseensa liittyvät sähköiset viestit ja asiakirjat käyttäen digitaalisia palveluita tai muita sähköisiä tiedonsiirtomenetelmiä. Käytännössä säännös tarkoittaa, että viranomaisella on velvollisuus järjestää palvelutoimintansa siten, että sähköinen asiointi viranomaisen kanssa on mahdollista kaikissa viranomaisen toimialaan ja toimivaltaan kuuluvissa asioissa. Koska digipalvelulaissa viranomaiselle on säädetty velvollisuus tarjota hallinnon asiakkaalle mahdollisuutta lähettää viranomaiselle sähköisiä viestejä, ei asiointimahdollisuus rajaudu pelkästään asioiden vireillepanoon. Digitaalisia palveluja ja muita sähköisiä tiedonsiirtomenetelmiä käyttäen on pystyttävä asioimaan viranomaisen kanssa mistä tahansa syystä, joka liittyy hallinnon asiakkaan tarpeeseen asioida hallinnossa.²⁹

Digipalvelulaissa säädetyn perusteella kaikki asian vireillepanot ja asiankäsittelyn välitoimenpiteet on pystyttävä hoitamaan myös sähköisesti, ellei muualla laissa ole toisin säädetty, koska laissa on myös mainittu sähköiset asiakirjat, jotka on voitava toimittaa viranomaiselle sen käytössä olevien sähköisten tiedonsiirtomenetelmien avulla. Lain 2 luvun säännös ei siten pohjautu vain viestien lähettämiseen viranomaisen ja hallinnon asiakkaan välillä vaan se tarkoittaa viranomaiselle säädettyä kattavaa velvollisuutta sähköisen asioinnin järjestämiseen ja digitaalisten palvelujen tarjoamiseen viranomaisen toimialalla.³⁰ Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) osaltaan menettelysäännöstensä kautta tukee digitaalisten palvelujen järjestämistä ja asiointia viranomaisissa.

Kaikkien viranomaisten ei välttämättä ole tarkoituksenmukaista kehittää omia digitaalisia palveluja. Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016, jäljempänä tukipalvelulaki) tarkoituksena on parantaa julkisten palvelujen saatavuutta, laatua, tietoturvaluutta, yhteentoimivuutta ja ohjausta sekä edistää julkisen hallinnon toiminnan tehokkuutta ja tuottavuutta. Lakiin sisältyvät hallinnon yhteisiä sähköisen asioinnin tukipalveluja koskevat säännökset. Tukipalveluilla tarkoitetaan yhteistä sähköisen asioinnin tukipalvelua, jota käyttäjäorganisaatio käyttää asiointipalvelunsa tai muun sille

²⁹ Voutilainen 2020, s. 190

³⁰ Ibid.

kuuluvan tehtävän taikka sen tarjoaman palvelun tukena. Laissa säädetään tukipalvelujen toiminnallisuuksista, palvelutuottajien vastuista ja tehtävistä sekä henkilötietojen ja muiden tietojen käsittelystä tukipalvelujen tuottamiseksi. Laissa säädetään myös velvollisuudesta ja oikeudesta käyttää yhteisiä tukipalveluja. Lähtökohtaisesti viranomaisella on velvollisuus käyttää lain 3 §:ssä lueteltuja tukipalveluja (Suomi.fi-palvelut) muutamia poikkeuksia lukuun ottamatta. Tukipalveluja tuottaa pääasiallisesti Digi- ja väestötietovirasto.

6.7.2. Henkilöllisyyden osoittaminen sähköisissä julkisissa palveluissa

Vaikka tunnistuslaki sääntelee kansallisesti vahvaa sähköistä tunnistamista, siinä ei säädellä siitä, milloin organisaatioiden asiointipalveluissa tulisi käyttää lain tarkoittamaa vahvaa sähköistä tunnistamista henkilöiden tunnistamiseksi. Vahvan sähköisen tunnistamisen käyttöveloitteesta säädetään laissa digitaalisten palvelujen tarjoamisesta (306/2019). Lain 6 §:ssä on säännökset palvelun käyttäjän sähköisen tunnistamisen vaatimuksista ja rajoituksista. Ennen digipalvelulain voimaantuloa sääntelyssä ei ole ollut selkeitä säännöksiä tilanteista, joissa palvelun käyttäjä pitäisi tunnistaa ja tunnistamismahdollisuuden puuttuminen on nähty esteenä sähköiselle asioinnille viranomaisissa. Laissa käyttäjällä tarkoitetaan luonnollista henkilöä, joka käyttää digitaalista palvelua joko oman asiansa hoitamiseen taikka toisen luonnollisen henkilön tai oikeushenkilön puolesta. Digipalvelulain esitöiden mukaisesti laki on nähtävissä hallintolakia ja muita hallinnon yleislakeja täydentävänä erityislakina, jossa määritellään digitaalisille palveluille asetettavat erityiset vaatimukset ja pyritään turvaamaan kaikille yhtäläinen mahdollisuus asiansa hoitamiseen palvelun laadusta riippumatta sekä vastaamaan mahdollisimman hyvin yhteiskunnallisten erityisryhmien tarpeisiin palvelujen saamisessa. (HE 60/2018 vp)

Digipalvelulain 6 §:n mukaisesti vahvan sähköisen tunnistamisen vaatimukselle tulee olla perusteltu tarve palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi. Mikäli digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi, palvelun käyttäjä on tällöin tunnistettava vahvasti. Pykälän nojalla on kuitenkin mahdollista painavasta perustellusta syystä hyödyntää muuta vastaavaa tietoturvalista tunnistuspalvelua.

Hallituksen esityksessä (HE 60/2018) on tarkennettu tilanteita, jossa tulisi vaatia vahvaa sähköistä tunnistusta. Esitöiden mukaan digipalvelulain nojalla viranomaisen arvioitavaksi jää tapauskohtaisesti tunnistamisen vaatimus asiointipalveluissaan. Viranomainen voi vaatia sähköistä tunnistamista

esimerkiksi silloin, kun käyttäjä pääsee palvelussa katsomaan omia tietojaan taikka valtuutuksen perusteella edustamansa henkilön tietoja. Vahvaa sähköistä tunnistamista olisi kuitenkin käytettävä erityisesti palveluissa, joissa käyttäjä pääsee näkemään tai käsittelemään terveydentilaansa koskevia tietoja, muita erityisiin henkilötietoryhmiin kuuluvia tietoja, sosiaalihuollon asiakkuutta koskevia tietoja, oppilashuoltoon liittyviä tietoja sekä liike- ja ammattisalaisuuksia. (HE 60/2018 vp)

Muussa lainsäädännössä on suhteellisen vähän säännöksiä siitä, milloin sähköinen asiointi edellyttää nimenomaan vahvaa sähköistä tunnistamista. Esimerkiksi sähköisestä asioinnista viranomaistoiminnasta annetun lain (13/2003) 18 §:ssä edellytetään todisteellisen tiedoksiannon yhteydessä tunnistautumistekniikkaa, joka on tietoturvallinen ja todisteellinen. Erityislainsäädäntöön sisältyy kuitenkin jonkun verran säännöksiä henkilöllisyyden osoittamisesta tiettyä toimialaa tai palvelua koskevassa sähköisessä asioinnissa. Tällöin laissa saatetaan edellyttää joko tunnistuslain mukaisten vahvan sähköisen tunnistusvälineiden käyttöä taikka muuta tietoturvallista tunnistamistapaa. Erityislait saattavat myös yleisesti edellyttää, että henkilöllisyys voidaan luotettavasti todistaa. Erityisesti terveydenhuoltoon liittyvässä sähköisessä asioinnissa saatetaan lain tasolla edellyttää nimenomaisesti tunnistuslain mukaista vahvaa sähköistä tunnistamista.

Julkishallinnon organisaatioilla on tukipalvelulain mukaan velvoite ensisijaisesti käyttää vahvaan sähköiseen tunnistamiseen lain 3 §:n 4-kohdassa tarkoitettua luonnollisen henkilön tunnistuspalvelua, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön tunnistuslaissa tarkoitettua tunnistuspalvelun tarjoajan palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle (Suomi.fi-tunnistus). Lähtökohtaisesti julkishallinnon organisaation on hyödynnettävä Suomi.fi-tunnistusta asiointipalveluissa, joissa vahva sähköinen tunnistaminen on tarpeen. Tällä hetkellä valtio kilpailuttaa Suomi.fi –palveluun käytettäväksi luottamusverkoston toimijoiden tunnistuspalvelut.

6.7.3. Tiedonhallinta

Viranomaisen tuottaessa digitaalisia palveluja, on lainsäädännössä huomioitu viime vuosina myös korostuneemmin tiedonhallinta ja sitä kautta tiedon yhteentoimivuus. Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jäljempänä tiedonhallintalaki) tarkoituksena on varmistaa viranomaisten tietoaaineistojen yhdenmukainen, laadukas ja tietoturvallinen hallinta, mahdollistaa viranomaisten tietoaaineistojen turvallinen ja tehokas

hyödyntäminen sekä edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta.

Tiedonhallintalaissa säädetään tiedonhallinnan järjestämisestä, tietoturvallisuudesta, tietoaineistojen muodostamisesta ja sähköisestä luovutustavasta, asianhallinnasta sekä julkisen hallinnon tiedonhallinnan yleisestä ohjauksesta. Tiedonhallintalaissa säädetään myös laajasti siitä, miten tietoa voidaan luovuttaa teknisten rajapintojen avulla. Henkilötietojen luovutuksesta teknisten rajapintojen avulla viranomaisten välillä säädetään tiedonhallintalain 22 §:ssä ja lain 24 §:ssä säädetään tietoaineistojen luovuttamisesta rajapinnan avulla muille kuin viranomaisille. Lähtökohtaisesti viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus. Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä siten, että teknisesti varmistetaan luovutettavien tietojen tapauskohtainen tarpeellisuus tai välttämättömyys tietojen saavan viranomaisen tehtävien hoitamiseksi, jos luovutettavat tiedot ovat henkilötietoja tai salassa pidettäviä tietoja. Viranomaisen voi luovuttaa teknisten rajapintojen avulla tietoja muulle kuin toiselle viranomaiselle, jos tiedot saavalla toimijalla on erikseen laissa säädetty tiedonsaantioikeus ja oikeus käsitellä näitä tietoja.

Tiedonhallintalain 20 §:ssä säädetään tietoaineistojen keräämisestä viranomaistoimintaa varten. Viranomaisen on pyrittävä hyödyntämään toisen viranomaisen tietoaineistoja, jos viranomaisella on oikeus saada tarvittavat tiedot toiselta viranomaiselta teknisen rajapinnan tai katseluyhteyden avulla. Tietojen hyödyntämisessä on huolehdittava asianosaisen tai muun hallinnon asiakkaan oikeusturvasta. Lisäksi jos viranomaisella on oikeus saada toisen viranomaisen tietovarannosta tehtäviensä hoitamista varten tietoja luotettavasti ja ajantasaisesti teknisen rajapinnan tai katseluyhteyden avulla, se ei saa vaatia asiakastaan esittämään tai toimittamaan tällaista todistusta tai otetta, ellei se ole välttämätöntä asian selvittämiseksi.

Säännöksen tarkoituksena on vähentää viranomaisten rinnakkaista ja päällekkäistä tietojen keräämistä hallinnon asiakkailta sekä varmistaa, että viranomaiset käyttäisivät ajantasaisia tietoja niiden alkuperäisistä tietolähteistä. Asiakkailta pyydettävän tiedon osalta lain esitöissä tuodaan esiin, että viranomaisilla on useissa tilanteissa mahdollisuus saada tehtäviensä hoitamiseen tarvitsemansa erilaisiin todistuksiin ja otteisiin liittyvät tiedot toiselta viranomaiselta ajantasaisesti. Tästä syystä ei ole perusteita, että hallinnon asiakasta edellytettäisiin toimittamaan tällaiset tiedot. Jos

viranomaisella olisi tehtäviensä hoitamista varten oikeus saada luotettavasti ja ajantasaisesti teknisen rajapinnan tai katseluyhteyden avulla toisen viranomaisen tietovarannosta sellaisia tietoja, joita otteesta tai todistuksesta ilmenisi, ei otteita tai todistuksia saisi vaatia hallinnon asiakkaalta. Asiakasta ei myöskään muulla tavalla saisi vaatia toimittamaan vastaavaa tietoa. Tarkoituksena on varmistaa, ettei jo kerran asiakkaalta saatua tai muutoin viranomaisen rekisteröimää tietoa kysyttäisi uudestaan hallinnon asiakkaalta. (HE 284/2018 vp)

6.8. Henkilöllisyysasiakirjojen sääntely

6.8.1. Henkilöllisyysasiakirjojen sääntelystä yleisesti

Suomen lainsäädäntö ei sääntele yleisellä tasolla sitä, millaisilla asiakirjoilla henkilöllisyyden voi osoittaa. Kansallisesti ei ole käytössä virallisen henkilöllisyystodistuksen käsitettä tai lainsäädännössä asetettuja edellytyksiä sille, millaiset asiakirjat voivat toimia henkilöllisyystodistuksina tai mitkä asiakirjat tulee hyväksyä. Virallinen henkilöllisyystodistus on vanha nimike, josta luovuttiin nimenomaisesti 1980-luvun lopussa, kun siirryttiin paperisista henkilöllisyystodistuksista henkilökortteihin.³¹ Nykyisin lainsäädäntö ja henkilöllisyyden osoittamisen käytännöt perustuvat yhtäältä tiettyjen viranomaisen myöntämien asiakirjojen sääntelyyn (passi, henkilökortti) sekä toisaalta tietyssä viranomaisessa, toimialalla tai asiointitapahtumassa tapahtuvan kasvokkain tehtävän tunnistamisen sääntelyyn eri laeissa. Kasvokkain tehtävän henkilöllisyyden todentamisen tavat ovat lisäksi käytännössä voineet muotoutua moninaisiksi.

Passi ja henkilökortti ovat poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja. Ne ovat tietyin henkilökortteja koskevin poikkeuksin myös matkustusasiakirjoja. Passilaissa ja henkilökorttilaissa säädetään esimerkiksi näiden asiakirjojen myöntämisestä, luovuttamisesta ja peruuttamisesta. Keskeiseksi niissä säädetään niistä edellytyksistä, joilla asiakirja voidaan myöntää, ja henkilön tunnistamisesta passia tai henkilökorttia myönnettäessä. Passilaissa ei säädetä nimenomaisesti sen asemasta henkilöllisyyttä osoittavana asiakirjana, mutta henkilökorttilain 1 §:n mukaan laissa säädetään Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle henkilöllisyyden osoitukseksi myönnettävästä henkilökortista. Lait eivät erikseen velvoita toimijoita hyväksymään asiakirjoja henkilöllisyystodisteina tai henkilöä tunnistettaessa.

³¹ Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) - Työryhmän loppuraportti (Sisäasiainministeriön julkaisu 32/2010, s. 31)

Passilaissa ja henkilökorttilaissa säädetään, että hakijan on lähtökohtaisesti passia tai henkilökorttia hakiessaan esitettävä voimassa oleva henkilöllisyyttä osoittava asiakirja. Poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista säädetään tarkemmin valtioneuvoston asetuksella. Passeista ja henkilökorteista annetussa valtioneuvoston asetuksessa (1167/2016) säädetään seuraavaa:

Tunnistamisasiakirjana henkilökorttia ja passia haettaessa hyväksytään passilain (671/2006) 3, 3 a–3 c ja 4 §:ssä tarkoitettu voimassa oleva passi, henkilökorttilain (663/2016) 1 §:n 1 ja 2 momentissa tarkoitettu voimassa oleva henkilökortti sekä ulkomaalaislain (301/2004) 134 §:ssä tarkoitettu muukalaispassi ja 135 §:ssä tarkoitettu pakolaisen matkustusasiakirja.

Jos 1 momentissa tarkoitettu muukalaispassissa tai pakolaisen matkustusasiakirjassa on ulkomaalaislain 136 §:n 5 momentissa tarkoitettu merkintä selvittämättömästä henkilöllisyydestä, asiakirjaa ei kuitenkaan hyväksytä tunnistamisasiakirjana passi- ja henkilökorttimenettelyssä.

Asetus koskee nimenomaisesti vain sitä, mitkä asiakirjat hyväksytään henkilöllisyyttä osoittaviksi myönnettäessä passia ja henkilökorttia. Käytännössä se kuitenkin asettaa hyväksyttävän menettelyn tason myös muussa asiointissa, jossa henkilöllisyydestä on varmistettava korkealla luotettavuudella.

Lainsäädännössä on voitu erikseen säätää jossakin fyysisessä asiointitapahtumassa tehtävästä tunnistamisesta tai henkilöllisyyden osoittamisesta. Näissä yhteyksissä määritellään myös, millä asiakirjalla tai menettelyllä tunnistaminen tapahtuu. Tämä voi tapahtua yleisesti tai edellyttämällä erityisesti passin tai henkilökortin käyttämistä. Tunnistuksen mukaan henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan. Esimerkkinä yleisestä luotettavuuden vaatimuksesta on rahanpesusääntely, jossa edellytetään asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella.

6.8.2. Henkilökortin sääntely

Henkilökorttilaissa (663/2016) säädetään Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle henkilöllisyyden osoitukseksi myönnettävästä henkilökortista. Laissa säädetty koskee tietysti myös ulkomaalaisen henkilökortista, alaikäisen henkilökorttia ja väliaikaista henkilökorttia. Henkilökortin myöntää poliisilaitos.

Alaikäinen voi saada sekä tavallisen henkilökortin että erityisen alaikäisen henkilökortin. Alaikäisen henkilökortti voidaan myöntää ilman huoltajan suostumusta eikä se toimi matkustusasiakirjana. Tavallinen henkilökortti voidaan myöntää alaikäiselle hakijalle lähtökohtaisesti vain huoltajien suostumuksella.

Henkilökortti on lain 2 §:n mukaan myös matkustusasiakirja, kun se on myönnetty Suomen kansalaiselle. Matkustusasiakirjoja eivät kuitenkaan ole alaikäisen henkilökortti, väliaikainen henkilökortti tai pelkkään sähköiseen asiointiin tarkoitettu henkilökortti, joka voidaan myöntää rikoksesta epäillylle tai tuomitulle ennen rangaistuksen suorittamista.

Henkilökorttiin sisältyy väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 61 §:n 3 momentissa tarkoitettu Digi- ja väestötietoviraston myöntämä kansalaisvarmenne. Tämä ei koske alaikäisen henkilökorttia eikä väliaikaista henkilökorttia.

Henkilökortin myöntämisen edellytyksenä on, että hakija on tunnistettu ja hänen henkilöllisyytensä on luotettavasti todennettu. Hakijan on henkilökorttia hakiessaan esitettävä voimassa oleva henkilöllisyyttä osoittava asiakirja. Jos hakijalla ei ole esittää tällaista asiakirjaa, henkilökortin myöntävä viranomainen tunnistaa hakijan ja todentaa tämän henkilöllisyyden. Sähköinen asiointi edellyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) tarkoitettua tunnistusvälinettä.

7. Toimintamallin kilpailu- ja valtioneuvosto-oikeudelliset näkökohdat

7.1. Yleisesti kilpailu- ja valtioneuvosto-oikeudellisesta

7.1.1. Soveltamisala ja taloudellisen toiminnan käsite

Kilpailu- ja valtioneuvosto-oikeudellisuus koskee kaikkia taloudellista toimintaa harjoittavia yksiköitä, riippumatta niiden oikeudellisesta muodosta tai rahoitustavasta. Taloudellisen toiminnan arviointi on toiminta- ei organisaatiokohtaista. Kilpailu- ja valtioneuvosto-oikeudellisuutta sovelletaan lähtökohtaisesti kaikkeen toimintaan, jossa palveluja tai tavaroita tarjotaan markkinoilla.³² Esimerkiksi kansallisen lainsäädännön tuoma asema osana julkista hallintoa ei ole tässä suhteessa merkityksellistä.

³² Kts. esim. yhteisöjen tuomioistuimen tuomio 16.6.1987, komissio v. Italia, 118/85, ECLI:EU:C:1987:283, 7 kohta; yhteisöjen tuomioistuimen tuomio 18.6.1998, komissio v. Italia, C-35/96, ECLI:EU:C:1998:303, 36 kohta; yhteisöjen tuomioistuimen tuomio 12.9.2000, Pavlov ym., yhdistetyt asiat C-180/98–C-184/98, ECLI:EU:C:2000:428, 75 kohta.

Arvioitaessa sitä, onko kyse taloudellisesta toiminnasta, voidaan tarkastella esimerkiksi sitä, onko palveluille olemassa markkina taikka olisivatko muut toimijat halukkaita ja kykeneviä tuottamaan palvelua markkinalla. Taloudellisten ja muiden kuin taloudellisten toimintojen välinen ero riippuu jossain määrin myös valtion poliittisista valinnoista ja taloudellisesta kehityksestä. Toiminta, joka yhdessä jäsenvaltiossa katsottaisiin taloudelliseksi ei välttämättä ole sitä toisessa jäsenvaltiossa.³³

Arvioinnissa on annettu painoarvoa esimerkiksi sille, harjoitetaanko vastaavaa toimintaa markkinoille yksityisten toimesta³⁴ vai onko palvelutuotanto kokonaisuutena varattu julkishallinnolle³⁵. Esimerkiksi tapauksessa *Ambulanz Glöckner* (C-475/99) EU-tuomioistuimien katsoi, että sairaankuljetusten tarjoaminen oli taloudellista toimintaa pelkästään sillä perusteella, että palveluita oli aikaisemmin tarjonnut yksityinen toimija.³⁶ Toiminta voi myös olla taloudellista sillä perusteella, että muut toiminnanharjoittajat olisivat halukkaita ja pystyisivät tuottamaan palvelua markkinoilla. Arvioinnissa ei myöskään ole merkitystä sillä, että jokin palvelu tuotetaan itse.³⁷ Esimerkiksi viranomaisen päätös olla sallimatta sitä, että kolmannet osapuolet tuottaisivat tiettyä palvelua, ei tarkoita, etteikö kyse voisi olla taloudellisesta toiminnasta.³⁸

Kiellettyä valtiontukea tai kilpailuneutraliteettia koskeva sääntely ei tule sovellettavaksi, kun kyse on viranomaisesta, joka toimii julkisen vallan käyttäjänä tai viranomaisen ominaisuudessaan. Julkisen sektorin elimen voidaan katsoa toimivan julkisen vallan käyttäjänä, kun kyseessä oleva toiminta kuuluu valtion keskeisiin tehtäviin tai liittyy näihin tehtäviin luonteeltaan, tavoitteeltaan sekä siihen sovellettavilta säännöiltään.³⁹ Jos jäsenvaltio ei ole päättänyt ottaa käyttöön markkinamekanismeja, toiminnot, jotka luontaisesti ovat osa viranomaisten erioikeuksia ja joiden suorittamisesta valtio vastaa, eivät yleensä ole taloudellisia toimintoja.⁴⁰

Taloudellisen toiminnan arviointi on toiminta- ei organisaatiokohtaista. Jos julkisyhteisö harjoittaa taloudellista toimintaa, joka voidaan erottaa julkisen vallan käytöstä, tulee valtiontuen mahdollisuus arvioitavaksi tämän toiminnan

³³ Komission tiedonanto Euroopan unionin toiminnasta tehdyn sopimuksen 107 artiklan 1 kohdassa tarkoitettusta valtiontuen käsitteestä (2016/C 262/01), para 13.

³⁴ Kuoppamäki, Petri: Uusi kilpailuoikeus (2018, Alma Talent), s. 58. (Alma Verkkokirjahylly, 18.1.2021 14:33:12)

³⁵ Kuoppamäki, s. 59.

³⁶ Kuoppamäki, s. 59.

³⁷ Komission tiedonanto (2016/C 262/01), para 14.

³⁸ Komission tiedonanto (2016/C 262/01), para 14.

³⁹ Yhteisöjen tuomioistuimen tuomio 16.6.1987, komissio v. Italia, 118/85, ECLI:EU:C:1987:283, 7 ja 8 kohta.

⁴⁰ Komission tiedonanto (2016/C 262/01), para 17; HE 40/2013 vp, s. 31.

osalta. Jos sitä vastoin taloudellista toimintaa ei voida erottaa julkisen vallan käytöstä, kaikki kyseisen yhteisön toiminnot liittyvät edelleen julkisen vallan käyttöön⁴¹.

Kokonaisuudessaan on huomattava, että toiminnan luonne voi myös muuttua ajan mittaan. Taloudellisten ja muiden kuin taloudellisten toimintojen välinen ero riippuu jossain määrin jäsenvaltioiden poliittisista valinnoista ja taloudellisesta kehityksestä. Toiminta, joka on tänään taloudellista voi tulevaisuudessa myös lakata olemasta taloudellista, ja päinvastoin.⁴²

7.1.2. Kilpailuneutraliteetti

Kilpailulain (948/2011) 4 a luku turvaa yksityisen ja julkisen välistä kilpailuneutraliteettiä. Kilpailuneutraliteetti tarkoittaa sitä, että julkisella ja yksityisellä elinkeinotoiminnalla on tasapuoliset toimintaedellytykset. Kilpailulain kilpailuneutraliteettia turvaavien säännösten tavoitteena on varmistaa, että julkiset toimijat eivät saa kilpailuetuja, joita yksityiset toimijat eivät voi saada ja jotka voivat vääristää kilpailua. Sääntelyn taustalla on julkisten toimijoiden erilainen asema suhteessa yksityiseen sektoriin. Julkisen sektorin harjoittama toiminta voi olla etulyöntiasemassa johtuen lainsäädännöstä, omistussuhteista, rahoituksesta tai muista institutionaalisista tekijöistä⁴³. Kilpailuneutraliteettivajeen seurauksena tehokkaita yrityksiä saattaisi poistua markkinoilta, kannusteet uusien tuotteiden ja tuotantotapojen kehittämiseen laimenisivat ja tuotannon kilpailuttamisen edellytykset kärsisivät taantuvista markkinoista (HE 40/2013 vp, s. 22). Tarkoituksena on varmistaa yhtenäiset kilpailuolosuhteet, ei estää julkisia toimijoita tarjoamasta palveluita⁴⁴.

KKV:n on kilpailulain 30 a §:n mukaan pyrittävä poistamaan menettely tai rakenne, joka vääristää tai on omiaan vääristämään terveen ja toimivan kilpailun edellytyksiä markkinoilla taikka estää tai on omiaan estämään terveen ja toimivan taloudellisen kilpailun syntymistä tai kehittymistä. Tarkastelu koskee taloudellista toimintaa (kts. yllä). Kilpailua vääristävällä tai estävällä rakenteella tarkoitetaan esimerkiksi liikelaitos- tai virastorakenteessa harjoitettua elinkeinotoimintaa, joka rakenteesta johtuvien verotuksellisten etujen ja konkurssisuojaan vuoksi saattaa vääristää kilpailua yksityisten toimijoiden kanssa (HE 40/2013 vp, s. 33). Kilpailua vääristävällä tai estävällä

⁴¹ Komission tiedonanto (2016/C 262/01), para 18.

⁴² Komission tiedonanto (2016/C 262/01), para 13 ja 15.

⁴³ Oinonen, Mika: EU:n ja Suomen kilpailuvalvonta, s. 267. (Alma Verkkokirjahylly 27.4.2020 10:10:31). Kts. myös HE 40/2013 vp, s. 22.

⁴⁴ Oinonen, s. 266.

menettelyllä tarkoitetaan kaikkia sellaisia toimintatapoja, joiden seurauksena kilpailu ei ole tasapuolista julkisen ja yksityisen sektorin elinkeinotoiminnan välillä (HE 40/2013 vp, s. 32). Kielletty menettely voi ilmetä esimerkiksi julkishallinnon yksikön mahdollisuutena hyödyntää taloudellisessa toiminnassaan viranomaistoiminnassa saatuja tietovarantoja tai markkinahintaisia tukipalveluja, kustannuksia vastaamattomana alihinnoitteluna, taloudellisen toiminnan ja muun toiminnan välisenä ristisubventiona taikka julkisyhteisön harjoittamaan taloudelliseen toimintaan kohdistuvana valikoivana tukena (HE 40/2013 vp, s. 32-33). Arvio on tehtävä aina tapauskohtaisesti.

Kun kysymys on taloudellisesta toiminnasta, pelkästään tehtävästä säätäminen lain tasolla ei sinänsä estä neutraliteettisääntösten soveltumista. Neutraliteettisääntelyn soveltamiskoikeudesta koskevan kilpailulain 30 b §:n soveltamiskynnys on korkea. Kilpailulain esitöiden mukaan kilpailun vääristymiseen tai estymiseen ei voitaisi puuttua, jos kielteiset vaikutukset kilpailuun seuraavat väistämättä lainsäädännöstä ilman, että taloudellisesta toiminnasta vastaavalla taholla olisi harkintavaltaa tai liikkumavaraa kilpailuneutraliteettia vaarantavan taloudellisen lopputuloksen osalta (HE 40/2013 vp).

Vaikka valtion lähtökohtaisesti katsottaisiin harjoittavan taloudellista toimintaa markkinoilla, julkisen sektorin elinkeinotoimintaan voi liittyä myös yhteiskunnallisia tavoitteita, joita ei voida sivuuttaa yksin kilpailun tasapuolisuuden vaatimuksen perusteella. Kilpailuneutraliteetin vajeeseen puututtaessa tulisi ottaa huomioon myös yleisemmät yhteiskunnalliset tavoitteet, joita toiminnalla toteutetaan ja punnita niitä kilpailun vääristymisestä aiheutuvaan haittaan. Kilpailulaki sisältää poikkeuksen merkittävään kansalaisten hyvinvointiin, turvallisuuteen tai muuhun sellaiseen yleiseen etuun liittyville tehtäville, jos kilpailuneutraliteettisääntelyn soveltaminen johtaisi siihen, ettei tällaisia etuja voitaisi tarkoitettulla tavalla turvata kansalaisille. Poikkeuksen soveltaminen edellyttäisi, että yleisen edun toteuttaminen olisi tosiasiallisesti mahdotonta ilman kilpailuneutraliteettia vaarantavia vaikutuksia ja ettei yleistä etua voitaisi toteuttaa vähemmän kilpailuneutraliteettia vaarantavalla tavalla. (HE 40/2013 vp, s. 23)

7.1.3. Kielletty valtiontuki

Kiellettyä valtiontukea on SEUT 107 artiklan pääsäännön mukaan jäsenvaltion myöntämä taikka valtion varoista muodossa tai toisessa myönnetty tuki, joka vääristää tai uhkaa vääristää kilpailua suosimalla jotakin yritystä tai tuotannonalaa, siltä osin kuin se vaikuttaa jäsenvaltioiden väliseen kauppaan.

Euroopan unionin tuomioistuin määrittelee yritykset taloudellista toimintaa harjoittaviksi yksiköiksi, riippumatta niiden oikeudellisesta muodosta ja rahoitustavasta⁴⁵. Edellä on kuvattu tarkemmin taloudellisen toiminnan arviointia ja tältä osin valtiontukisääntelyn soveltamisalaa.

Kielletyn valtiontuen käsitteeseen katsotaan sisältyvän neljä edellytystä:

1. Kyse on valtion toimenpiteestä ja valtion varoilla toteutetusta toimenpiteestä.
2. Toimenpide vääristää tai uhkaa vääristää kilpailua.
3. Toimenpide on omiaan vaikuttamaan jäsenvaltioiden väliseen kauppaan.
4. Toimenpide antaa etua sille, joka on toimenpiteen kohteena.⁴⁶

Valtiontuen käsite on objektiivinen ja oikeudellinen käsite, joka on määritelty suoraan sopimuksessa Euroopan unionin toiminnasta. Komissio on antanut tiedonannon Euroopan unionin toiminnasta tehdyn sopimuksen 107 artiklan 1 kohdassa tarkoitetusta valtiontuen käsitteestä (2016/C 262/01), mutta viime kädessä perussopimusta ja valtiontuen käsitettä tulkitsee unionin tuomioistuin.

Edun myöntäminen suoraan tai välillisesti valtion varoista ja toimenpiteen katsominen valtion toteuttamaksi ovat kaksi erillistä ja yhteisesti vaikuttavaa ehtoa valtiontuen olemassaololle.⁴⁷ Tapauksissa, joissa viranomaisen myöntää edun tuensaajalle, toimenpide on peräisin valtiolta, vaikka kyseinen viranomaisen olisi oikeudellisesti riippumaton muista viranomaisista. Sama pätee, kun viranomaisen nimeää yksityisen tai julkisen tahon hallinnoimaan toimenpidettä, joka tuottaa edun.⁴⁸ Julkisen yrityksen toteuttaman toimenpiteen voidaan päätellä johtuvan valtiosta asiaa koskevien seikkojen ja toimenpiteen toteuttamishetkellä vallinneiden olosuhteiden perusteella.⁴⁹ Valtion varat taas käsittävät kaikki julkisen sektorin varat, kuten jäsenvaltioiden alueviranomaisten varat ja tietyissä tilanteissa yksityisten elinten varat.⁵⁰ Se, että etua tuovaa toimenpidettä ei rahoita valtio suoraan vaan julkinen tai yksityinen elin, jonka valtio on perustanut tai nimennyt hallinnoimaan tukea, ei välttämättä tarkoita, että kyseistä toimenpidettä ei rahoiteta valtion varoista.⁵¹

⁴⁵ Komission tiedonanto (2016/C 262/01), para 7.

⁴⁶ Alkio, Mikko: Valtiontuet, 2.1 Tuen käsitteestä (Alma verkkokirjahylly 6.5.2020 13:58:6)

⁴⁷ Komission tiedonanto (2016/C 262/01), para 38.

⁴⁸ Komission tiedonanto (2016/C 262/01), para 39.

⁴⁹ Komission tiedonanto (2016/C 262/01), para 42.

⁵⁰ Komission tiedonanto (2016/C 262/01), para 48.

⁵¹ Komission tiedonanto (2016/C 262/01), para 50.

Valtiontuen antama etu on mikä tahansa taloudellinen hyöty, jota yritys ei olisi voinut saada tavanomaisissa markkinaolosuhteissa, toisin sanoen ilman valtion toimenpidettä.⁵² Kun arvioidaan toimenpiteen antamaa etua, merkitystä on ainoastaan toimenpiteen vaikutuksilla yritykseen, ei valtion toimenpiteen syyllä eikä tavoitteella. Edusta on kyse aina, kun yrityksen taloudellinen tilanne paranee sellaisen valtion toimenpiteen johdosta, jonka ehdot poikkeavat tavanomaisista markkinaehdoista.⁵³

Valtiontukikäsitteen piiriin eivät kuulu kaikki talouden toimijoita suosivat toimenpiteet, vaan ainoastaan ne, joilla myönnetään etua tietyille valikoiduille yrityksille tai yrityslajeille tai toimialoille.⁵⁴ Toimenpiteen aineellinen valikoivuus merkitsee sitä, että toimenpide koskee ainoastaan tiettyjä yrityksiä (yrityksryhmiä) tai tiettyjä toimialoja tietyssä jäsenvaltiossa. Aineellinen valikoivuus voidaan osoittaa oikeudellisesti tai tosiasiallisesti.⁵⁵ Alueellinen valikoivuus arvioidaan maantieteellisesti ja sellaiset toimenpiteet, joiden soveltamisala kattaa jäsenvaltion koko alueen, eivät kuulu alueellista valikoivuutta koskevan kriteerin piiriin. Kaikki toimenpiteet, joita sovelletaan vain tiettyihin jäsenvaltion osiin, eivät kuitenkaan ole automaattisesti valikoivia.⁵⁶

Valtion toimenpiteen katsotaan vääristävän tai uhkaavan vääristää kilpailua, jos se on omiaan parantamaan tuensaajan kilpailuasemaa verrattuna muihin yrityksiin, joiden kanssa se kilpailee. Käytännössä kilpailun katsotaan yleensä vääristyvän perussopimuksen 107 artiklan 1 kohdan mukaisesti, jos valtio myöntää taloudellista etua yritykselle kilpailulle vapautetulla alalla, jolla on tai voisi olla kilpailua.⁵⁷

Kauppaan kohdistuvan vaikutuksen osalta on riittävää, että tuki on omiaan vaikuttamaan kauppaan. Unionin tuomioistuimet ovat erityisesti todenneet, että kun ”tuki vahvistaa yrityksen asemaa jäsenvaltioiden välisessä kaupassa muihin, kilpaileviin yrityksiin verrattuna, tuen on katsottava vaikuttavan jäsenvaltioiden väliseen kauppaan”⁵⁸ Julkisen tuen voidaan katsoa pystyvän vaikuttamaan jäsenvaltioiden väliseen kauppaan, vaikka tuensaaja ei ole suoraan mukana rajat ylittävässä kaupassa. Esimerkiksi tuki voi vaikeuttaa

⁵² Komission tiedonanto (2016/C 262/01), para 66.

⁵³ Komission tiedonanto (2016/C 262/01), para 67.

⁵⁴ Komission tiedonanto (2016/C 262/01), para 117.

⁵⁵ Komission tiedonanto (2016/C 262/01), para 120.

⁵⁶ Komission tiedonanto (2016/C 262/01), para 142.

⁵⁷ Komission tiedonanto (2016/C 262/01), para 187.

⁵⁸ Komission tiedonanto (2016/C 262/01), para 190.

muihin jäsenvaltioihin sijoittautuneiden toimijoiden pääsyä markkinoille ylläpitämällä tai lisäämällä paikallista tarjontaa.⁵⁹

7.2. Toiminnallinen ratkaisu kilpailu- ja valtiontukioikeudellisesta näkökulmasta

7.2.1. Toiminnallisen ratkaisun elementit

Edellä on kuvattu digitaalinen henkilöllisyys –hankkeen tavoitteita sekä niitä toiminnallisia ratkaisuja, joilla näitä tavoitteita on tarkoitus edistää. Tässä arviomuistiossa kuvatusta ratkaisusta voidaan tunnistaa neljä kokonaisuutta, joita niiden luonteen vuoksi on arvioitava oikeudellisesta näkökulmasta erillisinä. Näitä ovat:

1. Digitaalisen identiteetin muodostaminen ja myöntäminen.
2. Ratkaisut, jotka mahdollistavat digitaalisen henkilöllisyyden osoittamisen käyntiasioinnissa.
3. Ratkaisut, jotka mahdollistavat muiden viranomaistietojen, kuten lupien tai vahvistettujen rekisteritietojen esittämisen.
4. Digitaalisen henkilöllisyyden osoittaminen julkisen sektorin asiointipalveluissa sähköisesti.

Näitä kokonaisuuksia arvioidaan seuraavissa osissa 7.2.2.-7.2.5. kilpailu- ja valtiontukisääntelyn näkökulmasta. Hankkeessa on selvitetty, missä määrin toiminnallisiin ratkaisuihin sisältyy riskejä siitä, että toimintaan sovellettaisiin kilpailuneutraliteettia ja kiellettyä valtiontukea koskevaa sääntelyä, ja että tämä sääntely voisi muodostua esteeksi hankkeen toteuttamiselle tai asettaisi merkittäviä rajoitteita ratkaisujen toteutukselle. Alustava johtopäätös on, että olennaisilta osin suunniteltu toiminta on perusteltua. Analyysiä on kuitenkin jatkettava hankkeen aikana suhteessa ratkaisujen tarkentuviin yksityiskohtiin.

Hanke kattaa osin myös yksityisen sektorin sähköisiin asiointipalveluihin liittyviä tavoitteita. Arviomuistion toiminnallisessa osassa ei vielä esitetä konkreettisia ratkaisuja, jotka olisivat suoraan käytettävissä sellaisiin tunnistuspalveluihin tai sähköisiin asiointipalveluihin, joita yksityinen sektori tarjoaa. Esitettävät ratkaisut voisivat kuitenkin tuottaa hyötyjä myös tunnistuspalveluiden tarjoajille tai yksityisen sektorin sähköisille asiointipalveluille, mutta ne edellyttävät myös yksityisen sektorin palveluiden kehittämistä. Hankkeen edetessä ja myös yksityisellä sektorilla hyödynnettävien ratkaisujen tarkentuessa, on tehtävä vielä erikseen erityisesti valtiontuki- ja kilpailuoikeudellinen arvio näiden ratkaisujen osalta.

⁵⁹ Komission tiedonanto (2016/C 262/01), para 191.

7.2.2. Digitaalisen identiteetin muodostaminen

Digitaalisen identiteetin muodostamisella tarkoitetaan menettelyä, jossa väestötietojärjestelmään rekisteröidyn henkilön ydinidentiteetti yhdistetään luonnolliseen henkilöön. Tästä yhteydestä luodaan digitaalinen todistus, joka vastaisi luonteeltaan nykyistä kansalaisvarmenteen tunnistusvarmennetta: sen tarkoitus on luotettavasti ja muuttamattomasti todentaa, että ydinidentiteetti kuuluu tietylle luonnolliselle henkilölle.

Lähtökohtaisesti tämä tapahtuisi poliisin passin tai henkilökortin myöntämisprosessissa siten, että prosessi ja siihen osallistuvat toimijat olisivat pitkälti samat, kuin henkilökortin sirulle myönnettävää kansalaisvarmennetta luotaessa. Toissijaisesti käyttöönotto voitaisiin myös mahdollistaa jälkikäteen siten, että henkilöllisyys todistetaan olemassa olevan passin avulla ja suoritetaan digitaalisesti biometrinen vertailu. Molemmissa tapauksissa digitaalisen henkilöllisyyden muodostaminen perustuu siihen, että viranomaisen yhdistää vahvistetun väestötietojärjestelmään rekisteröidyn ydinidentiteetin ja tietyn luonnollisen henkilön. Jälkimmäisessä tapauksessa yhdistäminen on tapahtunut kertaalleen passia myönnettäessä ja viranomaisen vahvistaa digitaalisessa menettelyssä, että nimenomaan tämä luonnollinen henkilö esittää voimassa olevan passin ja tälle voidaan myöntää digitaalinen henkilöllisyys.

Väestötietolain 5 §:n mukaan väestötietojärjestelmää pidetään yhteiskunnan toimintojen ja tietohuollon sekä sen jäsenille kuuluvien oikeuksien ja velvollisuuksien mahdollistamiseksi, toteuttamiseksi ja turvaamiseksi. Väestötietojärjestelmässä luotu identiteetti on keskeinen yksilön oikeusaseman kannalta ja heijastaa niitä oikeuksia, jotka henkilöllä Suomalaisen yhteiskunnan osana on. Rekisteritietojen pohjalta voidaan tietojen julkisen luotettavuuden nojalla tehdä myös yksilön oikeuksiin ja velvollisuuksiin vaikuttavia hallinnollisia ratkaisuja. Tämän identiteetin luominen ja ylläpito on Digi- ja väestötietovirastolle säädetty viranomaistehtävä.

Fyysisen henkilön yhdistäminen tämän VTJ:stä ilmenevään ydinidentiteettiin tunnistustapahtumassa on perinteisesti ollut viranomaistehtävä. Sisäministeriön identiteettiohjelman loppuraportissa (Sisäasiainministeriön julkaisuja 32/2010) on todettu, että poliisin lakisääteinen perustehtävä on myöntää henkilöllisyyttä osoittavat asiakirjat. Toisin sanoen poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja ovat vain henkilökortti ja passi. Asiakirjan luotettavuus ei perustu pelkästään sen vaikeaan fyysiseen väärennettävyyteen vaan myös ja eritoten myöntöprosessin luotettavuuteen. Myöntöprosessissa poliisi tunnistaa henkilön luotettavasti ja myöntää turvatasoltaan korkeatasoisen, vaikeasti väärennettävän asiakirjan. Poliisi siis myöntää todistuksen henkilöllisyydestä.

Passin ja henkilökortin myöntämisen osalta kyse on hallintotoiminnasta ja merkittävästä julkisen vallan käytöstä.⁶⁰

Yllä kuvattu toimenpide, jossa viranomaisen yhdistää fyysisen luonnollisen henkilön tämän ydinidentiteettiin ja muodostaa liitoksesta digitaalisen todistuksen tai kredentiaalin voidaan rinnastaa passin ja henkilökortin myöntämiseen viranomaistehtävänä. Valtion takaaman henkilöllisyyden suojeleminen liittyy keskeisesti henkilön oikeusturvaan ja viranomaisen myötävaikutus kredentiaalin myöntämisessä varmistaa sen luotettavuuden.

Säädettäessä voimassa olevaa väestötietolakia katsottiin, että tietoyhteiskunnan ja turvallisen sähköisen asioinnin perusedellytysten takaaminen sekä sähköisessä asiointitapahtumassa tarvittavan sähköisen henkilöllisyyden luominen kansalaisille ovat luonteeltaan sellaisia yhteiskunnan perustoimintoihin kuuluvia tehtäviä, joiden hoitaminen tulisi olla julkisen vallan vastuulla. (HE 89/2008 vp)

Kilpailu- ja valtiontukioikeudellisesta näkökulmasta yksikön katsotaan toimivan julkisen vallan käyttäjänä silloin, kun kyseessä oleva toiminta kuuluu valtion keskeisiin tehtäviin tai liittyy näihin tehtäviin luonteeltaan, tavoitteeltaan sekä siihen sovellettavilta säännöiltään.⁶¹ Yleisesti ottaen toiminnot, jotka luontaisesti ovat osa viranomaisten erioikeuksia ja joiden suorittamisesta valtio vastaa, eivät ole taloudellisia toimintoja, ellei jäsenvaltio ole päättänyt ottaa käyttöön markkinamekanismeja.⁶² Esimerkiksi Digi- ja väestötietoviraston kansalaisvarmenteita koskevaa palvelun tarjontaa on pidetty julkisen vallan käyttönä eikä kansalaisvarmennetta ole pidetty taloudellisena toimintana, vaan julkisen vallan käyttönä tunnistusvälineen tarjoamisessa (HE 36/2009 vp, s.87). Kansalaisvarmenteen tuottaminen on kuitenkin henkilökorttilaissa (663/2016) sidottu henkilökorttiin.

Henkilön ydinidentiteetin luominen ja ylläpito väestötietojärjestelmässä on selkeästi julkisen vallan käyttöä. Tähän identiteettiin pohjautuvien virallisten henkilöllisyyttä osoittavien asiakirjojen (passin ja henkilökortin) myöntäminen on sekin julkisen vallan käyttöä. Kun viranomaisen yhdistää fyysisen luonnollisen henkilön tämän väestötietojärjestelmään perustuvaan ydinidentiteettiin ja liitoksesta muodostetaan digitaalinen todistus yhteiskunnan

⁶⁰ Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. (Sisäasiainministeriön julkaisuja 32/2010)s, 28.

⁶¹ C-364/92, SAT v. Eurocontrol, Kok. 1994, s. I-43, 30 kohta

⁶² Komission tiedonanto Euroopan unionin valtiontukisääntöjen soveltamisesta yleisiin taloudellisiin tarkoituksiin liittyvien palvelujen tuottamisesta myönnettävään korvaukseen, OJ C 8 02 11.1.2012, s. 4, kappale 16

toiminnoissa hyödynnettäväksi, ollaan henkilön oikeusaseman näkökulmasta vastaavassa tilanteessa kuin passia tai henkilökorttia myönnettäessä.

Digitaalinen identiteetti, eli käytännössä viranomaisen vahvistama ja luoma digitaalinen todistus luonnollisen henkilön ja virallisen rekisteri-identiteetin yhteydestä, vastaisi luonteeltaan passin tai henkilökortin käyttöä virallisen henkilöllisyyttä osoittavan asiakirjana. Tällaisen aseman edellyttämiä lainsäädännön muutostarpeita on kuvattu tarkemmin jäljempänä osassa 8.1. Henkilökortin ja passin myöntäminen on viranomaisille kuuluva yksinoikeus (HE 36/2009 vp, s.87). Digitaalisen identiteetin luomista ja myöntämistä voidaan verrata näiden asiakirjojen myöntämiseen, olettaen että sen asema vahvistetaan lainsäädännössä. Vaikka yksityiset toimijat voivat myöhemmin asiakirjojen avulla todentaa henkilöllisyyden ja todeta niiden perusteella yhteyden luonnollisen henkilön ja identiteetin välillä, asiakirjan luonteeseen kuuluu keskeisesti julkisen vallan käyttö. Vaikka yksityiset toimijat voisivat myös digitaalisen identiteetin pohjalta todeta yhteyden luonnollisen henkilön ja identiteetin välillä ja myöntää omia tunnistusvälineitään, laissa säädetyn digitaalisen todisteen myöntäminen olisi julkisen vallan käyttöä.

Digitaalisen identiteetin muodostaminen, eli valtion takaaman ydinidentiteetin muodostaminen digitaalisessa muodossa, olisi julkisen vallan käyttöä eikä siihen pitäisi liittyä riskiä siitä, että sitä pidettäisiin taloudellisena toimintana. Tämä edellyttäisi kuitenkin, että digitaalisen identiteetin muodostaminen osoitettaisiin lailla viranomaisen tehtäväksi ja identiteetin asemasta henkilöllisyyttä osoittavana asiakirjana tai vastaavana sähköisenä todisteena säädettäisiin erikseen.

Ratkaisun arvioinnin osalta on myös huomioitava mahdollisuus, että digitaalinen identiteetti myönnettäisiin olemassa olevia vahvan sähköisen tunnistuksen välineitä käyttäen. Tällöin yksityisen sektorin toimija on suorittanut ensitunnistuksen tunnistuslain mukaisesti, ja identiteetin taustalla on olemassa oleva viranomaisen henkilöllisyysasiakirja. Digitaalista identiteettiä myönnettäessä kyse olisi tällöinkin siitä, että viranomainen muodostaa julkista valtaa käyttäen yhteyden luonnollisen henkilön ja rekisteri-identiteetin välillä digitaalisesti todisteeksi. Tällaisessa tilanteessa päätös kuitenkin perustuisi siihen, että henkilöllä on hallussaan vahvan sähköisen tunnistamisen väline, ja viranomainen luottaa tunnistustapahtuman osoittavan tämän yhteyden. Olennaista on, että tässäkin tilanteessa viranomainen tekee julkista valtaa käyttäen päätöksen siitä, että yhteys on riittävällä tavalla osoitettu. Päätöksen tekevä virkamies toimii virkavastuulla. Näiden tilanteiden osalta on kuitenkin jatkovalmistelussa arvioitava tarkemmin yksityisen sektorin tunnistusvälineen

vaikutusta digitaaliselle identiteetille sekä erityisesti vastuukysymyksiä ja niiden yhteyttä julkisen vallan käyttöön.

7.2.3. Sovellus, josta identiteetin voi todentaa käytäntöissä

Hankkeessa luodaan mobiilisovellus, jolla digitaalinen identiteetti voitaisiin todentaa käytäntöissä yhteydessä samalla tavoin kuin henkilöllisyys voidaan todentaa henkilökortista tai passista. Vaikka identiteetti olisi digitaalinen ja henkilöllisyys osoitettaisiin digitaalisesti, mobiilisovelluksen käyttö rinnastuisi lähinnä passiin tai henkilökorttiin käyttöön henkilöllisyyttä osoittavina asiakirjoina. On huomattava, että sovellus ei toimisi matkustusasiakirjana. Digitaalisen identiteetin suhteesta henkilöllisyyden osoittamisen sääntelyyn on arvioitu jäljempänä osassa 8.1.

Olettaen, että mobiilisovelluksen ylläpitäminen ja tarjoaminen olisi kytketty digitaalisen identiteetin myöntämiseen ja se olisi säädetty lailla viranomaisen tehtäväksi, mobiilisovelluksen ylläpitämiseen ja tarjoamiseen ei pitäisi liittyä riskiä siitä, että sitä pidettäisiin taloudellisena toimintana. Kysymys olisi virallisen fyysisen henkilöllisyydestä tarjoamiseen rinnastuvasta toimenpiteestä, joka liittyy kiinteästi digitaalisen identiteetin luomiseen ja henkilön mahdollisuuden osoittaa digitaalinen identiteettinsä. Henkilöllisyyttä osoittavien asiakirjojen myöntäminen ja hallinta on viranomaisen lakisääteinen tehtävä, näitä asiakirjoja koskevien erityislakien nojalla, sekä hyvin perinteistä julkisen vallan käyttöä. Olennainen osa näiden asiakirjojen myöntämisestä on sen mahdollistaminen, että niitä voidaan käyttää asiointitilanteissa henkilöllisyyden osoittamiseen. Perinteisten fyysisten asiakirjojen osalta asiakirjan myöntäminen ja sen käytön mahdollistamista ei käytännössä voida erottaa toisistaan. Digitaalisessa toimintamallissa kyse voi teknisessä mielessä olla eri palveluista, mutta yhteys julkisen vallan käyttöön on molempien osalta ilmeinen.

Sovellus ja siihen liittyvät palvelut, jotka mahdollistavat digitaalisen henkilöllisyyden osoittamisen käytäntöissä, ovat viranomaistehtäviä ja julkisen vallan käyttöä. Riskiä taloudellisesta toiminnasta ei ole, kunhan digitaalisen henkilöllisyyden asemasta henkilöllisyyden osoittavana asiakirjana säädetään lailla ja siihen liittyvien palveluiden tuottaminen säädetään lailla viranomaisten tehtäväksi.

Hankkeen toteutukseen ja teknisiin ratkaisuihin liittyvät valinnat voisivat yhdessä markkinoiden kehityksen kanssa johtaa siihen, että markkinoille kehittyisi myöhemmin yksityisten toimijoiden tarjoamia sovelluksia tai palveluita, jotka mahdollistaisivat digitaalisen identiteetin esittämisen asiointitilanteissa. Tästä näkökulmasta on erityisen tärkeää, että viranomaisen

myöntämän digitaalisen identiteetin asema henkilöllisyyttä osoittavana asiakirjana sekä viranomaisten tehtävät palvelun tuottamisessa on säädetty lailla.

7.2.4. Mahdollisuus esittää muita lupia/attribuutteja sovelluksessa

Hankkeen suunnitellussa toimintamallissa henkilö voi osoittaa mobiilisovelluksella myös yksittäisiä ydinidentiteettiin sisältyviä henkilötietoja, esimerkiksi ikänsä, antamatta laajempia henkilöllisyyttä koskevia tietoja. Lisäksi mobiilisovellusta ja toimintamallia suunnitellaan siten, että ratkaisu sisältäisi valmiuden osoittaa myös muita valtion vahvistamia attribuutteja, esimerkiksi henkilökortin sisältämä kasvokuva tai ajoneuvon ajo-oikeus. Hankkeen aikana ei kuitenkaan otettaisi käyttöön tällaisia laajempia ominaisuuksia.

Siltä osin, kun on kyse ydinidentiteettiin sisältyvistä henkilöllisyystiedoista, toiminta vertautuu edelleen henkilöllisyyttä osoittaviin asiakirjoihin ja niiden tuottamiseen julkisen vallan käyttönä. Tätä on käsitelty edellä osassa 7.2.4. Toiminnan luonnetta ei muuta se, että yksittäiset tiedot ovat osoitettavissa siten, että henkilön ei tarvitse esittää koko asiakirjaa tietosisältöineen. Käyttötarkoitus ja viranomaisen rooli on vastaava, mutta sovellus mahdollistaisi tietosuojan ja henkilön yksityisyyden suojan kannalta paremmat menettelyt asiointitapahtumassa.

Siltä osin, kun tarkastellaan muiden kuin ydinidentiteettiin sisältyvien henkilötietojen esittämistä, on arvioinnissa keskeistä esitettävien tietojen alkuperä ja suhde digitaaliseen henkilöllisyyteen.

Suunnitellussa toimintamallissa valmius tietojen esittämisen, kohdistuisi eri julkishallinnon rekistereihin perustuviin tietoihin, kuten viranomaisten myöntämiin lupiin. Siinä määrin, kun kyse on viranomaisen hallussa olevista tiedoista, joista viranomaisen on annettava otteita tai luvista, jotka annetaan henkilölle edelleen esitettäväksi, on toiminnan viranomaisluonne selkeä. Julkisen vallan käytön piirissä olevan digitaalisen henkilöllisyyden osoittaminen yhdistettynä virallistiedon esittämiseen on edelleen katsottava keskeiseksi viranomaistehtäväksi.

Attribuuttien liittämisen mobiilisovellukseen ja niiden esittämisen mobiilisovelluksessa voidaan perustella liittyvän henkilön valtion takaamaan ydinidentiteettiin ja siten edellä kohdissa 7.2.3 ja 7.2.4 käsiteltyihin julkisen vallan käyttönä pidettävään digitaalisen identiteetin muodostamiseen ja mobiilisovelluksen ylläpitämiseen ja tarjoamiseen. Toiminta ei tällaisenaan

sisältäisi riskiä siitä, että se katsottaisiin taloudelliseksi olettaen, että toiminnan perusteista ja viranomaisen tehtävistä säädetään lailla.

Jatkotyössä olisi kuitenkin huomioitava, että muiden tietojen esittäminen sovelluksen yhteydessä ei oletettavasti tulisi viranomaistoiminnan ja julkisen vallan käytön piiriin tavalla, joka poistaisi taloduellisen toiminnan riskin. Näin on erityisesti, mikäli jatkossa markkinoille tulisi myös yksityisten toimijoiden sovelluksia tai palveluita, joissa olisi mahdollista esittää tavalla tai toisella varmennettuja henkilötietoja.

7.2.5. Sovelluksen etäkäyttö: tunnistuspalvelu julkisen sektorin asiointipalveluihin

Taloudellinen toiminta: Valtiontuki- ja kilpailusääntelyn soveltuminen

Hankkeen suunnitellussa toimintamallissa mobiilisovellusta voitaisiin käyttää henkilöllisyyden osoittamiseen myös sähköisesti erilaisissa julkisen sektorin sähköisissä asiointipalveluissa. Ratkaisu tarjottaisiin julkishallinnon asiointipalveluille suomi.fi –tunnistuksen avulla. Suomi.fi –tunnistus todentaisi digitaalisen todisteen aitouden ja voimassaolon ja voisi välittää tarvittavat henkilöllisyystiedot eteenpäin asiointipalvelulle. Suomi.fi –tunnistuksessa ei täten enää tarvitsisi hyödyntää luottamusverkoston tunnistuspalveluita tai henkilökortilla olevaa kansalaisvarmennetta. Arvioitaessa tätä palvelua kilpailu- ja valtiontukisääntelyn valossa on olennaista huomata, että henkilöllisyyden osoittaminen tapahtuu teknisenä menettelynä eri tavoin nykyisen luottamusverkoston avulla ja suunnitellun digitaalisen henkilöllisyyden avulla. Luonnollisen henkilön ja tunnistusta tarvitsevan asiointipalvelun näkökulmasta lopputulos on kuitenkin sama: henkilöllisyys voidaan todentaa ja henkilö kykenee asioimaan palvelussa.

Sen arvioimiseksi, soveltuvatko valtiontuki- ja kilpailusäännökset tiettyyn toimintaan, on ensin arvioitava, onko toiminnassa kyse julkisen vallan käytöstä vai taloudellisesta toiminnasta. Jos toiminta on luonteeltaan taloudellista, valtiontuki- ja kilpailuoikeussäännöt tulevat sovellettavaksi. Siitä, mitä pidetään julkisen vallan käyttönä ja mitä taloudellisena toimintana, ei ole olemassa valtiontuki- tai kilpailuoikeudessa tyhjentäviä listauksia. Se, mitä pidetään julkisen vallan käyttönä tai taloudellisena toimintana, voi myös vaihdella jäsenmaittain sen mukaan, millainen rooli valtiolla on eri toiminnoissa ja mitä toimintoja on vapautettu markkinoiden hoidettaviksi. Jäsenvaltiot voivat näin ollen pyrkiä säätämään tiettyjä toimintoja viranomaistehtäviksi ja pyrkiä näin osoittamaan, että niissä on kyse julkisen vallan käyttämisestä eikä taloudellisesta toiminnasta. Se, että jokin tehtävä on laissa osoitettu viranomaisten tehtäväksi, ei kuitenkaan automaattisesti tee tehtävästä julkisen

vallan käyttöä, joka jäisi valtiontuki- ja kilpailusääntöjen soveltamisalan ulkopuolelle.

Kilpailu- ja valtiontukisääntely koskee kaikkia taloudellista toimintaa harjoittavia yksiköitä, riippumatta niiden oikeudellisesta muodosta tai rahoitustavasta. Taloudellisen toiminnan määritelmän kannalta merkitystä ei ole esimerkiksi sillä, toimiiko jäsenvaltio suoraan sellaisen elimen välityksellä, joka on osa julkishallintoa, vaiko sellaisen yksikön välityksellä, jolle jäsenvaltio on antanut erityis- tai yksinoikeuksia.⁶³ Olennaista on itse toiminnan luonne, ei se, millainen organisaatio toimintaa harjoittaa.

Oikeuskäytännön perusteella taloudellista toimintaa on lähtökohtaisesti kaikki sellainen toiminta, jossa tavaroita tai palveluita tarjotaan tietyillä markkinoilla ja jota voisi ansaintatarkoituksessa edes periaatteessa hoitaa yksityinen toimija.⁶⁴ Kysymys siitä, liittyykö tietty viranomaiselle kaavailtu toiminta julkisen vallan käyttöön vai taloudellisen toiminnan harjoittamiseen, on kuitenkin ensisijaisesti arvioimalla, liittyykö toiminta luonteensa, tavoitteensa tai siihen sovellettavien sääntöjen perusteella julkisen vallan käyttöön.⁶⁵

Lähtökohtaisesti on huomattava, että suunnitellun julkishallinnon tunnistuspalvelun tarjoaminen tapahtuisi tilanteessa, joilla yksityiset toimijat tarjoavat erilaisia tunnistusvälineitä ja tunnistuspalveluita. Luottamusverkostossa on kyse yksityisistä palveluntarjoajista koostuvan markkinan sääntelystä (HE 36/2009 vp, s. 87) ja sähköistä tunnistamista ei enää sinänsä pidetä julkisena hallintotehtävänä (kts. esim. PeVL 16/2009 vp). Huomattava on lisäksi, että tällä hetkellä julkishallinnon toimijat ostavat tunnistustapahtumansa pääasiassa näiltä luottamusverkostoon kuuluvilta yksityisen sektorin toimijoilta. Digi- ja väestötietovirasto on toistaiseksi kilpailuttanut Suomi.fi –palvelussa käytettävän tunnistusvälityspalvelun.⁶⁶ Arvioitaessa suunnitellun toiminnan luonnetta on siis huomioitava, että markkinoilla on yksityisen sektorin toimijoita ja kilpailua näiden toimijoiden kesken.

⁶³ 18.3.1997, Diego Cali & Figli, C-343/95 kohdat 16, 18 ja 23

⁶⁴ EUT, C-35/96 Italia (1998), 36 kohta - Tältä osin on aluksi huomattava, että vakiintuneen oikeuskäytännön mukaan yrityksen käsitteeseen kuuluvat kaikki taloudellista toimintaa harjoittavat yksiköt riippumatta niiden oikeudellisesta muodosta tai rahoitustavasta (asia C-41/90, Höfner ja Elser, tuomio 23.4.1991, Kok. 1991, s. I-1979, 21 kohta; asia C-244/94, Fédération française des sociétés d'assurances ym., tuomio 16.11.1995, Kok. 1995, s. I-4013, 14 kohta ja asia C-55/96, Job Centre, tuomio 11.12.1997, Kok. 1997, s. I-7119, 21 kohta) ja taloudellista toimintaa on kaikki toiminta, jossa tavaroita tai palveluja tarjotaan tietyillä markkinoilla (asia 118/85, komissio v. Italia, tuomio 16.6.1987, Kok. 1987, s. 2599, 7 kohta).

⁶⁵ T-461/13 Espanja v. komissio, ECLI:EU:T:2015:891 kohta 40

⁶⁶ Kts. esim. tiedote vuoden 2020 kilpailutuksesta: <https://dvv.fi/-/digi-ja-vaestotietovirasto-valitsi-vahvan-tunnistamisen-valityspalveluntarjoajaksi-op-yrityspankin>

Nämä olosuhteet viittaavat siihen, että kyse olisi taloudellisesta toiminnasta myös silloin, kun julkissektori tuottaisi itse korvaavat palvelut asiakkaidensa tunnistamiseksi. Julkiselle sektorille tarjottavaan tunnistuspalveluun liittyy kuitenkin myös elementtejä, joiden perusteella voitaisiin argumentoida, että kysymyksessä on julkisen vallan käyttö tai ainakin siihen erottamattomasti liittyvä taloudellinen toiminta, joka jäisi valtiontukisääntelyn ulkopuolelle.

Ensinnäkin tunnistuspalvelun voitaisiin argumentoida liittyvän luonteensa ja tavoitteensa perusteella julkisen vallan käyttönä pidettävän digitaalisen identiteetin myöntämiseen (kts. tarkemmin 9.2.2.) sekä valtion tehtäviin henkilön ydinidentiteetin vahvistajana. Väestötietojärjestelmässä luotu identiteetti on keskeinen yksilön oikeusaseman kannalta ja heijastaa niitä oikeuksia, jotka henkilöllä suomalaisen yhteiskunnan osana on. Tämän identiteetin luominen ja ylläpito on Digi- ja väestötietovirastolle säädetty viranomaistehtävä. Myös digitaalisen identiteetin muodostaminen olisi edellä tehdyn arvion pohjalta julkisen vallan käyttöä olettaen, että digitaalisen identiteetin muodostaminen osoitettaisiin lailla viranomaisen tehtäväksi ja identiteetin asemasta henkilöllisyyttä osoittavana asiakirjana tai vastaavana sähköisenä todisteena säädettäisiin erikseen.

Digitaalisen identiteetin myöntämisessä henkilölle itselleen luodaan digitaalinen todistus väestötietojärjestelmään sisältyvän ydinidentiteetin ja luonnollisen henkilön yhteydestä. Todistus on viranomaisen vahvistama osoitus siitä, että tietyllä luonnollisella henkilöllä on tietty vahvistettu henkilöllisyys. Todistus myönnettäisiin julkista valtaa käyttäen ja virkavastuulla. Henkilön näkökulmasta on olennaista, että tätä todistusta voidaan myös hyödyntää yhteiskunnan palveluissa ja identiteetti on osoitettavissa. Käytettäessä fyysisiä henkilöllisyysasiakirjoja tätä ei ole tarpeen varmistaa erikseen, vaan asiakirjat ovat lähtökohtaisesti käytettävissä henkilön valitsemissa tilanteissa. Digitaalisen todistuksen osalta on tarpeen tuottaa myös sellaiset ratkaisut, jotka mahdollistavat todisteen aitouden ja voimassaolon varmistamisen sekä sen todentamisen, että todisteen esittävä henkilö on identiteetin haltija. Tältä osin julkisen sektorin tunnistuspalvelulla on kiinteä yhteys digitaalisen identiteetin myöntämiseen. Ratkaisujen tarkoituksena on varmistaa, että digitaalista identiteettiä voidaan hyödyntää julkissektorin palveluissa.

Toiseksi julkissektorin tunnistuspalvelulla voidaan nähdä kiinteä yhteys viranomaisen velvollisuuteen tarjota erilaisia sähköisiä palveluita. Henkilön mahdollisuutta osoittaa henkilöllisyytensä julkisissa sähköisissä palveluissa voitaisiin pitää keskeiseen viranomaistoimintaan olennaisesti liittyvänä toimintana. Digipalvelulaissa viranomaisille on säädetty sähköisen asioinnin järjestämisvelvoite, lain 5 §:n mukaan viranomaisen on tarjottava jokaiselle

mahdollisuus toimittaa asiointitarpeeseensa liittyvät sähköiset viestit ja asiakirjat käyttäen digitaalisia palveluita tai muita sähköisiä tiedonsiirtomenetelmiä. Käytännössä sähköisten julkisten palveluiden tarjoaminen ei ole mahdollista ilman, että henkilöllisyys voidaan luotettavasti todentaa asiointitilanteessa. Valtiolla voidaan nähdä olevan keskeisesti vastuu myös siitä, että kaikki henkilöryhmät kykenevät tällä tavoin asioimaan sähköisesti ja heillä on käytössään välineet, jotka mahdollistavat henkilöllisyyden osoittamisen luotettavasti ja turvallisesti. Kokonaisuudessa, jossa valtio myöntää julkista valtaa käyttäen digitaalisen identiteetin, voidaan nähdä kiinteä yhteys tätä identiteettiä hyödyntävän tunnistuspalvelun sekä sähköisten palveluiden tarjoamisveloitteen välillä. Julkisen sektorin tunnistuspalvelu liittyy tavoitteiltaan ja luonteeltaan keskeisten viranomaistehtävien hoitamiseen.

Toiminnan arviointiin voidaan saada tukea kahdesta komission ratkaisusta. Komission päätös SA.25745 koski Saksan konkurssihuutokauppojen internet-sivustoa.⁶⁷ Tapauksessa konkurssihuutokaupoista tietoja julkaisevan sivuston ylläpitäjä valitti lakisääteisesti huutokauppojen järjestämisestä ja niistä ilmoittamisesta vastuussa olevan viranomaisen perustamasta huutokauppasivustosta, jonka viranomainen oli perustanut tiedotustarkoituksessa. Sivuston ylläpitoa rahoitettiin julkisista varoista, jonka valittaja esitti olevan kiellettyä valtiontukea. Komissio katsoi kuitenkin, ettei viranomainen ollut ottanut käyttöön markkinamekanismeja, vaan se oli ottanut sille kuuluvan velvollisuuden itselleen hoidettavaksi tuottamallaan palvelulla. Komissio totesi, ettei viranomaisen toimintaa ole katsottava automaattisesti luonteeltaan taloudelliseksi, vaikka se tulee markkinoille, joilla yksityiset jo toimivat. Komission esittämän näkemyksen mukaan viranomainen ei luovu oikeudestaan harjoittaa julkisen vallan käyttöä vastaavaa toimintaa, vaikka yksityiset toimijat olisivatkin olleet nopeampia tarjoamaan tällaisia palveluita. Sivuston rahoituksen ei katsottu muodostavan Euroopan unionin toiminnasta tehdyn sopimuksen (”SEUT”) 107(1) artiklan mukaista kiellettyä valtiontukea.

Toinen komission päätös SA.34646 koski valitusta Alankomaiden perustamasta internetpalvelusta, jonka kautta julkiset hankinnat voitiin toteuttaa. Valittajien mukaan kyseessä oli valtion ryhtyminen taloudelliseen toimintaan ja palvelu rikkoi kilpailuoikeudellista sääntelyä saavuttamalla määräävän markkina-aseman. Komissio kuitenkin katsoi, että kyseessä ei ollut valtiontuki eikä taloudellinen toiminta, sillä palvelulla toteutettiin julkisen vallan käyttöä tavoitteena täyttää julkisista hankinnoista annetun direktiivin (2014/24/EU) valtiolle asettamat velvoitteet. Myös tässä tapauksessa laissa oli asetettu

⁶⁷ Vrt. Komission päätös SA.25745 Saksan konkurssihuutokauppojen internet-sivustosta (2013/NN) (ex CP 11/2008) kohta 36

viranomaiselle velvollisuus, jonka täyttämistä viranomaisen tuottamalla palvelulla huolehdittiin. Tällaisen velvoitteen toteuttamista ei pidetty luonteeltaan taloudellisena, vaan julkisen vallan käyttönä. Viranomaiselle ei oltu laissa asetettu rajoitteita palvelun tuottamiseen, edellyttäen, että lakisääteiset velvoitteet täytettiin. Palvelun tuottamisella valtion sisäisesti voitiin myös varmistaa, että julkiset yksiköt pystyivät tarjoamaan sähköiset palvelunsa laissa edellytetyn laatuina.⁶⁸

Edellä esitettyjen ratkaisujen perusteella voidaan argumentoida, että tunnistuspalveluiden tarjoaminen julkisen sektorin sähköisiin asiointipalveluihin voisi, vaikka markkinoilla on vastaavaa yksityistä toimintaa, jäädä taloudellisen toiminnan käsitteen ulkopuolelle. Tapauksia voidaan verrata käsillä olevaan tilanteeseen, jossa keskeiseksi viranomaistehtäväksi on nähtävissä sekä digitaalisen henkilöllisyyden myöntäminen, että luotettavien sähköisten asiointikanavien tarjoaminen julkisiin palveluihin. Viranomaiselle on asetettu lähtökohtainen velvoite tuottaa palvelunsa myös sähköisesti ja tähän kokonaisuuteen kuuluu myös tunnistamisen mahdollistaminen. Markkinoilla on jo yksityisiä toimijoita, jotka tuottavat tunnistuspalveluita. Mutta viranomaisen toimintaa ei tulisi automaattisesti katsoa taloudelliseksi eikä se ole luopunut oikeudestaan harjoittaa tällaista keskeistä viranomaistoimintaa. Komission ratkaisun valossa viranomaisen tulisi voida toteuttaa digitaalisten palvelujen tarjoaminen lain edellyttämällä tavalla ilman tunnistamispalvelun ostamista markkinoilta.

Toimintaa harjoittavan yksikön mahdollisesti saama tuki ei muodostaisi SEUT 107(1) artiklan mukaista kiellettyä valtiontukea tai rikkoisi kilpailulain säännöksiä kilpailuneutraliteetista. Edellä mainituissa komission ratkaisuissa painottuu kuitenkin toiminnan liittyminen viranomaiselle kuuluvan, lakiin perustuvan velvoitteen täyttämiseen tai toteuttamiseen. Digitaalisen identiteetin hankkeessa on tarkkaan arvioitava, millä tavoin sekä identiteetin myöntämisestä, että henkilöllisyyden osoittamisesta sähköisissä viranomaispalveluissa tulisi säätää lailla.

Kummassakaan viitatussa komission ratkaisussa SA.34646 ja SA.25745 ei kuitenkaan käsitelty nimenomaisesti kysymystä siitä, miten yksityisten toimijoiden vähenevät tulot vaikuttavat kyseessä olevan toiminnan valtiontuki- tai kilpailuoikeudelliseen arvioon. Tältä osin jatkovalmistelussa on vielä arvioitava tarkemmin hankkeen vaikutuksia ja niiden suhdetta oikeudelliseen arvioon.

⁶⁸ Komission päätös SA.34646 Alankomaiden julkisten hankintojen alusta TenderNedistä, kohta 67

Julkiselle sektorille tarjottavan tunnistuspalvelun voidaan perustella liittyvän luonteensa, tavoitteensa tai siihen sovellettavien sääntöjen perusteella julkisen vallan käyttöön. Selvityksen tässä vaiheessa, palvelun toteuttamista pidetään lähtökohtaisesti mahdollisena, mutta jatkotyössä on kiinnitettävä erityistä huomiota ratkaisun yksityiskohtiin sekä siihen, missä määrin viranomaisen velvoitteet perustuisivat lainsäädäntöön. Luonnollisesti ratkaisun vaikutukset ja muut oikeudelliset kysymykset on arvioitava erikseen ja ne voivat vaikuttaa toteutukseen.

Ottaen huomioon, että näkemys toiminnan luonteesta edellyttää hyvin moniulotteisen sääntelykokonaisuuden tulkintaa ja on riippuvainen toiminnan yksityiskohdista, on seuraavassa arvioitu vielä niitä kysymyksiä, jotka voisivat vaikuttaa kielletyn valtiontuen tai kilpailuneutraliteettiongelman arviointiin. Mikäli sääntely ei sovellu, ei toimintaan liity myöskään riskejä näiden kysymysten osalta. Mutta jatkotyötä varten on tarpeen hahmottaa sitä, miten toimintaa voitaisiin arvioida suhteessa kiellettyyn valtiontukeen tai kilpailuneutraliteettiin.

Kielletty valtiontuki

Tilanteessa, jossa julkissektorin tunnistuspalvelu katsottaisiin taloudelliseksi toiminnaksi, olisi arvioitava myös, muodostuuko toiminnan rahoitus tai toimintaa harjoittavien yksiköiden saama muu etu kielletyksi valtiontueksi. Tältä osin tulevat arvioitavaksi kielletyn valtiontuen edellytykset. Seuraavassa on arvioitu mahdollisesti esiin tulevia kysymyksiä siltä varalta, että toiminta jatkoselvityksen perusteella katsottaisiin taloudelliseksi.

Ensimmäinen edellytys valtion toteuttamasta ja valtion varoilla toteutetusta toimenpiteestä täytyisi oletettavasti kohtuullisen helposti. Edun myöntäminen suoraan tai välillisesti valtion varoista ja toimenpiteen katsominen valtion toteuttamaksi ovat kaksi erillistä ja yhteisesti vaikuttavaa ehtoa valtiontuen olemassaololle.⁶⁹ Etu taas on mikä tahansa taloudellinen hyöty, jota toimija ei olisi voinut saada tavanomaisissa markkinaolosuhteissa, ilman valtion toimenpidettä.⁷⁰ Toteutuksen rahoitus valtion varoista taikka toimijalle viranomaisasemasta tai –resursseista aiheutuva etu voivat muodostua tällaiseksi valtiosta johtuvaksi ja valtion varoilla toteutettavaksi toimenpiteeksi.

Toinen edellytys vaikutuksesta kilpailuun tarkoittaa, että toimenpiteen on vääristettävä tai uhattava vääristää kilpailua markkinoilla. Tämä puolestaan

⁶⁹ Komission tiedonanto (2016/C 262/01), para 38.

⁷⁰ Komission tiedonanto (2016/C 262/01), para 66.

edellyttää sitä, että toimenpide on omiaan parantamaan tuensaajan kilpailuasemaa verrattuna muihin yrityksiin, joiden kanssa se kilpailee. Markkinoilla toimivan yrityksen saadessa valtion toimenpiteestä etua voidaan katsoa lähtökohtaisesti, että etu potentiaalisesti tai tosiasiallisesti vääristää kilpailua, jos kyseinen etu parantaa yrityksen mahdollisuutta kilpailla markkinoilla.⁷¹ Julkinen sektori ostaa tällä hetkellä tunnistustapahtumansa kilpaillulta markkinalta, joten arvio kohdistuu erityisesti siihen, saisiko julkissektorin tunnistuspalvelua tuottava toimija sen asemaa parantavaa etua. Yksikön katsottaisiin todennäköisesti saavan kilpailuetua siitä, että tätä toimintaa rahoitettaisiin valtion varoista tai yksikkö voisi hyödyntää viranomaisresursseja. Julkisen sektorin yksityisiltä palveluntarjoajilta hankkimat tunnistuspalvelut muodostavat lisäksi merkittävän osan tunnistuspalveluiden markkinoista. Riski kilpailun vääristymiseen tunnistuspalvelujen markkinoilla olisi tältä osin huomionarvoinen.

Kilpailuvaikutusedellytyksen täyttymisessä annetaan kuitenkin tiettyä merkitystä myös toimenpiteen kielteisten ja myönteisten vaikutusten punninnalle.⁷² Vaikka edellä kuvatut tekijät puoltavat sitä, että kilpailuedellytys voisi täytyä, digitaalisella identiteetillä ja siihen liittyvällä julkisen sektorin tunnistuspalvelulla voidaan myös nähdä olevan hyötyjä, jotka puoltavat vastakkaista arviota. Erityisesti julkissektorin tunnistuspalvelun osalta hyötynä nähdään mahdollisuus varmistaa valtion takaaman identiteetin osoittaminen julkissektorin sähköisissä asiointipalveluille kaikille henkilöryhmille. Mikäli toiminnan yhteys julkisen vallan käyttöön jää epävarmaksi, kilpailuvaikutusarviointia tulisi vielä tehdä tarkemmin erityisesti markkinaselvitysten valossa sen arvioimiseksi, kuinka paljon suunniteltu ratkaisu todella vaikuttaa kilpailuun ja mitä osoitettavissa olevia myönteisiä vaikutuksia sillä on.

Kolmas valtioneuvoston edellytys on, että tuki vaikuttaa jäsenvaltioiden väliseen kauppaan. Lähtökohtaisesti kauppavaikutusedellytys täyttyy helposti kilpailuille avoimilla markkinoilla, koska sen edellytyksenä ei ole, että tuensaaja itse osallistuu rajat ylittävään kauppaan. Se, että muihin jäsenvaltioihin sijoittautuneet toimijat osallistuvat markkinoille tai niillä on ainakin intressi osallistua markkinoilla, riittää kauppavaikutuskriteerin täyttymiseen. Tunnistuslaki mahdollistaa muuhun Euroopan talousalueen jäsenvaltioon sijoittautuneen tunnistuspalvelun tarjoajan liittymisen luottamusverkkoon. Tunnistuspalveluiden markkinoilla on sekä kotimaisia

⁷¹ Asia C-730/79, Philip Morris, tuomio 17.9.1980, Kok., -02671, 11 kohta; T-298/97, T-312/97 jne. Alzetta, yhdistetyt asiat, tuomio 15.6.2000, Kok., II-2319, kohta 80

⁷² Komission tiedonanto Puitteet tutkimus- ja kehitystyöhön sekä innovaatiotoimintaan myönnettävälle valtioneuvostolle, 2014/C 198/01, 27.6.2014

toimijoita kuin myös muihin Euroopan talousalueen jäsenvaltioihin sijoittautuneita toimijoita. Myös markkinoille tuloon on kiinnostusta uusilla kotimaisilla sekä ulkomaisilla yrityksillä (HE 237/2020 vp s. 6). Markkinaa pidettäisiin todennäköisesti kansainvälisenä tai sen katsottaisiin olevan laajempi kuin pelkästään Suomi. Hankkeella annetun tuen vaikutusta ei voida myöskään pitää pelkästään paikallisena.⁷³ Näin ollen tuella voisi olla vaikutusta jäsenvaltioiden väliseen kauppaan SEUT 107(1) artiklan tarkoittamalla tavalla. Mikäli toiminta katsottaisiin taloudelliseksi, voisi myös kauppavaikutusedellytys todennäköisesti täytyä.

Neljäs edellytys, on tuen valikoivuus ja tarkoittaa sitä, että etu tai toimenpide kohdistuu valikoiduille yrityksille tai toimialoille. Käsillä olevassa toimintamallissa valikoivuusedellytys voisi täytyä ensinnäkin sillä perusteella, että valtionrahoitteisesti toteutettu mobiilisovelluksen ylläpitäminen ja tarjoaminen annettaisiin tietyn yksikön tehtäväksi.

Kokonaisuudessaan julkissektorin tunnistuspalveluun liittyy tekijöitä, jotka voisivat puoltaa kielletyn valtiontuen olemassaoloa, mikäli toiminta katsottaisiin taloudelliseksi. Edellytysten on kuitenkin kaikkein täytyttävä, jotta kielletty tuki on käsillä. Erityisesti kilpailuvaikutuksen osalta nähdään toimintamallista aiheutuvan myös hyötyjä, jotka voisivat tarkoittaa sitä, että edellytykset eivät kokonaisuudessaan täyty. Olennaista kuitenkin on, että toiminnalla nähdään edellä kuvatusti kiinteä yhteys keskeisiin viranomaistehtäviin tavalla, joka sulkisi pois valtioneuvoston sääntelyn soveltamisen. Tehty selvitys ei tältä osin aiheuta estettä hankkeelle.

Kilpailuneutraliteetti

Tilanteessa, jossa julkissektorin tunnistuspalvelu katsottaisiin taloudelliseksi toiminnaksi, olisi se arvioitava myös kilpailuneutraliteettisääntelyn näkökulmasta. Tällöin on arvioitava, sisältyykö siihen menettely tai rakenne, joka vääristää tai on omiaan vääristämään terveen ja toimivan kilpailun edellytyksiä markkinoilla taikka estää tai on omiaan estämään terveen ja toimivan taloudellisen kilpailun syntymistä tai kehittymistä. Seuraavassa on arvioitu mahdollisesti esiin tulevia kysymyksiä siltä varalta, että toiminta jatkoselvityksen perusteella katsottaisiin taloudelliseksi.

Kilpailuneutraliteettisäännökset ovat valtioneuvoston sääntelystä erillinen kokonaisuutensa, mutta molemmat voivat tulla sovellettavaksi tietyn toiminnan arviointiin. Hankkeen kannalta tämä tarkoittaa myös sitä, että vaikka suunniteltu

⁷³ Komission tiedonanto (2016/C 262/01), para 196

toimintamalli tai jokin sen osa ei muodostaisi kiellettyä valtiontukea ja olisi siten sisämarkkinoille sopiva toimi, sovellettavaksi voisivat edelleen tulla kilpailuneutraliteettisäännökset. Se, vaarantaako menettely tai toiminnan rakenne kilpailuneutraliteettia, on harkittava aina tapauskohtaisesti kokonaisarviointin perusteella.

Tästä näkökulmasta julkishallinnon tunnistuspalvelua tuottava yksikön ei tulisi saada asemansa vuoksi perusteetonta etua suhteessa nykyisiin tai tuleviin markkinatoimijoihin. Kilpailulain 30 §:n nojalla mikä tahansa taloudellisessa toiminnassa käytetty menettely tai toiminnan rakenne, joka estää tai vääristää kilpailua markkinalla, oikeuttaa Kilpailu- ja kuluttajaviraston puuttumaan toimintaan.

Kilpailuneutraliteettia vaarantavia järjestelyitä saattaisivat taloudellisessa toiminnassa olla esimerkiksi se, että tästä toiminnasta vastaavalla yksiköllä on mahdollisuus hyödyntää taloudellisessa toiminnassaan viranomaistoiminnassa saatuja tietovarantoja, infrastruktuuria tai ei-markkinahintaisia tukipalveluja tai se, että se voisi hinnoitella mobiilisovelluksen ylläpitämisestä ja tarjoamisesta perittävät maksut ei-markkinahintaisesti. Se, missä muodossa mobiilisovellusta ylläpitävä ja tarjoava yksikkö toimisi, ei ole ratkaisevaa kilpailuneutraliteettisäännösten soveltamisessa, koska niitä voidaan soveltaa esimerkiksi mihin tahansa valtion tai sen määräysvaltaan kuuluvaan yksikköön. Kuitenkin mitä ilmeisempi yksikön toimintamuotoon perustuvan liiketaloudellisen riskin puuttuminen kilpailuilla markkinoilla on, sitä todennäköisempiä kilpailuneutraliteettiongelmat voivat olla.⁷⁴

Jos mobiilisovellusta ylläpitävällä ja tarjoavalla yksiköllä olisi samaan aikaan sekä markkinaehtoisesti toimiva tunnistuspalvelu että velvollisuus tuottaa muita julkisia palveluita, on yksikön kustannusten korvaamiseen ja sen palveluiden hinnoitteluun kiinnitettävä erityistä huomiota. Julkisten palveluiden tarjoamisveloitteesta johtuvat kustannukset tulisi riittävässä määrin korvata läpinäkyvällä tavalla, mutta samalla estää se, että julkisen palvelun tuottamiseen perustuvilla tuotoilla rahoitettaisiin taloudellisena toimintana pidettävää toimintaa siten, että tällaisten palveluiden hinnoittelu aiheuttaisi häiriöitä markkinoilla.⁷⁵ Mahdollisen ristiinsubventoinnin välttämiseksi toimintojen kirjanpidoissa tulee selkeästi käydä ilmi palvelujen erottaminen.

⁷⁴ Komission kirje asiassa Palmia, 14.4.2010

⁷⁵ Julkisen yrityksen toimimista sekä ei-taloudellisen toiminnan harjoittajana että kilpailijana vapaille markkinoilla itse tuottamallaan palvelulla on arvioitu myös unionin oikeuskäytännössä. Esimerkiksi unionin tuomioistuimen julki-sasiamies korosti 28.9.2006 antamassaan ratkaisussa ei-taloudellisen julkisen toiminnan ja toiminnan yksityisen osan erottamisen tärkeyttä sekä kiinnitti huomiota eron tekemisessä myös lainsäädännöllisten takeiden tarpeeseen.

Kilpailuneutraliteettia turvaavasta kirjanpidon eriyttämisestä säädetään tarkemmin kilpailulain 30 d §:ssä.

Kilpailulaissa on säädetty poikkeuksesta kilpailuneutraliteettia vääristävään toimintaan puuttumisesta. Poikkeus rajoittaa kilpailu- ja kuluttajaviraston valtaa puuttua toimintaan tapauksessa, jossa kilpailuneutraliteetin vaje johtuu väistämättä lainsäädännöstä tai jos merkittävän yleisen edun turvaaminen estyisi kilpailun esteeseen tai vääristymään puututtaessa. Poikkeukset mahdollistavat sen, että julkisyhteisön toiminnasta aiheutuvaan kilpailun vääristymiseen tai estymiseen ei voida puuttua, jos toiminnan kielteiset vaikutukset seuraavat väistämättä lainsäädännöstä ilman, että taloudellisesta toiminnasta vastaavalla taholla olisi harkintavaltaa tai liikkumavaraa kilpailuneutraliteettia vaarantavan taloudellisen lopputuloksen osalta. (HE 40/2013 vp s. 35) Tämä perustuu kilpailulain 30 a §:ään ja säännös merkitsee sitä, että Kilpailu- ja kuluttajavirastolla ei ole toimivaltaa puuttua muusta lainsäädännöstä seuraavaan kielteiseen vaikutukseen markkinoilla. Vaikka toimintaa ei tässä vaiheessa lähtökohtaisesti pidetä sellaisena, joka tulisi kilpailulain soveltamisalaan, on huomattava, että toiminnan asianmukainen sääntely vähentää myös riskiä myöhemmin ilmaantuvista ongelmista.

Mikäli suunniteltu toiminta muodostuisi taloudelliseksi, olisi erityistä huomiota kiinnitettävä toiminnan sääntelyyn sekä siihen, missä määrin rakenteet tai menettelyt seuraisivat suoraan lainsäädännöstä. Lisäksi olisi huomiota kiinnitettävä toiminnan erottamiseen muusta viranomaistoiminnasta. Mahdollisia kilpailua vääristäviä rakenteita voitaisiin myös ratkaista yhtiöittämällä tai muuten ulkoistamalla toimintaa. Olennaista kuitenkin on, että toiminnalla nähdään tässä vaiheessa kiinteä yhteys keskeisiin viranomaistehtäviin tavalla, joka sulkisi pois kilpailulain soveltamisen. Tehty selvitys ei tältä osin aiheuta estettä hankkeelle.

7.3. Yhteenveto ja selvittävät kysymykset

Edellä on arvioitu neljää arviomuistiossa kuvatun ratkaisun elementtiä kilpailu- ja valtioneuvoston sääntelyn valossa. Digitaalisen identiteetin muodostaminen nähdään alustavan arvion perusteella julkisen vallan käyttönä ja keskeisenä viranomaistehtävänä digitalisoituvassa yhteiskunnassa. Digitaalisen henkilöllisyyden osoittaminen käyntiasioinnissa mobiilisovelluksen avulla on samalla tavoin katsottavissa julkisen vallan käytöksi. Sen osalta on kuitenkin erityisen tärkeää, että digitaalisen identiteetin asema henkilöllisyyden osoittamisessa säädetään lailla ja sen suhde henkilökortin sääntelyyn ratkaistaan. Ratkaisut, jotka mahdollistavat henkilöllisyystietojen esittämisen, vertautuvat henkilöllisyysasiakirjojen esittämiseen ja voidaan oikein

säänneltynä nähdä niin ikään julkisen vallan käyttönä. Mahdollisten laajempien viranomaistietojen osalta tällainen toiminta olisi lähtökohtaisesti keskeistä viranomaistoimintaa, mutta laajennettaessa tietopohjaa olisi hyvin tarkkaan arvioitava esitettävien tietojen alkuperä, niiden sääntely ja suhde digitaaliseen identiteettiin. Muiden kuin viranomaistietojen osalta toiminta edellyttäisi tarkempaa arviointia, eikä sitä voida oletusarvoisesti pitää keskeisenä viranomaistehtävänä.

Arvioitavista kokonaisuuksista moniulotteisin on niin sanottu julkisen sektorin tunnistuspalvelu, joka mahdollistaisi digitaalisen identiteetin käyttämisen henkilöllisyyden osoittamiseksi julkissektorin asiointipalveluissa. Olemassa oleva markkina, jolta julkissektori tällä hetkellä ostaa tunnistuspalvelunsa, viittaisi siihen, että kyse olisi taloudellisesta toiminnasta. Toiminnalla voidaan kuitenkin nähdä olevan kiinteä yhteys julkisen vallan käyttöön siten, että siihen ei sovellettaisi kilpailu- ja valtioneuvoston sääntelyä. Digitaalisen henkilöllisyyden myöntäminen ja luotettavien sähköisten asiointikanavien tarjoaminen julkisiin palveluihin voidaan molemmat nähdä keskeiseksi viranomaistoiminnaksi. Valtion vahvistamaan digitaaliseen identiteettiin kuuluu olennaisesti se, että valtio myös varmistaa henkilöllisyyden käytettävyyden. Toisaalta viranomaisella on lähtökohtainen velvoite tuottaa palvelunsa myös sähköisesti ja tähän kokonaisuuteen kuuluu myös tunnistamisen mahdollistaminen. Näillä perusteilla toimintaa ei pidetä sellaisena taloudellisena toimintana, johon sovellettaisiin kiellettyä valtioneuvoston tukea tai kilpailuneutraliteettia koskevaa sääntelyä.

Selvityksen tässä vaiheessa näistä elementeistä koostuvan palvelukokonaisuuden toteuttamista pidetään lähtökohtaisesti mahdollisena, mutta jatkotyössä on kiinnitettävä erityistä huomiota ratkaisun yksityiskohtiin sekä siihen, missä määrin viranomaisen velvoitteet perustuisivat lainsäädäntöön. Hankkeessa olisi jatkossa kiinnitettävä huomiota myös siihen, millä tavoin ratkaisun kehittyvät yksityiskohdat mahdollisesti vaikuttavat näihin arvioihin.

8. Muut hankkeen etenemisen kannalta olennaiset oikeudelliset kysymykset

8.1. Henkilöllisyysasiakirjat ja digitaalinen identiteetti

Kuten edellä on kuvattu, Suomen lainsäädäntö ei sääntele yleisellä tasolla sitä, millaisilla asiakirjoilla henkilöllisyyden voi osoittaa. Passia ja henkilökorttia säännellään matkustusasiakirjoina ja osin henkilöllisyyttä osoittavina asiakirjoina niitä koskevissa erityislaeissa. Lisäksi erilaisia asiointitilanteita koskevissa laeissa saatetaan asettaa edellytyksiä henkilöllisyyden

osoittamisesta. Hankkeen toteuttamiselle on olennaista, millainen asema mobiilihenkilökortilla olisi henkilöllisyyden osoittamisen välineenä. Mikäli mobiilihenkilökortti vertautuisi luotettavuudeltaan passiin ja henkilökorttiin henkilöllisyyttä osoittavana asiakirjana, sen aseman tulisi perustua lainsäädäntöön.

Ensimmäinen vaihtoehto on, että digitaaliseen henkilöllisyyteen perustuva mobiilihenkilökortti olisi uusi henkilökortin tyyppi henkilökorttilain piirissä. Henkilökorttilain 1 §:n 1 momentin mukaan laissa säädetään Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle henkilöllisyyden osoitukseksi myönnettävästä henkilökortista. Mobiilihenkilökortti vertautuisi esimerkiksi alaikäisen henkilökorttiin siten, että se ei toimisi matkustusasiakirjana. Kortilla olisi kuitenkin mahdollista asioida sähköisesti (jäljempänä osa 10.2.) ja se toimisi henkilöllisyydistuksena. Tällä tavalla säännellyn mobiilihenkilökortin asema henkilöllisyyttä osoittavana asiakirjana johtuisi luonnollisesti henkilökorttilaista. Todennäköisesti tällöin ei olisi tarpeen tarkastella laajemmin sitä, millä tavoin henkilöllisyyden osoittamisen tapoja on säännelty muussa erityislainsäädännössä. Henkilökorttilaissa tulisi tällöin säännellä erikseen mobiilihenkilökortin myöntämistä, sitä koskevia menettelyitä ja esimerkiksi mobiilihenkilökortin voimassaoloaika.

Toinen vaihtoehto on, että kaikista henkilökorttilain mukaisista henkilökorteista olisi mahdollista saada digitaalinen versio. Mobiilihenkilökortti ei tällöin olisi erillinen henkilökortin tyyppi, vaan vaihtoehtoinen alusta, jolla myönnetty henkilökortti, alaikäisen henkilökortti tai väliaikainen henkilökortti olisi käytettävissä. Myös tässä tapauksessa mobiilihenkilökortin asema henkilöllisyyttä osoittavana asiakirjana johtuisi henkilökorttilaista. Tässä vaihtoehdossa mobiilihenkilökortti olisi sidoksissa kunkin henkilökortin voimassaoloaikaan ja se voitaisiin myöntää enintään viideksi vuodeksi.

Kolmas vaihtoehto on, että mobiilihenkilökortista säädettäisiin erikseen henkilökorttilain ulkopuolella. Tällöin sääntely voitaisiin myös yhdistää laajempaan digitaalisen identiteetin ja Digi- ja väestötietoviraston varmenteiden sääntelyyn. Olennaista henkilöllisyysasiakirjojen sääntelyn näkökulmasta olisi kuitenkin, että kyse digitaalisesta asiakirjasta, joka olisi juridisesti erillinen suhteessa henkilökorttiin. Tässä vaihtoehdossa olisi myös säädettävä erikseen mobiilihenkilökortin asemasta henkilöllisyyttä osoittavana asiakirjana. Tällöin on huomioitava, että asiointia koskevat erityislait sääntelevät henkilöllisyyden osoittamista eri tavoin – on mahdollista, että osassa viitataan suoraan henkilökorttiin ja passiin. Säädösteknisesti olisi arvioitava, miten erillisen mobiilihenkilökortin asema voidaan varmistaa uutena henkilöllisyyttä osoittavana asiakirjana.

Yhteenvedona, digitaalisen identiteetin hankkeessa tulee ensisijaisesti arvioitavaksi se, millä tavoin mobiilihenkilökortin asema henkilöllisyyttä osoittavana asiakirjana varmistetaan lainsäädännön keinoin. Tarkasteltaessa henkilöllisyyden osoittamisen ja asioinnin sääntelyä kokonaisuutena, voidaan kuitenkin myös kysyä, olisiko kansallisesti tarvetta yleistasoiselle sääntelylle henkilöllisyyden osoittamisesta erilaisissa tilanteissa. Tällöin olisi mahdollista arvioida henkilöllisyyden osoittamista kokonaisuutena, sekä fyysisessä että sähköisessä asiointissa. Tämä on tarpeen, sillä arkipäivän asiointi on enenevässä määrin yhdistelmä sekä fyysisiä että digitaalisia palvelukanavia. Tulevaisuuden asiointitapojen moninaisuus saattaisi edellyttää laajempaa arviota henkilöllisyyden osoittamisen tavoista, luotettavuudesta ja sääntelystä yhteiskunnan eri osa-alueilla.

8.2. Vahva sähköinen tunnistaminen ja digitaalinen identiteetti

8.2.1. Valtion ratkaisun suhde vahvaan sähköiseen tunnistamiseen

Tunnistuslain 1 §:n mukaan siinä säädetään vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta tunnistuspalveluita käyttäville palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille. Lakia ei sovelleta yhteisön sisäiseen tunnistamiseen käytettävien palveluiden tarjontaan. Kysymyksessä voi tällöin olla vahvan sähköisen tunnistuspalvelun tarjoaminen, mutta palvelua ei tarjota yleisölle eikä toiselle palveluntarjoajalle. Lakia ei sovelleta myöskään yhteisöön, joka käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan (ns. in house). Tällöin palveluntarjoajan tavoitteena on oman palvelunsa tarjoaminen, ja tunnistaminen liittyy siihen ainoastaan sivutuotteena. Näihin tapauksiin sovelletaan kuitenkin tiettyjä lain vastuukysymyksiä koskevia säännöksiä.

Tunnistuslaissa yhdistyy kaksi kokonaisuutta, jotka teoriassa olisivat erotettavissa toisistaan: vahvan sähköisen tunnistamisen sääntely sekä tällaisia vahvan sähköisen tunnistamisen palveluita tarjoavan luottamusverkoston sääntely. Kansallinen sääntely on tähän asti lähtenyt siitä olettamasta, että vahvan sähköisen tunnistamisen tasoista palvelua tuotetaan ainoastaan luottamusverkoston piirissä. Digitaalisen identiteetin hankkeen näkökulmasta on kuitenkin tarpeen arvioida erikseen sitä, onko tuotetuissa ratkaisuisa kyse toiminnasta, joka täyttää vahvalle sähköiselle tunnistukselle asetettava tekniset ja menettelylliset edellytykset, sekä toisaalta sitä, mikä toiminnan suhde on luottamusverkostoon.

Tunnistuslain 10 §:ssä säädetään tunnistuspalvelun tarjoajan velvollisuudesta ilmoittaa toiminnan aloittamisesta Liikenne- ja viestintävirastolle (Traficom). Mikäli ilmoitusta ei tehdä, eikä palveluntarjoaja tule osaksi luottamusverkostoa, se ei voi tarjota tunnustuslain tarkoittamaa vahvaa sähköistä tunnistusvälinettä. Tunnistuspalvelun tarjoaja voi kyllä teoriassa tarjota tunnistusvälinettä ilman vahvan sähköisen tunnistuspalveluntarjoajan asemaa, mutta tällöin se ei voi osoittaa täyttävänsä kansalliset ja kansainväliset määräykset vahvasta sähköisestä tunnistamisesta.

Tunnistuslain mukaan vahvalla sähköisellä tunnistamisella tarkoitetaan henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnusteen aitouden ja oikeellisuuden todentamista sellaista sähköistä menetelmää käyttäen, joka:

- 1) tarjoaa merkittävän luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävässä määrin henkilöllisyyden väärinkäytön tai muuttamisen riskiä (korotettu taso); tai
- 2) tarjoaa korkeamman luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on estää henkilöllisyyden väärinkäyttö tai muuttaminen (korkea taso).

Tunnistusvälineellä tarkoitetaan aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen, eli prosessiin, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön sähköisen tunnistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen.

Tunnustuslaki ja sen vahvan sähköisen tunnistamisen sääntely on lähtökohtaisesti kirjoitettu teknologianeutraaliksi (HE 36/2009 vp, s. 41). Valtion tuottama digitaalinen identiteetti siinä muodossa, kuin se on tässä arviomuistiossa kuvattu, sopii näihin tunnustuslain määritelmiin. Mikäli ratkaisu tultaisiin notifioimaan rajat ylittävän tunnistamisen välineeksi, sen olisi tätä varten myös mukauduttava näihin samoihin määritelmiin. Digitaalisen henkilöllisyyden osoittaminen sähköisessä asiointipalvelussa ei näin ollen

tavoitteiltaan, menetelmältään tai luotettavuudeltaan tulisi olennaisesti eroamaan tunnistuslain olettamista tunnistuspalveluista. Koska tunnistuslaki on teknologianeutraali, ei mahdollinen tekninen toteutus olennaisesti vaikuttaisi tähän arvioon. Olennainen ero on, että kyse olisi digitaalisesta henkilöllisyydestä ja tätä henkilöllisyyttä osoittavasta välineestä, jotka valtio myöntää ja tuottaa käyttäen julkista valtaa – osana julkisten palvelujen tuottamista.

Olennainen ero nykyisen vahvan sähköisen tunnistamisen välineiden ja suunnitellun ratkaisun välillä on myös, että se ei tulisi osaksi luottamusverkostoa. Vaikka menetelmä lähtökohtaisesti täyttäisi tunnistuslain kuvauksen tunnistusvälineestä, se ei olisi tunnistuslain mukainen tunnistuspalvelu, koska sitä ei tarjottaisi luottamusverkostossa välitettäväksi. Näin ollen, se ei nykyisen lainsäädännön valossa myöskään olisi vahvaa sähköistä tunnistamista – tai sitä ei juridisesti voitaisi sellaiseksi kutsua.

Digitaalisen henkilöllisyyden tuottamisesta ja siihen liittyvästä tunnistuspalvelusta, jonka avulla henkilöllisyys voitaisiin osoittaa julkisien sektorin asiointipalveluissa, tulisi säätää erikseen lailla. Mikäli valtion menetelmä ei olisi tunnistuslain mukainen luottamusverkostossa välitettävä tunnistuspalvelu, mutta sille haluttaisiin saada vahvan sähköisen tunnistamisen status tai vastaavasti tietoturvallisen tunnistusvälineen status, tulisi myös tästä säätää erikseen. Edellä jaksossa 6.7.2. on kuvattu enemmän sitä, millä tavoin kansallisessa lainsäädännössä edellytetään henkilöllisyyden todentamista sähköisessä asiointissa. Tarvittavilla lainsäädäntömuutoksilla olisi varmistettava, että tuotettava digitaalinen identiteetti olisi myös lainsäädännön näkökulmasta käytettävissä erilaisissa julkisissa palveluissa, jotka voivat tällä hetkellä asetta hyvin erilaisia vaatimuksia henkilöllisyyden todentamiselle – osa myös edellyttää nimenomaan tunnistuslain mukaista välinettä.

Digitaalista identiteettiä koskevassa sääntelyssä olisi otettava kantaa ainakin viranomaisten tehtäviin, tietojen käsittelyyn, tuotettavaan palveluun ja sen käytettävyyteen erilaisissa asiointitilanteissa. Erityisesti olisi myös huomioitava ne tunnistamisen luotettavuutta ja turvallisuutta koskevat edellytykset, jotka on kansallisesti sisällytetty tunnistuslakiin. Säädetäessä erikseen tunnistusvälineen tuottamisesta, tulisi laissa huomioida erikseen esimerkiksi varmuustason sääntely. Luottamusverkostoin toimijoita koskee lisäksi muun muassa auditointivelvollisuus, muutosilmoitusvelvollisuus, häiriöilmoitusvelvollisuus sekä sopimusvelvollisuus. Lisäksi muut tunnistuslain mukaiset vaatimukset tulevat automaattisesti koskemaan luottamusverkostossa olevia vahvan tunnistuspalvelun tarjoajia. Lainsäädännön valmistelussa olisi

arvioitava digitaalisen identiteetin suhde näihin erilaisiin tunnistuslaissa ratkaistuihin kysymyksiin.

8.2.2. Digitaalisen identiteetin hyödyntäminen sähköisessä asiointissa

Edellä jaksossa X kuvatusti, digipalvelulain säännökset velvoittavat viranomaisia tarjoamaan palvelujaan digitaalisesti. Digipalvelulain 6 §:ssä säädetään lisäksi sähköisen tunnistamisen edellyttämisestä. Laissa säädetään sekä niistä tilanteista, joissa sähköisen tunnistamisen edellyttäminen on perusteltua, sekä tilanteista, joissa palvelun käyttäjä on tunnistettava vahvasti. Lisäksi erityislakeihin sisältyy jonkin verran sääntelyä siitä, millä tavoin henkilöllisyys on osoitettava tietyillä toimialoilla tai palveluissa, kun asiointi tapahtuu sähköisesti. Tilanteissa, joissa henkilö on tunnistettava vahvasti, on julkishallinnolla tukipalvelulain mukainen velvollisuus käyttää Suomi.fi-tunnistuspalvelua, johon kilpailutetaan luottamusverkoston toimijoiden tunnistuspalvelut.

Digitaalisen identiteetin ratkaisua on arvioitava myös suhteessa sähköisen asiointin ja tukipalvelujen sääntelyyn. Valtion digitaalinen identiteetti olisi jatkossa tarkoitus olla tietoturvallinen ja todisteellinen tunnistusväline, jonka avulla käyttäjä voisi todentaa henkilöllisyytensä sekä käyntiasioinnissa että tunnistautua julkishallinnon sähköisiin asiointipalveluihin. Edellä kuvatusti ratkaisu edellyttää tunnistuslaista erillistä erityislainsäädäntöä. Tällaisen erityislainsäädännön kautta luotava luotettavan vahvan sähköisen tunnistamisen status on olennainen myös sähköisen asiointin näkökulmasta. Siinä määrin, kun nykyinen lainsäädäntö edellyttää vahvaa sähköistä tunnistamista tai vastaavia ratkaisuja, on erityislainsäädännöllä varmistettava, että digitaalisen identiteetin ratkaisu täyttää nämä edellytykset. Paikoin tämä saattaa edellyttää myös muutoksia tiettyjä asiointipalveluja koskeviin erityislakeihin.

Säädösvalmistelun yhteydessä olisi lisäksi arvioitava mahdolliset säädösmuutokset tukipalvelulakiin. Tukipalvelulaissa säädetään Suomi.fi-tunnistamisesta ja siitä, että tunnistamistapana käytetään tunnistuslain mukaisia tunnistusvälineitä. Olisi arvioitava, onko valtion digitaalinen identiteetti 5-kohdan mukainen ”muu tunnistusmenetelmä”, vai edellyttäisikö valtion välineen hyväksyminen säädösmuutoksia tukipalvelulain osalta.

Edellä todetusti digipalvelulaissa säädetään tarpeesta ja velvollisuudesta tunnistaa henkilö julkishallinnon sähköisissä asiointipalveluissa, mutta sääntelyä sisältyy myös erilaisiin erityislakeihin. Valmistelussa on tunnistettu mahdollinen tarve arvioida laajemmin henkilöllisyyden osoittamisen sääntelyä yleisellä tasolla. Tässä yhteydessä voitaisiin myös selvittää, tulisiko Suomessa

säätää yleisemmin luotettavista tavoista osoittaa henkilöllisyys sähköisesti, mukaan lukien siitä, millaisia tapoja viranomaistoiminnassa voidaan tai tulee hyväksyä.

8.3. eIDAS ja digitaalinen identiteetti

Esiselvitysvaiheessa on tunnistettu yhtenä ratkaistavana asiana Suomen osalta kansallisen tunnistusvälineen notifiointi ja rajat ylittävä tunnistaminen. Tällä hetkellä haasteita aiheuttaa toisaalta se, että valtion oma tunnistusväline henkilökortti ei ole levinnyt niin laajalle joukolle, että henkilökortin notifiointi tosiasiallisesti edistäisi kansalaisten vastavuoroista tunnistamista jäsenvaltioiden välillä. Toisaalta taas kansalliset sähköiset asiointipalvelut on rakennettu usein siten, että henkilö tunnistetaan suomalaisen henkilötunnuksen perusteella. Rajat ylittävät tunnistusvälineet taas sisältävät kaikki omat tunnisteensa, joiden perusteella tunnistautuva henkilö identifioidaan. Tämä aiheuttaa haasteita kansallisille asiointipalveluille tarjota tosiasiallisesti sähköistä asiointia tunnistauduttaessa eIDAS-tunnistusvälineellä.

Edellytyksenä tunnistusjärjestelmän notifiointille on, että järjestelmän puitteissa myönnetyllä tunnistusvälineellä on mahdollista tunnistautua sähköisesti vähintään yhteen julkisen sektorin palveluun ja että kyseisessä palvelussa vaaditaan tiettyä tunnistamisen varmuustasoa. Tunnistusjärjestelmän ja tunnistusmenetelmän on täytettävä eIDAS-vaatimukset, jotta tunnistusvälinettä voidaan vastavuoroisessa tunnistamisessa hyödyntää. Kansallisen arvioinnin luotettavuus testataan vertaisarvioinnissa.

Tunnistuslaissa tunnistuspalvelun tarjoajalle ja sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset on yhdenmukaistettu eIDAS-asetuksen kanssa. Sähköisen tunnistuksen järjestelmään, joka notifioidaan eIDAS-asetuksen mukaisesti ja täyttää sen mukaiset edellytykset, täyttää automaattisesti myös kansalliset tunnistuslain mukaiset edellytykset. Järjestelmä, joka notifioidaan eIDAS-yhteensopivaksi on lähtökohtaisesti tunnistuslain mukainen tunnistuspalvelu ja tällä hetkellä oletus on, että palvelu ilmoitettaisiin myös osaksi luottamusverkostoa.

Tunnistuslaki ei lähtökohtaisesti mahdollista sitä, että vahvan sähköisen tunnistusvälineen tarjoaja tarjoaisi välinettä kuulumatta luottamusverkostoon. Hallituksen esityksessä (272/2014) todetaan 12 a §:n perusteluissa organisaation mahdollisuudesta tarjota tunnistuspalvelua ilmoittamatta toiminnastaan Traficomille, mutta tällöin tunnistuspalvelun tarjoajalla ei ole vahvan sähköisen tunnistuspalvelun tarjoajan asemaa. Tällöin

palveluntarjoajalla ei ole virallista näyttöä siitä, että se täyttäisi kansalliset ja kansainväliset määräykset vahvasta sähköisestä tunnistamisesta.

Valtion digitaalinen identiteetti ei lähtökohtaisesti olisi osa luottamusverkostoa, eikä siihen sovellettaisi tunnistuslain mukaisia vaatimuksia. Kuten edellä on mainittu, valtion välineestä tulisi säätää erityislainsäädännössä, ja sen status tulisi määritellä kyseisessä laissa myös suhteessa eIDAS-asetuksen mukaisiin vaatimuksiin. Valtion tunnistusjärjestelmän ja sen puitteissa myönnettävän tunnistusmenetelmän/tunnistusvälineen varmuustaso ja varmuustason määrittelytapa olisi sääntelyn avulla määriteltävä suhteessa eIDAS-varmuustasoihin (eIDAS art 6 c). Mahdollisesti laissa voitaisiin viitata varmuustasoasetukseen, tehdä erillinen lista vaatimuksista tunnistusvälineelle taikka lisätä valtioneuvoston asetuksella erikseen säädettäväksi tunnistusvälineen varmuustasosta. Lisäksi tulisi arvioida erillisen valvojan viranomaisen rooli suhteessa valtion tuottamaan välineeseen. eIDAS-asetuksen mukaiset vaatimukset arvioidaan viime kädessä notifiointiprosessin yhteydessä.

Liikenne- ja viestintäviraston tehtävänä on tunnistuslain 42 a §:n mukaan notifioida suomalaisia tunnistusjärjestelmiä komissiolle. Lähtökohtaisesti tunnistuslain sääntely ei estäisi rajat ylittävän tunnistusvälineen notifiointia lain ulkopuolella. Mikäli kuitenkin jatkovalmistelussa todettaisiin tunnistuslaissa olevan esteitä lain ulkopuolisen välineen notifiointiselle, tulisi edelleen selvittää mahdollisuudet tunnistuslain muuttamiseen niiltä osin. Jatkovalmistelussa olisi myös arvioitava, liittykö notifiointimenettelyyn tai Liikenne- ja viestintäviraston rooliin erityiskysymyksiä tilanteessa, jossa ilmoitettava tunnistusjärjestelmä ei olisi osa luottamusverkostoa.

8.4. Tiedonhallinta

Digitaalisen identiteetin attribuuttitietojen luovuttamiseen ja tallentamiseen liittyy tiedonhallinnan ja tietosuojan näkökulmasta selvitettäviä kysymyksiä ja linjattavia asioita. Tavoitteena on tarjota digitaalinen identiteetti yksilön osoitettavaksi erilaisissa asiointitilanteissa. Tavoite eroaa toteutukseltaan esimerkiksi luottamusverkoston mukaisesta yksilön tunnistamisesta ja henkilötietojen luovuttamisesta asiointipalveluun. Luottamusverkoston mukaisessa henkilön tunnistamisessa tunnistuspalvelun tarjoaja luovuttaa tiedot asiointipalvelulle, ei tunnistuksen kohteena oleva yksilö. Viranomaisten välisistä tiedon luovutuksista sekä yleisemmin tiedon luovuttamisesta viranomaisten rekistereistä on säädetty kansallisesti varsin laajasti. Viranomaisen luovuttaessa henkilötietoja lähtökohtana on viranomaisen velvollisuus todeta tiedon saajan oikeus käsitellä näitä tietoja. Tietojen liikkuminen hallinnossa siten, että yksilö itse myöntää pääsyn tietoihin tai

luovuttaa ne toiselle asiointipalvelulle edellyttää erityistarkastelua nykyainsäädännön valossa.

Viranomainen käsittelee ensisijaisesti henkilötietoja tietosuojasetuksen 6 artiklan laillisuusperiaatteen nojalla eli käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Yksityisen sektorin toimijat taas käsittelevät henkilötietoja esimerkiksi lain nojalla, sopimukseen nojautuen taikka henkilön antaman suostumukseen perustuen. Luovutettaessa tietoja valtion ydinidentiteetistä viranomaisille, oletuksena tulisi olla lakisääteinen oikeus tietojen käsittelyyn. Viranomainen ei lähtökohtaisesti voi käsitellä henkilötietoja suostumuksen perusteella. Esimerkiksi tietosuojasetuksen johtolauseen 43 mukaisesti viranomaisen ja rekisteröidyn suhteen välillä on selkeä epäsuhta. Suostumuksen ei voida katsoa olevan vapaaehtoisesti annettu, mikäli rekisterinpitäjänä on viranomainen ja sen vuoksi epätodennäköistä, että suostumus olisi annettu rekisteröidyn omasta vapaasta tahdosta.

Digitaaliseen identiteettiin liittyvien attribuuttitietojen luovuttamisesta ja hyödyntämisestä tulisi todennäköisimmin säätää erikseen. Tämä on tarpeen, sillä voimassa oleva sääntely nojaa pitkälti viranomaisten välisiin tietojen luovutuksiin ja niiden sääntelyyn. Viranomaisen luovuttaessa henkilötietoja rekisteristään on julkisuuslain 13 §:n nojalla selvitettävä henkilötietojen käsittelyn peruste sekä se, miten tietojen suojaus on tarkoitus järjestää. Viranomaisten tietojen luovutusta sääntelee julkisuuslain lisäksi usein toimialatai tietovarantokohtainen erityislainsäädäntö, joka voi asettaa edellytyksiä tiedon luovuttamiselle. Mikäli ratkaisussa tiedot olisivat digitaalisella todisteella tai mobiilisovelluksessa hyödynnettävänä ja yksilö itse käynnistää niiden luovutuksen toiselle taholle, kyse olisi olennaisesta toimintatavan muutoksesta. Jos viranomaisen tulisi jokaisen tunnustustapahtuman yhteydessä selvittää se, mikä on henkilötietojen käsittelyperuste ja onko vastaanottajalla lain nojalla oikeus käsitellä henkilötietoja, mobiilihenkilökortin käytettävyyden alenisi merkittävästi. Digitaalisen identiteetin yleisen sääntelyn lisäksi tulisi arvioida mahdolliset muutokset myös näitä tietoja koskevaan erityislainsäädäntöön.

Lainsäädäntövaiheessa olisi kirkastettava myös sitä, mikä olisi viranomaisen vastuu henkilötietojen luovutuksessa ja millä edellytyksillä henkilötiedot luovutettaisiin yksilön itsensä käyttöön siten, että hän voisi itse osoittaa henkilöllisyytensä erilaisissa asiointitilanteissa. Tietojen osoittamisen analogian tulisi pohjautua nykyiseen kansalaisvarmenteen mukaiseen tiedonluovutukseen sekä käyntiasioinnissa osoitettavaan henkilöllisyyden todentamiseen henkilökortin avulla.

Toisaalta on huomattava, että mobiilihenkilökorttia käytettäisiin jatkossa Suomi.fi-tunnistuksen kautta tunnistauduttaessa julkishallinnon asiointipalveluihin. Organisaation tulee hakea Suomi.fi-tunnistuksen käyttöoikeutta erillisellä käyttöluvahakemuksella, jonka yhteydessä organisaatio ilmoittaa tarvittavat henkilötiedot asiointipalvelukohtaisesti. Digi- ja väestötietovirasto myöntää luvan tunnistuspäalvelun käyttöön ja samalla sen, mitä henkilötietoja organisaatiolle luovutetaan. Henkilön tunnistautuessa julkishallinnon asiointipalveluun, välittää Suomi.fi-tunnistus käyttöluvahakemusprosessin yhteydessä ilmoitetut henkilötiedot asiointipalvelulle. Tällöin henkilötiedot välitetään väestötietojärjestelmästä suoraan asiointipalveluun. Lainvalmisteluvaiheessa tulisikin tarkastella digitaalisen identiteetin ydintietojen luovuttamista ja määrittelyä Suomi.fi-käyttöluvahakemusprosessin yhteydessä. Olisi tarkasteltava sitä, millä tavoin loppukäyttäjä voisi itse määrittellä luovutettavia henkilötietoja Suomi.fi-tunnistuspäalvelun kautta. Edellä mainittujen tiedonluovutussääntöjen lisäksi on huomioitava tukipalvelulain säännökset ja käytännön vaatimukset luovutettaessa henkilötietoja Suomi.fi-tunnistuksen kautta. Alustavien arvioiden mukaan tukipalvelulaki edellyttäisi muutoksia tietojen luovutussääntösten näkökulmasta.

Mobiilihenkilökortin käytön laajetessa sekä julkiselle että mahdollisesti yksityiselle sektorille, muodostaisi se toteutuessaan huomattavan määrän dataa yksilön toiminnasta. Henkilöllisyyttä osoittava asiakirjaa voidaan hyödyntää usealla eri yhteiskunnan sektorilla ja mitä laajemmin valtion takaaman identiteetin ja siihen liittyvien tietojen tarkistus otetaan käyttöön, sitä suuremman vastuun se muodostaa henkilötietojen suojalle. Tavoitteena on, että mobiilihenkilökortin käytöstä syntyvää lokia pseudonymisoitaisiin ja hajautettaisiin, jolloin tiettyjä henkilön tietoja korvattaisiin koodatuilla tietueilla ja hajautettaisiin eri tietosisäلتöihin. On kuitenkin huomattava jäljitettävyyden mahdollistaminen, jotta väärinkäyttötapauksia voitaisiin jäljittää.

Tiedonhallintalain 17 § edellyttää viranomaista lokitietojen keräämiseen huolehtimalla tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista ja keräämällä tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Käyntiasioinnin yhteydessä todistettavasta fyysisestä henkilökortista ei suuressa osassa tapauksia jää jälkeä siitä, että henkilöllisyys on osoitettu jollain tavalla. Esimerkiksi kaupassa asioidessa henkilöllisyys tulee osoittaa ikärajavaltottujen tuotteiden kohdalla. Mikäli henkilöllisyys osoitetaan fyysisellä asiakirjalla, ei tästä jää tosiasiasa jälkeä sähköisiin rekistereihin. Mikäli henkilöllisyys osoitetaan sähköisellä mobiilihenkilökortilla, tietosuoja-asetuksen ja tiedonhallintalain mukaisten

säädösten nojalla tulisi arvioida se, mitä tietoja tosiasiallisesti on tarkoituksenmukaista lokittaa ja mihin tiedot tallennetaan.

IV OSA: YHTEENVETO

Tämän arviomuistion alussa kuvatusti valtiovarainministeriössä on selvitetty sitä, miten digitalisoinnin keinoin voitaisiin varmistaa suoraan kansalaiselle myönnettävien, henkilöllisyyttä määrittävien asiakirjojen tai vahvistettujen tietojen käyttö koko henkilön identiteettiä ja tunnistamista koskevan ekosysteemin toiminnan tehostamiseksi. Tämän tavoitteen saavuttamiseksi luonnosteltuja keinoja on arvioitu tässä muistiossa oikeudellisten reunaehtojen ja olemassa olevan sääntelyn valossa. Alussa on lisäksi kuvattu tulevaisuuden tavoitetilaa, missä kansalaisen ydinidentiteetin säilyttävä ja kontrolloiva identiteetilompakko olisi ”kontrollipiste”, missä kaikki henkilön transaktiot tapahtuisivat lompakko-operaattoreiden tarjoaman digitaalisen lompakon kautta. Tällöin valtion rekistereissä olevia vahvistettuja tietoja voitaisiin tuoda henkilön identiteetilompakkoon, josta henkilö voisi osoittaa omia tietojaan sekä julkiselle että yksityiselle sektorille.

Kootusti hankkeen tavoitteena on:

- luoda kaikille Suomessa väestötietojärjestelmään kirjatuille henkilöille digitaalinen identiteetti ja sen osoittava digitaalinen todiste;
- tuottaa ja tarjota käyttäjälle yksi digitaalinen tallennusmenetelmä (digitaalinen lompakko), jolla digitaalista identiteettiä voidaan käyttää ja siihen liitettyjä varmennettuja väittämiä (tietoja) voidaan välittää digitaalisiin palveluihin;
- tuottaa poliisin tai ulkoministeriön myöntämään passiin ja henkilökorttiin pohjautuva henkilöllisyyden osoittamisen ratkaisu (mobiilihenkilökortti);
- luoda valmiudet tallentaa ja välittää eri viranomaisten myöntämää varmennettua tietoa (lupa, henkilöön liittyvä tieto) viranomaisen tuottamaan digitaalisen identiteetin tallennusvälineeseen (digitaalinen lompakko)
- luoda valmiudet tallentaa myös yksityisen puolen varmennettua tietoa, esim. tietoa digitaalisesta arvosta (digitaalinen euro, maksusitoumukset, palvelusetelit) viranomaisen tuottamaan digitaalisen identiteetin tallennusvälineeseen (digitaalinen lompakko), jolloin sillä voisi siirtää digitaalista arvoa toiseen digitaaliseen lompakkoon tai digitaaliseen maksupalveluun.

Hankkeen aikana toteutettavana tavoitteena siten on, että valtion varmistamat henkilöllisyyttä määrittävät tiedot tulevat kansalaisen käyttöön uudessa digitaalisessa muodossaan, esimerkiksi puhelinsovelluksena, sekä käyntiasioinnissa että sähköisessä asioinnissa. Tätä tavoitetta puoltavat

henkilön identiteettitietoihin liittyvät ihmis- ja perusoikeusnäkökohdat sekä henkilön omien tietojen hallinnan merkitys. Henkilön digitaalinen identiteetti ja sen hyödyntämismahdollisuudet ovat keskeisessä asemassa turvattaessa osallistumisoikeuksia, hyvää hallintoa ja yhdenvertaisuutta digitaalisessa yhteiskunnassa.

Tässä arviomuistiossa kuvatussa ratkaisusta on tunnistettu neljä kokonaisuutta, joita niiden luonteen vuoksi on arvioitu oikeudellisesta näkökulmasta erillisinä valtiontuki- ja kilpailuoikeudellisten säädösten valossa. Näitä ovat:

1. Digitaalisen identiteetin muodostaminen ja myöntäminen.
2. Ratkaisut, jotka mahdollistavat digitaalisen henkilöllisyyden osoittamisen käyntiasioinnissa.
3. Ratkaisut, jotka mahdollistavat muiden viranomaistietojen, kuten lupien tai vahvistettujen rekisteritietojen esittämisen.
4. Digitaalisen henkilöllisyyden osoittaminen julkisen sektorin asiointipalveluissa sähköisesti.

Kokonaisuuksia on arvioitu sen pohjalta, olisiko ratkaisu osa julkisen hallintotehtävän hoitamista, vai liittyisikö siihen sellaisia valtiontuki- taikka kilpailulainsäädännöllisiä riskejä, ettei valtio voisi kyseistä ratkaisua tuottaa. Digitaalisen identiteetin muodostaminen ja digitaalisen henkilöllisyyden osoittaminen käyntiasioinnissa mobiilisovelluksen avulla nähdään julkisen vallan käyttönä ja keskeisinä viranomaistehtävänä digitalisoituvassa yhteiskunnassa. Ratkaisut, jotka mahdollistavat henkilöllisyystietojen esittämisen, vertautuvat henkilöllisyysasiakirjojen esittämiseen ja voidaan oikein säänneltynä nähdä niin ikään julkisen vallan käyttönä.

Arvioitavista kokonaisuuksista moniulotteisin on julkisen sektorin tunnistuspalvelu, joka mahdollistaisi digitaalisen identiteetin käyttämisen henkilöllisyyden osoittamiseksi julkissektorin asiointipalveluissa. Olemassa olevasta markkinasta huolimatta toiminnalla voidaan nähdä olevan kiinteä yhteys julkisen vallan käyttöön siten, että siihen ei sovelleta kilpailu- ja valtiontukisääntelyä. Digitaalisen henkilöllisyyden myöntäminen ja luotettavien sähköisten asiointikanavien tarjoaminen julkisiin palveluihin voidaan molemmat nähdä keskeiseksi viranomaistoiminnaksi. Valtion vahvistamaan digitaaliseen identiteettiin kuuluu olennaisesti se, että valtio myös varmistaa henkilöllisyyden käytettävyyden. Toisaalta viranomaisella on lähtökohtainen velvoite tuottaa palvelunsa myös sähköisesti ja tähän kokonaisuuteen kuuluu myös tunnistamisen mahdollistaminen. Näillä perusteilla toimintaa ei pidetä sellaisena taloudellisena toimintana, johon

sovellettaisiin kiellettyä valtiontukea tai kilpailuneutraliteettia koskevaa sääntelyä.

Muistiossa on kilpailu- ja valtiontukinäkökulmien lisäksi tarkastelu erityisesti mobiilisovelluksen suhdetta henkilöllisyyttä osoittaviin asiakirjoihin, tunnistuslakiin sekä tiedonhallintaan. Säädettyä valtion digitaalisen identiteetin muodostamisesta, tarjoamisesta ja sen hyödyntämisestä, on tunnistettu alustavia sääntelyn muutostarpeita, jotka tulisi lainsäädännön valmisteluvaiheessa huomioida.

Muistiossa esitetyn arvion mukaan hankkeessa tulee ensisijaisesti arvioitavaksi se, millä tavoin mobiilihenkilökortin asema henkilöllisyyttä osoittavana asiakirjana varmistetaan lainsäädännön keinoin. Jotta mobiilihenkilökorttia tosiasiallisesti voitaisiin yhteiskunnassa hyödyntää, olisi sille luotava sääntelyn avulla rinnakkainen asema fyysisen henkilökortin kanssa. On myös tunnistettu kysymys siitä, olisiko kansallisesti tarvetta yleistasoiselle sääntelylle henkilöllisyyden osoittamisesta erilaisissa tilanteissa. Tulevaisuuden asiointitapojen moninaisuus saattaisi edellyttää laajempaa arviota henkilöllisyyden osoittamisen tavoista, luotettavuudesta ja sääntelystä yhteiskunnan eri osa-alueilla. Esimerkiksi konkreettinen pohdittava kysymys on, pitäisikö kaikilla suomalaisilla olla virallinen henkilöllisyystodistus tai mikä on digitaalisen henkilöllisyystodistuksen rooli?

Mobiilihenkilökorttia voitaisiin hyödyntää sekä käyntiasioinnissa että sähköisissä asiointipalveluissa. Oikeudellisen arvion mukaan digitaalisen henkilöllisyyden osoittaminen sähköisessä asiointipalvelussa ei tavoitteiltaan, menetelmältään tai luotettavuudeltaan tulisi olennaisesti eroamaan tunnistuslain olettamista tunnistuspalveluista. Olennainen ero on, että kyse olisi digitaalisesta henkilöllisyydestä ja tätä henkilöllisyyttä osoittavasta välineestä, jotka valtio myöntää ja tuottaa käyttäen julkista valtaa osana julkisten palvelujen tuottamista. Väline ei kuitenkaan tulisi osaksi luottamusverkostoa eikä se siten olisi tunnistuslain mukainen tunnistuspalvelu. Tämän vuoksi digitaalisen henkilöllisyyden tuottamisesta ja siihen liittyvästä tunnistuspalvelusta tulisi säätää erikseen lailla. Sääntelyssä olisi otettava kantaa ainakin viranomaisten tehtäviin, tietojen käsittelyyn, tuotettavaan palveluun ja sen käytettävyyteen erilaisissa asiointitilanteissa. Erityisesti olisi myös huomioitava ne tunnistamisen luotettavuutta ja turvallisuutta koskevat edellytykset, jotka on kansallisesti sisällytetty tunnistuslakiin.

Tiedonhallinnan osalta muistiossa on arvioitu erityisesti tietosisältöön sekä sen hyödyntämiseen liittyviä kysymyksiä. Lähtökohtaisesti tietojen osoittamisen analogian tulisi pohjautua nykyiseen kansalaisvarmenteen mukaiseen

tiedonluovutukseen sekä käyntiasioinnissa osoitettavaan henkilöllisyyden todentamiseen henkilökortin avulla. Toisaalta taas on huomattava, että mobiilihenkilökorttia käytettäisiin jatkossa Suomi.fi-tunnistuksen kautta tunnistauduttaessa julkishallinnon asiointipalveluihin, jolloin tiedonluovutus tapahtuisi tunnistuspalvelun kautta sen nykyisten toiminnallisuuksien avulla. Välitettäessä henkilötietoja yksityiselle sektorille, olisi jatkotarkastelussa kuitenkin selvitettävä tiedonhallintaprosessit laajemmin.

Tässä muistiossa on käsitelty niitä keskeisimpiä ratkaisuja, joita hankkeessa on suunniteltu toteutettavan digitaalisen henkilöllisyyden ja siihen liittyvien sähköisen asioinnin ratkaisujen osalta. Konkreettinen juridinen tarkastelu on kuitenkin sähköisen asioinnin osalta toistaiseksi rajattu ratkaisuihin, jotka mahdollistavat digitaalisen henkilöllisyyden hyödyntämisen julkisen sektorin palveluissa. Osassa 2 kuvatut hankkeen tavoitteet ja erityisesti osassa 1 kuvatut visiot sähköisen asioinnin tulevaisuudesta ja siihen liittyvästä EU-kehityksestä edellyttävät uusia avauksia myös yksityisen sektorin palveluihin. Muistiossa on myös todettu, että raja yksityisen ja julkisen sektorin asioinnin välillä on osin vaikeasti hahmotettavissa ja tulee jatkossa edelleen hämärtymään. Nämä muutokset vaativat uusia toimintamalleja ja -tapoja myös digitaalisen identiteetin kansalliseen lainsäädäntöön, toteutukseen ja hyödyntämiseen.

Tämän muistion tavoitteena on esitettyjen ratkaisujen arvioinnin lisäksi käynnistää keskustelu siitä, millä tavoin esitetyt digitaalisen identiteetin ratkaisut voisivat palvella koko yhteiskuntaa. Arviomuistion sisältämän tulevaisuuden vision pohjalta on tarkoituksenmukaista arvioida myös sitä, millä tavalla valtion tuottaman digitaalisen identiteetin avulla yksilöllä olisi nykyistä parempi mahdollisuus hallita itseään koskevien tietojen välittämistä digitaalisiin palveluihin. Tämä muutos voisi palvella nykyisiä ja uusia digitaalisen identiteetin palvelutuottajia sekä laajemmin yksityisen sektorin asiointipalveluita. Muistiossa esitetyt ratkaisut voivat osin olla käytettävissä myös näiden toimijoiden tarpeisiin. Kehitystä olisi kuitenkin tehtävä yhteistyössä viranomaisten ja yksityisen sektorin kanssa. Tämä edellyttää myös näkemystä digitaalisen identiteetin hallinnan ja käytön tulevaisuudesta sekä tunnustuslain tulevista kehitystarpeista.

Kirjallisuuslähteet

Alkio, Mikko: Valtiontuet, 2.1 Tuen käsitteestä (Alma verkkokirjahylly)

Heikkilä, Satu – Hirvelä Päivi: Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 642. (Alma Verkkokirjahylly)

Husa, Jaakko – Pohjolainen, Teuvo: Julkisen vallan oikeudelliset perusteet: Johdatus julkisoikeuteen (2014) (Alma Verkkokirjahylly)

Kuoppamäki, Petri: Uusi kilpailuoikeus (2018, Alma Talent) (Alma Verkkokirjahylly, 18.1.2021 14:33:12)

Mäenpää Olli: Hallintolaki ja hyvän hallinnon takeet, 2008 (Edilex)

Mäenpää, Olli: Yleinen hallinto-oikeus, s. 95 (Alma Verkkokirjahylly)

Niemivuo, Matti – Keravuori-Rusanen, Marietta – Kuusikko, Kirsi: Hallintolaki (2010)

Oinonen, Mika: EU:n ja Suomen kilpailuvalvonta, s. 267. (Alma Verkkokirjahylly)

Voutilainen Tomi: Digitaalisten palvelujen sääntely (2020) (Alma Verkkokirjahylly)

Voutilainen Tomi: ICT-oikeus sähköisessä hallinnossa (2009) (Edilex)

Voutilainen Tomi: Sähköisen identiteetin käytöstä julkisessa hallinnossa (Referee-artikkeli, Edilex 2008/8)