

Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista sekä laki digitaalisesta henkilöllisyystodistuksesta. Lisäksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annettua lakia, väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annettua lakia, henkilötietojen käsittelystä poliisitoimessa annettua lakia, henkilökorttilakia, passilakia sekä hallinnon yhteisistä sähköisen asioinnin tukipalveluista annettua lakia ehdotetaan muutettavaksi.

Ehdotuksella on tarkoitus mahdollistaa digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen tuottaminen ja käyttö. Kyse olisi uusista digitaalista asiointia tukevista mobiilisovelluksista, joita Poliisi ja Digi- ja väestötietovirasto tuottaisivat vahvistettujen henkilötietojen osoittamiseksi. Digitaalinen henkilöllisyystodistus toimisi myös henkilöllisyyttä osoittavana asiakirjana passin ja henkilökortin tavoin ja sisältäisi lisäksi vahvan sähköisen tunnistautumisen ominaisuuden. Laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista sisältäisi säännökset digitaalisen henkilöllisyyden tietojärjestelmästä, joka toimisi sekä digitaalisen henkilöllisyystodistuksen että ulkomaalaisen digitaalisen asiointivälineen perustana. Sääntely koskisi viranomaisten tehtävien lisäksi muun muassa tietojärjestelmän vaatimuksia ja tietoturvallisuutta sekä henkilötietojen käsittelyä.

Lisäksi esityksellä mahdollistettaisiin vaihtoehtoinen tunnistusväline sellaisille henkilöille, jotka eivät halua tai voi käyttää mobiilisovellusta. Tunnistusväline toimisi julkisen sektorin sähköisessä asioinnissa ja sen myöntäisi Digi- ja väestötietovirasto.

Esitys liittyy valtion vuoden 2023 talousarvioesitykseen ja on tarkoitettu käsiteltäväksi sen yhteydessä. Lait on tarkoitettu tulemaan voimaan 1.9.2023.

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ.....	1
PERUSTELUT	5
1 Asian tausta ja valmistelu	5
1.1 Tausta	5
1.2 Valmistelu	5
2 Nykytila ja sen arviointi.....	7
2.1 Toimintaympäristö yleisesti.....	7
2.2 Henkilöllisyyttä osoittavat asiakirjat: passi ja henkilökortti	7
2.3 Vahva sähköinen tunnistaminen	10
2.4 Vahvan sähköisen tunnistamisen luottamusverkosto ja markkina	11
2.5 Digi- ja väestötietoviraston varmennepalvelut.....	13
2.6 Sähköinen tunnistautuminen julkishallinnon palveluihin	14
2.7 Komission ehdotus eIDAS-asetuksen muuttamiseksi.....	16
3 Tavoitteet.....	17
4 Ehdotukset ja niiden vaikutukset	18
4.1 Keskeiset ehdotukset.....	18
4.2 Pääasialliset vaikutukset.....	21
4.2.1 Taloudelliset vaikutukset	21
4.2.1.1 Vaikutukset kotitalouksiin	21
4.2.1.2 Vaikutukset yrityksiin palveluiden tarjoajina	23
4.2.1.3 Vaikutukset yrityksiin palveluiden hyödyntäjinä.....	26
4.2.1.4 Kilpailuvaikutukset	28
4.2.1.5 Vaikutukset tunnistusmarkkinoiden kehittymiseen	35
4.2.1.6 Vaikutukset sisämarkkinoihin.....	36
4.2.1.7 Vaikutukset julkiseen talouteen	37
4.2.1.8 Vaikutukset kansantalouteen.....	41
4.2.2 Vaikutukset viranomaisten toimintaan.....	41
4.2.2.1 Vaikutukset tehtäviin ja menettelytapoihin.....	41
4.2.2.2 Vaikutukset organisaatioon ja henkilöstöön	43
4.2.2.3 Vaikutukset viranomaisten tiedonhallintaan	44
4.2.3 Ympäristövaikutukset	47
4.2.4 Muut yhteiskunnalliset vaikutukset.....	47
4.2.4.1 Vaikutukset kansalaisten asemaan yhteiskunnassa ja kansalaisyhteiskunnan toimintaan.....	47
4.2.4.2 Vaikutukset lapsiin.....	49
4.2.4.3 Vaikutukset työllisyyteen ja työelämään.....	50
4.2.4.4 Vaikutukset rikoksentorjuntaan ja turvallisuuteen	50
4.2.4.5 Tietoyhteiskuntavaikutukset	51
5 Muut toteuttamisvaihtoehdot	56
5.1 Vaihtoehdot ja niiden vaikutukset.....	56
5.2 Ulkomainen lainsäädäntö ja muut ulkomailla käytetyt keinot	60
5.2.1 Tanska	60
5.2.2 Viro	61
5.2.3 Norja.....	62

5.2.4 Alankomaat	63
5.2.5 Saksa	64
6 Lausuntopalaute ja jatkovalmistelu	66
6.1 Lausuntopalaute	66
6.2 Jatkovalmistelu.....	69
7 Säännöskohtaiset perustelut	70
7.1 Laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista	70
7.2 Laki digitaalisesta henkilöllisyystodistuksesta.....	86
7.3 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta	93
7.4 Laki henkilötietojen käsittelystä poliisitoimessa annetun lain 16 §:n ja 22 §:n muuttamisesta.....	100
7.5 Laki henkilökorttilain muuttamisesta.....	101
7.6 Laki passilain muuttamisesta	101
7.7 Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta	101
7.8 Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:n ja 9 §:n muuttamisesta	107
8 Lakia alemman asteinen sääntely	107
9 Voimaantulo	107
10 Toimeenpano ja seuranta	107
11 Suhde muihin esityksiin.....	108
11.1 Esityksen riippuvuus muista esityksistä.....	108
11.2 Suhde talousarvioesitykseen	109
12 Suhde perustuslakiin ja säätämisyjärjestys	109
12.1 Tehtävien siirtäminen viranomaisten välillä	109
12.2 Yksityisyyden suoja ja henkilötietojen suoja	110
12.3 Yhdenvertaisuus.....	117
12.4 Lainsäädäntövallan siirtäminen viranomaiselle	121
LAKIEHDOTUKSET	123
Laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista.....	123
Laki digitaalisesta henkilöllisyystodistuksesta.....	132
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta.....	136
Laki henkilötietojen käsittelystä poliisitoimessa annetun lain 16 ja 22 §:n muuttamisesta	140
Laki henkilökorttilain muuttamisesta.....	142
Laki passilain muuttamisesta	143
Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta	144
Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 ja 9 §:n muuttamisesta.....	147
LIITE	149
RINNAKKAISTEKSTIT	149
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta.....	149

Laki henkilötietojen käsittelystä poliisitoimessa annetun lain 16 ja 22 §:n muuttamisesta	155
Laki henkilökorttilain muuttamisesta.....	157
Laki passilain muuttamisesta	158
Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta	159
Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 ja 9 §:n muuttamisesta.....	164

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Pääministeri Marinin hallitusohjelmassa (<https://valtioneuvosto.fi/marinin-hallitus/hallitusohjelma>, s. 107) on asetettu tavoitteeksi, että Suomi tunnetaan edelläkävijänä, jossa digitalisaation ja teknologisen kehityksen luomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen. Tavoitteena on nostaa julkisen sektorin teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä. Hallitusohjelmassa on asetettu tavoitteiksi muun muassa edistää Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen sekä edistää toimivien tunnistusratkaisujen kehittymistä. Hallitusohjelmassa on lisäksi nostettu esiin sekä henkilön mahdollisuudet hallita omia julkisissa palveluissa olevia tietojaan että riittävät tukipalvelut sähköisten julkisten palveluiden käyttöön kansalaisten yhdenvertaisuuden varmistamiseksi.

Hallitusohjelman tavoitteiden saavuttamiseksi valtiovarainministeriö on asettanut hankkeen digitaalisen henkilöllisyyden ja sen hyödyntämistapojen kehittämiseksi. Hankkeen yhteydessä valtiovarainministeriö on asettanut digitaalisen henkilöllisyyden lainsäädäntötyöryhmän sekä vaikutusarvioinnin alatyöryhmän valmistelevaan ehdotukset sellaiseksi lainsäädännöksi, joka mahdollistaa digitaalisen todisteen luomisen sekä sen hyödyntämisen yhteiskunnan palveluissa henkilöllisyyden ja varmennettujen identiteettitietojen osoittamiseksi.

Hallituksen esityksen taustalla vaikuttaa myös digitaalisia identiteettiratkaisuja koskeva kehitys EU:ssa. Euroopan komissio antoi 3.6.2021 ehdotuksen COM (2021)281 Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 muuttamiseksi. Kyseinen ehdotus ja myöhemmin annettava varsinainen muutosasetus tulevat vaikuttamaan merkittävästi digitaalisen henkilöllisyyden ja siihen liittyvien palveluiden toteuttamiseen Suomessa.

1.2 Valmistelu

Ehdotetun digitaalisen henkilöllisyyden lainsäädännön taustalla on pidempiaikainen kehitys henkilöllisyyden ja digitaalisten palvelujen alalla. Henkilön virallisen identiteetin hallinnointia ja käyttöä koskevia selvityksiä on toteutettu viimeisen vuosikymmenen aikana useissa eri hankkeissa. Kattavimpana selvityksenä voidaan pitää sisäministeriön joulukuussa 2010 julkaistua identiteettiohjelman loppuraporttia (Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010, <https://julkaisut.valtioneuvosto.fi/handle/10024/79876>), jossa kuvataan tuolloin viranomaisen tuottaman identiteetin luomiseen, hallinnointiin ja käyttöön kohdistuneita kehitystarpeita. Osa raportin ehdotuksista on toteutunut sen julkaisun jälkeen.

Valtiovarainministeriö pyysi syksyllä 2018 silloiselta Väestörekisterikeskukselta esiselvitystä sähköisen tunnistamisen vaihtoehtoista (<https://julkaisut.valtioneuvosto.fi/handle/10024/161432>), 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 mahdollisimman laajasti koko väestön saatavilla syrjimättömästi henkilön iästä tai fyysisistä rajoitteista huolimatta. Kansalaisten lisäksi myös Suomessa asoivien ulkomaalaisten henkilöiden tunnistamisen tulisi olla mahdollista. Selvitystyötä arvioi valtiovarainministeriön asettama ohjausryhmä, joka ei kuitenkaan ollut päätelmissään yksimielinen. Eriävän mielipiteen

jättivät liikenne- ja viestintäministeriö, Kilpailu- ja kuluttajavirasto ja Liikenne- ja viestintävirasto Traficom. Lisäksi digitaalisissa palveluissa tapahtuvaa henkilöllisyyden osoittamista, todentamista ja tunnistamista on kuvattu myös useissa sähköistä tunnistamista koskeissa hallituksen esityksissä.

Sähköistä tunnistamista koskevien selvitysten ohella valtiovarainministeriön asettama henkilö-tunnuksen uudistamista pohtinut työryhmä käsitteli huhtikuussa 2020 julkaisemassaan loppuraportissa (HETU-uudistuksen loppuraportti (Valtiovarainministeriön julkaisuja – 2020:20, <https://julkaisut.valtioneuvosto.fi/handle/10024/162162>) henkilön yksilöimistä varten tarvittavien rekisteröintitietojen ja -menettelyiden muutostarpeita.

Valtiovarainministeriö asetti 8.10.2020 hankkeen digitaalisen henkilöllisyyden ja sen hyödyntämistapojen kehittämiseksi (<https://vm.fi/hanke?tunnus=VM161:00/2020>). Hankkeen toimikausi on 8.10.2020 – 30.6.2023. Hankkeelle asetettiin ohjausryhmä, joka koostui valtiovarainministeriön, sisäministeriön, liikenne- ja viestintäministeriön, sosiaali- ja terveysministeriön, opetus- ja kulttuuriministeriön sekä työ- ja elinkeinoministeriön edustajista. Ohjausryhmän työtä tuki valtiovarainministeriön, Digi- ja väestötietoviraston ja Poliisihallituksen edustajista koostuva sihteeristö, joka valmisti ohjausryhmälle esiteltävät asiat.

Hanke koostuu kahdesta työpaketista, joihin liittyviä tehtäviä on toteutettu soveltuvin osin rinnakkain. Hankkeen 1. työpaketin selvitysten tulokset sekä linjaukset koottiin 18.3.2021 julkaistuihin arviomuistioon digitaalisen henkilöllisyyden kehityksestä (<https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=938337e8-306d-4737-bc4b-02bd2911f308>). Valtiovarainministeriö pyysi lausuntoja arviomuistiosta lausuntopalvelu.fi-järjestelmän kautta aikavälillä 18.3.2021–30.04.2021. Lausuntoja annettiin yhteensä 117 kappaletta. Lausunnot sekä lausuntotiivistelmä löytyvät edellä mainituilta hankkeen sivuilta. Digitaalisen henkilöllisyyden kehitystä koskevan arviomuistion ohella Traficom ja Kilpailu- ja kuluttajavirasto ovat tehneet oman selvityksenä sähköisen tunnistamisen markkinoista (https://www.trafficom.fi/sites/default/files/media/publication/S%C3%A4hk%C3%B6isen_tunnistamisen_markkinat_-_S%C3%A4hk%C3%B6inen%20tunnistaminen%20turvallisen%20asioinnin%20mahdollistajana%2017%2003%202021p.pdf).

Hankkeen 2. työpaketin mukaiset toimenpiteet aloitettiin kesällä 2021. Hankkeelle asetettiin 23.6.2021 lainsäädäntötyöryhmä, joka koostui valtiovarainministeriön, sisäministeriön, opetus- ja kulttuuriministeriön, liikenne- ja viestintäministeriön, työ- ja elinkeinoministeriön sekä sosiaali- ja terveysministeriön jäsenistä ja Liikenne- ja viestintäviraston, Digi- ja väestötietoviraston sekä poliisihallituksen asiantuntijoista. Lisäksi hankkeelle asetettiin vaikutusarvioinnin alatyöryhmä, joka koostui valtiovarainministeriön, sisäministeriön, liikenne- ja viestintäministeriön, Liikenne- ja viestintäviraston, Digi- ja väestötietoviraston, poliisihallituksen ja Kuluttaja- ja kilpailuviraston jäsenistä. Ryhmät osallistuivat hallituksen esityksen valmisteluun, mutta aikataulullisista syistä hallituksen esitys viimeisteltiin valtiovarainministeriön virkatyönä.

Valtiovarainministeriö pyysi lausuntoja luonnoksesta hallituksen esitykseksi digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi lausuntopalvelu.fi-järjestelmän kautta aikavälillä 21.2.–8.4.2022. Lausuntopyyntöön saapui lausuntoja määräajassa yhteensä 651 kappaletta. Näistä 127 lausuntoa tuli organisaatioilta. Kymmenen vastaajaa ilmoitti, että heillä ei ole asiaan lausuttavaa. Lisäksi luottamusverkoston toimijoilta tiedusteltiin lausuntoa vielä määräajan päätyttyä erikseen. Tiedusteluun vastanneet vahvistivat, etteivät jätä asiasta erikseen lausuntoa vaan kertoivat yhtyvän etujärjestöjen (Finanssiala ry:n tai FiComin) lausuntoihin. Kansalaispalautteena saatuja lausuntoja saapui määräajassa yhteensä 524 kappaletta. Lausunnot ja lausuntotiivistelmä ovat nähtävillä valtioneuvoston hankeikkunassa (hanketunnus VM092:00/2021).

Lakiehdotuksen sisältöä on käsitelty Digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmän kokouksissa 1.6.2022 sekä 23.6.2022.

2 Nykytila ja sen arviointi

2.1 Toimintaympäristö yleisesti

Esityksen kohteena oleva lainsäädäntö ja toiminnalliset ratkaisut tulisivat osaksi toimintaympäristöä, jossa henkilöllisyyttä osoitetaan ja henkilöön liittyviä tietoja käsitellään hyvin erilaisin tavoin. Kansalaisilla ja muilla suomalaisessa yhteiskunnassa asioivilla henkilöillä on tarve esittää itseään koskevia henkilötietoja sekä todistaa henkilöllisyytensä monenlaisissa tilanteissa sekä perinteisillä henkilöllisyyttä osoittavilla asiakirjoilla fyysisessä asiointitilanteessa että sähköisesti erilaisissa asiointipalveluissa. Tarve henkilön tunnistamiselle voi perustua käytännön tarpeeseen tai toimintatapaan, mutta sitä voidaan edellyttää myös lainsäädännössä tai sopimusperusteisesti. Esimerkiksi kuluttajansuojalaissa (38/1978) on asetettu henkilöllisyyden huolellista todentamista koskeva velvoite kuluttajaluottosopimusten osalta ja tarkennettu edelleen sitä, miten henkilöllisyys on todennettava sähköisen asioinnin tilanteessa.

Nykytilassa menetelmiä henkilöllisyyden osoittamiseksi ja tietojen esittämiseksi tarkastellaan useimmiten joko sähköisen asioinnin tai perinteisen käyntiasioinnin näkökulmasta. Ensimmäisen tyypillisenä esimerkkinä voidaan pitää vahvaa sähköistä tunnistautumista pankkitunnuksilla ja jälkimmäisen tyypillisenä esimerkkinä passin esittämistä henkilöllisyystodistuksena. Asiointitilanteet ovat kuitenkin kehittyneet monimuotoisemmiksi, ja esimerkiksi käyntiasioinnissa voitaisiin hyödyntää myös sähköisen asioinnin menetelmiä. Toisaalta sähköisessä asiointissa voidaan kehitystä viedä kohti henkilön hallussa olevia vahvistettuja asiakirjoja – periaatteellisesti samalla tavoin, kuin viranomaisen myöntämä passi on henkilön itsensä hallussa ja vapaasti esitettävissä. Digitaalisen henkilöllisyyden kehitys edellyttää toimintaympäristön tarkastelua kokonaisuutena ja esitykseen sisältyvät ehdotukset koskettavat sekä sähköisen asioinnin ja tunnistamisen että perinteisten henkilöllisyyttä osoittavien asiakirjojen sääntelyä. Molempien nykytilaa on tarkasteltu jäljempänä.

2.2 Henkilöllisyyttä osoittavat asiakirjat: passi ja henkilökortti

Yleisesti henkilöllisyyttä osoittavista asiakirjoista

Suomen lainsäädäntö ei säätele 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. Lainsäädäntö ja henkilöllisyyden osoittamisen käytännöt perustuvat yhtäältä tiettyjen viranomaisen myöntämien asiakirjojen, käytännössä passin ja henkilökortin, sääntelyyn sekä toisaalta tietyssä viranomaisessa, toimialalla tai asiointitapahtumassa tapahtuvan kasvokkain tehtävän tunnistamisen sääntelyyn. 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. Voimassa oleva passi tai henkilökortti on tällä hetkellä noin 4,1 miljoonalla suomalaisella, joista alaikäisiä on noin 580 000. Passeja ja henkilökortteja myönnetään vuosittain yhteensä noin 1,1 miljoonaa kappaletta, ja yhteensä voimassa olevia passeja ja henkilökortteja on noin 4,8 miljoonaa kappaletta.

Passilaissa (671/2006) ja henkilökorttilaissa (663/2016) säädetään esimerkiksi näiden asiakirjojen myöntämisestä, luovuttamisesta ja peruuttamisesta. Kekseistä niissä ovat säännökset 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.

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 passeista ja henkilökorteista annetulla valtioneuvoston asetuksella (1167/2016).

Henkilökortti ja sen myöntäminen

Henkilökorttilaissa säädetään Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle henkilöllisyyden osoitukseksi myönnettävästä henkilökortista. Lain 1 pykälän 2 momentin mukaan mitä henkilökorttilaissa säädetään henkilökortista, koskee myös Suomessa oleskelevalle ulkomaalaiselle henkilölle myönnettävää henkilökorttia (ulkomaalaisen henkilökortti), alaikäiselle henkilölle ilman huoltajien suostumusta myönnettävää henkilökorttia (alaikäisen henkilökortti) ja väliaikaista henkilökorttia.

Suomen kansalaiselle myönnettyä henkilökorttia voidaan lain 2 §:n mukaan käyttää passin sijasta matkustusasiakirjana passilain 2 §:n 1 momentin nojalla annettujen säännösten mukaisesti. Pykälän 2 momentin mukaan mitä 1 momentissa säädetään, ei koske alaikäisen henkilökorttia, 15 §:ssä tarkoitettua väliaikaista henkilökorttia eikä 17 §:n 3 momentissa tarkoitettua henkilökorttia.

Henkilökorttia haetaan poliisilta. Hakemus voidaan panna vireille sähköisesti. Hakijan tulee saapua henkilökohtaisesti viranomaisen luokse hakemuksen täydentämistä varten, jollei 10 §:stä muuta johdu. Henkilökorttilain 10 §:n mukaan hakijan ei tarvitse saapua henkilökohtaisesti viranomaisen luokse henkilökorttia sähköisesti haattaessa, jos 1) hakijalle on henkilökorttihakemusta edeltävän kuuden vuoden aikana myönnetty Suomen kansalaisen henkilökortti tai passi, jota haattaessa 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.

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 viivästymisestä aiheutuisi kohtuutonta haittaa, henkilökortti voidaan lain 16 §:n nojalla myöntää ilman tämän suostumusta. Alaikäiselle hakijalle voidaan ilman huoltajien suostumusta myöntää alaikäisen henkilökortti. Kyse on alaikäisen erityisestä henkilökorttityypistä, jota koskevaan hakemukseen ei tarvita huoltajien suostumusta. Alaikäisen henkilökortin myöntämiselle ei säädetä henkilökorttilaissa alaikäraja.

Henkilökorttia koskevaan hakemukseen on liitettävä hakijan kasvokuva, josta hakija on hyvin tunnistettavissa. Passiin ja henkilökorttiin liitettävästä kasvokuvasta annetun sisäministeriön asetuksen (1168/2016) 1 §:n mukaan passihakemukseen ja henkilökorttihakemukseen tulee liittää yksi enintään kuusi kuukautta vanha mustavalkoinen tai värillinen valokuva hakijan kasvoista.

Henkilökortin siru ja sen tietoturva

Unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä annettu Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157, jäljempänä EU:n ID-asetus, tuli voimaan elokuun alussa 2019. EU:n ID-asetuksen 3 artiklan 5 kohdan mukaan henkilökortteihin on sisällyttävä erittäin turvallinen tallennusväline, jonka on sisällettävä biometrisiä tietoja, jotka ovat kortin haltijan kasvokuva ja kaksi sormenjälkeä yhteentoimivassa digitaalisessa muodossa. Jäsenvaltioiden on biometristen tunnisteiden keräämisessä sovellettava komission täytäntöönpanopäätöksessä C(2018) 7767 vahvistettuja teknisiä eritelmiä.

Henkilökorttilain 5 §:n mukaan henkilökortissa on tekninen osa, johon talletetaan kansalaisvarmenteen tiedot, sähköisen asioinnin edellyttämät kortinhaltijan tunnistautumistiedot ja välttämättömät tiedot. Tekniseen osaan voidaan tallettaa myös 4 §:n 1 momentissa tarkoitetut tiedot. Alaikäisen henkilökortissa ja väliaikaisessa henkilökortissa ei ole pykälässä tarkoitettua teknistä osaa. Viittaus lain 4 §:n 1 momenttiin tarkoittaa sitä, että henkilökortin teknisessä osassa eli sirussa voi olla henkilökortin haltijan sukunimi, etunimet, sukupuoli, syntymäaika ja henkilötunnus, henkilökortin myöntämispäivä ja viimeinen voimassaolopäivä, henkilökortin myöntänyt viranomainen, kortin numero ja Suomen kansalaisten osalta tieto kansalaisuudesta. Henkilökortin siruun voidaan tallettaa myös kortinhaltijan valokuva ja nimikirjoitus.

Kuten edellä ilmenee, EU:n ID-asetuksessa säädetään, että kansallisten EU:n jäsenvaltioiden myöntämien henkilökorttien on täytettävä EU:n ID-asetuksessa säädetyt turvallisuutta koskevat vähimmäisvaatimukset sekä tietyt eritelmit. Sormenjälki on biometrisenä tunnisteena pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Biometriset tunnisteet asettavat erityisiä vaatimuksia tietoturvalle, jotta yksityisyyden suojan toteutuminen voidaan varmistaa. Tästä syystä henkilökortin siruun liittyvästä tietoturvasta olisi säädettävä henkilökorttilaissa.

EU:n ID-asetuksen johdantokappaleen 40 kohdan mukaan rekisteröidyillä olisi oltava pääsy henkilökorteissaan ja oleskeluasiakirjoissaan käsitelyihin henkilötietoihin ja mahdollisuus oikeista niistä siten, että myönnetään uusi asiakirja, jos kyseiset tiedot ovat virheellisiä tai puutteellisia. Kortinhaltijan oikeudesta tarkastaa teknisen osan sisältämät henkilötiedot ja tarvittaessa pyytää tietojen korjaamista tai poistamista säädetään henkilökorttilain 8 §:ssä.

Passi ja sen myöntäminen

Passilain 3 §:n mukaan matkustusoikeuden osoittamiseksi Suomen kansalaiselle myönnetään hakemuksesta passi, jollei laista muusta johdu. Passilain 5 §:ssä säädetään passin sisällöstä ja sen 1 momentin mukaan passiin merkitään hakijan sukunimi, etunimet, sukupuoli, syntymäaika ja henkilötunnus, kansalaisuus, syntymäkotikunta, passin myöntämispäivä ja viimeinen voimassaolopäivä, passin myöntänyt viranomainen ja passin numero. Passissa on lisäksi passinhaltijan kasvokuva ja nimikirjoitus. Kelpoisuusalueeltaan rajoitettuun passiin merkitään ne maat, joihin se oikeuttaa matkustamaan, tai ne maat, joihin passi ei oikeuta matkustaman. Syntymäkotikunnan sijaan merkitään ”ulkomaat”, jos hakijan syntymäkotikuntaa ei voida luotettavasti selvittää tai jos syntymäkotikunnan merkitseminen passiin todennäköisesti vaarantaisi passinhaltijan turvallisuutta. Passi on voimassa viisi vuotta sen myöntämispäivästä.

Passilain 5 a §:ssä säädetään passin teknisestä osasta ja tietojen tarkastamisesta. Sen 1 momentin mukaan 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. Pykälän 2 momentin mukaan tekniseen

osaan talletetaan passinhaltijan kasvokuva sekä 6 a §:ssä tarkoitetut sormenjäljet tarvittavine lisätietoineen siten kuin EU:n passiasetuksessa säädetään. Tekniseen osaan voidaan tallettaa myös 5 §:n 1 momentissa tarkoitetut tiedot. Passinhaltijan oikeudesta tarkastaa passin tekniseen osaan hänestä talletetut tiedot säädetään EU:n passiasetuksessa. Pykälän 3 momentin mukaan passin turvatekijöistä ja biometrisistä tunnisteista säädetään EU:n passiasetuksessa. Biometrisen tunnisteiden sisältävän passin kannessa on tätä osoittava tunnuskuva.

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. Passin tekniseen osaan talletettujen tietojen aitouden ja eheyden varmistamiseen liittyvät sekä sormenjälkien lukemisessa tarvittavat varmenteet luo Digi- ja väestötietovirasto. Ulkoasiainministeriö vastaa diplomaattipassin ja virkapassin sekä 10 §:ssä tarkoitetun ulkomaan edustuston myöntämän passin tekniseen osaan talletettujen tietojen suojaamisesta.

Passia haetaan poliisilta. Hakemus voidaan panna vireille sähköisesti. Hakijan tulee kuitenkin saapua henkilökohtaisesti viranomaisen luokse hakemuksen täydentämistä varten. Passilain 6 §:n 4 momentin mukaan passihakemukseen on liitettävä hakijan kasvokuva, josta hakija on hyvin tunnistettavissa. Hakijan on esitettävä tunnistamisasiakirjana voimassa oleva henkilöllisyysosoittava asiakirja. Jos hakijalla ei ole esittää tunnistamisasiakirjaa, passin myöntävä viranomainen suorittaa tunnistamisen. Sähköinen asiointi edellyttää tunnistus- ja luottamuspalvelulaissa tarkoitettua tunnistusvälinettä. Pykälän 5 momentin mukaan Poliisin myöntämistä henkilöllisyysosoittavista asiakirjoista säädetään tarkemmin valtioneuvoston asetuksella. Hakemukseen liitettävien kasvokuvien lukumäärästä sekä kasvokuvalle asetettavista vaatimuksista voidaan antaa tarkempia säännöksiä sisäministeriön asetuksella. Alaikäiselle myönnetään passi, jos hänen huoltajansa siihen suostuvat.

Mikäli hakija hakee uutta passia sähköisesti kuuden vuoden kuluessa aiemman passin tai henkilökortin myöntämisestä ja aiempaa passia tai henkilökorttilain 2 §:n 1 momentissa tarkoitettua varten on annettu sormenjäljet ja annettu nimikirjoitusnäyte, passia haettaessa ei 6 b §:n mukaan edellytetä hakijan henkilökohtaista läsnäoloa. Hakijalta ei tällöin oteta sormenjälkiä uutta passia varten. 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.

2.3 Vahva sähköinen tunnistaminen

Vahvassa sähköisessä tunnistamisessa on kyse henkilöllisyyden todentamisesta sähköisesti. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009, jäljempänä *tunnistus- ja luottamuspalvelulaki*) säädetään vahvan sähköisen tunnistamisen vaatimuksista ja tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille. Lain tarkoituksena on sääntelyn avulla pyrkiä edistämään vahvan sähköisen tunnistamisen markkinaehtoista kehittymistä. Lain keskeisenä tavoitteena on edistää sähköisen asioinnin ja palvelujen käytön turvallisuutta lisäämällä vahvan sähköisen tunnistamisen käyttöä. Vahvan sähköisen tunnistamisen avulla kuluttajat voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa ja sähköisten asiointipalveluiden tarjoajat voivat tunnistaa asiakkaansa. Liikenne- ja viestintävirasto valvoo tunnistus- ja luottamuspalvelulain noudattamista.

Tunnistus- ja luottamuspalvelulaki sisältää vahvan sähköisen tunnistamisen määritelmän sekä sitä koskevat tarkemmat vaatimukset. Nämä vaatimukset on yhdenmukaistettu sähköisestä tun-

nistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (jäljempänä *eIDAS-asetus*) kanssa. eIDAS-asetus koskee sähköisen tunnistamisen osalta jäsenvaltioiden ilmoittamia eli notifioituja sähköisen tunnistamisen järjestelmiä. Kansallinen tunnistusmenetelmä voidaan ilmoittaa EU:n komissiolle eIDAS-asetuksen mukaisesti. Ilmoitettua tunnistusmenetelmää on mahdollista käyttää muiden jäsenvaltioiden julkishallinnossa asioimiseen. Asetuksessa säädetään millaisia sähköisen tunnistamisen järjestelmiä jäsenvaltiot voivat ilmoittaa komissiolle, miten ilmoittaminen tapahtuu ja millaisia vaatimuksia ilmoitettaville tunnistamisjärjestelmille ja tunnistusmenetelmille on asetettu. Asetuksessa ja sen nojalla annetuissa täytäntöönpanosäädöksissä on määritelty tunnistuspalveluille kolme varmuustasoa: matala, korotettu ja korkea. Suomessa toimivilta vahvan sähköisen tunnistamisen järjestelmiltä vaaditaan vähintään samat luotettavuutta ja tietoturvaa koskevat vaatimukset kuin eIDAS-asetus täytäntöönpanosäädöksineen vaatii rajat ylittäviltä sähköisen tunnistamisen järjestelmiltä korotetulla varmuustasolla.

Tunnistus- ja luottamuspalvelulain mukaan vahvalla sähköisellä tunnistamisella tarkoitetaan henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteiden aitouden ja oikeellisuuden todentamista sellaista sähköistä menetelmää käyttäen, joka täyttää eIDAS-asetuksen korotetun tai korkean varmuustason vaatimukset. Kyse on siis henkilöllisyyden osoittamisesta sähköisesti vahvaa sähköistä tunnistusvälinettä käyttäen. Tunnistus- ja luottamuspalvelulain 2 §:n mukaan tunnistusvälineellä tarkoitetaan eIDAS-asetuksen 3 artiklan 2 kohdassa tarkoitettua sähköisen tunnistamisen menetelmää. eIDAS-asetuksessa käytetään tunnistusvälineen kanssa samassa merkityksessä sähköisen tunnistamisen menetelmän käsitettä.

Lain määritelmä on teknologianeutraali ja kuvaa mitä tahansa joko fyysisessä, sähköisessä tai tiedollisessa muodossa olevia asioita, jotka yhdessä muodostavat tunnistusvälineen. Vahva sähköinen tunnistusväline voi siis perustua teknisesti eri menetelmiin. Väline voi tarkoittaa esimerkiksi SIM-kortille tai muulle kortille sijoitettua varmennetta ja sen käyttämiseen tarvittavaa PIN-koodia, käyttäjätunnusta ja siihen yhdistettyä vaihtuvaa salasanaa, tai sormenjälkeä ja siihen yhdistettävää PIN-koodia. Suomessa nykyisin käytettäviä vahvoja sähköisiä tunnistusvälineitä ovat pankkien tarjoamat pankkitunnukset ja teleyritysten mobiilivarmenne sekä poliisin myöntämällä henkilökortilla oleva Digi- ja väestötietoviraston myöntämä kansalaisvarmenne ja Digi- ja väestötietoviraston myöntämät organisaatiokorteilla olevat organisaatiovarmenteet.

2.4 Vahvan sähköisen tunnistamisen luottamusverkosto ja markkina

Tunnistus- ja luottamuspalvelulaissa säädetään tunnistuspalvelun tarjoajien luottamusverkostosta. Vahvan sähköisen tunnistuspalvelun tarjoajien tulee ennen toimintansa aloittamista tehdä kirjallinen ilmoitus Liikenne- ja viestintävirastolle. Ilmoituksen tehneet tunnistuspalvelun tarjoajat muodostavat suoraan lain nojalla sähköisen tunnistamisen luottamusverkoston. Tunnistus- ja luottamuspalvelulaissa on säädetty niistä velvoitteista, jotka liittyvät tunnistuspalvelun tarjoajien toimintaan luottamusverkostossa, kuten toimijoiden välisistä keskeisistä tarjonta- ja yhteistyövelvoitteista, tunnistustapahtumista perittävistä enimmäishinnoista sekä velvollisuudesta arvioida tarjottavan tunnistusvälineen vaatimustenmukaisuus. Luottamusverkostoa koskevalla sääntelyllä on luotu sähköisen tunnistamisen markkinat asettamalla tunnistuspalvelun tarjoajien toiminnalle tietyt vaatimukset ja säätämällä niiden valvonnasta.

Luottamusverkostossa toimivat kahdenlaiset toimijat: tunnistusvälineiden tarjoajat ja tunnistusvälityspalvelun tarjoajat. Tunnistus- ja luottamuspalvelulaissa säädetään näitä toimijoita koskevista velvollisuuksista ja toiminnasta luottamusverkostossa. Tunnistusvälineen tarjoajat sekä

tunnistusvälityspalvelun tarjoajat ovat molemmat tunnistuspalvelun tarjoajia. Tunnistuspalvelun tarjoaja on siis näiden kahden käsitteen yläkäsite. Tunnistusvälineen tarjoajilla tarkoitetaan niitä toimijoita, jotka tarjoavat tunnistusvälineitä käyttäjille eli luonnollisille tai oikeushenkilöille. Suomessa tunnistusvälineen tarjoajia ovat pankit, teleyritykset ja Digi- ja väestötietovirasto. Tunnistusvälityspalvelun tarjoajilla tarkoitetaan puolestaan niitä tahoja, jotka välittävät tunnistustapahtumia sähköisille asiointipalveluille. Tunnistusvälityspalvelun tarjoajat tekevät sopimuksia tunnistusvälineiden tarjoajien kanssa siitä, että ne voivat välittää tunnistusvälineillä tehtäviä tunnistustapahtumia asiointipalveluille. Sama palveluntarjoaja voi halutessaan toimia sekä välineen että välityspalvelun tarjoajana.

Liikenne- ja viestintäviraston rekisterissä on tällä hetkellä 16 vahvan sähköisen tunnistuspalvelun tarjoajaa. Näistä omaa vahvaa sähköistä tunnistusvälinettä tarjoaa 14 toimijaa. Muidenkin kuin oman vahvan sähköisen tunnistusvälineen käyttäjien tunnistusta välittäviä tunnistuspalveluja on kahdeksan. Tunnistusvälityspalvelun tarjoajista kaksi tarjoaa pelkästään välityspalvelua eli ne eivät tarjoa omaa vahvaa sähköistä tunnistusvälinettä. Vahvan sähköisen tunnistusvälityspalvelun tarjoajista kuusi välittää sähköisille asiointipalveluille kaikkia Suomessa käytössä olevia tunnistusvälineitä pois lukien Digi- ja väestötietoviraston henkilö- ja organisaatiovarmenteita. Digi- ja väestötietovirasto toimii välityspalveluna oman tunnistusvälineensä osalta.

Tarkasteltaessa vahvojen sähköisten tunnistuspalvelujen markkinaa kokonaisuudessaan voidaan todeta, että tunnistusvälityspalvelun tarjoajien tulo markkinoille on merkittävästi muuttanut markkina-asetelmia ja välityspalveluiden markkinaosuus myynnistä asiointipalveluille on jo huomattava. Yksittäisen välityspalvelun markkinaosuuteen vaikuttaa paljon se, toimittaako välityspalvelu kilpailutuksen perusteella tunnistusta julkiselle sektorille. Digi- ja väestötietovirasto vastaa keskitetysti koko julkisen hallinnon vahvan sähköisen tunnistamisen hankkimisesta ja välittämisestä organisaatioiden käyttöön suomi.fi-tunnistuksen välityspalvelun kautta.

Sähköiset asiointipalvelut, kuten verkkokaupat ja julkishallinnon sähköiset palvelut, hankkivat vahvaa sähköistä tunnistamista asiointipalveluunsa keskitetysti luottamusverkostosta. Aiemmin haasteena on ollut, että sähköisten palveluiden tarjoajat eivät voineet hankkia eri tunnistusvälineitä käyttävien asiakkaiden tunnistusta kootusti ja tosiasiallisesti kilpailuttaa sähköisiä tunnistuspalveluja eivätkä siten voineet aktiivisesti hallita tunnistamispalveluiden hyödyntämisestä heille koituvia kustannuksia. Luottamusverkostosääntelyllä luotiin sähköisten palveluiden tarjoajille paremmat mahdollisuudet vaikuttaa ja hallita tunnistamisesta aiheutuvia kustannuksia. Luottamusverkostosääntelyn tarkoituksena on lisäksi luoda edellytyksiä uusien tunnistusvälineiden markkinoille tulolle ja uudentilaisille tunnistamiseen liittyville liiketoimintamahdollisuuksille. Samalla tarkoituksena on taata myös nykyisten tunnistusvälineiden käytön häiriötön jatkuminen.

Tunnistus- ja luottamuspalvelulaki ei nykyisin tunnista sellaista tilannetta, jossa vahvan sähköisen tunnistusvälineen tarjoaja tarjoaisi välinettä kuulumatta luottamusverkostoon tai että vahvaa sähköistä tunnistamista tarjotaan luottamusverkoston ulkopuolella. Tunnistuspalvelua on nykyisen lainsäädännön puitteissa mahdollista tarjota tekemättä ilmoitusta Liikenne- ja viestintävirastolle, mutta tällöin tunnistuspalvelun tarjoajalla ei ole vahvan sähköisen tunnistuspalvelun tarjoajan asemaa. Sillä ei myöskään ole todennettua näyttöä siitä, että se noudattaisi toiminnassaan samoja vaatimuksia, kuin luottamusverkostossa toimivat tunnistuspalvelun tarjoajat eikä se kuulu Liikenne- ja viestintäviraston valvonnan piiriin.

Tällä hetkellä merkittävä yksittäinen tunnistuspalvelujen ostaja on Digi- ja väestötietovirasto, joka välittää keskitetysti tunnistuspalveluja julkiselle hallinnolle Suomi.fi-tunnistuksen kautta. Jos jätetään huomiotta ne tunnistustapahtumat, joissa on kyse tunnistautumisesta tunnistusväli-

neen tarjoajan omiin palveluihin, mikä ei lukeudu vahvan sähköisen tunnistamisen lainsäädännön piiriin ja soveltamisalaan, niin arviolta noin 60–75 prosenttia tunnistustapahtumista kohdistuu julkisen hallinnon palveluihin Suomi.fi-tunnistuksen kautta. Digi- ja väestötietovirasto onkin merkittävä asiakas tunnistuspalvelujen tarjoajille. Julkisen sektorin toimijat ovat usein lainsäädännöllä velvoitettuja käyttämään vahvaa sähköistä tunnistamista sähköisissä asiointipalveluissaan, joissa käsitellään henkilötietoja tai muutoin salassa pidettävää tietoa.

Loput, arviolta noin 25–40 prosenttia tunnistustapahtumista kohdistuu yksityisen sektorin ja kolmannen sektorin toimijoiden tarjoamiin sähköisiin asiointipalveluihin. Useaan yksityisen sektorin toimijaan kohdistuu velvoite tunnistaa asiakkaansa vahvasti, minkä seurauksena ne ovat ottaneet vahvan sähköisen tunnistamisen käyttöön tarjoamissaan sähköisissä asiointipalveluissa. Merkittävin vahvan sähköisen tunnistamisen käyttöalue liittyy yksityisellä sektorilla verkkopankissa asiointiin ja maksamiseen. Muualla yksityisellä sektorilla asiakkaiden tunnistamisessa vahvaa sähköistä tunnistamista käyttävät muun muassa apteekit, lääkäriasemat ja muut terveydenhuoltopalveluja tarjoavat yritykset, vakuutusyhtiöt, teleyritykset, sähköyritykset, postipalveluyritykset ja matkustuspalveluja tarjoavat yritykset. Yksityisen sektorin ja kolmannen sektorin sähköisissä asiointipalveluissa vahvan sähköisen tunnistamisen käyttö on kuitenkin vielä kehitysvaiheessa ja suurimmassa osassa palveluja ei ole käytössä vahvaa sähköistä tunnistusta. Vahvojen sähköisten tunnistuspalvelujen kasvupotentiaali yksityisten ja kolmannen sektorin sähköisissä asiointipalveluissa on siten suuri.

Suomi.fi -tunnistamisen kautta vahvalla sähköisellä tunnistusvälineellä julkisen hallinnon palveluihin tehtyjen tunnistustapahtumien määrä on kasvanut nopeasti. Vuonna 2017 Suomi.fi -tunnistamisen kautta tunnistauduttiin noin 55 miljoonaa kertaa, kun vuonna 2018 tunnistauduttiin jo noin 82 miljoonaa ja vuonna 2019 107 miljoonaa kertaa. Nopeaa kehitystä selittää se, että julkisen hallinnon palveluita on siirretty vuosina 2017–2019 nopeaa vauhtia sähköisesti saataville ja palveluiden käyttämisessä on vaadittu asiakkaan vahvaa sähköistä tunnistamista. Nopea kasvuvauhti on kuitenkin tasaantunut ja, kun vuonna 2018 vuotuinen tunnistustapahtumamäärän kasvu oli noin 50 prosenttia edellisvuoteen verrattuna, vuonna 2019 kasvu oli enää 31 prosenttia. Vastaavaa kattavaa aineistoa tunnistusvälineiden käytöstä yksityisissä sähköisissä asiointipalveluissa ei ole tietojen hajanaisuuden ja liikesalaisen luonteen vuoksi käytössä.

On odotettavissa, että julkisen hallinnon palveluihin tehtyjen tunnistustapahtumien määrän kasvu tulee edelleen tasaantumaan, ja vuosina 2021 ja 2022 vuotuinen kasvu tulisi syksyllä 2021 tehtyjen arvioiden mukaan olemaan noin 20 prosenttia. Tämän jälkeen kasvun oletetaan tasaantuvan entisestään. Korona toi vuonna 2020 odotettua suuremman hyppäyksen, noin 36 prosentin lisäyksen edelliseen vuoteen, mutta vuoden 2020 tapahtumamäärien oletetaan määrittelevän tapahtumille uuden tason tulevina vuosina. Suurimmat julkisen sektorin toimijat ovat pääosin sähköistäneet palvelunsa, joten merkittäviä hyppäyksiä ei ole enää odotettavissa, mutta käyttäjien siirtymä tuo kasvua vielä muutaman vuoden. Tämän jälkeen tunnistustapahtumamäärien odotetaan tasaantuvan noin 10 prosentin vuosikasvuvauhdin tasolle.

2.5 Digi- ja väestötietoviraston varmennepalvelut

Digi- ja väestötietoviraston varmennepalveluista säädetään laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009, jäljempänä *VTJ-laki*), tarkemmin sen 6 luvussa. Lain 61 §:ssä säädetään varmennetun sähköisen asioinnin palveluista ja sen 1 momentin mukaan Digi- ja väestötietoviraston tehtävänä on tuottaa, tarjota ja hallinnoida varmennetussa sähköisessä asiointissa käytettäväksi tarkoitettu kansalaisvarmenne sekä sen käyttöön välittömästi liittyvät varmennehakemisto- ja sulkulistapalvelut. VTJ-lain 61 §:n 2 momentin mukaan Digi- ja väestötietovirasto voi lisäksi tuottaa varmennetussa sähköisessä asiointissa käytettäväksi seuraavat palvelut: 1) muun varmenteen kuin kansalaisvarmenteen tarjoaminen ja

hallinnointi; 2) varmennetun sähköisen asioinnin osapuolten todentaminen ja asioinnin hallinnointi; 3) sähköisten asiakirjojen ja viestien sähköinen allekirjoittaminen ja salaaminen; 4) sähköisen asiakirjojen ja viestien aitouden, luottamuksellisuuden ja eheyden säilyttäminen ja varmentaminen; 5) varmennetun sähköisen asiointitapahtuman toimijoiden aseman tai roolin varmentaminen; 6) muun varmenteen kuin kansalaisvarmenteen käyttöön liittyvien varmennehakemisto- ja sulkulistapalveluiden tarjoaminen ja hallinnointi; 7) varmennetun aikaleimapalvelun tarjoaminen ja hallinnointi; 8) muu vastaava varmennetun sähköisen asioinnin toiminto tai palvelu.

Kansalaisvarmenteella tarkoitetaan Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämää varmennetta, joka sisältyy henkilökorttilaissa 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 Digi- ja väestötietoviraston myöntämää varmennetta, jota käytetään edellä mainittuun tarkoitukseen ja joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetyt vaatimukset. Kansalaisvarmenteessa on varmenteen haltijan yksilöivänä tunnistetietona sähköinen asiointitunnus tai muu sellainen henkilön yksilöivä tunnistetieto, joka ei sisällä henkilöön liittyviä tietoja. Kansalaisvarmenteeseen ja muuhun Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämään varmenteeseen voi sisältyä myös muita varmenteen käytössä tarvittavia välttämättömiä teknisiä tietoja. Digi- ja väestötietovirasto päättää näistä tiedoista. Henkilökorttiin sisältyvän kansalaisvarmenteen hakemiseen sovelletaan henkilökorttilakia.

Kun henkilön tiedot talletetaan ensimmäisen kerran väestötietojärjestelmään, hänelle on annettava sähköisen asiointitunnuksen antamisessa tarvittava yksilöllinen tekninen tunnistetieto. Tekninen tunnistetieto annetaan automaattisesti väestötietojärjestelmästä. 63 §:n pykälän 2 momentin mukaan Digi- ja väestötietovirasto muuttaa teknisen tunnistetiedon yksilölliseksi sähköiseksi asiointitunnukseksi, kun 1) henkilölle myönnetään ensimmäisen kerran kansalaisvarmenne tai muu Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä varmenne; tai 2) henkilöllä, jonka tiedot on tallennettu väestötietojärjestelmään, ei ole sähköistä asiointitunnusta ja Digi- ja väestötietovirasto saa 43 §:n 2 momentin 2 kohdassa tarkoitetulta varmentajalta pyynnön muuttaa tämän henkilön tekninen tunnistetieto sähköiseksi asiointitunnukseksi.

Kansalaisvarmenteet ja muut Digi- ja väestötietoviraston myöntämät yleisesti sähköisessä asiointissa käytettävät luonnollisen henkilön varmenteet sekä niihin sisältyvät tiedot voidaan tallettaa Digi- ja väestötietoviraston pitämään julkiseen hakemistoon, josta jokaisella on oikeus saada tietoja siten kuin viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999, jäljempänä *julkisuuslaki*) säädetään viranomaisen julkisesta asiakirjasta.

2.6 Sähköinen tunnistautuminen julkishallinnon palveluihin

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 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.

Digipalvelulaissa säädetyn perusteella kaikki asian vireillepanot ja asiankäsitteilyn 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. Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) osaltaan menettelysäännöstensä kautta tukee digitaalisten palvelujen järjestämistä ja asiointia viranomaisissa.

Vahvan sähköisen tunnistamisen käyttövelvoitteesta julkisen hallinnon osalta säädetään digipalvelulain 6 §:ssä, jonka mukaan 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 perustelusta syystä hyödyntää muuta vastaavaa tietoturvallista tunnistuspalvelua.

Hallituksen esityksessä eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta (HE 60/2018 vp) on tarkennettu tilanteita, jossa tulisi vaatia vahvaa sähköistä tunnistusta. Esitöiden mukaan digipalvelulain nojalla viranomaisen arvioitavaksi jää tapauskohtaisesti tunnistamisen vaatimus asiointipalveluissaan. Viranomaisen 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 tunnistus- ja luottamuspalvelulain 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 tunnistus- ja luottamuspalvelulain mukaista vahvaa sähköistä tunnistamista.

Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016, jäljempänä *tukipalvelulaki*) tarkoituksena on parantaa julkisten palvelujen saatavuutta, laatua, tietoturvallisuutta, 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 (esim. viranomaisena) käyttää asiointipalvelunsa tai muun sille 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. Tukipalvelutuotanto on joitain poikkeuksia lukuun ottamatta keskitetty Digi- ja väestötietovirastoon.

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 tunnistus- ja luottamuspalvelulaissa tarkoitettun 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.

2.7 Komission ehdotus eIDAS-asetuksen muuttamiseksi

Komissio on antanut kesäkuussa 2021 lainsäädäntöehdotuksen Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehiksen vahvistamisen osalta (COM (2021) 281 final). Kyse on siis edellä kohdassa 2.3 tarkemmin selostetusta eIDAS-asetusta koskevasta muutosehdotuksesta (myöhemmin *eIDAS-muutosehdotus*). Ehdotuksessa luodaan yhteinen lainsäädäntökehikko eurooppalaiselle digitaalisen identiteetin lompakkosovellukselle. Ehdotuksella halutaan erityisesti varmistaa luotettavien ja turvallisten digitaalisten identiteettiratkaisujen saatavuus kaikille EU:ssa. Tavoitteena on lisäksi, että julkisen ja yksityisen sektorin palveluntarjoajat voivat luottaa kehitettäviin digitaalisiin identiteettiratkaisuihin, kun käyttäjät asioivat ja tunnistautuvat heidän palveluihinsa.

eIDAS-muutosehdotuksessa luodaan yhteinen lainsäädäntökehikko eurooppalaiselle digitaalisen identiteetin lompakkosovellukselle. Tämä on muutosehdotuksen keskeisin uudistus. Lompakkosovelluksen yksi keskeisimmistä toiminnallisuuksista olisi mahdollistaa sovelluksen käyttäjälle sähköinen tunnistautuminen. Lisäksi lompakkosovelluksen käyttäjä voisi osoittaa itseään koskevia henkilötietoja ja todistuksia sekä tehdä sähköisiä allekirjoituksia. Kaikilla jäsenvaltioilla olisi ehdotuksen mukaan velvollisuus tarjota vähintään yksi asetuksen mukainen lompakkosovellus. Lompakkosovellus voisi olla julkisen tai yksityisen sektorin tuottama. Lompakkosovelluksen käyttö olisi kansalaisille ilmaista ja vapaaehtoista. Lompakkosovellusta tulisi ehdotuksen mukaan voida käyttää mahdollisimman laajasti yhteiskunnan palveluissa niin julkisella kuin yksityisellä sektorilla.

eIDAS-muutosehdotus sisältää myös yhteiset vaatimukset sellaisille luottamuspalveluille, joilla mahdollistetaan henkilötietojen ja todistusten tarjoaminen sähköisessä muodossa (asetusehdotuksen mukaan sähköiset attribuuttitodistukset). Organisaatiot ja tahot voisivat tarjota myöntämänsä henkilötiedot ja todistukset (kuten tutkintotodistukset ja lisenssit) luottamuspalveluna sähköisesti käyttäjän lompakkosovellukseen. Asetus määritteli vaatimukset tarjottavalle palvelulle eli sähköisille attribuuttitodistuksille sekä palveluntarjoajalle. Tarjoamalla palveluitaan asetuksen vaatimusten mukaisesti palveluntarjoaja voi osoittaa, että sen tarjoama palvelu on

luotettava. Luotettavuuden lisäämiseksi luottamuspalveluiden tarjoajan on mahdollista hakea palvelulleen viranomaishyväksyntää.

Komission edotuksesta on laadittu eduskunnalle U-kirjelmä, joka sisältää Suomen kannan (U 41/2021 vp, https://www.eduskunta.fi/FI/vaski/Kirjelma/Documents/U_41+2021.pdf). Komission ehdotuksen käsittely on aloitettu EU:n neuvoston teletyöryhmässä.

Kun eIDAS-muutosehdotuksen käsittely saadaan aikanaan päätökseen, tulee kansallisesti arvioitavaksi, halutaanko kansallisen lainsäädännön yhdenmukaistamista eIDAS-asetuksen vaatimusten kanssa edelleen jatkaa. Nykyisin kansalliset vahvan sähköisen tunnistamisen vaatimukset on haluttu yhdenmukaistaa eIDAS-asetuksen vaatimusten kanssa, kuten on kuvattu edellä tarkemmin kohdassa 2.3. Joka tapauksessa digitaalisen henkilöllisyyden ja sähköisen asioinnin maailma on myös kansallisesti kehittymässä suuntaan, jossa henkilö itse kontrolloi häneen liittyvien tietojen jakamista kolmansille osapuolille uudenlaisten identiteetin hallintaan liittyvien ratkaisujen avulla. eIDAS-asetusta koskevan lainsäädäntöehdotuksen perusteella EU:ssa tällaiseksi ratkaisuksi ollaan kehittämässä eurooppalaista digitaalisen identiteetin lompakkosovellusta. Kuten edellä on kuvattu, on mahdollista, että eIDAS-asetus tulee tulevaisuudessa velvoittamaan jäsenvaltioita asetuksen mukaisten lompakkosovellusten tarjoamiseen.

Tavoitteet eIDAS-muutosehdotuksen käsittelyaikataulusta ovat kunnianhimoisia ja tässä vaiheessa asetuksen voimaantulon aikataulu on vielä epävarmaa. Uudenlaisten digitaalisen henkilöllisyyden ratkaisujen kehittäminen ja saatavuus kansallisella tasolla on kuitenkin tärkeää jo tällä hetkellä. Kansallisen tason kehitystyön etenemisen ei tulisi olla täysin sidottua EU-valmisteluun. Tästä huolimatta on kuitenkin erittäin tärkeää kiinnittää kansallisella tasolla huomiota myös EU:n tasolla tapahtuvaan kehitystyöhön, jotta välttäisi päällekkäiseltä kehitystyöltä ja kustannuksilta. Kansallisella tasolla tapahtuvan kehitystyön tulee joka tapauksessa olla jo tässä vaiheessa mahdollisimman yhdenmukaista tulevan eIDAS-sääntelyn kanssa ja luoda edellytyksiä toteuttaa tulevaisuudessa myös eIDAS-asetuksen vaatimukset täyttäviä lompakkosovelluksia.

3 Tavoitteet

Esityksen tavoitteena on edistää pääministeri Marinin hallitusohjelmassa asetettua tavoitetta, jonka mukaan 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. Esityksen tavoitteena on lisäksi hallitusohjelman mukaisesti edistää Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen sekä edistää toimivien tunnistusratkaisujen kehittymistä. Tavoitetta edistettäisiin mahdollistamalla lainsäädännössä Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluiden sekä laajasti yhteiskunnan palveluissa käytettävän Poliisin tarjoaman digitaalisen henkilöllisyystodistuksen tuottaminen.

Esityksellä edistetään myös henkilön mahdollisuuksia hallita omia julkisissa palveluissa olevia tietojaan (ns. itsehallittava identiteetti, Self-sovereign identity), mikä on myös kirjattu hallitusohjelmaan. Tavoitteena on ensivaiheessa mahdollistaa tiettyjen henkilöllisyyttä koskevien tietojen esittäminen henkilön itsensä toimesta sekä luoda perusratkaisut ja käytännöt itsehallittavien viranomaistietojen esittämiseksi, jotta kehitystä voidaan viedä eteenpäin tulevaisuudessa.

Esityksen keskeisenä tavoitteena on lisäksi mahdollistaa tunnistautuminen sähköisiin asiointipalveluihin yhdenvertaisesti myös ulkomaalaisille. Lisäämällä Digi- ja väestötietoviraston teh-

täväksi myös ulkomaalaisen digitaalisen asiointivälineen tuottaminen ja luomalla asiointivälineen hyödyntämiselle lainsäädännölliset edellytykset pyritään parantamaan ulkomaalaisten mahdollisuutta asioida suomalaisissa sähköisissä asiointipalveluissa. Lisäksi esityksen tavoitteena on edistää mahdollisuutta sähköiseen asiointiin myös henkilöille, jotka eivät joko voi tai halua käyttää älypuhelinia. Esityksen tavoitteena on lisäksi varmistaa julkisen hallinnon vahvan sähköisen tunnistamisen kustannusten ennakoitavuus.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Yleisesti

Esityksessä ehdotetaan uutta lainsäädäntöä koskien uusia viranomaisen tuottamia digitaalisen asiointin palveluita, sekä näiden tuottamiseen ja käyttöön liittyvää toiminnallista muutosta. Esityksessä ehdotetaan tuotettavaksi digitaalinen henkilöllisyystodistus, ulkomaalaisen digitaalinen asiointiväline ja luonnollisen henkilön tunnistusväline. Ne olisivat uusia henkilöllisyyden ja henkilötietojen osoittamiseen sekä sähköiseen tunnistamiseen tarkoitettuja ratkaisuja luonnollisille henkilöille. Niiden tarkoituksena on varmistaa, että suomalaisen yhteiskunnan palveluissa asioivilla henkilöillä olisi laajasti mahdollisuus esittää viranomaisen vahvistama henkilöllisyys sekä henkilöllisyyteen liittyviä vahvistettuja tietoja erilaisissa asiointitilanteissa.

Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen osalta kyse olisi myös kehityksestä, joka mahdollistaa henkilön itsensä valita esitettävät henkilötiedot kohti itsehallittavaa henkilötietojen esittämistä. Henkilön omien tietojen toimittamista digitaalisessa ympäristössä henkilön itsensä hallittavaksi kutsutaan yleisesti itsehallittavaksi identiteetiksi. Itsehallittavalla identiteetillä (engl. Self-Sovereign Identity, SSI) tarkoitetaan henkilötietojen käsittelyn mallia, jossa henkilö voi itse hallinnoida joko itseltään tai luotettavalta kolmannelta taholta lähtöisin olevien henkilötietojensa osoittamista asiointipalvelulle, jossa henkilötietoja tarvitaan. Käytännössä itsehallittavuudella tarkoitetaan siis sitä, että henkilöt hallitsevat itse omia henkilötietojaan eli päättävät itse niiden käytöstä. Tässä vaiheessa itsehallittavat henkilötiedot kuitenkin rajautuisivat niihin tietoihin, jotka ovat johdettavissa digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen perustana olevista henkilöllisyyttä osoittavista asiakirjoista.

Digitaalisen henkilöllisyyden palvelut ja ydinidentiteetin todiste

Esityksessä ehdotetaan säädettäväksi uusi laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista. Ehdotetun lainsäädännön mukaan Digi- ja väestötietoviraston tehtävänä olisi jatkossa tuottaa digitaalisen henkilöllisyyden tietojärjestelmää, joka koostuisi digitaalisen henkilöllisyyden sovelluksesta ja siihen liittyvästä taustajärjestelmästä. Kyse olisi käytännössä Digi- ja väestötietoviraston tehtävästä tuottaa henkilön mobiilipäätelaitteeseen ladattavaa sovellusta, jonka avulla on mahdollista käyttää digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä. Digi- ja väestötietoviraston tuottama sovellus toimisi teknisenä pohjana digitaaliselle henkilöllisyystodistukselle ja ulkomaalaisen digitaaliselle asiointivälineelle. Laki sisältäisi säännökset digitaalisen henkilöllisyyden tietojärjestelmän olennaisista tietoturva vaatimuksista ja edellyttäisi tietojärjestelmän säännöllistä tietoturvallisuuden arviointilaitoksen tekemää arviointia. Laissa säädettäisiin lisäksi siitä, että tietojärjestelmän tulisi täyttää samat vaatimukset, kuin mitä edellytetään nykyisin vahvoilta sähköisiltä tunnistusvälineiltä.

Esityksessä ehdotetaan lisäksi, että Digi- ja väestötietoviraston tehtävänä olisi tuottaa ydinidentiteetin todisteita. Ydinidentiteetin todiste olisi ehdotetun lainsäädäntökokonaisuuden keskeinen osa, sillä voimassa oleva ydinidentiteetin todiste olisi edellytys digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen asiointivälineen käytölle. Ydinidentiteetin todiste toimisi teknisesti luotettavana tapana osoittaa sähköisesti, että todisteen haltijalla on olemassa väestötietojärjestelmään rekisteröity henkilöllisyys. Toisin sanoen kyseessä olisi vahvistettu ja teknisesti tarkistettavissa oleva tieto siitä, että henkilöllä on Suomessa rekisteröity ja edelleen olemassa oleva identiteetti. Käytännössä ydinidentiteetin todiste olisi ensivaiheessa varmenne. Digi- ja väestötietovirasto muodostaisi, myöntäisi ja rekisteröisi ydinidentiteetin todisteen, kun henkilö ottaa käyttöön digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen.

Digitaalinen henkilöllisyystodistus

Esityksessä ehdotetaan säädettäväksi uusi laki, jossa säädettäisiin digitaalisesta henkilöllisyystodistuksesta. Digitaalinen henkilöllisyystodistus mahdollistaisi haltijalleen henkilöllisyyden sekä tiettyjen häneen liittyvien vahvistettujen tietojen osoittamisen. Kyse olisi niistä vahvistetuista tiedoista, jotka ovat johdettavissa digitaalisen henkilöllisyystodistuksen perustana olevasta henkilöllisyyttä osoittavasta asiakirjasta eli käytännössä henkilön voimassaolevan passin tai henkilökortin tiedoista. Digitaalinen henkilöllisyystodistus ei kuitenkaan toimisi matkustusasiakirjana. Esityksessä ehdotetaan, että digitaalisen henkilöllisyystodistuksen toimintaperiaate perustuisi itsehallittavaan henkilötietojen esittämiseen. Tällä tarkoitetaan sitä, että henkilö voisi itse päättää kenelle hän haluaa osoittaa digitaalisen henkilöllisyystodistuksen sisältämiä tietojaan ja mitä tietoja hän haluaa osoittaa. Viranomaisella ei olisi mahdollisuutta määrätä tietojen osoittamisesta eikä viranomaisella olisi pääsyä digitaalisen henkilöllisyystodistuksen tietoihin.

Esityksessä ehdotetun lainsäädännön mukaan henkilöllä olisi suoraan voimassaolevan henkilökortin tai passin nojalla oikeus digitaaliseen henkilöllisyystodistukseen. Oikeutta ei kuitenkaan syntyisi väliaikaisen henkilökortin, alle 15-vuotiaalle myönnetyn alaikäisen henkilökortin, väliaikaisen passin tai hätäpassin perusteella. Esityksessä ehdotetaan, että henkilökorttilakiin ja passilakiin otettaisiin nimenomaiset säännökset siitä, minkä henkilöllisyyttä osoittavien asiakirjojen perusteella oikeus digitaaliseen henkilöllisyystodistukseen syntyy. Digitaalisessa henkilöllisyystodistuksessa ei näin ollen olisi kyse uudesta lupatyypistä eikä sitä myönnettäisi erikseen, vaan oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon syntyisi suoraan voimassaolevan henkilökortin tai passin perusteella. Vaikka henkilöllä olisi oikeus digitaaliseen henkilöllisyystodistukseen olisi sen varsinainen käyttöönotto kuitenkin täysin vapaaehtoista. Digitaalisen henkilöllisyystodistuksen käyttöönotto olisi maksutonta.

Esityksessä ehdotetun lainsäädännön mukaan digitaalista henkilöllisyystodistusta voitaisiin käyttää henkilöllisyyden osoittamiseen käyntiasioinnissa eli asioitaessa kasvokkain jonkin palveluntarjoajan luona samalla tavoin kuin nykyisin käytetään henkilökorttia ja passia. Lisäksi digitaalista henkilöllisyystodistusta voisi käyttää sähköisessä asioinnissa henkilöllisyyden osoittamiseen vastaavasti kuin nykyisiä vahvoja sähköisiä tunnistusvälineitä käytetään. Tämän mahdollistamiseksi esityksessä ehdotetaan muutoksia tunnistus- ja luottamuspalvelulakiin, jossa muutettaisiin vahvan sähköisen tunnistamisen määritelmää niin, että myös digitaalisella henkilöllisyystodistuksella tapahtuva sähköinen tunnistaminen kuuluisi määritelmän piiriin. Näin digitaalisella henkilöllisyystodistuksella tapahtuva sähköinen tunnistaminen saisi vastaavan vahvan sähköisen tunnistamisen aseman, kuin nykyisillä vahvoilla sähköisillä tunnistusvälineillä on.

Esityksessä ehdotetaan lisäksi, että tunnistus- ja luottamuspalvelulaissa säädettäisiin jatkossa uudesta digitaalisen henkilöllisyyden palvelujen tarjoajan roolista ja tämän velvollisuudesta tarjota digitaalista henkilöllisyystodistusta luottamusverkostossa välitettäväksi. Käytännössä tunnistus- ja luottamuspalvelulain tarkoittama digitaalisen henkilöllisyyden palvelujen tarjoaja olisi Digi- ja väestötietovirasto. Sääntelyllä mahdollistettaisiin digitaalisen henkilöllisyystodistuksen käyttäminen vahvaan sähköiseen tunnistamiseen yksityisen sektorin sähköisissä asiointipalveluissa luottamusverkoston välityksellä sekä sen hyödyntäminen nykyisten tunnistusvälineiden tarjoajien tekemässä tunnistusvälineen hakijan niin kutsutussa ensitunnistamisessa. Ehdotetun lainsäädännön mukaan digitaalisen henkilöllisyyden palvelujen tarjoaja ei kuitenkaan tulisi luottamusverkoston osapuoleksi ja tunnistus- ja luottamuspalvelulakia sovellettaisiin digitaalisen henkilöllisyyden palvelujen tarjoajaan vain niiltä osin, kuin siitä olisi nimenomaisesti säädetty.

Ulkomaalaisen digitaalinen asiointiväline

Esityksessä ehdotetaan säädettäväksi uudesta ulkomaalaisen digitaalisesta asiointivälineestä. Asiointiväline mahdollistaisi haltijalleen henkilöllisyyden sekä tiettyjen muiden vahvistettujen tietojen osoittamisen. Kyse olisi niistä tiedoista, jotka voidaan johtaa asiointivälineen perustana olevasta ulkomaisesta henkilöllisyysasiakirjasta sekä ulkomaalaiselle rekisteröidystä suomalaisesta henkilötunnuksesta. Esityksessä ehdotetaan, että digitaalista henkilöllisyystodistusta vastaavalla tavalla myös ulkomaalaisen digitaalisen asiointivälineen toimintaperiaate perustuisi itsehallittavaan henkilötietojen esittämiseen. Asiointivälinettä voisi kuitenkin käyttää vain sähköisessä asiointissa, sillä asiointivälineeseen ei olisi mahdollista viedä sen haltijasta kasvokuvaa, joka on edellytys kasvokkain tapahtuvan asioinnin luotettavuudelle. Asiointiväline kuitenkin edistäisi ulkomaalaisten mahdollisuutta asioida sähköisesti ja ehkäisisi rinnakkaisten henkilöllisyyksien muodostumista viranomaisrekistereissä.

Esityksen ehdotusten mukaan ulkomaalaisen digitaalisen asiointivälineen myöntäisi Digi- ja väestötietovirasto. Asiointivälineen myöntäminen edellyttäisi henkilön rekisteröintiä väestötietojärjestelmään siten, että menettelyn yhteydessä ulkomaan kansalaiselle myönnetään henkilötunnus. Tässä kohtaa tämän esityksen ehdotukset ovat kytköksissä henkilötunnuksen uudistamista koskevan esityksen ehdotusten kanssa, sillä niiden myötä henkilötunnuksen myöntäminen ulkomaan kansalaiselle olisi mahdollista entistä laajemmalle henkilökoukulle. Lisäksi henkilötunnus voitaisiin myöntää etärekisteröintimenettelyssä ilman, että ulkomaan kansalainen saapuu Suomeen. Myös ulkomaalaisen digitaalinen asiointiväline voitaisiin ottaa käyttöön etärekisteröintimenettelyn yhteydessä. Ulkomaalaisen digitaalinen asiointiväline olisi maksullinen siten, että sen käyttöönottoon sisältyisi viranomaismaksu. Tämän jälkeen asiointivälineen käyttö olisi kuitenkin maksutonta.

Ulkomaalaisen digitaalinen asiointivälineitä voisi esityksen ehdotusten mukaan olla kahdenlaisia riippuen siitä, miten asiointivälineen haltija on asiointivälinettä myönnettäessä tunnistettu. Etärekisteröintimenettely ei ylittäisi luotettavuudeltaan samalle tasolle kuin kasvokkain tapahtuva henkilön tunnistaminen ja tästä syystä pelkästään etärekisteröinnin perusteella myönnetty asiointiväline kelpaisi sähköiseen asiointiin vain silloin, kun lainsäädännössä ei edellytetä vahvaa sähköistä tunnistamista. Toisin sanoen pelkästään etärekisteröinnin perusteella myönnetty asiointiväline ei vastaisi luotettavuudeltaan vahvaa sähköistä tunnistusvälinettä. Ehdotusten mukaan olisi asiointipalveluiden itse määritettävissä, mihin palveluihin ne voisivat hyväksyä tunnistautumisen asiointivälineellä, joka on luotettavuudeltaan vahvaa sähköistä tunnistamista matalampi.

Ulkomaalaisen digitaalinen asiointiväline voisi kuitenkin saavuttaa luotettavuudeltaan vahvaa sähköistä tunnistamista vastaavan tason silloin, kun henkilö on jossakin vaiheessa tunnistettu kasvokkain. Ulkomaalainen saattaisi esimerkiksi myöhemmin saapua Suomeen, jolloin hän voisi asioida Digi- ja väestötietovirastossa, jolloin hänet voitaisiin tunnistaa. Kasvokkain tunnistamisen jälkeen ulkomaalaisen digitaalista asiointivälinettä voitaisiin käyttää sähköisessä asiointissa myös silloin, kun edellytetään vahvan sähköisen tunnistamisen käyttöä. Tämän mahdollistamiseksi esityksessä ehdotetaan vastaavia muutoksia tunnistus- ja luottamuspalvelulakiin, kuin digitaalisen henkilöllisyystodistuksen osalta. Muutoksilla vahvistettaisiin näissä tilanteissa ulkomaalaisen digitaalisen asiointivälineen asema vahvassa sähköisessä tunnistamisessa sekä mahdollistettaisiin sen välittäminen luottamusverkostossa.

Luonnollisen henkilön tunnistusväline

Esityksessä ehdotetaan lisäksi säädettävän luonnollisen henkilön tunnistusvälineestä. Luonnollisen henkilön tunnistusväline voitaisiin myöntää henkilölle vastaavilla edellytyksillä, kuin nykyisiä vahvoja sähköisiä tunnistusvälineitä myönnetään. Luonnollisen henkilön tunnistusväline vastaisi myös toiminnallisuuksiltaan ja luotettavuudeltaan nykyisiä vahvoja sähköisiä tunnistusvälineitä. Luonnollisen henkilön tunnistusvälineen käyttöönotto olisi maksullista, mutta tämän jälkeen sen käyttö olisi maksutonta.

Luonnollisen henkilön tunnistusväline olisi tarkoitettu sellaisille henkilöille, joilla ei ole mahdollisuutta tai halua käyttää digitaalista henkilöllisyystodistusta sen vuoksi, että se toimii älypuhelimessa olevan mobiilisovelluksen avulla. Luonnollisen henkilön tunnistusväline olisi käytettävissä ainoastaan tukipalvelulain mukaisesti ja se mahdollistaisi sähköisen tunnistautumisen viranomaisten sähköisiin palveluihin. Näin tunnistusväline mahdollistaisi jokaiselle julkisen sektorin sähköisten palvelujen käytön. Tunnistusvälinettä ei kuitenkaan tarjottaisi tunnistusvälineeksi luottamusverkostoon eikä sillä siten olisi mahdollista tunnistautua yksityisen sektorin sähköisiin asiointipalveluihin.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

4.2.1.1 Vaikutukset kotitalouksiin

Ehdotuksilla arvioidaan olevan jonkin verran vaikutuksia kotitalouksien taloudelliseen asemaan, mutta näitä voidaan pitää henkilötasolla maltillisina. Digitaalisen henkilöllisyystodistuksen tai luonnollisen henkilön tunnistusvälineen saamisen ehtona oleva voimassa oleva passi tai henkilökortti on maksullinen viranomaisen myöntämä asiakirja. Digitaalisen henkilöllisyystodistuksen osalta kyse on näihin asiakirjoihin liittyvästä lisäpalvelusta. Voimassa oleva passi tai henkilökortti on tällä hetkellä noin 4,1 miljoonalla suomalaisella, ja näistä alaikäisiä on noin 580 000. Passeja ja henkilökortteja myönnetään vuosittain yhteensä noin 1,1 miljoonaa kappaletta, ja yhteensä voimassa olevia passeja ja henkilökortteja on noin 4,8 miljoonaa kappaletta. Ehdotuksella olisi siten vaikutuksia varsin laajaan joukkoon suomalaisia. Lukumäärien taustalla on huomattava, että esimerkiksi verkkopankin käyttämiseen tarvittavien pankkitunnusten saaminen ilman passia tai henkilökorttia ei ole ollut mahdollista vuoden 2019 alusta voimaantulleen vahvaa sähköistä tunnistamista koskevan lain muutosten myötä.

Digitaalisen henkilöllisyystodistuksen ja sen tuottamiseen liittyvät kustannukset ehdotetaan liittäväksi osittain osaksi passin ja henkilökortin kustannuksia valtion maksuperustelain mukai-

sesti. Digitaalisen henkilöllisyystodistuksen kustannukset lisäävät passin ja henkilökortin tuottamisen kiinteitä kuluja noin 3 euroa myönnettyä asiakirjaa kohti (arvioitu 1,1 miljoonalla vuosittain myönnettyllä asiakirjalla). Ehdotuksella olisi näin ollen mahdollisesti vaikutuksia passin ja henkilökortin hintaan. Passin ja henkilökortin hinta vaihtelee vuosittain myöntömäärien perusteella, joten ehdotusten lopullinen vaikutus kansalaiselle riippuu myös muista tekijöistä. Passin hinta on 44–50 euroa ja henkilökortin hinta 54–60 euroa vuonna 2022. Molempien asiakirjojen hinta on edullisempi sähköisellä hakemuksella. Ehdotuksen myötä passin tai henkilökortin hintaan kohdistuisi maltillinen korotuspaine. Passin ja henkilökortin viranomaiskustannusten lisäksi kustannuksina tulee huomioida myös valokuvan hinta (noin 0–20 euroa). Tästä näkökulmasta ehdotuksen taloudelliset vaikutukset kotitalouksiin ovat varsin maltillisia.

Passin tai henkilökortin voi saada toimeentulotuen yhteydessä maksusitoumuksella tietyin ehdoin. Pienituloisille, jotka eivät ole oikeutettuja toimeentulotukeen, passin tai henkilökortin maksuista aiheutuva kustannus voi kuitenkin olla merkityksellinen.

Digitaalisen henkilöllisyystodistuksen hyödyntäminen edellyttää käyttäjältään älypuhelinta. Tilastokeskuksen vuonna 2021 laatiman Väestön tieto- ja viestintätekniikan käyttö –tutkimuksen mukaan 88 prosentilla suomalaisista oli käytössään älypuhelin (Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö (verkkojulkaisu), ISSN=2341-8699. 2021. Helsinki. Tilastokeskus. Saantitapa: http://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_tie_001_fi.html). Ikäluokassa 16–54 –vuotiaat älypuhelin on käytössä yli 96 prosentilla kansalaisista. Lisäksi tablettitietokone löytyy 53 prosentista kotitalouksista. Liikenne- ja viestintävirasto Traficomin Viestintäpalvelujen kuluttajatutkimuksessa 2021 (<https://www.traficom.fi/fi/julkaisut/viestintäpalvelujen-kuluttajatutkimus-2021>) arvioidaan, että 89,7 prosentilla suomalaisista on älypuhelin. Voidaan arvioida, että ehdotuksen mukaisen digitaalisen henkilöllisyystodistuksen edellyttämä laite on siis olemassa useimmilla kotitalouksilla, eikä ehdotuksesta siten aiheudu merkittäviä lisäkustannuksia kotitalouksille.

Ehdotuksen varmuustaso- ja muut tietoturva-vaatimukset asettavat vaatimuksia loppukäyttäjän mobiililaitteen tietoturvaominaisuuksille. Tämä rajaa osan käytössä olevista mobiililaitteista ratkaisun ulkopuolelle. Käytännössä vaatimukset liittyvät tiedon suojaamiseen mobiililaitteella. Sovellustason suojaus ei ole suunniteltujen ratkaisujen näkökulmasta riittävä vaan myös laite-tason suojaus on tarpeen. Suomessa käytössä olevista Android-laitteista 80–90 prosenttia täyttää tällä hetkellä vähimmäisvaatimukset laitetason suojauksesta. Suomessa käytetyistä iOS-puhelimista vastaavan ominaisuuden arvioidaan löytyvän vuoden 2023 alussa 100:sta prosentista laitekannasta. Vaatimus laitetason suojauksesta tarkentuu toteutuksen ja tietoturva-arviointien myötä ja tämä voi muuttaa tuettujen laitteiden osuutta. Vastaavasti osuudet muuttuvat laitekan-nan uudistuessa. On kuitenkin tunnistettu, että tuettujen laitteiden määrällä on merkitystä siihen, millaisia taloudellisia vaikutuksia ehdotuksella on suhteessa kotitalouksiin.

Ehdotuksen mukaan luonnollisen henkilön tunnistusväline olisi vaihtoehtoinen ratkaisu julkisen sektorin digitaalisten palvelujen käytön vaatimaan sähköiseen tunnistautumiseen, jos henkilö ei halua tai voi käyttää mobiilipäätelaitteella olevaa digitaalista henkilöllisyystodistusta. Luonnol-lisen henkilön tunnistusvälineen tuottamista esitettäisiin rahoitettavaksi osittain budjettirahoitettuna siten, että asiakashintaa subventoidaan jatkuvien kustannusten osalta Digi- ja väestötietovirastolle myönnettävällä arviomäärärahalla. Tällöin luonnollisen henkilön tunnistusvälineen asiakashinta asettuisi noin tai jonkin verran alle arvioidun omakustannusarvon. Asiakashinta-arviona on valmistelussa pidetty 10 euron ja 20 euron välillä olevaa maksua. Tämä vastaisi muiden vastaavien yksityisen sektorin tuottamien palveluiden hintatasoa. Käyttäjä saisi yhdellä maksulla enintään kaksi laitetta 10 vuoden aikana. Asiakkaan maksama hinta määriteltäisiin tarkemmin erikseen annettavalla maksuperustelain mukaisella asetuksella.

Ehdotuksilla arvioidaan olevan jonkin verran vaikutuksia myös ulkomaalaisiin, joilla on asiointitarve suomalaisissa digitaalisissa palveluissa. Näitä vaikutuksia voidaan pitää henkilötasolla maltillisina. Ulkomaalaisen asiointivälineen saamisen ehtona on voimassa oleva jonkin maan passi tai henkilökortti. Ulkomaalaisen asiointivälineen hinnaksi arvioidaan muodostuvan noin 7 euroa perustuen 64 000 vuotuisen käyttäjään. Käyttäjämääräarvio perustuu Digi- ja väestötietoviraston nykyisin tarjolla olevaan ulkomaalaisten tunnistuspalvelun käyttäjämäärään sekä opetus- ja kulttuuriministeriön arvioon Suomesta opiskelupaikkaa hakevien määrästä. Ulkomaalaisen asiointivälineen hinta saattaa vaihdella vuosittain todellisen käyttäjämäärän perusteella.

4.2.1.2 Vaikutukset yrityksiin palveluiden tarjoajina

Vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinoilla toimii sekä tunnistusvälineiden että tunnistusvälityspalvelujen tarjoajia, jotka tarjoavat tunnistuspalveluja kuluttajille ja sähköisille asiointipalveluille. Sama yritys voi toimia molemmissa rooleissa. Kaiken kaikkiaan Liikenne- ja viestintäviraston rekisterissä on tällä hetkellä 16 vahvan sähköisen tunnistuspalvelun tarjoajaa. Näistä omaa vahvaa sähköistä tunnistusvälinettä tarjoaa 14 toimijaa ja muidenkin kuin oman vahvan sähköisen tunnistusvälineen käyttäjien tunnistusta välittäviä tunnistuspalveluja on kahdeksan. Tunnistusvälityspalvelun tarjoajista kaksi tarjoaa pelkästään välityspalvelua eli niillä ei ole omaa vahvaa sähköistä tunnistusvälinettä tarjottavana sähköisille asiointipalveluille. Vuonna 2021 on tullut vireille yhden uuden välityspalvelun ilmoitus toiminnan aloittamisesta. Vahvan sähköisen tunnistusvälityspalvelun tarjoajista kuusi välittää sähköisille asiointipalveluille kaikkia Suomessa käytössä olevia tunnistusvälineitä pois lukien Digi- ja väestötietoviraston henkilö- ja organisaatiovarmenteita.

Tunnistusvälineiden tarjoajille arvioidaan aiheutuvan *digitaalista henkilöllisyystodistusta* koskevista esityksistä sekä negatiivisia että positiivisia vaikutuksia. Yhtäältä, jos digitaalisen henkilöllisyystodistuksen käytöstä tulee laajamittaista sähköisten asiointipalvelujen ja tunnistusvälityspalveluiden piirissä, voi tämä johtaa tilanteeseen, jossa pelkästään tunnistusvälineitä tarjoavien toimijoiden liiketoimintamahdollisuudet heikentyvät. Tämä voi johtaa investointihalukkuuden vähenemiseen tunnistusvälineitä tarjoavien toimijoiden piirissä ja mahdollisesti myös toimijoiden poistumiseen vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinoilta. Tämä voisi puolestaan vaikuttaa tunnistusvälineiden käyttäjien mahdollisuuksiin käyttää sähköisiä asiointipalveluja. Lisäksi uusien tunnistusvälineiden tarjoajien mielenkiinto tuoda markkinoille uusia tunnistusvälineitä voi heiketä tai tunnistusvälineitä voidaan pyrkiä tarjoamaan matalammalla varmuustasolla. Näiden muutosten todennäköisyyteen vaikuttaa se, että miten laajasti digitaalista henkilöllisyystodistusta otetaan käyttöön ja miten laajasti sen käyttöä mahdollistetaan tunnistusvälityspalveluissa ja sähköisissä asiointipalveluissa. Jos digitaalisen henkilöllisyystodistuksen käyttö jää vähäiseksi, myös vaikutukset nykyisille ja uusille vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinoilla toimiville toimijoille jäävät vähäisiksi.

Toisaalta ehdotus mahdollistaisi nykyisille vahvan sähköisen tunnistusvälineen tarjoajille digitaalisen henkilöllisyystodistuksen hyödyntämisen osana vahvan sähköisen tunnistusvälineen myöntämisprosessia. Henkilön digitaalinen ensitunnistaminen ja tämän tiedon tallentaminen on jonkin verran edullisempaa kuin ensitunnistaminen fyysisestä asiakirjasta. Nykyisin erityisesti fyysisen asiakirjan tarkastaminen asiakaspalvelijan toimesta, asiakirjan mahdollinen kopiointi sekä kopion tallentaminen fyysisen asiakirjan käyttämisestä aiheuttavat kustannuksia, jotka poistuvat digitaalisen henkilöllisyystodistuksen hyödyntämisen myötä. Digitaalisen henkilöllisyystodistuksen laajalla käytöllä maksuttomana ensitunnistamisvälineenä voikin jossain määrin vähentää vahvan sähköisen tunnistusvälineen myöntämiseen liittyviä kustannuksia.

Digitaalinen henkilöllisyystodistus olisi käyttöönotettavissa yhtenä uutena tunnistustapana sähköisissä asiointipalveluissa todennäköisesti varsin pienillä muutoksilla, jos nykyiset tunnistusvälityspalvelun tarjoajat toimivat sen välittäjänä. Tällöin luottamusverkoston tunnistusvälityspalvelujen kautta digitaalisella henkilöllisyystodistuksella olisi nopeasti yhtä laajat käyttömahdollisuudet kuin nykyisin käytössä olevilla tunnistusvälineillä. Käyttöönotto tunnistusvälityspalveluissa edellyttäisi uusien integrointimenetelmien toteuttamista johtuen siitä, että digitaalisen henkilöllisyystodistuksen rajapintatoteutukset poikkeavat nykyisistä luottamusverkoston rajapintatoteutuksista. Tällä voi olla vähäisiä kustannusvaikutuksia tunnistusvälityspalveluiden tarjoajille.

Digitaalista henkilöllisyystodistusta ja erityisesti Digi- ja väestötietoviraston tuottamaa ydinidentiteetin todistetta koskevat ehdotukset saattavat pidemmällä aikavälillä lisätä nykyisten tunnistusvälityspalvelun tarjoajien liiketoimintamahdollisuuksia. Tulevaisuudessa erilaiset digitaaliset identiteettilompakot ja mahdollisesti näihin talletettava ydinidentiteetin todiste sekä muut varmennetut henkilöön liittyvät tiedot voivat luoda täysin uuden liiketoiminta-alueen, joka olisi merkittävästi nykyistä vahvan sähköisen tunnistamisen liiketoimintaa laajempi. Digitaalisen henkilöllisyystodistuksen ehdotus voi kuitenkin lyhyellä aikavälillä mahdollisesti vähentää pelkästään tunnistuspalvelua tarjoavien toimijoiden liiketoimintamahdollisuuksia.

Ehdotuksella ei arvioida olevan suoria vaikutuksia vahvan sähköisen tunnistamisen tarjoamisen mahdollisuuksiin, mutta ehdotuksella voi olla vaikutuksia vahvan sähköisen tunnistamisen yleiseen hintatasoon ja siten liiketoiminnan yleiseen kannattavuuteen. Tällä hetkellä tunnistusvälityspalvelun tarjoajat maksavat tunnistusvälineen tarjoajille niin sanotun tukkuhinnan, joka voi olla enintään 3 senttiä tapahtumalta. Sähköisten asiointipalvelujen tarjoajat maksavat tunnistusvälityspalvelun tarjoajalle sopimuksessa sovitun hinnan, johon voi kuulua kiinteä hinta ja tapahtumapohjaisesti tunnistustapahtuman hinta (3 senttiä lisättynä tunnistusvälityspalvelun tarjoajan osuudella). Tämän lisäksi kuluttajat maksavat pääsääntöisesti kuukausikohtaista korvausta tunnistuspalvelun käyttöoikeudesta. Kuluttajien kannalta tunnistuspalvelut ovat usein osa peruspankkipalveluita, joiden ohessa he saavat myös vahvan sähköisen tunnistamisen palvelut käyttöönsä. Mobiilioperaattoreiden tarjoama mobiilivarmenne perustuu myös pääsääntöisesti kuluttajalta veloittettavaan kuukausilaskutukseen. Olennaista on, että digitaalisen henkilöllisyyden osalta digitaalinen henkilöllisyystodistus on maksullinen tuote kansalaiselle, mutta sen hyödyntäminen olisi lähtökohtaisesti maksutonta asiointipalveluille ja muille luottaville osapuolille. Tämä muuttaa jonkin verran kulujen painottumista nykyisestä mallista. Tämä koskee erityisesti tunnistusvälityspalvelun tarjoajia, joille digitaalisen henkilöllisyystodistuksen hyödyntäminen olisi maksutonta ja tunnistusvälityspalvelun tarjoaja voisi itse määrittellä millaisen korvauksen se perii sähköisiltä asiointipalvelulta.

Digitaalisen henkilöllisyystodistuksen vaikutuksia vahvan sähköisen tunnistamisen liiketoiminnan kannattavuuteen kokonaisuutena on vaikea arvioida, erityisesti koska digitaalisen henkilöllisyystodistuksen käyttöasteesta kansalaisten parissa tai siihen kytkeytyvistä palveluista ei ole vielä tietoa. Todelliseen käyttäjämäärään tulee vaikuttamaan erityisesti esitettävän ratkaisun helppokäyttöisyys sekä käyttömahdollisuudet eri palveluissa.

Digitaalisella henkilöllisyydellä on todennäköisesti vaikutuksia tunnistustapojen kehittymiseen, mutta kehityssuuntaan vaikuttavat olennaisesti myös tunnistamisen tarpeet sekä EU-tasolla tapahtuva kehitys. Esimerkiksi eIDAS-muutosehdotus sekä syksyllä 2021 käynnistynyt tiettyjen EU-alueella toimivien liikepankkien digitaalisen lompakon kehityshanke tulevat osaltaan määrittämään myös Suomessa tapahtuvaa sähköisen tunnistamisen kehittymistä.

Ehdotuksen valmisteluvaiheessa on arvioitu, ettei kaikkien nykyisten palvelujen tarjoajien kohdalla oman liiketoiminnan ulkopuolelle myymä vahvan sähköisen tunnistamisen palvelu ole kovin kannattavaa liiketoimintaa. Useimmat tarjoavat asiakkailleen tämän mahdollisuuden, koska haluavat palvella omia asiakkaitaan mahdollistamalla heille tutun menetelmän vahvaan sähköiseen tunnistautumiseen myös muihin kuin omiin pankkipalveluihin. Ehdotuksella voi olla vaikutuksia eri toimijoiden halukkuuteen tarjota omia tunnistusvälineitään sähköisen tunnistamisen luottamusverkoston kautta laajempaan käyttöön. Tällä voi olla myös laajemmin vaikutuksia eri toimijoiden halukkuuteen investoida vahvojen sähköisten tunnistusvälineiden kehitykseen ja tämä voisi lopulta johtaa tilanteeseen, jossa toimijoita poistuu luottamusverkostosta.

Julkisen sektorin osalta sähköisen tunnistamisen välityspalveluna toimisi jatkossakin Digi- ja väestötietoviraston ylläpitämä suomi.fi-tunnistuksen välityspalvelu. Ehdotuksella ei olisi vaikutuksia nykyisten vahvan sähköisen tunnistamisen toimijoiden mahdollisuuksille tarjota palveluja myös julkiselle sektorille. Digitaalista henkilöllisyyttä koskevan hankkeen osalta tavoitteena on julkisen sektorin sähköisen tunnistamisen kulujen hallittavuus ja tällä voi olla vaikutuksia siihen kokonaissummaan, mitä julkinen sektori jatkossa maksaa yksityisen sektorin tuotamasta sähköisestä tunnistamisesta.

Ehdotettava sääntely ei ota kantaa julkisen hallinnon tulevaan rooliin sähköisen tunnistamisen ostajana. Valtiovarainministeriön asettaman Digitaalisen henkilöllisyyden –hankkeen yhtenä tavoitteena on kuitenkin luoda edellytyksiä julkisen sektorin sähköisen tunnistamisen kustannustason hallinnalle. Hankkeen aikana on katsottu, että jatkossakin julkisen sektorin sähköisiin asiointipalveluihin tulisi olla mahdollista tunnistautua kaikilla niillä tunnistuspalveluilla, joiden kanssa asiasta on sovittu. Julkisen hallinnon sähköisen tunnistamisen kustannuksiin tulee vaikuttamaan merkittävästi se, miten laajasti digitaalista henkilöllisyydestä tullaan ottamaan käyttöön. Jos käyttö jää vähäiseksi, julkishallinnolle muiden tunnistusvälineiden käytöstä syntyvät kustannukset voivat kasvaa, kun vahvan sähköisen tunnistamisen volyymi kasvaa. Vastaavasti jos digitaalista henkilöllisyydestä otetaan laajasti käyttöön kansalaisten keskuudessa, kustannukset voivat laskea. Tällä voi olla vaikutuksia luottamusverkoston kautta tapahtuvaan vahvan sähköisen tunnistamisen liiketoimintaan ja sen kannattavuuteen sekä mahdollisuuksiin markkinaehtoisien vahvan sähköisen tunnistamisen tarjontaan yksityisen sektorin palveluihin.

Ulkomaalaisten digitaalista asiointivälinettä koskevalla ehdotuksella ei arvioida olevan merkittäviä taloudellisia vaikutuksia nykyisiin sähköisen tunnistamisen toimijoihin. Ulkomaalaisen digitaalinen asiointiväline olisi ulkomaalaisille käytettävissä ensisijaisesti julkisen sektorin digitaalisissa palveluissa, mutta ulkomaalaisen digitaalista asiointivälinettä voivat hyödyntää myös yksityisen sektorin toimijat vastaavalla tavalla kuin digitaalista henkilöllisyydestä. Ulkomaalaisten mahdollisuudet saada nykyisen sääntelyn mukainen vahva sähköisen tunnistamisen väline on esityksen valmistelussa tunnistettu yhdeksi merkittäväksi haasteeksi ulkomaalaisten asiointimahdollisuuksille suomalaisissa viranomaisissa. Tätä on pyritty ottamaan huomioon mahdollistamalla ulkomaalaisen digitaalisen asiointivälineen varmuustason nostaminen asioimalla kasvokkain, jolloin tieto kasvokkain tapahtuneesta tunnistamisesta voidaan sisällyttää osaksi ulkomaalaisen digitaalisen asiointivälineen tietosisältöä. Toisaalta ulkomaalaisen digitaalisen asiointivälineen käytön laajuus tulee riippumaan myös siitä, että miten laajasti yksityisen ja julkisen hallinnon sähköiset asiointipalvelut tulevat hyväksymään etärekisteröitymisen kautta käyttöön otetut asiointivälineet.

Luonnollisen henkilön tunnistusvälineellä voi lähtökohtaisesti olla taloudellisia vaikutuksia nykyisten sähköisen tunnistamisen toimijoiden liiketoimintaan vähentämällä näiden julkiselta sektorilta saamia tunnistuspalveluiden tuottoja. Luonnollisen henkilön tunnistusväline olisi vaihto-

ehtoinen ratkaisu julkisen sektorin digitaalisten palvelujen käytön vaatimaan sähköiseen tunnistautumiseen, jos henkilö ei halua tai voi käyttää mobiilipäätelaitteella olevaa digitaalista henkilöllisyystodistusta. Luonnollisen henkilön tunnistusvälineen käytön laajuuden ei kuitenkaan arvioida olevan suuruusluokaltaan merkittävää, joten taloudelliset vaikutukset ovat yksittäisten talouden toimijoiden kohdalla varsin pieniä.

4.2.1.3 Vaikutukset yrityksiin palveluiden hyödyntäjinä

Digitaalinen henkilöllisyystodistus olisi sähköisten asiointipalvelujen hyödynnettävissä joko nykyisten tunnistusvälityspalvelujen kautta tai suoraan hyödyntäen Digi- ja väestötietoviraston tuottamia rajapintoja. Ehdotuksessa laiksi Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista ehdotetaan Digi- ja väestötietovirastolle velvoitetta tarjota lukijarajapintaa digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin tarkastamiseen käynti- ja sähköisessä asiointissa.

Digitaalinen henkilöllisyystodistus toimisi tunnistusvälineenä siten, että asiointivälineen haltija valitssee itse vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle. Tämä toimintamalli poikkeaa nykyisestä vahvan sähköisen tunnistamisen luottamusverkoston toimintamallista, jossa asiointipalvelu määrittelee ne tiedot, joita se tarvitsee ja jotka se hankkii vahvaa sähköistä tunnistamista tarjoavilta tunnistuspalveluilta.

Siltä osin, kun asiointipalvelut haluavat ottaa käyttöön myös ehdotetut asiointiratkaisut ne joutuisivat tekemään jonkinlaisia muutoksia omiin asiointipalveluihinsa uuden toimintamallin hyödyntämiseksi. Näin ehdotuksen johdosta voisi syntyä välillisiä kustannuksia. Digi- ja väestötietovirasto päättäisi rajapintapalvelujen tarkemmasta sisällöstä, joten jatkossa on tarpeen arvioida tarkemmin, kuinka isosta muutoksesta lopulta on kyse teknisen toteutuksen näkökulmasta. Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen asiointivälineen suora hyödyntäminen sähköisessä tai käyntiasioinnissa edellyttäisi asiointipalveluilta myös uusiin teknisiin protokolliin perustuvien integraatioiden toteuttamista. Johtuen näiden protokollien suhteellisesta tuoreudesta on tärkeää, että asiointipalveluille viestitään riittävän tarkalla tasolla, miten integraatio on toteutettavissa tietoturva ja tietosuoja huomioiden.

Käyttöönotto ei kuitenkaan olisi pakollista ja siten kustannukset ovat asiointipalvelujen näkökulmasta valinnaisia. Lisäksi tulee huomioida, että käytännössä kaikki nykyiset vahvaa sähköistä tunnistamista hyödyntävät yksityisen sektorin palvelut käyttävät nykyisiä luottamusverkoston tunnistusvälityspalveluja. Ehdotuksen perusteella ei ole perusteltua olettaa, että yritykset tulisivat rakentamaan laajassa mittakaavassa omia, suoria rajapintayhteyksiä Digi- ja väestötietoviraston palveluihin. Tällöin monille nykyisille sähköisen tunnistamisen hyödyntäjille digitaalinen henkilöllisyystodistus olisi tarjolla yhtenä uutena tunnistuspalveluna, eikä aiheuttaisi muutoksia.

Palveluja hyödyntävien yritysten näkökulmasta teknisiä muutuskustannuksia merkityksellimpi vaikutus voi olla ehdotuksen mukaisella toimintamallin muutoksella, joka kohdistuu sähköiseen asiointiin ja käyntiasiointiin, kun käyttäjän tulee valita itse, mitä varmennettuja henkilötietoja haluaa osoittaa asiointipalvelulle. Käyttäjille muutos on merkittävä. Tämä voi lisätä erilaisten asiakaskyselyjen määrää esimerkiksi asiointipalvelua tarjoavissa yrityksissä.

Asiointitilanteessa asiointipalvelu pyytää varmennettuja henkilötietoja, jotka digitaalisen henkilöllisyystodistuksen käyttäjän tulee esittää. Digitaalisen henkilöllisyystodistuksen käyttöliittymän tulee osoittaa käyttäjälle mille asiointipalvelulle tietoja ollaan osoittamassa ja muutoinkin tukea käyttäjää päätöksen tekemisessä. Käyttäjän tulee lisäksi vapauttaa tiedonsiirron suo-

jaamisessa käytettävät salausavaimet avainsäilöstä antamalla viimeisessä vaiheessa todennustekijä (esim. PIN-koodi), jolla avaimet vapautetaan varmennettujen henkilötietojen siirtämistä varten. Alla olevassa kaaviossa kuvataan miten todisteen esittäminen asiointitilanteessa voisi tapahtua:



Kuva 1 Vahvistettujen tietojen esittäminen asiointitilanteessa

Asiointipalvelujen osalta toimenpiteitä voi edellyttää myös tarvittavien määrittelyjen tekeminen sellaisissa tapauksissa, että käyttäjä ei halua välittää asiointipalvelulle kaikkia sen pyytämiä tietoja. On mahdollista, että osa tai kaikki mahdollisesti vaadittavista muutoksista voidaan toteuttaa nykyisten tunnistusvälityspalvelujen toimesta, jolloin asiointipalvelujen ei välttämättä tarvitse tehdä muutoksia. Myös toimintamallista johtuvat kustannukset olisivat harkinnanvaraisia siten, sillä ratkaisujen hyödyntäminen ei tulisi pakolliseksi.

Arvioitaessa ehdotuksen vaikutuksia sähköisen tunnistamisen käyttöön ja hyödyntämiseen olennaista on, miten laajasti sähköiset palvelut ovat halukkaita tai kykenevät hyödyntämään digitaalisen henkilöllisyyden palvelua sähköisenä tunnistautumismenetelmänä sekä kansalaisten halukkuutta käyttää digitaalista henkilöllisyystodistusta sähköisen tunnistamisen välineenä.

Liikenne- ja viestintäviraston maaliskuussa 2021 julkaisemassa sähköisen tunnistamisen markkinaselvityksessä todetaan: ”Suurin osa käyttäjistä selkeästi käyttäisi vahvaa sähköistä tunnistusvälinettä tunnistautumisessa, jos vain sähköisten asiointipalvelujen tarjoajat mahdollistaisi sen palveluissaan ([Sähköisen tunnistamisen markkinat - Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana \(traficom.fi\)](#), sivu 40). Kansalaisten näkökulmasta vahvalle sähköiselle tunnistukselle sähköisissä asiointipalveluissa on selkeää kysyntää eivätkä nykyiset käyttömahdollisuudet vastaa tätä tarvetta.” Kuluttajat siis haluaisivat hyödyntää useammassa palvelussa vahvan sähköisen tunnistamisen välineitä.

Ehdotuksilla voi olla vaikutuksia siihen, että nykyistä useampi asiointipalvelu tarjoaisi käyttäjilleen mahdollisuuden vahvaan sähköiseen tunnistamiseen, erityisesti jos vahvaan sähköiseen tunnistamiseen liittyvät kustannukset laskisivat ja olisivat ennakoitavia asiointipalveluja tuottavien organisaatioiden näkökulmasta. Nykyinen vahvan sähköisen tunnistamisen luottamusveroston sisäinen veloitusmalli perustuu tapahtumakohtaiseen enimmäishintasääntelyyn, joka ei

teoriassa estä puhtaasti kiinteähintaisten sopimusten tekoa asiointipalveluille, mutta käytännössä on tehnyt sen harvinaiseksi.

Ehdotuksella voi olla positiivisia taloudellisia vaikutuksia niille toimijoille, jotka kykenevät hyödyntämään digitaalisen henkilöllisyystodistuksen mahdollisuuksia omassa liiketoiminnassaan vaihtoehtona perinteisemmälle käyntiasioinnille ja henkilöllisyysasiakirjojen esittämiseen. Esimerkiksi sellaiset asiakkuuden avaamisprosessit, jotka nykyisin vaativat asiakkaan fyysistä läsnäoloa ja virallisen henkilöllisyystodistuksen näyttämistä olisi mahdollista toteuttaa täysin digitaalisesti. Tämä voi mahdollistaa uusia toimintamalleja ja -tapoja asiakkuuden avaamiseen sekä yleisesti digitaalisten palvelujen tarjoamiseen.

Digitaalisen henkilöllisyystodistuksen käyttöönotto käyntiasioinnissa edellyttää todennäköisesti jonkinlaisia muutoksia palveluntuottajan toimintamalleihin. Ehdotuksen mukaan digitaalisen henkilöllisyystodistuksen voi käyntiasioinnissa tarkastaa Digi- ja väestötietoviraston tuottamalla mobiilisovelluksella. Mobiilisovelluksen käyttö edellyttää, että asiointipisteen virkailijan käytössä on mobiililaite. Vaihtoehtoisesti tarkastusrajoituksen käyttäminen edellyttää teknisiä muutoksia viranomaisen käyntiasioinnin virkailijajärjestelmiin. Käyntiasiointitoiminnallisuuden toteuttaminen edellyttää hyödyntävilta organisaatioilta investointeja, joiden tasosta ei ole toistaiseksi arvioita.

Esitykseen sisältyvät säädösehdotukset eivät sisällä velvollisuutta hyväksyä digitaalinen henkilöllisyystodistus henkilöllisyyden tarkastamisessa. Ehdotuksen mukaan digitaalinen henkilöllisyystodistus olisi virallinen, poliisin myöntämä henkilöllisyyttä osoittava asiakirja. Jos digitaalisen henkilöllisyystodistuksen käyttö yleistyy, voidaan kuitenkin olettaa, että palveluntuottajille syntyy vähintään asiakastarpeen kautta paine hyväksyä digitaalinen henkilöllisyystodistus tunnistusasiakirjana.

Ulkomaalaisten digitaalista asiointivälinettä koskevalla ehdotuksella voi olla taloudellisia ja toiminnallisia vaikutuksia niille toimijoille, jotka tarjoavat palveluitaan sellaisille ulkomaalaisille, joilla ei tällä hetkellä ole mahdollista saada sähköistä tunnistusvälinettä. Ulkomaalaisen asiointiväline mahdollistaa sähköisten palveluiden tarjoamisen myös ulkomaalaisille, mutta tämä edellyttää muutoksia asiointipalveluun ja sen taustajärjestelmiin. Toimijoiden onkin tarkoituksenmukaista arvioida tapauskohtaisesti, ovatko muutokset kannattavia suhteessa niistä saatavaan hyötyyn.

Luonnollisen henkilön tunnistusväline ei ole ehdotuksen mukaisesti yksityisen sektorin asiointipalvelujen hyödynnettävissä, vaan se toimisi sähköisen tunnistamisen välineenä julkishallinnon sähköisissä palveluissa niiden käyttäjien osalta, joilla ei ole mahdollista hyödyntää mobiililaitteeseen pohjautuvaa digitaalista henkilöllisyystodistusta tai muita sähköisen tunnistamisen välineitä. Näin ollen luonnollisen henkilön tunnistusvälineellä ei ole suoria vaikutuksia yksityisen sektorin sähköiseen asiointiin.

4.2.1.4 Kilpailuvaikutukset

Kilpailuoikeudellisista lähtökohdista

Digitaalisen henkilöllisyyden palveluihin liittyy EU-lainsäädännön valtioneuvoston päätös (Sopimus Euroopan Unionin toiminnasta 107 art.) ja kansallista kilpailuneutraaliteettia koskevaa lainsäädäntöä (kilpailulain 4 a luku) koskevia kysymyksiä. SEUT 107 artiklan 1 kohdan mukaan

jäsenvaltion myöntämä taikka valtion varoista muodossa tai toisessa myönnetty tuki, joka vääristää tai uhkaa vääristää kilpailua suosimalla jotakin yritystä tai tuotannonalaa, ei sovellettu sisämarkkinoille, siltä osin kuin se vaikuttaa jäsenvaltioiden väliseen kauppaan.

Esityksen valmistelun yhteydessä on arvioitu näitä kysymyksiä suhteessa ydinidentiteetin todistamiseen, digitaaliseen henkilöllisyystodistukseen, ulkomaalaisen digitaaliseen asiointivälineeseen sekä luonnollisen henkilön tunnistusvälineeseen. Arvioinnissa on tarkasteltu tilanteita, joissa julkisyhteisö toimii tunnistusvälineen tarjoajana, välityspalveluiden tarjoajana tai asiointipalvelun tarjoajana.

Kilpailu- ja valtiontukisääntely koskee taloudellista toimintaa harjoittavia yksiköitä, riippumatta niiden oikeudellisesta muodosta tai rahoitustavasta. Esikysymyksenä tämän sääntelyn soveltamiselle on siten arvioitava, onko kyse taloudellisesta toiminnasta. Tällöin voidaan tarkastella esimerkiksi sitä, onko palveluille olemassa markkina taikka olisivatko muut toimijat ha lukkaita ja kykeneviä tuottamaan palvelua markkinalla. Kiellettyä valtiontukea tai kilpailuneutraliteettia koskeva sääntely ei tule sovellettavaksi, kun kyse on viranomaisesta, joka toimii julkisen vallan käyttäjänä tai viranomaisen ominaisuudessaan. Jos julkisyhteisö harjoittaa taloudellista toimintaa, joka voidaan erottaa julkisen vallan käytöstä, tulee valtiontuen mahdollisuus arvioitavaksi tämän toiminnan osalta. Jos sitä vastoin taloudellista toimintaa ei voida erottaa julkisen vallan käytöstä, kaikki kyseisen yhteisön toiminnot liittyvät edelleen julkisen vallan käyttöön.

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. 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.

Taloudellisen ja muun kuin taloudellisen toiminnan selventämiseksi unionin tuomioistuin on johdonmukaisesti katsonut, että taloudellista toimintaa on kaikki toiminta, jossa tavaroita tai palveluita tarjotaan markkinoilla. Se, onko tietyille palveluille markkinat, voi riippua siitä, kuinka kyseiset palvelut on järjestetty asianomaisessa jäsenvaltiossa, ja voi siksi vaihdella jäsenvaltiosta toiseen. Lisäksi poliittisten valintojen tai taloudellisen kehityksen johdosta tietyn toiminnan luokittelu voi muuttua ajan mittaan. Mikä ei ole tarkasteluhetkellä taloudellista toimintaa, voi muuttua sellaiseksi tulevaisuudessa, ja päinvastoin (Komission tiedonanto Euroopan unionin toiminnasta annetun 107 artiklan 1 kohdassa tarkoitetusta valtiontuen määritelmästä (2016/C 262), kohta 12-13).

Jos julkisyhteisö harjoittaa taloudellista toimintaa, joka voidaan erottaa julkisen vallan käytöstä, kyseinen yhteisö toimii yrityksenä tämän toiminnan osalta. Jos sitä vastoin taloudellista toimintaa ei voida erottaa julkisen vallan käytöstä, kaikki kyseisen yhteisön toiminnot liittyvät edelleen julkisen vallan käyttöön, eivätkä ne sen vuoksi kuulu yrityksen käsitteen piiriin (Komission tiedonanto 2016/C 262), kohta 18).

Valtiontukilainsäädännön lisäksi on huomattava, että jos jäsenvaltio on päättänyt ottaa käyttöön markkinamekanismeja, ja toimintaa on luonteeltaan pidettävä taloudellisena, on sovellettava myös kilpailulain 4 a lukua kilpailuneutraliteetista.

Kilpailulain 4 a luvun kilpailuneutraliteettisääntelyn tavoitteena on antaa kansalliselle viranomaiselle toimivaltaa kilpailuneutraliteettiin liittyvissä asioissa, jotka ovat usein johtaneet ko-

missiolle tehtyihin kanteluihin ja näin luoda edellytyksiä tällaisten kilpailuongelmien ratkaisemiseen kansallisella tasolla. Kilpailulain 4 a lukua ei lain 30 b §:n mukaan sovelleta, jos menettely tai toiminnan rakenne seuraa välittömästi lainsäädännöstä taikka jos soveltaminen estäisi merkittävän kansalaisten hyvinvointiin, turvallisuuteen tai muuhun sellaiseen yleiseen etuun liittyvän tehtävän hoitamisen. Mikäli digitaalisen henkilöllisyystodistuksen tarjoaminen katsottaisiin joltain osin taloudelliseksi toiminnaksi ja muuten kilpailuneutraliteettisääntelyn vastaiseksi, olisi asiaa esitetyn sääntelyn perusteella arvioitava kilpailulain 30 b §:n mukaisesti välittömästi lainsäädännöstä seuraavana menettelynä tai rakenteena. Kilpailuneutraliteettisääntösten mukaan markkinoilla tapahtuva taloudellinen toiminta on hinnoiteltava markkinaperusteisesti. KKV voisi kilpailulain perusteella puuttua myös esimerkiksi viranomaisen yksityisen elinkeinotoiminnan kanssa samoilla markkinoilla harjoittamaan taloudelliseen toimintaan tai sen tässä toiminnassa nauttimiin perusteettomiin kilpailuetuihin.

Digitaalinen henkilöllisyystodistus, ulkomaalaisen digitaalinen asiointiväline, ydinidentiteetin todiste sekä luonnollisen henkilön tunnistusväline

Esikysymyksenä on käsiteltävä sitä, miltä osin digitaalinen henkilöllisyystodistus, ydinidentiteetin todisteen myöntäminen, ulkomaalaisen digitaalisen asiointivälineen tai luonnollisen henkilön tunnistusvälineen tarjoamisen voidaan katsoa olevan julkisen vallan käyttöä ja miltä osin mahdollisesti on kysymys taloudellisesta toiminnasta.

Digitaalisella henkilöllisyystodistuksella on kiinteä yhteys passiin ja henkilökorttiin. Henkilön väestötietojärjestelmään rekisteröityyn henkilöllisyyteen pohjautuvien virallisten henkilöllisyyttä osoittavien asiakirjojen (passin ja henkilökortin) myöntämisen on katsottava olevan julkisen vallan käyttöä riippumatta siitä, onko passi tai henkilökortti fyysinen esine vai digitaalinen. Kun viranomainen yhdistää fyysisen luonnollisen henkilön tämän väestötietojärjestelmään perustuvaan ydinidentiteettiin ja liitoksesta muodostetaan digitaalinen todiste erilaisissa asiointitilanteissa hyödynnettäväksi ja todiste luovutetaan sovelluksessa henkilön omaan hallintaan, ollaan henkilön oikeusaseman näkökulmasta vastaavassa tilanteessa kuin passia tai henkilökorttia myönnettäessä. Digitaalinen henkilöllisyystodistus olisi esitetyn sääntelyn mukaan henkilöllisyyttä osoittava asiakirja henkilökortin ja passin tavoin. Sitä voitaisiin käyttää ja se voitaisiin hyväksyä henkilöllisyyden osoittamisen tarkoituksessa samalla tavoin, kuin henkilökortti ja passi.

Ulkomaalaisen digitaalinen asiointiväline on henkilöllisyyttä koskevien sekä muiden vahvistettujen tietojen osoittamiseen sähköisessä asiointissa tarkoitettu asiointiväline ja se tarjotaan käytettäväksi digitaalisen henkilöllisyyden sovelluksen avulla. Ulkomaalaisen digitaalinen asiointiväline olisi siten todennettavissa samalla tavoin kuin digitaalinen henkilöllisyystodistus digitaalisen henkilöllisyyden sovelluksen avulla ja mahdollistaisi omalta osaltaan sen, että ulkomaalainen voi asioida suomalaisten viranomaisten kanssa.

Ulkomaalaisen digitaalisen asiointivälineen yhteys julkisen vallan käyttöön ei kuitenkaan olisi yhtenevä digitaalisen henkilöllisyystodistuksen kanssa, sillä sen myöntäminen ja käyttö eivät ole kiinteässä yhteydessä passiin ja henkilökorttiin. Ulkomaalaisen digitaalinen asiointiväline ei olisi passiin ja henkilökorttiin verrattavissa oleva henkilöllisyyttä osoittava asiakirja. Sillä voidaan kuitenkin nähdä olevan kiinteä yhteys väestön rekisteröintiin, joka tapahtuu viranomaisen ominaisuudessa.

Asiointivälineen tarkoitus olisi mahdollistaa ulkomaiseen henkilöllisyysasiakirjaan perustuvien henkilötietojen esittäminen sähköisessä asiointissa, ehkäistä rinnakkaisten henkilöllisyyksien muodostumista asiointitapahtumissa ja viranomaisrekistereissä, sekä lisätä esitettävien tietojen

luotettavuutta. Asiointivälineen myöntäminen edellyttäisi henkilön rekisteröintiä väestötietojärjestelmään siten, että menettelyn yhteydessä ulkomaan kansalaiselle myönnetään henkilötunnus. Vain viranomaisen toteuttama ratkaisu rekisteröintimenettelyineen mahdollistaisi tällaisen yksilöllisen identiteetin suomalaisessa yhteiskunnassa. Henkilön yksilöinti osana väestön rekisteröintiä on luonnollisesti viranomaisen, tässä tapauksessa Digi- ja väestötietoviraston erioikeuksiin kuuluvaa toimintaa.

Sen lisäksi että ulkomaalaisen asiointivälineellä olisi mahdollista asioida viranomaisten kanssa, lainsäädäntö mahdollistaisi, että se olisi käytettävissä yksityisissä asiointipalveluissa. Kuitenkin, mikään muu toimija kuin viranomainen ei voisi tuottaa edellä kuvatulla tavalla yksilöivää, väestön rekisteröintiin perustuvaa asiointivälinettä. Johtuen toiminnan kiinteästä yhteydestä väestön rekisteröintiin, olisi kysymys toiminnasta, joka on luontaisesti osa viranomaisten erioikeuksia – ei lähtökohtaisesti taloudellisesta toiminnasta.

Ydinidentiteetin todiste toimisi teknisesti luotettavana tapana osoittaa, että todistetta hallitsevalle henkilölle on väestötietojärjestelmään rekisteröity ydinidentiteetin sisältämä henkilöllisyys. Ydinidentiteetin todiste sisältyisi digitaaliseen henkilöllisyystodistukseen ja ulkomaalaisen digitaaliseen asiointivälineeseen. Kun väestötietojärjestelmän ylläpitäminen ja väestön rekisteröinti kuuluvat viranomaisen tehtäviin, on ydinidentiteetin todisteen myöntämistä pidettävä viranomaistehtävän erottamattomana osana.

Luonnollisen henkilön tunnistusvälineen osalta kysymys on fyysisestä välineestä, joka on käytettävissä ilman mobiilipäätelaitetta tai sirukorttia, ja jonka ainoa käyttötarkoitus on mahdollistaa henkilön sähköinen asiointi suomalaisten viranomaisten kanssa. Luonnollisen henkilön tunnistusvälineen osalta voidaan arvioida sen vaikutusta välineen tarjoamiseen tarvittavien laitteiden markkinaa sekä sähköisen asioinnin markkinaa. Digi- ja väestörekisteriviranomainen hankkisi laitteet rajapintaratkaisuihin tavanomaisen julkisen hankintamenettelyn perusteella eli markkinaehtoisesti. Luonnollisen henkilön tunnistusvälinettä ei tarjottaisi käytettäväksi tunnistus- ja luottamuspalvelulaisissa säädetyn vahvan sähköisen tunnistamisen markkinamekanismin kautta, ja se jäisi siten vahvan sähköisen asioinnin markkinoiden ulkopuolelle. Olennaista on, että välineen käyttö olisi rajattu vain julkisen sektorin asiointipalveluihin, joiden osalta viranomaisilla on velvollisuus tarjota palvelunsa myös sähköisesti. Luonnollisen henkilön tunnistusvälineen osalta on kuitenkin mahdollista, että toimintaa olisi arvioitava taloudellisena, joten tältä osin kilpailuvaikutuksia arvioidaan vielä tarkemmin jäljempänä.

Sähköinen asiointi, käyntiasiointi ja niihin liittyvien rajapintojen kilpailuvaikutusten arviointi

Digitaalisen henkilöllisyyden sovellus voisi sisältää joko digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen. Digitaalisen henkilöllisyyden sovelluksella ja luonnollisen henkilön tunnistusvälineellä voitaisiin asioida sähköisesti. Vahvalle sähköiselle tunnistamiselle sähköisessä asioinnissa on Suomessa luotu kilpaillut markkinat tunnistus- ja luottamuspalvelulaila. Markkinoiden olemassaolosta ei kuitenkaan yksiselitteisesti ja väistämättä voida johtaa päätelmää siitä, että luonnollisen henkilön tunnistusvälineen tai digitaalisen henkilöllisyyden sovelluksen tarjoamisen olisi katsottava olevan taloudellista toimintaa. Komission päätös SA.25745 koski Saksan konkurssihuutokauppojen internet-sivustoa ja siinä komissio totesi, ettei viranomaisen toimintaa ole katsottava automaattisesti luonteeltaan taloudelliseksi, vaikka se tulee markkinoille, joilla yksityiset jo toimivat. Komission esittämän näemyksen mukaan viranomainen ei luovu oikeudestaan harjoittaa julkisen vallan käyttöä vastaavaa toimintaa, vaikka yksityiset toimijat olisivatkin olleet nopeampia tarjoamaan tällaisia palveluita. Toinen komission päätös SA.34646 koski valitusta Alankomaiden perustamasta internetpalvelusta, jonka kautta julkiset hankinnat voitiin toteuttaa. Laissa oli asetettu viranomaiselle

velvollisuus, jonka täyttämistä viranomaisen tuottamalla palvelulla huolehdittiin. Tällaisen velvoitteen toteuttamista ei pidetty luonteeltaan taloudellisena, vaan julkisen vallan käyttönä.

Edellä esitettyjen ratkaisujen perusteella voidaan nähdä, että tunnistuspalveluiden tarjoaminen julkisen sektorin sähköisiin asiointipalveluihin voisi, vaikka markkinoilla on vastaavaa yksityistä toimintaa, jäädä taloudellisen toiminnan käsitteen ulkopuolelle. Viranomaiselle on asetettu digipalvelulaissa lähtökohtainen velvoite tuottaa palvelunsa myös sähköisesti ja tähän kokonaisuuteen voidaan tulkita kuuluvan myös velvoite mahdollistaa kaikille pääsy sähköisiin asiointipalveluihin. Kaikilla julkisen hallinnon asiakkaila ei syystä tai toisesta ole mahdollisuutta saada markkinaehtoisesti tuotettuja tunnistusvälineitä, joten viranomaisen tulisi viime kädessä mahdollistaa luonnollisen henkilön tunnistusvälineen avulla kaikille mahdollisuus saada tunnistusväline viranomaisen sähköisiin palveluihin.

Luonnollisen henkilön tunnistusväline vastaa ominaisuuksiltaan lähtökohtaisesti nykyisessä luottamusverkostossa saatavilla olevia tunnistusvälineitä, eikä sillä ole digitaalista henkilöllisyystodistusta vastaavaa kiinteää yhteyttä virallisten henkilöllisyyttä osoittavien asiakirjojen myöntämiseen tai väestön rekisteröinnin viranomaistehtäviin. Kysymys olisi siten lähtökohtaisesti taloudellisesta toiminnasta, mikäli välinettä tarjottaisiin markkinoille käytettäväksi asiointipalveluissa.

Ehdotuksen mukaan luonnollisen henkilön tunnistusvälinettä voitaisiin kuitenkin käyttää ainoastaan viranomaisten asiointipalveluissa. Se ei tulisi luottamusverkostoon tai muuten käytettäväksi yksityisen sektorin asiointipalveluissa, eikä siten suoraan kilpailisi markkinoilla olevien muiden tunnistusvälineiden kanssa. Kun luonnollisen henkilön tunnistusväline on tarkoitettu henkilöille, jotka eivät pysty käyttämään sovelluspohjaista tunnistusvälinettä, on sen kohde-ryhmä varsin rajoitettu.

Kuluttajien kannalta valtion tarjoaman luonnollisen henkilön tunnistusväline merkitsisi, että luottamusverkoston kautta saatavilla olevien vahvojen sähköisten tunnistusvälineiden lisäksi käytettävissä olisi uusi fyysinen ja saavutettava tunnistusväline, jolla olisi kuitenkin mahdollista asioida ainoastaan viranomaisten kanssa. Kuluttajien valinnanvara parantuisi näin ollen, kun valtio samanaikaisesti edelleen mahdollistaisi asiointin luottamusverkostossa olevilla vahvan sähköisen asiointin välineillä. Tällä hetkellä ensisijaisesti pankit tarjoavat tällaisia saavutettavia vaihtoehtoisia tunnistusvälineitä joita voidaan käyttää kaikissa asiointipalveluissa, niin julkisissa kuin yksityisissä. Voidaan siten arvioida, että niissä tilanteissa, joissa kuluttajalla on mahdollisuus käyttää pankin tunnistusvälinettä julkisissa asiointipalveluissa, kysyntä valtion tarjoamalle luonnollisen henkilön tunnistusvälineelle jäisi pieneksi. Valtion kannalta on kuitenkin tärkeää varmistaa, että henkilöillä on mahdollisuus asioida viranomaisilla ilman, että heiltä edellytetään pankin tai muun yksityisen tahon asiakkuutta myös silloin, kun he eivät halua tai voi käyttää sovelluspohjaista tunnistusvälinettä. Kysymys on tältä osin yhdenvertaisuusperiaatteen toteuttamisesta. Niille kuluttajille, jotka tarvitsevat tällaista vaihtoehtoista tunnistusvälinettä asioidakseen sähköisesti viranomaisella, tarjoutuisi näin ollen uusi vaihtoehto. Voidaan pitää epätodennäköisenä, että valtion tuottamalla luonnollisen henkilön tunnistusvälineellä olisi merkittävää vaikutusta nykyiseen luottamusverkostomarkkinan toimintaan.

Digitaalisen henkilöllisyyden sovelluksen avulla olisi mahdollista käyttää sekä digitaalista henkilöllisyystodistusta että ulkomaalaisen digitaalista asiointivälinettä. Digitaalisen henkilöllisyyden sovelluksella olisi mahdollista asioida sähköisesti, ja sikäli kuin on kysymys passin tai henkilökortin lisäpalveluna myönnettävästä digitaalisesta henkilöllisyystodistuksesta, myös sen käyttäminen käyntiasioinnin yhteydessä olisi mahdollista. Digitaalisen henkilöllisyystodistuksen käyttäminen asioidessa paikan päällä viranomaisen luona eli käyntiasioinnin yhteydessä

edellyttää, että mobiilisovelluksen käyttörajapinta sen mahdollistaa, ja että henkilöllisyydestä voidaan varmistua tietoturvallisesti lukijarajapinnan avulla.

Lienee mahdollista katsoa, että sellaisen digitaalisen rajapinnan luominen digitaalisen henkilöllisyyden sovellukseen, joka mahdollistaa henkilöllisyyden todentamisen, kuuluu erottamattomana osana henkilöllisyystodistuksen myöntämiseen, sillä henkilöllisyystodistus menettäisi käytännössä merkityksensä, jos sitä ei pystyisi käyntiasioinnin yhteydessä lukemaan tai muulla tavalla todentamaan.

Digitaalisen henkilöllisyyden sovelluksesta erillisenä asiana on arvioitava lukijarajapinta ja lukijarajapinnan sisältävän tarkastussovelluksen tuottaminen. Lukijarajapinnan ja tarkastussovelluksen tarkemmat määritykset määritteli Digi- ja väestötietovirasto tietoturvalisuusvaatimuksesta aiheutuvista syistä. Lakiehdotuksen mukaan Digi- ja väestötietovirasto velvoitettaisiin myös tuottamaan yksi sellainen tarkastussovellus, jonka avulla henkilöllisyystodistus voidaan lukea. Tarkastussovellus olisi vapaasti kaikkien halukkaiden saatavilla korvauksetta.

Myös muut kuin Digi- ja väestötietovirasto voisivat kehittää Digi- ja väestötietoviraston määrittelemiä teknisiä vaatimuksia täyttäviä tarkastussovelluksia. Tarkastussovelluksen tuottaminen voidaan siten mahdollisesti pitää taloudellisena toimintana. Kun tarkastussovellus tuotettaisiin julkisena hankintana, voidaan sen tuottaminen kuitenkin joka tapauksessa katsoa tapahtuvan markkinaehtoisesti.

Tällä hetkellä markkinoilla ei ainakaan Suomessa vaikuttaisi olevan soveltuvia digitaalisen henkilökortin tai digitaalisen passin tarkastussovelluksia. Ehdotuksella ei siten arvioida olevan kielteisiä vaikutuksia olemassa olevilla tarkastussovellusten markkinoilla. Voidaan pitää mahdollisena tai jopa todennäköisenä, että vastaisuudessa markkinoille tulisi muita kuin Digi- ja väestötietoviraston tuottamia tarkastussovelluksia. Toisaalta on tässä yhteydessä todettava, että itse tarkastussovelluksen kaupallinen merkitys todennäköisesti on vähäinen, ja on oletettavaa, että sopivia tarkastussovelluksia pikemminkin syntyy oheistuotteina muille palveluille.

Digitaaliseen henkilöllisyystodistukseen liittyvän sähköisen asioinnin ratkaisun osalta voidaan todeta, että ratkaisu on verrannollinen käyntiasioinnissakin käytettyyn ratkaisuun. Kuten käyntiasioinninkin osalta myös sähköisen asioinnin osalta sähköisen asioinnin rajapinnan tuottamista voidaan pitää erottamattomana osana viranomaisen toimintaa ja mahdollisuutta käyttää digitaalista henkilöllisyystodistusta.

Tuottaessaan henkilölle digitaalisen henkilöllisyystodistuksen, josta todistuksen vahvistetut tiedot voidaan esittää myös digitaalisesti sähköisessä asiointissa, viranomainen rekisteröi henkilön identiteettiä koskevat ydintiedot, varmentaa henkilöllisyyden kasvotusten ja myöntää henkilölle ydinidentiteetin todisteen, josta tämä luonnolliseen henkilöön liitetty identiteetti voidaan todentaa. Nämä olisivat kaikki laissa säädettyjä viranomaisen tehtäviä. Samaten kuin käyntiasioinnissa digitaalisen henkilöllisyystodistuksen käyttö siten, että on mahdollista todentaa henkilön itse esittämät vahvistetut tiedot asioinnin yhteydessä, on mahdollista vain, jos henkilöllisyystodistuksessa on sen sähköiseen lukemiseen tarvittava rajapinta. Tarvittavan rajapinnan määrittelemisen voidaan siksi nähdä luonnollisena ja välttämättömänä jatkumona ydinidentiteetin todisteen ja digitaalisen henkilöllisyystodistuksen myöntämiselle siten, että kyse on edelleen julkisen vallan käytöstä.

Koska digitaalista henkilöllisyystodistusta voidaan käyttää sähköiseen asiointiin, sillä voi olla vaikutusta sähköistä asiointia koskevien tunnistamismarkkinoiden toimintaan. Kysymys on tällöin välillisistä vaikutuksista tunnistus- ja luottamuspalvelulaissa säänneltyyn markkinaan. Jos henkilöt ottaisivat digitaalista henkilöllisyystodistusta laajasti käyttöön, voisi tämä vähentää

olemassa olevien sähköisten tunnistusvälineiden käyttöä, millä olisi vaikutusta tunnistusvälityspalveluiden tarjoajien ja tunnistusvälineiden tarjoajien liiketoimintaan. Kyseinen toiminta ja ehdotettu sääntely vastaavat tältä osin kuitenkin jo kansalaisvarmennetta koskevaa sääntelyä, joka tarjotaan luottamusverkoston kautta asiointipalvelulle, ja jonka osalta on pidetty selvänä, että kysymys on julkisen vallan käytöstä (HE 36/2009 vp, s.87). Myös Valtiontalouden tarkastusvirasto on tunnistuspalveluiden kehittämisestä ja käytöstä julkisessa hallinnossa antamassaan raportissa (161/2008) katsonut, että Väestörekisterikeskuksen kansalaisvarmennetoiminnassa on kyse viranomaistoiminnoista, kun taas muu laatuvarmenteiden tai muiden varmenteiden liikkeelle lasku ei tätä ole. Myös ulkomaalaisen digitaalisen asiointivälineen osalta arvioitiin edellä, että asiointivälineen myöntämisen voidaan katsoa olevan viranomaisen erioikeuksien piiriin kuuluvaa toimintaa. Samaten kuin digitaalisen henkilöllisyystodistuksen osalta välineen käyttämisen mahdollistaminen sähköisessä asiointissa voidaan katsoa olevan erottamaton osa viranomaisen toimintaa.

Samankaltaisella tavalla kuin kansalaisvarmenteenkin osalta esityksellä mahdollistettaisiin se, että digitaalista henkilöllisyystodistus voitaisiin ottaa käyttöön myös yksityisissä asiointipalveluissa. Myös ulkomaalaisen digitaalinen asiointiväline olisi mahdollista ottaa käyttöön yksityisissä asiointipalveluissa. Siinäkin tapauksessa, että digitaalisen henkilöllisyystodistuksen käytön mahdollistaminen myös yksityisissä asiointipalveluissa katsottaisiin olevan taloudellista toimintaa, ei sen tarjoaminen käytettäväksi välttämättä olisi valtiontuki- ja kilpailulainsäädännön kannalta ongelmallista. Tässä tapauksessa olisi huomioitava, että ehdotuksen mukaan digitaalisen henkilöllisyystodistuksen rajapinta olisi avoin ja maksuton, jolloin asiointipalvelut voisivat kytkeytyä siihen suoraan tai tunnistusvälityspalvelun tarjoajien rakentamien rajapintojen kautta. Kilpailuvaikutusten osalta on siten mahdollista, että tunnistusvälityspalvelun tarjoajille syntyisi ehdotuksen perusteella uutta liiketoimintaa.

Ei ole kaikilta osin yksiselitteistä verrata digitaalisen henkilöllisyyden sovelluksen käyttöä sähköisessä asiointissa nykyisiin tunnistusmarkkinoihin, sillä digitaalisen henkilöllisyyden sovellus poikkeaa useassa suhteessa nykyisistä tunnistusvälinemarkkinoilla olevista ratkaisuista. Ensinnäkin digitaalisen henkilöllisyyden sovellus perustuu henkilön itse hallinnoimaan identiteettiin. Tämä merkitsee käytännössä, että tunnistautumisen yhteydessä sovelluksesta välittyvät tiedot eivät vastaa sitä tietokokonaisuutta mikä nykyisin välittyy tunnistus- ja luottamuspalvelulain säännösten perusteella. Toiseksi tunnistusvälineen (eli digitaalisen henkilöllisyyden sovelluksen) tarjoajan ei ole mahdollista velottaa tunnistustapahtumakohtaista hintaa, sillä tunnistusvälineen tarjoajalle ei tule tietoa siitä, kun henkilö käyttää digitaalisen henkilöllisyyden sovellusta sähköiseen asiointiin. Tieto välittyy ainoastaan sovelluksesta asiointipalvelulle.

Sikäli kuin lukijarajapinnan käyttäminen edellyttäisi investointeja laitteisiin, kuten älypuheliin tai erillisiin digitaalisten henkilöllisyystodistusten lukulaitteisiin, ne ovat saatavilla markkinoilta, eikä niiden tarjoamisesta säädettäisi lailla. Julkiset asiointipalvelut hankkisivat tarvittavan laitteiston markkinoilta kilpailuttamalla. Samaten tarvittavat tietoliikenneyhteydet olisivat saatavilla vapailta markkinoilta. Ehdotuksella ei myöskään olisi vaikutusta mahdollisuuteen tarjota tunnistamispalveluita tunnistus- ja luottamuspalvelulain sääntelemän markkinan ulkopuolella.

Yhteenveto palvelujen tarjoamisen luonteesta

Edellä kuvatuin perustein voidaan katsoa, että poliisi ja Digi- ja väestötietovirasto toimivat viranomaisen ominaisuudessa, kun ne tuottavat digitaalisen henkilöllisyystodistuksen ja sen käytön mahdollistavia palveluita. Digitaalinen henkilöllisyystodistus olisi henkilöllisyyttä osoitta-

vana asiakirjana, ja henkilökorttiin ja passiin kiinteästi kytkeytyvänä lisäpalveluna, julkisen vallan käytön piirissä, eikä toimintaa siten voida katsoa taloudelliseksi. Henkilöllisyyttä osoittavan asiakirjan myöntäminen ja sen käytön mahdollistaminen yhteiskunnassa on luonnollisesti viranomaisen, tässä tapauksessa poliisin erioikeuksiin kuuluvaa toimintaa.

Digi- ja väestötietoviraston toimintaa digitaalisen henkilöllisyyden tietojärjestelmästä, ydinidentiteetin todisteesta, ulkomaalaisen digitaalisesta asiointivälineestä, digitaalisen henkilöllisyyden hallintapalvelusta, lukijarajapinnasta ja tarkastussovelluksesta koostuvan digitaalisen henkilöllisyyden palveluiden ja digitaalisen henkilöllisyyden sovelluksen tuottamiseksi voidaan pitää julkisen vallan käyttöön tai viranomaisen erioikeuksiin kuuluvaa toimintaa erottamattomasti kuuluvina tehtävinä. Vastaavasti Digi- ja väestötietoviraston kansalaisvarmenteita koskevaa palvelun tarjontaa on pidetty julkisen vallan käyttönä eikä kansalaisvarmentetta ole pidetty taloudellisenä toimintana, vaan julkisen vallan käyttönä tunnistusvälineen tarjoamisessa (HE 36/2009 vp, s.87 sekä PeVL 2/2002). Kansalaisvarmenteen tuottaminen on henkilökorttilaissa sidottu henkilökorttiin.

4.2.1.5 Vaikutukset tunnistusmarkkinoiden kehittymiseen

Esityksellä on arvioitu olevan vaikutuksia nykyisten tunnistusmarkkinoiden osapuoliin, mutta valmistelun yhteydessä on myös tunnistettu, että toimintaympäristö on laajemmin muutoksen ja kehityksen kohteena. On esimerkiksi oletettavaa, että ero sähköisen asioinnin ja käyntiasioinnin välillä tulevaisuudessa vähenee tai poistuu. Lisäksi henkilön mahdollisuus itse määritellä itsestään annettavat tiedot yhdistettynä tiedon minimoimisen periaatteen kanssa johtaa itsehallittavan identiteetin merkityksen kasvamiseen. Pitkällä tähtäimellä voidaan näin arvioida, että nykyiseen tunnistus- ja luottamuspalvelulakiin perustuvien markkinoiden tilalle tulevat mahdollisesti kehittymään uudenlaiset tunnistautumisen ja vahvistettujen tietojen markkinat. Muutoksen nopeuteen ja suuntaan vaikuttaa merkittävässä määrin EU:n eIDAS-muutosehdotus, jolla luodaan yhteinen lainsäädäntö eurooppalaisille digitaalisen identiteetin lompakko-sovelluksille. eIDAS-muutosehdotuksen sisältöä on kuvattu tarkemmin esityksen jaksossa 2.6.

Esityksen mukainen digitaalisen henkilöllisyyden sovellus ei itsessään vielä muodosta digitaalista lompakkoa. Vasta sen jälkeen kun eIDAS-muutosehdotus on hyväksytty, on mahdollista ryhtyä toimeen asetuksen täytäntöön panemiseksi. Tämänhetkisen asetusluonnoksen mukaan vaikuttaa siltä, että jäsenvaltioille tulee velvollisuus tuottaa vähintään yksi asetuksen vaatimukset täyttävä lompakko-sovellus. Säänneltyjen markkinoiden puuttuessa toimijat voivat tällä hetkellä kehittää vapaasti omia lompakko-sovelluksia ja vastaavia ratkaisuja, mutta lainsäädännöllisiä raameja niiden hyväksynnälle ja luottamukselle ei vielä ole.

Esitys ei sisällä ehdotusta ydinidentiteetin todisteiden myöntämiseksi yksityisille palveluntarjoajille liitettäväksi mahdollisiin kehitteillä oleviin yksityisiin lompakoihin. Toisaalta toimijoilla on jo nyt mahdollisuus tuottaa digitaalisia identiteettilompakoita, joka sisältää kyseisen toimijan hallinnoiman identiteetin ja jotka voivat nojautua Digi- ja väestötietoviraston tuottamiin VTJ-tietopalveluissa rekisteröityihin tietoihin. Tällä hetkellä onkin vireillä kehitystyötä eri toimialoilla identiteettilompakkoratkaisujen kehittämiseksi. Uusia tunnistautumISRatkaisuja kehitetään esimerkiksi Suomen tunnistautumisosuuskunnassa. Esityksen mukaan valtion tuottama digitaalinen henkilöllisyystodistus ja ulkomaalaisen digitaalinen asiointiväline olisi mahdollista ottaa käyttöön yksityisissä asiointipalveluissa, mikäli ne näin päättäisivät, joko kytkeytymällä suoraan valtion tarjoamaan rajapintaan tai tunnistusvälityspalvelun tarjoaman ratkaisun välityksellä, mutta väline ei olisi osa kansallista luottamusverkostoa, kuten eivät olisi myöskään mahdolliset yksityisten toimijoiden toteuttamat uudentyyppiset asiointivälineet.

Esityksen valmistelun aikana on mahdollisimman pitkälti pyritty ottamaan huomioon myös edellä kuvattu markkinoiden kehitys ja itsehallittavan identiteetin periaatteeseen perustuvien lompakkosovellusten tarjoaminen, siten, ettei syntyisi päällekkäistä kehitystyötä ja ylimääräisiä kustannuksia. Toisaalta eräänä kansallisen kehitystyön lähtökohtana on ollut luoda edellytyksiä lompakkosovellusten tarjoamiseen tulevaisuudessa siten, että eIDAS-muutosehdotuksen hyväksymisen jälkeen ehditään ajoissa toimeenpanna jäsenvaltioille tulevia velvoitteita. Lähtökohtaisesti on pyritty siihen, ettei valtion toimenpiteillä vaikeuteta yksityisten toimijoiden itsestä kehitystyötä tai luoda sääntelyä, teknisiä ratkaisuja tai organisatorisia rakenteita, jotka voisivat olla ristiriidassa eIDAS-muutosehdotuksen kanssa. eIDAS-muutosehdotuksen mukaan niin julkiset viranomaiset kuin yksityiset toimijat voisivat toimia lompakkosovellusten tarjoajina.

Kun arvioidaan esityksen vaikutusta markkinoiden kehitykseen, voidaan pitää mahdollisena, että markkinaosapuolten investoinnit nykyisiin tunnistusmarkkinoihin vähenevät. Tähän vaikuttavat kuitenkin esitetyjen ratkaisujen lisäksi yleinen sähköiseen asiointiin liittyvien ratkaisujen ja markkinoiden kehitys, esimerkkinä EU-tason lompakkosovelluksia koskeva kehitys. Kun valtio myös jatkossa mahdollistaisi sähköisen asiointin nykyisillä sähköisillä tunnistusvälineillä, olisi markkinoiden mahdollinen siirtymä varsin hallittua.

Ehdotuksen mukainen ratkaisu voidaan nähdä yhtenä askeleena kohti identiteettilompakkoihin perustuvia toimintamalleja ja se edesauttaa sitä, että Suomessa voidaan toimeenpanna eIDAS-muutosehdotuksen edellyttämät muutokset ja täyttää sen asettamat velvoitteet ripeästi asetuksen hyväksymisen jälkeen. Tämän voidaan arvioida edistävän myös yksityisten tunnistusvälineiden ja tunnistusvälityspalveluiden oikea-aikaista markkinoillepääsyä, sikäli kun ne tulevat olemaan riippuvaisia valtion tarjoamista perusratkaisuista kuten ydinidentiteetin todisteesta.

4.2.1.6 Vaikutukset sisämarkkinoihin

Ehdotuksilla on eräiltä osin vaikutuksia sisämarkkinoiden toimintaan. Sisämarkkinanäkökulmasta kansallinen digitaalinen henkilöllisyysratkaisu sekä ulkomaalaisen digitaalinen asiointiväline ovat tekijöitä rajat ylittävän sähköisen tunnistamisen mahdollistamiseksi tulevaisuudessa. Vaikka kyse on ensimmäisessä vaiheessa kansallisista ratkaisuista, ne pohjautuvat tulevaisuuden ratkaisuja valmistauduttaessa eIDAS-muutosehdotukseen ja sen pohjalta kehitettävään uudenlaisiin rajat ylittävään käyttöön tarkoitettuihin henkilöllisyyden ja vahvistettujen tietojen hallintaan liittyviin ratkaisuihin.

Moni jo voimassa oleva EU-säädös lähtee siitä, että sähköiset asiointipalvelut tulisi olla myös muiden kuin suomalaisten käyttäjien käytettävissä, ja toisaalta muiden jäsenvaltioiden asiointipalvelut tulisi olla suomalaisten käyttäjien käytettävissä. Tällaisia EU-säädöksiä ovat muun muassa yhteisestä digitaalisesta palveluväylästä annettu asetus ((EU) 2018/1724), palveluista sisämarkkinoilla annettu direktiivi (2006/123/EY) sekä digitaalisten välineiden ja prosessien käytöstä yhtiöoikeuden alalla annettu direktiivi (2019/1151). Ehdotetut ratkaisut ovat osa kehitystä, jolla Suomessa tavoitellaan toimivia eIDAS-muutosehdotuksen edellyttämiä rajat ylittävän asiointin ratkaisuja. Tavoitteena on, että yksi tai useampi ehdotuksen mukainen ratkaisu tulisi notifioidaan eIDAS-asetuksen mukaisessa menettelyssä, mahdollistaen sen, että Suomen kansalaiset ja suomalaiset elinkeinonharjoittajat voivat tunnistaautua muiden jäsenvaltioiden viranomaisten palveluihin siltä osin, kun ne ovat saatavilla rajat ylittävälle käyttäjille. Tällä hetkellä suomalaisilla ei ole käytössään tunnistusvälinettä, joka mahdollistaa rajat ylittävän sähköisen tunnistautumisen.

Jotta ulkomailla asuvat suomalaiset ja ulkomaalaiset henkilöt voivat käyttää digitaalisia asiointipalveluita, tulisi heidän yksilöintinsä olla mahdollista. Maahantulovaiheen sujuvuus on olennainen osa kansainvälisten osajien houkuttelua. Työn tai opiskelupaikan hakeminen ulkomailta käsin on kuitenkin haasteellista, sillä tietyt viranomaispalvelut edellyttävät vahvaa sähköistä tunnistautumista. Kansallinen digitaalinen henkilöllisyysratkaisu sekä ulkomaalaisen digitaalinen asiointiväline voisivat tarjota ratkaisuja myös tähän haasteeseen ja siten edistää työntekijöiden liikkuvuutta.

Ehdotuksilla voidaan nähdä olevan vaikutuksia kansalaisten ja elinkeinonharjoittajien vapaan liikkuvuuden parantamiseen sisämarkkinoilla, jos ehdotuksen mukaiset sähköisen tunnistautumisen ratkaisut mahdollistavat viranomaisten digitaalisten asiointipalveluiden paremman käytön koko EU:n alueella. Tämä tukee osaltaan myös yritysten kilpailukyvyyn ja kasvumahdollisuuksien kehittymistä sisämarkkinoilla, jos yritysten pääsy muiden jäsenmaiden markkinoille helpottuu. Kansalaisten vapaan liikkuvuuden mahdollisuuksien parantumisella voi olla positiivisia vaikutuksia muun muassa osaamiseen ja työvoiman saatavuuteen.

4.2.1.7 Vaikutukset julkiseen talouteen

Yleisesti

Ehdotuksella on vaikutuksia julkiseen talouteen. Suunniteltujen ratkaisujen toteutuskustannusten arvioidaan olevan yhteensä noin 17,5 miljoonaa euroa ja vuotuisten käyttökulujen yhteensä noin 7 miljoonaa euroa. Osa ehdotukseen liittyvistä ylläpitokustannuksista on tarkoitus kattaa toimintaan liittyvillä asiakasmaksuilla ja osa palveluiden kustannuksista esitetään katettavaksi osin budjettirahoitteisena. Ehdotuksella arvioidaan olevan vaikutuksia toteuttavien viranomaisten määrärahatarpeeseen.

Ehdotuksen toteutuskustannukset katetaan valtiovarainministeriölle vuoden 2020 talousarviossa myönnetystä määrärahasta (28.70.01).

Digitaalisen henkilöllisyyden ratkaisuihin liittyvän ydinidentiteetin todisteen ylläpito katettaisiin kokonaan valtion budjetista. Tämä ydinidentiteetin todiste (varmenne) olisi digitaalisen henkilöllisyyden ratkaisujen välttämätön osa, ja sitä olisi tulevaisuudessa mahdollista hyödyntää myös mahdollisen tulevan eIDAS-muutosehdotuksen mukaisen lompakkosovelluksen perustana. Vielä valmistelussa oleva EU-lainsäädäntö tulee todennäköisesti linjaamaan, että lompakkosovelluksen käytön tulisi olla käyttäjälle maksutonta, silloin kun lompakkosovelluksen käyttäjä on luonnollinen henkilö. Ydinidentiteetin todisteen ylläpidon on arvioitu aiheuttavan Digi- ja väestötietovirastolle vuodesta 2023 alkaen 2 miljoonan euron vuosittaiset kustannukset, jotka kohdistuisivat valtiovarainministeriön hallinnonalalle momentille 28.30.03. Digi- ja väestötietoviraston toimintamenot (siirtomääräraha 2 v).

Luonnollisen henkilön tunnistusvälineen ylläpidon kustannukset esitetään katettavaksi osittain valtion budjetista niin, että välinettä tarjotaan alennetun omakustannusarvon suoritteena eli asiakashintaa subventoidaan sen jatkuvien kustannusten osalta siten että luonnollisen henkilön tunnistusvälineen asiakasmaksu asettuisi 10 euron ja 20 euron välille. Tämä aiheuttaisi Digi- ja väestötietovirastolle vuodesta 2023 alkaen arviolta enintään 1 miljoonan euron vuosittaiset kustannukset, jotka kohdistuisivat valtiovarainministeriön hallinnonalalle momentille 28.30.03. Digi- ja väestötietoviraston toimintamenot (siirtomääräraha 2 v).

Ehdotuksen vaikutuksia toteuttavien viranomaisten näkökulmasta arvioidaan tarkemmin alla toimijakohtaisesti. Ehdotuksesta ei arvioida aiheutuvan välittömiä vaikutuksia ratkaisua mahdollisesti hyödyntävien viranomaisten määrärahoihin, koska käyttöönotto perustuu vapaaehtoisuuteen. Näiden muiden viranomaisten määrärahatarpeet tulisi käsitellä erikseen osana julkisen talouden suunnitelmaa ja talousarviovalmistelua. Sähköisen asioinnin osalta ratkaisut olisivat hyödynnettävissä suomi.fi –tunnistamisen kautta ilman erillisiä tietojärjestelmämuutoksia. Käyntiasioinnissa ratkaisua käyttöönotettaessa kustannuksia syntyy tarvittavien lukijalaitteiden tai mobiililaitteiden hankinnasta sekä tarkastusrajoituksen mahdollisista integroinneista asiakasjärjestelmiin. Näitä harkinnanvaraisia kustannuksia on arvioitu sähköisten asiointipalveluiden näkökulmasta tarkemmin jaksossa 4.2.1.3.

Digi- ja väestötietovirasto

Digitaalisen henkilöllisyystodistuksen ja siihen liittyvien palvelujen, ulkomaalaisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen kehityskustannusten arvioidaan olevan Digi- ja väestötietoviraston osalta noin 16 miljoonaa euroa. Kehityskustannukset katetaan valtiovarainministeriölle vuoden 2020 talousarvioesityksessä myönnetystä määrärahasta. Digitaalisen henkilöllisyystodistuksen käyttöönoton jälkeisinä ensimmäisinä vuosina ratkaisun jatkokehitys ja käyttöönottojen tehostettu tuki aiheuttaisivat arviolta 1–2 miljoonan euron lisäkustannukset vuosittain.

Digitaalisen henkilöllisyyden vuotuisista käyttökustannuksista esitetään keskistetyksi katettavaksi 3–3,5 miljoonaa euroa, josta noin 2 miljoonaa euroa kohdistuisi digitaalisen henkilöllisyystodistuksen ja siihen liittyvien palvelujen kustannusten kattamiseen Digi- ja väestötietoviraston toimintamenojärjestelmälle myönnettävästä määrärahasta ja luonnollisen henkilön tunnistusvälineen kustannusten kattamiseen esitetään enintään yhden miljoonan euron vuositaita arviomäärärahaa. Määrärahatarpeet huomioitaisiin vuoden 2023 talousarvioesityksestä alkaen.

Luonnollisen henkilön tunnistusvälineen ylläpidon kustannukset esitetään katettavaksi osittain valtion budjetista niin, että välinettä tarjotaan alennetun omakustannusarvon suoritteena eli asiakashintaa subventoidaan sen jatkuvien kustannusten osalta. Luonnollisen henkilön tunnistusvälineen ja siihen liittyvien palveluiden vuosikustannukset riippuvat jonkin verran käyttäjämääristä. Palvelun toteuttamiskuluiksi on arvioitu noin 750 000 euroa sekä kiinteiksi kustannuksiksi on arvioitu noin 461 000 euroa vuodessa. Digi- ja väestötietoviraston arvion mukaan 30 000 käyttäjällä luonnollisen henkilön tunnistusvälineen tuottamisen ja tarjoamisen kustannukset olisivat noin 600 000 euroa vuodessa. Esityksen valmistelussa on arvioitu, että luonnollisen henkilön tunnistusvälineen asiakasmaksu tulisi asettua 10 euron ja 20 euron välille, joka olisi suunnilleen samalla tasolla markkinoilla olevien yksityisen sektorin tarjoamien vastaavien välineiden kanssa. Digi- ja väestötietovirastolle esitetään tätä varten myönnettäväksi enintään 1 miljoonan vuotuinen arviomääräraha, josta voidaan kattaa luonnollisen henkilön tunnistusvälineen tarjoamisesta aiheutuvia kustannuksia.

Ulkomaalaisen digitaalisen asiointivälineen ja siihen liittyvien palvelujen vuosikustannuksiksi on arvioitu noin 1,55 miljoonaa euroa, josta asiakasmaksuilla on esitetty katettavaksi välineen käyttöönottoon ja käyttöön liittyvät ylläpitokustannukset, noin 350 000 euroa vuosittain. Ulkomaalaisen digitaalisen asiointivälineen arvioitu vuosittainen käyttöönottomäärä on noin 64 000 kappaletta, jolloin asiakasmaksun määräksi muodostuisi noin 12–13 euroa yhtä välineen käyttöönottoa kohden.

Ehdotuksella voi olla jonkin julkisen talouden menoja alentavia vaikutuksia Digi- ja väestötietoviraston suomi.fi-tunnistuspalvelun kautta julkisen sektorin organisaatioiden digitaalisiin palveluihin välitettyihin, yksityisiltä vahvan sähköisen tunnistamisen toimijoilta ostettuihin tunnistustapahtumiin ja niistä perittäviin maksuihin. Vaikutus riippuu siitä, kuinka laajasti digitaalista henkilöllisyystodistusta, ulkomaalaisen digitaalista asiointivälinettä tai luonnollisen henkilön tunnistusvälinettä käytettäisiin tunnistustapana julkisiin palveluihin yksityisen sektorin tarjoamien tunnistusvälineiden sijasta.

Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen sekä myöhemmin mahdollisesti kehitettävän eurooppalaisen identiteettilompakon arvioidaan vaikuttavan pitkällä aikavälillä Digi- ja väestötietoviraston väestötietojärjestelmän tietopalveluista yksityiseltä sektorilta saatavaan tulokertymään. Vaikutukset alkavat arviolta vuonna 2025, kun ratkaisun käyttö kuluttajilla on oletettavasti vakiintunut ja palveluntarjoajat ovat integroineet toiminnallisuuden omiin järjestelmiinsä. Kuitenkin palveluntarjoajien on ylläpidettävä rinnakkaisia VTJ-yhteyksiä niiden kuluttaja-asiakkaiden palvelemiseksi, jotka eivät käytä digitaalista identiteettilompakkoa. Tämä lisää palveluntarjoajille kohdistuvia kustannuksia. Arvio Digi- ja väestötietoviraston tulon menetyksistä on alkuvaiheessa noin 50 000 euroa vuodessa. Tulon menetys voi kasvaa myöhemmin, ydintietojen laajentuessa siten, että menetys olisi seuraavilla kehyskausilla jopa 0,5–0,7 miljoonaa euroa.

Poliisi

Digitaalisen henkilöllisyystodistuksen tuottaminen ja käyttöönotto aiheuttavat Poliisille jatkuvia ja kertaluonteisia kustannuksia, jotka katettaisiin osin asiakasmaksuilla, osin valtiovarainministeriölle myönnetystä määrärahasta ja osin poliisin määrärahoista.

Ehdotettu sääntely ei edellytä Poliisin näkökulmasta erillistä päätöksentekoa tai muuta erillistä menettelyä digitaalisen henkilöllisyystodistuksen myöntämisen osalta. Päätös, jolla passi tai henkilökortti myönnetään, sisältää myös hakijalle tulevan oikeuden ottaa käyttöön digitaalinen henkilöllisyystodistus. Siirtymäsäännöksen seurauksena tämä koskee myös ennen lain voimaantuloa myönnettyjä passeja ja henkilökortteja.

Poliisille kohdistuvien digitaaliseen henkilöllisyystodistukseen liittyvien yhteydenottojen määrä on vaikeasti arvioitavissa, koska tähän vaikuttaa sekä välineen käyttäjien määrä, että toteutetun välineen käytettävyys. Määrän ei kuitenkaan uskota ainakaan ensimmäisenä vuonna olevan sellainen, että se edellyttäisi henkilöstöresurssin lisäämistä poliisin neuvontapalveluun. Vähäiseen lisäresurssin tarpeeseen on kuitenkin syytä varautua tulevaisuudessa. Yhteydenottojen määrää voidaan hillitä hyvällä tiedottamisella sekä pitämällä kattavasti asiaa koskevaa tietoa saatavilla verkkosivuilla.

Uuden tunnistamistavan käyttöönotto ja uudet tehtävät edellyttävät uutta laitteistoa sekä henkilöstön koulutusta. Lupatiskoille tulevat lukijalaitteet sekä mobiililaitteisiin asennettava lukijaohjelmisto katetaan valtiovarainministeriölle vuoden 2020 talousarvioesityksessä myönnetystä määrärahasta. Keskeisimmät koulutettavat kokonaisuudet liittyvät digitaalisen henkilöllisyystodistuksen hallintaan käytettävän viranomaisportaalin ja uusien lukijalaitteiden käytön kouluttamiseen. Näiden osalta on keskeistä, että tarvittava koulutusmateriaali ja koulutusympäristöt olisivat käytettävissä mahdollisimman hyvissä ajoin ennen digitaalisen henkilöllisyystodistuksen käyttöönottoa. Kattavampaa koulutusta edellytetään niille poliisin lupahallinnon työntekijöillä, jotka toteuttavat digitaaliseen henkilöllisyystodistukseen liittyviä uusia tehtäviä, eli käyttöönottoa ja peruuttamista. Tämä koskee arviolta 400 henkilöä.

Digitaalisen henkilöllisyystodistuksen vuosittaisesta ylläpidosta syntyy Poliisille kohdistuvia kustannuksia, jotka katettaisiin maksuasetuksen mukaisesti passien ja henkilökorttien asiakasmaksuilla. Digitaalisen henkilöllisyystodistuksen käyttöönotto edellyttää ylläpidon osalta ympärivuorokautista varallaoloa, jotta välineen turvallinen ja luotettava käyttö voidaan taata. Tarvittavaksi henkilöresurssiksi on arvioitu kaksi henkilötyövuotta. Lisäksi varallaolosta aiheutuu erinäisiä muita ylläpitokustannuksia. Ylläpitokustannusten arvioidaan olevan noin 300 000 euroa vuodessa. Arvioitu kustannus kattaa poliisin oman työn lisäksi TUVE Valtorilta ostettavan tuen sekä poliisin sovellustoimittajan kulut.

Arvioitaessa lisätyöstä seuraavia kustannuksia voidaan yksittäisen tunnin hinta laskea seuraavalla tavalla. Yhden henkilötyövuoden hinta matkustusasiakirjaprosessissa on noin 54 000 euroa. Tuntihinta saadaan laskennallisesti käyttäen suhdelukua 1640 tuntia, jolloin tuntihinnaksi saadaan 33 euroa. Lisätyötä aiheutuu siten yllä esitetyn arvion perusteella n. 1800 tuntia, jolloin työmäärän lisääntymistä seuraavat kustannukset ovat 59 400 euroa. Koska peruuttamiseen liittyvä päätöksenteko ei ole lupavaroilla rahoitettavaa toimintaa tulee kyseinen arviolta n. 3300 euron suuruinen summa katettavaksi poliisin määrärahoista. Muilta osin syntyvät kustannukset liittyvät maksullisiin lupiin ja tulee siten vyöryttää myönnettävien lupien hintaan. Passeja ja henkilökortteja tullaan myöntämään vuoden 2023 aikana arviolta 1,1–1,3 miljoonaa kappaletta, joten lisätyön aiheuttama kustannusvaikutus myönnettyä passia ja henkilökorttia kohti on n. 0,04–0,05 euroa.

Ulkoasiainhallinto

Digitaalisen henkilöllisyystodistuksen käyttöönotosta aiheutuu ulkoasiainhallinnolle kertaluonteisia kustannuksia laitehankinnoista.

Ulkoasiainhallinnon osalta on arvioitu QR-lukijalaittehankintojen osalta yksittäisen lukijan hinnaksi noin 300 euroa. Ulkoministeriön näkemyksen mukaan Suomen edustustojen asiakaspalvelupisteessä tulisi kussakin olla ainakin yksi QR-koodilukija ja mahdollisesti edustuston henkilökunnan virkapuhelimissa myös ladattuna ao. lukija-ominaisuus. Lisäksi QR-koodilukija tulisi liittää myös kiertäviin kannettaviin passisalkkuihin. Alustavana arviona kustannukset laitehankinnoista olisivat sadalle kappaleelle noin 30 000 euroa sekä mahdolliset lähetys- ja asennuskulut. Suomen edustustojen palvelupisteisiin tulevat lukijalaitteet sekä mobiililaitteisiin asennettava lukijaohjelmisto katetaan valtiovarainministeriölle vuoden 2020 talousarviossa myönnetystä määrärahasta (28.70.01).

Ulkoasiainhallinnon osalta digitaalisen henkilöllisyystodistuksen pysyvät kustannukset koostuvat lisätyön aiheuttamisista henkilöstökustannuksista asiakaspalvelussa.

Digitaalinen henkilöllisyystodistus tulee todennäköisesti työllistämään Suomen edustustojen asiakaspalvelua enemmän kuin esimerkiksi Suomessa poliisia sen vuoksi, että läheskään kaikilla ulkosuomalaisilla ei ole suomalaisia pankkitunnuksia, mobiilivarmennetta tai henkilökortin kansalaisvarmennetta, jotka mahdollistaisivat digitaalisen henkilöllisyystodistuksen käyttöönoton sähköisesti.

Käyntiasiointia edustustoissa digitaalisen henkilöllisyystodistuksen käyttöönottamiseksi arvioidaan tulevan vuoden 2023 aikana noin 10 000 asiointikertaa. Asiointit keskityisivät erityisesti niiden edustustojen toimipiirien alueille, joissa on paljon ulkosuomalaisia. Jatkossa käyntiasiointin määrän voidaan arvioida tasaantuvan jonkin verran, mutta on kuitenkin vaikea arvioida käyntiasiointien tarkkaa määrää jatkossa. Lisäksi on huomioitava, että asiakasyhteydenottojen

määrä voi suurusluokaltaan vaihdella vuosittain, minkä vuoksi keskimääräistä arvioita vuosittaisten yhteydenottojen määrästä on vaikea tässä vaiheessa esittää. On myös otettava huomioon digitaalisen henkilöllisyystodistuksen voimassaolon määräaikaisuus ja esimerkiksi se, että älypuhelimien rikkoontumisen vuoksi tai vaihtamisen yhteydessä myös digitaalinen henkilöllisyystodistus tulee ottaa käyttöön uudelleen, mikä edellyttää käyntiasiointia edustustossa, jos henkilöllä ei ole suomalaisia pankkitunnuksia, mobiilivarmennetta tai henkilökortin kansalaisvarmennetta. Yksittäisen asiakasyhteydenoton hoitamiseen edustustossa voidaan arvioida kuluvan noin 15 minuuttia, joten vuosittaiseksi työnääräksi muodostuu vuoden 2023 osalta 2500 tuntia. Kustannusarvio 2500 työtunnille laskettuna keskimääräisellä tuntipalkalla 84,50 euroa on 211250 euroa, jolla olisi noin 10–20 euron nostava vaikutus ulkoasiainhallinnon myöntämien passien ja henkilökorttien asiointimaksuihin.

Digitaalisen henkilöllisyystodistuksen käyttöönottoon liittyvästä asiakaspalvelusta aiheutuvat lisämenot kohdentuvat ulkoasiainhallinnon maksulliseen toimintaan ja ne tulisi maksuperustelain mukaisesti kattaa digitaalisen henkilöllisyystodistuksen käyttöönottoon liittyvällä asiointimaksulla. Asiointimaksusta säädettäisiin ulkoministeriön asetuksessa ulkoasiainhallinnon suoritteiden maksullisuudesta (650/2020).

4.2.1.8 Vaikutukset kansantalouteen

Esityksellä ei arvioida olevan vaikutuksia kansantalouteen lyhyellä aikavälillä, mutta pidemmällä aikavälillä ehdotuksella voi olla vähäisiä vaikutuksia. Esityksellä pyritään luomaan pohjaa nykyistä laajemmalle digitaalisten palvelujen käytölle yhteiskunnan eri toimintasektoreilla. Digitaalista henkilöllisyystodistusta ja ydinidentiteetin todistetta koskevilla ehdotuksilla toteutetaan ensimmäisiä askelia kohti itsehallittavaa digitaalista identiteettiä. Ehdotettava toimintamalli muuttaa nykyistä sähköisen tunnistamisen markkinan toimintaideaa, mutta voi samalla luoda nykyistä merkittävästi suurempia vaikutuksia digitaalisen palvelutuotannon osalta sekä esimerkiksi eri kanavissa tapahtuvien asiointien turvallisuuden kohdalla.

Ulkomaalaisen digitaalisen asiointivälineen käyttöönotolla voi olla vaikutusta Suomen houkuttelevuuteen investointikohteena ja ulkomaalaisten asiantuntijoiden kohdemaana, kun helpotetaan investoijien ja maahanmuuttoa harkitsevien asiantuntijoiden sähköisten palvelujen käyttöä.

4.2.2 Vaikutukset viranomaisten toimintaan

4.2.2.1 Vaikutukset tehtäviin ja menettelytapoihin

Ehdotuksilla olisi vaikutuksia henkilöllisyysasiakirjoja nykyisellään myöntävien viranomaisten nykyisiin tehtäviin. Ehdotus digitaalisesta henkilöllisyystodistuksesta toisi uusia tehtäviä poliisille sekä ulkoasiainhallinnolle digitaalisen henkilöllisyystodistuksen myöntämisen osalta.

Ehdotus Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista lisäisi jonkin verran Digi- ja väestötietoviraston tehtäviä nykyisestä. Ehdotuksen merkittävimmät vaikutukset tältä osin liittyvät digitaalisen henkilöllisyyden tietojärjestelmään ja sen hallintaan sekä ulkomaalaisen digitaalisen asiointivälineen tuottamiseen. Digi- ja väestötietoviraston tehtävänä on tuottaa mobiilisovelluksesta ja siihen liittyvästä taustajärjestelmästä koostuvaa digitaalisen henkilöllisyyden tietojärjestelmää, jonka avulla voidaan osoittaa vahvistettuja tietoja sähköisessä asiointissa tai käyntiasioinnissa. Digi- ja väestötietoviraston tehtävänä on myös tuottaa, tarjota ja hallinnoida ydinidentiteetin todistetta, sekä tuottaa ja myöntää ulkomaalaisen digitaalisen asiointiväline. Uusia tehtäviä olisi myös ratkaisujen tuottamiseen liittyvien toiminnallisuuden,

kuten hallintapalvelun, lukijarajapinnan sekä tarkastussovelluksen tuottamisessa. Digi- ja väestötietoviraston tehtävistä säädettäisiin uudessa laissa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista.

Ehdotuksen mukaan digitaalinen henkilöllisyystodistus olisi virallinen, poliisin myöntämä henkilöllisyyttä osoittava asiakirja. Poliisi hyväksyisi digitaalisen henkilöllisyystodistuksen käytön myös passin, henkilökortin tai muiden lupien noutamiseen. Poliisi on arvioinut toimenpiteitä ja vaikutuksia, joita tulisi tehdä digitaalisen henkilöllisyystodistuksen myöntämisen sekä käytön mahdollistamiseksi asioitaessa poliisin kanssa. Vaikutukset liittyvät lähinnä tarvittavien laitteiden hankintaan. Poliisiasemien lupahallinnon asiointipaikoille tulisi hankkia lukijalaitteet, joita voidaan hyödyntää, kun avustetaan digitaalisen henkilöllisyystodistuksen käyttöönotossa sekä digitaalisen henkilöllisyystodistuksen tarkastamiseen, kun se esitetään henkilöllisyyden osoituksena.

Lisäksi poliisin on tarkoitus mahdollistaa käyttö kenttätoiminnassa, jolloin digitaalisen henkilöllisyystodistuksen tarkastamiseen hyödynnetään poliisin mobiililaitteita. Digitaalisen henkilöllisyystodistuksen käytön mahdollistamisella ei katsota olevan laitteisiin liittyvien kustannusten lisäksi muita kuin vähäisiä koulutustarpeeseen liittyviä vaikutuksia.

Ulkoasiainhallinnon osalta vaikutukset liittyvät lähinnä tarvittavien laitteiden hankintaan, asiakaspalveluun sekä Suomen edustustojen henkilöstön koulutustarpeeseen. Digitaalinen henkilöllisyystodistus tulee todennäköisesti työllistämään Suomen edustustojen asiakaspalvelua jonkin verran enemmän kuin esimerkiksi Suomessa poliisia sen vuoksi, että läheskään kaikilla ulko-suomalaisilla ei ole suomalaisia pankkitunnuksia, mobiilivarmennetta tai henkilökortin kansalaisvarmennetta, jotka mahdollistaisivat digitaalisen henkilöllisyystodistuksen käyttöönoton sähköisesti. Digitaalisen henkilöllisyystodistuksen tarkastaminen toteutetaan siten, että sen tulisi lyhentää jokaiseen tunnistustapahtumaan tarvittavaa aikaa. Verrattuna perinteisiin fyysisiin asiakirjoihin tarkastustapahtuma voi keskittyä lähes kokonaisuudessaan sen varmistamiseen, että kyseinen henkilö on se, jonka tiedot välittyvät digitaalista henkilöllisyystodistusta käytettäessä. Perinteisten fyysisten asiakirjojen osalta tarkastustilanteessa tulee aina huomioida mahdollisuus siitä, että esitetty asiakirja on väärennetty tai sen sisältämiä tietoja on muilla tavoin manipuloitu. Digitaalisen henkilöllisyystodistuksen ollessa kyseessä tällaista vaaraa ei ole, koska tietoja ei saa luettua onnistuneesti, jos kyse ei ole viranomaisen luovuttamista ajantasaisista tiedoista. Tarkistettaessa digitaalista henkilöllisyystodistusta tarkastussovelluksessa kasvokuva on myös mahdollista esittää huomattavasti suurempana kuin fyysisessä tunnistusasiakirjassa. Tämä nopeuttaa kasvokuvan vertaamista henkilöllisyystodistusta osoittavaan henkilöön ja lisää varmuutta asiointitilanteessa.

Liikenne- ja viestintävirasto Traficom toimii tunnistus- ja luottamuspalvelulain mukaisena valvovana viranomaisena ja osallistuu luottamusverkoston toimijoiden välisen yhteistyön koordinointiin. Hallituksen esityksellä luodaan luottamusverkostoon uusia tehtäviä, kun jatkossa tunnistusvälityspalvelun tarjoajat voivat välittää myös digitaalista henkilöllisyystodistusta sekä ulkomaalaisen digitaalista asiointivälinettä tunnistusvälineiden lisäksi. Tällä on vaikutusta Traficomien tehtäviin.

Ehdotuksen mukaan Digi- ja väestötietovirastolle syntyy velvollisuus päättää Traficomia ja Poliisihallitusta kuultuaan digitaalisen henkilöllisyyden tietojärjestelmän tarkemmista teknisistä vaatimuksista ja tietoturva vaatimuksista. Lisäksi Traficomilta pyydetään lausunto kahden vuoden välein tehtävästä arviointilaitoksen tekemästä arvioinnista.

Valtion tieto- ja viestintätekniikkakeskus Valtori tuottaa valtionhallinnon toimialariippumattomat ICT-palvelut. Valtorin tehtäväksi voidaan nähdä Digi- ja väestötietoviraston julkaiseman sovelluksen jakaminen keskitetysti valtionhallinnon työntekijöiden virkapuhelimiin.

Arvioitaessa muutoksia viranomaisten toimintaan digitaalisen henkilöllisyystodistuksen hyödyntäjinä on erotettava toisistaan sähköinen asiointi ja käyntiasiointi. Viranomaisten sähköisissä asiointipalveluissa ratkaisun käyttöönotto ei edellytä muutoksia, koska se tarjotaan hyödynnettäväksi Digi- ja väestötietoviraston tuottamana suomi.fi-tunnistuspalvelun kautta. Muutoksia saattaa kuitenkin näkyä käyttäjälle esimerkiksi pyyntönä luovuttaa tunnistamiseen tarvittavat tiedot asiointipalvelulle joko suoraan tai suomi.fi-palvelun kautta. Käyttäjän näkökulmasta muutos tietojen kysymiseen tulisi tehdä yhdenmukaisesti.

Käyntiasiointipalveluissa vastaavaa välityspalvelua ei ole käytettävissä, jolloin digitaalisen henkilöllisyystodistuksen käyttöönotto edellyttää muutoksia vähintään viranomaisten toimintamalleihin. Ehdotuksen mukaan digitaalisen henkilöllisyystodistuksen voisi käyntiasioinnissa tarkastaa Digi- ja väestötietoviraston tuottamalla mobiilisovelluksella. Mobiilisovelluksen käyttö edellyttää, että asiointipisteen virkailijan käytössä on mobiililaite. Vaihtoehtoisesti tarkastusraportin käyttäminen edellyttää teknisiä muutoksia viranomaisen käyntiasioinnin virkailijajärjestelmiin. Digi- ja väestötietoviraston tehtävänä olisi määritellä vaatimukset muille sovelluksille ja ratkaisuille, jotka mahdollistaisivat todistuksen lukemisen rajapinnan avulla.

Digi- ja väestötietovirasto myöntää ulkomaalaisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen henkilöllisyyden osoittamiseen sähköisissä asioinnissa. Välineitä ei ole tarkoitus hyödyntää käyntiasioinnissa. Viranomaisten sähköisissä asiointipalveluissa käyttöönotto ei edellytä muutoksia, koska ratkaisu tarjotaan hyödynnettäväksi Digi- ja väestötietoviraston tuottamana Suomi.fi-tunnistuspalvelun kautta.

Ulkomaalaisen asiointivälineen myöntäminen tapahtuu pääasiassa etärekisteröintiä hyödyntäen. Ulkomaalaisten henkilöiden saapuessa Suomeen he voivat kuitenkin korottaa asiointivälineensä varmuustasoa tunnistautumalla kasvokkain Digi- ja väestötietoviraston asiointipisteissä. Tämä voi vaikuttaa asiointipisteiden käyntimääriin, jos ulkomaalaisen asiointivälinettä otetaan laajasti käyttöön myös henkilöiden toimesta, jotka asioivat Suomessa. Digi- ja väestötietoviraston vastuulla on myös luonnollisen henkilön tunnistusvälineen myöntämiseen liittyvät toimenpiteet, mikä voi kasvattaa tarvetta asioinneille Digi- ja väestötietoviraston asiointipisteissä.

4.2.2.2 Vaikutukset organisaatioon ja henkilöstöön

Digitaalisen henkilöllisyyden tietojärjestelmän, ulkomaalaisen digitaalisen asiointivälineen sekä luonnollisen henkilön tunnistusvälineen tuottamisen on arvioitu aiheuttavan Digi- ja väestötietovirastolle noin 20–25 henkilötyövuoden lisätarpeen. Virkatyö liittyy erilaisiin asiakastukitehtäviin sekä tietojärjestelmän kehittämiseen ja ylläpitoon liittyviin tehtäviin. Poliisille on arvioitu aiheuttavan noin 2 henkilötyövuoden lisätarve tietojärjestelmän ylläpitoon liittyviin tehtäviin.

Ulkomaalaisten etärekisteröinnin ja alaikäisten tunnistamisen on arvioitu kasvattavan Opetushallituksen asiakasneuvonnan ja viestinnän tarvetta. Neuvontaan ja viestintään liittyvä lisätyö olisi käyttöönottovaiheessa arviolta 2 henkilötyövuotta, ylläpitovaiheessa arviolta 0,5 henkilötyövuotta.

Traficomille ehdotuksen on arvioitu aiheuttavan 1 henkilötyövuoden lisätarpeen. Virkatyö liittyy ehdotuksen mukaisten lakisääteisten tehtävien (lausuminen arviointikriteeristöä, lausuminen auditoinneista) lisäksi mm. arviointikriteeristön valmistelun tukitehtäviin, tiedottamiseen ja

yhteydenpitoon Digi- ja väestötietoviraston ja luottamusverkoston suuntaan, mahdollisten häiriötilanteiden selvittämiseen, mikäli häiriötilanteet vaikuttavat luottamusverkostoon, Traficom-määräysten, ohjeiden ja suositusten mahdollisiin päivitystarpeisiin yhteentoimivuuden varmistamiseksi sekä kansalaisten neuvontaan uusien välineiden suhteesta olemassa oleviin vahvan sähköisen tunnistamisen välineisiin. Lisäksi Traficomille nähdään vähintään avustava rooli, kun ehdotettua ratkaisua lähdetään notifioimaan EU:n rajat ylittäväksi ratkaisuksi, sekä avustava rooli Digi- ja väestötietoviraston lukijasovelluksen määräyksen valmistelussa.

4.2.2.3 Vaikutukset viranomaisten tiedonhallintaan

Ehdotuksella on vaikutuksia poliisin sekä Digi- ja väestötietoviraston tiedonhallintaan. Ehdotuksien valmisteluvaiheessa, helmikuussa 2020, Poliisihallitus sekä Digi- ja väestötietovirasto ovat tehneet tiedonhallintalain 9 §:n mukaisen lausuntopyynnön valtiovarainministeriölle. Lausuntopyynnöissä ja valtiovarainministeriön pyyntöihin laatimissa lausunnossa on arvioitu suunnitellun muutoksen vaikutuksia tiedonhallintaan. Nämä arviot ovat pääsääntöisesti edelleen paikkansapitäviä, mutta hankkeen edetessä on tehty eräitä aikaisemmista suunnitelmista poikkeavia linjauksia, jotka vaikuttavat keskeisellä tavalla poliisin ja Digi- ja väestötietoviraston tiedonhallintaan.

Keskeisin muutos suhteessa aiemmin esitettyihin muutosvaikutuksiin koskee digitaalisen henkilöllisyyden toimintalogiikkaa. Alkuperäisen suunnitelman mukaan digitaalisen henkilöllisyydestodistuksen oli määrä toimia siten, että tiedot luovutettaisiin tietojen tarkastajalle aina sovellusta käytettäessä suoraan Poliisihallituksen ylläpitämistä passi- ja henkilökorttirekistereistä käyttäjän antaman valtuutuksen perusteella. Suunnitellusta toimintamallista oli määrä syntyä suuri määrä lokitietoja koskien välineen käyttöä.

Ehdotettavan sääntelyn mukaan tiedot luovutettaisiin käyttäjän itsensä hallittavaksi sovellukseen. Luovuttamisen jälkeen tiedot eivät olisi enää viranomaisen tietoja eikä niitä koskisi viranomaisen tiedonhallintaan liittyvät vastuut. Tietoja ei siten luovutettaisi viranomaisen rekisteristä suoraan yksityisille toimijoille esimerkiksi henkilöllisyyden tarkastustilanteessa. Tarkastustilanteessa olisi myös ehdotuksen mukaisesti mahdollista varmistua tietojen ajantasaisuudesta, mutta ajantasaisuuden varmistaminen tapahtuisi Digi- ja väestötietoviraston toimesta eikä henkilötietoja luovutettaisi suoraan viranomaiselta tarkastajalle.

Tietojen luovutusta kuitenkin tapahtuu edelleen suunnitellussa toteutuksessa myös viranomaissektorin ulkopuolelle, koska jatkossa tiedot luovutetaan yksityishenkilöille digitaalisen henkilöllisyydestodistuksen käyttöönoton yhteydessä. Tietojen luovutus tapahtuu siis kyseessä olevalle henkilölle itselleen siten, että viranomainen luovuttaa varmenneet henkilötiedot hänen hallussaan olevalle laitteelle. Digitaalisen henkilöllisyydestodistuksen osalta tietojen lähteenä on poliisin passi- tai henkilökorttirekisteri, jossa olevat luvanhaltijan tiedot poliisi luovuttaa Digi- ja väestötietovirastolle, joka huolehtii tietojen lisäämisestä käyttäjän sovellukseen.

Digitaalisen henkilöllisyydestodistuksen toteuttaminen edellyttää poliisin osalta uuden tietojärjestelmän käyttöönottoa. Kyseessä on Henkilökortti ja passi -tietojärjestelmään eli Heko-Passiin kiinteästi liittyvä MHEKO edustapalvelu, jonka tehtävänä on välittää henkilökortti- ja passirekisterin tietoja Digi- ja väestötietovirastolle. Toteutuksessa ei ole tarvetta tehdä muutoksia poliisin sähköiseen asiointialustaan.

Ehdotukset aiheuttaisivat Digi- ja väestötietovirastolle uusia lakisääteisiä tehtäviä ja niiden tuottamiseen liittyviä uusia tietojärjestelmiä sekä tietovarantoja. Digi- ja väestötietovirasto tuottaisi jatkossa digitaalisen henkilöllisyyden tietojärjestelmän, joka mahdollistaa digitaalisen henkilöllisyydestodistuksen ja ulkomaalaisen asiointivälineen tuottamisen ja käyttämisen. Lisäksi Digi- ja

väestötietovirastolle tulisi tehtäväksi tarjota luonnollisen henkilön tunnistusvälinettä. Luonnollisen henkilön tunnistusvälineen tuottaminen edellyttäisi taustapalveluja välineen hallinnoimiseksi.

Ehdotusten mukaisen digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen toimintatapa on osittain verrattavissa Digi- ja väestötietoviraston nykyisin tuottamiin henkilövarmenteisiin, joissa varmenteella olevat henkilötiedot luovutetaan henkilölle itselleen hyödynnettäväksi. Ehdotuksen mukaisessa ratkaisussa käsiteltävä tietomäärä olisi kuitenkin huomattavasti suurempi ja sisältäisi myös poliisin rekistereistä saatavaa tietoa. Lisäksi ratkaisu eroaa sen osalta, että alustana toimii mobiilisovellus. Samoin tiedon varmentamiseen liittyvä ratkaisu on verrattavissa Digi- ja väestötietoviraston nykyisin tuottamiin varmennepalveluihin.

Ehdotuksen mukainen toimintamalli poikkeaa huomattavasti nykyisestä sähköisen tunnistamisen toimintaperiaatteista. Digi- ja väestötietovirastolle ei palveluita tuottavana toimijana synny vastaavaa kattavaa tapahtumatierekisteriä palvelun käyttämisestä kuten sähköisten tunnistuspalveluiden tai esimerkiksi sähköisen asiointin tukipalveluiden tuottamisesta syntyy. Ehdotuksen mukainen toimintamalli on vastaava kuin passin ja henkilökortin käyttäminen käyntiasioinnissa; käyttäjän vastuu korostuu.

Ehdotus sisältää uusia Digi- ja väestötietoviraston rekisterinpidon vastuulle tulevia henkilötietoja sisältäviä rekistereitä, kuten esimerkiksi laiterekisteri sekä rekisteri ulkomaalaisen digitaalisista asiointivälineistä. Digi- ja väestötietovirasto rekisterinpitäjänä vastaisi rekistereihin tallennettavien tietojen asianmukaisesta hallinnoinnista ja niiden luovuttamisesta henkilön itsensä haltuun.

Ehdotus aiheuttaa erityisiä tehtäviä, jotka edellyttävät pääsyä tietoihin, joiden osalta näitä tietoja käsittelevien henkilöiden luotettavuus on arvioitava. Ehdotus aiheuttaa myös erityisiä tehtäviä, jotka edellyttävät pääsyä toimitiloihin, joissa työskentelevien henkilöiden luotettavuus on arvioitava. Näitä tehtäviä ovat esimerkiksi tietojärjestelmien hallinnointiin liittyvät tehtävät sekä ratkaisun edellyttämät asiakastukitehtävät. Ehdotuksen ei kuitenkaan ole arvioitu aiheuttavan muutosta Digi- ja väestötietoviraston toimintatapoihin liittyen virkamiehenä tai ostopalveluiden kautta hankittuna asiantuntijana työskentelevien henkilöiden luotettavuuden arviointiin; nykyisten toimintamallien ja -menetelmien on arvioitu olevan riittäviä.

Ehdotuksen mukaan digitaalinen henkilöllisyystodistus sisältää passi- tai henkilökorttirekisteriin tallennetun kasvokuvan. Julkisuuslain 24 § 1 momentin 4 kohdan perusteella poliisi on tullut kinnut, että passin ja henkilökortin osalta salassa pidettäviä tietoja ovat sormenjäljet, kasvokuva ja passin tai henkilökortin numero. Näin ollen esityksen mukaisen ratkaisun tuottaminen edellyttää salassa pidettävän tiedon eli passin tai henkilökortin kuvan käsittelyä. Ratkaisun kehittämisen ja ylläpidon aikana voidaan käsitellä Digi- ja väestötietoviraston tai poliisin tietojärjestelmien turvajärjestelyihin liittyvää salassa pidettäväksi luokiteltua tai turvallisuusluokiteltua tietoa.

Ehdotus sisältää myös tietoturvallisuutta koskevaa erityissääntelyä digitaalisen henkilöllisyyden tietojärjestelmää koskevista keskeisistä laatu- ja tietoturvallisuusvaatimuksista. Tietojärjestelmään sekä Digi- ja väestötietoviraston tehtäviin sovellettaisiin tiedonhallintalakia, mukaan lukien sen 4 lukua, jossa säädetään julkisen hallinnon tietoturvallisuuden perustason vaatimuksista. Ehdotus sisältäisi erityiset vaatimukset, jotka kohdistuisivat digitaalisen henkilöllisyyden tietojärjestelmään näiden perustason vaatimusten lisäksi sekä niiden tarkennuksena. Sääntelyn tarkoituksena ei olisi poiketa tiedonhallintalaissa yleisesti säädetystä.

Ehdotuksen mukaan ratkaisussa syntyvä digitaalisen henkilöllisyyden tietojärjestelmä on oltava aina saatavilla ja näin sen voidaan tulkita olevan kriittinen uusi järjestelmäkokonaisuus. Digitaalisen henkilöllisyyden tietojärjestelmä hyödyntää poliisin heko-passi-järjestelmää, jonka saatavuusvaatimus nousee muutoksen myötä kriittiseksi. Muut hyödynnettävät olemassa olevat järjestelmät (väestötietojärjestelmä, varmennejärjestelmä) on jo luokiteltu kriittiseksi. Ehdotuksen mukaan ratkaisussa ei hyödynnetä Digi- ja väestötietoviraston tietovarannoissa sijaitsevaa salassa pidettävää tai turvaluokiteltavaa tietoa.

Esitys ei aiheuta muutoksia viranomaisen toimitiloihin eikä sillä ole vaikutuksia tietojenkäsittely-ympäristön fyysiseen turvallisuuteen. Uudistus ei muuta käyttöoikeuksia tai kirjautumistapa olemassa olevissa tietojärjestelmissä. Uusien tietojärjestelmien käyttöoikeudet määrittämään tarvelähtöisesti noudattaen käyttöoikeuksien minimoinnin perusteita.

Ehdotus aiheuttaa tarpeen toteuttaa lokitus uusiin tietojärjestelmiin liittyen digitaalisen henkilöllisyyden palveluihin sekä luonnollisen henkilön tunnistusvälineeseen. Digi- ja väestötietovirastolle kertyy kattavasti lokitietoa liittyen digitaalisen henkilöllisyyden palveluihin siltä osin, kun kyse on varmennettujen henkilötietojen viemisestä henkilön hallussa olevaan mobiililaitteeseen sekä laitehallinnasta mutta varsinaisesta digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen käytöstä ei synny lokitietoa. Luonnollisen henkilön tunnistusvälineen osalta lokitietoa kertyy sekä välineen hallinnoinnista, että käytöstä.

Ehdotukset eivät aiheuta muutoksia viranomaisten tapaan muuttaa asiakirjat sähköiseen muotoon tai riskejä sähköiseen muotoon muutetun asiakirjan luotettavuuteen tai eheyteen. Ehdotukset eivät aiheuta poikkeamistarvetta sähköiseen muotoon muuttamiselle eikä muutoksia tietoaaineiston saatavuuteen koneluettavassa muodossa. Ehdotuksissa kuvattu itsehallittavan identiteetin malli tuo muutoksia viranomaisen toimesta tapahtuvaan tietojen käyttöön sekä asiakkaan ja hyödyntäjän tiedon välittämisen tapoihin, ja mahdollisuuksiin asioida sähköisesti.

Esitys aiheuttaa muutoksia viranomaisten tiedonsaantioikeuksiin. Digitaalisen henkilöllisyyden järjestelmän tuottaminen digitaalisen henkilöllisyystodistuksen osalta edellyttää, että Digi- ja väestötietovirastolla on oikeus saada käyttöönsä poliisin rekisteröimiä passiin ja henkilökorttiin liittyviä tietoja esimerkiksi digitaalisen henkilöllisyystodistuksen käyttöönottilanteissa. Tämä toteutetaan teknisten rajapintojen avulla.

Uudistus aiheuttaa joitakin teknisiä muutoksia poliisin tiedonsaantimahdollisuuksiin. Poliisin on saatava käyttöönsä digitaalisen henkilöllisyyden järjestelmään rekisteröityjä tietoja digitaaliseen henkilöllisyystodistukseen liittyen, jotta voi tuottaa niihin liittyvät rekisteröintitehtävät. Tämä toteutetaan katseluyhteyden avulla.

Ulkomaalaisten digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen rekisteröintiä voitaisiin tuottaa yhteispalvelulain perusteella yhteispalveluna muiden viranomaisten kanssa. Tämän toteuttaminen edellyttää, että ko. viranomaisilla on tiedonsaantimahdollisuudet digitaalisen henkilöllisyyden järjestelmään ulkomaalaisten digitaalisen asiointivälineen osalta sekä luonnollisen henkilön tunnistusvälineeseen liittyvään järjestelmään. Tämä toteutetaan teknisten rajapintojen avulla. Esityksessä ei määritetä tietojen tai asiakirjojen säilytysaikoja, joten Digi- ja väestötietoviraston on määritettävä ne. Perusteena voidaan käyttää esimerkiksi tunnistus- ja luottamuspalvelulain 24 §. Esityksen mukaan asiakirjojen voimassaoloaika perustuu myöntämisen taustalla olevan tunnistusasiakirjan voimassaoloaikaan. Tällä on arvioitu olevan vaikutuksia arkistointiaikoihin.

Esityksen mukaista ulkomaalaisen digitaalista asiointivälinettä voi käyttää suomi.fi-tunnistuksen kautta. Ulkomaalaisen digitaalinen asiointiväline tarjotaan vastaavilla rajapinnoilla kuin

vahvat sähköiset tunnistusvälineet nykyisin, mutta rajapintojen tietorakenne poikkeaa. Ulkomaalaisen digitaalisen asiointivälineen hyödyntäminen edellyttää käyttöönottovalta organisaatiolta muutoksia teknisiin rajapintoihin.

Esitys perustuu digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen osalta siihen, että tiedot luovutetaan henkilölle itselleen ja ovat sen jälkeen henkilön itsensä hallittavissa. Digi- ja väestötietovirasto ei osallistu tietojen käyttötilanteisiin eikä voi selvittää tietojen käyttötarkoitusta. Esityksen mukaisen luonnollisen henkilön tunnistusvälineen tietojen käyttötarkoitus selvitetään suomi.fi-tunnistuksen käyttöönottoprosessien ja -toimintamallien mukaisesti.

Esityksen mukainen ratkaisu tuottaa asiarekisteriin rekisteröiviä tietoja. Esityksen mukaan Digi- ja väestötietoviraston on annettava päätös, jos ulkomaalaisen digitaalista asiointivälinettä tai luonnollisen henkilön tunnistusvälinettä ei myönnetä hakijalle. Samoin päätös tulee antaa, jos Digi- ja väestötietovirasto peruu välineen ilman sen haltijan pyyntöä. Digitaalisen henkilöllisyystodistuksen osalta vastaavaa ei ole esitetty.

Esitys aiheuttaa muutoksia asianhallintajärjestelmään asianumeroiden sekä metatietojen määrittelyn kautta. Tämän lisäksi on määritettävä asiakirjojen julkisuusarvo. Uudistuksessa ei ehdoteta muutoksia voimassa olevaan asiakirjojen julkisuutta ja salassapitoa koskevaan sääntelyyn. Uudistus aiheuttaa päivitystarpeen viraston asiakirjajulkisuuskuvaukseen.

4.2.3 Ympäristövaikutukset

Ehdotuksella voi olla vähäisiä ympäristövaikutuksia lähinnä mahdollisesti lisääntyvän digitaalisen asioinnin sekä päätelaitekannan mahdollisen kasvun kautta. Digitaalisen asioinnin voidaan olettaa olevan lähtökohtaisesti jonkin verran ympäristönäkökulmista parempi käyntiasiointiin verrattuna, mutta tähän vaikuttaa esimerkiksi se, millä tavoin käyntiasioinnin vaatima liikkuminen asiointipaikkaan tehdään. Pelkästään ehdotuksesta johtuva päätelaitekannan kasvaminen on todennäköisesti varsin vähäistä. Päätelaitteiden valmistukseen liittyvät ympäristönäkökulmat on kuitenkin syytä huomioida. Erityisesti jos ehdotuksen seurauksena suuri joukko kansalaisia ottaa esimerkiksi luonnollisen henkilön tunnistusvälineen käyttöön kaiken varalta, vaikuttaisi tämä ehdotuksen ympäristövaikutuksiin. Ehdotuksen ympäristövaikutuksia tulisi kuitenkin seurata jatkossa, jotta yleisesti digitaalisten palvelujen tuotannon ja käytön ympäristövaikutusten ymmärrys ja mittaamisosaaminen kehittyisi.

4.2.4 Muut yhteiskunnalliset vaikutukset

4.2.4.1 Vaikutukset kansalaisten asemaan yhteiskunnassa ja kansalaisyhteiskunnan toimintaan

Ehdotuksilla pyritään edistämään kansalaisten yhdenvertaisia mahdollisuuksia asioida ja toimia yhteiskunnan jäsenenä erilaisissa asiointikanavissa ja palveluprosesseissa. Ehdotuksilla on vaikutuksia kansalaisten ja Suomessa oleskelevien yhdenvertaisuuteen sekä lasten asemaan. Ehdotuksen mukainen digitaalinen henkilöllisyystodistus mahdollistaa kansalaisille uuden menetelmän ja tavan osoittaa henkilöllisyys digitaalisen palvelun avulla käynti- ja digitaalisessa asiointissa. Ehdotuksen arvioidaan edistävän kansalaisten yhdenvertaista asemaa yhteiskunnassa, vaikka käytännössä kansalaisten mahdollisuudet käyttää digitaalista henkilöllisyystodistusta voivat olla erilaisia johtuen ratkaisun käyttämiseen liittyvistä vaatimuksista sekä taloudellisista tai henkilön fyysisistä toimintaedellytyksistä johtuvista syistä.

Ehdotuksella kokonaisuudessaan arvioidaan olevan pääasiassa positiivisia vaikutuksia kotitalouksien asemaan digitaalisten palvelujen käyttömahdollisuuksien osalta. Ehdotuksen mukaisesti digitaalinen henkilöllisyystodistus olisi mahdollista saada asiakkuudesta riippumatta, kuten passi tai henkilökortti. Tämä lisää kansalaisten yhdenvertaisia mahdollisuuksia toimia tasa-arvaisesti digitaalisessa yhteiskunnassa ja antaa lisää mahdollisuuksia hyödyntää erilaisia digitaalisen tunnistamisen ja henkilöllisyyden osoittamisen menetelmiä sekä tapoja. Toisaalta digitaalisten asiointipalvelujen ei ole pakko hyväksyä digitaalista henkilöllisyystodistusta palvelusaan, joten tosiasialliset vaikutukset kansalaisten mahdollisuuksiin selviävät vasta palvelun tultua käyttöön. Jatkossa tuleekin arvioida säännöllisesti digitaalisen henkilöllisyyden käyttömahdollisuuksia ja niihin liittyviä seikkoja.

Käytännössä ehdotettu digitaalinen henkilöllisyystodistus vaatii tallennus- ja alustaksi riittävän nykyaikaisen älylaitteen. Suurin osa päätelaitteista sisältää runsaasti erilaisia avustavia teknologioita (esimerkiksi näytön sisällön koon muuttaminen, erilaiset kontrastimahdollisuudet, puheohjaus), jolloin digitaalisen henkilöllisyystodistuksen tallennus- ja alustat ovat pääsääntöisesti esteettömiä. Digitaalisen henkilöllisyystodistuksen sovelluksen tulee täyttää laissa digitaalisten palvelujen tarjoamisesta mobiilisovelluksille säädetyt saavutettavuusvaatimukset, joten kokonaisuutena digitaalinen henkilöllisyystodistus tulee olemaan laajan käyttäjäjoukon käyttömahdollisuuksien piirissä. Euroopan parlamentin ja neuvoston direktiivi 2019/882 tuotteiden ja palvelujen esteettömyysvaatimuksista tulee asettamaan yhdenmukaisia esteettömyysvaatimuksia EU-sisämarkkinoilla myytävälle päätelaitteille. Direktiivin toimeenpanevat kansalliset lakiehdotukset ovat parhaillaan eduskuntakäsittelyssä ja ehdotettavien esteettömyyttä koskevien lakien soveltaminen alkaisi ehdotuksen mukaan vuonna 2025.

Digitaalinen henkilöllisyystodistus ja luonnollisen henkilön tunnistusväline olisi tarkoitus tulevaisuudessa ilmoittaa eIDAS-asetuksen mukaisesti rajat ylittävään asiointiin korotetulla varmuustasolla. Tämä parantaisi kansalaisten mahdollisuutta rajat ylittävään asiointiin EU:n sisällä. Tällöin digitaalisella henkilöllisyystodistuksella ja luonnollisen henkilön tunnistusvälineellä pystyisi kirjautumaan muiden jäsenvaltioiden julkishallinnon digitaalisiin palveluihin, jos nämä mahdollistavat tunnistautumisen korotetulla varmuustasolla. Ratkaisut eivät edelleenkään mahdollista tunnistautumista asiointipalveluihin, jotka edellyttävät korkeaa varmuustasoa.

Digitaalinen henkilöllisyystodistus voi helpottaa merkittävästi erityisesti ulkosuomalaisten mahdollisuuksia asioida suomalaisissa digitaalisissa palveluissa, erityisesti julkisen sektorin digitaalisissa palveluissa, koska digitaalisen henkilöllisyystodistuksen saa passin tai henkilökortin yhteydessä ja se on todennäköisesti helpommin käyttöönotettava ja käytettävä vahvaan sähköiseen tunnistamiseen kuin nykyisin henkilökortilla oleva kansalaisvarmenne. Toisaalta ulkosuomalaisten osuus digitaalisten palvelujen kokonaiskäyttäjämäärästä on suhteellisen pieni. Ulkosuomalaisten osalta on eri yhteyksissä tuotu esille vaikeus hoitaa asiointia Suomeen juuri puuttuvien vahvojen sähköisten tunnistusvälineiden vuoksi. Digitaalinen henkilöllisyystodistus mahdollistaisi uuden tavan sähköiseen tunnistautumiseen ainakin julkisen sektorin digitaalisiin palveluihin. Jos yksityisen sektorin toimijat alkavat hyödyntämään digitaalista henkilöllisyystodistusta, ulkosuomalaisten asiointimahdollisuudet suomalaisissa digitaalisissa palveluissa paranevat merkittävästi nykyisestä.

Digitaalisella henkilöllisyystodistuksella voi olla vaikutuksia sellaiseen käyntiasointiin, jossa henkilön tulee osoittaa henkilöllisyytensä. Digitaalinen henkilöllisyystodistus voisi helpottaa esimerkiksi suunnittelematonta pankkiasiointikäyntiä, jos pankki hyväksyisi digitaalisen henkilöllisyystodistuksen henkilöllisyyden osoittamiseen käyntiasioinnissa. Ehdotuksella voi olla pidemmällä aikavälillä positiivinen vaikutus henkilöllisyyden osoittamisen tapojen yhdenmukaistamiseen käyntiasioinnissa esimerkiksi vähentämällä henkilöiden epätietoisuutta, milloin hen-

kilöllisyystodistukseksi käy ajokortti ja milloin vaaditaan passi tai henkilökortti. Yleisesti ottaen digitaalinen henkilöllisyystodistus veisi henkilöllisyyden osoittamista kohti samaa toimintamallia kuin esimerkiksi erilaiset mobiilimaksamisen ratkaisut, joissa henkilö ei tarvitse makсутapahtumaa varten muuta kuin mobiililaitteen ja siinä olevan mobiililompakon tallennettuine maksukortteineen.

Ehdotettu luonnollisen henkilön tunnistusväline olisi vaihtoehtoinen tunnistustapa niille henkilöille, jotka eivät voi tai halua käyttää digitaalista henkilöllisyystodistusta tunnistautuessaan julkisen sektorin digitaalsiin palveluihin. Luonnollisen henkilön tunnistusväline voisi mahdollistaa sähköisen tunnistautumisen julkishallinnon asiointipalveluihin henkilöille, jotka eivät käytä mobiililaitteita. Luonnollisen henkilön tunnistusvälineen arkipäiväinen käyttö saattaisi olla vähäistä, mutta se on merkityksellinen henkilöiden yhdenvertaisuuden ja sähköisen tunnistamisen varautumisen näkökulmasta. Arviolta vähäisestä käyttötiheydestä voi seurata suhteessa kasvanut tukipalvelujen määrä esimerkiksi erilaisten käyttöneuvonnan tai unohtuneiden tunnusluku- jen tapaisina palvelupyynnöinä.

Esitys sisältää ehdotukset myös ulkomaalaisen digitaalisesta asiointivälineestä. Ehdotus voi helpottaa merkittävästi ulkomaalaisten henkilöiden mahdollisuuksia asioida suomalaisissa digitaalisissa palveluissa. Tällä hetkellä asiointi perustuu suurelta osin joko viranomaiskohtaisesti tehtäviin ratkaisuihin tai, ulkomaalaisen henkilön asioidessa yrityksen puolesta, Digi- ja väestötietoviraston tuottamaan ulkomaan kansalaisen tunnistuspalveluun eli Finnish Authenticator-tunnistuspalveluun.

4.2.4.2 Vaikutukset lapsiin

Ehdotuksella voi olla vähäisiä vaikutuksia lapsiin. Ehdotus voi parantaa lasten mahdollisuuksia asioida tietyissä palveluissa digitaalisesti sekä myös vanhempien mahdollisuuksia hoitaa lastensa asioita, mutta vaikutukset kohdistuvat pääasiassa yli 15-vuotiaisiin. Digitaalisen henkilöllisyystodistuksen voisi saada kuka tahansa, jolla on suomalainen passi tai henkilökortti. Alaikäisistä 15 vuotta täyttäneet voisivat saada digitaalisen henkilöllisyystodistuksen myös ilman vanhempien suostumusta. Alle 15-vuotiaat voisivat saada digitaalisen henkilöllisyystodistuksen samoin ehdoin kuin passin tai henkilökortin eli huoltajien suostumuksella. Ehdotus ei käytännössä muuta alle 15-vuotiaiden nykyistä mahdollisuutta saada vahva sähköinen tunnistusväline, mutta tuo nykyisen kansalaisvarmenteen rinnalle uuden vaihtoehdon.

Yli 15-vuotiaiden osalta asema ja tosiasialliset mahdollisuudet digitaaliseen asiointiin muuttuisivat ehdotusten myötä jonkin verran nykyisestä. Tänä päivänä lasten mahdollisuudet ja oikeudet saada vahvana sähköisenä tunnistusvälineenä toimivat pankkitunnukset tai mobiilivarmenne vaihtelevat myöntäjittäin. Joillakin toimijoilla ei ole ikärajoja palvelujen saamiselle huoltajien suostumuksella, osalla palveluiden saamiselle on asetettu ikäraja (esimerkiksi 12 vuotta) ja vaatimus huoltajien suostumukselle. Jatkossa yli 15-vuotias, jolla on voimassa oleva passi tai henkilökortti voisi saada digitaalisen henkilöllisyystodistuksen ilman huoltajien suostumusta.

Ehdotukset mahdollistavat alaikäisille yli 15-vuotiaille hieman nykyistä laajemmat mahdollisuudet asioida erilaisissa digitaalisissa palveluissa vahvasti tunnistettuina. Nykyisinkin lapsilla on mahdollista saada erilaisia vahvan sähköisen tunnistamisen välineitä, mutta myöntämisen ikärajat ja käytänteet vaihtelevat toimijoittain. Samalla on kuitenkin huomattava, että tunnistusvälineiden saamisen lisäksi kaikilla digitaalisilla asiointipalveluilla ei välttämättä ole kykyä ottaa vastaan myös alaikäisiä itsenäisesti asioivia, jos asiointijärjestelmät on lähtökohtaisesti rakennettu vain täysi-ikäisiä varten. Tämä edellyttää asiointipalveluilta mahdollisesti kykyä ja tarvetta tunnistaa, minkä ikäiset voivat asioida palvelussa sekä iän tarkastamista ja sen toteuttamista osaksi asiointiprosessia.

Alaikäisten mahdollisuudella saada digitaalinen henkilöllisyystodistus ja sen vaatimalla asiointitarpeella voi olla vaikutusta myös poliisin toimintaan. Esitetyt muutokset mahdollistavat sen, että alaikäinen voi ottaa digitaalisen henkilöllisyystodistuksen itsenäisesti käyttöön, jos hänellä on voimassa oleva matkustusoikeudellinen passi tai henkilökortti tai hän on viisitoista vuotta täyttänyt ja hänellä on ilman huoltajien suostumusta myönnetty alaikäisen matkustusoikeudeton henkilökortti. Koska kaikilla passin tai matkustusoikeudellisen henkilökortin omaavilla on ikään katsomatta oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon tarkoittaa se sitä, että tällaisilla alaikäisillä olisi myös itsenäinen oikeus asioida poliisin luona digitaalisen henkilöllisyystodistuksen käyttöönottamiseksi.

4.2.4.3 Vaikutukset työllisyyteen ja työelämään

Ehdotuksilla arvioidaan olevan positiivisia vaikutuksia työllisyyteen, työelämään ja -tehtäviin liittyvien digitaalisten palvelujen käyttömahdollisuuksiin sekä ulkomaalaisten työllistymismahdollisuuksiin. Digitaalinen henkilöllisyystodistus mahdollistaa henkilölle henkilöllisyyden osoittamisen digitaalisen asioinnin yhteydessä myös työtehtäviin liittyen. Tämä voi lisätä viranomaisrekisteristä peräisin olevien henkilöllisyyttä osoittavien tietojen hyödyntämistä yrityksille suunnattujen digitaalisten palvelujen käyttökontekstissa.

Ulkomaalaisen digitaalinen asiointiväline voi helpottaa ulkomaalaisen henkilön työllistymistä mahdollistamalla heille nykyistä tasapuolisemmat edellytykset hoitaa työhön liittyviä tehtäviä myös digitaalisissa asiointipalveluissa. Ulkomaalaisen digitaaliseen asiointivälineeseen liittyvä keskeisesti henkilötunnuksen uudistamiseen liittyvät lainsäädäntömuutokset, joiden tarkoituksena yhdessä digitaaliseen henkilöllisyyteen liittyvien ehdotusten kanssa on sujuvoittaa ulkomaalaisen henkilön mahdollisuuksia rekisteröidä henkilöllisyytensä myös suomalaiseen väestötietojärjestelmään ja saada nykyistä helpommin suomalainen henkilötunnus. Ulkomaalaisen digitaalinen asiointiväline ja suomalainen henkilötunnus mahdollistavat yhdessä henkilön muuta digitaalista asiointia sekä palvelujen saamista. Tänä päivänä henkilötunnusta edellytetään ja sitä hyödynnetään Suomessa laajalti, sekä julkisella, että yksityisellä sektorilla erilaisten palveluprosessien toteuttamisessa.

4.2.4.4 Vaikutukset rikosentorjuntaan ja turvallisuuteen

Ehdotuksella digitaalisesta henkilöllisyystodistuksesta voi olla vaikutuksia digitaalisen palvelutoiminnan yleiseen turvallisuuteen ja luotettavuuteen. Ehdotus voi lisätä esimerkiksi kuluttajien välisen kaupan luotettavuutta ja vähentää erilaisilla digitaalisilla alustoilla tapahtuvia petoksia, jos ehdotuksen myötä digitaalisen henkilöllisyystodistuksen ja vahvan sähköisen tunnistamisen käyttö laajenee kuluttajien välisiin kauppapaikkoihin. Digitaalinen henkilöllisyystodistus voi mahdollisesti lisätä myös henkilöllisyyden tarkastamista kuluttajien välisessä kasvokkainkaupankäynnissä ja tämä voi osaltaan vähentää näissä kauppatilanteissa tapahtuvia petoksia.

Ulkomaalaisen digitaalisen asiointivälineen osalta on huomioitu turvallisuusnäkökulmat ja siihen liittyvät riskit suhteessa rikollisuuden kasvamiseen. Yhdessä henkilötunnuksen uudistamista koskevien lainsäädäntömuutosten kanssa nyt esitettävillä muutoksilla tehdään perustavanlaatuisia muutoksia rekisterihenkilöllisyyden luomiseen. Valmistelun yhteydessä on kiinnitetty erityistä huomiota ulkomaalaisen digitaalisen asiointivälineeseen liittyvän etäasioinnin turvallisuuteen ja siihen, että yhteiskunnassa riittävällä tavalla tiedostetaan etärekisteröintimenetelyyn liittyvä epävarmuus henkilöllisyystietojen luotettavuudesta. Näillä toimenpiteillä pyritään estämään petosrikollisuuden kasvua ja siten poliisin työtaakan lisääntymistä. Etärekiste-

röinnin turvallisuuteen on kiinnitetty erityistä huomiota ratkaisun hyödyntämän kasvojentunnistuksen turvallisuuden näkökulmasta, jotta voidaan varmistua siitä, että kasvojentunnistusta ei käytetä väärin.

Ehdotuksen mukaan poliisilla ja Digi- ja väestötietovirastolla olisi velvollisuus reagoida digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen väärinkäyttötilanteisiin siten, että välineen käyttö esim. identiteettivarkauden tapauksessa estyy. Vastaavalla tavalla tulee kyetä reagoimaan tilanteisiin, joissa asiointipalvelu esim. kerää henkilötietoja väärin perustein. Näiden velvoitteiden täyttämiseksi on vaikutusta poliisin ja Digi- ja väestötietoviraston työmääriin. Väärinkäyttötilanteisiin reagoimisen ohella on valmistelussa pidetty tärkeänä pystyä havainnoimaan väärinkäyttötilanteita esim. niissä tilanteissa, joissa ulkomaalaisen digitaalista asiointivälinettä pyritään väärinkäyttämään rekisteröimällä suuria määriä ulkomaalaisten digitaalisia identiteettejä haittaamistarkoituksessa. Väärinkäyttötilanteiden ennakkoinnin osalta on todettu keskeiseksi, että poliisi ja Digi- ja väestötietovirasto ylläpitävät ajantasaista uhkatilannekuvaa ja varmistuvat siitä, että riittävät tietoturvakontrollit ovat käytössä näihin uhiin reagoimiseksi.

Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen rajapintojen suora hyödyntäminen ei edellytä asiointipalveluilta rekisteröintiä, joten rikollisten on mahdollista pyrkiä luomaan asiointipalveluita, jotka pyrkivät keräämään henkilötietoja perusteettomasti esim. tietojen kalastelun avulla. Väärin perustein toimivien asiointipalveluiden toimintaedellytyksiä pyritään rajoittamaan esim. varmistumalla asiointipalveluiden tunnistamisesta, viestimällä loppukäyttäjille selkeästi tietojen osoittamisesta, ja opastamalla loppukäyttäjää palveluiden turvallisesta käytöstä. Lisäksi on huomioitu tilanteet, joissa loppukäyttäjät tarkoituksellisesti luovuttavat digitaalisen henkilöllisyystodistuksensa tai ulkomaalaisen digitaalisen asiointivälineensä rikollisten käyttöön esim. taloudellisen hyödyn takia. Näitä tilanteita varten myös asiointipalveluilla tulee olemaan mahdollisuus ilmoittaa väärinkäyttötilanteista poliisille ja Digi- ja väestötietovirastolle.

4.2.4.5 Tietoyhteiskuntavaikutukset

Henkilötietojen käsittely ja tietosuojat

Ratkaisun piirissä ja niiden avulla käsitellään laajasti sekä Suomen kansalaisten että suomalaisia sähköisiä asiointipalveluja käyttävien ulkomaalaisten tietoja. Toteutuksessa hyödynnetään olemassa olevia rekistereitä ja luodaan myös uusia rekistereitä (esim. laiterekisteri ja tapahtumatiorekisteri). Rekisterinpitäjyyteen ja käsittelyperusteisiin liittyviä kysymyksiä on kuvattu tarkemmin säädöskohtaisissa perusteluissa.

Ehdotuksen mukaisen digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen henkilötietojen säilyttämisen ja välittämisen toimintaperiaate eroavat nykyisten vahvojen sähköisten tunnistusvälineiden toimintamalleista. Digitaalinen henkilöllisyystodistus ja ulkomaalaisen digitaalinen asiointiväline sisältävät vahvistetut henkilötiedot, joiden käyttämisestä yksilö päättää. Yksilön on siis mahdollista määrittää, mitkä henkilötiedot hän osoittaa palveluntarjoajalle. Ehdotuksen mukaan myös tietojen välittämisen toimintaperiaate olisi uudenlainen; digitaalista henkilöllisyystodistusta ja ulkomaalaisen digitaalista asiointivälinettä olisi mahdollista hyödyntää suoraan asiointipalvelusta ilman, että välissä on tunnistusvälityspalvelu. Todellinen vaikutus jää tämän osalta todennäköisesti alkuvaiheessa pieneksi, koska voidaan olettaa, että ratkaisua hyödynnetään alkuvaiheessa lähinnä tunnistusvälityspalveluiden, Suomi.fi-tunnistuksen ja muiden vastaavien palveluiden avulla.

Henkilötietojen laajamittainen käsittely yhdistettynä uusien teknisten ratkaisujen käyttöön merkitsee todennäköisesti tietosuoja-asetuksen mukaista korkeaa riskiä henkilötietojen käsittelylle. Tästä johtuen tietosuoja-asetuksen 35 artiklan mukainen tietosuojavaikutusten arviointi on tarpeen siinä vaiheessa, kun ratkaisun tekniset suunnitelmat ja käyttömallit tarkentuvat. Myös olemassa olevien rekistereiden osalta ollaan ottamassa käyttöön uusia käytötapoja, mikä edellyttää tietosuojavaikutusten arvioinnin päivittämistä.

Henkilöiden luopuessa digitaalisen henkilöllisyystodistuksen, ulkomaalaisen digitaalisen asiointivälineen, tai luonnollisen henkilön tunnistusvälineen käytöstä on riski, että sensitiivisiä tietoja, kuten kryptografista materiaalia, jää henkilöiden käyttämiin päätelaitteisiin, joten näiden osalta pyritään varmistumaan riittävästä mekanismeista tietojen turvalliseksi hävittämiseksi.

Itsehallittavuuden näkökulmasta pyritään varmistumaan siitä, että digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen liikkeellelaskija ei kykene seuraamaan miten kyseisiä välineitä käytetään henkilötietojen osoittamisessa sähköisessä tai käyntiasioinnissa. Tähän liittyen on keskeistä varmistua siitä, että esimerkiksi sulkulistojen käyttöön tai lokitietojen keräämiseen liittyen ei synny mahdollisuutta seurata välineiden käyttöä asiointipalveluissa. Tämä vaatimus on kuitenkin arvioitava suhteessa väärinkäyttötilanteiden havainnoinnista johtuviin tarpeisiin.

Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen käyttöön liittyy näitä varten luotavan laiterekisterin käyttö. Laiterekisteriin kerätään tietoa mobiilipäätelaitteesta, jossa kyseinen väline on otettu käyttöön. Laiterekisterin osalta varmistutaan siitä, että siihen kerätään vain tarpeelliset tiedot välineiden turvallisen käytön näkökulmasta ja että laiterekisterin tietoja ei perusteettomasti yhdistellä muiden rekistereiden tietojen kanssa.

Tietojen virheettömyyden ja korjaamisen näkökulmasta esityksessä on kuvattu tavat, joilla digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen sisältämät varmenneet henkilötiedot voidaan tuoreuttaa niiden pohjana olevista rekistereistä. Varmenneet henkilötiedot henkilöiden mobiilipäätelaitteessa ovat lyhytikäisiä verrattuna pitkäikäiseen ydinidentiteetin todisteeseen. Tuoreuttaminen on suunniteltu tapahtuvan käyttäjän nimenomaisesti pyynnöstä, jotta ratkaisu edelleen edistäisi itsehallittavuuden periaatetta. Digitaalisen henkilöllisyystodistuksen käyttö kuitenkin käytännössä edellyttäisi tietojen tuoreuttamista tietyin väliajoin, jotta voidaan varmistaa välineessä olevien tietojen olevan ajan tasalla. Asiointipalveluille toimitetaan myös tieto varmennettujen henkilötietojen tuoreutusajankohdasta, jolloin asiointipalvelut voivat itse riskiperusteisesti päättää luottavatko ne osoitettuihin tietoihin vai edellyttävätkö tietojen tuoreuttamista ennen niiden hyväksymistä.

Kansainvälisten tiedonsiirtojen näkökulmasta ratkaisun toteutuksessa pyritään siihen, että henkilötietoja ei siirretä EU/ETA-alueen ulkopuolelle. Tämä varmistetaan etenkin kolmansien osapuolien sovelluskomponenttien näkökulmasta.

Loppukäyttäjän näkökulmasta on keskeistä, että ratkaisussa ei välineen myöntämisen jälkeen ole keskitettyä tahoa, joka määrittäisi miten välinettä käytetään, vaan käyttäjä tekee itse päätöksen siitä, haluaako osoittaa henkilötietojaan tietylle luottavalle taholle. Ratkaisun osalta on pyritty tukemaan loppukäyttäjää tässä päätöksenteossa, jotta hän voi varmistua siitä, että luottava taho on varmasti se, joka väittää olevansa. Luottavan tahon näkökulmasta pyritään varmistumaan siitä, että henkilötiedot osoitetaan luotettavasta välineestä ja että henkilöllä on tosiasiallinen kontrolli osoitettuihin henkilötietoihin, että ne on myöntänyt luotettava taho, ja että tiedot ovat ajantasaiset ja niitä ei olla peruutettu. Digitaaliseen henkilöllisyyteen liittyvässä vies-

tinnässä panostetaan vastuiden selkeään kuvaamiseen ja lisäksi tuetaan loppukäyttäjää välineiden tietoturvalisessä ja tietosuojan huomioivassa käytössä. Viestintää tuetaan mahdollisesti myös digitaalisen henkilöllisyyden hyödyntäjien koulutuksella ja opastuksella.

Luottavat tahot voivat halutessaan hyödyntää digitaalista henkilöllisyystodistusta ja ulkomaalaisen digitaalista asiointivälinettä suoraan sähköisessä asiointissa ja käyntiasioinnissa ilman riippuvuutta keskitetystä tahosta. Tämä tarkoittaa, että mahdolliset kontrollikyvykkyudet, jotka auttavat loppukäyttäjää tekemään informoidun päätöksen tietojen jakamisesta sisällytetään digitaaliseen henkilöllisyystodistukseen ja ulkomaalaisen digitaaliseen asiointivälineeseen. Luotavilta tahoilta edellytetään lisäksi erilaisia toimenpiteitä tai toiminnallisuuksia: 1) mahdollisuutta tunnistaa luottava taho siten, että loppukäyttäjä voi varmistua kenelle on jakamassa tietojaan; 2) kattavaa tietosuojakäytäntöjen kuvaamista; 3) vain kyseisessä käyttötapauksessa tarpeellisten varmennettujen tietojen keräämistä; ja 4) sulkulistojen tarkastamista ja eheystarkastusten suorittamista. Sekä digitaalisen henkilöllisyyden palveluilta että asiointipalveluilta edellytetään oletusarvoisen tietosuojan huomioimista ja tämä voi edellyttää koulutuksia ja opastusta myös asiointipalveluille, jotta ne voivat noudattaa oletusarvoisen tietosuojan mukaista käyttötarkoitussidonnaisuutta kerätessään henkilötietoja hyödyntäessään digitaalisen henkilöllisyyden palveluja. Oletusarvoisen tietosuojan ohella digitaalisen henkilöllisyyden palveluilta edellytetään eettisten näkökantojen huomiointia.

Oletusarvoiseen tietosuojaan ja yleisen tietosuoja-asetuksen mukaiseen henkilötietojen käsittelyyn kuuluu olennaisena osana myös tietojen minimoinnin periaatteen noudattaminen. Tämän periaatteen paremmaksi noudattamiseksi digitaalinen henkilöllisyystodistus ja ulkomaalaisen digitaalinen asiointiväline mahdollistavat ns. valikoivan esittämisen, jossa henkilö voi itse päättää mitä tietojaan jakaa asiointipalvelun kanssa. Valinnan pitää mahdollistua myös tosiasiallisesti siten, että asiointipalvelut asettavat pakollisiksi vain ne tiedot, jotka ne oikeasti tarvitsevat toimintansa takaamiseksi.

Tietoturvallisuus

Itsehallittavuus digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen käytössä vähentää riippuvuutta keskitetyistä komponenteista (esim. keskitetyistä tunnistuspalveluista) käytettäessä kyseisiä välineitä varmennettujen henkilötietojen osoittamisessa. Välineiden käyttöä edellytetään korkeaa käytettävyyttä ja sovitujen palvelutasojen noudattamista, joten palvelukokonaisuuden kannalta varmistutaan riittävästä jatkuvuudenhallinnan menetelmistä, kyvystä palautua häiriötilanteista, ja menetelmistä viestiä loppukäyttäjille ja luotaville tahoille palvelun käytettävyydestä. Olennaista on myös varmistua taustapalveluiden mahdollisuudesta säätää niiden kapasiteettia dynaamisesti, jotta voidaan vastata palvelun muuttuviin käyttötarpeisiin. Nykyinen vahvan sähköisen tunnistamisen kansallinen toteutus nojaa pääasiassa pankkien ja teleoperaattorien tarjoamiin vahvan sähköisen tunnistamisen menetelmiin ja näin ollen yksittäisen tunnistusmenetelmän käytön estyminen ei estä koko vahvan sähköisen tunnistamisen hyödyntämistä kansallisesti. Digitaalisen henkilöllisyystodistuksen kannalta varmistutaan riittävästä resilienssistä kriisitilanteiden osalta, jolloin digitaalisen henkilöllisyystodistuksen käytön estyessä voidaan varmistua vahvan sähköisen tunnistamisen saatavuudesta. Tämä tarkoittaa, että digitaalinen henkilöllisyystodistus ei saa muodostua ainoaksi tavaksi suorittaa vahvaa sähköistä tunnistautumista sähköisiin asiointipalveluihin. Jatkuvuudenhallinnan näkökulmasta varaudutaan myös kansainvälisiin kriisitilanteisiin esim. niissä tilanteissa, joissa pääsy digitaalisen henkilöllisyystodistuksen jakelun kannalta keskeisiin palveluihin (esim. sovelluskaupat) estyy tai heikkenee.

Soveltuvia osia digitaalisen henkilöllisyystodistuksen, ulkomaalaisen digitaalisen asiointivälineen, ja luonnollisen henkilön tunnistusvälineen kokonaisuudesta on suunniteltu hankittavaksi kolmansilta osapuolilta. Näiden osakomponenttien toimittajien osalta varmistetaan siitä, että alihankintaketjujen kautta hankituissa riippuvuuksissa noudatetaan samoja tietoturvapoikkeamien käsittelyn mekanismeja kuin mitä palvelun itsensä tuottamisessa komponenteissa. Vastaava pätee myös avoimen lähdekoodin riippuvuuksissa, joita hyödynnetään palvelujen toteutuksessa. On varmistuttava siitä, että tietoja ei siirry mobiililaitteista tai luottavilta tahoilta esimerkiksi analytiikka- tai vianselvitysratkaisujen kautta ulkoisille tahoille. Näitä riskejä pyritään hallitsemaan laatimalla alihankintaketjuihin kuuluvien toimijoiden kanssa kirjalliset sopimukset heitä koskevista velvoitteista ja pyrkiä varmistumaan näiden velvoitteiden noudattamisesta.

Itsehallittavuuden myötä kokonaisuudessa tulnaisiin toteuttamaan integraatoratkaisuja, joissa hyödynnettävät protokollat ja standardit ovat uusia verrattuna moniin muihin tunnistus- ja luottamuspalvelujen toteuttamisessa käytettäviin standardeihin ja protokolliin. Tässä yhteydessä varmistetaan siitä, että standardien ja protokollien määrittelyssä on varmistuttu riittävällä tasolla riittävien eheyden ja luottamuksellisuuden takaavien tietoturvakontrollien olemassaolosta ja että mahdollisesti puuttuvia kontroleja kompensoidaan kansallisilla määrityksillä.

Digitaalisen henkilöllisyyden osalta esityksessä on huomioitu riskilähtöisyys sekä palvelujen ja ratkaisujen käyttöön liittyvät keskeisimmät uhat sekä tietoturvan että tietosuojan näkökulmasta. Lisäksi lainsäädäntö velvoittaa palvelujen tuottajat ylläpitämään ajantasaista riski- ja uhkatietoa siten, että näiden tietojen ylläpitoon ja tarvittaviin toimenpiteisiin liittyvät roolit ja vastuut ovat määriteltynä. Digitaalisen henkilöllisyyden palvelujen tietoturvakontrolleilta odotetaan myös joustavuutta, jotta voidaan varmistua niiden tehokkuudesta uusia tietoturvauhkia ja muuttuvaa uhkaympäristöä vastaan. Mobiililaitteiden osalta tietoturvakontrollien tulisi myös huomioida laitteiden elinkaaret, jotta uusia tietoturvakontroleja voidaan ottaa käyttöön sitä mukaa, kun laitevalmistajat tuovat niitä saataville.

Ratkaisuja tuottavilta toimijoilta edellytetään määrämuotoisen muutostenhallintaprosessin olemassaoloa. Muutostenhallinnan näkökulmasta on keskeistä tunnistaa tilanteet, joissa joudutaan tekemään taaksepäin yhteensopivuuden rikkovia muutoksia loppukäyttäjien ja luottavien tahojen näkökulmasta, jotta pystytään minimoimaan näiden vaikutukset palvelujen käyttöön. Muutostenhallinnan näkökulmasta keskeistä on myös määritellä tilanteet, joissa välineiden käyttö tulee estää ennen kuin käyttäjä asentaa päivitetyn sovellusversion tai tilanteet, joissa muutosten laajuus edellyttää uutta arviointilaitoksen suorittamaa vaatimuksenmukaisuuden tarkastamista.

Ehdotuksen mukainen lainsäädäntökokonaisuus asettaa selkeät suuntaviivat häiriötilanteiden hallinnan vaatimuksille ja häiriötilanteista viestimiselle. Loppukäyttäjälle on olennaista saada näkyvyys siihen, miten tämä on käyttänyt digitaalista henkilöllisyystodistustaan ja ulkomaalaisen digitaalista asiointivälinettä, sekä mahdollisuus tallentaa olennaiset käyttöön liittyvät lokitiedot turvalliseen paikkaan. Olennaista on myös määrittää rajat sille, kuinka moneen laitteeseen digitaalinen henkilöllisyystodistus tai ulkomaalaisen digitaalinen asiointiväline voidaan ottaa käyttöön. Kaikissa tilanteissa loppukäyttäjällä tulisi säilyä näkyvyys siihen, missä laitteissa digitaalinen henkilöllisyystodistus ja ulkomaalaisen digitaalinen asiointiväline on käytössä. Ehdotettu lainsäädäntö antaa mahdollisuuden digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen peruuttamisen väärinkäyttötilanteissa, jos esim. väline joutuu oikeudettomasti toisen henkilön hallintaan. Lainsäädännössä on myös mahdollisuus estää väärin käyttäytyvän asiointipalvelun mahdollisuus hyödyntää digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä, jos asiointipalvelu esim. suorittaa tietojenkalastelua.

Lainsäädäntö edellyttää palvelun toimittamisessa kykyä havaita mahdollisia väärinkäyttötilanteita, mutta tämä on suhteutettava ratkaisun itsehallittavuuteen ja yksityisyydensuojaan. Hätätilanteiden osalta ratkaisu tarjoaa kyvykkyydet estää pääsy tietoihin siten, että joko käyttäjä itse tai palveluntarjoaja voi estää pääsyn niihin. Nämä tilanteet on oltava selkeästi kuvattuina ja lisäksi loppukäyttäjille ja luottaville tahoille on voitava selkeästi viestiä miten heidän tulisi toimia mahdollisissa väärinkäyttötilanteissa.

Digitaalisen henkilöllisyyden ja ulkomaalaisen digitaalisen asiointivälineen tapauksessa henkilötietoja luovutetaan käyttäjän haltuun hänen henkilökohtaiseen mobiilipäätelaitteeseensa. Mobiilipäätelaitteiden käyttöjärjestelmätoimittajat tarjoavat uusimmissa versioissaan kyvykkyyden hyödyntää laitteiden turvaelementtejä, jolloin voidaan varmistua loogisella tasolla kryptografisia menetelmiä hyödyntäen tietojen erottelusta mobiilipäätelaitteen päässä. Toisaalta on olennaista varmistaa, että kyseinen päätelaite tarjoaa riittävät suojausmekanismit tiedon luottamuksellisuudelle ja eheydelle. Tällä voi olla vaikutusta siihen millaisissa laitteissa digitaalista henkilöllisyystodistusta tai ulkomaalaisen asiointivälinettä voidaan käyttää ja joissain tilanteissa käyttö voi estyä, jos käyttäjä ei esimerkiksi kykene päivittämään mobiilipäätelaitteensa käyttöjärjestelmäversiota vaaditulle tasolle.

Henkilökohtaisten mobiilipäätelaitteiden tapauksessa keskitetyillä palveluntuottajilla on vähemmän mahdollisuuksia kontrolloida esimerkiksi sitä, sisältääkö laite mahdollisia haittaohjelmia. Näissäkin tilanteissa tulee varmistua siitä, että haittaohjelma ei kykene vaarantamaan mobiilipäätelaitteeseen tallennettujen henkilötietojen luottamuksellisuutta ja eheyttä. Tämä edellyttää sensitiivisten tietojen eriyttämistä muista sovelluksista loogisella tasolla kryptografisia menetelmiä hyödyntäen.

Johtuen siitä, että käyttäjät voivat osoittaa henkilötietojaan suoraan luottaville tahoille, siirtyä vastuuta tietoturvan toteutumisesta luottaville tahoille. Tällöin integraatioiden turvallisuuden kannalta on keskeistä varmistaa, että luottavat tahot tekevät riittävät eheys- ja sulkulistatarkastukset. Käyntiasioinnissa tullaan hyödyntämään lähilukurajapintojen kautta tapahtuvaa tiedonsiirtoa. Sekä käyntiasioinnissa että sähköisessä asiointissa on olennaista, että tiedonsiirrossa käytetään salattua tiedonsiirtoa myös sanomatasolla.

Loppukäyttäjän tulee myös pystyä lopettamaan digitaalisen henkilöllisyystodistuksen, ulkomaalaisen digitaalisen asiointivälineen, tai luonnollisen henkilön tunnistusvälineen käyttö. Kun käyttäjä lopettaa näiden välineiden käytön tietyllä laitteella, niin tulee kyetä varmistumaan siitä, että kyseiselle laitteelle käyttöön otettua välinettä ei ole enää mahdollista käyttää ja että tiedot poistetaan turvallisesti. Tietojen poistaminen on mahdollistettava käyttäjän omin toimenpitein myös etänä, jos käyttäjä esimerkiksi menettää mobiilipäätelaitteensa hallinnan.

Salausavainten hallinnan näkökulmasta ydinidentiteetin todisteeseen kytkeytyvän salausavainmateriaalin luomisessa on varmistuttava turvallisten avaintenluontimekanismien käytöstä. Lisäksi pitää varmistua siitä, että avainmateriaalit ovat itsehallittavia eli vain kyseisen henkilön hallinnassa ja että ne eivät paljastu missään tilanteessa esimerkiksi palvelun taustajärjestelmille. Tietoturva vaatimusten kautta veloitetaan käyttämään turvallisia salausalgoritmeja.

Tietoturvan varmistamisen kannalta keskeisenä osa-alueena on arviointilaitoksen määrääjain suorittaman vaatimuksenmukaisuuden arviointi. Lainsäädäntö antaa suuntaviivat käytettävien kriteeristöjen osalta, joita vasten vaatimuksenmukaisuutta arvioidaan. Kriteeristöjen valinnan osalta Digi- ja väestötietovirastolla on velvollisuus kuulla Traficomia ja Poliisihallitusta. Kriteeristöjen valintaan tulee kiinnittää huomiota siten, että sillä katetaan kokonaisturvallisuus sekä sähköisen että käyntiasioinnin osalta. Lisäksi kriteeristöjen tulee huomioida kokonaisvaltaisesti digitaalisen henkilöllisyyden palvelujen tietoturvan johtamismallin vaatimuksenmukaisuutta.

Asiointipalveluilta ei edellytetä erillistä rekisteröintiä niiden hyödyntäessä digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä sähköisessä asiointissa. Jotta loppukäyttäjät voivat varmistua siitä, että asiointipalvelut ovat niitä mitä ne väittävät olevansa, tulee Digi- ja väestötietovirasto asettamaan vaatimuksia asiointipalveluiden tunnistamisessa käytettäviltä varmenteilta. Hyväksytyjen varmenteiden myöntäjien valintaan tulee kiinnittää huomiota, jotta näillä voidaan varmentaa asiointipalvelun kytkeytyminen taustalla olevaan oikeushenkilöön. Lisäksi niissä tilanteissa, joissa asiointipalvelujen havaitaan esim. keräävän henkilötietoja väärin perustein (esim. tietojen kalastelun avulla), tulee asiointipalvelun tietojen kerääminen voida estää lisäämällä asiointipalvelun varmenne erilliselle sulkulistalle.

Etärekisteröinnin kautta käyttöön otettaviin ulkomaalaisten digitaalisiin asiointivälineisiin liittyy epävarmuustekijöitä koskien niiden varmuustasoa. Asiointipalveluille välitetään tieto siitä, perustuuko ulkomaalaisen digitaalinen asiointiväline etärekisteröintiin vai onko välineen haltijan henkilöllisyys varmennettu kasvokkain. Asiointipalvelut voivat käyttää tätä tietoa tehdäkseen riskiperustaisen päätöksen siitä, että sallivatko ne pelkän etärekisteröinnin kautta käyttöön otettujen ulkomaalaisten digitaalisten asiointivälineiden käytön palveluissaan.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Sähköisen asiointin markkinaehtoinen kehittyminen

Esityksen valmistelussa on harkittu erilaisia vaihtoehtoja esityksen tavoitteiden edistämiseksi. Ensinnäkin on harkittu vaihtoehtoa, jossa nykylainsäädäntöön ei tehtäisi merkittäviä muutoksia, jolloin sähköinen asiointi ja vahva sähköinen tunnistaminen kehittyisivät edelleen markkinaehtoisesti. Vahvan sähköisen tunnistamisen lainsäädäntöä ja palveluita on Suomessa kehitetty pitkään markkinaehtoisuudelle perustuen. Markkinoiden kehittäminen ja vauhdittaminen on kuitenkin edellyttänyt useita lainsäädäntömuutoksia tunnistus- ja luottamuspalvelulakiin (HE 83/2017 vp, HE 264/2018 vp ja HE 237/2020 vp). Laissa on säädetty muun muassa markkina-toimijoiden välisestä velvollisuudesta sopimusten tekemiseen sekä tunnistustapahtumista perittävistä enimmäishinnasta. Kyse on siten melko pitkälle markkinatoimijoiden elinkeinonvapautteen puuttuvasta sääntelystä. Sähköisen tunnistamisen saatavuus asiointipalveluille kehittyi ennen vuoden 2019 lainmuutosta hitaasti, mutta sen jälkeen tunnistusvälityspalveluiden tarjonta asiointipalveluille on lähtenyt hyvin käyntiin.

Tunnistus- ja luottamuspalvelulain sääntely tunnistamisen tietoturvallisuusvaatimuksista on teknologianeutraalia ja käyttäjille tarjottavat tunnistusvälineet ovatkin kehittyneet. Tarjolle on tullut yhä enemmän esimerkiksi mobiilisovelluksia ja tunnuslukulaitteita ja markkinoilla on viereillä useita hankkeita uusien tunnistusmenetelmien tarjoamiseksi esimerkiksi mobiilioperaattoreilla, Findy-ryhmällä ja Suomen tunnistosuuskunnalla. Kansalaisten joukossa on kuitenkin edelleen tiettyjä henkilöryhmiä, joilla ei ole tällä hetkellä mahdollisuutta saada vahvaa sähköistä tunnistusvälinettä. Useat tunnistusvälineen tarjoajat tarjoavat tunnistusvälineen esimerkiksi 15 vuotta täyttäneille ja finanssialan sääntelyssä velvoitetaan tarjoamaan tunnistusväline osana peruspankkipalvelua, mutta esteenä vahvan sähköisen tunnistusvälineen saamiselle voi olla se, että henkilöä ei ole merkitty väestötietojärjestelmään, että henkilöllä ei ole tunnistus- ja luottamuspalvelulain ensitunnistamisessa edellyttämää Suomen tai ETA-valtion, Sveitsin tai San Marinin viranomaisen myöntämää passia tai henkilökorttia eikä poliisi pysty tunnistamaan henkilöä tai että henkilöllä ei ole mahdollisuutta hankkia matkapuhelinliittymää tai pankkitiliä.

Digitaalisia palveluita käytetään yhä enemmän ja asiointi on siirtymässä monilla toimialoilla pääasiallisesti digitaalseksi. Digitaalisten palvelukanavien tullessa käytetyimmiksi laajasti yhteiskunnassa, nousee esille vielä aiempaa voimakkaampi tarve varmistaa, että jokaisella on pääsy palveluihin ja mahdollisuus ottaa osaa digitaaliseen yhteiskuntaan. Valmistelussa ei ole systemaattisesti analysoitu sitä vaihtoehtoa, että tunnistuspalveluiden tarjoajille säädettäisiin yleispalveluluonteisia tarjontavaihtoehtoja, mutta voidaan arvioida, että ainakaan ilman uutta sääntelyä vahvan sähköisen tunnistamisen markkinaehtoinen kehittyminen ei täysin takaa esityksen tavoitteiden toteutumista liittyen yhdenvertaisten edellytysten ja mahdollisuuksien tuottamiseen jokaiselle hyödyntää digitaalista henkilöllisyyttä yhteiskunnan palveluissa.

Digitaalisten palveluiden kehittyminen edellyttää myös digitaalisen henkilöllisyyden ratkaisujen kehittämistä, jotta voidaan varmistaa niiden vastaavan moderneja teknologioita hyödyntävien palveluiden vaatimuksiin. Vahvan sähköisen tunnistamisen nykyinen toimintamalli pohjautuu markkinaehtoiseen toimintaan, jossa tunnistuspalveluja tarjoavat pääasiassa yksityiset yritykset ja identiteetin hallinta on osin näiden palveluntarjoajien hallinnassa. Yhteiskunnassa on kuitenkin kasvanut tarve uudentaa palveluille, jotka mahdollistavat henkilöön liittyvien tietojen hallinnan ja käytön henkilön itsensä toimesta ja riippumatta siitä onko henkilö tietyn palveluntarjoajan asiakkaana. Asiointitapahtuman luonne ei aina vaadi tiettyjen yksilöivien henkilötietojen toimittamista asiointipalveluun. Riittävää asioinnin kannalta voi olla myös esimerkiksi pelkän iän osoittaminen ja todistaminen sähköisesti. Vahvassa sähköisessä tunnistamisessa välitettävät henkilötiedot ovat pysyneet hyvin samanlaisina eikä asiointipalveluille ole tullut tarjolle lisähenkilötietoja tai köyhdytettyjä henkilötietoja, eli esimerkiksi pelkän ikätiedon vahvistamista, tai muita pseudonymisoituja sähköisiä vahvistuksia, vaikka tunnistus- ja luottamuspalvelulaki sen mahdollistaa. Tämän esityksen tavoitteena on rakentaa edellytyksiä tällaisten monimuotoisempien palveluiden syntymiselle sekä varmistaa, että yhteiskunnassa on perusvalmius tarjota myös henkilön itsensä hallittavissa olevia henkilötietojen ja muiden vahvistettujen tietojen osoittamisen ratkaisuja. Näitä palveluita ja valmiuksia ei ole syntynyt nykyisen sähköisen tunnistamisen toimintamallin piirissä ja voidaan arvioida, että tavoitteiden saavuttaminen edellyttää muutosta myös viranomaisten vahvistaman henkilöllisyyden osalta.

Tehdään tarvittavat ratkaisut ja muutokset vasta komission eurooppalaisen digitaalisen identiteetin lainsäädännön toimeenpanon yhteydessä

Toiseksi esityksen valmistelussa on harkittu vaihtoehtoa, jossa odotettaisiin uuden eurooppalaisen digitaalisen identiteetin lainsäädännön vahvistamista. Kansalliset ratkaisut ja muutokset tehtäisiin siis vasta EU lainsäädännön kansallisten toimeenpanotoimien yhteydessä. Komission eurooppalaisesta digitaalista identiteettiä koskevasta lainsäädäntöehdotuksesta on kerrottu tarkemmin esityksen kohdassa 2.7. Komission lainsäädäntöehdotuksella on tarkoitus luoda yhteiset lainsäädännölliset raamit eurooppalaiselle digitaalisen identiteetin lompakkosovellukselle, jolla olisi mahdollista osoittaa lompakkosovelluksen haltijaan liittyviä vahvistettuja tietoja. Lompakkosovellus perustuisi myös EU:ssa ajatukselle, jonka mukaan lompakkosovelluksen haltija hallitsee itse omia tietojaan ja päättää niiden jakamisesta ja käytöstä. Tämän esityksen valmistelussa on tunnistettu, että komission lainsäädäntöehdotuksessa on monilta osin kyse vastaavanlaisesta digitaaliseen henkilöllisyyteen ja sen käyttöön liittyvästä ratkaisusta kuin tämän esityksen mukaisissa ehdotuksissa on kyse. Valmistelussa on tunnistettu riski, että esityksen mukaiset ehdotukset voivat olla osittain päällekkäisiä samaan aikaan valmisteltavan EU-lainsäädännön kanssa.

Komission lainsäädäntöehdotus sisältää jäsenvaltioihin kohdistuvan velvoitteen antaa käyttöön EU-lainsäädännön mukainen lompakkosovellus 12 kuukauden kuluessa lainsäädännön voimaantulosta. Lompakkosovelluksen voisi tarjota jäsenvaltio, jäsenvaltion valtuuttama toimija

tai jäsenvaltion tunnustama toimija eli myös vaatimukset täyttävä yksityisen sektorin toimija. On huomattava, että kyse on komission ehdotuksesta lompakkosovellusta koskevaksi lainsäädännöksi ja todennäköisesti annetun ehdotuksen sisältö tulee muuttumaan. Lopullisesta lainsäädännön sisällöstä tai voimaantulon ajankohdasta ei ole varmuutta. Voidaan kuitenkin arvioida, että EU-lainsäädäntö tulisi edellyttämään jossakin muodossa lompakkosovelluksen kehittämistä ja tarjolle saattamista jäsenvaltioissa. Lompakkosovelluksessa on kyse uudenaikaisesta sähköiseen asiointiin liittyvästä palvelusta ja vahvasta sähköisestä tunnistusvälineestä. Sen kehittämiseen on varattava riittävästi aikaa. Jos lompakkosovellukseen liittyvä kehitystyö aloitetaan vasta siinä vaiheessa, kun lopullisen EU-lainsäädännön sisältö on tiedossa, on olemassa todennäköinen riski siitä, että lompakkosovellusta ei ehditä Suomessa antamaan EU-lainsäädännön edellyttämässä määräajassa julkisen tai yksityisen sektorin toimesta, tai että kehitystyössä ei aikataulun vuoksi kyetä riittävän laadukkaaseen kansalliset tarpeet huomioivaan valmisteluun.

Kansallisen kehitystyön ja EU-lainsäädännön valmistelun samanaikaisuudessa on arvioitu olevan riski siitä, että ristiriitaisuuksia voi syntyä. Myös hallintovaliokunta on pitänyt tärkeänä, että kansallinen digitaalisen henkilöllisyyden hanke huomioi eIDAS-asetuksen muutokset siten, etteivät hankkeet ole keskenään ristiriidassa. Kustannusten ja kehitystyön päällekkäisyyden välttämiseksi tulisi valiokunnan mukaan kiinnittää huomiota kansallisen työn yhteensovittamiseen EU-valmistelun kanssa. (HaVL 34/2021 vp).

Toisaalta valmistelun samanaikaisuudesta voidaan arvioida olevan myös etua. Osittain rinnakkainen kansallinen kehitystyö lisää tietoa ja näkemyksiä siitä, millaisia teknisiä tai toiminnallisia ratkaisuja eurooppalaisessa yhteistyössä olisi tarkoituksenmukaista edistää. Näin Suomi voi harkitusti pyrkiä vaikuttamaan EU-lainsäädännön sisältöön, jotta siinä otettaisiin huomioon myös kansalliset erityistarpeet ja kansallisessa kehitystyössä toimiviksi havaitut ratkaisut. Kansalliseen kehitystyöhön liittyvällä sidosryhmäkuulemisella voidaan myös kartoittaa yksityisen sektorin toimijoiden näkemyksiä teknisistä ja taloudellisista seikoista, joihin Suomella voi olla syytä vaikuttaa EU-lainsäädäntötyössä.

Kehitetään nykyistä kansalaisvarmennetta

Ehdotettavan uuden lain digitaalisesta henkilöllisyystodistuksesta sijaan kansalaisvarmennetta voitaisiin kehittää edelleen siten, että sitä hyödynnettäisiin laajemmin yhteiskunnassa. Voimassa olevan sääntelyn nojalla tunnistusvälineinä käytetään verkkopankkitunnuksia, henkilökortin kansalaisvarmennetta, organisaatiokortin tunnistusvarmennetta ja mobiilivarmennoita. Sirulliseen henkilökorttiin ja organisaatiokorttiin sisältyy Digi- ja väestötietoviraston myöntämä kansalaisvarmenne tai tunnistusvarmenne. Varmenne mahdollistaa henkilön luotettavan tunnistamisen sähköisessä asiointissa.

Kansalaisvarmenne on kuitenkin käytössä vain 6 prosentilla tunnistusvälineiden käyttäjistä, joten sen laajamittaisempi hyödyntäminen vaatisi nykytilaan verrattuna kehitystyötä. Digi- ja väestötietovirasto teki syksyllä 2021 selvityksen henkilökortin hakemisen, käyttöönoton ja käytön asiakaspolun nykyhaasteista. Keskeisesti selvityksessä todettiin, että käyttäjän pitää ymmärtää, tietää ja osata paljon kansalaisvarmenteen käyttöönotosta ja sen hyödyntämisestä. Käyttöön tarvittavien laitteiden tekniset ominaisuudet pitää ymmärtää, jotta tietää mitä laitteita voi käyttää, mitä ohjelmistoja ja lisälaitteita ne vaativat. Lisäksi kansalaisvarmenteen hyödyntäminen vaatii erillisen lukijalaitteen, jota ei käyttöönottoprosessin yhteydessä automaattisesti tule mukana. Yhteenvedona selvityksen perusteella Digi- ja väestötietovirasto totesi, että haastavimmat puutteet liittyvät kortinlukijalaitteen ja sovelluksen käytettävyyteen. Koska aktiivisia käyttäjiä on vähän, myöskään asiointipalvelut eivät useinkaan tue kansalaisvarmenteella tunnistautumista.

Ehdotettavan sääntelyn tavoitteena on tuottaa digitaalinen henkilöllisyystodistus, joka ei ole sama kuin vahva sähköinen tunnistusväline, vaikka se sisältää myös vahvan sähköisen tunnistamisen ominaisuuden. Digitaalisella henkilöllisyystodistuksella on vahva kytkös passiin ja henkilökorttiin; se on henkilöllisyyttä osoittavana asiakirjana käytännössä näiden vaihtoehto. Se ei kuitenkaan toimi matkustusasiakirjana. Digitaalisen henkilöllisyystodistuksen myöntää Poliisi ja sen tiedot perustuvat Poliisin vahvistamiin ja rekisteröimiin tietoihin. Nykyinen kansalaisvarmenne on puhtaasti tunnistusväline, eikä sen ole arvioitu olevan teknologialtaan sillä tasolla, että varmenteen kehittäminen tulevaisuuden digitaalseksi henkilöllisyystodistukseksi olisi tarkoituksenmukaista. eIDAS-kehityksen myötä digitaalisen henkilöllisyystodistuksen sisältämä ydinidentiteetin todiste voi olla myös jokin muu kuin varmenne. Nykyisen kansalaisvarmenteen sääntely pohjautuu varmennepalvelusääntelyyn, ja voidaan arvioida, ettei nykyinen varmentesääntely olisi riittävä pohja digitaalisen henkilöllisyyden palvelujen kehittämiselle. Voidaan myös arvioida, ettei kansalaisvarmenteen hyödyntäminen tulevaisuudessakaan olisi digitaalisessa maailmassa tarkoituksenmukaista sen vaatiessa erillistä lukijalaitesovellusta.

Digitaalisen henkilöllisyyden palvelujen tarjoaja tulisi osaksi luottamusverkostoa

Esityksen valmistelussa on arvioitu myös vaihtoehtoa, jossa digitaalisen henkilöllisyyden palvelujen tarjoaja tulisi osaksi luottamusverkostoa sen sijaan, että sille säädettäisiin oma erillinen rooli tunnistus- ja luottamuspalvelulaissa. Kansallisesta luottamusverkostosta ja siihen liittyvästä sääntelystä on kerrottu tarkemmin esityksen jaksoissa 2.1 ja 2.2. Mikäli digitaalisen henkilöllisyyden palvelujen tarjoaja tulisi osaksi luottamusverkostoa, siihen ja sen tarjoamiin välineisiin sovellettaisiin tunnistus- ja luottamuspalvelulain sääntelyä. Digitaalisen henkilöllisyyden palvelujen tarjoajalla tarkoitetaan käytännössä Digi- ja väestötietovirastoa. Esityksen mukaan sen tehtävänä olisi tuottaa digitaalisen henkilöllisyyden sovellusta, jonka avulla digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä on mahdollista käyttää.

Digitaalisella henkilöllisyystodistuksella ja ulkomaalaisen digitaalisella asiointivälineellä mahdollistettaisiin henkilöllisyyden osoittaminen sähköisesti. Käyttäjän näkökulmasta kyse olisi hyvin samankaltaisesta toiminnasta kuin mitä nykyisillä tunnistusvälineillä on mahdollista toteuttaa eli tunnistautua sähköisesti asiointipalveluun palveluiden käyttämiseksi. Esityksen tavoitteiden mukaisesti digitaalisella henkilöllisyystodistuksella sekä ulkomaalaisen digitaalisella asiointivälineellä edistetään henkilön mahdollisuuksia hallita omia julkisissa palveluissa olevia tietojaan. Tästä syystä ne perustuvat hyvin erilaiseen toimintamalliin, kuin nykyisin luottamusverkostossa tarjottava tunnistusvälineet. Tämä merkitsee käytännössä, että käytettäessä digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä henkilön sähköiseen tunnistamiseen, niistä välittyvät tiedot eivät välttämättä vastaa sitä tietokokonaisuutta, jota nykyisin edellytetään luottamusverkostossa välitettävän tunnistautumisen yhteydessä. Toisena keskeisenä toimintamalliin liittyvänä erona on, että digitaalisen henkilöllisyyden palvelujen tarjoajalle ei tule tietoa siitä, kun henkilö käyttää digitaalisen henkilöllisyyden sovellusta sähköiseen asiointiin. Näin ollen digitaalisen henkilöllisyyden palvelujen tarjoajan ei ole mahdollista veloittaa tunnistus- ja luottamuspalvelulain mukaista tunnistustapahtumakohtaista hintaa.

Mikäli digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä tarjotaisiin tunnistusvälineinä luottamusverkostossa, ei niitä olisi mahdollista toteuttaa edellä kuvatuilla tavoilla vaan ainakin niiltä osin toimintamallia tulisi muuttaa. Tämä tarkoittaisi kuitenkin sitä, että esityksellä ei enää yhtä voimakkaasti kyettäisi edistämään henkilön mahdollisuuksia hallita omia julkisissa palveluissa olevia tietojaan.

Asemaa luottamusverkoston ulkopuolella puoltaa osaltaan myös, että vaikka digitaalisella henkilöllisyystodistuksella ja ulkomaalaisen digitaalisella asiointivälineellä mahdollistettaisiin myös henkilöllisyyden osoittaminen sähköisesti, eivät ne kuitenkaan pelkisty vain sähköisiksi tunnistusvälineiksi, vaan kyse on laajemmasta kokonaisuudesta. Ehdotetun digitaalisen henkilöllisyystodistuksen osalta kyse on virallisesta henkilöllisyyttä osoittavasta asiakirjasta, jonka tuottamisesta poliisi ja Digi- ja väestötietovirasto vastaavat viranomaisen ominaisuudessa. Vaikka nykyisiä tunnistusvälineitä voidaan käyttää luotettavaan sähköiseen henkilöllisyyden osoittamiseen, ei tunnistusvälineissä kuitenkaan ole kyse henkilöllisyyttä osoittavista asiakirjoista.

5.2 Ulkomainen lainsäädäntö ja muut ulkomailla käytetyt keinot

5.2.1 Tanska

Tanskaa on jo vuosia pidetty yhtenä digitalisoituneimmista Euroopan maista ja sillä on selkeä sähköisen tunnistamisen strategia. Kansallisen sähköisen tunnistamisen kehittämiseen liittyvät suuret päätökset on tehty digitalisointistrategioiden puitteissa. Strategiaa edustavat esimerkiksi asiakirjat Digital Strategy 2016-2020 ja The future infrastructure for digital identities in Denmark.

Tanskassa on käytössä sähköinen tunnistusjärjestelmä NemID, joka on kehitetty yhteistyössä julkisen sektorin ja Tanskan pankkien kanssa. NemID:n avulla voi asioida sekä julkisen että yksityisen sektorin palveluissa. Vuosien 2021 ja 2022 aikana MitID on porrastetusti korvaamassa NemID:n. MitID edustaa NemID:n uutta sukupolvea ja on käyttäjäystävällinen ja tulevaisuuteen suuntautunut avain verkkopankkiin ja digitaaliseen postiin. MitID:ssä on myös NemID:hen verrattuna monia lisäominaisuuksia ja toimintoja, esimerkiksi uusien allekirjoitusstandardien noudattaminen sekä älypuhelinpohjaiset, salasanapohjaiset ja fyysiset todennustekijät. Aiempi olemassa oleva infrastruktuuri tarkistettiin ja arvioitiin uudelleen, jotta käyttöön saatiin käsite sertifioitu sähköisen tunnistamisen välityspalvelu, joka voi välittää tunnistustapahtumia loppukäyttäjien ja asiointipalveluiden välillä. MitID:n tavoitteena on muun muassa luoda parempia hallinnollisia ratkaisuja yrityksille ja laajentaa henkilökohtaisen sähköisen tunnistamisen käyttöä siten, että käyttäjän henkilökohtainen MitID voidaan yhdistää yhteisön tunnukseseen. Lisäksi MitID:n myötä erilaiset kirjautumistavat lisääntyvät. Tämän ohella MitID erottelee sähköisen tunnistamisen ja sähköisen allekirjoittamisen, sekä mahdollistaa eri suojaustasojen palveluiden käytön.

MitID rakentuu yhdelle yhteiselle ydinidentiteetille, jota käyttävät julkisten toimijoiden lisäksi myös rahoituslaitokset ja muut yksityiset palveluntarjoajat, jotka tarvitsevat turvallisia digitaalisia identiteettitietoja. Yksi päätavoitteista on, että kaikki rekisteröidyt ydinidentiteetit ovat käytettävissä eri toimialojen ja palveluntarjoajien välillä. MitID:n kohdalla verkkopalveluntarjoajat eivät tunnista käyttäjiä itse, vaan tunnistaminen on sertifioitujen välityspalveluiden tehtävä. Välityspalveluina voivat toimia julkisen sektorin toimijat ja yksityisen sektorin toimijat, erityisesti pankit. Välityspalveluita tarjotaan kilpailluilla markkinoilla, mutta MitID:llä tunnistautuminen on maksutonta.

MitID:n käyttö tapahtuu pääasiassa puhelimeen tai tablettiin ladattavan sovelluksen avulla, mutta muina vaihtoehtoina ovat MitID code display, joka on pieni, kertakäyttöisen salasanana näyttävä laite, MitID audio code reader, joka on tarkoitettu esimerkiksi näkövammaisille, sekä MitID chip henkilöille, jotka tarvitsevat MitID-kirjautumista useita kertoja päivässä esimerkiksi työnsä vuoksi. NemID:stä on versio myös oikeushenkilöiden käyttöön, ja MitID:stä tällainen versio ollaan julkaisemassa keväällä 2022.

MitID:n kehittäminen tapahtuu valtion ja Finance Denmarkin (Tanskan pankkiyhdistyksen) yhteistyönä. MitID:ssä korvataan NemID:n aikainen jako kahteen itsenäiseen osaan – ”pankkiratkaisuun” ja teknologialtaan julkisen avaimen arkkitehtuuriin perustuvaan ”OCES-ratkaisuun” – yhteisellä identiteetillä ja uusilla todennuskeinoilla, joissa on yksi ydinidentiteetti, joka tukee todentamista ja digitaalisten henkilöidentiteetin elinkaaren käsittelyä.

Toinen sähköisen tunnistamisen ratkaisu, joka Tanskassa on käytössä, on NemLog-in. NemLog-in on kirjautumisratkaisu, joka mahdollistaa pääsyn viranomaisten itsepalveluratkaisuihin niin kunnissa, alueilla kuin valtiolla. NemLog-inin avulla sisään tarvitsee kirjautua vain kerran tunnistautuakseen kaikkiin sitä käyttäviin palveluihin. NemLogi-iniin kirjaututaan NemID:llä tai MitID:llä ja se toimii tunnistustapahtuman välittäjänä. Palveluntarjoajat käyttävät NemLog-in-tunnusta todentamiseen.

NemID:n, MitID:n ja NemLog-inin kattamien palveluiden valikoima on erittäin laaja kattaen kaikki pankki- ja vakuutussektorin tarjoamat sähköiset palvelut sekä joukon muita yksityisiä palveluita. Näiden avulla voidaan käyttää myös esimerkiksi osoitteen borger.dk palveluita. Borger.dk on virallinen yhden luukun portaali, jossa ovat saatavilla käytännössä kaikki Tanskan julkiset palvelut.

Vaikka kansallisen sähköisen tunnistamisen välineen käyttö ei ole pakollista, miljoonat Tanskan kansalaiset käyttävät sähköistä tunnistautumista ja käyttötapauksia on kuukausittain yli 60 miljoonaa. Tanska ei tällä hetkellä myönnä kansallista henkilökorttia.

5.2.2 Viro

Viro on yksi digitalisoituneimmista Euroopan maista ja yksi edistyneimmistä sähköisen tunnistamisen ratkaisujen käyttöönotossa. Virossa sähköisen tunnistamisen politiikasta ja strategiasta vastaa kaksi ministeriötä: sisäministeriö ja talous- ja viestintäministeriö.

Vuonna 2020 Viron sisäministeriö julkaisi uuden Sisäisen turvallisuuden kehittämissuunnitelman 2020–2030. Suunnitelman mukaan Viro tavoittelee vakaata ja kestävää identiteetinhallinnan järjestelmää, jossa huomioidaan turvallisuusnäkökulmat. Lisäksi suunnitelman mukaan Virossa tulee tarjota käyttäjäystävällinen ja moderni sähköisen tunnistamisen sovellusympäristö, mikä vahvistaa myös tietoyhteiskunnan kehitystä. Edellä mainittujen tavoitteiden saavuttamiseksi Virossa pyritään turvaamaan identiteetinhallinnan ja henkilöiden tunnistamisen vakaus, käyttämään moderneja teknologisia ratkaisuja ja kehittämään prosessien automatisointia, sekä laajentamaan sähköisen tunnistamisen käyttöä. Askeleita tavoitteiden saavuttamiseen ovat sellaisen henkilötodistuksen jatkuva kehittäminen johon liittyy digitaalinen todennus ja laadukkaat sähköisen allekirjoituksen luontitoiminnot, vähintään kahden erillisen julkisen sektorin sähköisen tunnistamisvälineen olemassaolon varmistaminen, kestävän ohjelmistoliiketoimintamallin ja -turvallisuuden varmistaminen sekä julkisen ja yksityisen sektorin yhteistyön varmistaminen ja kyky käsitellä riski- ja vaaratilanteita.

Virossa on käytössä useita erilaisia julkisen ja yksityisen sektorin myöntämiä sähköisen tunnistamisen välineitä. Suosituimpia ovat seuraavat seitsemän välinettä, joista kuusi ensimmäistä ovat valtion omistamia ja Euroopan unionille notifioituja (kaikkien varmuustaso ”korkea”) ja yksi yksityinen sähköisen tunnistamisen menetelmä, jota ei ole notifioitu. Kaikki välineet myönnetään vain luonnollisille henkilöille. Välineet ovat fyysinen ID-kortti kehittyneillä sähköisillä toiminnoilla, digitaalinen ID eli sähköinen väline jota voidaan käyttää vain sähköisessä ympäristössä, e-kansalaisen digitaalinen ID joka myönnetään muulle kuin Viron kansalaiselle ja jota voidaan käyttää henkilön tunnistamiseen ja sähköiseen allekirjoittamiseen vain sähköi-

sessä ympäristössä, sekä mobiili-ID joka on sähköisessä ympäristössä käytettävä väline henkilön tunnistamiseen ja sähköiseen allekirjoittamiseen. Mobiili-ID on vapaaehtoinen vaihtoehto ID-kortilla tapahtuvalle sähköiselle tunnistamiselle. Lisäksi käytössä ovat diplomaattihenkilökortti joka voidaan käyttää sekä fyysisessä että sähköisessä ympäristössä tunnistautumiseen, kolmannen maan kansalaisille myönnettävä oleskelulupakortti jota voidaan käyttää sähköisessä ympäristössä tunnistautumiseen ja sähköiseen allekirjoittamiseen, sekä smart-ID joka on yksityisen sektorin tarjoama notifiointon tunnistamisratkaisu, jota voidaan käyttää myös hyväksytyn sähköisen allekirjoituksen luomiseen. Valtion tarjoamien välineiden hankkiminen on käyttäjälle maksullista. Smart-ID on käyttäjälle maksuton, se saa rahoituksensa sitä hyödyntävien sähköisten palveluiden tarjoajilta.

Virolla ei ole lähivuosille suunnitelmia kehittää uusia menetelmiä sähköiseen tunnistamiseen, mutta päivityksiä on suunniteltu oleskelulupakortin ja ID-kortin kohdalle. Lisäksi Mobiili-ID:lle ollaan tuottamassa aiemman Mobiili-ID:n korvaavaa ratkaisua, uusi Mobiili-ID on tarjottu julkaista vuoden 2022 alussa.

Viron kansallisessa digitaalisen identiteetin viitekehityksessä valtiolla on johtava rooli sekä säätelijänä että digitaalisen identiteetin tarjoajana. Vaikka myös yksityiset palveluntarjoajat, jotka voivat toimia sähköisen tunnistamisen välittäjinä, tarjoavat vaihtoehtoisia tunnistuskeinoja, pysyy taustalla oleva identiteetti samana ja yksityiset ratkaisut hyödyntävät valtion luomaa identiteettiä.

Virossa ID-kortti on pakollinen kaikille yli 15-vuotiaille kansalaisille ja noin 99 prosenttia Viron väestöstä käyttää ID-korttia. Julkiset palvelut ovat saatavilla sähköisesti eesti.ee-portaalin kautta. Myös monia yksityisen sektorin palveluja voidaan käyttää sähköisen tunnistamisen avulla. Tietojärjestelmäviranomaisella (RIA) on merkittävä rooli sähköisen henkilöllisyyden muotoilussa ja kehittämisessä Virossa. Tietojärjestelmäviranomainen vastaa siitä, että sirullista ID-korttia voivat käyttää kaikki halukkaat. Virossa selvitetään myös mahdollisuutta ottaa käyttöön biometrisiä tunnisteita helpottamaan henkilöiden tunnistamista. Viro seuraa sähköisen tunnistamisen riskejä ja ratkaisuja yhteistyössä eri valtioiden ja kansallisten kumppaneiden kanssa.

5.2.3 Norja

Norjan BankID on yleinen sähköisen tunnistamisen järjestelmä, jota käyttävät kaikki norjalaiset pankit. BankID perustuu yhteiseen infrastruktuuriin, jossa kaikki käyttäjien yksityiset avaimet todennusta ja allekirjoitusta varten säilytetään keskitetyssä palvelussa, mikä tarkoittaa käytännössä sitä, että BankID tarjoaa etäallekirjoituspalvelun. BankID-järjestelmä edellyttää EU:n eIDAS-säätelyn mukaisesti hyväksytyjen varmenteiden käyttöä allekirjoituksiin, eli kaikkien BankID-myöntäjien on oltava hyväksytyjä luottamuspalveluntarjoajia. Huolimatta lukuisista luottamuspalveluiden tarjoajista, Norjan markkinoilla ei ole hyväksytyn sähköisen allekirjoituksen luontivälineitä tai etäpalveluita. Tämä tarkoittaa, että suurin osa sähköisistä allekirjoituksista on kehittyneitä sähköisiä allekirjoituksia, jotka on myönnetty käyttämällä hyväksytyjä varmenteita.

BankID:stä on olemassa myös mobiiliversio, jossa yksityinen avain on tallennettu SIM-kortille, kuten Mobiilivarmenne Suomessa ja mID Virossa ja Liettuaassa. Kaikki norjalaiset matkapuhelinoperaattorit tekevät yhteistyötä BankID:n kanssa. BankID Mobilella on käytössään hyväksytty varmenne sähköiseen allekirjoitukseen, mutta sillä voi allekirjoittaa vain lyhyitä tekstimuotoisia lausuntoja. Norjan valtio on luonut BankID:lle vaihtoehtoisen ratkaisun nimeltään MinID. MinID:n avulla kansalaiset voivat käyttää julkisia palveluita, jotka eivät vaadi korkeinta turvallisuustasoa. Muita Norjassa käytössä olevia tunnistamisvälineitä ovat esimerkiksi yksityisen sektorin tuottamat Buypass ja Commfides.

Julkisen sektorin organisaatioilla laajasti käytössä oleva kirjautumisportaali ID-porten on tarjonnut pääsyn noin 2000 verkkopalveluun vuodesta 2020 lähtien. ID-porten on julkishallinnon ylläpitämä ja mahdollistaa useiden kirjautumistapojen käytön, kuten MinID, BankID mobile, BankID, Buypass ja Commfides. ID-porten -portaalin kautta voi kirjautua myös valtion luomaan keskitettyyn sähköisen allekirjoitus- ja työnkulttuuriportaalin.

Norja on myös kehittänyt keskitetyn asiointipisteen nimeltä Altinn. Sen tehtävänä on koota yhteen kaikki tiedot, joita kaikki eurooppalaiset palveluntarjoajat tarvitsevat yrityksen perustamiseen Norjassa. Julkiselle sektorille raportoivassa Altinnin-portaalissa on juridisesti sitova suositusratkaisu, joka koostuu todentamisesta, suostumuksesta sekä tapahtumaketjun aikaleimalla tallentavasta lokista.

Norjassa QWAC-palveluita tarjotaan sekä paikallisille että kansainvälisille markkinoille. Hyväksytyjä sähköisiä leimoja tarjotaan, mutta validointipalveluita ei ole. Julkisen sektorin organisaatiot käyttävät ei-hyväksyttyä sähköistä jakelupalvelua. Hyväksytyille luottamuspalveluille on olemassa vahvat yritysmarkkinat. Yleensä työntekijälle myönnetään erillinen sertifikaatti käytettäväksi työsuhteen yhteydessä, usein yhdessä yrityksen sähköisen leiman kanssa.

Norjassa ei ole tällä hetkellä Euroopan unionille notifioitua sähköisen tunnistamisen järjestelmää, vaikka halua notifiointiin on esiintynyt. Kansalaisten tunnistuspalveluiden käytössä BankID hallitsee selvästi Norjan markkinoita ja arviot sen käyttöasteesta väestön keskuudessa vaihtelevat 90–98 prosentin välillä. BankID Mobilen markkinaosuus on noin 50 prosenttia. Valtion ylläpitämä MinID-järjestelmä on käytön laajuuden suhteen kaukana tästä, sillä valtion ID-porten -portaalissa on kuukausittain yli kymmenen kertaa enemmän BankID-kirjautumisia kuin MinID-kirjautumisia. COVID-19-pandemialla on ollut suuri vaikutus Norjan sähköisten palveluiden käyttöön, käyttömäärät ovat kasvaneet moninkertaisesti verrattuna pandemiaa edeltävään aikaan.

Koska Norjan lainsäädännössä hyvin harvoin edellytetään allekirjoittamista, nojaa verkkoasiointi Norjassa vahvasti todentamiseen yhdessä tarkastuslokien kanssa. Jos allekirjoitus vaaditaan, on kehittynyt sähköinen allekirjoitus hyväksytyllä varmenteella yleisin, koska tällä hetkellä tarjolla ei ole hyväksytyjen allekirjoitusten luontivälineitä, joten Norjan markkinoilla ei ole hyväksyttyä allekirjoitusratkaisua.

5.2.4 Alankomaat

Alankomaiden Digitaalisen hallinnon Agenda (DIGibeter) korostaa digitaalisen identiteetin merkitystä ja kuvailee sitä digitaalisen hallinnon pilariksi. Agendassa kuvattuja toimia ja prioriteetteja ovat muun muassa turvallisten sähköisten tunnistamismenetelmien käytön laajentaminen, avoimen sähköisen tunnistamisjärjestelmän saatavuuden varmistaminen, digitaaliseen identiteettiin liittyvien sovellusten kehittäminen yhdessä Hollannin kuntaliiton kanssa ja piloteissa kymmenen kunnan kanssa sekä verkkoasioinnin mahdollistaminen toisen henkilön tai yrityksen puolesta. Edistymisestä raportoidaan parlamentille kahdesti vuodessa.

Alankomaissa on tällä hetkellä käytössä kaksi sähköisen tunnistamisen järjestelmää: DigiD luonnollisille henkilöille ja eHerkenning oikeushenkilöille. DigiD koostuu käyttäjätunnuksesta ja salasananasta sekä valinnaisesta lisävarmennusvaiheesta tekstiviestillä tai vaihtoehtoisesti DigiD-mobiilisovelluksen kautta. Palvelut veloitetaan julkishallinnolta. Tällä hetkellä DigiD:n tai eHerkenningin käyttö ei ole pakollista, paitsi digitaalisissa julkishallinnon palveluissa kuten sähköisessä veroilmoituksessa. Sekä DigiD:n että eHerkenningin käyttö on viime vuosina lisääntynyt merkittävästi.

Alankomaissa on valmisteilla digihallintolaki, jonka tarkoituksena on mahdollistaa kansalaisten ja yritysten kirjautuminen valtion palveluihin turvallisesti ja luotettavasti, jotta kansalaiset voivat hyödyntää sähköistä tunnistamista ja nykyistä luotettavampaa turvatasoa. Lain mukaan avoimet standardit ovat pakollisia. Laissa kuvataan myös standardit tunnistusvälineiden tarjoajille.

Alankomaissa on tällä hetkellä sekä julkisia että yksityisiä sähköisen tunnistamisen palveluntarjoajia. Verkkoasiointi julkisissa palveluissa edellyttää DigiD:n käyttämistä. Digihallintolain mukaan sähköinen pääsy julkisiin palveluihin on kuitenkin sallittu yksityisten yritysten tai julkisen ja yksityisen sektorin yhteistyössä kehittämien digitaalisten identiteettiratkaisujen kautta. Oikeushenkilöiden käyttämän eHerkennyksen kohdalla käyttäjät voivat valita valtion tunnustamien yksityisten tunnistuspalveluntarjoajien välillä.

Alankomaisessa henkilökortissa on NFC-tekniikka ja kortti voidaan skannata, jotta kansalaisen DigiD-tiliä voidaan käyttää arkaluontoisempiin palveluihin ja arkaluontoisempiin tietoihin. Hallituksella on myös suunnitelmia nostaa tunnistamismenetelmien turvallisuustasoa. Sekä DigiD että eHerkennykseen on notifioitu eIDAS-varmuustasoltaan korotetuksi ja korkeaksi.

5.2.5 Saksa

Saksan liittovaltion talous- ja energiaministeriön Digitaalinen strategia 2025 asettaa kymmenen askelta, jotta Saksasta tulisi Euroopan digitalisoiduin valtio. Strategian viides askel "Tietoturvan vahvistaminen ja tiedollisen autonomian kehittäminen" korostaa sitä, että Saksa tasoittaa tietä sähköisen tunnistamisen kansainväliselle käyttöönnotolle ja asettaa standardit EU:n laajuiselle turvalliselle ja luotettavalle sähköiselle asioinnille.

Saksassa on viime vuosina laadittu sähköistä tunnistamista koskevaa lainsäädäntöä. Sähköisen tunnistamisen edistämisestä annetun lain (Gesetz zur Förderung des elektronischen Identitätsnachweises) voimaantulo vuonna 2017 edisti sähköisen tunnistamisen käyttöä kansallisen eID-kortin kautta. Ensimmäiset eID-kortit – kansalliset henkilökortit eID-lisätoiminnoilla – julkaistiin jo vuonna 2010. Uusi lainsäädäntö kuitenkin edisti eID-toiminnallisuuden aktivointia ja käyttöä. Lisäksi muut organisaatiot ja yritykset voivat tarjota sähköisen tunnistamisen ratkaisuja. Lainsäädäntö yksinkertaistaa yritysten ja viranomaisten valtuutusprosessia tunnistuspalvelujen tarjoamiseen. Toinen sähköistä tunnistamista koskeva laki Onlinezugangsgesetz tuli voimaan elokuussa 2017. Lain mukaan liittovaltion, osavaltioiden ja kuntien on tarjottava hallintopalvelujaan digitaalisesti vuoteen 2022 mennessä.

Digitaalisen Saksan yhdeksän kohdan suunnitelman mukaan yksi Saksan tavoitteista on sähköisen identiteetin perustaminen kolmella tavalla: eID-lisätoimintojen käyttöönotto matkapuhelimissa – muun muassa online ID-toiminto, sähköisen tunnistamisen käytön helpottaminen muun muassa optimoimalla PIN-koodin palautusmenettely ja käyttö yritysverkoissa, sekä teollisuuden ottaminen mukaan sähköisen tunnistamisen kaupalliseen käyttöön.

Kansallisen henkilökortin ja henkilökorttiin aktivoitavan eID-lisätoiminnon lisäksi Saksassa asuvat EU:n ulkopuoliset kansalaiset voivat saada sähköisen oleskeluluvan (Aufenthaltstitel). Nämä tunnistusvälineet on notifioitu yhden sähköisen tunnistamisjärjestelmän kahtena osana rajat ylittävään käyttöön eIDAS-asetuksen mukaisesti.

Saksan henkilökorttilaki (Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis) astui voimaan 1.11.2019. Henkilökortti on fyysinen kortti, joka sisältää sirun, ja jolla voidaan tunnistautua sähköisesti erilaisiin julkisiin ja yksityisiin palveluihin. Henkilökortin eID-lisätoiminnallisuutta

voivat käyttää myös sellaisen EU-maan kansalaiset, joiden kotimaassa ei (vielä) ole notifioitua sähköisen tunnistamisen järjestelmää riippumatta siitä, oleskelevatko nämä henkilöt Saksassa vai eivät. Kortti voidaan myöntää vähintään 16-vuotiaalle EU:n tai ETA-alueen kansalaiselle ja se on voimassa kymmenen vuotta. Kortin hankkiminen on maksullista. eID-kortti on tarkoitettu sähköiseen tunnistautumiseen, eikä se korvaa passia tai henkilöllisyystodistusta, joten eID-korttia ei voi käyttää matkustusasiakirjana. eID-kortilla voi kuitenkin tunnistautua myös paikan päällä ja sitä voi käyttää joko yhdessä tietokoneen tai älypuhelimien kanssa.

Julkisen identiteetin hallinnan ja tunnistamisen järjestelmän lisäksi Saksassa on myös yksityisen sektorin ratkaisuja. Ratkaisujen toimivuus on kuitenkin alempi kuin valtion välineillä, ne eivät esimerkiksi vastaa rahanpesun vastaisen direktiivin (EU) 2015/849 mukaisten sähköisen tunnistamisen vaatimuksia.

Muita sähköisen tunnistamisen ratkaisuja, jotka käyttävät osittain uudelleen saksalaista eID:tä, ovat Deutsche Postin kehittämä PostID-järjestelmä, jonka avulla käyttäjät voivat arkistoida henkilötiedot alkuperäisen tunnistamisen jälkeen ja käyttää niitä uudelleen muihin prosesseihin, pankkijärjestelmiin kerättyihin tietoihin perustuva sähköinen tunnistamisratkaisu Identity Giro, säästöpankkien ja osuuspankkien YES-järjestelmä, jonka avulla käyttäjät voivat käyttää verkkopankkipalveluita, sekä Verimi, joka on kirjautumisratkaisu, jossa käyttäjät voivat tallentaa henkilökorttinsa tai ajokorttinsa tunnistautuakseen ja voidakseen rekisteröityä ja käyttääkseen tätä rekisteröintiä erilaisiin kumppanipalveluihin, tällä hetkellä enimmäkseen rahoitus- ja vakuutusyhtiöiden palveluihin.

eID-kortin käyttöönoton ohella Saksan painopiste on yhdeksänkohtaisen suunnitelman mukaan mobiilin eID:n käyttöönotossa. Kehitteillä on myös useita uusia sähköisen tunnistamisen ratkaisuja. Tällainen on esimerkiksi tällä hetkellä testaukseen saatavilla oleva järjestelmä SmartLogin, joka tarjoaa käyttäjälle pääsyn Smart Walleettiin, johon käyttäjä voi tallentaa henkilötietonsa ja käyttää niitä eri palveluntarjoajien kanssa.

Eräs Saksassa suunnitteilla oleva kehityskohde on erilaisten sähköisen tunnistamisen keinojen kautta saavutettavien palveluiden määrän laajentaminen. Esimerkiksi YES-järjestelmä antaa käyttäjille mahdollisuuden hyödyntää henkilötietojaan muiden palveluntarjoajien hyväksi. Lisäksi liittovaltion talous- ja energiaministeriön rahoittaman OPTIMOS-hankkeen tavoitteena on ottaa käyttöön Secure eID -sovellus sähköisen tunnistamisen palvelulla, joka tukee verkkotunnistusta ja -todennusta sekä henkilötietojen siirtoa.

Osa Saksan sähköisen tunnistamisen ratkaisuista perustuu valtion vastuulla oleviin ratkaisuihin ja osa yksityisten toimijoiden kehittämiin. Toisaalta kansallinen eID-kortti on täysin julkisen sektorin palvelu, jossa valtio toimii identiteetin tarjoajana. Muut edellä esitellyt eID-välineet ovat yksityisten yritysten toimittamia – näiden kohdalla valtio toimii sähköisen tunnistamisen välittäjänä identiteetin tarjoajien ja palveluntarjoajien yhdistämisessä.

Lokakuun 2018 tilastojen mukaan Saksassa oli yli 75 miljoonaa eID-korttia ja 12 miljoonaa sähköistä oleskelulupaa. eID-kortti mahdollistaa pääsyn yli 60 palveluun, joiden tarjoajiin kuuluu sekä julkisia että yksityisiä toimijoita. Liittovaltion palveluihin voi päästä yhden portaalin kautta, mutta koska useita digitaalisia palveluita hallitaan paikallisella tasolla, yhden yhteyspisteen periaatteen edistämä sähköisen tunnuksen käyttö on täysin tehokasta vasta kun liittovaltion ja paikalliset portaalit on yhdistetty. Kansallista eID-korttia käyttämällä voi kuitenkin asioida myös paikallistason portaaleissa. Yleinen tiedottaminen sähköisten tunnistamisvälineiden käyttöön liittyen tapahtuu erillisen verkkosivuston kautta.

Saksassa sähköisen tunnistamisen käyttöä vahvistetaan entisestään vuoteen 2022 mennessä, jolloin liittovaltion, osavaltioiden ja kuntien on tarkoitus tarjota Saksassa kaikkia hallintopalveluita digitaalisesti hallintoportaalien kautta ja linkittää nämä portaalit verkkoon, johon pääsee myös eID-kortilla ja muilla helppokäyttöisillä tunnistamiskeinoilla. Mitä korkeampi hallinnollisen palvelun turvallisuustaso on, sitä korkeammat ovat vaatimukset käytettävälle tunnistusvälineille. eID-korttiin tulevaisuudessa suunnitellut muutokset keskittyvät lähinnä pieniin säätöihin sirun lukemiseen käytettävään pääsyprotokollaan liittyen. Sormenjälkien liittäminen korttiin on nykyään pakollista.

6 Lausuntopalaute ja jatkovalmistelu

6.1 Lausuntopalaute

Valtiovarainministeriö pyysi lausuntoja luonnoksesta hallituksen esitykseksi digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi lausuntopalvelu.fi-järjestelmän kautta aikavälillä 21.2.–8.4.2022. Lausuntopyyntöön saapui lausuntoja määräajassa yhteensä 651 kappaletta. Näistä 127 lausuntoa tuli organisaatioilta. Kymmenen vastaajaa ilmoitti, että heillä ei ole asiaan lausuttavaa. Lisäksi luottamusverkoston toimijoilta tiedusteltiin lausuntoa vielä määräajan päätyttyä erikseen. Tiedusteluun vastanneet vahvistivat, etteivät jätä asiasta erikseen lausuntoa vaan kertoivat yhtyvnsä etujärjestöjen (Finanssiala ry:n tai FiComin) lausuntoihin. Kansalaispalautteena saatuja lausuntoja saapui määräajassa yhteensä 524 kappaletta. Lausunnot ja lausuntotivistelmä ovat nähtävillä valtioneuvoston hankeikkunassa (hanketunnus VM092:00/2021). Selkeä enemmistö vastanneista organisaatioista piti esityksessä ehdotettuja tavoitteita ja ratkaisuja yleisesti ottaen kannatettavina. Lausunnoissa nähtiin, että digitaalisten palvelujen ja sähköisen asioinnin nopea yleistyminen ja kehittyminen luovat tarvetta henkilön itse hallitsemaalle digitaaliselle identiteetille niin julkisissa kuin yksityisissä asiointipalveluissa.

Lausuntopalautteessa nostettiin toistuvasti esille, että kansallisen digitaalisen henkilöllisyystodistuksen ja siihen liittyvien palvelujen kehittämisessä tulee huomioida samanaikaisesti EU-tasolla käynnissä oleva eIDAS-muutosehdotus ja eurooppalaisen digitaalisen identiteetin lainsäädännön kehittäminen. Lausuntopalautteen perusteella hallituksen esityksen perusteluja on täydennetty niin, että esityksestä kävisi selkeämmin ilmi ehdotettavan lainsäädännön ja eIDAS-muutosehdotuksen suhde. Kilpailu- ja kuluttajaviraston lausuntopalautteen johdosta kilpailuvaikutuksia on täydennetty kuvauksella esityksen mukaisten ehdotusten suhteesta tunnistusmarkkinoiden kehittämiseen.

Myös Digi- ja väestötietovirasto nosti lausunnossaan esiin, että Suomen lainsäädäntö ei saa muodostaa estettä eurooppalaisen identiteettilompakon toteutukselle. Digi- ja väestötietoviraston lausunnon mukaan digitaalisen henkilöllisyyden liittäminen vahvasti nykyisiin, fyysisiin tunnistusasiakirjoihin estäisi tulevaisuudessa suomalaisten digitaalisten identiteettilompakkojen täysimääräisen hyödyntämisen. Lausunnon mukaan jo nyt tehtävän ratkaisun perustana tulisi olla Digi- ja väestötietoviraston vahvistama digitaalinen identiteetti, jolla olisi ratkaisun tietoturvallisuuteen perustuva elinkaari erillään digitaalisesta henkilöllisyystodistuksesta. Lausuntopalautteen johdosta hallituksen esityksessä ehdotettua sääntelyä on muutettu niin, että Digi- ja väestötietoviraston tuottamalla ydinidentiteetin todisteella olisi itsenäinen, tietoturvallisuuteen perustuva voimassaoloaika. Näin ollen ydinidentiteetin todisteen voimassaolo ei olisi sidottu digitaalisen henkilöllisyystodistuksen perustana olevan henkilöllisyyttä osoittavan asiakirjan voimassaoloon.

Lausuntopalautteessa toivottiin, että yksityisen sektorin toimijoille mahdollistettaisiin palveluiden luominen valtion tuottamaan ydinidentiteettiin pohjautuen. Myös Liikenne- ja viestintämi-

nisteriö korosti lausunnossaan, että ydinidentiteetin todiste tulisi suunnitella siten, että sitä voidaan tulevaisuudessa hyödyntää myös yksityisen sektorin tuottamissa lompakkosovelluksissa ja mahdollistaa siten vastaavien tuotteiden kehittäminen ja kilpailu myös yksityisellä sektorilla. Esityksen perusteluja on tarkennettu lausuntopalautteen johdosta niin, että esityksestä kävisi selkeästi ilmi tulevaisuuden tavoitteena olevan mahdollistaa myös yksityiselle sektorille ydinidentiteetin todisteen hyödyntäminen niiden tuottamien palvelujen perustana. Esityksessä ehdotettuun sääntelyyn ei kuitenkaan ehdoteta muutoksia.

Digi- ja väestötietovirasto nosti lausunnossaan esiin, että esityksessä tulisi ottaa kantaa siihen, miten kansalaisen on mahdollista varmistua hyödyntävän palvelun identiteetistä osoittaessaan omia henkilötietojaan. Esitystä on täydennetty Digi- ja väestötietoviraston lausunnon pohjalta uusilla säännöksillä ehdotettuun lakiin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista. Lakiehdotukseen lisättiin 8 §, jossa säädettäisiin luottavan osapuolen todentamisesta ja todentamiseen liittyvien tietojen rekisteristä ja 26 §, jossa säädettäisiin luottavan osapuolen ilmoitusvelvollisuudesta.

Finanssiala ry ja Kilpailu- ja kuluttajavirasto toivat lausunnoissaan esille, että ehdotetussa lainsäädännössä on kysymys kansalaisen hallussa ja käytössä olevasta tunnistusvälineestä ja sen sääntelystä ja tästä syystä lainsäädännöstä tulee käydä tarkasti ilmi digitaalisen henkilöllisyystodistuksen ja luonnollisen henkilön tunnistusvälineen haltijan oikeudet ja velvollisuudet. Ehdotettuun lakiin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista on lausuntopalautteen johdosta lisätty uusi 28 §, jossa säänneltäisiin digitaalisen henkilöllisyyden soveluksen oikeudetonta käyttöä koskevista vastuunrajoituksista.

Ulkomaalaisen digitaalisen asiointivälineen osalta lausuntopalautteessa nostettiin esiin haasteena, että asiointipalvelut joutuvat itse määrittelemään sen, hyväksyvätkö ne asiointivälineellä pääsyn palveluihinsa silloin, kun asiointiväline ei yllä luotettavuudeltaan vahvan sähköisen tunnistamisen tasolle. Lausuntopalautteen mukaan voisi olla tarkoituksenmukaista säätää erikseen tiedoista, jotka edellyttävät korkeamman varmuustason asiointivälineen käyttämistä. Lausuntopalautteen pohjalta esitykseen ei kuitenkaan ehdoteta muutoksia, sillä tällainen sääntely voisi rajoittaa mahdollisuutta hyödyntää asiointivälinettä asiointipalveluihin tunnistauduttaessa. Asiointipalveluiden tarjoajilla itsellään on parhaat edellytykset arvioida, mitä palveluita voidaan tarjota henkilölle, joka käyttää tunnistautumiseen etärekisteröintiin perustuvaa asiointivälinettä. Tästä syystä on tarkoituksenmukaista, että asiointipalvelut tekevät itse riskiarvioihin pohjautuen päätökset siitä, miten asiointivälinettä voi hyödyntää niiden palveluissa.

Useat lausunnonantajat pitivät ulkomaalaisen digitaalisen asiointivälineen käyttöä haastavana, jos väline ei saa vastaavaa asemaa kuin vahvalla sähköisellä tunnistamisella on. Hallituksen esityksessä ehdotettua sääntelyä on muutettu lausuntopalautteen perusteella niin, että siitä kävisi selkeämmin ilmi, että ulkomaalaisen digitaalisia asiointivälineitä voi olla luotettavuudeltaan kahdenlaisia riippuen siitä perustuuko asiointiväline vain etärekisteröintiin vai kasvokkain tunnistamiseen. Lisäksi ehdotettua sääntelyä on täydennetty niin, että ulkomaalaisen digitaalinen asiointiväline saisi vahvan sähköisen tunnistamisen aseman silloin, kun henkilö on tunnistettu kasvokkain ja myös asiointivälineellä tapahtuvaa henkilön tunnistamista voitaisiin välittää tunnistus- ja luottamuspalvelulain mukaisessa luottamusverkostossa.

Tietosuojavaltuutetun toimisto piti lausunnossaan hyvänä, että rekisterinpitäjät sekä rekisterinpitäjien vastuut nyt kysymyksessä olevien käsittelytoimien osalta on ehdotuksessa määritetty selkeästi ja tietosuojasetuksen sallima kansallinen liikkumavara huomioiden. Oikeusministeriön lausunnon mukaan esityksen merkittävimmät täydennystarpeet liittyvät tietosuojan ja tietoturvallisuuden riskien arviointiin ja ministeriö esitti lausunnossaan useita yksityiskohtaisia

huomioita ja tarkennusehdotuksia tietosuojaa koskeviin lainsäädäntöehdotuksiin sekä niiden perusteluihin. Hallituksen esityksen sääntelyä ja sen perusteluja on täydennetty oikeusministeriön lausunnossa ehdotetuilla tavoilla. Myös esityksen vaikutusarvioita henkilötietojen suojaan ja tietoturvallisuuteen on täydennetty lausuntopalautteen johdosta.

Oikeusministeriön lausunnossaan esittämän arvion mukaan lakiehdotusten ja niiden säännöskohtaisten perustelujen sekä toisaalta tietosuoja-asetuksen 4 artiklan 1 kohdan määritelmän ja johdanto-osan 51 kappaleen valossa ehdotettava sääntely tarkoittaisi selvästi kasvokuvien osalta biometristen tietojen käsittelyä. Oikeusministeriön mukaan säätämisyjärjestystä koskevat perustelut vaatisivat näiltä osin muutoksia ja täydentämistä. Hallituksen esityksen jatkovalmistelussa on tehty oikeusministeriön lausuntopalautteen johdosta arviointia kasvokuvien biometrisestä käsittelystä. Oikeusministeriön esittämästä arviosta huolimatta esityksessä on pitäydytty jo aiemmin esitykseen sisältyneessä arvioissa, jonka mukaan kyse ei ole biometristen tietojen käsittelystä. Esityksen säätämisyjärjestystä koskevia perusteluja on kuitenkin täydennetty tältä osin.

Useissa lausunnoissa kannatettiin sitä, että laissa asetetaan selkeä vaatimus digitaalisen henkilöllisyyden tietojärjestelmän turvallisuudelle ja hyväksymismenettelylle. Liikenne- ja viestintävirasto Traficom lausunnossa pidettiin tärkeänä ja kannatettavana sitä, että laissa esitetään säädettäväksi tietoturvaluusvaatimukset ja että Digi- ja väestötietovirasto kuulisi Traficomia ennen kuin se antaa tietoturvaluusvaatimuksia koskevan päätöksen. Poliisihallitus nosti kuitenkin lausunnossaan esiin tarpeen säännellä tarkemmin digitaalisen henkilöllisyydestä koko-naisturvaluudesta siten, että myös käyntiasioita koskevien ratkaisujen turvallisuus tulee selkeästi huomioiduksi. Hallituksen esitykseen ei kuitenkaan ehdoteta lausuntopalautteen perusteella tarkempaa sääntelyä digitaalisen henkilöllisyydestä turvallisuusvaatimuksista. Tällainen yksityiskohtainen sääntely ei olisi tarkoituksenmukaista teknologian kehittyessä sekä standardien muuttuessa ja päivittyessä tasaisin väliajoin. Ehdotettuun lakiin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista on kuitenkin Poliisihallituksen lausuntopalautteen johdosta tehty 5 §:ään lisäys, jonka mukaan Digi- ja väestötietovirastolla on velvollisuus kuulla myös poliisihallitusta ennen kuin se antaa päätöksen tietoturvaluusvaatimuksista.

Erityisesti työ- ja elinkeinoministeriö, Kilpailu- ja kuluttajavirasto ja FiCom lausuiivat esityksen kilpailuvaikutuksista. Kriittisiä huomioita esittivät erityisesti Kilpailu- ja kuluttajavirasto sekä FiCom. Lausunnoissa pidettiin todennäköisenä, että ratkaisuun saattaisi liittyä viranomaistoinnista erotettavaa taloudellista toimintaa. Lisäksi lausunnossa todettiin, että tulevaisuudessa lompakkosovellusten tarjoaminen voi muodostua taloudelliseksi toiminnaksi markkinoilla valitsevassa kilpailutilanteessa, eikä valtio saa saada ehdotetun uudistuksen johdosta perusteetonta etulyöntiasemaa markkinoilla. Myös Traficom, Elisan ja Telian lausunnoissa todettiin, että vaikutuksia luottamusverkoston markkinoihin ja tekniseen toimintaan ei oltu arvioitu tarpeeksi syvällisesti. Lausunnoissa tuotiin esille, että on epäselvää, miten uusi väline vaikuttaisi markkinoihin ja tunnistuspalveluiden hintoihin. Esityksen kilpailuvaikutuksia ja vaikutuksia luottamusverkoston toimijoihin on täydennetty merkittävästi lausuntopalautteen pohjalta.

Lausuntopalautteessa nähtiin esityksen puutteena, että se ei sisällä ehdotusta kansalliseksi ratkaisuksi puhelinpalveluissa tehtävään vahvaan sähköiseen tunnistamiseen. Hallituksen esitykseen ei ole lausuntopalautteen johdosta sisällytetty puhelinasiointia koskevia säännöksiä, sillä esityksen tavoitteena ei ole ehdottaa varsinaisia ratkaisuja tähän haasteeseen. Tässä yhteydessä on kuitenkin todettava, että hallituksen esityksen mukaiset ehdotukset eivät millään tavoin estä tai rajoita mahdollisuutta puhelinasiointinissa tehtävän vahvan sähköisen tunnistamisen ratkaisujen kehittämiseen Suomessa.

Esitykseen tehtiin lausuntopalautteen perusteella lisäksi useita muita teknisiä muutoksia. Lisäksi esityksen vaikutusten arviointia on täydennetty lausuntopalautteen perusteella.

Ehdotetusta lainsäädännöstä saatu kansalaispalaute oli lähes poikkeuksetta kriittistä. Erityisesti annetussa palautteissa nostettiin esiin huoli Suomen valtion arvioidusta muuttumisesta kontrollivaltioksi ja huoli digitaalisen henkilöllisyystodistuksen pakollisuudesta, näkemyksiä järjestelmän tarpeettomuudesta sekä tietoturvallisuuteen liittyviä epäilyjä. Syynä palautteelle vaikuttaisi olevan virheellisesti tehdyt tulkinnat hankkeen tavoitteista ja ehdotetun lainsäädännön sisällöstä. Esityksen tavoitteena ei ole lisätä valtion kontrollimahdollisuuksia suhteessa kansalaisiin vaan päinvastoin parantaa kansalaisten mahdollisuutta hallita omia tietojaan entistä paremmin ja turvallisemmin. Digitaalinen henkilöllisyystodistus, ulkomaalaisen digitaalinen asiointiväline tai luonnollisen henkilön tunnistusväline eivät olisi pakollisia eikä kenenkään tarvitsisi ottaa sellaista vastoin tahtoaan käyttöönsä. Lausuntopalautteen johdosta näitä asioita on pyritty nostamaan selkeämmin esiin hallituksen esityksessä.

6.2 Jatkovalmistelu

Monissa lausunnoissa otettiin kantaa luonnollisen henkilön tunnistusvälineen käyttöalaan. Lähtökohtaisesti mahdollisuutta hyödyntää luonnollisen henkilön tunnistusvälinettä myös yksityisen sektorin palveluissa kannatettiin. Käyttöalan laajentamisen mahdollisuutta selvitettiin jatkovalmistelun aikana. Selvitysten perusteella kävi kuitenkin ilmi, että käyttöalan laajentaminen olisi haasteellista erityisesti kilpailuoikeuteen liittyvien kysymysten takia, sillä markkinoilla on jo tarjolla vastaavanlaisia tunnistusvälineitä. Esitykseen ei tästä syystä ehdoteta muutoksia luonnollisen henkilön tunnistusvälineen käyttöalaan. Luonnollisen henkilön tunnistusvälineen käytötarvetta kuitenkin seurataan.

Yhdenvertaisuusvaltuutettu nosti esiin lausunnossaan, että linjaukset ja käytännöt, joiden mukaan vahvoja sähköisiä tunnistusvälineitä ei voitaisi myöntää avustajaa käyttävälle vammaiselle henkilölle, ovat ongelmallisia yhdenvertaisuuslain näkökulmasta. Lausuntopalautteen mukaan tulisi harkita mahdollisuutta selventää esityksessä, että kyse ei olisi välineen oikeudettomasta käytöstä eikä luovuttamisesta toisen henkilön käyttöön silloin, kun vammaisen henkilön avustaja avustaa vammaista henkilöä tämän pyynnöstä välineen käyttämisessä. Jatkovalmistelussa selvitettiin, olisiko ehdotettuja täsmennyksiä mahdollista tehdä kansallisen ja EU-sääntelyn sallimissa rajoissa. EU-sääntelyyn liittyvän tulkinnan osalta näkemystä kysyttiin myös muilta EU-jäsenvaltioilta. Vastausten perusteella muissa jäsenvaltioissa on tulkittu EU:n varmuustasoasetusta vastaavalla tavalla kuin Suomessa eikä tunnistusvälineitä ole myönnetty henkilöille, jotka eivät käytännössä pysty tai eivät oikeudellisesti voi käyttää tunnistusvälinettä itsenäisesti. Esitykseen ei tästä syystä ehdoteta muutoksia.

Yhdenvertaisen sähköisen asioinnin mahdollistaminen on kuitenkin tärkeää, vaikka tässä esityksessä ei ole ratkaistu kaikkia tähän liittyviä lausuntopalautteessa esiin nostettuja haasteita. Jatkossa olisikin selvitettävä eri vaihtoehtoja haasteiden ratkaisemiseksi. Selvitettäviä vaihtoehtoja olisivat mahdollisuudet kansallisen sääntelyn muuttamiseen esimerkiksi siten, että tiettyjä EU-tasoisia vaatimuksia ei edellytettäisi kansallisella tasolla taikka siten, että valtuutuksen kehittämiselle ja käytölle luotaisiin edellytyksiä. Samassa yhteydessä olisi tarkoituksenmukaista arvioida vielä myös luonnollisen henkilön tunnistusvälineen käyttöalan laajentamista käyttötarpeen ja yhdenvertaisuuden näkökulmasta. Yhdenvertaisuuden näkökulmasta olisi tarkoituksenmukaista samassa yhteydessä arvioida myös sen mahdollistamista, että luonnollisen henkilön tunnistusvälineen hankkimiseksi voisi saada toimeentulotuen yhteydessä maksusitoumuksen tietyin ehdoin.

7 Säännöskohtaiset perustelut

7.1 Laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista

1 luku. Yleiset säännökset.

1 §. Soveltamisala. Pykälässä säädettäisiin lain soveltamisalasta. Pykälän mukaan laissa säädettäisiin Digi- ja väestötietoviraston tuottamista digitaalisen henkilöllisyyden palveluista sekä niiden hyödyntämisestä. Digitaalisen henkilöllisyyden palveluilla tarkoitettaisiin digitaalisen henkilöllisyyden tietojärjestelmää, ydinidentiteetin todistetta, ulkomaalaisen digitaalista asiointivälinettä, digitaalisen henkilöllisyyden hallintapalvelua sekä lukijarajapintaa ja tarkastussovellusta.

2 §. Määritelmät. Pykälä sisältäisi olennaiset laissa käytetyt käsitteet ja niiden määritelmät. Pykälän *1 kohdan* mukaan laissa tarkoitettaisiin digitaalisen henkilöllisyyden palveluilla Digi- ja väestötietoviraston tuottamia digitaalisen henkilöllisyyden tietojärjestelmää, ydinidentiteetin todistetta, ulkomaalaisen digitaalista asiointivälinettä, digitaalisen henkilöllisyyden hallintapalvelua, lukijarajapintaa ja tarkastussovellusta. Pykälän *2 kohdan* mukaan ydinidentiteetillä tarkoitettaisiin sellaista väestötietojärjestelmään rekisteröityjen henkilötietojen kokonaisuutta, jonka avulla henkilöllisyys voidaan yleisesti yksilöidä, ja joka koostuu VTJ-lain 13 §:n 1 momentin 1 ja 2 kohdassa tarkoitetuista tiedoista. Kyseiset tiedot ovat henkilön täydellinen nimi ja henkilötunnus, syntymäaika, yksilöintitunnus sekä tekninen tunnistetieto ja sähköinen asiointitunnus. Pykälän *3 kohdan* mukaan laissa tarkoitettaisiin vahvistetuilla tiedoilla viranomaisen sähköisesti varmentamia henkilötietoja. Kyse olisi tiedoista, jotka ovat peräisin viranomaisen hallinnoimasta tietovarannosta tai rekisteristä, ja joiden aitouden ja muuttumattomuuden viranomainen on teknisesti varmentanut. Pykälän *4 kohdan* mukaan digitaalisella henkilöllisyystodistuksella tarkoitettaisiin digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:n mukaista poliisin myöntämää todistusta. Pykälän *5 kohdan* mukaan teknisellä alustalla tarkoitettaisiin käyttäjän mobiilipäätelaitetta, johon digitaalinen henkilöllisyystodistus tai ulkomaalaisen digitaalinen asiointiväline sisältyy. Pykälän *6 kohdan* mukaan digitaalisen henkilöllisyyden sovelluksella tarkoitettaisiin henkilöllisyystodistuksen haltijan mobiilipäätelaitteella sijaitsevaa sovellusta, joka mahdollistaa digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen käytön. Henkilö lataisi itse sovelluksen puhelimeensa, jonka jälkeen olisi mahdollista ottaa todisteet käyttöönsä. Pykälän *7 kohdan* mukaan laissa luottavalla osapuolella tarkoitettaisiin luonnollista henkilöä tai oikeushenkilöä, jolle digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen haltija osoittaa henkilöllisyytensä tai vahvistettuja tietoja. Oikeushenkilöiden osalta kyse olisi erilaisista sähköisistä asiointipalveluista tai fyysisistä asiointipisteistä, joissa on tarve tunnistaa henkilö tai vahvistaa tiettyjä häneen liittyviä tietoja palvelujen tarjoamista varten. Luottavan osapuolen tietojen käsittelyn tarkoitus ei olisi määritelmän kannalta merkityksellinen, vaan olennaista olisi, että digitaalisen henkilöllisyyden tai ulkomaalaisen digitaalisen asiointivälineen haltijalla olisi tarve osoittaa henkilöllisyytensä tai siihen liittyviä vahvistettuja tietoja, ja vastavuoroisesti luottavalla osapuolella olisi tarve voida luottaa näihin tietoihin. Pykälän *8 kohdan* mukaan käyntiasioinnilla tarkoitettaisiin asiointitilanteita, joissa digitaalisen henkilöllisyystodistuksen haltija ja luottava osapuoli ovat läsnä samanaikaisesti samassa paikassa ja digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai muita häneen liittyviä vahvistettuja tietoja luottavalle osapuolelle. Kyse olisi kasvokkain tapahtuvasta vuorovaikutustilanteesta, jossa digitaalisen henkilöllisyystodistuksen haltijalla olisi tarve osoittaa henkilöllisyytensä tai häneen liittyviä muita vahvistettuja tietoja luottavalle osapuolelle. Merkitystä ei olisi sillä, tapahtuisiko todistuksen esittäminen toiselle luonnolliselle henkilölle yksityiselämän piirissä vai esimerkiksi elinkeinonharjoittajan edustajalle. Käyntiasioinnilla ei kuitenkaan tarkoitettaisi esimerkiksi tilanteita, joissa henkilö on läsnä fyysisessä tilassa, mutta asioi automaatin tai muun teknisen päätelaitteen kanssa.

3 §. *Digitaalisen henkilöllisyyden palvelujen rekisterinpitäjä.* Pykälässä säädettäisiin digitaalisen henkilöllisyyden palvelujen rekisterinpitäjästä. Digitaalisen henkilöllisyyden palveluilla tarkoitettaisiin digitaalisen henkilöllisyyden tietojärjestelmää, ydinidentiteetin todistetta, ulkomaalaisen digitaalista asiointivälinettä, digitaalisen henkilöllisyyden hallintapalvelua sekä lukijarajapintaa ja tarkastussovellusta. Kyseisten rekisterien tietosisällöstä säädettäisiin erikseen omassa pykälässään, mutta tässä pykälässä säädettäisiin kunkin rekisterin rekisterinpitäjästä ja rekisterinpitoon liittyvästä tietosuoja-asetuksen mukaisesta kansallisesta liikkumavarasta. Kyseistä liikkumavaraa sovellettaisiin siten kaikkiin digitaalisen henkilöllisyyden palvelujen rekistereihin, joita Digi- ja väestötietovirasto tuottaa.

Tietosuoja-asetuksen 4 artiklan 7 kohdan mukaan rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä tietosuoja-asetuksen 6 artiklan 3 kohdan mukaisen kansallisen liikkumavaran puitteissa, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Tietosuoja-asetuksen kansallisen liikkumavaran puitteissa on mahdollista säädellä 6 artiklan 1 kohdan c ja e alakohdassa tarkoitettujen käsittelyn tarkoituksesta, jonka on oltava tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Kansallinen liikkumavara mahdollistaa erityisen sääntelyn, jolla mukautetaan tietosuoja-asetuksen soveltamista muun muassa koskien rekisterinpitäjän suorittaman tietojenkäsittelyn lainmukaisuutta, yhteisöjä joille ja tarkoituksia joihin henkilötietoja voidaan luovuttaa sekä käsittelytoimia ja –menettelyjä. Lisäksi jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhtainen sillä tavoiteltuun oikeutettuun päämäärään nähden. Rekisterinpitäjäksi tulee joka tapauksessa osoittaa sellainen taho, joka tosiasiallisesti käyttää rekisterinpitäjälle kuuluvaa määräysvaltaa ja voi toteuttaa rekisterinpitäjälle kuuluvat velvoitteet. Digitaalisen henkilöllisyyden palvelujen tuottamisen yhteydessä tapahtuvan henkilötietojen käsittelyn oikeusperuste olisi tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta.

Ehdotetun pykälän mukaan Digi- ja väestötietovirasto olisi digitaalisen henkilöllisyyden palvelujen tuottamisen yhteydessä tapahtuvan henkilötietojen käsittelyn rekisterinpitäjä ja vastaisi tältä osin tietosuoja-asetuksen rekisterinpitäjälle asettamista velvoitteista. Tuottamisen yhteydessä tapahtuva henkilötietojen käsittely kattaisi muun muassa henkilötietojen riittävästä tietoturvasta huolehtimisen sekä palvelujen tuottamiseksi välttämättömien henkilötietojen yhdistämisen digitaalisen henkilöllisyyden tietojärjestelmän tarjoamiseksi. Pykälän toisen virkkeen mukaan Digi- ja väestötietovirastolla ei olisi kuitenkaan oikeutta digitaalisen henkilöllisyyden palvelujen tuottamisen yhteydessä käsiteltävien henkilötietojen luovuttamiseen luottavalle osapuolelle. Tässä olisi hyödynnetty tietosuoja-asetuksen kansallista liikkumavaraa ja säädetty henkilötietojen luovuttaminen käsittelytoimena Digi- ja väestötietoviraston rekisterinpitäjyyden ulkopuolelle. Digitaalisen henkilöllisyyden palveluissa, käytännössä digitaalisen henkilöllisyyden tietojärjestelmässä, käsiteltävien henkilötietojen osoittaminen luottaville osapuolille olisi täysin luonnollisen henkilön omassa hallinnassa: henkilö voisi itse päättää mille taholle ja missä yhteydessä hän osoittaisi henkilöllisyytensä ja vahvistettuja tietojaan.

Digitaalisen henkilöllisyyden palveluihin sisältyvä digitaalisen henkilöllisyyden tietojärjestelmä mahdollistaisi digitaalisesta henkilöllisyydestä annetun lain 3 §:n mukaisen poliisin tuottaman digitaalisen henkilöllisyydestä käytön. Digitaalisesta henkilöllisyydestä annetun lain 5 §:ssä säädettäisiin rekisteristä digitaalisista henkilöllisyydestä, jota poliisi ylläpitäisi ja jonka rekisterinpitäjänä poliisi toimisi.

2 luku. Digitaalisen henkilöllisyyden tietojärjestelmän olennaiset vaatimukset ja niiden arviointi

4 §. *Digitaalisen henkilöllisyyden tietojärjestelmä.* Pykälässä säädettäisiin digitaalisen henkilöllisyyden tietojärjestelmästä, joka olisi keskeinen uusi Digi- ja väestötietoviraston tarjoama digitaalisen henkilöllisyyden palvelu. Pykälän 1 *momentissa* säädettäisiin Digi- ja väestötietoviraston tehtäväksi tuottaa digitaalisen henkilöllisyyden sovellusta ja siihen liittyvästä taustajärjestelmästä koostuvaa digitaalisen henkilöllisyyden tietojärjestelmää. Tietojärjestelmä muodostuisi luonnollisen henkilön tekniselle alustalleen asentamasta sovelluksesta ja siihen liittyvästä Digi- ja väestötietoviraston hallinnoimasta taustajärjestelmästä. Ehdotetun momentin mukaan digitaalisen henkilöllisyyden tietojärjestelmän avulla tulisi voida osoittaa vahvistettuja tietoja sähköiselle asiointipalvelulle tai käyntiasioinnissa käytettävälle päätelaitteelle. Vahvistettujen tietojen osoittamisella tarkoitettaisiin digitaalisen henkilöllisyyden tietojärjestelmää hyödyntävän luonnollisen henkilön suorittamaa vahvistettujen tietojen osoittamista luottavalle osapuolelle joko sähköisessä asiointissa tai käyntiasioinnissa. Termillä ”osoittaminen” viitataan tilanteisiin, jossa rekisteröity antaa oman harkintansa perusteella tietonsa luottavalle osapuolelle.

Ehdotetun 2 *momentin* mukaan digitaalisen henkilöllisyyden tietojärjestelmän tarkoituksena on mahdollistaa ulkomaalaisen digitaalisen asiointivälineen ja digitaalisesta henkilöllisyydestä annetun lain mukaisen digitaalisen henkilöllisyydestodistuksen tuottaminen ja hyödyntäminen. Saman tietojärjestelmän ehdotettaisiin siis toimivan sekä digitaalisen henkilöllisyydestodistuksen että ulkomaalaisen digitaalisen asiointivälineen teknisenä toteutuksena. Tietojärjestelmää käytettäisiin digitaalisen henkilöllisyydestodistuksen tuottamiseen esimerkiksi siten, että digitaalisesta henkilöllisyydestodistuksesta annetun lain mukainen digitaalisen henkilöllisyydestodistuksen haltija, eli teknisellä alustallaan mobiilisovellusta käyttävä luonnollinen henkilö, todistaisi sähköisesti luottavalle osapuolelle henkilöllisyytensä ja päättäisi tässä yhteydessä tiettyjen vahvistettujen tietojen osoittamisesta luottavalle osapuolelle. Vahvistettuja tietoja voisi osoittaa digitaalisen henkilöllisyyden tietojärjestelmällä myös käyntiasioinnissa siten, että mobiilisovellusta käyttävä luonnollinen henkilö osoittaisi luottavalle osapuolelle henkilöllisyytensä mobiilisovelluksella ja tämän jälkeen osoittaisi käyntiasioinnissa tarvittavat vahvistetut tiedot luottavalle osapuolelle langattomia lähilukuyhteyksiä hyödyntäen.

5 §. *Laatu- ja tietoturvallisuusvaatimukset.* Pykälässä säädettäisiin digitaalisen henkilöllisyyden tietojärjestelmää koskevista keskeisistä laatu- ja tietoturvallisuusvaatimuksista. Digi- ja väestötietoviraston tulisi viranomaisena noudattaa tiedonhallintalain 4 luvussa säädettyjä julkisen hallinnon tietoturvallisuuden perustason vaatimuksia sen tuottaessa digitaalisen henkilöllisyyden tietojärjestelmää. Ehdotettu pykälä sisältäisi erityiset vaatimukset, jotka kohdistuisivat digitaalisen henkilöllisyyden tietojärjestelmään tiedonhallintalaissa säädettyjen tietoturvallisuuden perustason vaatimusten lisäksi sekä niiden tarkennuksena. Sääntelyn tarkoituksena ei olisi siis poiketa tiedonhallintalaissa yleisesti säädetystä.

Pykälän 1 *momentissa* säädettäisiin, että tietojärjestelmän olisi oltava aina käytettävissä ja sillä olisi oltava tarpeelliset varajärjestelmät häiriötilanteiden varalle. Säännöksen tarkoituksena on varmistaa, että tietojärjestelmän häiriö tai toimintakatkos ei vaaranna sen avulla tuotettavia palveluita, tai siihen sisältyvien tietojen turvallisuutta. Digi- ja väestötietoviraston olisi tehtävä tarvittavat toimenpiteet, jotta tietojärjestelmän toiminta voidaan varmistaa kaikissa olosuhteissa. Tällä tarkoitettaisiin erityisesti sellaisia varajärjestelmiä, joiden avulla toiminta voidaan turvata häiriötilanteiden aikana. Vaatimus tietojärjestelmän katkeamattomasta käytettävyydestä edellyttäisi kuitenkin käytännössä myös organisaation toiminnassa tehtävää varautumista.

Pykälän 2 momentti sisältäisi erityiset vaatimukset tietojärjestelmän tietoturvallisuudelle. Digi- ja väestötietoviraston olisi huolehdittava tietojärjestelmän tietoturvallisuudesta hallinnollisilla ja teknisillä toimenpiteillä siten, että vaatimukset täyttyvät. Hallinnollisilla toimenpiteillä tarkoitettaisiin tietojärjestelmän hallinnoinnin tai viraston toiminnan järjestämistä vaatimusten edellyttämällä tavalla. Teknisillä toimenpiteillä tarkoitettaisiin teknisiä menettelyitä ja ratkaisuja. Pykälän 2 momentin 1 kohdan mukaan Digi- ja väestötietoviraston olisi huolehdittava, että tietojärjestelmä ja siinä käsitellyt tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Momentin 2 kohdan mukaan Digi- ja väestötietoviraston olisi huolehdittava, että tietoja ja tietojärjestelmiä eivät voi muuttaa muut kuin siihen oikeutetut. Edellytys olisi keskeinen digitaalisen henkilöllisyyden tietojärjestelmän avulla tuotettavien palveluiden kannalta. Digitaalisen henkilöllisyydestodistuksen ja ulkomaalaisen digitaalisen asiointivälineen luotettavuus perustuisi tietojen muuttumattomuudelle ja ajantasaisuudelle. Momentin 3 kohdan mukaan Digi- ja väestötietoviraston olisi huolehdittava, että tiedot ja tietojärjestelmät ovat ainoastaan niiden käyttöön oikeutettujen hyödynnettävissä. Momentin 4 kohdan mukaan Digi- ja väestötietoviraston olisi huolehdittava, että tiedot ja tietojärjestelmät kestävät odotettavissa olevat edistyneet tietoturva-uhat. Digi- ja väestötietoviraston olisi toiminnassaan varmistettava, että sillä on ajantasainen tieto järjestelmien toimintaan mahdollisesti kohdistuvista uhkista ja teknologian kehityksestä. Tietojärjestelmän turvallisuutta olisi arvioitava ja kehitettävä säännöllisesti. Momentin 5 kohdan mukaan Digi- ja väestötietoviraston olisi huolehdittava, että tietoihin ja tietojärjestelmiin kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat kyetään havaitsemaan. Säännös edellyttäisi, että Digi- ja väestötietovirasto ottaa käyttöön tarvittavat tekniset ja hallinnolliset toimenpiteet, jotta poikkeamat järjestelmän toiminnassa havaitaan ja niiden johdosta ryhdytään riittäviin toimenpiteisiin mahdollisten uhkien ehkäisemiseksi.

Ehdotetun pykälän 2 momentin tietyt vaatimukset ovat vastaavia kuin eräät tietosuoja-asetuksen vaatimukset henkilötietojen käsittelyä koskien. Henkilötietojen suoja tulee turvata ensisijaisesti tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla ja kansallisesti ei tulisi säätää asiasta, josta jo säädetään yleisessä tietosuoja-asetuksessa. Tietojärjestelmän tietoturvallisuuden varmistaminen edellyttää kuitenkin myös muiden kuin tietosuoja-asetuksen 4 artiklan 1 kohdan mukaisten henkilötietojen suojaamista, joten tältä osin ehdotettu sääntely ei koske sellaisenaan henkilötietojen käsittelyä, vaan kyse on ensisijaisesti muiden tietoturvallisuuden varmistamiseksi käsiteltävien tietojen suojaamisesta. Tietoturva-vaatimuksista säätäminen ei kuitenkaan vaikuttaisi rekisterinpitäjän yleisen tietosuoja-asetuksen mukaiseen velvollisuuteen toteuttaa asianmukaiset tietoturvatoinenpiteet tai tähän liittyvään rekisterinpitäjän vastuuseen henkilötietojen käsittelyn osalta. Siltä osin kuin erityiset vaatimukset kuitenkin kohdistuisivat henkilö-tietoihin, olisi kyse tietosuoja-asetuksen 5 artiklan 1 kohdan d alakohdan mukaisen täsmällisyysperiaatteen sekä 5 artiklan 1 kohdan f alakohdassa tarkoitettujen eheyden ja luottamuksellisuuden täsmäntämisestä yksittäisessä tilanteessa kansallisen liikkumavaran puitteissa.

Pykälän 3 momentissa säädettäisiin Digi- ja väestötietoviraston velvollisuudesta päättää tietojärjestelmän tarkemmista teknisistä vaatimuksista sekä tietoturva-vaatimuksista. Viraston tehtävänä olisi määrittää tietojärjestelmälle tarkemmat tekniset vaatimukset sekä tietoturva-vaatimukset. Vaatimusten olisi kuitenkin perustuttava tähän lakiin, sähköisestä tunnistamisesta ja luottamuspalveluista annettuun EU:n asetukseen ja yleisesti tunnettuihin kansallisiin tai kansainvälisiin standardeihin. Digi- ja väestötietovirasto päättää säädettyjen vaatimusten täyttämässä ja arvioinnissa sovellettavat standardit, tekniset eritelmät tai kriteeristöt. Tällaisia standardeja ja arviointikriteeristöjä olisivat esimerkiksi kansallinen Katakri eli kansallinen turvallisuusauditoitinkriteeristö sekä kansainvälinen ISO 27001 –tietoturvallisuuden hallinnan standardi. Ennen tietoturva-vaatimuksista päättämistä Digi- ja väestötietoviraston olisi kuultava Liikenne- ja viestintävirastoa ja digitaalisen henkilöllisyydestodistuksen teknisten määritysten osalta kuultava lisäksi Poliisihallitusta. Kuulemisen tarkoituksena olisi varmistaa, että Digi- ja väestötietoviras-

ton päättämät tietojärjestelmän tekniset vaatimukset ja tietoturva vaatimukset vastaavat arviointityössä yleisesti käytettyjä tietoturva vaatimuksia, ne on valmisteltu asianmukaisesti ja ne ovat yhdenmukaisia tietojärjestelmälle ja järjestelmässä tuotetulle 6 §:ssä säädettyä tunnistusjärjestelmälle säädettyjen vaatimusten, yleisesti tunnettujen standardien ja tietoturvallisuuden arviointikriteeristöjen kanssa.

6 §. Tunnistusjärjestelmää koskevat vaatimukset. Pykälässä säädettäisiin digitaalisen henkilöllisyyden tietojärjestelmän sisältämän tunnistamisjärjestelmän vaatimuksista. Koska tietojärjestelmä mahdollistaisi sekä digitaalisen henkilöllisyydestä tuotettua että ulkomaalaisen digitaalisen asiointivälineen tuottamisen, olisi tunnistusjärjestelmiä koskevia vaatimuksia arvioitava näiden osalta erikseen. Tunnistusjärjestelmän tulisi *1 momentin* mukaan täyttää vähintään sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason vaatimukset. Vaatimusten täyttäminen olisi edellytys sille, että tunnistusjärjestelmää voidaan hyödyntää digitaalisen henkilöllisyydestä tuotettua tunnistamista. Tarkemmat vaatimukset määrittäisivät teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoa varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetun Komission täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti.

Pykälän *2 momentissa* säädettäisiin poikkeuksesta 1 momentissa säädettyyn siten, että tunnistusjärjestelmän ei tarvitsisi täyttää varmuustasojen korkea tai korotettu mukaisia rekisteröintiä koskevia vaatimuksia ulkomaalaisen digitaalisen asiointivälineen osalta. Rekisteröintiä koskevilla vaatimuksilla tarkoitettaisiin varmuustasoasetuksen liitteen osassa ”2.1. Rekisteröinti” tarkoitettuja teknisiä eritelmiä ja menettelyitä. Poikkeus koskisi kuitenkin tunnistusjärjestelmän toimintaa tai hallinnointia vain siltä osin, kun kyse on yksinomaan ulkomaalaisen digitaalista asiointivälinettä koskevista menettelyistä ja teknisistä ratkaisuista.

7 §. Ennen tietojärjestelmän käyttöönottoa julkaistavat tiedot. Ehdotetun *1 momentin* mukaan Digi- ja väestötietovirastolla olisi velvollisuus ilmoittaa julkisesti ennen tietojärjestelmän käyttöönottoa momentissa säädetty tiedot. Tietojärjestelmän käyttöönotolla tarkoitettaisiin sitä, kun tietojärjestelmää ensimmäisen kerran tarjotaan ja siten mahdollistetaan digitaalisen henkilöllisyydestä tuotettua ja ulkomaalaisen digitaalisen asiointivälineen käyttöönotto. Digi- ja väestötietovirasto voisi itse päättää, miten se julkaisee ehdotetun momentin mukaiset tiedot. Se voi tapahtua esimerkiksi viraston verkkosivuilla. Tarkoitus on, että tiedot tulevat sellaisten tahojen tietoon ja saataville, jotka aikovat hyödyntää tietojärjestelmään perustuvia palveluita, käytännössä digitaalista henkilöllisyydestä tai ulkomaalaisen digitaalista asiointivälinettä toiminnassaan.

Ehdotetun 1 momentin *1 kohdan* mukaan olisi julkaistava päivämäärä, josta alkaen luottavan osapuolen on mahdollista hyödyntää tietojärjestelmää. Tarkoitus on, että tietojärjestelmän hyödyntäjillä olisi selkeä tieto siitä, mistä alkaen tietojärjestelmää voitaisiin hyödyntää. Esimerkiksi luottamusverkoston tunnistuspalvelun tarjoajilla olisi näin saatavilla tieto siitä, mistä alkaen digitaalista henkilöllisyydestä on mahdollista hyödyntää ensitunnistamisessa tai välittää sen käyttäjiä koskevia tunnistustapahtumia luottamusverkostossa.

Ehdotetun 1 momentin *2 kohdan* mukaan ilmoitusvelvollisuus koskisi myös tietojärjestelmän ominaisuuksia ja kuvausta tarjottavista teknisistä rajapinnoista ja testausjärjestelyistä. Tarkoitus on, että näiden tietojen julkaiseminen mahdollistaisi tietojärjestelmän ja siten myös digitaalisen henkilöllisyydestä tuotettua ja ulkomaalaisen digitaalisen asiointivälineen hyödyntämisen mahdollisimman helposti ja nopeasti. Ulkomaalaisen digitaalista asiointivälinettä ja digitaalista hen-

kilöllisyystodistusta hyödyntäviä tahoja voisivat olla esimerkiksi luottamusverkoston tunnistuspalvelun sekä muut digitaalisten palvelujen tarjoajat. Tietojärjestelmän ominaisuuksien osalta ilmoituksen tulisi sisältää tiedot niistä seikoista, jotka ovat tarpeen tunnistusvälityspalvelulle, kun digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä hyödynnetään luottamusverkostossa. Ilmoituksen tulisi sisältää tiedot siitä, mitä tunnistetietoja henkilöstä on saatavilla digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen kautta. Tunnistetiedot jaetaan EU:n eIDAS-asetusta tarkentavassa rajat ylittävää tunnistamista koskevassa komission täytäntöönpanoasetuksessa (EU) 2015/1501 pakollisiin ja valinnaisiin. Teknisten rajapintojen ja testausjärjestelyjen osalta olisi ilmoitettava ainakin tieto siitä, minkä protokollan mukaisia rajapintoja on tarjolla.

Ehdotetun 1 momentin 3 kohdan mukaan tulisi ilmoittaa myös tieto suoritetusta vaatimustenmukaisuuden arvioinnista. Tietojärjestelmän vaatimustenmukaisuuden arvioinnista säädettäisiin ehdotetun lain 10 §:ssä. Sen mukaan tietojärjestelmän vaatimustenmukaisuus on osoitettava tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Ilmoituksessa voisi siis olla arviointilaitoksen antama todistus osoituksena suoritetusta vaatimustenmukaisuuden arvioinnista. Tieto vaatimustenmukaisuuden arvioinnista olisi tarpeen, jotta digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen hyödyntäjät voivat varmistua siitä, että niiden tuottamiseen liittyvä tietojärjestelmä täyttää sille asetetut vaatimukset.

Ehdotetun 1 momentin 4 kohdan mukaan Digi- ja väestötietoviraston olisi ilmoitettava myös muista toiminnan kannalta välttämättömistä ehdoista. Mahdollisia muita toiminnan kannalta välttämättömiä ehtoja voisivat käytännössä olla esimerkiksi muiden kuin luottamusverkostoon kuuluvien eli rekisteröimättömien tunnistuspalvelun tarjoajien ja Digi- ja väestötietoviraston oikeudet ja velvollisuudet sekä luottavien osapuolten eli hyödyntäjien ja näiden mahdollisten palveluntarjoajien väliset vastuut. Luottamusverkoston tunnistuspalveluiden oikeuksista ja velvollisuuksista digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen hyödyntämisessä ja välittämisessä säädetään tunnistus- ja luottamuspalvelulaissa.

Ehdotetun 2 momentin mukaan Digi- ja väestötietoviraston olisi viipymättä julkaistava ehdotuksessa 1 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista. Ilmoitus olisi tehtävä myös toiminnan lopettamisesta.

Ehdotetun pykälän mukaisella julkaisulla voidaan nähdä olevan kaksi pääasiallista tarkoitusta, joissa yhdistyy nykyisen tunnistus- ja luottamuspalvelulain 10 ja 12 b §:n tavoitteet. Koska tunnistus- ja luottamuspalvelulain 10 ja 12 b § eivät soveltuisi digitaalisen henkilöllisyyden tietojärjestelmän tarjoajaan, olisi tarpeen säätää erikseen tietyistä perusvaatimuksista, jotka sen olisi täytettävä ja joiden täyttymisestä sen olisi ilmoitettava niille, jotka tietojärjestelmän avulla tuotettavia palveluita aikovat hyödyntää.

8 §. Luottavan osapuolen todentaminen. Pykälän 1 momentissa säädettäisiin tietoturva vaatimuksista tilanteessa, jossa digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä hyödynnettäisiin suoran teknisen rajapinnan kautta. Lain 26 §:ssä tarkoitettu luotettava osapuoli olisi todennettava tietoturvallisesti digitaalisen henkilöllisyyden sovelluksen avulla haltijan osoittaessa vahvistettuja henkilötietojaan. Luottavan osapuolen todentaminen voitaisiin tehdä luottavalle osapuolelle myönnetyn hyväksytyn varmenteen avulla tai muulla luotettavalla ja tietoturvallisella tavalla. Digi- ja väestötietoviraston tulisi varmistaa teknisen toteutuksen avulla, että digitaalisen henkilöllisyyden sovelluksen avulla olisi mahdollista tarkistaa luottavan osapuolen hyväksytty varmenne taikka muu vastaava Digi- ja väestötietoviraston määrittelemä hyväksytty todentamisen tapa.

Pykälän 2 *momentin* mukaan Digi- ja väestötietoviraston tehtävänä olisi määrittää luottavalle osapuolelle asetettavat hyväksyttävät todentamisen tavat 5 §:ssä tarkoitetussa päätöksessä osana muita digitaalisen henkilöllisyyden tietojärjestelmän tarkempia teknisiä vaatimuksia sekä tietoturva-vaatimuksia.

Pykälän 3 *momentin* mukaan luottavan osapuolen toimesta tapahtuvan haltijan vahvistettujen henkilötietojen käytön mahdollistamiseksi ja virheellisen käytön estämiseksi Digi- ja väestötietovirasto ylläpitäisi listaa todentamisessa hyväksytyistä todentamisen tavoista sekä listaa luottavalle osapuolelle myönnettyistä ei-hyväksytyistä todentamisen tavoista. Tämä voisi tarkoittaa esimerkiksi listaa hyväksytyistä varmentajista sekä listaa luottavalle osapuolelle myönnettyistä ei-hyväksytyistä varmenteista. Varmenteeseen pohjautuvassa todentamisen tilanteessa digitaalisen henkilöllisyyden sovelluksen avulla olisi mahdollista varmistaa luottavan osapuolen käyttämän varmenteen osalta, että kyseessä olisi hyväksytyn varmentajan myöntämä hyväksytty varmenne eikä varmenne ole sulkulistalla.

9 §. Ilmoitukset uhkista ja häiriöistä. Pykälässä säädettäisiin Digi- ja väestötietoviraston velvollisuudesta ilmoittaa digitaalisen henkilöllisyyden palvelujen toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä taikka palvelun keskeytyksistä. Lisäksi olisi ilmoitettava niistä toimista, joilla uhkia tai häiriöitä voidaan eri tahojen toimesta torjua sekä näiden toimenpiteiden arvioituista kustannuksista. Ilmoituksessa on kerrottava uhkan tai häiriön arvioitu kesto. Lisäksi olisi ilmoitettava, kun uhka tai häiriö päättyy. Pykälän mukaan ilmoitus tehtäisiin luottaville osapuolille, digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntäjille sekä digitaalisen henkilöllisyyden sovelluksen haltijoille, mikäli se katsotaan tarkoituksenmukaiseksi. Ehdotettu pykälä ei sisällä yksityiskohtaisia vaatimuksia siitä, miten ilmoittaminen tulisi tehdä. Digi- ja väestötietoviraston on siis harkittava kulloinkin tehokas ilmoittamistapa. Ehdotetun pykälän mukaan ilmoittaminen olisi tehtävä ilman aiheetonta viivytystä. Tiedottamisen tarkempi ajankohta jäisi siten Digi- ja väestötietoviraston harkintaan. Luottavalla osapuolella tarkoitettaisiin kaikkia digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntäjiä eli ilmoituksen kohteena olisivat sekä yksityisen sektorin että julkisen sektorin organisaatiot.

10 §. Vaatimustenmukaisuuden arviointi. Pykälässä säädettäisiin tietojärjestelmän vaatimustenmukaisuuden osoittamisesta ja arvioinnista. Pykälän 1 *momentin* mukaan tietojärjestelmän vaatimustenmukaisuus olisi osoitettava tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tietoturvallisuuden arviointilaitoksella tarkoitettaisiin Liikenne- ja viestintäviraston hyväksymiä vaatimustenmukaisuuden arviointilaitoksia, joiden toimintaan sovelletaan tietoturvallisuuden arviointilaitoksista annettua lakia (1405/2011). Tietoturvallisuuden vaatimustenmukaisuuden osoittamisesta säättäminen ei vaikuttaisi rekisterinpitäjän yleisen tietosuoja-asetuksen mukaiseen velvollisuuteen toteuttaa asianmukaiset tietoturvatoimenpiteet tai tähän liittyvään rekisterinpitäjän vastuuseen. Tietoturvallisuuden arvioiminen toimisi yleisen tietosuoja-asetuksen mukaisena ylimääräisenä suojatoimena. Digi- ja väestötietoviraston tulisi huolehtia tietosuoja-asetuksen 35 artiklan mukaisesta tietosuoja koskevasta vaikutustenarvioinnista ja huomioida tietosuoja-asetuksen tietoturvallisuutta koskevat vaatimukset.

Pykälän 2 *momentissa* säädettäisiin siitä menettelyssä, jossa arviointi on suoritettava. Digi- ja väestötietoviraston olisi tietojärjestelmän tarjoajana tehtävä hakemus arvioinnista. Tietoturvallisuuden arviointilaitos arvioi tällöin hakemuksesta täyttääkö tietojärjestelmä sitä koskevat vaatimukset esitetyn lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti. *Momentissa* säädettäisiin lisäksi, että arviointiperusteina olisi käytettävä esitetyn lain mukaisia vaatimuksia, erityisesti 5 ja 6 §:ssä säädetyt vaatimukset, sekä Digi- ja väestötietoviraston 5 §:n 3 *momentin* mukaisesti päättämiä vaatimuksia.

Pykälän 3 *momentissa* säädettäisiin, että arviointilaitoksen on annettava arvioinnista todistus sekä siihen liittyvä tarkastusraportti. Digi- ja väestötietoviraston olisi pyydettävä arvioinnista lausunto arviointilaitosten toimintaa valvovalta Liikenne- ja viestintävirastolta. Lausunnon tarkoituksena olisi varmistaa, että laadittu arviointi täyttää sille tietoturvallisuuden arviointilaitoksista annetussa laissa asetetut vaatimukset. Arvioinnin tekemiseen liittyy säännönmukaisesti myös tulkintakysymyksiä ja lausuntoinstrumentti mahdollistaa sen, että Liikenne- ja viestintävirasto voi tarvittaessa osallistua tulkintoihin liittyvään neuvontaan. Pykälän 4 *momentin* mukaan arviointilaitoksen myöntämä todistus on voimassa enintään kaksi vuotta. Käytännössä Digi- ja väestötietoviraston olisi pykälän 1 ja 3 *momentin* nojalla saatettava tietojärjestelmä tietoturvallisuuden arviointilaitoksen arvioitavaksi vähintään kahden vuoden välein. *Momentissa* säädettäisiin lisäksi, että tietoturvallisuuden arviointilaitos voi salassapitosäännösten estämättä vaatia Digi- ja väestötietovirastolta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Muuten todistuksen antamiseen sovellettaisiin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 *momenttia*, jossa säädetään todistuksen antamisesta ja tietosisällöstä.

3. luku. Ydinidentiteetin todiste

11 §. *Ydinidentiteetin todiste.* Pykälässä säädettäisiin ydinidentiteetin todisteesta ja sen tietosisällöstä. Ydinidentiteetin todisteesta säädettäisiin tämän lain yhteydessä, sillä se voisi olla varmenne tai muu vastaava tekninen todiste, eikä sen sijoittaminen VTJ-lain varmennesaäntelyyn olisi näin ollen teknologianeutraaliuden näkökulmasta perusteltua. Pykälän 1 *momentin* mukaan ydinidentiteetin todisteella tarkoitettaisiin sellaista Digi- ja väestötietoviraston tuottamaa todistetta, jonka avulla voidaan luotettavasti osoittaa, että todistetta hallitsevalle henkilölle on väestötietojärjestelmään rekisteröity ydinidentiteetin sisältämä henkilöllisyys. Ydinidentiteetin todiste toimitettaisiin aina henkilön itsensä haltuun joko digitaaliseen henkilöllisyystodistukseen tai ulkomaalaisen digitaaliseen asiointivälineeseen – todiste ei olisi itsenäinen palvelu eikä sellaista olisi mahdollista nyt esitettävän sääntelyn nojalla myöntää muuhun tekniseen alustaan. Digi- ja väestötietovirasto vastaisi tältä osin digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineeseen olennaisesti liittyvän teknisen toiminnallisuuden tuottamisesta sekä tähän liittyvistä menettelyistä. Digi- ja väestötietovirasto voisi hyödyntää ydinidentiteetin todisteen tuottamisessa VTJ-lain 61 §:n 2 *momentin* 6 kohdan mukaisia varmennehakemisto- ja sulkulistapalveluja.

Pykälän 2 *momentissa* säädettäisiin ydinidentiteetin todisteen tietosisällöstä. Ydinidentiteetin todisteeseen sisältyisivät *momentin* 1–6 kohdan mukaan henkilön VTJ-lain 11 a §:n mukainen yksilöintitunnus (1 kohta); sarjanumero (2 kohta); todisteen myöntömaa (3 kohta); todisteen voimassaoloaika (4 kohta); todisteen haltijan julkinen avain (5 kohta); sekä todisteiden allekirjoittajan tiedot (6 kohta). Ydinidentiteetin todisteen voimassaoloaika määräytyisi kulloinkin voimassa olevien tietoturvallisuuteen liittyvien määritysten mukaisesti. Ydinidentiteetin voimassaoloajasta ei säädettäisi tarkkarajaisesti laissa, sillä tietoturvallisuuteen liittyvät ratkaisut voivat muuttua ja siten vaikuttaa myös todisteen voimassaoloaikaan. Ydinidentiteetin todiste ei kuitenkaan olisi voimassa ilman, että se sijaitisi erillisellä teknisellä alustalla. Mikäli ulkomaalaisen digitaalinen asiointiväline taikka digitaalinen henkilöllisyystodistus peruutettaisiin taikka niiden voimassaolo päättyisi, päättyisi myös ydinidentiteetin todisteen voimassaoloaika.

Pykälän 3 *momentin* säädettäisiin eIDAS-asetuksen 8 artiklan 2 kohdan mukaisten varmuustasojen mukaisista vaatimuksista ja niiden kohdistamisesta ydinidentiteetin todisteeseen. Ydinidentiteetin todisteen tulisi 3 *momentin* mukaan täyttää vähintään sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason vaatimukset. Vaatimusten täyttäminen olisi edellytys sille, että

ydinidentiteetin todistetta voidaan hyödyntää digitaalisessa henkilöllisyystodistuksessa tai ulkomaalaisen digitaalisessa asiointivälineessä. Tarkemmat vaatimukset määrittäisivät teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetun Komission täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti.

12 §. Ydinidentiteetin todisteen myöntäminen. Pykälässä säädettäisiin ydinidentiteetin todisteen myöntämisestä sekä myöntämistä koskevista edellytyksistä. Pykälän *1 momentin* mukaan Digi- ja väestötietoviraston tehtävänä olisi myöntää ydinidentiteetin todiste. Todiste myönnettäisiin digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä varten, niiden käyttöönoton yhteydessä. Ydinidentiteetin todiste toimitettaisiin siihen liitettylle tekniselle alustalle siten kuin ulkomaalaisen sähköisen asiointivälineen ja digitaalisen henkilöllisyystodistuksen käyttöönotosta erikseen säädetään.

Pykälän *2 momentissa* säädettäisiin ydinidentiteetin myöntämiseen liittyvästä menettelystä. Momentin mukaan Digi- ja väestötietovirastolla olisi oikeus salassapitosäännösten estämättä saada henkilön passin tai henkilökortin voimassaolotiedot henkilökorttilain 31 §:ssä tarkoitettusta henkilökorttirekisteristä tai passilain 29 §:ssä tarkoitettusta passirekisteristä ydinidentiteetin todisteen myöntämiseksi tilanteessa, jossa todiste liitetään digitaaliseen henkilöllisyystodistukseen.

Pykälän *3 momentin* mukaan ydinidentiteetin todisteen rekisteröinnin edellytyksenä olisi varmuustasoasetuksessa säädetyn lisäksi, että henkilö on rekisteröity väestötietojärjestelmään. Käyttöönoton edellytyksenä olisi siten, että tekninen alusta on ollut todistetusti henkilön hallussa digitaalisen henkilöllisyyden tai ulkomaalaisen digitaalisen asiointivälineen myöntämisen hetkellä. Väestötietojärjestelmään rekisteröinnin osalta edellytys täyttyisi myös VTJ-lain 9 a §:n mukaisessa etärekisteröintimenettelyssä tehdyllä rekisteröinnillä.

13 §. Ydinidentiteetin todisteiden rekisteri. Pykälässä säädettäisiin ydinidentiteetin todisteiden tuottamiseen ja hallinnointiin liittyvistä rekistereistä, joiden rekisterinpitäjänä Digi- ja väestötietovirasto toimii ehdotetun 3 §:n mukaisesti. Rekistereiden ylläpitoon liittyvän henkilötietojen käsittelyn oikeusperusteena olisi tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohhta. Ehdotettavan pykälän *1 momentissa* säädettäisiin ydinidentiteetin todisteiden rekisteristä, johon tallennetaan VTJ-lain 11 a §:n mukainen yksilöintitunnus sekä muut varmenteen käytössä tarvittavat välttämättömät tekniset tiedot. Muita varmenteen käytössä tarvittavia välttämättömiä teknisiä tietoja ovat ainakin varmenteen sarjanumerot, tiedot varmenteiden myöntömaasta, varmenteiden voimassaoloajat, varmenteen haltijoiden julkiset avaimet sekä varmenteiden allekirjoittajana toimivan Digi- ja väestötietoviraston tiedot.

Pykälän *2 momentissa* säädettäisiin henkilöihin liitettyistä teknisistä alustoista pidettävästä rekisteristä, eli laiterekisteristä. Digi- ja väestötietoviraston ylläpitämään laiterekisteriin tallennettaisiin henkilöiden yksilöivät tunnistetiedot, henkilöön liitettyjen teknisten alustojen eli mobiilipäätelaitteiden tekniset tiedot sekä laitetiedot, kuten esimerkiksi laitetunnisteet. Lisäksi laiterekisteriin voitaisiin tallentaa muut ydinidentiteetin todisteen tuottamiseksi tarvittavat henkilöiden teknisiin alustoihin liittyvät välttämättömät tiedot. Laiterekisterin tiedot erottavat laitteet haltijoineen toisistaan, siinäkin tapauksessa, jos samalla henkilöllä olisi useampia laitteita. Laiterekisterin tietoja tarvittaisiin lisäksi erityisesti virheiden ja väärinkäytösten selvittelyssä sekä virheellisten toimintaketjujen jäljittämässä. Mobiilipäätelaitteen teknisten tietojen voidaan siten katsoa olevan tietosuoja-asetuksen 5 artiklassa säädettyjen periaatteiden mukaisia mukaan lukien henkilötietojen tarpeellisuutta koskeva vaatimus.

4. luku. Ulkomaalaisen digitaalinen asiointiväline

14 §. *Ulkomaalaisen digitaalinen asiointiväline.* Pykälässä säädettäisiin Digi- ja väestötietoviraston tehtävästä tuottaa ja tarjota ulkomaalaisen digitaalista asiointivälinettä. Ulkomaalaisen digitaalinen asiointiväline olisi henkilöllisyyttä koskevien tietojen sekä muiden vahvistettujen tietojen osoittamiseen tarkoitettu asiointiväline. Ulkomaalaisen digitaalinen asiointiväline olisi siis lähtökohtaisesti sellaisille ulkomaan kansalaisille tarkoitettu asiointiväline, joilla olisi tarve asioida sähköisesti suomalaisissa asiointipalveluissa. Asiointivälineen avulla muut kuin suomen kansalaiset voisivat osoittaa väestötietojärjestelmään rekisteröityjä henkilöllisyyttä koskevia tietojaan sekä osoittaa vahvistettuja tietojaan sähköisissä palveluissa. Ulkomaalaisen digitaalinen asiointiväline ei kuitenkaan olisi passiin tai henkilökorttiin verrattavissa oleva henkilöllisyyttä osoittava asiakirja.

15 §. *Ulkomaalaisen digitaalisen asiointivälineen myöntäminen.* Pykälässä säädettäisiin ulkomaalaisen digitaalisen asiointivälineen myöntämisestä. Pykälän 1 momentin mukaan Digi- ja väestötietovirasto myöntäisi ulkomaalaisen digitaalisen asiointivälineen joko henkilön asioidessa henkilökohtaisesti Digi- ja väestötietovirastossa tai VTJ-lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä. Digi- ja väestötietovirasto voisi myöntää ulkomaalaisen digitaalisen asiointivälineen ulkomaan kansalaiselle, joka on saanut suomalaisen henkilötunnuksen.

Pykälän 2 momentin mukaan Digi- ja väestötietoviraston tulisi tunnistaa henkilö VTJ-lain 9 a §:ssä tarkoitetusta matkustusasiakirjasta, kun henkilölle myönnetään ulkomaalaisen digitaalinen asiointiväline henkilökohtaisen asioinnin yhteydessä. Kasvokkain tunnistamisessa Digi- ja väestötietovirasto voisi todentaa hakijan henkilöllisyyden eli suorittaa ensitunnistamisen kasvokkain. Tunnistamisen yhteydessä tulisi lisäksi varmistua siitä, että henkilön tiedot on talletettu väestötietojärjestelmään ja hänelle on annettu henkilötunnus. Asiointivälineen myöntämisen edellytyksenä siis olisi, että henkilölle on annettu henkilötunnus. Kasvokkain tapahtuvassa tunnistamisessa ulkomaalaisen digitaalinen asiointiväline voisi olla varmuustasoltaan korkeampi kuin pelkkään etärekisteröintiin pohjautuva asiointiväline. Asiointivälineen haltija voisi myös etärekisteröintimenettelyn jälkeen käydä henkilökohtaisesti tunnistautumassa viranomaisen luona, jolloin hänen asiointivälineensä varmuustasoa voisi olla mahdollista korottaa.

Pykälän 3 momentissa säädettäisiin poikkeuksesta hallintolaissa säädettyyn. Jos ulkomaalaisen digitaalinen asiointiväline myönnettäisiin, hakijalle ei annettaisi erillistä hallintopäätöstä tai valitusosoitusta. Käytännössä asiointivälineen myöntäminen olisi osoitus myönteisestä hallintopäätöksestä, eikä erilliselle valitusosoitukselle taikka päätökselle olisi hakijan oikeusturvan kannalta erityistä tarvetta. Asiointivälineen käytön ehdot sekä muut hakijan kannalta olennaiset seikat tulisi antaa tiedoksi asiointivälineen hakemisen yhteydessä. Hakijalle annettaisiin kuitenkin kielteisestä päätöksestä hallintopäätös sekä valitusosoitus hallintolain mukaisesti.

16 §. *Ulkomaalaisen digitaalisen asiointivälineen sisältämät tiedot.* Pykälässä säädettäisiin ulkomaalaisen digitaalisen asiointivälineen tietosisällöstä. Pykälän 1 momentin mukaan ulkomaalaisen digitaalisen asiointivälineen haltijalle toimitettaisiin kopio häneen liittyvistä väestötietojärjestelmän tiedoista henkilön itsensä hallittavaksi. Itsehallittavuudella tarkoitettaisiin sitä, että ulkomaalaisen digitaalisen asiointivälineen haltijalle toimitetut tiedot olisivat tietojen toimittamisen jälkeen asiointivälineen haltijan omia tietoja, eikä viranomaisella olisi mahdollisuutta määrätä siitä, missä ja mihin tarkoituksiin henkilö omia tietojaan osoittaa. Viranomaisella ei olisi myöskään pääsyä henkilölle toimitettuihin tietoihin enää sen jälkeen, kun ne on toimitettu henkilön tekniseen alustaan, joka sisältää ulkomaalaisen digitaalisen asiointivälineen. Varmennettu kopio tiedoista toimitettaisiin fyysisesti henkilön tekniselle alustalle, eikä sitä enää toimitamisen jälkeen säilytettäisi viranomaisen tietojärjestelmässä. Alkuperäiset rekisteritiedot, joiden pohjalta henkilölle toimitettavat vahvistetut tiedot luodaan säilyvät kuitenkin viranomaisen

rekisterissä ja viranomaisen vastaa edelleen näistä alkuperäisistä tiedoista. Varmennettu kopio tiedoista tallennettaisiin fyysisesti asiointivälineen haltijan teknisen alustan eli mobiilipäätelaitteen turvaelementeille, jossa sijaitseville tiedoille viranomaisilla ei ole pääsyä. Näiden henkilön tekniselle alustalle toimitettujen tietojen käsittelyssä ei sovellettaisi henkilötietojen suojaa koskevaa lainsäädäntöä, sillä luonnollinen henkilö käsittelisi näitä omia henkilötietojaan tietosuojasetuksen 2 artiklan 2 kohdan c alakohdan mukaisesti yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa, jolloin kyseisten tietojen käsittely olisi tietosuojalainsäädännön aineellisen soveltamisalan ulkopuolella. Kyseisten tietojen käsittelyyn ei sovellettaisi myöskään tiedonhallintalakia, sillä tiedot eivät enää olisi julkisuuslain 5 §:n 2 momentin mukaisia viranomaisen asiakirjoja, kun ne eivät olisi enää viranomaisen hallussa. Vahvistetut tiedot henkilön itsensä haltuun toimittava rekisterinpitäjä vastaisi kuitenkin toimittamiensa tietojen eheydestä ja luottamuksellisuudesta tietosuojasetuksen 5 artiklan 1 kohdan f alakohdan mukaisesti siten, että mikäli tietojen toimittaminen henkilön itsensä haltuun epäonnistuisi tai tiedot olisivat virheellisiä, olisi vastuu edelleen viranomaisella.

Ulkomaalaisen digitaalinen asiointiväline sisältäisi momentissa yksilöidyt luonnollisen henkilön tiedot sellaisina, kuin ne sisältyvät väestötietojärjestelmään. Ulkomaalaisen digitaaliseen asiointivälineeseen sisältyisivät momentin 1–5 kohdan mukaan henkilön etunimi (1 kohta); sukunimi (2 kohta) syntymäaika (3 kohta); henkilötunnus (4 kohta); sekä syntymäajasta johdetut ikätodisteet (5 kohta). Momentin 5 kohdassa ikätodisteilla tarkoitettaisiin todisteita, joita voitaisiin käyttää henkilön osoittaessa ikää palveluille. Tällöin asiointitilanteessa osoitettaisiin esimerkiksi ainoastaan tieto siitä, onko henkilö täysi-ikäinen vai ei, sen sijaan, että osoitettaisiin tarkka tieto henkilön iästä. Ikätodisteiden laskemiseksi Digi- ja väestötietovirasto laskee sovelukseen vietävät ikätodisteet syntymäajan sekä lataushetken perusteella.

Pykälän 2 momentin mukaan Digi- ja väestötietoviraston olisi varmennettava 1 momentissa tarkoitetut vahvistetut tiedot ennen niiden toimittamista väestötietojärjestelmästä henkilön itsensä haltuun ulkomaalaisen digitaaliseen asiointivälineeseen. Tiedot olisi varmennettava siten, että luottava osapuoli kykenee varmistumaan tietojen oikeellisuudesta ja ajantasaisuudesta tarkistamalla varmenteen voimassaolon. Ulkomaalaisen digitaalisen asiointivälineen sisältämiin vahvistettuihin tietoihin olisi mahdollista luottaa samalla tavoin, kuin jos tiedot luovutettaisiin Digi- ja väestötietoviraston rekisteristä. Pykälässä säädettäisiin lisäksi tarkentavasti siitä, ettei Digi- ja väestötietovirastolla olisi oikeutta käsitellä henkilölle toimitettuja vahvistettuja tietoja sen jälkeen, kun tiedot on toimitettu ulkomaalaisen digitaalisen asiointivälineen haltijalle. Säännöksen tarkoituksena olisi korostaa tietojen toimittamista henkilön itsensä hallittavaksi. Digi- ja väestötietovirastolla olisi edelleen oikeus käsitellä omissa rekistereissään olevia samoja tietoja, mutta virastolla ei olisi tietojen toimittamisen jälkeen oikeutta käsitellä henkilölle toimitettuja kopioita kyseisistä tiedoista.

17 §. Ulkomaalaisen digitaalisen asiointivälineen hyödyntäminen. Pykälässä säädettäisiin siitä, millä tavalla ulkomaalaisen digitaalista asiointivälinettä voitaisiin hyödyntää. Asiointiväline voisi olla varmuustasoltaan joko heikko taikka korotettu riippuen siitä, millä tavalla ensitunnistaminen on tehty. Pykälän 1 momentissa säädettäisiin asiointivälineen hyödyntämisestä heikon tason välineenä. Momentin mukaan, mikäli ulkomaalaisen digitaalinen asiointiväline olisi myönnetty VTJ-lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä, luottava osapuoli voisi hyödyntää asiointivälinettä sen sähköisissä palveluissa vain silloin, kun lainsäädäntö ei edellyttäisi tunnistuslain tarkoittamaa vahvan sähköisen tunnistamisen käyttämistä.

Etärekisteröintimenettelystä säädetään VTJ-lain 9 a §:ssä ja se on samaa myöntöprosessia ulkomaalaisen digitaalisen asiointivälineen myöntöprosessin kanssa. VTJ-lain 9 a §:n mukaisesti etärekisteröintimenettelyn keskeisin ero perinteisiin rekisteröintimenettelyihin olisi se, ettei

henkilöä tunnistettaisiin siinä lainkaan viranomaisessa kasvokkain. Menettely perustuisi sen sijaan sähköisesti tapahtuvaan asiakirjan lukemiseen. Menettely edellyttäisi sitä, että rekisteröintiä pyytävällä henkilöllä olisi käytössään matkustusasiakirja, jonka tekniseltä osalta on mahdollista sähköisesti lukea hänen kasvokuvansa ja muut rekisteröinnissä edellytettävät tiedot. Menettelyyn sisältyvä henkilöllisyyden varmistaminen ei ylittäisi varmuudeltaan samalle tasolle kuin perinteinen kasvokkain tunnistaminen. Etärekisteröinnin yhteydessä kerättävistä tiedoista säädettäisiin VTJ-lain 9 b §:ssä.

Ulkomaalaisen digitaalisen asiointivälineen myöntöprosessin pohjautuessa etärekisteröintimenettelyyn, asiointiväline ei olisi varmuustasoltaan yhtä luotettava kuin vahvaan sähköiseen tunnistusvälineeseen pohjautuva henkilön tunnistaminen. Ulkomaan kansalainen voisi hyödyntää asiointivälinettä asioidessaan sähköisesti asiointipalveluissa, mutta asiointivälineeseen luottava osapuoli arvioisi sen, hyväksyykö se etärekisteröintimenettelyyn pohjautuvan asiointivälineen hyödyntämisen ja näin esitettävät tiedot omassa asiointipalvelussaan.

Pykälän 2 momentissa säädettäisiin asiointivälineen kasvokkain tunnistamiseen perustuvasta asiointivälineen hyödyntämisestä. Mikäli Digi- ja väestötietovirasto olisi tunnistanut ulkomaalaisen digitaalisen asiointivälineen haltijan tunnistuslain 17 §:ssä säädetyn mukaisesti, luottava osapuoli voisi hyödyntää asiointivälinettä vahvaan sähköiseen tunnistamiseen siten kuin tunnistuslaissa säädetään. Käytännössä kasvokkain tunnistaminen mahdollistaisi joko asiointivälineen myöntämisen henkilölle, jolla ei välinettä ole ennestään taikka asiointivälineen varmuustason korottamisen heikon tason välineestä korotetulle tasolle. Korotetun tason asiointivälinettä olisi käytännössä vahvan sähköisen tunnistamiseen rinnastuva väline ja sitä voitaisiin hyödyntää luottamusverkostossa siten, kuin tunnistuslaissa välineen hyödyntämisestä säädetään.

18 §. *Vahvistettujen tietojen osoittaminen sähköisessä asiointinnissa.* Pykälässä säädettäisiin ulkomaalaisen digitaalisen asiointivälineen hyödyntämisestä sähköisessä asiointinnissa. Ulkomaalaisen digitaalinen asiointiväline mahdollistaisi henkilöllisyyden ja vahvistettujen tietojen osoittamisen tunnistauduttaessa sekä julkisen että yksityisen sektorin sähköisen asiointin palveluihin. Sähköisessä asiointinnissa asiointivälineen haltija valitsisi itse vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle, eikä kyseessä olisi tiedon luovutuksesta viranomaisen rekisteristä, vaan henkilö osoittaisi itse suoraan henkilötietojaan sähköisesti niille toimijoille, jotka asiointipalvelussaan mahdollistavat asiointivälineen hyödyntämisen. Käytännössä sähköisessä asiointinnissa ulkomaalaisen digitaalista asiointivälinettä hyödynnettäisiin siten, että Digi- ja väestötietovirasto tuottaisi luottaville osapuolille tarjottavaa rajapintaa, joka mahdollistaisi asiointivälineen sisältämän ydinidentiteetin todisteen ja vahvistettujen henkilötietojen sekä ikätodisteiden käyttämisen suoraan sovelluksesta hyödyntävissä palveluissa. Henkilö osoittaisi itse henkilöllisyytensä asiointipalvelussa ja voisi tunnistustapahtuman yhteydessä valita ne tiedot, jotka hän haluaa luottavalle osapuolelle osoittaa. Sähköisen asiointin yhteydessä luovutettaisiin kuitenkin aina asiointipalvelulle tieto välineen varmuustasosta, jotta asiointipalvelu pystyisi arvioimaan tunnistamisen riittävyttä ja luotettavuutta suhteessa tunnistautumista vaativaan asiointipalveluun.

Sääntelyn lähtökohtana olisi pykälän mukaisesti haltijan oikeus itse valita vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle. Muu lainsäädäntö saattaa kuitenkin rajoittaa tätä oikeutta. Käytännössä tällainen tilanne olisi esimerkiksi, kun ulkomaalaisen digitaalista asiointivälinettä hyödynnetään Suomi.fi-tunnistuksen kautta asioidessa viranomaisen sähköisissä palveluissa. Hyödynnettäessä asiointivälinettä Suomi.fi-tunnistuksen kautta asiointivälineen haltija voisi osoittaa Suomi.fi-tunnistukselle ainoastaan ydinidentiteetin todisteen tiedot ja Suomi.fi-tunnistus toimisi muutoin voimassa olevan lain mukaisesti hakien muut väestötietojärjestelmän tiedot henkilöstä suoraan väestötietojärjestelmästä.

19 §. Rekisteri ulkomaalaisen digitaalisista asiointivälineistä. Pykälässä säädettäisiin ulkomaalaisen digitaalisista asiointivälineistä pidettävästä rekisteristä, jonka rekisterinpitäjänä Digi- ja väestötietovirasto toimisi ehdotetun 3 §:n mukaisesti. Rekisteriä ylläpidettäisiin ulkomaalaisen digitaalisen asiointivälineen tarjoamista ja tuottamista varten. Rekisteriin sisältyisi tieto ulkomaalaisten digitaalisista asiointivälineistä, niiden haltijoista ja asiointivälineiden voimassaolosta. Rekisterin ylläpitoon liittyvän henkilötietojen käsittelyn oikeusperusteena olisi tietosuojasetuksen 6 artiklan 1 kohdan c alakohhta.

20 §. Ulkomaalaisen digitaalisen asiointivälineen voimassaolo. Pykälässä säädettäisiin ulkomaalaisen digitaalisen asiointivälineen voimassaolosta, joka olisi voimassa enintään viisi (5) vuotta sen myöntämisestä. Käytännössä enimmäisvoimassaolon määrittelemisen tarkoittaisi sitä, että väline myönnettäisiin turvallisuustekijöihin perustuen. Asiointivälineen voimassaoloaika voisi olla alle viisi vuotta, mikäli sen todettaisiin olevan turvallisuuteen liittyvien perusteiden nojalla tarpeen.

21 §. Ulkomaalaisen digitaalisen asiointivälineen uusiminen. Pykälässä säädettäisiin mahdollisuudesta uusia ulkomaalaisen digitaalinen asiointiväline. Digi- ja väestötietovirasto voisi uusia ulkomaalaisen digitaalisen asiointivälineen voimassaolon asiointivälineen haltijan pyynnöstä. Asiointivälineen uusimisessa tulisi noudattaa varmuustasoasetuksen liitteen kohdassa 2.2.4 säädettyjä vaatimuksia. Liitteen kohdassa 2.2.4 on erilaiset vaatimukset koskien varmuustasoja heikko, korotettu ja korkea. Asiointiväline olisi uusittava liitteen vaatimusten mukaisesti riippuen uusittavan välineen varmuustasosta. Mikäli kyseessä olisi heikon tason väline, voisi uusiminen perustua liitteen vaatimuksiin heikon tason välineen uusimisesta. Mikäli kyseessä taas olisi korotetun tason taikka sitä korkeampi väline, olisi noudatettava mitä kyseisen tason välineen korottamisesta liitteessä säädetään.

22 §. Ulkomaalaisen digitaalisen asiointivälineen peruuttaminen. Pykälän 1 momentissa säädettäisiin ulkomaalaisen digitaalisen asiointivälineen peruuttamisesta sekä välineen haltijan pyynnöstä että Digi- ja väestötietoviraston aloitteesta. Asiointivälineen peruuttamisen yhteydessä peruutettaisiin myös siihen liitetty ydinidentiteetin todiste.

Pykälän 2 momentin mukaan Digi- ja väestötietoviraston tulisi peruuttaa ulkomaalaisen digitaalinen asiointiväline sen haltijan pyynnöstä. Lisäksi säädettäisiin Digi- ja väestötietovirastolle oikeus peruuttaa asiointiväline tai estää sen käyttö ilman pyyntöä, jos sillä on syytä epäillä, että joku muu kuin se, jolle asiointiväline on myönnetty, käyttää sitä tai että asiointivälineen käytön turvallisuus on muutoin vaarantunut.

Digi- ja väestötietoviraston olisi ilmoitettava haltijalle niin pian kuin mahdollista asiointivälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä. Tämä vastaisi tunnistus- ja luottamuspalvelulain 26 §:n 2 momentin sääntelyä, jonka mukaan tunnistusvälineen tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.

23 §. Ulkomaalaisen digitaalisen asiointivälineen myöntämiseen ja peruuttamiseen liittyvien tehtävien hoitaminen yhteispalvelussa. Pykälän nojalla myös muut viranomaiset voisivat hoitaa ulkomaalaisen digitaaliseen asiointivälineeseen liittyviä asiakaspalvelutehtäviä. Pykälän 1 momentissa säädettäisiin mahdollisuudesta hoitaa ulkomaalaisen digitaalisen asiointivälineen käyttöönottoon liittyviä tehtäviä yhteispalvelulain nojalla. Ehdotetun 1 momentin mukaan Digi- ja väestötietovirasto voisi antaa ulkomaalaisen digitaalisen asiointivälineen myöntämiseen ja peruuttamiseen sekä asiointivälineen rekisteritietojen ylläpitoon liittyviä avustavia tehtäviä yhteispalvelussa hoidettavaksi. Näihin tehtäviin voisi kuulua asiointivälineen käyttöönotto, asiointivälineen liittäminen tekniseen alustaan sekä asiointivälineen peruuttaminen sen haltijan

pyynnöstä. Tehtäväkokonaisuus ei merkittävästi eroaisi yhteispalvelulain mukaisesti hoidettavista tehtävistä eikä pitäisi sisällään julkisen vallan käyttöön liittyviä tehtäviä.

Yhteispalvelussa suoritettavaan tehtävään sovellettaisiin muuten, mitä yhteispalvelulaissa säädetään. Yhteispalvelulain 8 §:n mukaan yhteispalvelun järjestämisestä on tehtävä kahden tai useamman viranomaisen keskeinen kirjallinen, toistaiseksi tai määräajan voimassa oleva toimeksiantosopimus. Sopimuksessa on sovittava muun muassa siitä, mitä asiakaspalvelutehtäviä sopimus koskee ja missä laajuudessa niitä hoidetaan yhteispalveluna. Lisäksi on sovittava esimerkiksi salassa pidettävien tietojen ja henkilötietojen käsittelyyn liittyviä velvoitteita koskevista käytännön järjestelyistä.

Henkilötietojen käsittelystä sovittaessa olisi luonnollisesti otettava huomioon tietosuojasetuksesta johtuvat vaatimukset. Asetuksen 28 artiklassa muun muassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Artiklan mukaan toimeksiantosuhdetta on määritettävä käsittelysopimuksella tai ”muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla”, ellei käyttäjäorganisaation tehtävistä säädetä yksiselitteisesti lailla. Vaikka rekisterinpitäjällä on lähtökohtainen vastuu henkilötietojen käsittelystä ja käyttämistään henkilötietojen käsittelijöistä, asetuksen mukaan myös käsittelijä voi joutua itseensä vastuuseen rikkoessaan asetuksen säännöksiä.

Ehdotetun 3 *momentin* mukaan yhteispalvelun toimeksisaajan tulisi siirtää asia Digi- ja väestötietoviraston käsiteltäväksi, jollei se lisäselvitysten jälkeenkään voi aktivoida taikka liittää haltijan henkilöllisyyttä asiointivälineeseen taikka peruuttaa asiointivälinettä sen haltijan pyynnöstä. Digi- ja väestötietoviraston olisi tällöin otettava asia käsittelyyn ja tehdä asiassa lopullinen ratkaisu.

5 luku. Digitaalisen henkilöllisyyden palvelujen hyödyntämisestä

24 §. Digitaalisen henkilöllisyyden hallintapalvelu. Pykälässä säädettäisiin Digi- ja väestötietoviraston tehtävästä tuottaa viranomaiskäyttöön erillistä sähköistä hallintapalvelua ydinidentiteetin todisteen, ulkomaalaisen digitaalisen asiointivälineen sekä digitaalisen henkilöllisyystodistuksen hallinnoimiseksi. Hallintapalvelua olisi mahdollista käyttää digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen aktivoinnissa ja käyttönotossa, niiden linkittämisessä tekniseen alustaan sekä välineiden peruuttamiseen. Hallintapalvelua voisivat hyödyntää sellaiset viranomaistahot, joiden tehtävänä olisi toteuttaa edellä mainittuja toimia. Hallintapalvelu olisi digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen hallinnointiin liittyvä tukipalvelu. Henkilötiedot kulkisivat hallintapalvelun kautta, mutta palveluun ei tallennettaisi henkilöiden tietoja.

25 §. Lukijarajapinta ja tarkastussovellus. Pykälän 1 *momentissa* säädettäisiin Digi- ja väestötietoviraston tehtävästä tuottaa ja tarjota lukijarajapintaa ja tarkastussovellusta, joita luottavien osapuolten tulisi käyttää digitaalisen henkilöllisyystodistuksen käyntiasioinnissa. Lukijarajapinnalla ja siihen liittyvällä tarkastussovelluksella tarkoitettaisiin sellaista teknistä toteutusta tai ratkaisua, jolla digitaalisen henkilöllisyystodistuksen tietoja on mahdollista lukea toisesta laitteesta tai järjestelmästä. Tarkastussovellus voisi esimerkiksi olla erillinen tarkastussovellus, kuten koronapassien tarkastussovellus ja lukijarajapinta esimerkiksi luottavien osapuolten järjestelmiin integroitava tarkastusrajapinta.

Pykälän 2 *momentissa* säädettäisiin muun tahon mahdollisuudesta tuottaa tarkastussovellus. Digi- ja väestötietoviraston tulisi kuitenkin hyväksyä muun tahon tuottama tarkastussovellus ennen kuin sitä voidaan käyttää henkilöllisyyden ja vahvistettujen tietojen tarkastamiseen käyn-

tiasioinnissa. Digi- ja väestötietoviraston hyväksyntä olisi tarpeen, jotta voitaisiin varmistaa sovelluksen luotettavuus ja tietoturvallisuus. Pykälän 3 *momentissa* edellytettäisiin, että Digi- ja väestötietovirasto antaa tarkemmat määräykset muiden tahojen tuottamien tarkastussovellusten tietoturvallisuudelle asetettavista vaatimuksista. Vaatimuksissa olisi edellytettävä vastaavaa tietoturvan tasoa kuin Digi- ja väestötietoviraston omassa lukijarajapinnassa vaaditaan.

26 §. Luottavan osapuolen ilmoitusvelvollisuus. Pykälässä säädettäisiin luottavan osapuolen ilmoitusvelvollisuudesta sekä Digi- ja väestötietoviraston velvollisuudesta pitää rekisteriä ilmoituksen tehneistä luottavista osapuolista sekä velvollisuudesta ylläpitää ja julkaista listaa niistä. Pykälän 1 *momentissa* säädettäisiin, että luottavalla osapuolella on velvollisuus ilmoituksen tekemiseen silloin, jos luottava osapuoli aikoo hyödyntää digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä toteuttamalla suoran teknisen rajapinnan. Suorasta teknisestä rajapinnasta olisi kyse silloin, kun luottava osapuoli toteuttaa itse teknisen rajapinnan omaan asiointipalveluunsa digitaalisen henkilöllisyystodistuksen tai asiointivälineen hyödyntämistä varten, eikä muu taho tai palvelu toimi osoitettavien tietojen välittäjänä. Suorasta teknisestä rajapinnasta ei olisi kyse esimerkiksi silloin, kun luottava osapuoli hyödyntää digitaalista henkilöllisyystodistusta tai asiointivälinettä tunnistus- ja luottamuspalvelulain 2 §:n 5 kohdassa tarkoitetun tunnistusvälityspalvelun tarjoajan tai tukipalvelulain 3 §:n 1 momentin 4 kohdassa tarkoitetun tukipalvelun välityksellä. Suorasta teknisestä rajapinnasta olisi kuitenkin kyse niissä tapauksissa, kun luottamusverkoston tunnistusvälityspalvelun tarjoajat toteuttavat tarvittavat rajapinnat digitaalisen henkilöllisyystodistuksen tai asiointivälineen tietojen välittämiseksi muille luottaville osapuolille.

Ilmoitus olisi tehtävä ennen kuin digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntäminen aloitetaan. Ilmoitus olisi tehtävä myös, jos tiedoissa tapahtuu muutoksia. Ilmoitusvelvollisuudessa ei ole kyse luvasta digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntämiseen, vaan ainoastaan velvollisuudesta ilmoittaa aikomuksesta hyödyntää niitä. Digi- ja väestötietovirasto ei siis voisi estää digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntämistä sillä perusteella, että sille ei ole tehty pykälässä tarkoitettua ilmoitusta.

Ilmoitusvelvollisuuden tarkoituksena olisi, että Digi- ja väestötietovirastolla olisi digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen käyttämisen mahdollistavan digitaalisen henkilöllisyyden sovelluksen tarjoajana selkeä tieto siitä, mitkä tahot hyödyntävät digitaalista henkilöllisyystodistusta tai asiointivälinettä suoraan. Tällä olisi merkitystä erityisesti niissä tilanteissa, joissa Digi- ja väestötietovirastolla on ehdotetun 9 §:n mukaisesti velvollisuus tehdä ilmoitus luottaville osapuolille häiriö- ja poikkeamatilanteissa.

Pykälän 2 *momentissa* säädettäisiin tiedoista, jotka luottavan osapuolen tulee vähintään liittää ilmoitukseen. Näitä tietoja olisivat luottavan osapuolen nimi, luottavan osapuolen täydelliset yhteystiedot sekä tiedot tarjottavista palveluista, joissa digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä tullaan hyödyntämään. Pykälän 3 *momentin* mukaan luottavan osapuolen on viipymättä ilmoitettava 2 *momentissa* tarkoitetuissa tiedoissa tapahtuneista muutoksista. Pykälän 4 *momentissa* säädettäisiin Digi- ja väestötietoviraston olevan rekisterinpitäjä 2 *momentissa* tarkoitettujen tietojen osalta. Lisäksi säädettäisiin Digi- ja väestötietoviraston velvollisuudesta ylläpitää ja julkaista listaa niistä luottavista osapuolista, jotka ovat tehneet pykälässä tarkoitetun ilmoituksen. Digi- ja väestötietovirasto voisi julkaista listaa esimerkiksi verkkosivuillaan. Tarkoituksena olisi tarjota tietoa digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen haltijoille siitä, mitkä luottavat osapuolet mahdollistavat tietojen osoittamisen digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen avulla palveluissaan, vaikka kyse ei olisikaan tyhjentyvästä listasta.

27 §. Digitaalisen henkilöllisyyden sovelluksen haltijan velvollisuudet. Pykälässä säädettäisiin digitaalisen henkilöllisyyden sovelluksen haltijan velvollisuuksista liittyen digitaalisen henkilöllisyyden sovelluksen säilyttämiseen ja käyttämiseen. Pykälän 1 momentin mukaan digitaalisen henkilöllisyyden sovelluksen haltijan olisi säilytettävä sovellusta huolellisesti. Huolellisuusvelvoite kohdistuisi erityisesti niihin yksilöiviin tietoihin, joiden avulla sovellusta on mahdollista käyttää, kuten PIN-koodiin tai muuhun vastaavaan tunnuslukuun tai tunnisteeseen. Arvioitaessa sitä, millaisia varotoimia sovelluksen haltijalta voidaan kohtuudella edellyttää, on otettava huomioon, että sovellus sisältyy henkilön mobiililaitteeseen, jota haltija käyttää usein ja jota hän kuljettaa mukanaan. Kohtuullisiin varotoimiin kuuluisi esimerkiksi se, että laitteen, jolla sovellus on, tallella oloa seurataan olosuhteiden edellyttämällä tavalla. Varotoimien huolellisuutta arvioidaan kokonaisuutena. Sovelluksen haltijan huolellisuusvelvoite alkaa, kun hän on ottanut digitaalisen henkilöllisyyden sovelluksen käyttöön.

Pykälän 1 momentissa säädettäisiin lisäksi kiellosta luovuttaa digitaalinen henkilöllisyystodistus toisen käyttöön. Digitaalisen henkilöllisyyden sovelluksen sisältämä digitaalinen henkilöllisyystodistus tai ulkomaalaisen digitaalinen asiointiväline on tarkoitettu ainoastaan siihen liitetyn henkilön henkilöllisyyden ja vahvistettujen tietojen osoittamiseen. Esityksen sisältämien lainsäädäntöehdotusten mukaan digitaalinen henkilöllisyystodistus tai ulkomaalaisen digitaalinen asiointiväline voidaan peruuttaa, jos joku muu kuin niiden haltija käyttää digitaalista henkilöllisyystodistusta tai asiointivälinettä.

Pykälän 2 momentissa säädettäisiin digitaalisen henkilöllisyyden sovelluksen haltijan velvollisuudesta ilmoittaa, jos tekninen alusta katoaa, joutuu oikeudettomasti toisen haltuun tai sitä käytetään oikeudettomasti. Pykälässä tarkoitettaisiin sellaisen teknisen alustan eli mobiililaitteen katoamista, jossa digitaalisen henkilöllisyyden sovellus on otettu käyttöön. Ilmoitus olisi tehtävä Digi- ja väestötietovirastolle ilman aiheetonta viivytystä sen jälkeen, kun sovelluksen haltija on havainnut asian. Sovelluksen haltijan vastuu sen oikeudettomasta käytöstä päättyisi sen jälkeen, kun ilmoitus on tehty. Sitä, onko sovelluksen haltija tehnyt ilmoituksen ilman aiheetonta viivytystä, arvioidaan tapauskohtaisesti olosuhteet huomioon ottaen. Ilmoitukselle ei määriteltäisi määrättyä muotoa. Digi- ja väestötietoviraston olisi mahdollistettava ilmoituksen tekeminen kaikkina vuoden päivinä ja kaikkina vuorokaudenaikoina.

28 §. Digitaalisen henkilöllisyyden sovelluksen oikeudetonta käyttöä koskevat vastuunrajoitukset. Pykälässä säänneltäisiin digitaalisen henkilöllisyyden sovelluksen haltijan vastuusta tilanteissa, jossa toinen henkilö käyttää tai on käyttänyt digitaalisen henkilöllisyyden sovellusta oikeudettomasti. Pykälää sovellettaisiin esimerkiksi silloin kun mobiilipäätelaite, jossa digitaalisen henkilöllisyyden sovellus on otettu käyttöön, on kadonnut tai varastettu ja sen löytänyt tai anastanut henkilö onnistuu käyttämään digitaalisen henkilöllisyyden sovelluksen sisältämää digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä. Tunnistus- ja luottamuspalvelulain 27 §:ssä on nykyisin vastaavat säännökset tunnistusvälineen haltijan vastuusta tunnistusvälineen oikeudettomasta käytöstä. Vastaavasti maksupalvelulaissa on säännelty maksupalvelun käyttäjän vastuusta maksuvälineen oikeudettomasta käytöstä.

Pykälän 1 momentissa säädettäisiin tyhjentävästi niistä tilanteista, joissa digitaalisen henkilöllisyyden sovelluksen haltija vastaa sovelluksen sisältämän digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen asiointivälineen oikeudettomasta käytöstä. Sovelluksen haltija voisi momentin 1 kohdan mukaan joutua vastaamaan sellaisesta oikeudettomasta käytöstä, joka johtuu siitä, että sovelluksen haltija on luovuttanut sovelluksen toisen käyttöön. Säännöksessä tarkoitettua luovutuksesta olisi kyse silloin, kun sovelluksen haltija tietoisesti ja vapaaehtoisesti luovuttaa sovelluksen hallinnan toiselle. Säännös ei siis koskisi esimerkiksi tilanteita, joissa sovelluksen haltija väliaikaisesti luovuttaa toiselle säilytettäväksi laukun, jossa on sovelluksen sisältävä mobiilipäätelaite.

Momentin 2 kohdan mukaan sovelluksen haltija voisi joutua vastuuseen sovelluksen oikeudettomasta käytöstä, jos teknisen alustan katoaminen, joutuminen oikeudettomasti toisen haltuun tai sovelluksen oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää. Säännöksessä teknisellä alustalla tarkoitettaisiin sellaista mobiilipäätelaitetta, joka sisältää digitaalisen henkilöllisyyden sovelluksen. Momentin 3 kohdan mukaan sovelluksen haltija voisi lisäksi joutua vastuuseen sovelluksen oikeudettomasta käytöstä, jos hän on laiminlyönyt ehdotetun 27 §:n mukaisen velvollisuutensa ilmoittaa Digi- ja väestötietovirastolle teknisen alustan katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian.

Pykälän 2 momentissa säädettäisiin tilanteista, joissa digitaalisen henkilöllisyyden sovelluksen haltija ei kuitenkaan olisi vastuussa sovelluksen oikeudettomasta käytöstä, vaikka kyse olisi jonkin 1 momentissa säädetyn vastuun perusteen täyttymisestä. Momentin 1 kohdan mukaan sovelluksen haltija ei ole vastuussa sovelluksen oikeudettomasta käytöstä siltä osin kuin sitä on käytetty sen jälkeen, kun sovelluksen haltija on tehnyt Digi- ja väestötietovirastolle ehdotetun 27 §:n mukaisen ilmoituksen. Momentin 2 kohdan mukaan sovelluksen haltija ei myöskään olisi vastuussa sovelluksen oikeudettomasta käytöstä, jos hän ei ole voinut tehdä ehdotetun 27 §:n mukaista ilmoitusta sen vuoksi, että Digi- ja väestötietovirasto on laiminlyönyt velvollisuutensa huolehtia siitä, että ilmoitus on mahdollista tehdä milloin tahansa.

6 luku. Erinäiset säännökset

29 §. Muutoksenhaku. Pykälän 1 momentissa säädettäisiin oikeudesta vaatia hallintolaissa tarkoitettua oikaisua Digi- ja väestötietoviraston päätökseen, joka koskee ehdotetussa 15 §:ssä tarkoitettua ulkomaalaisen digitaalisen asiointivälineen myöntämistä tai 22 §:n 2 momentissa tarkoitettua asiointivälineen peruuttamista. Säännös olisi tarpeen, sillä on erikseen säädettävä siitä, mihin päätöksiin oikaisua saa vaatia. Kun hallintopäätökseen saa vaatia oikaisua, siihen ei saa hakea muutosta valittamalla. Pykälän 2 momentin mukaan muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

30 §. Voimaantulo. Pykälän 1 momentissa säädettäisiin lain voimaantulosta. Pykälän 2 momentti sisältäisi siirtymäsäännöksen, jonka mukaan Digi- ja väestötietoviraston olisi annettava 25 §:n 3 momentin mukaiset määräykset liittyen muiden tahojen tuottamiin tarkastussovelluksiin 4 kuukauden kuluessa ehdotetun lain voimaantulosta. Käytännössä siirtymäsäännös tarkoittaisi, että muut tahot eivät voisi tuottaa tarkastussovelluksia ennen kuin Digi- ja väestötietovirasto olisi tarvittavat määräykset antanut. Sääntelyn soveltamisen vaiheistaminen olisi tarpeen, jotta Digi- ja väestötietovirasto voisi ennen määräysten antamista varmistaa tarvittavat tietoturvallisuuteen liittyvät vaatimukset viraston oman tarkastussovelluksen kautta.

7.2 Laki digitaalisesta henkilöllisyystodistuksesta

1 luku. Yleiset säännökset

1 §. Lain tarkoitus. Ehdotetusta 1 §:stä ilmeni lain tarkoitus. Pykälän mukaan laissa säädettäisiin Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle myönnettävästä digitaalisesta henkilöllisyystodistuksesta. Laissa säädettäisiin muun muassa sen sisältämisestä tiedoista sekä sen käyttöönotosta, voimassaolosta ja käyttämisestä. Digitaalinen henkilöllisyystodistus olisi digitaalinen asiakirja, jolla henkilöllisyys ja siihen liittyviä vahvistettuja tietoja voitaisiin osoittaa, ja jonka henkilö voisi saada käyttöönsä, kun hänellä on voimassa oleva suomalainen passi tai henkilökortti.

2 §. Määritelmät. Pykälä sisältäisi olennaiset laissa käytetyt käsitteet ja niiden määritelmät. Pykälän *1 kohdan* mukaan laissa tarkoitettaisiin vahvistetuilla tiedoilla viranomaisen sähköisesti varmentamia henkilötietoja. Kyse olisi tiedoista, jotka ovat peräisin viranomaisen hallinnomasta tietovarannosta tai rekisteristä ja joiden aitouden ja muuttumattomuuden viranomainen on teknisesti varmentanut. Pykälän *2 kohdan* mukaan laissa luottavalla osapuolella tarkoitettaisiin luonnollista henkilöä tai oikeushenkilöä, jolle digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai vahvistettuja tietoja, ja jolla on tarve varmistua tietojen oikeellisuudesta. Oikeushenkilöiden osalta kyse olisi erilaisista sähköisistä asiointipalveluista tai fyysisistä asiointipisteistä, joissa on tarve tunnistaa henkilö tai vahvistaa tiettyjä häneen liittyviä tietoja palvelujen tarjoamista varten. Luottavan osapuolen tietojen käsittelyn tarkoituksella ei olisi merkitystä, vaan olennaista olisi, että digitaalisen henkilöllisyyden haltijalla olisi tarve osoittaa henkilöllisyytensä tai siihen liittyviä vahvistettuja tietoja, ja vastavuoroisesti luottavalla osapuolella olisi tarve voida luottaa näihin tietoihin. Pykälän *3 kohdan* mukaan laissa tarkoitettaisiin digitaalisen henkilöllisyystodistuksen haltijalla henkilöä, joka on ottanut käyttöönsä digitaalisen henkilöllisyystodistuksen. Pykälän *4 kohdan* mukaan teknisellä alustalla tarkoitettaisiin digitaalisen henkilöllisyystodistuksen haltijan mobiilipäätelaitetta, jossa digitaalinen henkilöllisyystodistus on otettu käyttöön. Pykälän *5 kohdan* mukaan käyntiasioinnilla tarkoitettaisiin asiointitilanteita, joissa digitaalisen henkilöllisyystodistuksen haltija ja luottava osapuoli ovat läsnä samanaikaisesti samassa paikassa ja digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai muita häneen liittyviä tietoja luottavalle osapuolelle. Kyse olisi kasvokkain tapahtuvasta vuorovaikutustilanteesta, jossa digitaalisen henkilöllisyystodistuksen haltijapyynnöstä osoittaa henkilöllisyytensä tai siihen liittyviä tietoja luottavalle osapuolelle. Merkitystä ei olisi sillä, tapahtuisiko todistuksen esittäminen toiselle luonnolliselle henkilölle yksityiselämän piirissä vai esimerkiksi elinkeinonharjoittajan tai viranomaisen edustajalle. Käyntiasioinnilla ei kuitenkaan tarkoitettaisi esimerkiksi tilanteita, joissa henkilö on läsnä fyysisessä tilassa, mutta asioi automaatin tai muun teknisen päätelaitteen kanssa. Pykälän *6 kohdan* mukaan ydinidentiteetin todisteella tarkoitettaisiin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 11 §:ssä tarkoitettua todistetta.

3 §. Digitaalinen henkilöllisyystodistus. Pykälässä säädettäisiin digitaalisesta henkilöllisyystodistuksesta ja sen tarkoituksesta ja toiminnasta. Pykälän *1 momentissa* säädettäisiin, että digitaalinen henkilöllisyystodistus on henkilöllisyyden sekä vahvistettujen tietojen osoittamiseen sähköisessä asiointissa ja käyntiasioinnissa tarkoitettu henkilöllisyystodistus. Digitaalinen henkilöllisyystodistus olisi siis lähtökohtaisesti henkilöllisyyttä osoittava asiakirja henkilökortin ja passin tavoin. Sitä voitaisiin käyttää ja se voitaisiin hyväksyä henkilöllisyyden osoittamisen tarkoituksessa samalla tavoin, kuin henkilökortti ja passi. Poliisi ei kuitenkaan tekisi erillistä myöntöpäätöstä digitaalisen henkilöllisyystodistuksen myöntämisestä tai käyttöönotosta. Sen sijaan oikeus digitaaliseen henkilöllisyystodistukseen syntyisi voimassaolevan henkilökortin tai passin perusteella siten kuin ehdotetussa henkilökorttilain (663/2016) 1 a §:ssä ja passilain (671/2006) 3 d §:ssä säädetään.

Lisäksi 1 momentissa säädettäisiin, että digitaalisen henkilöllisyystodistuksen tuottaisi poliisi. Ehdotettu sääntely olisi tarpeen, sillä myös Digi- ja väestötietovirasto osallistuisi digitaalisen henkilöllisyystodistuksen tekniseen toteuttamiseen osana digitaalisen henkilöllisyyden tietojärjestelmän toteuttamista. Poliisin ja Digi- ja väestötietoviraston roolien selkeyden varmistamiseksi olisi tarpeen säätää siitä, että digitaalinen henkilöllisyystodistus on poliisin tuote. Sääntely olisi lisäksi tarpeen myös siksi, ettei syntyisi epäselvyyttä siitä, voisiko myös joku muu taho tuottaa ehdotetun sääntelyn mukaisen digitaalisen henkilöllisyystodistuksen. Tarkoitus on, että mahdollisuus digitaalisen henkilöllisyystodistuksen tuottamiseen on vain poliisilla.

Pykälän *2 momentissa* säädettäisiin digitaalinen henkilöllisyystodistuksen tarjoamisesta käytettäväksi ehdotetun Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun

lain 2 §:n 6 kohdassa tarkoitetun digitaalisen henkilöllisyyden sovelluksen avulla. Digitaalista henkilöllisyystodistusta käytettäisiin siis Digi- ja väestötietoviraston tuottaman digitaalisen henkilöllisyyden sovelluksen avulla ja se olisi sidoksissa siihen mobiilipäätelaitteeseen, johon sovellus on asennettu. Digitaalista henkilöllisyystodistusta ei olisi mahdollista ottaa käyttöön muussa kuin momentissa tarkoitetussa sovelluksessa.

Pykälän 3 momentissa säädettäisiin, että poiketen siitä, mitä passilain 34 §:ssä ja henkilökorttilain 34 §:ssä säädetään passista ja henkilökortista perittävistä maksuista, digitaalisen henkilöllisyystodistuksen osalta maksu voidaan määrätä omakustannusarvoa pienemmäksi. Säännös mahdollistaisi sen, että digitaalisesta henkilöllisyystodistuksesta muodostuvaa omakustannusarvoa ei vyörytetä valtion maksuperustelain pääsäännön mukaisesti passien ja henkilökorttien hintoihin täysimääräisesti. Säännös olisi tarpeen sen varmistamiseksi, että passien ja henkilökorttien asiakashinnat nousisivat maltillisesti digitaalisen henkilöllisyystodistuksen kehittämisen johdosta. Kun digitaalinen henkilöllisyystodistus ei olisi erotettavissa henkilökortista tai passista eikä näin ollen olisi passista tai henkilökortista erillinen suorite vaan passin tai henkilökortin digitaalinen ilmentymä, olisi henkilöiden kannalta kohtuutonta periä siitä erillistä hintaa. Käytännössä siten digitaalisesta henkilöllisyystodistuksesta perittävästä maksusta vastaisi passin tai henkilökortin myöntävä viranomais. Säännös vastaisi myös tältä osin sitä, mitä kansalaisvarmenteesta on säädetty 72 §:ssä laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista.

2 luku. Digitaalisen henkilöllisyystodistuksen sisältämät tiedot ja voimassaolo

4 §. *Digitaalisen henkilöllisyystodistuksen sisältämät tiedot.* Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen sisältämistä tiedoista. Pykälän 1 momentin mukaan digitaalisen henkilöllisyystodistuksen haltijalle toimitettaisiin kopio häneen liittyvistä henkilökorttilain 31 §:ssä tarkoitetun henkilökorttirekisterin tai passilain 29 §:ssä tarkoitetun passirekisterin tiedoista sisältämistä tiedoista hänen itsensä hallittavaksi. Digitaalinen henkilöllisyystodistus sisältäisi momentissa yksilöidyt luonnollisen henkilön tiedot sellaisina, kuin ne sisältyvät henkilökorttirekisteriin tai passirekisteriin. Digitaalisen henkilöllisyystodistuksen tietojen lähderekisteri määräytyisi sen mukaan, kumpi rekisteri sisältää henkilöstä tuoreimmat tiedot. Henkilöllisyysasiakirjat eivät lain mukaan raukea tilanteessa, jossa henkilötiedot muuttuvat. Tästä syystä esiintyy käytännössä tilanteita, joissa henkilöllä on voimassa oleva passi ja henkilökortti, mutta niissä on toisistaan eroavat henkilötiedot. Digitaaliseen henkilöllisyystodistukseen olisi kuitenkin tarkoituksenmukaista toimittaa tuoreimmat tiedot, jolloin tiedot eivät välttämättä olisi samat kuin digitaalisen henkilöllisyystodistuksen käyttöönotossa käytetyssä viranomaisen henkilöllisyyttä osoittavassa asiakirjassa. Tämä olisi perusteltua, sillä käyttöönoton yhteydessä esitettävän passin tai henkilökortin tehtävänä on mahdollistaa käyttäjän tunnistaminen eikä sen suoraan tulisi määritellä digitaalisessa henkilöllisyystodistuksessa esitettävää tietosisältöä.

Tietojen toimittamisella henkilön itsensä hallittavaksi eli itsehallittavuudella tarkoitettaisiin sitä, että digitaalisen henkilöllisyystodistuksen haltijalle toimitetut tiedot olisivat tietojen toimittamisen jälkeen digitaalisen henkilöllisyystodistuksen haltijan omia tietoja. Tämä tarkoittaisi sitä, että viranomaisella ei olisi mahdollisuutta määrätä missä ja mihin tarkoituksiin henkilö omia tietojaan osoittaa. Viranomaisella ei olisi myöskään pääsyä henkilölle toimitettuihin tietoihin enää sen jälkeen, kun ne on toimitettu henkilön tekniseen alustaan, joka sisältää digitaalisen henkilöllisyystodistuksen. Varmennettu kopio tiedoista toimitettaisiin fyysisesti henkilön tekniselle alustalle, eikä sitä enää toimittamisen jälkeen säilytettäisi viranomaisen tietojärjestelmässä. Alkuperäiset rekisteritiedot, joiden pohjalta henkilölle toimitettavat vahvistetut tiedot luodaan säilyvät kuitenkin viranomaisen rekisterissä ja viranomaisella vastaisi edelleen näistä alkuperäisistä tiedoista. Varmennettu kopio tiedoista tallennettaisiin fyysisesti digitaalisen henkilöllisyystodistuksen haltijan teknisen alustan eli mobiilipäätelaitteen turvaelementeille, jossa

sijaitseville tiedoille viranomaisilla ei olisi pääsyä. Tilanne vastaisi esimerkiksi henkilölle luovutettavalle fyysiselle henkilökortille kopioituja henkilökorttirekisterin tietoja, jotka eivät enää henkilökortin luovuttamisen jälkeen ole viranomaisen asiakirjoja, eivätkä henkilökorttivaranomaisen rekisterinpitäjyyden piirissä. Näiden henkilön tekniselle alustalle toimitettujen tietojen käsittelyssä ei sovellettaisi henkilötietojen suojaa koskevaa lainsäädäntöä, sillä luonnollinen henkilö käsittelee näitä omia henkilötietojaan tietosuojasetuksen 2 artiklan 2 kohdan c alakohdan mukaisesti yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa, jolloin kyseisten tietojen käsittely olisi tietosuojalainsäädännön aineellisen soveltamisalan ulkopuolella. Kyseisten tietojen käsittelyyn ei sovellettaisi myöskään tiedonhallintalakia, sillä tiedot eivät enää olisi julkisuuslain 5 §:n 2 momentin mukaisia viranomaisen asiakirjoja, kun ne eivät olisi enää viranomaisen hallussa. Vahvistetut tiedot henkilön itsensä haltuun toimittava rekisterinpitäjä vastaisi kuitenkin toimittamiensa tietojen eheydestä ja luottamuksellisuudesta tietosuojasetuksen 5 artiklan 1 kohdan f alakohdan mukaisesti siten, että mikäli tietojen toimittaminen henkilön itsensä haltuun epäonnistuisi tai tiedot olisivat virheellisiä, olisi vastuu edelleen viranomaisella.

Lisäksi pykälän 1 momentissa säädettäisiin digitaalisen henkilöllisyystodistuksen haltijalle toimitettavien tietojen yksityiskohtaisesta sisällöstä. Digitaaliseen henkilöllisyystodistukseen sisältyisivät momentin 1–8 kohdan mukaan henkilön etunimet (1 kohta); sukunimi (2 kohta); syntymäaika (3 kohta); tieto henkilön sukupuolesta (4 kohta); tieto Suomen kansalaisuudesta (5 kohta); henkilötunnus tai muu kansallisen tason yksilöintitunnus (6 kohta); passi- tai henkilökorttirekisteriin talletettu kasvokuva (7 kohta); voimassa olevan suomalaisen passin tai henkilökortin voimassaoloaika (8 kohta); sekä todistuksen yksilöivä tunnus (9 kohta). Tietojen yksityiskohtaisen sisällön määrittämisessä olisi kyse tietosuojasetuksen 6 artiklan 3 kohdan mukaisen kansallisen liikkumavaran hyödyntämisestä, sillä kyseisen kohdan mukaan kansallisessa lainsäädännössä voidaan tarkemmin säännellä käsiteltävien henkilötietojen tyypistä.

Pykälän 2 momentissa säädettäisiin, että poliisin velvollisuudesta varmentaa 1 momentissa tarkoitettua vahvistettuja tiedot ennen niiden toimittamista passi- tai henkilökorttirekistereistä henkilön itsensä haltuun digitaaliseen henkilöllisyystodistukseen. Tiedot olisi vahvistettava siten, että luottava osapuoli kykenee varmistumaan tietojen oikeellisuudesta ja ajantasaisuudesta tarkistamalla tietojen voimassaolon. Digitaalisen henkilöllisyystodistuksen sisältämiin vahvistettuihin tietoihin olisi mahdollista luottaa samalla tavoin kuin passiin tai henkilökorttiin merkittyihin tietoihin. Pykälän 2 momentissa todettaisiin myös nimenomaisesti, että poliisilla ei olisi oikeutta käsitellä enää samoja digitaalisen henkilöllisyystodistuksen haltijalle toimitettuja vahvistettuja tietoja sen jälkeen, kun tiedot on toimitettu. Sääntelyn tarkoituksena on vielä erikseen korostaa sitä, että tiedot toimitetaan henkilön itsensä hallittavaksi, eikä poliisilla ole enää oikeutta henkilölle toimitettujen tietojen käsittelyyn.

Pykälän 3 momentissa säädettäisiin, että ehdotetun 1 momentin mukaisten tietojen aitouden ja eheyden varmistamiseen liittyvät varmenteet luo Digi- ja väestötietovirasto. Pykälän 3 momentissa säädettäisiin myös, että Digi- ja väestötietovirasto toimittaisi lisäksi henkilön syntymäajasta johdetut ikätodisteet digitaalisen henkilöllisyystodistuksen haltijalle. Ikätodisteilla tarkoitettaisiin todisteita, joita voitaisiin käyttää henkilön osoittaessa ikää palveluille. Tällöin asiointitilanteessa osoitettaisiin esimerkiksi ainoastaan tieto siitä, onko henkilö täysi-ikäinen vai ei, sen sijaan, että osoitettaisiin tarkka tieto henkilön iästä. Ikätodisteiden laskemiseksi Digi- ja väestötietovirasto laskee sovellukseen viettävät ikätodisteet syntymäajan perusteella.

Pykälän 4 momentissa säädettäisiin, että digitaalisen henkilöllisyystodistuksen tiedot päivitetään sen haltijan nimenomaisesta pyynnöstä. Kuitenkin 4 momentissa säädettäisiin myös, että digitaalisen henkilöllisyystodistuksen sisältämien tietojen tulisi olla aina ajan tasalla ja niiden tulisi vastata poliisin henkilökorttirekisterissä tai passirekisterissä olevia tietoja. Jos tiedot eivät

olisi ajan tasalla, ei digitaalista henkilöllisyystodistusta olisi mahdollista käyttää. Digitaalisen henkilöllisyyden tietojärjestelmän tulisi määrääjoin tarkastaa tietojen ajantasaisuus. Mikäli vahvistettujen tietojen havaittaisiin muuttuneen esimerkiksi uuden passin tai henkilökortin myöntämisen myötä, olisi digitaalisen henkilöllisyystodistuksen haltijan pyydettävä tietojen päivittämistä, jotta digitaalisen henkilöllisyystodistuksen käyttöä voisi jatkaa. Digitaalisen henkilöllisyystodistuksen käyttö estyisi, mikäli tiedot eivät olisi ajan tasalla. Digitaalisen henkilöllisyystodistuksen käyttöä olisi mahdollista jatkaa henkilöllisyystodistuksen haltijan päivittäessä sen sisältämät tiedot.

5 §. Rekisteri digitaalisista henkilöllisyystodistuksista. Pykälän 1 momentissa säädettäisiin Poliisin tehtävästä toimia rekisterinpitäjänä digitaalisten henkilöllisyystodistusten osalta. Rekisteriin voitaisiin tallentaa tiedot 4 §:n 1 momentin 1-9 kohdassa tarkoitetuista tiedoista siltä osin, kuin kyse on henkilöistä, joilla on oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon. Lisäksi rekisteriin tallennetaan tiedot digitaalisista henkilöllisyystodistuksista, todistusten haltijoista ja todistusten voimassaolosta. Rekisteriä ylläpidettäisiin digitaalisen henkilöllisyystodistuksen tarjoamista ja tuottamista varten. Rekisteriin tallennettaisiin tiedot niistä henkilöistä, joilla on oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon, ei vain niistä, jotka ovat ottaneet henkilöllisyystodistuksen käyttöönsä. Käytännössä rekisteri sisältäisi henkilötiedot niiden henkilöiden osalta, joilla on voimassa oleva passi tai henkilökortti. Poliisi toimisi kyseisen rekisterin rekisterinpitäjänä. Rekisterin ylläpitoon liittyvän henkilötietojen käsittelyn oikeusperusteena on tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta. Poliisin suorittamaan henkilötietojen käsittelyyn sovellettaisiin yleisesti tietosuoja-asetusta sekä rekisterissä käsiteltävien tietojen käytöstä, tarkastusoikeudesta ja luovuttamisesta säädetään laissa henkilötietojen käsittelystä poliisitoimissa (616/2019).

Perustuslakivaliokunnan aloitteesta (PeVL 6/2013 vp.) passilakiin lisättiin eduskuntakäsittelyn aikana säännös (35 § 3 mom) passien yksilöinnistä Suomen rajojen sisällä. Perustuslakivaliokunnan mielestä vaatimus yksilöinnin suorittamisesta Suomessa on perusteltu sekä tietojen luonteen että sen vuoksi, että tällöin yksityiseen palveluntuottajaan kohdistuvat hallinnon yleislaeista ja rikosoikeudellista virkavastuuta koskevista säännöksistä johtuvat velvoitteet tulevat sovellettaviksi palveluntuottajaan tämän hoitaessa julkista hallintotehtävää. Passilain 35 §:n 3 momentin mukaan palveluntuottajan tulee suorittaa passin yksilöinti ja passin toimittamista edeltävä laadun ja oikeasisältöisyyden tarkastaminen Suomessa. Vastaavasti henkilökorttilain 22 §:n 4 momentin mukaan palveluntuottajan tulee yksilöidä henkilökortti ja suorittaa henkilökortin toimittamista edeltävä laadun ja oikeasisältöisyyden tarkastaminen Suomessa.

Digitaalisessa henkilöllisyystodistuksessa käytetään rekisteriin talletettuja passin ja henkilökortin yksilöintitietoja. Uuden välineen käyttöönotto ei tarkoittaisi sitä, että tietojen käsittelyä koskevista säännöistä tulisi poiketa. Sääntöjen tarkoituksena on suojella kriittistä tietomassaa. Suojauksen tarve on yhtä suuri riippumatta siitä, yksilöidäänkö tiedot fyysiseen vai digitaaliseen henkilöllisyyttä osoittavaan asiakirjaan. Passi- ja henkilökorttirekisterien sisältö on yleisen turvallisuuden ja järjestyksen näkökulmasta kriittinen tietomassa, minkä vuoksi tietojen käsittelyn tulee tapahtua Suomen rajojen sisäpuolella. Mikäli tiedot ovat henkilöön liittyviä yksilöintitietoja tai niihin rinnastettavia tietoja tai kyse on edellä todettujen tietojen siirtämisestä, tietoja ei tule siirtää Suomen rajojen ulkopuolelle.

Pykälän 2 momentissa säädettäisiin rekisterin tietojen säilytysajasta. Rekisterin tiedot poistettaisiin viimeistään kymmenen vuoden kuluttua siitä, kun henkilön oikeus digitaaliseen henkilöllisyystodistukseen on päättynyt. Kymmenen vuoden säilytysaika olisi johdonmukainen laissa henkilötietojen käsittelystä poliisitoimissa pääasiassa noudatettujen säilytysaikojen kanssa.

6 §. Digitaalisen henkilöllisyystodistuksen käyttöönotto. Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen käyttöönotosta. Pykälän *1 momentissa* säädettäisiin digitaalisen henkilöllisyystodistuksen käyttöönototavoista. Digitaalinen henkilöllisyystodistus voitaisiin ensinnäkin ottaa käyttöön asioimalla toimivaltaisen passi- tai henkilökorttiviranomaisen luona. Toimivaltaisella viranomaisella tarkoitettaisiin poliisin lisäksi niitä viranomaisia, jotka on lueteltu passilain passin hakemista koskevassa 6 §:ssä. Digitaalista henkilöllisyystodistusta ei kuitenkaan voisi ottaa käyttöön asioimalla ulkoministeriössä. Ilman nimenomaista rajausta kuka tahansa voisi asioida ulkoministeriössä tarkoituksenaan ottaa digitaalinen henkilöllisyystodistus käyttöön. Ulkoministeriö kuitenkin myöntää ainoastaan diplomaatti- ja virkapasseja ja on varautunut vain niiden myöntämiseen ja järjestänyt sen perusteella asiakaspalvelutoimintansa. Tästä syystä olisi tarpeen rajata ulkoministeriö nimenomaisesti pois niistä viranomaisista, joiden luona asioidessa digitaalinen henkilöllisyystodistus voitaisiin ottaa käyttöön.

Pykälän 1 momentin mukaan digitaalinen henkilöllisyystodistus voitaisiin ottaa käyttöön myös sähköisesti. Tällöin edellytettäisiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 2 §:n 1 kohdassa tarkoitettua vahvaa sähköistä tunnistamista. Sähköisessä käyttöönotossa edellytettäisiin lisäksi, että henkilön voimassa olevan passin tai henkilökortin teknisen osan tiedot etäluetaan teknisen alustan avulla ja niitä verrataan vahvan sähköisen tunnistamisen tietoihin ja että nämä tiedot vastaavat toisiaan

Pykälän *2 momentissa* säädettäisiin, että käyttöönoton yhteydessä poliisi liittäisi Digi- ja väestötietoviraston myöntämän ydinidentiteetin todisteen luonnolliseen henkilöön.

7 §. Digitaalisen henkilöllisyystodistuksen käyttöönotto alaikäiselle. Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen käyttöönotosta silloin, kun käyttöönottajana on alaikäinen. Pykälän *1 momentissa* säädettäisiin, että alaikäisen osalta digitaalisen henkilöllisyystodistuksen käyttöönotto edellyttää hänen huoltajiensa suostumusta. Sääntelyn perusteella alaikäisen on siis mahdollista ottaa digitaalinen henkilöllisyystodistus käyttöön, mutta se edellyttäisi pääsäännön mukaan alaikäisen huoltajien suostumusta. Alaikäinen ei siis lähtökohtaisesti voisi ottaa digitaalista henkilöllisyystodistusta käyttöön itsenäisesti.

Pykälän *2 momentissa* säädettäisiin poikkeuksesta 1 momentin mukaiseen vaatimukseen. Momentin mukaan digitaalisen henkilöllisyystodistuksen käyttöönotto ei kuitenkaan edellyttäisi huoltajien suostumusta silloin, kun kyse on alaikäisestä henkilöstä, joka on täyttänyt 15 vuotta. Tarkoituksena olisi siis mahdollistaa, että 15 vuotta täyttänyt alaikäinen voisi ottaa digitaalisen henkilöllisyystodistuksen käyttöön itsenäisesti ilman, että hänen huoltajiensa suostumusta edellytetään.

8 §. Digitaaliseen henkilöllisyystodistukseen voimassaolo. Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen voimassaolosta. Pykälän *1 momentissa* säädettäisiin digitaalisen henkilöllisyystodistuksen voimassaolon päättyvän vuoden kuluttua siitä, kun sen perustana olevan henkilöllisyyttä osoittavan asiakirjan voimassaolo on päättynyt. Pykälän *2 momentissa* säädettäisiin, että henkilöllisyyttä osoittavalla asiakirjalla tarkoitetaan sitä passilain tai henkilökorttilain mukaisesti myönnettyä henkilöllisyyttä osoittavaa asiakirjaa, jonka perusteella henkilöllä on oikeus digitaaliseen henkilöllisyystodistukseen.

Sääntelyn tarkoituksena on, että myös digitaalinen henkilöllisyystodistus olisi aina voimassa, kun henkilöllä on voimassa oleva passi tai henkilökortti, jonka perusteella henkilöllä on oikeus digitaaliseen henkilöllisyystodistukseen. Digitaalista henkilöllisyystodistusta ei siis tarvitsisi ottaa uudelleen käyttöön aina kun henkilölle on myönnetty uusi digitaaliseen henkilöllisyystodistukseen oikeuttava henkilökortti tai passi, vaan digitaalisen henkilöllisyystodistus pysyy voimassa katkeamatta. Voimassaolon katkeamattomuus edellyttäisi säännöksen mukaan kuitenkin

sitä, että henkilö hankkii uuden digitaaliseen henkilöllisyystodistukseen oikeuttavan passin tai henkilökortin vuoden kuluessa siitä, kun henkilön kaikkien tällaisten asiakirjojen voimassaolo on päättynyt. Digitaalisen henkilöllisyystodistuksen voimassaolo siis päättyisi vuoden kuluttua siitä, kun henkilön digitaaliseen henkilöllisyystodistukseen oikeuttavien henkilöllisyyttä osoittavien asiakirjojen voimassaolo olisi päättynyt eikä henkilö ole vuoden aikana hankkinut uutta tällaista asiakirjaa.

9 §. Digitaalisen henkilöllisyystodistuksen peruuttaminen. Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen peruuttamisen tilanteista ja siitä, millä viranomaisella olisi oikeus tehdä peruutus kussakin tilanteessa. Pykälän 1 *momentissa* säädettäisiin, että digitaalinen henkilöllisyystodistus peruutetaan silloin, jos sen haltija sitä pyytää. Näissä tilanteissa peruuttamisen tekisi poliisi. Digitaalinen henkilöllisyystodistus peruutettaisiin myös, jos digitaalisen henkilöllisyystodistuksen haltija ilmoittaa teknisen alustan kadonneeksi tai joutuneeksi oikeudettomasti toisen haltuun. Näissä tilanteissa digitaalisen henkilöllisyystodistuksen voisi poliisin lisäksi peruuttaa myös Digi- ja väestötietovirasto. Digi- ja väestötietoviraston oikeus peruuttaa digitaalinen henkilöllisyystodistus näissä tilanteissa olisi tarpeen, sillä ehdotetun lain digitaalisen henkilöllisyyden palveluista 27 §:n mukaan digitaalisen henkilöllisyyden sovelluksen haltijan on tehtävä ilmoitus teknisen alustan katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä nimenomaisesti Digi- ja väestötietovirastolle. Jotta digitaalisen henkilöllisyystodistuksen oikeudeton käyttö voitaisiin estää mahdollisimman nopeasti, tulisi Digi- ja väestötietovirastolla olla oikeus peruuttaa digitaalinen henkilöllisyystodistus ilmoituksen saatuaan.

Pykälän 2 *momentissa* säädettäisiin, että digitaalinen henkilöllisyystodistus voidaan lisäksi peruuttaa, jos siinä on ilmeinen virheellisyys, sen taustalla oleva henkilöllisyyttä osoittava asiakirja peruutetaan tai sitä käyttää joku muu kuin digitaalisen henkilöllisyystodistuksen haltija tai sen käytön turvallisuus on muutoin vaarantunut. Näissä tilanteissa peruutuksen tekisi poliisi.

Digitaalinen henkilöllisyystodistus peruutettaisiin peruuttamalla siihen sisältyvä ydinidentiteetin todiste. Digi- ja väestötietovirasto peruuttaisi digitaalisen henkilöllisyystodistuksen haltijan ydinidentiteetin todisteen. Digitaalisen henkilöllisyystodistuksen peruuttamisen tulisi estää sen käyttö välittömästi sen jälkeen, kun peruuttaminen on tehty.

3 luku. Digitaalisen henkilöllisyystodistuksen käyttäminen

10 §. Vahvistettujen tietojen osoittaminen sähköisessä asiointissa. Pykälässä säädettäisiin digitaalisen henkilöllisyystodistuksen hyödyntämisestä sähköisessä asiointissa. Digitaalinen henkilöllisyystodistus mahdollistaisi henkilöllisyyttä koskevien ja muiden vahvistettujen tietojen osoittamisen tunnistauduttaessa sekä julkisen että yksityisen sektorin sähköisen asioinnin palveluihin. Pykälän 1 *momentin* mukaan sähköisessä asiointissa asiointivälineen haltija valitsee itse vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle, jollei muussa laissa toisin säädetä. Tällöin kyse ei olisi tiedon luovutuksesta viranomaisen rekisteristä, vaan henkilö osoittaisi itse suoraan henkilötietojaan sähköisesti niille toimijoille, jotka asiointipalvelussaan mahdollistavat digitaalisen henkilöllisyystodistuksen hyödyntämisen. Käytännössä sähköisessä asiointissa digitaalista henkilöllisyystodistusta hyödynnettäisiin siten, että Digi- ja väestötietovirasto tuottaisi luottaville osapuolille tarjottavaa rajapintaa, joka mahdollistaisi digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen ja vahvistettujen henkilötietojen sekä ikätodisteiden käyttämisen suoraan sovelluksesta hyödyntävissä palveluissa. Henkilö osoittaisi itse henkilöllisyytensä asiointipalvelussa ja voisi asiointitapahtuman yhteydessä valita ne tiedot, jotka haluaa luottavalle osapuolelle osoittaa. Sähköisen asioinnin yhteydessä välitetäisiin kuitenkin aina asiointipalvelulle tieto siitä, että kyseessä on poliisin vahvistamankäytännön henkilöllisyyttä osoittava asiakirja.

Sääntelyn lähtökohtana olisi pykälän mukaisesti haltijan oikeus itse valita vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle. Muu lainsäädäntö saattaa kuitenkin rajoittaa tätä oikeutta. Käytännössä tällainen tilanne olisi esimerkiksi, kun digitaalista henkilöllisyystodistusta hyödynnetään Suomi.fi-tunnistuksen kautta, kun henkilö haluaisi osoittaa henkilöllisyyttään viranomaisen sähköisessä asiointipalvelussa. Hyödynnettäessä todistusta Suomi.fi-tunnistuksen kautta haltija voisi osoittaa Suomi.fi-tunnistukselle ainoastaan ydinidentiteetin todisteen tiedot. Samoin digitaalisen henkilöllisyystodistuksen hyödyntäminen ja henkilötietojen osoittaminen luottamusverkoston kautta edellyttää tiettyjen tietojen luovuttamista tunnistusvälitilaspalveluille. Tällaisia tietoja ovat esimerkiksi henkilön yksilöivä tunniste ja henkilön etu- ja sukunimi.

Pykälän 2 momentin mukaan sähköisen asioinnin yhteydessä luovutettaisiin kuitenkin aina tieto poliisin tekemästä liitoksesta henkilön ydinidentiteettiin. Tämän avulla digitaaliseen henkilöllisyystodistukseen luottava osapuoli voisi varmistua henkilöllisyystodistuksen ja sen sisältämien vahvistettujen tietojen luotettavuudesta.

11 §. *Vahvistettujen tietojen osoittaminen käyntiasioinnissa.* Pykälässä säädettäisiin mahdollisuudesta käyttää digitaalista henkilöllisyystodistusta henkilöllisyyden sekä digitaalisen henkilöllisyystodistuksen sisältämien vahvistettujen tietojen osoittamiseen myös käyntiasioinnissa. Pykälän 1 momentissa säädettäisiin digitaalisen henkilöllisyystodistuksen sisältämien tietojen itsehallittavuudesta käyntiasioinnissa. Sen mukaan digitaalisen henkilöllisyystodistuksen haltijan olisi mahdollista itse valita ne vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle. Käyntiasioinnissa olisi kuitenkin aina osoitettava kasvokuva. Kasvokuvan osoittaminen olisi tarpeen, jotta luottava osapuoli voisi varmistua, että tiedot kuuluvat niitä osoittavalle henkilölle vertaamalla kasvokuvaa henkilöön.

Pykälän 2 momentissa säädettäisiin luottavan osapuolen oikeudesta tarvittaessa tarkistaa ydinidentiteetin todisteen voimassaolo Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 12 §:n mukaisesta ydinidentiteetin todisteiden rekisteristä. Tarkastaminen tapahtuisi käytännössä tarkastussovelluksen tai luottavan osapuolen järjestelmässä olevan lukijarajapinnan kautta. Pykälässä säädettäisiin, että ydinidentiteetin todisteen voimassaolo voitaisiin tarkistaa tarvittaessa. Ydinidentiteetin todisteen voimassaolon tarkastaminen ei olisi tarpeen kaikissa tapauksissa ja tästä syystä sitä ei säädettäisi pakolliseksi. Ydinidentiteetin todisteen voimassaolon tarkastaminen ei ole tarpeen esimerkiksi tilanteessa, jossa tarkastajalle riittäisi kasvokuvan ja luovutettujen tietojen liitoksen ja allekirjoitusten varmistaminen.

4 luku. Erinäiset säännökset

12 §. *Muutoksenhaku.* Pykälässä säädettäisiin muutoksenhausta. Pykälän 1 momentin mukaan poliisin päätökseen, joka koskee 9 §:n 2 momentissa tarkoitettua digitaalisen henkilöllisyystodistuksen peruuttamista saa vaatia oikaisua. Kyseisessä tilanteessa olisi kyse poliisin aloitteesta tehdystä peruuttamisesta. Oikaisuvaatimusmenettelystä säädetään hallintolaissa (434/2003). Pykälän 2 momentin mukaisesti muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

7.3 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta

2 §. *Määritelmät.* Voimassa olevan pykälän 1 momentin 2 kohdassa määritellään vahva sähköinen tunnistaminen. Määritelmä pysyisi asiallisesti ennallaan, mutta siihen lisättäisiin selvyyden vuoksi maininta digitaalisen henkilöllisyyden välineistä. Digitaalisen henkilöllisyyden välineen

määritelmä lisättäisiin 2 §:n uudeksi 13 kohdaksi. Digitaalisen henkilöllisyyden välineiden tarjoamisessa olisi kyse uudenlaisesta palvelusta, joka poikkeaa toimintamalleiltaan nykyisin tarjotusta vahvasta sähköisestä tunnistamisesta. Sääntely olisi siis tarpeen, jotta olisi selkeää, että myös digitaalisen henkilöllisyyden väline on sellainen sähköinen menetelmä, jota vahvan sähköisen tunnistamisen määritelmässä tarkoitetaan.

Sääntelyn mukaan digitaalisen henkilöllisyyden välineeseen perustuva tunnistaminen olisi vahvaa sähköistä tunnistamista silloin, kun se täyttää eIDAS-asetuksen 8 artiklassa tarkoitetun korotetun varmuustason tai korkean varmuustason vaatimukset. Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 14 §:ssä tarkoitettu ulkomaalaisen digitaalinen asiointiväline voisi tästä syystä olla digitaalisen henkilöllisyyden väline ainoastaan silloin, kun sen haltija on tunnistettu tunnistus- ja luottamuspalvelulain 17 §:ssä tarkoitetulla tavalla. Ulkomaalaisen digitaalinen asiointiväline voidaan myöntää myös etärekisteröintimenettelyn yhteydessä, mutta silloin väline ei täytä eIDAS-asetuksen 8 artiklassa tarkoitetun korotetun tai korkean varmuustason vaatimuksia. Tästä syystä etärekisteröintimenettelyn yhteydessä myönnettyyn ulkomaalaisen digitaaliseen asiointivälineeseen perustuva tunnistautuminen ei olisi tässä laissa tarkoitettua vahvaa sähköistä tunnistamista.

Nykyisin muualla lainsäädännössä edellytetään nimenomaan vahvan sähköisen tunnistamisen käyttöä tiettyihin palveluihin pääsemiseksi, esimerkiksi kuluttajansuojalain (38/1978) mukaisia kuluttajaluottoja haettaessa. Tarkoitus olisi, että jatkossa myös digitaalisen henkilöllisyyden välineiden avulla olisi mahdollista tunnistautua palveluihin, joissa lainsäädäntö edellyttää vahvan sähköisen tunnistamisen käyttöä.

Voimassa olevan pykälän 1 momenttiin lisättäisiin uusi *12 kohta*, jossa määriteltäisiin digitaalisen henkilöllisyyden palvelujen tarjoaja. Digitaalisen henkilöllisyyden palvelujen tarjoajalla tarkoitettaisiin sitä tahoa, joka tuottaa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa tarkoitettuja digitaalisen henkilöllisyyden palveluja ja joka ei ole pykälän 3 kohdassa tarkoitettu tunnistuspalvelun tarjoaja. Käytännössä digitaalisen henkilöllisyyden palvelujen tarjoajalla tarkoitetaan Digi- ja väestötietovirastoa. Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 4 §:ssä säädetään, että digitaalisen henkilöllisyyden välineiden hyödyntämiseksi tuotettavan tietojärjestelmän tuottaminen on Digi- ja väestötietoviraston tehtävä. Digitaalisen henkilöllisyyden palvelujen tarjoaminen on siten Digi- ja väestötietoviraston tehtävä. Digi- ja väestötietoviraston tarjoamiin digitaalisen henkilöllisyyden palveluihin sisältyy kuitenkin myös sellaisia asiointivälineitä, joita ei voida hyödyntää tunnistus- ja luottamuspalvelulain mukaisessa vahvassa sähköisessä tunnistamisessa. Tunnistus- ja luottamuspalvelulakia ei siis sovelleta esimerkiksi Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 4 luvussa tarkoitettuun ulkomaalaisen digitaaliseen asiointivälineeseen silloin, kun välineen haltija on tunnistettu Digi- ja väestötietoviraston varmennepalveluista annetun lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä.

Määritelmällä luotaisiin tunnistus- ja luottamuspalvelulakiin uusi rooli. Voimassa olevassa laissa on määritelty tunnistusvälineen tarjoaja sekä tunnistusvälityspalvelun tarjoaja, jotka molemmat ovat tunnistuspalvelun tarjoajia. Digitaalisen henkilöllisyyden palvelujen tarjoaja eroaisi laissa tarkoitetuista tunnistuspalvelun tarjoajista siten, että sen tarjoamassa palvelussa olisi ensisijaisesti kyse digitaalisesta henkilöllisyydestä. Digi- ja väestötietoviraston tuottama digitaalisen henkilöllisyyden tietojärjestelmä sisältäisi kuitenkin myös tunnistusjärjestelmän. Digitaalisen henkilöllisyyden palvelujen tarjoajan tuottamia digitaalisen henkilöllisyyden välineitä voisi siten hyödyntää myös henkilöllisyyden osoittamiseen.

Digitaalisen henkilöllisyyden palvelujen tarjoaja ei myöskään tulisi osapuoleksi kansalliseen vahvan sähköisen tunnistamisen luottamusverkostoon, vaan se tarjoaisi digitaalisen henkilöllisyyden välineitä tunnistusvälineenä luottamusverkoston tunnistuspalveluille erillisellä sääntelyllä. Digitaalisen henkilöllisyyden palvelujen tarjoajan toiminta ja velvollisuudet luottamusverkostossa eroaisivat siten voimassa olevassa laissa määriteltujen tunnistuspalvelun tarjoajien toiminnasta ja rooleista. Tästä syystä olisi perusteltua säätää digitaalisen henkilöllisyyden palvelujen tarjoajan roolista erikseen.

Digitaalisen henkilöllisyyden palvelujen tarjoaja tulisi käsitteellisesti erottaa tunnistuspalvelujen tarjoajista myös siksi, että tunnistuspalvelun tarjoajille on asetettu lain 10 §:ssä velvollisuus tehdä ilmoitus Liikenne- ja viestintävirastolle ja samalla liittyä osaksi luottamusverkostoa. Lisäksi digitaalisen henkilöllisyyden palvelujen tarjoajaan ei sovellettaisi useita muitakaan sellaisia tunnistus- ja luottamuspalvelulain säännöksiä, jotka koskevat tunnistuspalvelun tarjoajia. Esimerkiksi välineiden turvallisuusvaatimuksista, vaatimustenmukaisuuden arvioinnista, tietojen tallennusvelvollisuudesta, tarjonnasta käyttäjille ja vastuurajoituksista ei säädetä tunnistus- ja luottamuspalvelulaissa.

Vaikka digitaalisen henkilöllisyyden palvelujen tarjoaja ei olisi luottamusverkostossa tunnistusvälineen tarjoajan roolissa, olisi kyse kuitenkin käyttäjän kannalta samankaltaisesta toiminnasta kuin luottamusverkostossa toimivan tunnistusvälineen tarjoajan toiminta. Selvytyden vuoksi määritelmässä todettaisiin, että digitaalisen henkilöllisyyden palvelujen tarjoaja ei olisi tunnistuspalvelun tarjoaja.

Pykälän 1 momenttiin lisättäisiin myös uusi *13 kohta*, jossa määriteltäisiin digitaalisen henkilöllisyyden väline. Digitaalisen henkilöllisyyden välineellä tarkoitettaisiin sekä digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta että Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 14 §:ssä tarkoitettua ulkomaalaisen digitaalista asiointivälinettä. Ulkomaalaisen digitaalista asiointivälinettä voisi kuitenkin käyttää tunnistus- ja luottamuspalvelulaissa tarkoitettuun vahvaan sähköiseen tunnistamiseen vain silloin, kun sen haltija on tunnistettu 17 §:n mukaisesti. Ulkomaalaisen digitaalinen asiointiväline voidaan myöntää myös Digi- ja väestötietoviraston varmennepalveluista annetun lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä. Etärekisteröintimenettelyyn perustuva tunnistaminen ei kuitenkaan ole yhtä luotettava tapa tunnistaa välineen haltija, kuin tunnistus- ja luottamuspalvelulain 17 §:n mukaisesti tapahtunut ensitunnistaminen. Etärekisteröintimenettelyn yhteydessä myönnettyyn ulkomaalaisen digitaaliseen asiointivälineeseen perustuva sähköinen tunnistaminen ei siksi olisi tunnistus- ja luottamuspalvelulaissa tarkoitettua vahvaa sähköistä tunnistamista, eikä siihen perustuvia tunnistustapahtumia voisi välittää luottamusverkostossa.

7 b §. *Tieto passin, henkilökortin tai digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen voimassaolosta.* Pykälään lisättäisiin informatiivinen viittaus digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen voimassaolon tarkastamisesta. Kuten myöhemmin 17 §:n ja 17 b §:n yhteydessä on kuvattu, tunnistusvälineen tarjoajat voisivat hyödyntää digitaalista henkilöllisyystodistusta henkilön ensitunnistamiseen silloin, kun hänelle myönnetään uusi vahva sähköinen tunnistusväline. Tunnistuspalvelun tarjoaja voisi tällöin saada tiedon ensitunnistamisessa käytettävän digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen voimassaolosta joko Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 25 §:ssä tarkoitetun tarkastussovelluksen kautta tai Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 13 §:ssä tarkoitetusta ydinidentiteetin todisteiden rekisteristä. Digi- ja väestötietoviraston ylläpitämä rekisteri ydinidentiteetin todisteista on julkinen, ja sieltä voi tarkistaa digitaaliseen henkilöllisyystodis-

tukseen tallennetun ydinidentiteetin todisteen voimassaolon esimerkiksi sähköisessä asiointissa. Käyntiasioinnissa digitaalisen henkilöllisyystodistuksen käyttö on mahdollista joko Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 25 §:ssä tarkoitettua lukijarajapintaa tai tarkastussovellusta hyödyntäen. Mikäli käyntiasioinnissa hyödynnetään esimerkiksi kassajärjestelmään integroitua lukijarajapintaa, olisi tällöin huolehdittava siitä, että tarkastustoiminto integroidaan kassajärjestelmään, eli järjestelmä tarkastaa digitaalisen henkilöllisyystodistuksen voimassaolon ydinidentiteetin todisteiden rekisteristä samalla, kun se lukee digitaalisen henkilöllisyystodistuksen sisältämiä tietoja. Käyntiasioinnissa voitaisiin kuitenkin hyödyntää myös Digi- ja väestötietoviraston julkaisemaa tarkastussovellusta, joka tarkastaa digitaalisen henkilöllisyystodistuksen voimassaolon automaattisesti samalla, kun se näyttää käyttäjälle digitaalisesta henkilöllisyystodistuksesta luetut tiedot.

Lisäksi pykälään lisättäisiin tunnistusvälineen tarjoajan velvollisuus varmistaa, että ensitunnistamisessa käytettävä passi, henkilökortti tai digitaalinen henkilöllisyystodistus on voimassa. Käytännössä velvollisuus koskisi ainoastaan tilanteita, joissa ensitunnistaminen perustuu suomalaiseen passiin, henkilökorttiin tai digitaaliseen henkilöllisyystodistukseen. Tunnistus- ja luottamuspalvelulain 17 §:n mukaan ensitunnistaminen voisi perustua myös eräiden muiden maiden viranomaisten myöntämiin virallisiin henkilöllisyyttä osoittaviin asiakirjoihin, mutta näiden asiakirjojen voimassaoloa ei ole mahdollista tarkistaa sähköisesti. Velvollisuus varmistaa ensitunnistamisessa käytettävän asiakirjan voimassaolo koskisi vain 17 §:ssä tarkoitettuja ensitunnistustilanteita, eli tilanteita joissa vahvan sähköisen tunnistusvälineen hakijan henkilöllisyys varmennetaan uuden tunnistusvälineen myöntämisen yhteydessä. Voimassaolo olisi tarkistettava ensisijaisesti ennen tunnistusvälineen myöntämistä ja luovuttamista hakijalle. Jos voimassaolon tarkistaminen ei kuitenkaan ole mahdollista ensitunnistamisen yhteydessä esimerkiksi tietoliikennehäiriön tai muun käyttökatkon vuoksi, voisi voimassaolotarkistuksen tehdä myös jälkikäteen. Tunnistusvälineen tarjoajan olisi kuitenkin varmistettava, että tunnistusvälineettä ei voi käyttää ennen kuin voimassaolotarkistus on tehty. Tunnistusvälineen voisi näin ollen luovuttaa hakijalle ennen kuin voimassaolotarkistus on tehty, mutta tällöin väline tulisi aktiivoida käyttöön vasta myöhemmin.

Mahdollisuus tarkistaa ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolo poliisin tietojärjestelmästä on ollut käytössä jo vuodesta 2017 saakka, mutta tunnistusvälineiden tarjoajat ovat hyödyntäneet sitä vain harvoin. Sääntelyllä ei siten ole saatu parannettua tunnistusvälineiden myöntämisen turvallisuutta, vaan voimassaolon tarkistaminen on jäänyt tunnistuspalvelun oman riskiarvion varaan. Liikenne- ja viestintävaliokunta on pitänyt tärkeänä, että vahvan sähköisen tunnistusvälineen uusimiseen ja myöntämiseen liittyviä väärinkäytöksiä pyritään estämään kaikin käytössä olevin keinoin ja että mahdollisia lainsäädäntötarpeita seurataan (LiVM 6/2021 vp). Tunnistusvälineiden tarjoajille asetettava velvollisuus varmistaa poliisin tietojärjestelmästä, Digi- ja väestötietoviraston tarkastussovelluksesta tai ydinidentiteetin todisteiden rekisteristä saatava tieto asiakirjan voimassaolosta voisi parantaa tunnistusvälineiden myöntämisen turvallisuutta, kun voimassaolo tarkistettaisiin jatkossa aina. Passin tai henkilökortin voimassaolon varmistaminen poliisin tietojärjestelmästä ei ole maksullista, mutta saattaa edellyttää tunnistusvälineen tarjoajalta kansallisen palveluväylän liityntäpalvelimen perustamista.

12 e §. *Digitaalisen henkilöllisyyden palvelujen tarjoajan velvollisuudet luottamusverkostossa.* Pykälä olisi uusi ja koskisi vain digitaalisen henkilöllisyyden palvelujen tarjoajaa. Ehdotetun 1 momentin mukaan digitaalisen henkilöllisyyden palvelujen tarjoajan on tarjottava Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 4 §:ssä tarkoitettua digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää digitaalisen henkilöllisyyden välineeseen perustuvia tunnistustapah-
tunmia asiointipalveluille. Selvyyden vuoksi on todettava, että pykälä koskisi vain digitaalisen

henkilöllisyyden välineeseen perustuvien tunnistustapahtumien välittämistä. Digitaalisen henkilöllisyyden tietojärjestelmää hyödynnetään myös Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 4 luvussa tarkoitetun ulkomaalaisen digitaalisen asiointivälineen tuottamiseen ja käyttämiseen silloin, kun välineen käyttäjä on tunnistettu Digi- ja väestötietoviraston varmennepalveluista annetun lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä. Etärekisteröintimenettelyn perusteella myönnettyt ulkomaalaisen digitaaliset asiointivälineet eivät kuitenkaan kuulu tunnistus- ja luottamuspalvelulain soveltamisalaan eikä niihin perustuvia tunnistustapahtumia voi välittää luottamusverkostossa.

Kyse olisi sääntelystä, jolla digitaalisen henkilöllisyyden palvelujen tarjoaja velvoitetaan luovuttamaan käyttöoikeus tunnistuspalveluun tunnistusvälityspalveluille. Vastaavanlainen velvollisuus koskee voimassa olevan lain mukaan luottamusverkostossa toimivia tunnistusvälineen tarjoajia. Tunnistus- ja luottamuspalvelulaki soveltuu kuitenkin vain luottamusverkostossa toimiviin tunnistusvälityspalvelun tarjoajiin, joten pykälä ei soveltuisi digitaalisen henkilöllisyyden välineeseen perustuvan tunnistustapahtuman välittämiseen muiden kuin luottamusverkostoon kuuluvien tunnistusvälityspalvelun tarjoajien toimesta. Digitaalisen henkilöllisyyden välineet olisivat kuitenkin hyödynnettävissä myös luottamusverkoston ulkopuolella siten, kuin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 7 §:ssä säädetään.

Digitaalisen henkilöllisyyden palvelujen tarjoaja ei siis tulisi osapuoleksi kansalliseen vahvan sähköisen tunnistamisen luottamusverkostoon. Kuten edellä 2 §:n yhteydessä on selostettu, digitaalisen henkilöllisyyden palvelujen tarjoajan toiminnassa olisi kyse digitaalisen henkilöllisyyden luomisesta ja tätä henkilöllisyyttä osoittavista välineistä, jotka valtio myöntää osana julkisten palvelujen tuottamista.

Digitaalisen henkilöllisyyden palvelujen tarjoajan olisi tarjottava digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeus maksutta tunnistusvälityspalvelun tarjoajille. Voimassa olevan lain 12 c §:n mukaan tunnistusvälityspalvelun tarjoajan on suoritettava luottamusverkostossa toimiville tunnistuspalvelun tarjoajille korvaus tunnistuspalvelun käyttöoikeudesta. Digitaalisen henkilöllisyyden palvelujen tarjoaja ei kuitenkaan tulisi osaksi luottamusverkostoa, eikä 12 c §:n mukainen korvausvelvollisuus soveltuisi digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeuden hyödyntämiseen.

Sääntelyllä on tarkoitus varmistaa, että digitaalisen henkilöllisyyden välineet ovat koko yhteiskunnan hyödynnettävissä, vaikka digitaalisen henkilöllisyyden palvelujen tarjoaja ei olisi osa tunnistus- ja luottamuspalvelulain mukaista luottamusverkostoa. Velvollisuudella tarjota palvelunsa tunnistusvälityspalvelun tarjoajalle välitettäväksi varmistetaan, että asiointipalvelu voi edelleen hankkia asiakkaidensa tunnistuksen kootusti tarvitsematta erillisiä teknisiä rajapintoja tai erillistä sopimusta digitaalisen henkilöllisyyden palvelujen tarjoajan kanssa.

Sääntely ei kuitenkaan ottaisi kantaa digitaalisen henkilöllisyyden palvelujen tarjoajan ja sitä luottamusverkoston välityspalvelun kautta hyödyntävän luottavan osapuolen väliseen vastuunjakoon. Luottamusverkoston tunnistuspalvelut ja tunnistusvälityspalvelut vastaavat tunnistuspalveluistaan käyttäjille ja luottaville osapuolille tunnistus- ja luottamuspalvelulain mukaisesti (esimerkiksi 15 §:ssä säädetty tunnistusvälineen tarjoajan tiedonantovelvollisuus tunnistusvälineen hakijalle ja 18 §:n 2 momentissa säädetty tunnistuspalvelun tarjoajan huolehtimisvelvollisuus oikeustoimien tekemiselle asetettuihin estoihin ja rajoituksiin liittyen).

Ehdotetussa 1 momentissa on informatiivinen viittaus Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettuun lakiin. Ennen digitaalisen henkilöllisyyden tietojärjes-

telmän käyttöönottoa julkaistavista tiedoista on säädetty mainitun lain 7 §:ssä. Digitaalisen henkilöllisyyden palvelujen tarjoajaa ei velvoitettaisi julkaisemaan digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeuden toimitusehtoja, mutta sen olisi kuitenkin tarjottava sitä niiden tietojen mukaisesti, jotka se on etukäteen ilmoittanut.

Ehdotetun 2 *momentin* mukaan digitaalisen henkilöllisyyden palvelujen tarjoajan tulee itse määrittellä ne tekniset rajapinnat ja standardit, joilla se tarjoaa digitaalisen henkilöllisyyden tietojärjestelmää. Voimassa olevan lain mukaan luottamusverkoston toimijoilla on keskinäinen yhteistyövelvoite teknisten käytäntöjen yhteensovittamiseksi. Tätä on pidetty luottamusverkostossa välttämättömänä, jotta eri tunnistuspalvelut voivat tosiasiaassa yhteenliittää palvelunsa tarvitsematta erilaista teknistä toteutusta eri tunnistuspalveluiden kanssa. Vastaava yhteistyövelvoite ei kuitenkaan koskisi digitaalisen henkilöllisyyden palvelujen tarjoajaa. Digitaalisen henkilöllisyydestodistuksen hyödyntämiseksi tuotettavan digitaalisen henkilöllisyyden tietojärjestelmän yhteentoimivuutta luottamusverkoston tunnistuspalvelujen kanssa edistettäisiin Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavan lain 7 §:n 2 momentin mukaisella velvollisuudella tarjota digitaalisen henkilöllisyyden tietojärjestelmä niiden tietojen mukaisesti, jotka on etukäteen ilmoitettu. Muut tunnistuspalvelun tarjoajat voisivat rakentaa tarvittavat tekniset rajapinnat digitaalisen henkilöllisyyden hyödyntämiseksi näiden tietojen perusteella.

16 §. *Tunnistuspalvelun tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä.* Pykälään lisättäisiin uusi 3 *momentti*, joka koskisi tunnistuspalvelun tarjoajan mahdollisuutta ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä myös digitaalisen henkilöllisyyden palvelujen tarjoajalle. Vaikka digitaalisen henkilöllisyyden palvelujen tarjoaja ei olisikaan osa luottamusverkostoa, olisi digitaalisen henkilöllisyyden välineitä mahdollista hyödyntää luottamusverkostossa. Digitaalisen henkilöllisyyden palvelujen tarjoajan olisi siten tarpeen saada tieto välineiden käyttöön liittyvistä uhkista ja häiriöistä. Tunnistuspalvelun tarjoajan olisi salassapitosäännösten estämättä ilmoitettava ilman aiheutonta viivästystä 1 momentissa tarkoitetut tiedot myös digitaalisen henkilöllisyyden palvelujen tarjoajalle. Lisäksi tunnistuspalvelun tarjoaja voisi salassapitosäännösten estämättä ilmoittaa digitaalisen henkilöllisyyden palvelujen tarjoajalle 2 momentin mukaisia tietoja ja uhkien ja häiriöiden selvittämiseen liittyviä tietoja. Digitaalisen henkilöllisyyden palvelujen tarjoajan velvollisuudesta ilmoittaa vastaavia tietoja tunnistuspalvelun tarjoajalle säädettäisiin 16 a §:ssä. Valtioneuvoston asetuksessa (169/2016) vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta säädetään, että luottamusverkostoon kuuluva tunnistuspalvelun tarjoaja vastaa omalta osaltaan häiriötilanteiden selvittämisestä luottamusverkostossa. Tunnistuspalvelun tarjoajan ja digitaalisen henkilöllisyyden palvelujen tarjoajan välinen tiedonvaihto voisi olla tarpeen uhkien ja häiriöiden selvittämiseksi.

16 a §. *Digitaalisen henkilöllisyyden palvelujen tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä.* Pykälä olisi uusi ja koskisi vain digitaalisen henkilöllisyyden palvelujen tarjoajan ilmoitusvelvollisuutta. Pykälän 1 *momentissa* asetettaisiin digitaalisen henkilöllisyyden palvelujen tarjoajalle velvollisuus ilmoittaa digitaalisen henkilöllisyyden välineiden tietoturvaan, tietosuojaan tai digitaalisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista, häiriöistä tai palvelun keskeytyksistä sekä uhkien ja häiriöiden selvittämiseen liittyvistä tiedoista. Lisäksi olisi ilmoitettava niistä toimista, joilla uhkia tai häiriöitä voidaan eri tahojen toimesta torjua sekä näiden toimenpiteiden arvioiduista kustannuksista.

Ehdotetun *1 momentin* mukaan ilmoitus tehtäisiin sekä luottamusverkostossa toimiville tunnistuspalvelun tarjoajille, että Liikenne- ja viestintävirastolle. Luottamusverkoston tunnistuspalvelun tarjoajat voivat hyödyntää digitaalisen henkilöllisyyden välineitä, jolloin niiden on tarpeen tietää sen käyttöön liittyvistä uhkista, häiriöistä tai palvelun keskeytyksistä.

Vaikka Liikenne- ja viestintävirasto ei valvoisi digitaalisen henkilöllisyyden palvelujen tarjoajaa yleisesti, olisi ilmoitus Liikenne- ja viestintävirastolle kuitenkin tarpeen, sillä Liikenne- ja viestintävirasto valvoo toimintaa luottamusverkostossa, jossa myös digitaalisen henkilöllisyyden välineitä on mahdollista hyödyntää. Tarkoitus on, että luottamusverkoston valvova viranomaisena olisi tietoinen säännöksessä tarkoitetuista uhista ja häiriöistä. Liikenne- ja viestintävirasto voi esimerkiksi tarvittaessa osallistua tiedottamiseen, jotta tieto leviäisi mahdollisimman nopeasti silloin, kun tämänkaltaisen toiminta estäisi vahinkoja syntymästä.

Ehdotettu pykälä ei sisällä yksityiskohtaisia vaatimuksia siitä, miten ilmoittaminen tulisi tehdä. Digitaalisen henkilöllisyyden palvelujen tarjoajan on siis harkittava kulloinkin tehokas ilmoittamistapa. Ehdotetun pykälän mukaan ilmoittaminen olisi tehtävä ilman aiheetonta viivytystä. Tiedottamisen ajankohta jää siten digitaalisen henkilöllisyyden palvelujen tarjoajan harkintaan.

Pykälän *2 momentissa* säädettäisiin siitä, miten tunnistuspalvelun tarjoajat ja digitaalisen henkilöllisyyden palvelujen tarjoaja saavat käsitellä *1 momentin* ja *16 §:n 3 momentin* nojalla saamia tietoja. Luottamusverkostossa toimivien tunnistuspalvelun tarjoajien kesken vaihdettavan tiedon käsittelyperusteista on säädetty tunnistus- ja luottamuspalvelulain *12 a §:n 5 momentissa*. Kuitenkin myös tunnistuspalvelun tarjoajien ja digitaalisen henkilöllisyyden palvelujen tarjoajan välillä vaihdettavia tietoja olisi käsiteltävä vain siihen tarkoitukseen, jota varten ne on annettu. Lisäksi tietoja saisi käsitellä tunnistuspalvelun tarjoajan palveluksessa tai sen lukuun vain ne, jotka tarvitsevat tietoja välttämättä työssään.

17 §. *Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen.* Pykälän *2 momenttia* muutettaisiin siten, että silloin kun henkilön ensitunnistamisessa henkilön tunnistaminen perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, tunnistusvälineen tarjoaja voisi halutessaan varmentaa henkilön henkilöllisyyden myös digitaalisella henkilöllisyystodistuksella. Digitaalisesta henkilöllisyystodistuksesta annetun lain *3 §:n* mukaan digitaalinen henkilöllisyystodistus on henkilöllisyyden osoittamiseen tarkoitettu henkilöllisyystodistus. Digitaalisen henkilöllisyystodistuksen hyödyntämisestä ensitunnistamiseen säädettäisiin tarkemmin *17 b §:ssä*.

Pykälän *4 momentissa* säädetään ns. ensitunnistamisen ketjuttamisesta, eli tunnistusvälineen tarjoajan velvollisuudesta mahdollistaa myöntämänsä vahvan sähköisen tunnistusvälineen käyttäminen ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Momenttiin lisättäisiin selvyyden vuoksi maininta myös digitaalisen henkilöllisyyden palvelujen tarjoajasta ja digitaalisen henkilöllisyyden välineestä. Tunnistusvälineen tarjoajan olisi siten mahdollistettava myöntämänsä vahvan sähköisen tunnistusvälineen käyttäminen ensitunnistamiseen digitaalisen henkilöllisyyden välineen käyttöönoton yhteydessä. Selvyyden vuoksi todetaan, että ensitunnistamisen ketjuttamisesta perittävästä korvauksesta on säädetty *17 §:n 7 momentissa*, joka on voimassa määräaikaaisesti. Myös kyseinen hintasääntely soveltuisi tilanteisiin, joissa vahvaa sähköistä tunnistusvälinettä käytetään digitaalisen henkilöllisyyden välineen käyttöönottoon.

17 b §. *Digitaalinen henkilöllisyystodistus ensitunnistamisessa.* Pykälä olisi uusi ja koskisi vain digitaalisen henkilöllisyystodistuksen hyödyntämistä ensitunnistamisessa. Ehdotetun pykälän mukaan digitaalisen henkilöllisyyden palvelujen tarjoajan olisi mahdollistettava, että tunnistusvälineen tarjoajat voivat käyttää digitaalista henkilöllisyystodistusta ensitunnistamiseen, kun ne

myöntävät hakijalle uuden vahvan sähköisen tunnistusvälineen. Kyse olisi siis digitaaliseen henkilöllisyystodistukseen perustuvasta sähköisestä ensitunnistamisesta uuden vahvan sähköisen tunnistusvälineen myöntämiseksi eli niin sanotusta ensitunnistamisen ketjuttamisesta.

Tunnistusvälineen tarjoajilla tarkoitettaisiin tunnistus- ja luottamuspalvelulain 10 §:n mukaisesti Liikenne- ja viestintävirastoon ilmoituksen tehneitä palveluntarjoajia. Säännös koskisi vain tilanteita, joissa digitaalisella henkilöllisyystodistuksella luodaan toinen vahva sähköinen tunnistusväline eli tunnistusväline, joka tunnistus- ja luottamuspalvelulain 2 §:n 1 kohdan mukaisesti täyttää eIDAS-asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset. Tunnistus- ja luottamuspalvelulaki soveltuu vain luottamusverkostossa toimiviin tunnistusvälineen tarjoajiin, joten pykälä ei soveltuisi digitaalisen henkilöllisyystodistuksen käyttämiseen muiden kuin luottamusverkostoon kuuluvien tunnistusvälineiden luomiseen.

Digitaalisen henkilöllisyyden palvelujen tarjoajan olisi mahdollistettava digitaalisen henkilöllisyystodistuksen käyttäminen ensitunnistamiseen maksutta, eli se ei voisi periä tunnistusvälineen tarjoajilta korvausta tunnistus- ja luottamuspalvelulain 17 §:n 7 momentin mukaisesti.

Mitä digitaalisen henkilöllisyyden palveluista annetun lain 7 §:ssä säädetään ennen digitaalisen henkilöllisyyden tietojärjestelmän käyttöönottoa julkaistavista tiedoista, sovelletaan myös digitaalisen henkilöllisyystodistuksen käyttämiseen ensitunnistamisessa. Näin ollen digitaalisen henkilöllisyyden palvelujen tarjoaja esimerkiksi määrittelee ne tekniset rajapinnat ja standardit, joita käytetään digitaalisen henkilöllisyystodistuksen hyödyntämiseen ensitunnistamisessa.

42 a §. *Liikenne- ja viestintäviraston tehtävät.* Pykälän 3 momentin 2 kohtaa muutettaisiin siten, että Liikenne- ja viestintäviraston tehtävää ilmoittaa sähköisen tunnistamisen järjestelmiä Euroopan komissiolle rajattaisiin tunnistus- ja luottamuspalvelulain 10 §:n mukaisesti ilmoitettuihin tunnistuspalveluihin. Liikenne- ja viestintäviraston tehtävä ilmoittaa sähköisen tunnistamisen järjestelmiä Euroopan komissiolle ei siten koskisi digitaalisen henkilöllisyyden välineitä.

7.4 Laki henkilötietojen käsittelystä poliisitoimessa annetun lain 16 §:n ja 22 §:n muuttamisesta

16 §. *Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä.* Pykälän 1 momenttia ehdotetaan muutettavaksi siten, että siihen lisättäisiin uusi 16 kohta, jonka perusteella poliisilla olisi oikeus saada tietoja Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain mukaisesti ydinidentiteetin todisteen myöntämiseksi sekä digitaalisen henkilöllisyystodistuksen tuottamiseksi välttämättömistä tiedoista sekä henkilötietojen väärinkäytöepäilyjen, identiteettivarkauksien tai muiden vastaavien rikosten selvittämiseksi ja näiden ennalta estämiseksi. Samalla pykälän 1 momentin 15 kohtaan tehtäisiin tekninen muutos niin, että kohtien väliin ei jää pistettä. Muilta osin pykälään ei tehtäisi muutoksia.

22 §. *Muu henkilötietojen luovuttaminen viranomaisille.* Pykälän 1 momenttia ehdotetaan muutettavaksi siten, että siihen lisättäisiin uusi 18 kohta, jonka perusteella poliisi saisi salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona vain 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi Digi- ja väestötietovirastolle Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettussa laissa tarkoitettujen digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin tuottamista ja hallinnointia varten. Samalla pykälän 1 momentin 17 kohtaan tehtäisiin tekninen muutos siten, että kohtien väliin ei jää pistettä. Lisäksi ruotsinkielisessä laissa kyseiseen kohtaan lisättäisiin maininta palvelussuhdettehtävistä (tjänstgöringsuppdrag). Muutoksen jälkeen ruotsinkielinen laki vastaisi suomenkielistä lakia.

7.5 Laki henkilökorttilain muuttamisesta

1 a §. *Digitaalinen henkilöllisyystodistus.* Pykälä olisi uusi. Sen *1 momentin* mukaan henkilökorttiin sisältyisi oikeus ottaa käyttöön laissa digitaalisesta henkilöllisyystodistuksesta tarkoitettu henkilökorttiviranomaisen myöntämä digitaalinen henkilöllisyystodistus. Henkilöllä olisi siis suoraan oikeus saada digitaalinen henkilöllisyystodistus, jos hänelle on myönnetty henkilökortti. Poliisi ei tekisi erillistä myöntöpäätöstä digitaalisen henkilöllisyystodistuksen käyttöön otosta. Digitaalinen henkilöllisyystodistus otettaisiin käyttöön siten kuin ehdotetussa laissa digitaalisesta henkilöllisyystodistuksesta säädetään. Pykälän *2 momentin* mukaan oikeutta digitaalisen henkilöllisyystodistuksen käyttöönottoon ei sisältyisi väliaikaiseen henkilökorttiin eikä alle 15-vuotiaalle myönnettyyn alaikäisen henkilökorttiin.

Lisäksi ehdotetaan säädettäväksi siirtymäsäännöksestä lain voimaantuloon, jonka mukaan oikeus ottaa digitaalinen henkilöllisyystodistus käyttöön sisältyisi myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin henkilökortteihin.

7.6 Laki passilain muuttamisesta

3 d §. *Digitaalinen henkilöllisyystodistus.* Pykälä olisi uusi. Sen *1 momentin* mukaan passiin sisältyisi oikeus ottaa käyttöön laissa digitaalisesta henkilöllisyystodistuksesta tarkoitettu passiviranomaisen myöntämä digitaalinen henkilöllisyystodistus. Henkilöllä olisi siis suoraan oikeus saada digitaalinen henkilöllisyystodistus, jos hänelle on myönnetty passi. Poliisi ei tekisi erillistä myöntöpäätöstä digitaalisen henkilöllisyystodistuksen käyttöönotosta. Digitaalinen henkilöllisyystodistus otettaisiin käyttöön siten kuin ehdotetussa laissa digitaalisesta henkilöllisyystodistuksesta säädetään. Pykälän *2 momentin* mukaan oikeutta digitaalisen henkilöllisyystodistuksen käyttöönottoon ei sisältyisi väliaikaiseen passiin tai hätäpassiin.

Lisäksi ehdotetaan säädettäväksi siirtymäsäännöksestä lain voimaantuloon, jonka mukaan oikeus ottaa digitaalinen henkilöllisyystodistus käyttöön sisältyisi myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin passeihin.

7.7 Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta

6 b luku. Luonnollisen henkilön tunnistusväline

69 e §. *Luonnollisen henkilön tunnistusväline.* Pykälässä säädettäisiin uudesta luonnollisen henkilön tunnistusvälineestä. Kyse olisi Digi- ja väestötietoviraston tuottamasta fyysisestä tunnistusvälineestä, joka olisi ensisijaisesti tarkoitettu henkilöille, jotka eivät voi taikka halua käyttää muita valtion tarjoamia välineitä julkisen hallinnon sähköisiin palveluihin pääsemiseksi. Luonnollisen henkilön tunnistusväline tarjottaisiin julkisen hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain mukaisena tukipalveluna ja sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisena tunnistuspalveluna julkisen sektorin organisaatioille.

Pykälän *1 momentin* mukaan Digi- ja väestötietoviraston tehtävänä olisi myöntää luonnollisen henkilön sähköiseen tunnistamiseen tarkoitettua tunnistusvälinettä, joka täyttäisi 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. Ehdotettu momentti vastaisi olennaisilta osin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 kohdan mukaista vahvan sähköisen tunnistamisen määritelmää ja momentin tarkoituksena olisi asettaa Digi- ja

väestötietoviraston tuottamalle luonnollisen henkilön tunnistusvälineelle samat tunnistamisen tietoturvaluusvaatimukset kuin jo olemassa olevilla vahvan sähköisen tunnistamisen tunnistusvälineillä. Tunnistusväline ei kuitenkaan olisi osa tunnistus- ja luottamuspalvelulakia ja siten se ei olisi myöskään vahva sähköinen tunnistusväline. Se olisi kuitenkin digipalvelulain 6 §:n 2 momentin tarkoittama muu vastaava tietoturvaluinen tunnistusväline.

Pykälän 2 momentin mukaan Digi- ja väestötietovirasto luovuttaisi luonnollisen henkilön tunnistusvälineen henkilölle fyysisenä välineenä, joka olisi käytettävissä ilman mobiilipäätelaitetta tai sirukorttia. Momentti jättäisi tunnistusvälineen toteutusteknologian avoimeksi ja olisi siten välineen fyysisistä olomuotoa koskevaa vaatimusta lukuun ottamatta kirjoitettu teknologia-neutraaliksi. Kyseisen momentin tarkoituksena olisi säätää lain tasolla valtion tarjoamasta uudesta fyysisestä tunnistusvälineestä, jota esimerkiksi erityisryhmät voisivat hyödyntää tunnistautuessaan julkisen hallinnon asiointipalveluihin.

Pykälän 3 momentin mukaan Digi- ja väestötietovirasto tarjoaisi luonnollisen henkilön tunnistusvälinettä sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisena tunnistusvälineenä käytettäväksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:n 1 momentin 4 kohdassa tarkoitetun tukipalvelun välityksellä. Tukipalvelulain 4 §:n mukaan Digi- ja väestötietoviraston tehtävänä on tuottaa ja kehittää 3 §:n 1 momentin 1–7 kohdissa tarkoitettuja tukipalveluja. Tukipalvelulain 3 §:ssä säädetään tukipalveluista ja sen 1 momentissa listataan yhteiset sähköisen asioinnin tukipalvelut. Kyseisen 3 §:n 1 momentin 4 kohdassa säädetään luonnollisen henkilön tunnistuspalvelusta, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa tarkoitetun tunnistuspalvelun tarjoajan palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle.

Ehdotetun säännöksen 3 momentin mukaan luonnollisen henkilön tunnistusväline tarjottaisiin siten käytettäväksi osana nykyistä Suomi.fi-tunnistusta. Tukipalvelulain 5 §:ssä säädetään tukipalvelujen käytöstä julkisessa tehtävässä ja sen 1 momentissa valtion hallintoviranomaisille, virastoille, laitoksilla ja liikelaitoksille, kunnallisille viranomaisille niiden hoitaessa laissa niille säädettyjä tehtäviä sekä tuomioistuimille ja muille lainkäyttöelimille velvollisuus käyttää lain 3 §:n 1 momentin 1–4, 7 ja 8 kohdassa tarkoitettuja tukipalveluja, jollei viranomaisen ole teknisistä tai toiminnallisista tai kustannustehokkuuteen taikka tietoturvaluuteen liittyvistä syistä välttämätöntä käyttää toiminnassaan tai sen osassa muuta palvelua.

69 f §. *Rekisteri luonnollisen henkilön tunnistusvälineistä.* Pykälässä säädettäisiin luonnollisen henkilön tunnistusvälineiden rekisteristä. Rekisterin ylläpitoon liittyvän henkilötietojen käsittelyn oikeusperusteena on tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta. Ehdotetussa säännöksessä säädettäisiin luonnollisen henkilön tunnistusvälineen myöntämisen yhteydessä rekisteröitävistä henkilötiedoista henkilötietotyypeittäin. Sääntely ei olisi tyhjentävää, mutta se olisi omiaan antamaan rekisteröidylle kuvan siitä, minkälaisia henkilötietoja käsitellään ja käsiteltävät tiedot määräytyisivät lopulta käsittelyn tarkoituksen perusteella. Joka tapauksessa henkilötietojen käsittelyn on tietosuoja-asetuksen mukaisesti oltava perusteltua ja yhteensopivaa käytötarkoitukseen nähden.

Pykälän 1 momentin mukaan Digi- ja väestötietoviraston tehtävänä olisi ylläpitää luonnollisen henkilön tunnistusvälineen tarjoamista ja tuottamista varten rekisteriä myönnetyistä luonnollisen henkilön tunnistusvälineistä ja niiden haltijoista. Siinä säädettäisiin tarkemmin rekisteriin talletettavista tunnistusvälineen haltijan tiedoista. Rekisteriin tallennettavia tietoja olisivat henkilötiedot, jotka sisältyvät henkilöllisyyden varmentamiseen käytettyyn viranomaisen myöntä-

mään henkilöllisyyttä osoittavaan asiakirjaan sekä asiakirjan yksilöintitiedot (1 kohta), henkilötiedot, jotka välitetään henkilöllisyyden varmentamiseen käytetyn sähköisen tunnistusmenetelmän yhteydessä sekä tiedot sähköisestä tunnistusmenetelmästä (2 kohta), VTJ-lain 11 a §:n mukainen henkilön yksilöintitunnus (3 kohta), tunnistusvälineen yksilöivä tunniste (4 kohta), luonnollisen henkilön tunnistusvälineen haltijan yhteystiedot (5 kohta) sekä muut kuin 1–5 kohdassa tarkoitetut tunnistusvälineen tarjoamiseksi tarpeelliset tiedot.

Rekisteriin voitaisiin momentin *1 kohdan* mukaan tallentaa luonnollisen henkilön henkilötiedot, jotka sisältyvät henkilöllisyyden varmentamiseen käytettyyn viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan sekä asiakirjan yksilöintitiedot. Nämä tiedot tulisivat tallennettavaksi yksinomaan viranomaisen myöntämään asiakirjaan perustuvan ensitunnistamisen myötä. Tällöin tallennettaisiin myös kuva henkilöllisyyttä osoittavasta asiakirjasta tai asiakirjan oikeaksi todistettu jäljennös tai valokopio siitä.

Momentin *2 kohdan* mukaan rekisteriin voitaisiin tallentaa henkilötiedot, jotka välitetään henkilöllisyyden varmentamiseen käytetyn sähköisen tunnistusmenetelmän yhteydessä. Nämä tiedot olisivat käytännössä tietoja, joita välitetään Digi- ja väestötietovirastolle sen käyttäessä ensitunnistamiseen jonkin toisen tunnistuspalveluntarjoajan tunnistusmenetelmää. Lisäksi tallennettaisiin tiedot käytetystä tunnistusmenetelmästä.

Momentin 3–5 kohdissa säädettäisiin rekisteriin tallennettavaksi henkilön yksilöintitunnus sekä tunnistusvälineen yksilöivä tunniste ja tarvittavat yhteystiedot, jotta on mahdollista esimerkiksi ilmoittaa tunnistusvälineen haltijalle tunnistusvälineen käytön estämisestä tai peruuttamisesta.

Momentin *6 kohdassa* säädettäisiin mahdollisuudesta tallentaa rekisteriin muitakin luonnollisen henkilön tunnistusvälineen tarjoamiseksi tarpeellisia tietoja. Koska kyse on uudenlaisesta palvelusta, tässä vaiheessa ei ole vielä mahdollista tyhjentävästi määritellä kaikkia käsiteltäviä tietoja. Riippuen esimerkiksi henkilön ensitunnistamisen menetelmästä, voi tunnistusvälineen tarjoamiseksi olla tarpeen käsitellä muitakin kuin säännöksen 1–6 kohdissa tarkoitettuja tietoja. Siltä osin kuin tunnistusvälineen tarjoamiseen sisältyy fyysinen väline, voi se edellyttää muidenkin tietojen käsittelyä esimerkiksi tietoturvallisuuden varmistamiseksi. Lisäksi on otettava huomioon, että tunnistusvälineen tarjoamisessa voi olla tarpeen esimerkiksi täydentää henkilön tietoja sellaisilla henkilöltä itseltään saatavilla tiedoilla, jotka eivät ilmene viranomaisen myöntämästä henkilöllisyyttä osoittavasta asiakirjasta tai joita ei välitetä sähköiseen ensitunnistamiseen käytetystä toisen palveluntarjoajan tunnistuspalvelusta.

Pykälän *2 momentin* mukaan henkilötietojen käsittelystä luonnollisen henkilön tunnistusvälineen palvelutuotannossa, tunnistusvälinettä ja sen käyttöä koskevista vaatimuksista sekä palvelutuotannon ohjauksesta säädetään tukipalvelulain 3–5 luvussa. Tukipalvelulain 3 luvussa säädetään henkilö- ja muiden tietojen käsittelystä palvelutuotannossa, sen 4 luvussa tukipalvelujen ja niiden käyttöä koskevista vaatimuksista ja sen 5 luvussa ohjauksesta. Koska luonnollisen henkilön tunnistusvälinettä tarjottaisiin tukipalvelulain mukaisena tukipalveluna, on tarkoituksenmukaista, että tietojenkäsittelystä palvelutuotannossa ja palvelutuotantoa koskevista vaatimuksista sekä palvelutuotannon ohjauksesta säädettäisiin tukipalvelulaissa.

69 g §. Hakijan henkilöllisyyden todistaminen. Pykälässä säädettäisiin tunnistusvälineen myöntämiseen liittyvästä menettelystä. Pykälän *1 momentin* mukaan Digi- ja väestötietovirasto myöntäisi luonnollisen henkilön tunnistusvälineen hakemuksesta henkilölle. Tunnistusvälineen hakemisessa olisi kyse hallintopäätöksen tekemisestä, johon sovellettaisiin tavanomaista hallintolain mukaista asian käsittelyprosessia.

Pykälän 2 momentissa säädettäisiin ensitunnistamisen tekemisestä joko henkilökohtaisesti tai sähköisesti. Digi- ja väestötietoviraston olisi tunnistettava tunnistusvälineen hakija huolellisesti ennen myöntävän päätöksen tekemistä. Momentin mukaan luonnollisen henkilön tunnistaminen tulisi tehdä joko henkilökohtaisesti viranomaisen luona tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Ehdotetussa momentissa viitattaisiin EU:n sähköisen tunnistamisen varmuustasoasetuksen liitteen kohtaan 2.1.2, jossa säädetään luonnollisen henkilön henkilöllisyyden todistamisesta ja varmentamisesta silloin kun henkilö hakee korotetun tai korkean varmuustason sähköistä tunnistusvälinettä.

69 h §. Tunnistusvälineen myöntämiseen liittyvien tehtävien hoitaminen yhteispalvelussa. Pykälässä säädettäisiin mahdollisuudesta hoitaa tunnistusvälineen myöntämiseen liittyviä tehtäviä yhteispalvelulain nojalla. Ehdotetun 1 momentin mukaan näihin tehtäviin voisi kuulua tunnistusvälineen hakijan tai haltijan henkilöllisyyden todentaminen sekä tunnistusvälineen hakemiseen liittyvät neuvonta- ja tukitehtävät. Tehtäväkokonaisuus sisältyisi yhteispalvelulain 6 §:n mukaisiin tehtäviin eikä pitäisi sisällään julkisen vallan käyttöön liittyviä tehtäviä. Yhteispalvelussa suoritettavaan tehtävään sovellettaisiin muuten, mitä yhteispalvelulaissa säädetään. Yhteispalvelulain 8 §:n mukaan yhteispalvelun järjestämisestä on tehtävä kahden tai useamman viranomaisen keskeinen kirjallinen, toistaiseksi tai määräajan voimassa oleva toimeksiantosopimus. Sopimuksessa on sovittava muun muassa siitä, mitä asiakaspalvelutehtäviä sopimus koskee ja missä laajuudessa niitä hoidetaan yhteispalveluna. Lisäksi on sovittava esimerkiksi salassa pidettävien tietojen ja henkilötietojen käsittelyyn liittyviä velvoitteita koskevista käytännön järjestelyistä.

Henkilötietojen käsittelystä sovittaessa olisi luonnollisesti otettava huomioon tietosuojasetuksesta johtuvat vaatimukset. Asetuksen 28 artiklassa muun muassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Artiklan mukaan toimeksiantosuhtetta on määritettävä käsittelysopimuksella tai ”muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla”, ellei käyttäjäorganisaation tehtävistä säädetä yksiselitteisesti lailla. Vaikka rekisterinpitäjällä on lähtökohtainen vastuu henkilötietojen käsittelystä ja käyttämisestä henkilötietojen käsittelijöistä, asetuksen mukaan myös käsittelijä voi joutua itseensä vastuuseen rikkoessaan asetuksen säännöksiä.

Ehdotetun 3 momentin mukaan yhteispalvelun toimeksisaajan tulisi siirtää asia Digi- ja väestötietoviraston käsiteltäväksi, jollei se lisäselvitysten jälkeenkään voi todentaa hakijan henkilöllisyyttä. Digi- ja väestötietoviraston olisi tällöin ratkaistava henkilöllisyyden todentaminen ja mahdollisuus myöntää hakijalle tunnistusväline.

69 i §. Tieto passin tai henkilökortin voimassaolosta. Ehdotetun pykälän mukaan Digi- ja väestötietovirastolla olisi oikeus saada salassapitosäännösten estämättä teknisen rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta. Pykälän tarkoituksena olisi mahdollistaa luonnollisen henkilön tunnistusvälineen myöntäminen henkilölle, jolla on voimassa oleva passi tai henkilökortti. Digi- ja väestötietovirastolla tulisi olla erikseen laissa säädetty tiedonsaantioikeus näiden voimassaolotietojen tarkastamiseksi.

69 j §. Digi- ja väestötietoviraston tiedonantovelvollisuus. Pykälän 1 momentissa säädettäisiin tiedoista, jotka Digi- ja väestötietoviraston olisi annettava hakijalle ennen tunnistusvälineen myöntämistä. Tiedot olisi annettava tunnistusvälineen käytöstä (1 kohta); osapuolten oikeuksista ja velvollisuuksista (2 kohta); mahdollisista vastuunrajoituksista (3 kohta); sekä muista mahdollista tunnistusvälineen käyttöehdoista (4 kohta). Yleisesti ottaen ehdotetussa momen-

tissa tarkoitetut tiedot sisältyisivät Digi- ja väestötietoviraston ehtoihin tunnistusvälineen käytöstä. Tiedon antaminen ehdotetussa pykälässä edellyttäisi kuitenkin Digi- ja väestötietovirastolta aktiivisia toimenpiteitä.

Pykälän 2 momentin mukaan tiedot olisi annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voisi tallentaa ja toisintaa ne muuttumattomina.

69 k §. *Digi- ja väestötietoviraston oikeus peruuttaa tai estää tunnistusvälineen käyttö.* Pykälä sisältäisi Digi- ja väestötietoviraston oikeuden puuttua tunnistusvälineen käyttöön. Ehdotettu säännös on perusteltu sen johdosta, että toisen henkilöllisyyden väärinkäytöllä voi olla yksilön kannalta varsin kohtalokkaat seuraukset. Digi- ja väestötietoviraston oikeus peruuttaa väline tai estää sen käyttö on rajattu viiteen tilanteeseen.

Pykälän 1 momentin 1 kohdan mukaan Digi- ja väestötietovirastolla olisi oikeus peruuttaa tai estää tunnistusvälineen käyttö, jos Digi- ja väestötietovirastolla on syytä epäillä, että joku muu kuin se, jolle väline on myönnetty, käyttää sitä. Tällainen tilanne voi johtua siitä, että tunnistusvälineen haltija on luovuttanut välineen toisen käyttöön. Kohdassa tarkoitettu tilanne voi kuitenkin olla mahdollinen myös siten, että tunnistusvälineen haltija ei itse ole tietoinen tilanteesta. Momentin 2 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen olisi mahdollista myös silloin, jos Digi- ja väestötietovirasto havaitsee välineen sisältävän ilmeisen virheellisuuden. Kysymys olisi tällöin Digi- ja väestötietoviraston omasta virheestä, jota ei ole havaittu aikaisemmin. Momentin 3 kohdan mukaan tunnistusväline voidaan peruuttaa tai sen käyttö estää, jos Digi- ja väestötietovirastolla on syytä epäillä, että välineen käytön turvallisuus on vaarantunut. Säännös kattaa sekä tilanteet, joissa turvallisuuden vaarantuminen koskee vain kyseistä tunnistusvälinettä, että tilanteet, joissa tunnistusvälineen käyttö on vaarantunut järjestelmään yleisesti liittyvistä syistä. Momentin 4 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen olisi mahdollista silloin, jos välineen haltija käyttää välinettä olennaisesti käyttöehtojen vastaisella tavalla. On kuitenkin huomattava, että rikkomuksen on oltava olennainen, jotta Digi- ja väestötietovirasto voisi käyttää ehdotetussa pykälässä tarkoitettua oikeuttaan. Momentin 5 kohdan mukaan tunnistusvälineen peruuttaminen tai käytön estäminen olisi mahdollista myös silloin kun välineen haltija on kuollut. Koska tunnistusväline on henkilökohtainen, on paikallaan, että Digi- ja väestötietovirasto voi ryhtyä toimiin estääkseen välineen käytön mahdollisuudet tällaisessa tapauksessa.

Pykälän 2 momentin mukaan Digi- ja väestötietoviraston olisi ilmoitettava välineen peruuttamisesta tai käytön estämisestä ja peruuttamisen tai käytön estämisen ajankohdasta sekä peruuttamiseen tai käytön estämiseen johtaneista syistä välineen haltijalle. Ilmoitus on syytä tehdä niin pian kuin mahdollista. Säännös ei sisältäisi vaatimusta välittömästä ilmoittamisesta. Syynä tähän on se, että toisinaan voi olla parempi ensin pyrkiä korjaamaan esimerkiksi Digi- ja väestötietoviraston tiedossa oleva vaan ei yleisesti tiedossa oleva tietoturva-aukko. Harkinta tiedottamisen ajankohdasta jäisi siis Digi- ja väestötietoviraston tehtäväksi. Joka tapauksessa on selvää, että viranomaisen velvollisuutena on pyrkiä mahdollisten vahinkojen minimoimiseen.

Pykälän 3 momentin mukaan Digi- ja väestötietoviraston olisi palautettava mahdollisuus käyttää välinettä tai annettava välineen haltijalle uusi väline viipymättä 1 momentin 2 ja 3 kohdissa tarkoitetun syyn poistumisen jälkeen. Kohtien 1 ja 4 osalta Digi- ja väestötietovirastolla olisi vapaus omasta puolestaan harkita, voiko välineen haltija vielä jatkaa tunnistusvälineen käyttöä.

69 l §. *Luonnollisen henkilön tunnistusvälineen haltijan velvollisuudet.* Pykälässä säädettäisiin luonnollisen henkilön tunnistusvälineen haltijan velvollisuuksista, jotka velvoittavat tunnistusvälineen haltijaa hänen hyväksymiensä käyttöehtojen perusteella. Lisäksi pykälässä säädettäisiin

siin Digi- ja väestötietoviraston velvollisuudesta tarjota mahdollisuus tehdä milloin tahansa ilmoitus tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä.

Pykälän *1 momentin* mukaan tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sen käyttöehtojen mukaisesti. Ehdotetun momentin mukaan tunnistusvälineen haltijan on myös säilytettävä tunnistusvälinettä huolellisesti. Tunnistusväline käsittää myös tunnistamiseen tarvittavat yksilölliset tiedot, kuten esimerkiksi PIN-koodin tai muun tunnusluvun. Arvioitaessa sitä, millaisia varotoimia tunnistusvälineen haltijalta voidaan kohtuudella edellyttää, on otettava huomioon, että tunnistusvälineet on yleensä tarkoitettu käytettäväksi usein ja että niitä on sen vuoksi voitava kuljettaa mukana. Tunnistusvälineen haltijalta edellytettäviin kohtuullisiin varotoimiin voidaan yleensä katsoa kuuluvan esimerkiksi sen, että hän säilyttää tunnistusvälinettä ja sen käyttöön liittyviä yksilöllisiä tietoja niin, ettei sivullinen voi yhdistää niitä toisiinsa. Tunnistusvälineen haltijalta ei voida kuitenkaan vaatia kohtuuttoman pitkälle meneviä turvajärjestelyjä. Esimerkiksi se, että tunnistusvälineen haltija säilyttää sekä tunnistusvälinettä että tunnuslukua kotonaan, ei vielä sinänsä merkitse sitä, että hän olisi laiminlyönyt huolellisuusveloitteensa.

Pykälän *2 momentissa* säädetään kiellosta luovuttaa tunnistusvälinettä toisen käyttöön. Tunnistusvälineen luovuttamiskielto perustuu siihen, että tunnistusvälineen käytön kannalta olennainen kysymys on nimenomaisesti tiettyyn tunnistusvälineeseen liitettävän henkilön henkilöllisyys. Tämän johdosta on erityisen tärkeää, että tunnistusvälinettä ei saa luovuttaa toisen käyttöön.

Pykälän *3 momentissa* säädettäisiin tunnistusvälineen haltijan velvollisuudesta ilmoittaa Digi- ja väestötietovirastolle ilman aiheutonta viivytystä tunnistusvälineen joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä. Sitä, onko tunnistusvälineen haltija tehnyt ilmoituksen ilman aiheutonta viivytystä, arvioidaan tapauskohtaisesti olosuhteet huomioon ottaen. Ehdotetussa säännöksessä ei säädetä katoamisilmoituksen tekemiselle määrättyä muotoa.

Pykälän *4 momentissa* säädettäisiin Digi- ja väestötietoviraston velvollisuudesta tarjota mahdollisuus tehdä 3 momentissa tarkoitettu ilmoitus milloin tahansa. Digi- ja väestötietoviraston olisi tällöin viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen. Ilmaisulla ”milloin tahansa” tarkoitetaan ehdotetussa momentissa sitä, että tunnistusvälineen haltijan tulee voida tehdä ilmoitus kaikkina vuoden päivinä ja kaikkina vuorokaudenaikoina. Digi- ja väestötietovirasto voisi täyttää velvoitteensa esimerkiksi järjestämällä puhelinpäivystyksen, joka on jatkuvasti auki. Tunnistusvälineen haltijalla tulisi olla tosiasiallisesti aina mahdollisuus ilmoituksen tekemiseen. Tunnistusvälineen haltija ei vastaisi tunnistusvälineen oikeudettomasta käytöstä Digi- ja väestötietovirastolle tehdyn ilmoituksen jälkeen.

69 m §. Muutoksenhaku. Pykälässä säädettäisiin päätöksestä, jonka nojalla henkilö voisi hakea hallintolain nojalla oikaisua asiassaan. Pykälässä säädetyn *1 momentin* nojalla Digi- ja väestötietoviraston päätökseen, joka koskisi 69 e §:ssä tarkoitettuun luonnollisen henkilön tunnistusvälineen myöntämistä ja 69 k §:ssä tarkoitettuun luonnollisen henkilön tunnistusvälineen peruuttamista saisi vaatia oikaisua. Oikaisuvaatimusmenettelystä säädetään hallintolaissa. Pykälän *2 momentin* mukaan muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

7.8 Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:n ja 9 §:n muuttamisesta

3 §. Pykälän *1 momentin 4 kohtaa* ehdotetaan muutettavaksi siten, että kyseisen kohdan mukainen tukipalvelu voisi tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön myös VTJ-lain 6 b luvun mukaista palvelua käyttäen. VTJ-lain 6 b luvussa säädetään Digi- ja väestötietoviraston tuottamasta luonnollisen henkilön tunnistusvälineestä. Lisäksi kohdasta ehdotetaan myös korjattavaksi tunnistus- ja luottamuspalvelulain virheellinen säädöskoelmanumero.

9 §. *Palvelutuotannossa säännönmukaisesti hyödynnettävät tietolähteet.* Pykälää ehdotetaan muutettavaksi siten, että siitä poistettaisiin VTJ-lain säädösnumero. Ehdotetun 3 §:n muutoksen johdosta VTJ-lain säädösnumero tulisi jo kertaalleen mainituksi, joten sitä ei enää myöhemmissä pykälissä olisi tarpeen mainita uudelleen.

8 Lakia alemman asteinen sääntely

Lakiehdotuksessa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista asetetaan Digi- ja väestötietovirastolle uusia määräyksenantovaltuuksia koskien digitaalisen henkilöllisyyden palvelujen tietoturvasuhteita. Digitaalista henkilöllisyydestä olisi mahdollista hyödyntää käyntiasioinnissa erillisen tarkastussovelluksen avulla. Digi- ja väestötietovirasto tuottaisi oman tarkastussovelluksen käyntiasioinnissa hyödynnettäväksi. Lisäksi muut tahot voisivat tuottaa omaa tarkastussovellustaan. Digi- ja väestötietovirasto antaisi tarkemmat määräykset muiden tahojen tuottamille tarkastussovelluksille asetettavista vaatimuksista. Vaatimuksissa olisi edellytettävä vastaavaa tietoturvan tasoa kuin Digi- ja väestötietoviraston omassa lukijarajapinnassa vaaditaan.

Määräyksenantovaltuus pohjautuisi teknisiin vaatimusmäärittelyihin ja olisi luonteeltaan tietoturvasuhteiden mukainen. Ehdotettavan lain nojalla Digi- ja väestötietovirasto päättäisi digitaalisen henkilöllisyyden tietojärjestelmän tarkemmista teknisistä vaatimuksista sekä tietoturvasuhteista. Vaatimusten tulee perustua yleisesti tunnettuihin kansallisiin tai kansainvälisiin standardeihin. Laissa ei olisi tarkoituksenmukaista säätää yksityiskohtaisesti tietoturvasuhteista standardien muuttuessa ja päivittyessä tasaisin väliajoin. Tarkastussovelluksen tarkemmat tekniset tietoturvasuhteet tarkentuvat Digi- ja väestötietoviraston oman toteutuksen myötä. Digi- ja väestötietovirastolle säädettävä määräyksenantovaltuutus olisi perusteltua huomioiden määräyksen tekninen muoto sekä vaatimusten tarkentuminen erityisesti standardien ja yleisten tietoturvasuhteiden päivittymisen myötä. Määräyksenantovaltuudella mahdollistettaisiin vaatimustenmukaisuuden ajantasaisuus ilman säädösmuutostarpeita. Lain tasolla ei olisi tarkoituksenmukaista säädellä toteutettavien teknisten toimintojen yksityiskohtaisista teknisistä ratkaisuista, vaan sääntelyllä olisi pyrittävä teknologianeutraaliin ratkaisuun. Määräyksenantovaltuus mahdollistaisi Digi- ja väestötietovirastolle päivittää vaatimusmäärittelyjä tasaisin väliajoin.

9 Voimaantulo

Lait ehdotetaan tulemaan voimaan 1 päivänä syyskuuta 2023.

10 Toimeenpano ja seuranta

Ehdotettujen lakien voimaantulon jälkeen digitaalisen henkilöllisyyden palveluiden toimivuutta ja käyttöä tulisi seurata. Kansallisesti seurattaisiin myös EU:n lainvalmistelussa olevan

eIDAS-asetuksen muutoksen edistymistä, vaikutettaisiin sen sisältöön ja kehitettäisiin palveluita edelleen sen viitoittamaan suuntaan. Tämä todennäköisesti edellyttäisi myös muutoksia tämän esityksen sisältämiin lakiehdotuksiin tulevien vuosien aikana.

11 Suhde muihin esityksiin

11.1 Esityksen riippuvuus muista esityksistä

Esityksen sisältyvillä ehdotuksilla on yhteys valtiovarainministeriössä valmisteltuun hallituksen esitykseen eduskunnalle laiksi väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta sekä siihen liittyviksi laeiksi ja esitykset on tarkoitukseenmukaista käsitellä yhdessä. Tämän erillisen henkilötunnuksen uudistamista koskevan esityksen tavoitteena on uudistaa henkilötunnusjärjestelmää mahdollistamalla henkilötunnuksen myöntäminen ulkomaalaisille nykyistä laajemmin, mahdollistamalla sähköinen etärekisteröityminen väestötietojärjestelmään, kehittämällä väestötietojärjestelmän identiteettinhallintaa sekä luomalla edellytykset kokonaan uuden yksilöintitunnuksen käyttöönotolle.

Digitaalinen henkilöllisyystodistus ja ulkomaalaisen digitaalinen asiointiväline perustuisivat väestötietojärjestelmästä saatavaan keskitettyyn valtion takaamaan identiteettiin. Koska asiointiväline perustuisi aina väestötietojärjestelmän tietoihin, se olisi mahdollista myöntää ulkomaalaiselle vain, jos hänen tietonsa on ensin rekisteröity väestötietojärjestelmään. Henkilötunnuksen uudistamista koskevassa esityksessä ehdotettu väestötietojärjestelmään rekisteröitävien ulkomaalaisten henkilöpiirin laajentaminen ja etärekisteröintimahdollisuus liittyvät näin kiinteästi tämän ehdotuksen toteuttamiseen.

Digitaaliseen henkilöllisyystodistukseen sekä ulkomaalaisen digitaaliseen asiointivälineeseen liitettävä ydinidentiteetin todiste sisältäisi henkilötunnusjärjestelmän uudistamista koskevaan esitykseen sisältyvän uuden yksilöivän tunnuksen. Ydinidentiteetin todiste olisi julkinen ja saatavilla julkisesta varmennehakemistosta käytön aikana sekä sulkulistalta, kun sen käyttö loppuu. Julkisenä tunnisteena ei voitaisi tämän ehdotuksen mukaan käyttää henkilötunnusta. Henkilötunnuksen uudistamista koskevassa esityksessä säädettäisiin yksilöintitunnuksesta, tunnuksen antamisesta sekä sen hyödyntämisestä.

Hallituksen esitykseen eduskunnalle laiksi väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta sekä siihen liittyviksi laeiksi sisältyy sääntelyehdotuksia, joihin viitataan tähän esitykseen sisältyvässä lakiehdotuksessa 1 seuraavasti: 11 §:n 1 kohta, 15 §:n 1 momentti ja 17 §:n 1 momentti.

Oikeusministeriössä on parhaillaan valmisteilla hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi. Esitys sisältää ehdotuksen uudeksi yleissääntelyksi automaation käyttämisestä hallintoasian käsittelyssä, erityisesti hallintopäätösten teossa ja niiden valmistelussa. Sääntelyn on tarkoitus sisältää tarpeelliset säännökset automaation sallitusta käyttöalasta, tietojärjestelmiin kohdistuvista vaatimuksista, tietojärjestelmien hyväksynnästä ja valvonnasta, läpinäkyvyyden ja asiakirjajulkisuuden toteutumisesta sekä muut hyvän hallinnon, oikeusturvan ja muiden perusoikeuksien varmistamiseksi tarpeelliset säännökset.

Esityksessä ehdotettu ulkomaalaisen digitaalisen asiointivälineen myöntämistä koskeva etärekisteröintimenettely on tarkoitus toteuttaa ensisijaisesti automatisoituna ilman virkailijakäsittelyä. Asiointivälineen myöntämistä koskevassa menettelyssä ja sen olisi tarkoitus noudattaa mitä

oikeusministeriössä valmisteltavassa automaattista päätöksentekoa koskevassa hallinnon yleissääntelyssä tullaan säätämään. Tähän esitykseen sisältyvillä lakiehdotuksilla ei kuitenkaan ole varsinaista yhteyttä kyseisessä hallituksen esityksessä esitettävään sääntelyyn.

11.2 Suhde talousarvioesitykseen

Esitys liittyy esitykseen valtion vuoden 2023 talousarvioksi ja on tarkoitettu käsiteltäväksi sen yhteydessä.

12 Suhde perustuslakiin ja säätämisjärjestys

12.1 Tehtävien siirtäminen viranomaisten välillä

Esityksen mukaan laissa erikseen määriteltyjä, Digi- ja väestötietoviraston rekisterinpitoon liittyviä tehtäviä voitaisiin tuottaa viranomaisten yhteistyönä yhteispalvelulain mukaisessa yhteispalvelussa. Perustuslakivaliokunta on useissa eri lausunnoissaan ottanut kantaa säännösehdoituksiin, jotka koskevat tehtävien siirtämistä viranomaisten välillä. Valiokunta on suhtautunut pidättyvästi sääntelyyn, joka mahdollistaa tehtävien rajoituksettoman siirron toiselle viranomaiselle. Valiokunta on etenkin perusoikeuskysymysten sääntelyn yhteydessä pitänyt välttämättömänä, että toimivaltainen viranomainen ilmenee laista yksiselitteisesti tai muuten täsmällisesti tai että ainakin viranomaisten toimivaltasuhteiden lähtökohdat sekä toimivallan siirtämisen edellytykset ilmenevät laista riittävän täsmällisesti (esimerkiksi PeVL 7/2001 vp, PeVL 21/2001 vp, PeVL 45/2001 vp, PeVL 47/2001 vp, PeVL 52/2001 vp, PeVL 17/2004 vp, PeVL 18/2004 vp, PeVL 24/2006 vp, PeVL 51/2006 vp, PeVL 19/2009 vp ja PeVL 21/2009 vp). Lisäksi valiokunta on tehtävien siirtämistä koskevan sääntelyn yhteydessä kiinnittänyt huomiota henkilörekisterinpitovastuusta säätämisen selkeyteen ja lainmukaisuuteen (esimerkiksi PeVL 19/2009 vp).

Perustuslakivaliokunta on suhtautunut pidättyvästi sääntelyihin, jotka mahdollistavat julkista valtaa sisältävän toimivallan siirtämisen sopimusperusteisesti. Perustuslakivaliokunnan lausunnossa (PeVL 11/2004 vp) todetaan, että viranomaiselle kuuluvan hallintotehtävän siirtäminen sopimuksella toiselle viranomaiselle ei ole ongelmatonta. Asian kannalta merkityksellisiä säännöksiä ovat perustuslain 21 §, jonka mukaan jokaisella on oikeus saada asiansa käsiteltyksi lain mukaan toimivaltaisessa viranomaisessa sekä perustuslain 2 §:n 3 momentti, jonka mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia (PeVL 14/2003 vp, PeVL 52/2001 vp, PeVL 11/2002 vp ja PeVL 72/2002 vp).

Esityksen mukaan yhteispalvelussa hoidettavat rekisteröintiin liittyvät tehtävät määriteltäisiin laissa. Tehtävät olisivat yhteispalvelulain mukaisia, ulkomaalaisen digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen haltijaa koskevien henkilötietojen rekisteröintiin liittyvä rekisteröinti- ja neuvontatehtäviä. Nämä tehtävät eivät merkittävästi poikkea yhteispalvelulaissa siirrettäväksi mahdollistetuista tehtävistä. Yhteispalvelulain mukainen toimeksisaaja hoitaisi laissa erikseen määriteltyjä rekisteröintitehtäviä laissa säädettyjen edellytysten ja yhteispalvelusopimuksessa tarkemmin sovitun sekä Digi- ja väestötietoviraston antamien ohjeiden mukaisesti.

Toimeksisaajan palveluneuvojan tehtävänä esimerkiksi ulkomaalaisen digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen osalta olisivat asiointivälineen aktivointiin liittyviä tehtäviä. Nämä tehtävät ovat viranomaiselle kuuluvia hallintotehtäviä, mutta ne ovat luonteeltaan toimeksiantajana toimivaa Digi- ja väestötietovirastoa avustavia. Toimeksiantajana toimivan Digi- ja väestötietoviraston tehtävänä olisi lisäksi antaa toimeksisaajan henkilöstölle tehtävän edellyttämä ohjeistus ja koulutus. Tehtäviin ei sisältyisi julkisen vallan käyttöä, koska

Digi- ja väestötietovirastolla säilyisi edelleen rekisterinpitovastuu sekä rekisteröintiin liittyvä päätösvalta tilanteissa, joissa hallinnon asiakkaalle tulisi antaa päätös. Mikäli yhteispalvelun toimeksisaaja ei pystyisi esimerkiksi puuttuvien selvitysten takia lisäselvitysten jälkeenkään aktivoimaan ulkomaalaisen digitaalista asiointivälinettä tai luonnollisen henkilön tunnistusvälinettä, tulisi sen siirtää asia Digi- ja väestötietoviraston käsiteltäväksi. Digi- ja väestötietoviraston olisi tarvittaessa annettava päätös rekisteröinnistä tai tunnistusvälineen myöntämisestä kieltäytymisestä.

Esitettyjen avustavien tehtävien mahdollistaminen hoidettavaksi yhteispalvelussa on tarkoituksenmukaista. Ulkomaalaisen digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen hakijan tunnistaminen lain ja yhteispalvelusopimuksen perusteella muissakin viranomaisissa mahdollistaa sähköisessä ympäristössä tarjottavien palvelujen hyödyntämisen nykyistä laajemmalle käyttäjäpiirille sekä joustavoittaa ulkomaan kansalaisten sähköisen asioinnin käyttöönottoa viranomaisprosessien yhteydessä.

12.2 Yksityisyyden suoja ja henkilötietojen suoja

Johdanto ja kansallinen liikkumavara

Esitykseen sisältyisi henkilötietojen käsittelyä koskevaa erityislainsäädäntöä. Lakiehdotuksia on näin ollen arvioitava perustuslain 10 §:ssä tarkoitetun yksityiselämän suojan kannalta. Perustuslain 10 §:n mukaan jokaisella on oikeus yksityiselämän suojaan. Pykälän 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Lisäksi henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan käytännön mukaan lainsäätäjän liikkumalaa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvattun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa (ks. esim. PeVL 42/2016 vp, s. 2 ja PeVL 12/2016, s. 3).

Ehdotettu sääntely on merkityksellistä myös EU:n perusoikeuskirjan kannalta. EU:n perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan. Lisäksi Euroopan ihmisoikeussopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Artiklan on Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä katsottu kattavan myös henkilötietojen suojan (PeVL 28/2016 vp, s. 5).

Perustuslakivaliokunta on yleisen tietosuojasetuksen soveltamisalalla tarkistanut kantaansa henkilötietojen suojasta lailla säätämisen vaatimuksen osalta. Tietosuojasetuksen sääntely henkilötietojen suojasta on olennaisesti yksityiskohtaisempaa kuin kumotun henkilötietodirektiivin (95/46/EY) ja sen toimeenpanemiseksi annetun henkilötietolain sääntely. Perustuslakivaliokunta on pitänyt merkityksellisenä myös, että EU:n perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan. Valiokunta on painottanut, että EU:n henkilötietojen käsittelyä koskevaa lainsäädäntöä sovellettaessa on otettava huomioon mainitut perusoikeuskirjan artikkelit kiinnittäen huomiota siihen, että EU:n tuomioistuimen antamat tuomiot määrittävät näiltä osin yksityiselämän ja henkilötietojen suojan keskeistä sisältöä (PeVL 14/2018, s. 3).

Perustuslakivaliokunta on vakiintuneesti pitänyt henkilötietojen suojan kannalta tärkeänä sääntelykohteena rekisteröinnin tavoitetta. Lisäksi perustuslakivaliokunta on vakiintuneesti pitänyt henkilötietojen suojan kannalta tärkeänä sääntelykohteena ainakin rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia, mukaan luettuna tietojen luovutettavuus, sekä

tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa (ks. esim. PeVL 42/2016 vp, s. 2 ja PeVL 12/2016, s. 3). Lailla säätämisen vaatimus ulottuu myös mahdollisuuteen luovuttaa henkilötietoja teknisen käyttöyhteyden avulla. Lailla on säädettävä lisäksi mahdollisuudesta yhdistää rekisteritietoja (PeVL 17/2007 vp, s. 3 ja PeVL 30/2005 vp, s. 4). Henkilötietojen käsittelyä koskevan sääntelyn lain tasolla tulee lisäksi olla kattavaa ja yksityiskohtaista (ks. esim. PeVL 46/2016 vp, s. 5—6 ja siinä viitattut lausunnot).

Perustuslakivaliokunta on kiinnittänyt huomiota henkilötietojen käsittelyä koskevan sääntelyn raskauteen ja monimutkaisuuteen (ks. esim. PeVL 2/2018 vp, s. 4—8, 11, PeVL 49/2017 vp, s. 3, PeVL 31/2017 vp, s. 4 ja PeVL 71/2014 vp, s. 3). Valiokunta on katsonut, että henkilötietojen suojan toteuttaminen ei voi enää jatkossa perustua nykyisenkaltaisen sääntelymallin varaan. Henkilötietojen suojan toteuttaminen tulisi valiokunnan mukaan jatkossa ensisijaisesti taata yleisen tietosuoja-asetuksen ja säädettävän kansallisen yleislain nojalla. Tähän liittyen tulisi välttää kansallisen erityislainsäädännön säätämistä sekä varata sellaisen säätäminen vain tilanteisiin, joissa se on yhtäältä sallittua tietosuoja-asetuksen kannalta ja toisaalta välttämätöntä henkilötietojen suojan toteuttamiseksi (PeVL 2/2018 vp, s. 5).

Esityksessä ehdotettu henkilötietojen käsittelyä koskeva sääntely perustuisi yleisen tietosuoja-asetuksen 6 artiklan mukaiseen kansalliseen liikkumavaraan. Mainitun 6 artiklan 3 kohdassa tarkoitetun jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden. Mikäli tietoja käsitellään muuhun kuin niiden alkuperäiseen keräämistarkoitukseen, on sääntelyä arvioitava käyttötarkoitussidonnaisuuden periaatetta vasten siten kuten tietosuoja-asetuksen 6 artiklan 4 kohdassa säädetään. Sääntelyn on oltava välttämätön ja oikeasuhtainen toimenpide yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi. Sääntelyn on myös oltava oikeasuhtaista tavoitteeseen nähden, siinä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

Perustuslakivaliokunnan lausunnon (PeVL 14/2018 vp) mukaan erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä korkeampi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta. Perustuslakivaliokunta on lisäksi sekä ennen tietosuoja-asetuksen voimaantuloa että sen jälkeen vakiintuneesti painottanut arkaluonteisten henkilötietojen käsittelyyn liittyviä uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I).

Perustuslakivaliokunta on pitänyt henkilötietojen käsittelyä koskevassa valtiosääntöisessä arvioissa merkityksellisenä myös käsittelyn tarkoitusta yksilöön kohdistuvan julkisen vallan käytön mahdollistajana (PeVL 14/2018 vp, s. 6 ja PeVL 1/2018 vp, s. 6). Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin. Lailla säätämiseen taas kohdistuu yleinen vaatimus lain täsmällisyydestä ja tarkkuudesta. Toimivaltasääntely on valiokunnan käsityksen mukaan yleensä merkityksellistä myös perustuslaissa turvattujen perusoikeuksien näkökulmasta (PeVL 51/2006 vp, s. 2/I).

Esityksessä on otettu huomioon tietosuoja-asetuksen mukainen kansallinen liikkumavara rekistereiden tietosisällöstä ja rekisterinpitäjyydestä säätelemisen osalta: 1. lakiehdotuksessa sääde-

tään kansallisen liikkumavaran puitteissa Digi- ja väestötietoviraston rekisterinpitäjyydestä digitaalisen henkilöllisyyden palvelujen tuottamisessa sekä ydinidentiteetin todisteen ja ulkomaalaisen digitaalisen asiointivälineen tarjoamisessa. Vastaavasti 2. lakiehdotuksessa on säädetty poliisin rekisterinpitäjyydestä digitaalisista henkilöllisyystodistuksista muodostuvan rekisterin osalta. Lisäksi edellä mainittujen rekisterien henkilötietojen käsittelyn oikeusperusteet on tunnistettu tietosuoja-asetuksen edellyttämällä tavalla. Tietosuoja-asetuksen yleisluontoista sääntelyä yksityiskohtaisempia sääntely kyseisistä rekistereistä ja niiden rekisterinpitäjistä on tarpeellista ottaen huomioon lakiehdotusten mukaisten rekisterien keskeinen asema suomalaisten identiteettitietojen käsittelyssä ja kansallisten digitaalisten henkilöllisyyttä osoittavien asiakirjojen tuottamisessa. Erityissääntely digitaalisen henkilöllisyyden palveluja ja digitaalista henkilöllisyystodistusta koskevista rekistereistä on lisäksi perusteltua tietosuoja-asetuksen riskiperusteisen lähestymistavan näkökulmasta, sillä kansalaisten identiteettitietoihin uudenaikaiseen digitaaliseen käsittelyyn liittyy tavanomaista korkeampia riskejä muun muassa tietoturvallisuuden näkökulmasta. Tästä näkökulmasta on perusteltavissa, että nyt ehdotettava erityissääntely on välttämätöntä henkilötietojen suojan toteuttamiseksi.

Edellä mainituilla perusteilla esityksen sisältämien lakiehdotusten katsotaan olevan henkilötietojen käsittelyä koskevilta osin tarpeellisia sekä tietosuoja-asetuksen että perustuslain näkökulmasta.

Käsitteltävät henkilötiedot ja niiden turvallisuus

Perustuslakivaliokunta on kiinnittänyt erityistä huomiota sääntelytarpeeseen silloin, kun henkilötietoja käsittelee viranomainen (PeVL 15/2018 vp). Tietosuoja-asetuksen 6 artiklan c alakohdan mukaan käsittely on lainmukaista, jos käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Artiklan e alakohdan mukaan käsittely on lainmukaista, jos se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi (ks. PeVL 14/2018 vp, s. 4).

Perustuslakivaliokunta on kiinnittänyt erityistä huomiota siihen, että yksityiselämän suojaan kohdistuvia rajoituksia on arvioitava kulloisessakin sääntely-yhteydessä perusoikeuksien yleisten rajoitusedellytysten valossa (PeVL 42/2016 vp, s. 2-3). Lainsäätäjän liikkumavaraa rajoittaa henkilötietojen käsittelystä säädettäessä erityisesti se, että henkilötietojen suoja osittain sisältyy perustuslain 10 §:n samassa momentissa turvattu yksityiselämän suojan piiriin. Lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa.

Lakiehdotuksissa säädettäisiin uusista digitaalisen henkilöllisyyden palvelujen sekä digitaalisen henkilöllisyystodistuksen tuottamiseen liittyvistä rekistereistä. Näissä rekistereissä tulisiin pääosin käsittelemään jo olemassa olevissa viranomaisten rekistereissä olevia henkilötietoja, kuten väestötietojärjestelmään henkilöistä tallennettuja tietoja sekä henkilökorttilain 31 §:n mukaiseen henkilökorttirekisteriin sekä passilain 29 §:n mukaiseen passirekisteriin talletettuja rekisteritietoja. Siten käsiteltäviä henkilötietoja olisivat muun muassa VTJ-lain 13 §:n 1 momentissa luetellut tiedot, kuten henkilön täydellinen nimi, henkilötunnus sekä tekninen tunnistetieto ja sähköinen asiointitunnus, sekä valmistelussa olevan VTJ-lain 11 a §:n mukainen henkilön yksilöintitunnus. Muita käsiteltäviä henkilötietoja olisivat muun muassa henkilökortti- ja passi- rekisteriin talletetut henkilötietojen käsittelystä poliisitoimessa annetun lain 4 §:ssä tarkoitetut tarpeelliset henkilön perustiedot, kuten henkilön nimet, syntymäaika ja -paikka ja sukupuoli sekä henkilön valokuva, jonka hän on luovuttanut henkilökortti- tai passiviranomaiselle henkilökorttia tai passia hakiessaan.

Uusia henkilötietoja olisivat Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa säädettäväksi ehdotetun ydinidentiteetin todisteen sekä siihen liittyvien rekisterien tiedot. Nämä tiedot vastaisivat kuitenkin ensi vaiheessa pääosin VTJ-lain 6 luvussa säädettyjen Digi- ja väestötietoviraston varmennepalvelujen yhteydessä talletettavia tietoja. Täysin uusia tietoja sisältyisi kuitenkin 1. lakiehdotukseen sisältyvän 13 §:n 2 momentin mukaiseen laiterekisteriin, jonne tallennettaisiin henkilön yksilöivä tunnistetieto, henkilöön liitetyn teknisen alustan tekniset tiedot, laitetiedot sekä muut ydinidentiteetin todisteen tuottamiseksi välttämättömät tiedot. Tietoja luonnollisten henkilöiden mobiilipäätelaitteista ja niiden tiedoista ei ole aiemmin kerätty henkilökortin tai passin myöntämiseksi. Nämä tiedot ovat kuitenkin välttämättömiä ydinidentiteetin todisteen tuottamiseksi, joten niiden käsittely on välttämätöntä digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen tarjoamiseksi. Tietojen keräämisen välttämättömyyden kannalta merkitystä on myös sillä, että digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen käyttöönotto on vapaaehtoista, joten kaikilta kansalaisilta ja Suomessa oleskelevilta ei tulisi keräämään heidän mobiilipäätelaitteitaan koskevia teknisiä tietoja. Nämä tiedot kerättäisiin siis ainoastaan henkilöiltä, jotka haluaisivat ottaa käyttöön digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen.

Esityksessä on huomioitu tietosuoja-asetuksessa biometristen tietojen ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelylle asetetut edellytykset. Tietosuoja-asetuksen 4 artiklan 14 kohdan mukaan biometrisillä tiedoilla tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa. Tietosuoja-asetuksen 9 artiklan mukaan erityisiä henkilötietoryhmiä koskevaan käsittelyyn kuuluu muun muassa biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten. Tietosuoja-asetuksen 51 johdantokappaleessa kuitenkin nimenomaisesti todetaan, että valokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometristen tietojen määritelmään ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen. Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja ei pitäisi käsitellä, ellei käsittelyä sallita tietosuoja-asetuksessa vahvistetuissa erityistapauksissa tai esimerkiksi lakisääteisen velvoitteen noudattamista varten. Tällaista käsittelyä koskevien erityisvaatimusten lisäksi olisi sovellettava tietosuoja-asetuksen yleisiä periaatteita ja muita sääntöjä erityisesti lainmukaisen tietojenkäsittelyn osalta.

Digitaalisessa henkilöllisyystodistuksessa käyttäjän kasvokuva luovutetaan digitaalisessa muodossa hänen itsensä käytettäväksi mobiililaitteessa. Kuvaa käytetään käyttäjän tunnistamiseen käyntiasioinnin yhteydessä. Käyttäjän tunnistaminen tapahtuu tunnistajan silmämääräisen arvon perusteella vastaavalla tavalla kuin perinteisten virallisten henkilöllisyyttä osoittavien asiakirjojen kuten passin ja henkilökortin osalta. Digitaalisen henkilöllisyystodistuksen tarkastussovellus ei sisällä mitään erityisiä teknisiä menetelmiä, joita tunnistamisessa käytettäisiin, vaan se perustuu aina luonnollisen henkilön aistinvaraisesti tekemien havaintojen pohjalta tekemään punnintaan. Digitaalinen henkilöllisyystodistus ei itsessään mahdollista erityisten teknisten menetelmien käyttöä. Digitaalista henkilöllisyystodistusta koskevassa ehdotuksessa valokuvien käsittelyssä ei siten katsota olevan kyse tietosuoja-asetuksen 9 artiklassa tarkoitettusta biometristen tietojen käsittelystä henkilön yksiselitteistä tunnistamista varten.

Edellä mainitusta huolimatta henkilökortti- ja passirekisteriin talletetut henkilöiden valokuvat ovat salassa pidettäviä tietoja, jolloin näiden tietojen käsittelyssä tulisi noudattaa erityistä varovaisuutta. Tietojen käsittely tietojärjestelmissä edellyttää, että kaikki osapuolet voivat luottaa

siihen, että käytettävät teknisesti monimutkaiset tietojärjestelmäkokonaisuudet ovat periaatteiltaan, teknisiltä ratkaisuiltaan ja toteutukseltaan lainsäädännön mukaisia ja täyttävät kaikki tietoturvallisuuden vaatimukset. Lisäksi järjestelmien käyttäjien näkökulmasta on tarpeen, että tietojärjestelmäkokonaisuudet ovat keskenään yhteentoimivia ja täyttävät käytännön toiminnallisuudelle asetettavat vaatimukset.

Perustuslakivaliokunta on lisäksi korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettämistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mukaan ollut syytä suhtautua kielteisesti esimerkiksi laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä (PeVL 14/2009 vp, s. 4/II). Käyttötarkoitussidonnaisuudesta on voitu tällöin tehdä vain täsmällisiä ja vähäisiä luonnehdittavia poikkeuksia. Sääntely ei ole saanut johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi (ks. myös esim. PeVL 14/2017 vp, s. 5–6). Perustuslakivaliokunnan myötävaikutuksella säädettyyn henkilötietojen käytöstä poliisitoimissa annettuun lakiin sisältyy säännökset henkilökorttirekisterin ja passirekisterin tietojen käsittelystä muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen. Mainitun lain 13 §:n 3 momentin mukaan henkilön valokuvaa ja nimikirjoitusnäytettä saadaan asianomaisen henkilön suostumuksella käyttää muunkin hänen hakemansa hallintoluvan tai päätöksen valmistamiseen kuin sen asiakirjan valmistamiseen, johon henkilön valokuva ja nimikirjoitusnäyte on luovutettu.

Valiokunta on painottanut erityisesti, että esimerkiksi potilastietorekisterin kaltaisen arkaluonteisia tietoja sisältävän hajautetun rekisterin ollessa kyseessä on erityisen tärkeää varmistua siitä, että väärinkäytön estävät tietoturvajärjestelyt ovat toimivia ja käytettävissä heti, kun järjestelmä otetaan käyttöön (PeVL 41/2010 vp, s. 3/II). Siitä huolimatta, että passi- ja henkilökorttihakemustietoihin sisältyvät kasvokuvat eivät ole sellaisenaan biometrisiä tietoja, tulisi niiden käsittelystä noudattaa erityistä varovaisuutta niiden erityisen luonteen vuoksi.

Edellä mainitusta johtuen digitaalisen henkilöllisyystodistuksen käyttöönotossa tulisi erityisesti kiinnittää huomiota siihen, että tietoturvajärjestelyt ovat käytössä heti digitaalisen henkilöllisyyden tietojärjestelmän käytön alkaessa. Digitaalisen henkilöllisyyden palvelujen ja etenkin digitaalisen henkilöllisyyden tietojärjestelmän voidaan katsoa riskitasoltaan rinnastuvan arkaluonteisia tietoja sisältäviin potilastietojärjestelmiin, joten samaa vaatimusta tietoturvajärjestelyjen toimivuudesta ja käytettävyydestä heti palveluiden ja tietojärjestelmän käyttöönotossa voidaan pitää perusteltuina.

Esityksessä on yksilöity viranomaisten käsittelemät henkilötiedot ja siinä on erikseen säädetty tietoturvaluusvaatimuksista tietosuoja-asetuksen sekä tiedonhallintalain vaatimuksia yksityiskohtaisemmalla tasolla. Esityksen 1. lakiehdotuksen 5 §:ssä säädetään digitaalisen henkilöllisyyden tietojärjestelmän laatu- ja tietoturvaluusvaatimuksista seikkaperäisesti, jonka lisäksi 9 §:ssä säädetään Digi- ja väestötietoviraston velvollisuudesta ilmoittaa digitaalisen henkilöllisyyden palvelujen käyttäjille erilaisista palvelujen turvallisuuteen liittyvistä uhkista ja häiriöistä. Lisäksi 1. lakiehdotuksen 10 §:ssä säädetään erillisestä tietojärjestelmästä säännöllisin väliajoin tehtävästä tietojärjestelmän vaatimustenmukaisuuden arvioinnista, joka on tehtävä ennen tietojärjestelmän käyttöönottoa. Säädettyjen teknisten ja organisatoristen toimenpiteiden tarkoituksena on estää väärinkäytökset sekä lainvastainen pääsy digitaalisen henkilöllisyyden tietojärjestelmässä käsiteltäviin henkilötietoihin. Erityisiä toimenpiteitä ovat muun muassa pääsyhallinta- ja käyttöoikeushallintavaatimukset sekä erityiset vaatimukset edistyneiden tietoturva-uhkien kestämisestä ja merkittävien tietoturvaloukkausten ja -uhkien havaitsemisesta. Lisäksi erillinen vaatimus tietoturvaluuden arvioimisesta tietoturvaluuden arviointilaitoksen

toteuttamalla arvioinnilla toimisi tietosuoja-asetuksen 25 artiklan mukaisena ylimääräisenä suojatoimenä. Näin ollen esityksessä on huomioitu käsiteltävät henkilötiedot ja niiden suojaaminen tietosuoja-asetuksen ja perustuslakivaliokunnan edellyttämällä tavalla.

Tiedonsaantioikeudet

Perustuslakivaliokunta on arvioinut viranomaisten tietojen saamista ja luovuttamista salassapitovelvollisuuden estämättä koskevaa sääntelyä perustuslain 10 §:n 1 momentissa säädetyn yksityiselämän ja henkilötietojen suojan kannalta ja kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen (PeVL 15/2018 vp). Viranomaisen tietojensaantioikeus ja tietojen luovuttamismahdollisuus ovat voineet liittyä jonkin tarkoituksen kannalta "tarpeellisiin tietoihin", jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisällöt ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus "tietojen välttämättömyydestä" jonkin tarkoituksen kannalta (ks. esim. PeVL 17/2016 vp, s. 2-3). Valiokunta ei toisaalta ole pitänyt hyvin väljiä ja yksilöimättömiä tietojensaantioikeuksia perustuslain kannalta mahdollisina edes silloin, kun ne on sidottu välttämättömyyskriteeriin (PeVL 59/2010 vp, s. 4).

Perustuslakivaliokunta on painottanut, että erottelussa tietojen saamisen tai luovuttamisen tarpeellisuuden ja välttämättömyyden välillä on kyse tietosisältöjen laajuuden ohella myös siitä, että salassapitosäännösten edelle menevässä tietojensaantioikeudessa on viime kädessä kysymys siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tiedot omaavaan viranomaiseen kohdistuvan salassapidon avulla suojataan (PeVL 15/2018 vp). Mitä yleisluonteisempi tietojensaantiin oikeuttava sääntely on, sitä suurempi on vaara, että tällaiset intressit voivat syrjäytyä hyvin automaattisesti. Mitä täydellisemmin tietojensaantioikeus kytketään säännöksissä asiallisiin edellytyksiin, sitä todennäköisemmin yksittäistä tietojensaantipyyntöä joudutaan käytännössä perustelemaan. Myös tietojen luovuttajan on tällöin mahdollista arvioida pyyntöä luovuttamisen laillisten edellytysten kannalta. Tietojen luovuttaja voi lisäksi kieltäytymällä tosiasiallisesti tietojen antamisesta saada aikaan tilanteen, jossa tietojen luovuttamisvelvollisuus eli säännösten tulkinta saattaa tulla ulkopuolisen viranomaisen tutkittavaksi. Tämä mahdollisuus on tärkeä tiedonsaannin ja salassapitointressin yhteensovittamiseksi (PeVL 17/2016 vp, s. 6).

Esityksessä on huomioitu tiedonsaantioikeuksia koskeva perustuslakivaliokunnan lausuntokäytäntö. Viranomaisten tiedonsaantioikeuksista on esityksessä säädetty laissa henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta, jonka 16 §:ää muutettaisiin siten, että poliisilla olisi oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä tiedot Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain mukaisesti digitaalisen henkilöllisyydestodistuksen tuottamiseksi välttämättömistä tiedoista. Vastaavasti saman lain 22 §:ää muutettaisiin siten, että poliisilla olisi oikeus salassapitosäännösten estämättä luovuttaa 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi Digi- ja väestötietovirastolle Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa tarkoitettujen digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin todisteen tuottamista ja hallinnoimista varten. Näin ollen poliisin tiedonsaantioikeus kohdistuu ainoastaan digitaalisen henkilöllisyydestodistuksen tuottamisen kannalta välttämättömiin tietoihin ja Digi- ja väestötietoviraston tiedonsaantioikeus taas etukäteen määriteltyyn ja rajattuun tietojoukkoon, joita Digi- ja väestötietovirasto voisi käsitellä ainoastaan lainsäädännössä määriteltyihin käyttötarkoituksiin. Ehdotetun sääntelyn katsotaan tältä osin olevan yhdenmukaista perustuslakivaliokunnan tiedonsaantioikeuksia koskevan lausuntokäytännön kanssa.

Tiedollinen itsemääräämisoikeus ja itsehallittava identiteetti

Perustuslakivaliokunta on pitänyt tiedollista itsemääräämisoikeutta henkilötietojen suojan kannalta keskeisenä oikeutena (ks. esim. PeVL 23/2020 vp, s. 9, PeVL 2/2018 vp, s. 8). Valiokunnan käytännössä itsemääräämisoikeuden on katsottu kiinnittyvän useisiin perusoikeuksiin, erityisesti perustuslain 7 §:n säännöksiin henkilökohtaisesta vapaudesta ja koskemattomuudesta sekä perustuslain 10 §:n säännöksiin yksityiselämän suojasta (ks. PeVL 48/2014 vp, s. 2/II).

Ehdotetuissa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa ja digitaalisesta henkilöllisyystodistuksesta annetussa laissa digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen henkilön vahvistetut tiedot toimitettaisiin henkilölle hänen itsensä hallittavaksi. Ulkomaalaisen digitaalisen asiointivälineen osalta tiedot on lueteltu tyhjentävästi 1. lakiehdotuksen 16 §:ssä ja digitaalisen henkilöllisyystodistuksen osalta 2. lakiehdotuksen 4 §:ssä. Henkilön itsensä hallittavaksi toimitettavat tiedot olisivat ulkomaalaisen digitaalisen asiointivälineen osalta peräisin Digi- ja väestötietoviraston ja Ahvenanmaan valtioviraston VTJ-lain 4 §:n nojalla ylläpitämästä väestötietojärjestelmästä ja digitaalisen henkilöllisyystodistuksen osalta peräisin poliisin passilain 29 §:n tai henkilökorttilain 31 §:n nojalla ylläpitämästä passi- tai henkilökorttirekisteristä.

Henkilön omien tietojen toimittamista digitaalisessa ympäristössä henkilön itsensä hallittavaksi kutsutaan yleisesti itsehallittavaksi identiteetiksi. Itsehallittavalla identiteetillä (engl. Self-Sovereign Identity, SSI) tarkoitetaan henkilötietojen käsittelyn mallia, jossa henkilö voi itse hallinnoida joko itseltään tai luotettavalta kolmannelta taholta lähtöisin olevien henkilötietojensa osoittamista asiointipalvelulle, jossa henkilötietoja tarvitaan. Käytännössä itsehallittavuudella tarkoitetaan siis sitä, että henkilöt hallitsevat itse omia henkilötietojaan.

Esityksessä tietojen toimittamisella henkilön itsensä haltuun tarkoitetaan tietosuoja- ja informaatio-oikeudellisesta näkökulmasta sitä, että viranomainen toimittaa vahvistetut tiedot, jotka ovat sekä tietosuoja-asetuksen 4(1) artiklan mukaisia henkilötietoja että julkisuuslain 5 §:n 2 momentin mukaisia viranomaisen asiakirjoja, henkilön itsensä haltuun. Tämän seurauksena henkilölle toimitetut tiedot eivät olisi enää viranomaisen asiakirjoja, eivätkä enää viranomaisen rekisterinpitäjyyden piirissä. Henkilön itsensä suorittamaan omien tietojensa käsittelyyn ei enää sovellettaisi tietosuojaa ja tiedonhallintaa koskevaa lainsäädäntöä. Henkilöllä olisi oikeus osoittaa omia tietojaan vapaasti haluamilleen rekisterinpitäjille ja näiden tahojen suorittamaan henkilötietojen käsittelyyn sovellettaisiin jälleen täysimääräisesti tietosuoja-asetusta ja viranomais-toimijoiden tapauksessa tiedonhallintaa koskevaa lainsäädäntöä.

Vahvistettujen tietojen toimittaminen henkilön itsensä hallittavaksi vastaisi analogisesti tilannetta, jossa henkilö hakisi viranomaisen luota itseään koskevan fyysisen asiakirjan tai viranomaisen postittaisi asiakirjan henkilön kotiosoitteeseen. Kyse olisi näin ollen olemassa olevan toimintatavan siirtämistä digitaaliseen käsittely-ympäristöön. Vastaavaa toimintamallia ei ole kuitenkaan sähköisessä käsittely-ympäristössä aiemmin toteutettu, joten sen perustuslaillinen arviointi on tarpeen.

Lakiehdotuksissa ei kuitenkaan erikseen käytettäisi käsitettä ”itsehallittava identiteetti”. Tämä johtuu muun muassa siitä, että perustuslakivaliokunta on katsonut, että perusoikeusherkän ja EU-oikeuteen kytkeytyvän sääntelyn alueella tulisi suhtautua pidättyvästi siihen, että vakiintuneet ja voimassaolevaan oikeuteen perustuvat käsitteet korvataan lainsäädännössä selvästi epätasällisemmilla ja tulkinnallisilla epäselvyyksiin herkästi johtavilla uuskäsitteillä (PeVL

2/2018 vp, s. 8). Lausunnossa perustuslakivaliokunta otti kantaa käsitteeseen ”omadata” ja totesi kyseisen käsitteen suhteen perustuslain turvaamaan henkilötietojen suojaan olevan epäselvä.

Henkilötietojen toimittaminen digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen itsensä hallittavaksi ei kuitenkaan tarkoittaisi sitä, että viranomaiset, joiden rekistereistä vahvistetut tiedot toimitetaan, eivät enää vastaisi alkuperäisistä rekisteritiedoista. Kyse olisi pikemminkin otteen luovuttamisesta näistä rekisteritiedoista, joiden käsittelystä viranomaiset edelleen vastaisivat sekä viranomais- että rekisterinpitäjäroolissa. Vastavasti ne luottavat osapuolet, joille digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen haltijat osoittaisivat vahvistettuja tietojaan, vastaisivat näiden käsittelystä voimassa olevan tietosuojaja- ja muun lainsäädännön mukaisesti. Näin ollen yksityisen sektorin toimijoiden suorittamaan henkilötietojen käsittelyyn sovellettaisiin tavanomaisesti tietosuojasetusta ja julkisen sektorin toimijoihin tietosuojasetusta sekä muuta viranomaisia velvoittavaa lainsäädäntöä. Ehdotetun itsehallittavan identiteetin mallin katsotaan olevan yhdenmukaista perustuslain sääntelyn näkökulmasta. Perustuslakivaliokunta ei ole kuitenkaan aiemmin käsitellyt ehdotetun kaltaista henkilötietojen käsittelyn mallia. Näin ollen hallitus pitää suotavana, että perustuslakivaliokunta antaisi asiasta lausunnon.

12.3 Yhdenvertaisuus

Johdanto

Hallituksen esityksellä on vaikutuksia perustuslaissa turvatun yhdenvertaisuuden näkökulmasta. Hallituksen esityksen yhtenä tarkoituksena on edistää Suomen kansalaisten sekä Suomessa oleskelevien ulkomaalaisten yhdenvertaisia mahdollisuuksia käyttää digitaalisia palveluita ja siten asioida viranomaisen ja muiden toimijoiden kanssa sähköisesti. Sääntelyn keskeisenä tavoitteena on edistää positiivisesti perustuslaissa tarkoitetun yhdenvertaisuuden toteuttamista.

Perustuslain 6 §:n 1 momentin mukaan ihmiset ovat yhdenvertaisia lain edessä. Säännös ilmaisee paitsi vaatimuksen oikeudellisesta yhdenvertaisuudesta myös ajatuksen tosiasiallisesta tasa-arvosta. Siihen sisältyy mielivallan kieltö ja vaatimus samanlaisesta kohtelusta samanlaisissa tapauksissa. Yleistä yhdenvertaisuussäännöstä täydentää perustuslain 6 §:n 2 momentin sisältämä syrjintäkieltö, jonka mukaan ketään ei saa ilman hyväksyttävää perustetta asettaa eri asemaan sukupuolen, iän, alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella. Tällainen muu syy voi olla esimerkiksi asuinpaikka (ks. HE 309/1993 vp, s. 42–44; ks. esim. PeVL 15/2018 vp, s. 6–7, PeVL 26/2017 vp, s. 36–41 ja 44–45 ja PeVL 67/2014 vp, s. 3).

Yhdenvertaisuudesta ja syrjinnän kiellosta säädetään tarkemmin yhdenvertaisuuslaissa (1325/2014), jonka 2 luvussa kielletään sekä välitön että välillinen syrjintä. Lain 13 §:n mukaan syrjintä on välillistä, jos näennäisesti yhdenvertainen sääntö, peruste tai käytäntö saattaa jonkun muita epäedullisempaan asemaan henkilöön liittyvän syyn perusteella, paitsi jos säännöllä, perusteella tai käytännöllä on hyväksyttävä tavoite ja tavoitteen saavuttamiseksi käytetyt keinot ovat asianmukaisia ja tarpeellisia. Myös perustuslakivaliokunta on korostanut, että syrjintäkieltö koskee myös toimenpiteitä, jotka välillisesti johtavat syrjivään lopputulokseen (PeVL 31/2014 vp, s. 3).

Syrjintä kielletään nimenomaisesti myös Euroopan ihmisoikeussopimuksessa ja EU:n perusoikeuskirjassa. Euroopan ihmisoikeussopimuksen 14 artiklan mukaan tässä yleissopimuksessa

tunnustetuista oikeuksista ja vapauksista nauttiminen taataan ilman minkäänlaista sukupuoleen, rotuun, ihonväriin, kieleen, uskontoon, poliittisiin tai muihin mielipiteisiin, kansalliseen tai yhteiskunnalliseen alkuperään, kansalliseen vähemmistöön kuulumiseen, varallisuuteen, syntyperään tai muuhun asemaan perustuva syrjintää. EU-oikeudessa yhdenvertaisuusperiaate on vahvistettu Euroopan unionin perusoikeuskirjan 20 artiklassa, jonka mukaan kaikki ihmiset ovat yhdenvertaisia lain edessä. Syrjintäkielto sisältyy 21 artiklan 1 kohtaan, jossa kielletään kaikenlainen syrjintä, joka perustuu sukupuoleen, rotuun, ihonväriin tai etniseen taikka yhteiskunnalliseen alkuperään, geneettisiin ominaisuuksiin, kieleen, uskontoon tai vakaumukseen, poliittisiin tai muihin mielipiteisiin, kansalliseen vähemmistöön kuulumiseen, varallisuuteen, syntyperään, vammaisuuteen, ikään tai sukupuoliseen suuntautumiseen tai muuhun sellaiseen seikkaan. Artiklan 2 kohdassa kielletään lisäksi syrjintä kansalaisuuden perusteella.

Esityksessä tarkoitetut digitaalinen henkilöllisyystodistus, ulkomaalaisen digitaalinen asiointiväline ja luonnollisen henkilön tunnistusväline olisivat otettavissa käyttöön vapaaehtoisesti. Ehdotettujen palvelun käyttöönotto ei vaikuttaisi henkilön oikeuteen käyttää yhteiskunnan digitaalisia palveluja. Näin ollen näiden palvelujen tuottamisella ei olisi tältä osin yhdenvertaisuusvaikutuksia.

Esitykseen liittyy perustuslain 6 §:n sekä Euroopan ihmisoikeussopimuksen ja Euroopan unionin perusoikeuskirjan kannalta merkityksellisiä yhdenvertaisuuskysymyksiä, jotka liittyvät digitaalisen henkilöllisyystodistuksen, ulkomaalaisen digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen tarjoamiseen erityisryhmille sekä näiden ryhmien tosiasialliseen mahdollisuuteen hyödyntää ehdotettavia uusia välineitä sähköiseen asiointiin yhteiskunnan digitaalisissa palveluissa.

Digitaalinen henkilöllisyystodistus ja luonnollisen henkilön tunnistusväline

Hallituksen esityksen 2. lakiehdotukseen sisältyvät säännökset poliisin tarjoamasta digitaalisesta henkilöllisyystodistuksesta, jonka voisi ottaa käyttöön henkilö, jolla on voimassa oleva suomalainen passi tai henkilökortti. Henkilökortilla tarkoitetaan tässä yhteydessä myös ulkomaalaisen henkilökorttia ja yli 15-vuotiaan alaikäisen henkilökorttia. Digitaalisen henkilöllisyystodistuksen käyttöönotto edellyttää lisäksi älypuhelimien omistamista, sillä se on edellytyksenä ydinidentiteetin todisteen rekisteröimiseksi ja Digi- ja väestötietoviraston tuottaman mobiilisovelluksen asentamiseksi. Lisäksi henkilön itsensä hallittavaksi toimitettavat vahvistetut tiedot tallennettaisiin hänen omistamalleen älypuhelimelle.

Digitaalisen henkilöllisyystodistuksen käyttöönoton edellytykset, eli voimassa olevan suomalaisen passin tai henkilökortin sekä älypuhelimien omistaminen, voivat tosiasiallisesti estää tiettyjä henkilöryhmiä ottamasta digitaalista henkilöllisyystodistusta käyttöön.

Vaatimus voimassa olevan passin tai henkilökortin omistamisesta on kuitenkin välttämätön edellytys digitaalisen henkilöllisyystodistuksen hankkimiselle, sillä digitaalinen henkilöllisyystodistus on sähköinen vastine näille henkilöllisyysasiakirjoille. Kokonaisuuden arvioinnissa on lisäksi merkityksellistä, että passin tai kuvallisen henkilökortin hankkimiseen on mahdollista saada Kansaneläkelaitokselta perustoimeentulotukea, kun henkilöllisyysasiakirjan hankkiminen on henkilölle tai hänen perheenjäsenelleen välttämätöntä esimerkiksi pankissa asioimiseksi. Näin ollen vaatimuksen voimassa olevasta passista tai henkilökortista ei arvioida olevan ongelmallista yleisen yhdenvertaisuuslausekkeen tai syrjinnän kiellon näkökulmasta.

Myös vaatimusta mobiilipäätelaitteen (älypuhelimien) omistamisesta tulee arvioida yhdenvertaisuuden näkökulmasta. Lähtökohtaisesti kansalaisilla on mobiililaitteita hyvin laajasti käytössä, mutta osalla väestöstä laitetta ei kuitenkaan erinäisistä syistä ole käytössä. Tällaisia henkilöitä voivat olla esimerkiksi alle kouluikäiset lapset tai hyvin iäkkäät henkilöt. Olosuhteet ovat kuitenkin hyvin vaihtelevia ja kyse voisi myös olla henkilöistä, jotka eivät halua käyttää älypuhelinia. Digitaalinen henkilöllisyystodistus mahdollistaisi asiakkuudesta riippumattoman vahvan sähköisen tunnistautumisen sekä julkisen että yksityisen sektorin vahvaa sähköistä tunnistautumista edellyttäviin digitaalisiin palveluihin. Henkilöt, joilla ei ole käytössään älypuhelinia, voisivat ottaa sähköisessä asioinnissa digitaalisen henkilöllisyystodistuksen vaihtoehtona käyttöönsä luonnollisen henkilön tunnistusvälineen, jolla olisi mahdollista tunnistautua julkisen sektorin digitaalisiin palveluihin. Luonnollisen henkilön tunnistusväline olisi fyysinen väline, joka olisi käytettävissä ilman mobiilipäätelaitetta tai sirukorttia. Näin ollen julkisen sektorin digitaalisten palveluiden käyttämisen näkökulmasta sääntelyssä tarjottaisiin ratkaisu myös henkilöille, joilla ei ole älypuhelinia, ja tältä osin sääntely olisi perusteltua perustuslain 6 §:n näkökulmasta.

Luonnollisen henkilön tunnistusväline ei kuitenkaan mahdollistaisi sähköistä tunnistautumista vahvaa sähköistä tunnistautumista edellyttäviin yksityisen sektorin asiointipalveluihin. Tältä osin ratkaisu olisi perusteltavissa kilpailu- ja valtiontukioikeudellisen vaikutusarvion näkökulmasta. Kilpailuvaikutuksia on käsitelty tarkemmin edellä. Käytössä olisivat näissäkin tapauksissa soveltuvin osin yksityisten palveluntarjoajien tunnistusratkaisut sekä henkilökorttiin sisältyvä kansalaisvarmenne. Markkinaehtoisesti on tarjolla vastaavia vaihtoehtoisia tunnistusvälineitä, joiden avulla on mahdollista tunnistautua yksityisen sektorin asiointipalveluihin. Luonnollisen henkilön tunnistusväline lisäisi yhdenvertaisia mahdollisuuksia tunnistautua julkisen sektorin sähköisiin palveluihin ja mahdollistaisi viime kädessä kaikille mahdollisuuden asioida viranomaisen kanssa sähköisesti.

Käyntiasioinnissa digitaalisen henkilöllisyystodistuksen vaihtoehtona toimisivat nykyinen passi ja henkilökortti. Nämä toimivat jo nykyisin luotettavana tapana henkilöllisyyden osoittamiseen käyntiasioinnissa. Olemassa olevat henkilöllisyystodistukset eivät kuitenkaan mahdollista tietojen minimointia käyntiasioinnissa siten, että henkilöllisyyttä osoittava voisi luotettavasti todentaa asiointipalvelulle ainoastaan esimerkiksi kasvokuvansa ja ikänsä. Valikoitujen vahvistettujen tietojen osoittamiselle ei ole kuitenkaan vielä toistaiseksi olemassa sellaista valmista teknologiaa, jolla viranomaisten sähköisesti varmentamia henkilötietoja voitaisiin välittää luotaville osapuolille luotettavasti ilman älypuhelinia.

Edellä kuvatuin perustein digitaalisen henkilöllisyystodistuksen ja luonnollisen henkilön tunnistusvälineen muodostamaa kokonaisuutta voidaan pitää perustuslain 6 §:n mukaisena.

Ulkomaalaisen digitaalinen asiointiväline

Esityksen yhtenä tavoitteena on parantaa Suomessa oleskelevien ulkomaalaisten pääsyä yhteiskunnan tarjoamiin digitaalisiin palveluihin. Hallituksen esityksen 1. lakiehdotuksessa ehdotetaan Digi- ja väestötietoviraston tuotettavaksi uutta ulkomaalaisen digitaalista asiointivälinettä.

Ulkomaalaisen digitaalista asiointivälinettä voisi hakea ulkomaan kansalainen, jonka ei ole mahdollista saada suomalaista passia tai henkilökorttia, mutta jolla olisi tarve pystyä asioimaan suomalaisilla asiointipalveluissa. Digi- ja väestötietovirasto voisi myöntää asiointivälineen väestötietojärjestelmään rekisteröidylle ulkomaan kansalaiselle, joka on saanut suomalaisen henkilötunnuksen. Ulkomaalaisen digitaalinen asiointiväline ei olisi kuitenkaan passiin tai henkilökorttiin verrattavissa oleva henkilöllisyyttä osoittava asiakirja. Sitä ei olisi mahdollista hyödyntää käyntiasioinnissa, vaan asiointiväline olisi tarkoitettu ainoastaan sähköiseen asiointiin.

Ulkomaalaisen digitaalisen asiointivälineen voisi saada joko asioimalla henkilökohtaisesti Digi- ja väestötietovirastossa tai VTJ-lain 9 a §:n mukaisessa etärekisteröintimenettelyssä. Etärekisteröintimenettelyssä hankittu asiointiväline ei kuitenkaan olisi varmuustasoltaan yhtä luotettava kuin vahvaan sähköiseen tunnistusvälineeseen perustuva henkilön tunnistaminen. Näin ollen ulkomaan kansalainen olisi mahdollisuus käyttää asiointivälinettä sähköisessä asiointissa, mutta etärekisteröintimenettelyssä hankitun asiointivälineen käytännön hyödyntäminen olisi luottavien osapuolten päätettävissä sen matalamman varmuustason vuoksi.

Syyt ulkomaalaisen digitaalisen asiointivälineen eroille suhteessa digitaaliseen henkilöllisyystodistukseen johtuvat ennen kaikkea tietoturvallisuudesta: etärekisteröintimenettely ei ole yhtä luotettava menetelmä henkilöllisyyden tarkistamiseksi kuin henkilökohtainen asiointi viranomaisen luona ja ulkomaalaisen henkilöllisyysasiakirjan kasvokuva ei välttämättä täytä suomalaisille henkilökortti- ja passirekisteriin tallennetuilla kasvokuvilla asetettuja edellytyksiä. Näistä syistä ulkomaalaisen digitaalista asiointivälinettä ei ole mahdollista hyödyntää varsinaisena vahvan sähköisen tunnistamisen välineenä, eikä myöskään käyntiasioinnissa. Tietoturvalisuuden ja luotettavuuden varmistaminen henkilöllisyyden osoittamisessa on ensiarvoisen tärkeää ja näin ollen ulkomaalaisen digitaalisen asiointivälineen hyödynnettävyyttä on välttämättömästi rajoitettava edellä mainituilla tavoilla. Näin ollen sääntelyn katsotaan tältä osin täyttävän perustuslain 6 §:n edellytykset.

Alaikäiset

Hallituksen esityksellä olisi vaikutuksia alaikäisten asemaan digitaalisten palvelujen käyttäjinä. Perustuslain 6 §:n 3 momentin mukaan lapsia on kohdeltava tasa-arvoisesti yksilöinä, ja heidän tulee saada vaikuttaa itseään koskeviin asioihin kehitystään vastaavasti. Säännöksellä on sen esitöiden mukaan (HE 309/1993 vp, s. 45/I) korostettu vaatimusta lasten kohtelemisesta paitsi keskenään yhdenvertaisesti myös aikuisväestöön nähden tasa-arvoisina, periaatteessa yhtäläiset perusoikeudet omaavina ihmisinä. Lasta tulee kohdella yksilönä, ei pelkästään passiivisena toiminnan kohteena. Toisaalta säännös muodostaa perustan lasten vajaavaltaisena ja aikuisväestöä heikompana ryhmänä tarvitsemalle erityiselle suojelulle ja huolenpidolle (PeVL 64/2018 vp, s. 2).

Merkitystä on myös lapsen oikeuksien yleissopimuksella, jonka 1 artiklan mukaan lapsella tarkoitetaan jokaista alle 18-vuotiaasta henkilöä, ellei lapsen soveltuvien lakien mukaan täysi-ikäisyyttä saavuteta aikaisemmin.

Esityksen mukaan yli 15-vuotiaat voisivat ottaa digitaalisen henkilöllisyystodistuksen käyttöönsä ilman huoltajan suostumusta. Henkilökorttilakiin ehdotettavan uuden digitaalisen henkilöllisyystodistuksen käyttöoikeutta koskevan 1 a §:n pykälän mukaisesti henkilökorttiin sisältyisi oikeus digitaalisesta henkilöllisyystodistuksesta annetussa laissa tarkoitettuun henkilökorttiviranomaisen myöntämään digitaaliseen henkilöllisyystodistukseen. Oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon ei kuitenkaan sisälly väliaikaiseen henkilökorttiin eikä alle 15-vuotiaalle myönnettyyn alaikäiseen henkilökorttiin. Näin ollen esityksen voidaan katsoa parantavan alaikäisten yhdenvertaisuutta perustuslain 6 §:n 3 momentin tarkoittamalla tavalla siten, että esityksen mukaan 15–18-vuotiaat voisivat jatkossa saada käyttöönsä valtion tarjoaman vahvan sähköisen tunnistamisen sekä vahvistettujen tietojen osoittamisen mahdollistavan digitaalisen henkilöllisyystodistuksen henkilökorttilain mukaisen alaikäisen henkilökortin hakemisen yhteydessä ilman huoltajan suostumusta. Yli 15-vuotiaiden henkilöiden voidaan pääsääntöisesti arvioida olevan kypsyystasoltaan kykeneväisiä itsenäisesti hoitamaan omia asioitaan digitaalisissa palveluissa, joten tältä osin nyt ehdotettava sääntely edistäisi alaikäisten henkilöiden yhdenvertaista sähköistä asiointia yhteiskunnan sähköisissä palveluissa.

Esityksen mukaan alle 15-vuotiailla ei olisi kuitenkaan mahdollisuutta digitaalisen henkilöllisyystodistuksen käyttöönottoon tosiasiallisesti ilman huoltajan suostumusta. Sähköisessä asiointissa ei lähtökohtaisesti ole käyntiasioinnin tavoin mahdollista arvioida tapauskohtaisesti lapsen kehitystasoa ja kykyä tehdä asiaansa koskevia päätöksiä. Tämä puoltaa ikärajan asettamista siten, että sähköisessä asiointissa käytettävän henkilöllisyystodistuksen haltijan voidaan lähes poikkeuksetta olettaa kykenevän tekemään päätöksiä omassa asiassaan. Alle 15-vuotiaan olisi mahdollista saada todistus käyttöönsä vanhemman suostumuksella, näin varmistuen, että lapsen kehitystaso on huomioitu. Vaikka sääntely asettaa yli ja alle 15-vuotiaat alaikäiset erilaiseen asemaan, voidaan sääntelyä pitää yhdenvertaisuuden näkökulmasta perusteltuna.

12.4 Lainsäädäntövallan siirtäminen viranomaiselle

Lakiehdotuksessa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista säädetään Digi- ja väestötietovirastolle uusia määräyksenantovaltuuksia koskien digitaalisen henkilöllisyyden palvelujen tietoturvasuosuuksia. Digi- ja väestötietovirasto antaisi tarkemmat määräykset muiden tahojen tuottamille tarkastussovelluksille asetettavista vaatimuksista. Vaatimuksissa olisi edellytettävä vastaavaa tietoturvan tasoa kuin Digi- ja väestötietoviraston omassa lukijarajapinnassa vaaditaan.

Perustuslain 80 §:n 2 momentin mukaan viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Lisäksi valtuutuksen tulee perustuslain mukaan olla soveltamisalaltaan täsmällisesti rajattu. Erityinen syy säätää viranomaisen määräystenantovallasta on muun muassa tekninen ja vähäisiä yksityiskohtia koskeva sääntely (PeVL 52/2001 vp, PeVL 46/2001 vp), joka ei sisällä merkittävää harkintavallan käyttöä (PeVL 43/2000 vp). Määräyksenantovaltuuden kattamat asiat tulee määritellä tarkasti laissa ja sen soveltamisalan tulee olla täsmällisesti rajattu (HE 1/1998 vp).

Määräyksenantovaltuus pohjautuisi teknisiin vaatimusmäärittelyihin ja olisi luonteeltaan tietoturvasuosuuksien mukainen. Ehdotettavan lain nojalla Digi- ja väestötietovirasto päättäisi digitaalisen henkilöllisyyden tietojärjestelmän tarkemmista teknisistä vaatimuksista sekä tietoturvasuosuuksista. Vaatimusten tulee perustua yleisesti tunnettuihin kansallisiin tai kansainvälisiin standardeihin. Tarkastussovelluksen tarkemmat tekniset tietoturvasuosuuksien vaatimukset tarkentuvat Digi- ja väestötietoviraston oman toteutuksen myötä. Digi- ja väestötietovirastolle säädettävä määräyksenantovaltuutus olisi perusteltua huomioiden määräyksen tekninen muoto sekä vaatimusten tarkentuminen erityisesti standardien ja yleisten tietoturvasuosuuksien päivityksen myötä. Määräyksenantovaltuus mahdollistaisi Digi- ja väestötietovirastolle päivittää vaatimusmäärittelyjä tasaisin väliajoin.

Edellä kuvattu valtuutussäännös täyttää perustuslain 80 §:n 2 momentin edellytykset. Sääntelyn asiallinen merkitys ei edellytä, että asiasta säädettäisiin lailla tai asetuksella. Esitetty valtuutussäännös on tarkkarajainen, yksityiskohtainen ja soveltamisalaltaan täsmällisesti rajattu.

Edellä mainituilla perusteilla lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisyksityksessä. Hallitus pitää kuitenkin suotavana, että perustuslakivaliokunta antaisi asiasta lausunnon.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tässä laissa säädetään Digi- ja väestötietoviraston tuottamista digitaalisen henkilöllisyyden palveluista sekä niiden hyödyntämisestä.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

- 1) *digitaalisen henkilöllisyyden palveluilla* digitaalisen henkilöllisyyden tietojärjestelmää, ydinidentiteetin todistetta, ulkomaalaisen digitaalista asiointivälinettä, digitaalisen henkilöllisyyden hallintapalvelua, lukijarajapintaa ja tarkastussovellusta;
- 2) *ydinidentiteetillä* sellaista väestötietojärjestelmään rekisteröityjen henkilötietojen kokonaisuutta, jonka avulla henkilöllisyys voidaan yleisesti yksilöidä, ja joka koostuu väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 13 §:n 1 momentin 1 ja 2 kohdassa tarkoitetuista tiedoista;
- 3) *vahvistetuilla tiedoilla* viranomaisen sähköisesti varmentamia henkilötietoja;
- 4) *digitaalisella henkilöllisyystodistuksella* digitaalisesta henkilöllisyystodistuksesta annetun lain (/) 3 §:n 1 momentissa tarkoitettua todistusta;
- 5) *teknisellä alustalla* digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen haltijan mobiilipäätelaitetta;
- 6) *digitaalisen henkilöllisyyden sovelluksella* henkilöllisyystodistuksen haltijan mobiilipäätelaitteella sijaitsevaa sovellusta, joka mahdollistaa digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen käytön;
- 7) *luottavalla osapuolella* luonnollista henkilöä tai oikeushenkilöä, jolle digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen haltija osoittaa henkilöllisyytensä tai vahvistettuja tietoja;
- 8) *käyntiasioinnilla* asiointitilannetta, jossa digitaalisen henkilöllisyystodistuksen haltija ja luottava osapuoli ovat läsnä samanaikaisesti samassa paikassa ja digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai muita häneen liittyviä vahvistettuja tietoja luottavalle osapuolelle;

3 §

Digitaalisen henkilöllisyyden palvelujen rekisterinpitäjä

Digi- ja väestötietovirasto on digitaalisen henkilöllisyyden palvelujen rekisterinpitäjä. Digi- ja väestötietovirastolla ei ole kuitenkaan oikeutta digitaalisen henkilöllisyyden palvelujen tuottamisen yhteydessä käsiteltävien henkilötietojen luovuttamiseen luottavalle osapuolelle.

2 luku

Digitaalisen henkilöllisyyden tietojärjestelmän olennaiset vaatimukset ja niiden arviointi

4 §

Digitaalisen henkilöllisyyden tietojärjestelmä

Digi- ja väestötietoviraston tehtävänä on tuottaa digitaalisen henkilöllisyyden sovellusta ja siihen liittyvästä taustajärjestelmästä koostuvaa digitaalisen henkilöllisyyden tietojärjestelmää. Tietojärjestelmä sisältää tunnistusjärjestelmän, jonka avulla voidaan osoittaa vahvistettuja tietoja sähköisessä asiointissa tai käyntiasioinnissa.

Tietojärjestelmän tarkoituksena on mahdollistaa digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen tuottaminen ja hyödyntäminen.

5 §

Laatu- ja tietoturvallisuusvaatimukset

Digitaalisen henkilöllisyyden tietojärjestelmän on oltava aina käytettävissä ja sillä on oltava tarpeelliset varajärjestelmät häiriötilanteiden varalle.

Digi- ja väestötietoviraston on huolehdittava hallinnollisilla ja teknisillä toimenpiteillä tietojärjestelmän tietoturvallisuudesta siten, että:

- 1) tietojärjestelmä ja siinä käsitellyt tiedot ovat vain niiden käyttöön oikeutettujen saatavilla;
- 2) tietoja ja tietojärjestelmää eivät voi muuttaa muut kuin siihen oikeutetut;
- 3) tiedot ja tietojärjestelmä ovat niiden käyttöön oikeutettujen hyödynnettävissä;
- 4) tietojärjestelmä kestää odotettavissa olevat edistyneet tietoturvaluhat; ja
- 5) tietojärjestelmään kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat kyetään havaitsemaan.

Digi- ja väestötietovirasto päättää tietojärjestelmän tarkemmista teknisistä vaatimuksista sekä tietoturva vaatimuksista. Vaatimusten tulee perustua yleisesti tunnettuihin kansallisiin tai kansainvälisiin standardeihin. Digi- ja väestötietoviraston on ennen tietoturva vaatimuksista annettavaa päätöstä kuultava Liikenne- ja viestintävirastoa ja Poliisihallitusta.

6 §

Tunnistusjärjestelmää koskevat vaatimukset

Digitaalisen henkilöllisyyden tietojärjestelmän sisältämän tunnistusjärjestelmän tulee täyttää vähintään sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetun Euroopan parlamentin

ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason vaatimukset.

Tunnistusjärjestelmän ei tarvitse täyttää 1 momentissa tarkoitetun korotetun varmuustason mukaisia rekisteröintiä koskevia vaatimuksia ulkomaalaisen digitaalisen asiointivälineen tuotannossa.

7 §

Ennen tietojärjestelmän käyttöönottoa julkaistavat tiedot

Ennen kuin Digi- ja väestötietovirasto mahdollistaa digitaalisen henkilöllisyyden tietojärjestelmän hyödyntämisen, sen on julkaistava seuraavat tiedot:

- 1) päivämäärä, josta alkaen luottavan osapuolen on mahdollista hyödyntää tietojärjestelmää;
- 2) tietojärjestelmän ominaisuudet ja kuvaus tietojärjestelmää hyödyntäville tahoille tarjottavista teknisistä rajapinnoista ja testausjärjestelystä;
- 3) tieto suoritetusta vaatimustenmukaisuuden arvioinnista;
- 4) mahdolliset muut kuin 1–3 kohdassa tarkoitetut tietojärjestelmän hyödyntämisen kannalta välttämättömät ehdot.

Digi- ja väestötietoviraston on mahdollistettava digitaalisen henkilöllisyyden tietojärjestelmän hyödyntäminen julkaistujen tietojen mukaisesti. Digi- ja väestötietoviraston on viipymättä julkaistava 1 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista.

8 §

Luottavan osapuolen todentaminen

Digitaalisen henkilöllisyyden sovelluksen avulla on todennettava 26 §:ssä tarkoitettu luottava osapuoli varmenteen avulla tai muulla tietoturvallisella tavalla sovelluksen haltijan osoittaessa vahvistettuja henkilötietojaan digitaalisesta henkilöllisyystodistuksesta tai ulkomaalaisen digitaalisesta asiointivälineestä.

Digi- ja väestötietovirasto määrittää hyväksyttävät varmenteet tai muut todentamisen tavat 5 §:ssä tarkoitetussa päätöksessä osana muita digitaalisen henkilöllisyyden tietojärjestelmän tarkempia teknisiä vaatimuksia sekä tietoturva-vaatimuksia.

Digi- ja väestötietovirasto ylläpitää ja julkaisee listausta hyväksytyistä todentamisen tavoista sekä listausta luottavalle osapuolelle myönnettyistä ei hyväksytyistä varmenteista tai muista todentamisen tavoista.

9 §

Ilmoitukset uhkista ja häiriöistä

Digi- ja väestötietoviraston on ilman aiheutonta viivästystä ilmoitettava luottaville osapuolille, digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen digitaalisen asiointivälineen hyödyntäjille sekä digitaalisen henkilöllisyyden sovelluksen haltijoille palvelujen toimivuuteen, tietoturvaan tai käyttöön kohdistuvista havaituista merkittävistä uhkista tai häiriöistä taikka palvelun keskeytyksistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioituista kustannuksista. Ilmoituksessa on kerrottava uhkan tai häiriön arvioitu kesto. Lisäksi Digi- ja väestötietoviraston on ilmoitettava häiriön tai uhkan päättymisestä.

10 §

Vaatimustenmukaisuuden arviointi

Digitaalisen henkilöllisyyden tietojärjestelmän vaatimustenmukaisuus on osoitettava tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) 2 §:ssä tarkoitetun tietoturvallisuuden arviointilaitoksen antamalla todistuksella.

Tietoturvallisuuden arviointilaitos arvioi tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti Digi- ja väestötietoviraston hakemuksesta, täyttääkö tietojärjestelmä sitä koskevat vaatimukset. Arviointiperusteina on käytettävä tämän lain mukaisia ja Digi- ja väestötietoviraston asettamia vaatimuksia.

Tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan arvioinnista todistus sekä siihen liittyvä tarkastusraportti. Digi- ja väestötietoviraston on pyydettävä arvioinnista lausunto Liikenne- ja viestintävirastolta.

Arviointilaitoksen myöntämä todistus on voimassa enintään kaksi vuotta. Tietoturvallisuuden arviointilaitoksella on oikeus vaatia salassapitosäynnösten estämättä Digi- ja väestötietovirastolta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Todistuksen antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia.

3 luku

Ydinidentiteetin todiste

11 §

Ydinidentiteetin todiste

Ydinidentiteetin todiste toimii teknisesti luotettavana tapana osoittaa, että todistetta hallitsevalle henkilölle on väestötietojärjestelmään rekisteröity ydinidentiteetin sisältämä henkilöllisyys.

Ydinidentiteetin todiste sisältää seuraavat tiedot:

- 1) väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain 11 a §:n mukainen yksilöintitunnus;
- 2) sarjanumero;
- 3) todisteen myöntömaa;
- 4) todisteen voimassaoloaika;
- 5) todisteen haltijan julkinen avain; sekä
- 6) todisteen allekirjoittajan tiedot.

Ydinidentiteetin todisteen tulee täyttää vähintään 6 §:n 1 momentissa mainitun asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason vaatimukset.

12 §

Ydinidentiteetin todisteen myöntäminen

Digi- ja väestötietovirasto myöntää ydinidentiteetin todisteen, kun henkilö ottaa käyttöön ulkomaalaisen digitaalisen asiointivälineen tai digitaalisen henkilöllisyystodistuksen.

Digi- ja väestötietovirastolla on oikeus salassapitosäynnösten estämättä saada henkilön passin tai henkilökortin voimassaolotiedot henkilökorttilain (663/2016) 31 §:ssä tarkoitetusta henkilökorttirekisteristä tai passilain (671/2006) 29 §:ssä tarkoitetusta passirekisteristä digitaaliseen henkilöllisyystodistukseen liitettävän ydinidentiteetin todisteen myöntämiseksi.

Ydinidentiteetin todisteen rekisteröinnin edellytyksenä on, että henkilö on rekisteröity väestötietojärjestelmään.

13 §

Ydinidentiteetin todisteeseen liittyvät rekisterit

Ydinidentiteetin todisteiden rekisteriin tallennetaan väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain 11 a §:n mukainen yksilöintitunnus sekä muut todisteiden käytössä tarvittavat välttämättömät tekniset tiedot.

Henkilöihin liitetyistä teknisistä alustoista pidettävään laiterekisteriin tallennetaan henkilön yksilöivä tunnistetieto, henkilöön liitetyn teknisen alustan tekniset tiedot, laitetiedot sekä muut ydinidentiteetin todisteiden tuottamiseksi tarvittavat välttämättömät tiedot.

4 luku

Ulkomaalaisen digitaalinen asiointiväline

14 §

Ulkomaalaisen digitaalinen asiointiväline

Digi- ja väestötietoviraston tehtävänä on tuottaa ja tarjota ulkomaalaisen digitaalista asiointivälinettä, joka on henkilöllisyyttä koskevien sekä muiden vahvistettujen tietojen osoittamiseen sähköisessä asiainnissa tarkoitettu asiointiväline ja se tarjotaan käytettäväksi digitaalisen henkilöllisyyden sovelluksen avulla.

15 §

Ulkomaalaisen digitaalisen asiointivälineen myöntäminen

Digi- ja väestötietovirasto myöntää ulkomaalaisen digitaalisen asiointivälineen joko henkilön asioidessa henkilökohtaisesti Digi- ja väestötietovirastossa tai väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä.

Digi- ja väestötietoviraston tulee tunnistaa henkilö 1 momentin mainitussa lainkohdassa tarkoitetusta matkustusasiakirjasta ja varmistua, että henkilön tiedot on talletettu väestötietojärjestelmään ja hänelle on annettu henkilötunnus, kun henkilölle myönnetään ulkomaalaisen digitaalinen asiointiväline henkilökohtaisen asiainnin yhteydessä.

Jos ulkomaalaisen digitaalinen asiointiväline myönnetään, hakijalle ei anneta erillistä hallintopäätöstä tai valitusosoitusta.

16 §

Ulkomaalaisen digitaalisen asiointivälineen sisältämät tiedot

Ulkomaalaisen digitaalisen asiointivälineen myöntämisen yhteydessä Digi- ja väestötietovirasto toimittaa asiointivälineen haltijalle kopion häneen liittyvistä väestötietojärjestelmän tiedoista henkilön itsensä hallittavaksi. Asiointivälineen haltijalle toimitettavia tietoja ovat seuraavat henkilötiedot:

- 1) etunimet;
- 2) sukunimi;
- 3) syntymäaika;
- 4) henkilötunnus;
- 5) syntymäajasta johdetut ikätodisteet.

Digi- ja väestötietovirastolla on velvollisuus vahvistaa tiedot ennen niiden toimittamista henkilön itsensä haltuun siten, että luottava osapuoli kykenee varmistumaan tietojen oikeellisuudesta ja ajantasaisuudesta tarkistamalla ydinidentiteetin todisteen voimassaolon. Digi- ja väestötietovirastolla ei ole oikeutta käsitellä henkilölle toimitettuja vahvistettuja tietoja sen jälkeen, kun tiedot on toimitettu ulkomaalaisen digitaalisen asiointivälineen haltijalle.

17 §

Ulkomaalaisen digitaalisen asiointivälineen hyödyntäminen

Jos ulkomaalaisen digitaalinen asiointiväline on myönnetty väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain 9 a §:ssä säädetyn etärekisteröintimenettelyn yhteydessä, luottava osapuoli voi hyödyntää asiointivälinettä sen sähköisissä palveluissa silloin, kun laissa ei edellytetä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) tarkoittamaa vahvan sähköisen tunnistamisen käyttämistä.

Jos Digi- ja väestötietovirasto on tunnistanut ulkomaalaisen asiointivälineen haltijan 1 momentissa mainitun lain 17 §:n mukaisesti, luottava osapuoli voi hyödyntää ulkomaalaisen digitaalista asiointivälinettä vahvaan sähköiseen tunnistamiseen noudattaen, mitä mainitussa laissa säädetään.

18 §

Vahvistettujen tietojen osoittaminen sähköisessä asiointinnissa

Sähköisessä asiointinnissa ulkomaalaisen digitaalisen asiointivälineen haltija valitsee itse vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle, jollei muussa laissa toisin säädetä. Sähköisen asiointin yhteydessä luovutetaan kuitenkin aina tieto asiointivälineen varmuustasosta.

19 §

Rekisteri ulkomaalaisen digitaalisista asiointivälineistä

Digi- ja väestötietoviraston tehtävänä on pitää ulkomaalaisen digitaalisen asiointivälineen tarjoamista ja tuottamista varten rekisteriä ulkomaalaisen digitaalisista asiointivälineistä, asiointivälineiden haltijoista ja asiointivälineiden voimassaolosta.

20 §

Ulkomaalaisen digitaalisen asiointivälineen voimassaolo

Ulkomaalaisen digitaalinen asiointiväline on voimassa enintään viisi vuotta sen myöntämisestä.

21 §

Ulkomaalaisen digitaalisen asiointivälineen uusiminen

Digi- ja väestötietovirasto voi uusia ulkomaalaisen digitaalisen asiointivälineen voimassaolon asiointivälineen haltijan pyynnöstä. Asiointivälineen uusimisessa tulee noudattaa varmuus-

tasoasetuksen teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetun komission täytäntöpanoasetuksen (EU) 2015/1502 liitteen kohdassa 2.2.4 säädettyjä vaatimuksia.

22 §

Ulkomaalaisen digitaalisen asiointivälineen peruuttaminen

Digi- ja väestötietoviraston tulee peruuttaa ulkomaalaisen digitaalisen asiointiväline viipymättä sen haltijan pyynnöstä.

Digi- ja väestötietovirasto voi ilman pyyntöä peruuttaa ulkomaalaisen digitaalisen asiointivälineen tai estää sen käytön, jos sillä on syytä epäillä, että joku muu kuin se, jolle asiointiväline on myönnetty, käyttää sitä tai että asiointivälineen käytön turvallisuus on muutoin vaarantunut. Digi- ja väestötietoviraston on ilmoitettava asiointivälineen haltijalle ilman aiheetonta viivytystä asiointivälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.

23 §

Ulkomaalaisen digitaalisen asiointivälineen myöntämiseen ja peruuttamiseen liittyvien tehtävien hoitaminen yhteispalvelussa

Sen lisäksi, mitä julkisen hallinnon yhteispalvelusta annetun lain (223/2007) 6 §:ssä säädetään yhteispalvelussa hoidettavista tehtävistä, Digi- ja väestötietovirasto voi antaa ulkomaalaisen digitaalisen asiointivälineen myöntämiseen ja peruuttamiseen sekä asiointivälineen rekisteritietojen ylläpitoon liittyviä avustavia tehtäviä yhteispalvelussa hoidettavaksi. Näihin tehtäviin voi kuulua asiointivälineen:

- 1) käyttöönotto;
- 2) liittäminen tekniseen alustaan;
- 3) peruuttaminen haltijan pyynnöstä.

Jos yhteispalvelun toimeksisaaja lisäselvitysten jälkeenkään ei voi aktivoida asiointivälinettä tai liittää asiointivälineen haltijan henkilöllisyyttä asiointivälineeseen taikka peruuttaa asiointivälinettä sen haltijan pyynnöstä, on sen siirrettävä asia Digi- ja väestötietoviraston käsiteltäväksi.

5 luku

Digitaalisen henkilöllisyyden palvelujen hyödyntäminen

24 §

Digitaalisen henkilöllisyyden hallintapalvelu

Digi- ja väestötietoviraston tehtävänä on tuottaa digitaalisen henkilöllisyyden hallintapalvelua ydinidentiteetin todisteen, digitaalisen henkilöllisyydestodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen hallinnoimiseksi.

25 §

Lukijarajapinta ja tarkastussovellus

Digi- ja väestötietovirasto tuottaa ja tarjoaa lukijarajapintaa ja tarkastussovellusta, joilla voidaan käyntiasioinnissa tarkastaa henkilöllisyys ja vahvistettuja tietoja digitaalisesta henkilöllisyystodistuksesta.

Digi- ja väestötietovirasto voi myös hyväksyä muun tahon tuottaman tarkastussovelluksen käytettäväksi henkilöllisyyden ja vahvistettujen tietojen tarkastamiseen käyntiasioinnissa.

Digi- ja väestötietovirasto antaa tarkemmat määräykset muiden tahojen tuottamille tarkastussovelluksille asetettavista vaatimuksista. Vaatimuksissa on edellytettävä vastaavaa tietoturvan tasoa kuin Digi- ja väestötietoviraston omassa lukijarajapinnassa vaaditaan.

26 §

Luottavan osapuolen ilmoitusvelvollisuus

Jos luottava osapuoli hyödyntää digitaalisesta henkilöllisyystodistuksesta annetussa laissa tarkoitettua digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä suoran teknisen rajapinnan avulla, luottavan osapuolen on tehtävä ilmoitus ennen hyödyntämisen aloittamista Digi- ja väestötietovirastolle.

Ilmoituksessa on oltava ainakin seuraavat tiedot:

- 1) palveluntarjoajan nimi;
- 2) palveluntarjoajan täydelliset yhteystiedot;
- 3) tiedot tarjottavista palveluista, joissa digitaalista henkilöllisyystodistusta tai ulkomaalaisen digitaalista asiointivälinettä tullaan hyödyntämään.

Luottavan osapuolen on viipymättä ilmoitettava 2 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista.

Digi- ja väestötietovirasto toimii 2 momentissa tarkoitettujen tietojen rekisterinpitäjänä sekä ylläpitää ja julkaisee listausta 1 momentissa tarkoitetuista luottavista osapuolista.

27 §

Digitaalisen henkilöllisyyden sovelluksen haltijan velvollisuudet

Digitaalisen henkilöllisyyden sovelluksen haltijan on käytettävä sovellusta huolellisesti eikä hän saa luovuttaa sitä toisen käyttöön. Sovelluksen haltijan velvollisuus huolehtia sovelluksesta alkaa, kun hän on ottanut sovelluksen käyttöön.

Sovelluksen haltijan on ilmoitettava Digi- ja väestötietovirastolle teknisen alustan katoamisesta tai, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä ilman aiheutonta viivytystä havaittuaan asian. Digi- ja väestötietoviraston on tarjottava mahdollisuus ilmoituksen tekemiseen milloin tahansa.

28 §

Digitaalisen henkilöllisyyden sovelluksen oikeudetonta käyttöä koskevat vastuunrajoitukset

Digitaalisen henkilöllisyyden sovelluksen haltija vastaa sovelluksen oikeudettomasta käytöstä vain, jos:

- 1) hän on luovuttanut sovelluksen käyttöön oikeudettomalle;
- 2) teknisen alustan katoaminen tai, joutuminen oikeudettomasti toisen haltuun tai sovelluksen oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää; tai
- 3) hän on laiminlyönyt ilmoittaa Digi- ja väestötietovirastolle teknisen alustan katoamisesta tai, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä ilman aiheutonta viivytystä sen havaittuaan.

Sovelluksen haltija ei kuitenkaan vastaa sovelluksen oikeudettomasta käytöstä:

1) siltä osin kuin sovellusta on käytetty sen jälkeen, kun hän on ilmoittanut Digi- ja väestötietovirastolle teknisen alustan katoamisesta tai, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä;

2) jos sovelluksen haltija ei ole voinut tehdä ilmoitusta teknisen alustan katoamisesta tai, joutumisesta oikeudettomasti toisen haltuun tai sovelluksen oikeudettomasta käytöstä ilman aiheutonta viivytystä sen havaittuaan sen johdosta, että Digi- ja väestötietovirasto on laiminlyönyt 27 §:n 2 momentissa tarkoitetun velvollisuutensa huolehtia siitä, että sovelluksen haltijalla on milloin tahansa mahdollisuus tehdä kyseinen ilmoitus.

6 luku

Erinäiset säännökset

29 §

Muutoksenhaku

Digi- ja väestötietoviraston päätökseen, joka koskee 15 §:ssä tarkoitettua ulkomaalaisen digitaalisen asiointivälineen myöntämistä tai 22 §:n 2 momentissa tarkoitettua ulkomaalaisen digitaalisen asiointivälineen peruuttamista saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003).

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

30 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Digi- ja väestötietoviraston on annettava 25 §:n 3 momentissa tarkoitetut määräykset 4 kuukauden kuluessa tämän lain voimaantulosta.

2.

Laki

digitaalisesta henkilöllisyystodistuksesta

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Lain tarkoitus

Tässä laissa säädetään Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle tarjottavasta digitaalisesta henkilöllisyystodistuksesta.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

- 1) *vahvistetuilla tiedoilla* viranomaisen sähköisesti varmentamia henkilötietoja;
- 2) *luottavalla osapuolella* luonnollista henkilöä tai oikeushenkilöä, jolle digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai vahvistettuja tietoja;
- 3) *digitaalisen henkilöllisyystodistuksen haltijalla* henkilöä, joka on ottanut käyttöönsä digitaalisen henkilöllisyystodistuksen;
- 4) *teknisellä alustalla* digitaalisen henkilöllisyystodistuksen haltijan mobiilipäätelaitetta;
- 5) *käyntiasioinnilla* asiointitilannetta, jossa digitaalisen henkilöllisyystodistuksen haltija ja luottava osapuoli ovat läsnä samanaikaisesti samassa paikassa ja digitaalisen henkilöllisyystodistuksen haltija osoittaa henkilöllisyytensä tai muita häneen liittyviä vahvistettuja tietoja luottavalle osapuolelle.
- 6) *ydinidentiteetin todisteella* Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain (/) 11 §:ssä tarkoitettua todistetta.

3 §

Digitaalinen henkilöllisyystodistus

Digitaalinen henkilöllisyystodistus on henkilöllisyyden sekä vahvistettujen tietojen osoittamiseen sähköisessä asiointissa ja käyntiasioinnissa tarkoitettu henkilöllisyystodistus. Oikeudesta digitaaliseen henkilöllisyystodistukseen säädetään henkilökorttilaissa (663/2016) ja passilaissa (671/2006). Digitaalisen henkilöllisyystodistuksen tuottaa poliisi.

Digitaalinen henkilöllisyystodistus tarjotaan käytettäväksi Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain (/) 2 §:n 6 kohdassa tarkoitetun digitaalisen henkilöllisyyden sovelluksen avulla.

Poiketen siitä, mitä passilain 34 §:ssä ja henkilökorttilain 34 §:ssä säädetään passista ja henkilökortista perittävistä maksuista, digitaalisen henkilöllisyystodistuksen osalta maksu voidaan määrätä omakustannusarvoa pienemmäksi.

2 luku

Digitaalisen henkilöllisyystodistuksen sisältämät tiedot ja voimassaolo

4 §

Digitaalisen henkilöllisyystodistuksen sisältämät tiedot

Poliisi toimittaa digitaalisen henkilöllisyystodistuksen haltijalle kopion häneen liittyvistä henkilökorttilain 31 §:ssä tarkoitetun henkilökorttirekisterin tai passilain 29 §:ssä tarkoitetun passirekisterin sisältämistä tiedoista henkilön itsensä hallittavaksi. Digitaalisen henkilöllisyystodistuksen haltijalle toimitettavia tietoja ovat seuraavat henkilötiedot:

- 1) etunimet;
- 2) sukunimi;
- 3) syntymäaika;
- 4) tieto henkilön sukupuolesta;
- 5) tieto Suomen kansalaisuudesta;
- 6) henkilötunnus tai muu kansallisen tason yksilöintitunnus;
- 7) passi- tai henkilökorttirekisteriin talletettu kasvokuva;
- 8) voimassa olevan suomalaisen passin tai henkilökortin voimassaoloaika; sekä
- 9) todistuksen yksilöivä tunnus.

Poliisilla on velvollisuus varmentaa tiedot ennen niiden toimittamista henkilön itsensä haltuun digitaaliseen henkilöllisyystodistukseen siten, että luottava osapuoli kykenee varmistumaan tietojen oikeellisuudesta ja ajantasaisuudesta tarkistamalla varmenteen voimassaolon. Poliisilla ei ole oikeutta käsitellä henkilölle toimitettuja vahvistettuja tietoja sen jälkeen, kun tiedot on toimitettu digitaalisen henkilöllisyystodistuksen haltijalle.

Tietojen aitouden ja eheyden varmistamiseen liittyvät varmenteet luo Digi- ja väestötietovirasto. Lisäksi Digi- ja väestötietovirasto toimittaa syntymäajasta johdetut ikätodisteet digitaalisen henkilöllisyystodistuksen haltijalle.

Digitaalisen henkilöllisyystodistuksen tiedot päivitetään sen haltijan nimenomaisesta pyynnöstä. Digitaalisen henkilöllisyystodistuksen käytön edellytyksenä kuitenkin on, että sen sisältämät tiedot ovat ajan tasalla ja vastaavat 1 momentissa mainituissa rekistereissä olevia tietoja.

5 §

Rekisteri digitaalisista henkilöllisyystodistuksista

Poliisi pitää rekisteriä digitaalisista henkilöllisyystodistuksista. Rekisteriin saadaan tallentaa tiedot 4 §:n 1 momentin 1–9 kohdassa tarkoitetuista tiedoista siltä osin kuin kyse on henkilöistä, joilla on oikeus digitaalisen henkilöllisyystodistuksen käyttöönottoon. Lisäksi rekisteriin tallennetaan tiedot digitaalisista henkilöllisyystodistuksista, todistusten haltijoista ja todistusten voimassaolosta.

Rekisterin tiedot poistetaan viimeistään kymmenen vuoden kuluttua siitä, kun henkilön oikeus digitaaliseen henkilöllisyystodistukseen on päättynyt.

6 §

Digitaalisen henkilöllisyystodistuksen käyttöönotto

Henkilö voi ottaa digitaalisen henkilöllisyystodistuksen käyttöön asioimalla muun toimivaltaisen passi- tai henkilökorttiviranomaisen luona kuin ulkoministeriön luona, tai käyttäen vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 2 §:n 1 kohdassa tarkoitettua vahvaa sähköistä tunnistamista. Vahva sähköinen tunnistaminen edellyttää, että henkilön voimassa olevan passin tai henkilökortin teknisen osan tiedot on etäluettu ja ne vastaavat vahvassa sähköisessä tunnistamisessa saatuja tietoja.

Digitaalisen henkilöllisyystodistuksen käyttöönoton yhteydessä poliisi liittää Digi- ja väestötietoviraston myöntämän ydinidentiteetin todisteen luonnolliseen henkilöön.

7 §

Digitaalisen henkilöllisyystodistuksen käyttöönotto alaikäiselle

Alaikäinen voi ottaa digitaalisen henkilöllisyystodistuksen käyttöön, jos hänen huoltajansa siihen suostuvat.

Mitä 1 momentissa säädetään, ei koske 15 vuotta täyttänyttä alaikäistä.

8 §

Digitaaliseen henkilöllisyystodistukseen voimassaolo

Digitaalisen henkilöllisyystodistuksen voimassaolo päättyy vuoden kuluttua siitä, kun sen perustana olevan henkilöllisyyttä osoittavan asiakirjan voimassaolo on päättynyt.

Henkilöllisyyttä osoittavalla asiakirjalla tarkoitetaan sitä passilain tai henkilökorttilain mukaisesti myönnettyä henkilöllisyyttä osoittavaa asiakirjaa, jonka perusteella henkilöllä on oikeus digitaaliseen henkilöllisyystodistukseen.

9 §

Digitaalisen henkilöllisyystodistuksen peruuttaminen

Poliisi peruuttaa digitaalisen henkilöllisyystodistuksen, jos sen haltija sitä pyytää. Jos digitaalisen henkilöllisyystodistuksen haltija ilmoittaa teknisen alustan katoamisesta tai joutumisesta oikeudettomasti toisen haltuun, digitaalisen henkilöllisyystodistuksen voi peruuttaa myös Digi- ja väestötietovirasto.

Poliisi voi peruuttaa digitaalisen henkilöllisyystodistuksen, jos siinä on ilmeinen virheellisyys, sen taustalla oleva henkilöllisyyttä osoittava asiakirja peruutetaan tai sitä käyttää joku muu kuin digitaalisen henkilöllisyystodistuksen haltija tai sen käytön turvallisuus on muutoin vaarantunut.

3 luku

Digitaalisen henkilöllisyystodistuksen käyttäminen

10 §

Vahvistettujen tietojen osoittaminen sähköisessä asiointinnissa

Sähköisessä asiointinnissa digitaalisen henkilöllisyystodistuksen haltija valitsee itse vahvistetut tiedot jotka hän haluaa osoittaa luottavalle osapuolelle, jollei muussa laissa toisin säädetä.

Sähköisen asiointin yhteydessä luovutetaan kuitenkin aina tieto poliisin tekemästä liitoksesta henkilön ydinidentiteettiin.

11 §

Vahvistettujen tietojen osoittaminen käyntiasioinnissa

Käyntiasioinnissa digitaalisen henkilöllisyystodistuksen haltija valitsee itse ne vahvistetut tiedot, jotka hän haluaa osoittaa luottavalle osapuolelle. Käyntiasioinnissa on kuitenkin aina osoitettava kasvokuva.

Tietoja vastaanottavalla luottavalla osapuolella on oikeus tarkastaa digitaalisen henkilöllisyystodistuksen haltijan ydinidentiteetin todisteen voimassaolon Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 13 §:n 1 momentissa tarkoitetusta ydinidentiteetin todisteiden rekisteristä.

4 luku

Erinäiset säännökset

12 §

Muutoksenhaku

Poliisin päätökseen, joka koskee 9 §:n 2 momentissa tarkoitettua digitaalisen henkilöllisyystodistuksen peruuttamista saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003).

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

13 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

3.

Laki

vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 2 §:n 1 momentin 1 ja 11 kohta, 7 b §, 17 §:n 2 ja 4 momentti ja 42 a §:n 3 momentin 2 kohta,

sellaisina kuin ne ovat, 2 §:n 1 momentin 1 ja 11 kohta, 7 b § ja 17 §:n 2 momentti laissa 1009/2018, 17 §:n 4 momentti laissa 412/2019 ja 42 a §:n 3 momentin 2 kohta laissa 230/2021, sekä

lisätään 2 §:n 1 momenttiin, sellaisena kuin se on laissa 1009/2018, uusi 12 ja 13 kohta, lakiin uusi 12 e §, 16 §:ään, sellaisena kuin se on laissa 412/2019, uusi 3 momentti, jolloin nykyinen 3 momentti siirtyy 4 momentiksi, sekä lakiin uusi 16 a ja 17 b §

seuraavasti:

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *vahvalla sähköisellä tunnistamisella* sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteiden aitouden ja oikeellisuuden todentamista digitaalisen henkilöllisyyden välinettä tai muuta 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;

11) *vaatimustenmukaisuuden arviointilaitoksella* Liikenne- ja viestintäviraston hyväksymää tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettua elintä, joka on akkreditoitu mainitun asetuksen mukaisesti;

12) *digitaalisen henkilöllisyyden palvelujen tarjoajalla* tahoa, joka tuottaa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa (/), jäljempänä *digitaalisen henkilöllisyyden palveluista annettu laki*, tarkoitettuja digitaalisen henkilöllisyyden palveluja ja joka ei ole 3 kohdassa tarkoitettu tunnistuspalvelun tarjoaja;

13) *digitaalisen henkilöllisyyden välineellä* digitaalisesta henkilöllisyystodistuksesta annetun lain (/) 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta sekä digitaalisen henkilöllisyyden palveluista annetun lain 14 §:ssä tarkoitettua ulkomaalaisen digitaalista asiointivälinettä, jonka haltija on tunnistettu tämän lain 17 §:n mukaisesti.

7 b §

Tieto passin, henkilökortin tai digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteettin todisteen voimassaolosta

Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta. Tieto ensitunnistamisessa käytettävän digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen voimassaolosta voidaan tarkistaa digitaalisen henkilöllisyyden palveluista annetun lain 25 §:ssä tarkoitetun tarkastusovelluksen kautta sekä mainitun lain 13 §:ssä tarkoitetusta ydinidentiteetin todisteiden rekisteristä.

Tunnistusvälineen tarjoaja on velvollinen varmistamaan 1 momentissa tarkoitetut tiedot ensitunnistamisessa käytettävän asiakirjan voimassaolosta. Tunnistusvälineen tarjoajan on varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin asiakirjan voimassaolo on varmistettu.

12 e §

Digitaalisen henkilöllisyyden palvelujen tarjoajan velvollisuudet luottamusverkostossa

Digitaalisen henkilöllisyyden palvelujen tarjoajan on tarjottava maksutta digitaalisen henkilöllisyyden palveluista annetun lain 4 §:ssä tarkoitetun digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää digitaalisen henkilöllisyyden välineeseen perustuvia tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle. Ennen digitaalisen henkilöllisyyden tietojärjestelmän käyttöönottoa julkaistavista tiedoista säädetään mainitun lain 7§:ssä.

Digitaalisen henkilöllisyyden palvelujen tarjoajan tulee määritellä digitaalisen henkilöllisyyden tietojärjestelmän tarjoamisessa käytettävät tekniset rajapinnat ja standardit.

16 §

Tunnistuspalvelun tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä 1 momentissa tarkoitetut tiedot myös digitaalisen henkilöllisyyden palvelujen tarjoajalle. Lisäksi tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa digitaalisen henkilöllisyyden palvelujen tarjoajalle 2 momentissa tarkoitettuja tietoja sekä uhkien ja häiriöiden selvittämiseen liittyviä tietoja.

16 a §

Digitaalisen henkilöllisyyden palvelujen tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Digitaalisen henkilöllisyyden palvelujen tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä luottamusverkostossa toimiville tunnistuspalvelun tarjoajille sekä Liikenne- ja viestintävirastolle digitaalisen henkilöllisyyden välineen toimivuuteen, tietoturvaan, tietosujaan tai digitaalisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista, häiriöistä tai palvelun keskeytyksistä sekä uhkien ja häiriöiden selvittämiseen liittyvistä tiedoista. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioituista kustannuksista.

Tunnistuspalvelun tarjoaja ja digitaalisen henkilöllisyyden palvelujen tarjoaja saavat käyttää 1 momentin ja 16 §:n 3 momentin nojalla saatuja toisiaan koskevia tietoja vain siihen tarkoitukseen, jota varten ne on annettu. Tietoja saavat tunnistuspalvelun tarjoajan palveluksessa tai sen lukuun käsitellä ainoastaan ne, jotka tarvitsevat tietoja välttämättä työssään.

17 §

Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinin viranomaisen myöntämä passi tai henkilökortti. Halutesaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia tai digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta.

Tunnistusvälineen tarjoajan on mahdollistettava se, että toinen tunnistusvälineen tarjoaja tai digitaalisen henkilöllisyyden palvelujen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä tai digitaalisen henkilöllisyyden välinettä. Mitä 12 a ja 12 b §:ssä säädetään tunnistuspalvelun käyttöoikeuden luovutuksesta ja toimitusehtojen julkaisemisesta, sovelletaan myös tässä momentissa tarkoitettuun tunnistusvälineen käyttämiseen ensitunnistamisessa.

17 b §

Digitaalinen henkilöllisyystodistus ensitunnistamisessa

Digitaalisen henkilöllisyyden palvelujen tarjoajan on mahdollistettava se, että tunnistusvälineen tarjoaja voi maksutta käyttää digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Mitä digitaalisen henkilöllisyyden palveluista annetun lain 7 §:ssä säädetään ennen digitaalisen henkilöllisyyden tietojärjestelmän käyttöönottoa julkaistavista tiedoista, sovelletaan myös digitaalisen henkilöllisyystodistuksen käyttämiseen ensitunnistamisessa.

42 a §

Liikenne- ja viestintäviraston tehtävät

Liikenne- ja viestintäviraston tehtävänä on sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisesti:

2) ilmoittaa 10 §:n mukaisesti ilmoitettuja sähköisen tunnistamisen järjestelmiä Euroopan komissiolle asetuksen 7–10 artiklan mukaisesti;

Tämä laki tulee voimaan päivänä kuuta 20 . Sen 7 b §:n 2 momenttia sovelletaan kuitenkin vasta 1. päivästä joulukuuta 2023.

4.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain 16 ja 22 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan henkilötietojen käsittelystä poliisitoimesta annetun lain (616/2019) 16 §:n 1 momentin 15 kohta ja 22 §:n 1 momentin 17 kohta sekä
lisätään 16 §:n 1 momenttiin, sellaisena kuin se on osaksi laeissa 1162/2019, 632/2020 ja 1308/2021, uusi 16 kohta ja 22 §:n 1 momenttiin, sellaisena kuin se on osaksi laissa 632/2020, uusi 18 kohta seuraavasti:

16 §

Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä

Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilökisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tietoja rekistereistä siten kuin käytännön menettelyistä asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:

15) rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä; oikeudesta saada tietoja lentoliikenteen matkustajarekisteristä säädetään lentoliikenteen matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden torjunnassa annetussa laissa (657/2019);

16) Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa (/) tarkoitetuista rekistereistä digitaalisen henkilöllisyystodistuksen tuottamiseksi välttämättömistä tiedoista sekä henkilötietojen väärinkäyttöepäilyjen, identiteettivarkauksien tai muiden vastaavien rikosten selvittämiseksi ja näiden ennalta estämiseksi.

22 §

Muu henkilötietojen luovuttaminen viranomaisille

Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:

17) Puolustusvoimille, Tullille, Rajavartiolaitokselle ja Rikosseuraamuslaitokselle näiden palveluksessa olevan, ampuma-aseen kantamiseen virka-, työ- tai palvelustehtävässään oikeutetun henkilön ampuma-aseen kantamista koskevan sopivuuden arvioimista varten;

18) Digi- ja väestötietovirastolle 11 ja 12 §:ssä tarkoitettuja henkilötietoja Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa tarkoitettujen digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin todisteen tuottamista ja hallinnoimista varten.

Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

henkilökorttilain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään henkilökorttilakiin (663/2016) uusi 1 a § seuraavasti:

1 a §

Digitaalinen henkilöllisyystodistus

Henkilökorttiin sisältyy oikeus ottaa käyttöön digitaalisesta henkilöllisyystodistuksesta annettussa laissa (/) tarkoitettu digitaalinen henkilöllisyystodistus.

Mitä 1 momentissa säädetään, ei koske väliaikaista henkilökorttia eikä alle 15-vuotiaalle myönnettyä alaikäisen henkilökorttia.

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 1 a §:ssä tarkoitettua oikeutta ottaa digitaalinen henkilöllisyystodistus käyttöön sovelletaan myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin henkilökortteihin.

6.

Laki

passilain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään passilakiin (671/2006) uusi 3 d § seuraavasti:

3 d §

Digitaalinen henkilöllisyystodistus

Passiin sisältyy oikeus ottaa käyttöön digitaalisesta henkilöllisyystodistuksesta annetussa laissa (/) tarkoitettu digitaalinen henkilöllisyystodistus.

Mitä 1 momentissa säädetään, ei koske väliaikaista passia eikä hätäpassia.

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 3 d §:ssä tarkoitettua oikeutta ottaa digitaalinen henkilöllisyystodistus käyttöön sovelletaan myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin passeihin.

7.

Laki

väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lakiin (661/2009) uusi 6 b luku seuraavasti:

6 b luku

Luonnollisen henkilön tunnistusväline

69 e §

Luonnollisen henkilön tunnistusväline

Digi- ja väestötietoviraston tehtävänä on myöntää luonnollisen henkilön sähköiseen tunnistamiseen tarkoitettua tunnistusvälinettä, 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.

Luonnollisen henkilön tunnistusväline on fyysinen väline, joka on käytettävissä ilman mobiilipäätelaitetta tai sirukorttia.

Digi- ja väestötietovirasto tarjoaa luonnollisen henkilön tunnistusvälinettä sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisena tunnistusvälineenä käytettäväksi tukipalvelulain 3 §:n 1 momentin 4 kohdassa tarkoitetun tukipalvelun välityksellä.

69 f §

Rekisteri luonnollisen henkilön tunnistusvälineistä

Digi- ja väestötietoviraston tehtävänä on ylläpitää luonnollisen henkilön tunnistusvälineen tarjoamista ja tuottamista varten rekisteriä tunnistusvälineistä ja niiden haltijoista. Rekisteriin voidaan tallentaa tunnistusvälineen haltijan:

1) henkilötiedot, jotka sisältyvät henkilöllisyyden varmentamiseen käytettyyn viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan sekä asiakirjan yksilöintitiedot;

2) henkilötiedot, jotka välitetään henkilöllisyyden varmentamiseen käytetyn sähköisen tunnistusmenetelmän yhteydessä sekä tiedot sähköisestä tunnistusmenetelmästä;

3) 11 a §:n mukainen yksilöintitunnus;

4) tunnistusvälineen yksilöivä tunniste;

5) yhteystiedot;

6) muut kuin 1–5 kohdassa tarkoitetut tunnistusvälineen tarjoamiseksi tarpeelliset tiedot.

Henkilötietojen käsittelystä luonnollisen henkilön tunnistusvälineen palvelutuotannossa, tunnistusvälinettä ja sen käyttöä koskevista vaatimuksista sekä palvelutuotannon ohjauksesta säädetään tukipalvelulain 3–5 luvussa.

69 g §

Hakijan henkilöllisyyden todistaminen

Digi- ja väestötietovirasto myöntää luonnollisen henkilön tunnistusvälineen henkilölle hakemuksesta.

Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetun komission täytäntöönpanoasetuksen (EU) 2015/1502 liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 kohdassa tarkoitettuun vahvaan sähköiseen tunnistamiseen.

69 h §

Tunnistusvälineen myöntämiseen liittyvien tehtävien hoitaminen yhteispalvelussa

Sen lisäksi, mitä yhteispalvelulain 6 §:ssä säädetään yhteispalvelussa hoidettavista tehtävistä, Digi- ja väestötietovirasto voi antaa tunnistusvälineen myöntämiseen liittyviä avustavia tehtäviä yhteispalvelussa hoidettavaksi. Näihin tehtäviin voi kuulua tunnistusvälineen hakijan tai haltijan henkilöllisyyden todentaminen sekä tunnistusvälineen hakemiseen liittyvät neuvonta- ja tukitehtävät.

Jos yhteispalvelun toimeksisaaja lisäselvitysten jälkeenkään ei voi todentaa hakijan henkilöllisyyttä, on sen siirrettävä asia Digi- ja väestötietoviraston käsiteltäväksi.

69 i §

Tieto passin tai henkilökortin voimassaolosta

Digi- ja väestötietovirastolla on oikeus saada salassapitosäännösten estämättä teknisen rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.

69 j §

Digi- ja väestötietoviraston tiedonantovelvollisuus

Digi- ja väestötietoviraston on ennen tunnistusvälineen myöntämistä annettava hakijalle tiedot:

- 1) tunnistusvälineen käytöstä;
- 2) osapuolten oikeuksista ja velvollisuuksista;
- 3) mahdollisista vastuunrajoituksista; sekä
- 4) muista kuin 1-3 kohdassa tarkoitetuista mahdollisista tunnistusvälineen käyttöehdoista.

Edellä 1 momentissa tarkoitettut tiedot on annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voi tallentaa ja toisintaa ne muuttumattomina.

69 k §

Digi- ja väestötietoviraston oikeus peruuttaa tai estää tunnistusvälineen käyttöä

Digi- ja väestötietovirasto voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:

- 1) on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;

- 2) tunnistusväline sisältää ilmeisen virheellisyyden;
- 3) on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;
- 4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti käyttöehtojen vastaisella tavalla;
- 5) tunnistusvälineen haltija on kuollut.

Digi- ja väestötietoviraston tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.

Digi- ja väestötietoviraston on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.

69 l §

Luonnollisen henkilön tunnistusvälineen haltijan velvollisuudet

Luonnollisen henkilön tunnistusvälineen haltijan on käytettävä tunnistusvälinettä käyttöehtojen mukaisesti. Tunnistusvälineen haltijan on säilytettävä tunnistusvälinettä huolellisesti. Tunnistusvälineen haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.

Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

Tunnistusvälineen haltijan on ilmoitettava Digi- ja väestötietovirastolle tunnistusvälineen joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheutonta viivytystä havaittuaan asian.

Digi- ja väestötietoviraston on tarjottava mahdollisuus tehdä 3 momentissa tarkoitettu ilmoitus milloin tahansa. Digi- ja väestötietoviraston on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen. Tunnistusvälineen haltija ei vastaa välineen oikeudettomasta käytöstä Digi- ja väestötietovirastolle tehdyn ilmoituksen jälkeen.

69 m §

Muutoksenhaku

Digi- ja väestötietoviraston päätökseen, joka koskee 69 e §:ssä tarkoitetun luonnollisen henkilön tunnistusvälineen myöntämistä ja 69 k §:ssä tarkoitettuun luonnollisen henkilön tunnistusvälineen peruuttamista saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa.

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Tämä laki tulee voimaan päivänä kuuta 20 .

8.

Laki

hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 ja 9 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016) 3 §:n 1 momentin 4 kohta sekä 9 §:n 1 kohta, sellaisena kuin niistä on jälkimmäinen laissa 1174/2019, seuraavasti:

3 §

Tukipalvelut

Yhteisiä sähköisen asioinnin tukipalveluja ovat:

4) luonnollisen henkilön tunnistuspalvelu, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) tarkoitetun tunnistuspalvelun tarjoajan palvelua tai väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 6 b luvun mukaista palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle;

9 §

Palvelutuotannossa säännönmukaisesti hyödynnettävät tietolähteet

Digi- ja väestötietovirastolla on oikeus sille tässä laissa säädettyjen tehtävien hoitamiseksi käsitellä seuraaviin tietojärjestelmiin tallennettuja tässä pykälässä tarkoitettuja tietoja noudattaen tätä lukua:

1) väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa tarkoitetusta väestötietojärjestelmästä henkilön nimeä, henkilötunnusta, sähköistä asiantunnettua, kansalaisuutta, asiantunnettua, äidinkieltä, kuolinpäivää, edunvalvontaa, toimintakelpoisuuden rajoittamista, edunvalvontavaltuutusta ja lapsen huoltoa koskevia tietoja sekä yhteystietoja ja tietoa turvakiellosta;

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 15.9.2022

Pääministeri

Sanna Marin

kuntaministeri Sirpa Paatero

3.

Laki

vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 2 §:n 1 momentin 1 ja 11 kohta, 7 b §, 17 §:n 2 ja 4 momentti ja 42 a §:n 3 momentin 2 kohta,

sellaisina kuin ne ovat, 2 §:n 1 momentin 1 ja 11 kohta, 7 b § ja 17 §:n 2 momentti laissa 1009/2018, 17 §:n 4 momentti laissa 412/2019 ja 42 a §:n 3 momentin 2 kohta laissa 230/2021, sekä

lisätään 2 §:n 1 momenttiin, sellaisena kuin se on laissa 1009/2018, uusi 12 ja 13 kohta, lakiin uusi 12 e §, 16 §:ään, sellaisena kuin se on laissa 412/2019, uusi 3 momentti, jolloin nykyinen 3 momentti siirtyy 4 momentiksi, sekä lakiin uusi 16 a ja 17 b §

seuraavasti:

Voimassa oleva laki

Ehdotus

2 §

2 §

Määritelmät

Määritelmät

Tässä laissa tarkoitetaan:

1) *vahvalla sähköisellä tunnistamisella* sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteiden 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;

Tässä laissa tarkoitetaan:

1) *vahvalla sähköisellä tunnistamisella* sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteiden aitouden ja oikeellisuuden todentamista *digitaalisen henkilöllisyyden välinettä tai muuta* 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;

11) *vaatimustenmukaisuuden arviointilaitoksella* Liikenne- ja viestintäviraston hyväksymää tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen

11) *vaatimustenmukaisuuden arviointilaitoksella* Liikenne- ja viestintäviraston hyväksymää tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen

(ETY) N:o 339/93 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettua elintä, joka on akkreditoitu mainitun asetuksen mukaisesti.

(ETY) N:o 339/93 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettua elintä, joka on akkreditoitu mainitun asetuksen mukaisesti;

12) **digitaalisen henkilöllisyyden palvelujen tarjoajalla** tahoa, joka tuottaa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa (/), jäljempänä **digitaalisen henkilöllisyyden palveluista annettu laki**, tarkoitettuja digitaalisen henkilöllisyyden palveluja ja joka ei ole 3 kohdassa tarkoitettu tunnistuspalvelun tarjoaja;

13) **digitaalisen henkilöllisyyden välineellä** digitaalisesta henkilöllisyystodistuksesta annetun lain (/) 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta sekä digitaalisen henkilöllisyyden palveluista annetun lain 14 §:ssä tarkoitettua ulkomaalaisen digitaalista asiointivälinettä, jonka haltija on tunnistettu tämän lain 17 §:n mukaisesti.

7 b §

Tieto passin tai henkilökortin voimassaolosta

Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.

7 b §

*Tieto passin, henkilökortin **tai digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen** voimassaolosta*

Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta. *Tieto ensitunnistamisessa käytettävän digitaalisen henkilöllisyystodistuksen sisältämän ydinidentiteetin todisteen voimassaolosta voidaan tarkistaa digitaalisen henkilöllisyyden palveluista annetun lain 25 §:ssä tarkoitetun tarkastussovelluksen kautta sekä mainitun lain 13 §:ssä tarkoitetusta ydinidentiteetin todisteiden rekisteristä.*

Tunnistusvälineen tarjoaja on velvollinen varmistamaan 1 momentissa tarkoitetut tiedot ensitunnistamisessa käytettävän asiakirjan voimassaolosta. Tunnistusvälineen tarjoajan on varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin asiakirjan voimassaolo on varmistettu.

12 e §

Digitaalisen henkilöllisyyden palvelujen tarjoajan velvollisuudet luottamusverkostossa

Digitaalisen henkilöllisyyden palvelujen tarjoajan on tarjottava maksutta digitaalisen henkilöllisyyden palveluista annetun lain 4 §:ssä tarkoitetun digitaalisen henkilöllisyyden tietojärjestelmän käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää digitaalisen henkilöllisyyden välineeseen perustuvia tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle. Ennen digitaalisen henkilöllisyyden tietojärjestelmän käyttöönottoa julkaistavista tiedoista säädetään mainitun lain 7§:ssä.

Digitaalisen henkilöllisyyden palvelujen tarjoajan tulee määritellä digitaalisen henkilöllisyyden tietojärjestelmän tarjoamisessa käytettävät tekniset rajapinnat ja standardit.

16 §

Tunnistuspalvelun tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa kaikille luottamusverkoston jäsenille 1 momentissa tarkoitetuista uhkista ja häiriöistä sekä palvelun tarjoajista, joiden on syytä epäillä tavoittelevan oikeudetonta taloudellista hyötyä, antavan merkityksellisiä totuudenvastaisia tai harhaanjohtavia tietoja tai käsittelevän henkilötietoja lainvastaisesti.

16 §

Tunnistuspalvelun tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä 1 momentissa tarkoitettut tiedot myös digitaalisen henkilöllisyyden palvelujen tarjoajalle. Lisäksi tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa digitaalisen henkilöllisyyden palvelujen tarjoajalle 2 momentissa tarkoitettuja tietoja sekä uhkien ja häiriöiden selvittämiseen liittyviä tietoja.

16 a §

Digitaalisen henkilöllisyyden palvelujen tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Digitaalisen henkilöllisyyden palvelujen tarjoajan on salassapitosäännösten estämättä

ilmoitettava ilman aiheutonta viivästystä luottamusverkostossa toimiville tunnistuspalvelun tarjoajille sekä Liikenne- ja viestintävirastolle digitaalisen henkilöllisyyden välineen toimivuuteen, tietoturvaan, tietosuojaan tai digitaalisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista, häiriöistä tai palvelun keskeytyksistä sekä uhkien ja häiriöiden selvittämiseen liittyvistä tiedoista. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.

Tunnistuspalvelun tarjoaja ja digitaalisen henkilöllisyyden palvelujen tarjoaja saavat käyttää 1 momentin ja 16 §:n 3 momentin nojalla saatuja toisiaan koskevia tietoja vain siihen tarkoitukseen, jota varten ne on annettu. Tietoja saavat tunnistuspalvelun tarjoajan palveluksessa tai sen lukuun käsitellä ainoastaan ne, jotka tarvitsevat tietoja välttämättä työssään.

17 §

Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinin viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.

Tunnistusvälineen tarjoajan on mahdollistettava se, että toinen tunnistusvälineen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Mitä

17 §

Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinin viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia tai digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta.

Tunnistusvälineen tarjoajan on mahdollistettava se, että toinen tunnistusvälineen tarjoaja tai digitaalisen henkilöllisyyden palvelujen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnista-

Voimassa oleva laki

12 a ja 12 b §:ssä säädetään tunnistuspalvelun käyttöoikeuden luovutuksesta ja toimitusehtojen julkaisemisesta, sovelletaan myös tässä momentissa tarkoitettuun tunnistusvälineen käyttämiseen ensitunnistamisessa.

Ehdotus

miseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä *tai digitaalisen henkilöllisyyden välinettä*. Mitä 12 a ja 12 b §:ssä säädetään tunnistuspalvelun käyttöoikeuden luovutuksesta ja toimitusehtojen julkaisemisesta, sovelletaan myös tässä momentissa tarkoitettuun tunnistusvälineen käyttämiseen ensitunnistamisessa.

17 b §

Digitaalinen henkilöllisyystodistus ensitunnistamisessa

Digitaalisen henkilöllisyyden palvelujen tarjoajan on mahdollistettava se, että tunnistusvälineen tarjoaja voi maksutta käyttää digitaalisesta henkilöllisyystodistuksesta annetun lain 3 §:ssä tarkoitettua digitaalista henkilöllisyystodistusta ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Mitä digitaalisen henkilöllisyyden palveluista annetun lain 7 §:ssä säädetään ennen digitaalisen henkilöllisyyden tietojärjestelmän käyttöönottoa julkaistavista tiedoista, sovelletaan myös digitaalisen henkilöllisyystodistuksen käyttämiseen ensitunnistamisessa.

42 a §

Liikenne- ja viestintäviraston tehtävät

Liikenne- ja viestintäviraston tehtävänä on sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisesti:

2) ilmoittaa sähköisen tunnistamisen järjestelmiä Euroopan komissiolle asetuksen 7–10 artiklan mukaisesti;

42 a §

Liikenne- ja viestintäviraston tehtävät

Liikenne- ja viestintäviraston tehtävänä on sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisesti:

2) ilmoittaa *10 §:n mukaisesti ilmoitettuja* sähköisen tunnistamisen järjestelmiä Euroopan komissiolle asetuksen 7–10 artiklan mukaisesti;

Voimassa oleva laki

Ehdotus

*Tämä laki tulee voimaan päivänä kuuta 20 .
Sen 7 b §:n 2 momenttia sovelletaan kuitenkin
vasta 1. päivästä joulukuuta 2023.*

4.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain 16 ja 22 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan henkilötietojen käsittelystä poliisitoimesta annetun lain (616/2019) 16 §:n 1 momentin 15 kohta ja 22 §:n 1 momentin 17 kohta sekä
lisätään 16 §:n 1 momenttiin, sellaisena kuin se on osaksi laeissa 1162/2019, 632/2020 ja 1308/2021, uusi 16 kohta ja 22 §:n 1 momenttiin, sellaisena kuin se on osaksi laissa 632/2020, uusi 18 kohta seuraavasti:

Voimassa oleva laki

Ehdotus

16 §

Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä

Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tietoja rekistereistä siten kuin käytännön menettelyistä asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:

15) rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä; oikeudesta saada tietoja lentoliikenteen matkustajarekisteristä säädetään lentoliikenteen matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden torjunnassa annetussa laissa (657/2019).

22 §

16 §

Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä

Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tietoja rekistereistä siten kuin käytännön menettelyistä asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:

15) rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä; oikeudesta saada tietoja lentoliikenteen matkustajarekisteristä säädetään lentoliikenteen matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden torjunnassa annetussa laissa (657/2019);

16) Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain (/) mukaisesti digitaalisen henkilöllisyydistuksen tuottamiseksi välttämättömistä tiedoista sekä henkilötietojen väärinkäyttöepäilyjen, identiteettivarkauksien tai muiden vastaavien rikosten selvittämiseksi ja näiden ennalta estämiseksi.

22 §

Muu henkilötietojen luovuttaminen viranomaisille

Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:

17) Puolustusvoimille, Tullille, Rajavartiolaitokselle ja Rikosseuraamuslaitokselle näiden palveluksessa olevan, ampuma-aseen kantamiseen virka-, työ- tai palvelustehtävässään oikeutetun henkilön ampuma-aseen kantamista koskevan sopivuuden arvioimista varten.

Muu henkilötietojen luovuttaminen viranomaisille

Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:

17) Puolustusvoimille, Tullille, Rajavartiolaitokselle ja Rikosseuraamuslaitokselle näiden palveluksessa olevan, ampuma-aseen kantamiseen virka-, työ- tai palvelustehtävässään oikeutetun henkilön ampuma-aseen kantamista koskevan sopivuuden arvioimista varten;

18) Digi- ja väestötietovirastolle vain 11 ja 12 §:ssä tarkoitettuja henkilötietoja Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa tarkoitettujen digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin todisteen tuottamista ja hallinnoimista varten.

Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

henkilökorttilain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään henkilökorttilakiin (663/2016) uusi 1 a § seuraavasti:

Voimassa oleva laki

Ehdotus

1 a §

Digitaalinen henkilöllisyystodistus

Henkilökorttiin sisältyy oikeus ottaa käyttöön digitaalisesta henkilöllisyystodistuksesta annetussa laissa (/) tarkoitettu digitaalinen henkilöllisyystodistus.

Mitä 1 momentissa säädetään, ei koske väliaikaista henkilökorttia eikä alle 15-vuotiaalle myönnettyä alaikäisen henkilökorttia.

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 1 a §:ssä tarkoitettua oikeutta ottaa digitaalinen henkilöllisyystodistus käyttöön sovelletaan myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin henkilökortteihin.

6.

Laki

passilain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään passilakiin (671/2006) uusi 3 d § seuraavasti:

Voimassa oleva laki

Ehdotus

3 d §

Digitaalinen henkilöllisyystodistus

Passiin sisältyy oikeus ottaa käyttöön digitaaliseen henkilöllisyystodistuksesta annettussa laissa (/) tarkoitettu digitaalinen henkilöllisyystodistus.

Mitä 1 momentissa säädetään, ei koske väliaikaista passia eikä hätäpassia.

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 3 d §:ssä tarkoitettua oikeutta ottaa digitaalinen henkilöllisyystodistus käyttöön sovelletaan myös ennen tämän lain voimaantuloa myönnettyihin voimassa oleviin passeihin.

7.

Laki

väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annettuun lakiin (661/2009) uusi 6 b luku seuraavasti:

Voimassa oleva laki

Ehdotus

6 b luku

Luonnollisen henkilön tunnistusväline

69 e §

Luonnollisen henkilön tunnistusväline

Digi- ja väestötietoviraston tehtävänä on myöntää luonnollisen henkilön sähköiseen tunnistamiseen tarkoitettua tunnistusvälinettä, 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.

Luonnollisen henkilön tunnistusväline on fyysinen väline, joka on käytettävissä ilman mobiilipäätelaitetta tai sirukorttia.

Digi- ja väestötietovirasto tarjoaa luonnollisen henkilön tunnistusvälinettä sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisena tunnistusvälineenä käytettäväksi tukipalvelulain 3 §:n 1 momentin 4 kohdassa tarkoitetun tukipalvelun välityksellä.

69 f §

Rekisteri luonnollisen henkilön tunnistusvälineistä

Digi- ja väestötietoviraston tehtävänä on ylläpitää luonnollisen henkilön tunnistusvälineen tarjoamista ja tuottamista varten rekisteriä tunnistusvälineistä ja niiden haltijoista.

Rekisteriin voidaan tallentaa tunnistusvälineen haltijan:

1) henkilötiedot, jotka sisältyvät henkilöllisyyden varmentamiseen käytettyyn viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan sekä asiakirjan yksilöintitiedot;

2) henkilötiedot, jotka välitetään henkilöllisyyden varmentamiseen käytetyn sähköisen tunnistusmenetelmän yhteydessä sekä tiedot sähköisestä tunnistusmenetelmästä;

3) 11 a §:n mukainen yksilöintitunnus;

4) tunnistusvälineen yksilöivä tunniste;

5) yhteystiedot;

6) muut kuin 1–5 kohdassa tarkoitetut tunnistusvälineen tarjoamiseksi tarpeelliset tiedot.

Henkilötietojen käsittelystä luonnollisen henkilön tunnistusvälineen palvelutuotannossa, tunnistusvälinettä ja sen käyttöä koskevista vaatimuksista sekä palvelutuotannon ohjauksesta säädetään tukipalvelulain 3–5 luvussa.

69 g §

Hakijan henkilöllisyyden todistaminen

Digi- ja väestötietovirasto myöntää luonnollisen henkilön tunnistusvälineen henkilölle hakemuksesta.

Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoa varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetun komission täytäntöönpanoasetuksen (EU) 2015/1502 liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetty vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai vah-

vasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 kohdassa tarkoitettuun vahvaan sähköiseen tunnistamiseen.

69 h §

Tunnistusvälineen myöntämiseen liittyvien tehtävien hoitaminen yhteispalvelussa

Sen lisäksi, mitä yhteispalvelulain 6 §:ssä säädetään yhteispalvelussa hoidettavista tehtävistä, Digi- ja väestötietovirasto voi antaa tunnistusvälineen myöntämiseen liittyviä avustavia tehtäviä yhteispalvelussa hoidettavaksi. Näihin tehtäviin voi kuulua tunnistusvälineen hakijan tai haltijan henkilöllisyyden todentaminen sekä tunnistusvälineen hakemiseen liittyvät neuvonta- ja tukitehtävät.

Jos yhteispalvelun toimeksisaaja lisäselvitysten jälkeenkään ei voi todentaa hakijan henkilöllisyyttä, on sen siirrettävä asia Digi- ja väestötietoviraston käsiteltäväksi.

69 i §

Tieto passin tai henkilökortin voimassaolosta

Digi- ja väestötietovirastolla on oikeus saada salassapitosäännösten estämättä teknisen rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.

69 j §

Digi- ja väestötietoviraston tiedonantovelvollisuus

Digi- ja väestötietoviraston on ennen tunnistusvälineen myöntämistä annettava hakijalle tiedot:

- 1) tunnistusvälineen käytöstä;
- 2) osapuolten oikeuksista ja velvollisuuksista;
- 3) mahdollisista vastuunrajoituksista; sekä

4) muista kuin 1-3 kohdassa tarkoitetuista mahdollisista tunnistusvälineen käyttöehdoista.

Edellä 1 momentissa tarkoitetut tiedot on annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voi tallentaa ja toisintaa ne muuttumattomina.

69 k §

Digi- ja väestötietoviraston oikeus peruuttaa tai estää tunnistusvälineen käyttö

Digi- ja väestötietovirasto voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:

1) on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;

2) tunnistusväline sisältää ilmeisen virheelisyyden;

3) on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;

4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti käyttöehtojen vastaisella tavalla;

5) tunnistusvälineen haltija on kuollut.

Digi- ja väestötietoviraston tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.

Digi- ja väestötietoviraston on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.

69 l §

Luonnollisen henkilön tunnistusvälineen haltijan velvollisuudet

Luonnollisen henkilön tunnistusvälineen haltijan on käytettävä tunnistusvälinettä käyttöehtojen mukaisesti. Tunnistusvälineen haltijan on säilytettävä tunnistusvälinettä huolellisesti. Tunnistusvälineen haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.

Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

Tunnistusvälineen haltijan on ilmoitettava Digi- ja väestötietovirastolle tunnistusvälineen joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheutonta viivytystä havaittuaan asian.

Digi- ja väestötietoviraston on tarjottava mahdollisuus tehdä 3 momentissa tarkoitettu ilmoitus milloin tahansa. Digi- ja väestötietoviraston on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen. Tunnistusvälineen haltija ei vastaa välineen oikeudettomasta käytöstä Digi- ja väestötietovirastolle tehdyn ilmoituksen jälkeen.

69 m §

Muutoksenhaku

Digi- ja väestötietoviraston päätökseen, joka koskee 69 e §:ssä tarkoitetun luonnollisen henkilön tunnistusvälineen myöntämistä ja 69 k §:ssä tarkoitettuun luonnollisen henkilön tunnistusvälineen peruuttamista saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa.

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Tämä laki tulee voimaan päivänä kuuta 20 .

8.

Laki

hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 ja 9 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016) 3 §:n 1 momentin 4 kohta sekä 9 §:n 1 kohta, sellaisena kuin niistä on jälkimmäinen laissa 1174/2019, seuraavasti:

Voimassa oleva laki

Ehdotus

3 §

Tukipalvelut

Yhteisiä sähköisen asioinnin tukipalveluja ovat:

4) luonnollisen henkilön tunnistuspalvelu, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (533/2016) tarkoitetun tunnistuspalvelun tarjoajan palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle;

3 §

Tukipalvelut

Yhteisiä sähköisen asioinnin tukipalveluja ovat:

4) luonnollisen henkilön tunnistuspalvelu, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) tarkoitetun tunnistuspalvelun tarjoajan palvelua tai väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 6 b luvun mukaista palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle;

9 §

Palvelutuotannossa säännönmukaisesti hyödynnettävät tietolähteet

Digi- ja väestötietovirastolla on oikeus sille tässä laissa säädettyjen tehtävien hoitamiseksi käsitellä seuraaviin tietojärjestelmiin tallennettuja tässä pykälässä tarkoitettuja tietoja noudattaen tätä lukua:

1) väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista anne-

9 §

Palvelutuotannossa säännönmukaisesti hyödynnettävät tietolähteet

Digi- ja väestötietovirastolla on oikeus sille tässä laissa säädettyjen tehtävien hoitamiseksi käsitellä seuraaviin tietojärjestelmiin tallennettuja tässä pykälässä tarkoitettuja tietoja noudattaen tätä lukua:

1) väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista anne-

Voimassa oleva laki

tussa laissa (661/2009) tarkoitetusta väestötietojärjestelmästä henkilön nimeä, henkilötunnusta, sähköistä asiointitunnusta, kansalaisuutta, asiointikieltä, äidinkieltä, kuolinpäivää, edunvalvontaa, toimintakelpoisuuden rajoittamista, edunvalvontavaltuutusta ja lapsen huoltoa koskevia tietoja sekä yhteystietoja ja tietoa turvakiellosta;

Ehdotus

tussa laissa tarkoitetusta väestötietojärjestelmästä henkilön nimeä, henkilötunnusta, sähköistä asiointitunnusta, kansalaisuutta, asiointikieltä, äidinkieltä, kuolinpäivää, edunvalvontaa, toimintakelpoisuuden rajoittamista, edunvalvontavaltuutusta ja lapsen huoltoa koskevia tietoja sekä yhteystietoja ja tietoa turvakiellosta;

Tämä laki tulee voimaan päivänä kuuta 20 .
