



VALTIOVARAINMINISTERIÖ

Sähköinen tunnistaminen

Selvitys nykytilasta sekä kehittämistarpeista

Valtiovarainministeriön julkaisuja – 2019:20



Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja 2019:20

Sähköinen tunnistaminen: Selvitys nykytilasta sekä kehittämistarpeista

Väestörekisterikeskus



Valtiovarainministeriö Helsinki 2019

Valtiovarainministeriö

ISBN PDF: 978-952-367-000-6

Helsinki 2019

Kuvailulehti

Julkaisija	Valtiovarainministeriö	8.3.2019	
Tekijät	Juha Mitrunen, Timo Salovaara, Janne Viskari		
Julkaisun nimi	Sähköinen tunnistaminen: Selvitys nykytilasta sekä -kehittämistarpeista		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2019:20		
Diaari/hankenumero	VM/1699/00.01.00.01/2018	Teema	Julkisen hallinnon ICT
ISBN PDF	978-952-367-000-6	ISSN PDF	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-000-6		
Sivumäärä	53	Kieli	suomi
Asiasanat	tunnistaminen, vahva tunnistaminen, henkilötodistukset, sähköinen hallinto,		
Tiivistelmä	<p>Valtiovarainministeriö pyysi elokuussa 2018 Väestörekisterikeskusta selvittämään, kuinka tunnistautuminen julkishallinnon sähköisiin palveluihin olisi tarkoituksenmukaisinta järjestää. Selvityksen tavoitteena on löytää toimintamalli, jossa sähköinen tunnistaminen julkisen hallinnon palveluihin on mahdollisimman laajasti koko väestön saatavilla syrjimättömästi henkilön iästä tai fyysisistä rajoitteista huolimatta. Kansalaisten lisäksi myös Suomessa asioivien ulkomaalaisten henkilöiden tunnistamisen tulisi olla mahdollista.</p> <p>Sähköinen tunnistaminen jakautuu ensitunnistamiseen sekä tunnistusvälineellä kirjautumiseen asiointipalvelussa. Ensitunnistaminen tapahtuu joko asiointipisteessä, jossa virkailija tarkastaa henkilöllisyyden virallisesta henkilöllisyystodistuksesta, tai sähköisesti, kun kansalainen käyttää jo olemassa olevaa sähköistä tunnistusvälinettään jonkin toisen sähköisen tunnistusvälineen hankkimiseen.</p> <p>Selvitystyön keskeisin kehitysehdotus on ensitunnistamisen uudelleenorganisointi. Kansalaisten ensitunnistaminen voisi kuulua valtion ylläpitämään digitaaliseen perusinfrastruktuuriin. Valtio voisi tarjota sen peruspalveluna muun yhteiskunnan hyödynnettäväksi. Tämä selvitys käsittää kolme vaihtoehtoa sähköisen tunnistamisen toimintamalleiksi sekä ehdotuksen valtion tuottamiksi tunnistamisen peruspalveluiksi.</p>		
Kustantaja	Valtiovarainministeriö		
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi		

Presentationsblad

Utgivare	Finansministeriet	8.3.2019	
Författare	Juha Mitrunen, Timo Salovaara, Janne Viskari		
Publikationens titel	Elektronisk autentisering: Utredning av nuläget samt utvecklingsbehov		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2019:20		
Diarie-/projektnummer	VM/1699/00.01.00.01/2018	Tema	Offentliga förvaltningens ICT
ISBN PDF	978-952-367-000-6	ISSN PDF	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-000-6		
Sidantal	53	Språk	finska
Nyckelord	stark identifiering, identitetskort, e-government		
Referat	<p>I augusti 2018 begärde Finansministeriet att Befolkningsregistercentralen utreder hur identifiering i den offentliga förvaltningens elektroniska tjänster skulle kunna ordnas så ändamålsenligt som möjligt. Målet med utredningen är att hitta en verksamhetsmodell där den elektroniska identifieringen i offentliga förvaltningens tjänster är så tillgängligt som möjligt för hela befolkningen utan diskriminering och oavsett personens ålder eller fysiska begränsningar. Förutom finländska medborgare borde det också vara möjligt att identifiera utländska personer som utträttar ärenden i Finland.</p> <p>Elektronisk identifiering kan delas upp i inledande identifiering och inloggning i en e-tjänst med ett identifikationsverktyg. Den inledande identifieringen sker antingen vid en servicepunkt där en tjänsteman kontrollerar identiteten från ett officiellt identitetsbevis eller elektroniskt då medborgaren använder ett elektroniskt identifikationsverktyg för att skaffa ett annat elektroniskt identifikationsverktyg.</p> <p>Utredningens väsentligaste utvecklingsförslag är omorganisering av den inledande identifieringen. Den inledande identifieringen för medborgare kunde höras till den digitala grundläggande infrastrukturen som upprätthålls av staten. Staten kunde erbjuda den som en bastjänst för samhället att utnyttja. Denna utredning omfattar tre alternativa verksamhetsmodeller för elektronisk identifiering samt ett förslag på bastjänster för identifiering som staten producerar.</p>		
Förläggare	Finansministeriet		
Beställningar/distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi		

Description sheet

Published by	Ministry of Finance		8.3.2019
Authors	Juha Mitrunen, Timo Salovaara, Janne Viskari		
Title of publication	Electronic identification Report on current status and needs for development		
Series and publication number	Publications of the Ministry of Finance 2019:20		
Register number	VM/1699/00.01.00.01/2018	Subject	Public Sector ICT
ISBN PDF	978-952-367-000-6	ISSN PDF	1797-9714
Website address URN	http://urn.fi/URN:ISBN:978-952-367-000-6		
Pages	53	Language	Finnish
Keywords	strong identification, identity documents, electronic government		
<p>Abstract</p> <p>In August 2018, the Ministry of Finance requested that the Population Register Centre investigate how identification for the e-services of public administration could be organised most appropriately. The aim of the investigation was to find an operating model that would make electronic identification for public administration services available to the entire population as widely as possible, without discriminating anyone regardless of their age or physical restrictions. In addition to Finnish citizens, it should also be possible to identify foreigners who use the services in Finland.</p> <p>Electronic identification is divided into initial identification and logging into e-services with a token. Initial identification takes places either at a service point, where an official verifies the person's identity from an official personal identification document, or electronically, when citizens use an existing electronic token to acquire another electronic token.</p> <p>The most important development proposal made in the investigation is the reorganisation of initial identification. Initial identification of citizens could be part of the digital basic infrastructure maintained by central government. Central government could offer it as a basic service for the rest of the society. This report includes three alternative operating models for electronic identification and a proposal for the basic identification services provided by central government.</p>			
Publisher	Ministry of Finance		
Publication sales/ Distributed by	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi		

Sisältö

1	Selvityksen tarkoitus ja toimeksianto	10
2	Yhteenveto kehittämis ehdotuksista	13
2.1	Ehdotus valtion tuottamiksi tunnistamisen peruspalveluiksi	13
2.2	Esitettävät vaihtoehdot tunnistamisen toimintamalleiksi	16
3	Sähköisen tunnistamisen perusteita ja käsitteitä	19
3.1	Henkilön identiteetti ja tiedot	19
3.2	Tunnistaminen ja tunnistusväline	19
3.3	Ensimmäinen tunnistaminen	19
3.4	Varmuustaso	21
3.5	Luottamusverkosto	22
4	Sähköisen tunnistamisen nykytila Suomessa julkisen hallinnon tarpeiden näkökulmasta.....	24
4.1	Yleiset huomiot.....	24
4.2	Kansalaisten yhdenvertaisuus julkisissa palveluissa	25
4.2.1	Saavutettavuus sähköisen tunnistamisen käytössä	26
4.3	Eräiden erityisryhmien sähköinen tunnistaminen	27
4.3.1	Näkö- ja kuulovammaiset sekä kognitiivisista ongelmista kärsivät käyttäjät.....	27
4.3.2	Alaikäiset	28
4.3.3	Ulkosuomalaiset	29
4.3.4	Suomen viranomaisten kanssa asioivat ulkomaalaiset	29
4.3.5	Maahanmuuttajat.....	30
4.4	Julkishallinnon yhteinen välityspalvelu Suomi.fi-tunnistus	30
4.4.1	Suomi.fi-tunnistuksen transaktiomäärät, volyyymiennusteet ja kustannukset	31

5	Yksilökeskeisen tiedonhallinnan kehitysnäkymiä	33
5.1	Käyttäjän kontrolloima identiteetti.....	34
5.2	Hajautettu itsehallittava identiteetti.....	35
5.3	Yksilökeskeisen tiedonhallinnan ja tunnistamisen yhteensovittamisen haaste	35
5.4	Periaatteet datatalouden ja sähköisen tunnistamisen yhteen sovittamiseen	36
6	Kehittämisehdotukset	37
6.1	Ehdotus valtion tuottamiksi maksuttomiksi tunnistamisen peruspalveluiksi	37
6.1.1	Ehdotus valtion mahdollistamaksi ensitunnistamiseksi	37
6.1.2	Ehdotus valtion uudeksi tunnistusvälineeksi	38
6.1.3	Ehdotus valtuutustietojen hyödyntämisestä	41
6.1.4	Ehdotus portaittain vahvistuvasta identiteetistä.....	41
6.1.5	Ehdotus rajat ylittäväksi tunnistamiseksi	42
6.1.6	Ehdotuksen kustannukset	42
6.2	Ehdotukset kolmeksi vaihtoehtoiseksi tunnistamisen toimintamalliksi	45
6.2.1	Vaihtoehto 1: Valtio tarjoaisi tunnistusvälineen vain julkishallinnon käyttöön.....	45
6.2.2	Vaihtoehto 2: Valtio tarjoaisi tunnistusvälineen myös markkinatoimijoiden edelleen välitettäväksi luottamusverkostossa	46
6.2.3	Vaihtoehto 3: Käyttäjän hallinnoima identiteettilompakko.....	48
	LIITE Mobiilin sähköisen tunnistamisen ratkaisumalleja maailmalla	51
1.	Keskitettyt valtion tuottamat sähköisen tunnistamisen järjestelmät	51
2.	BankID-mallit	51
3.	Valtion ja pankkien konsortiot.....	52
4.	Attribuuttien jakoon perustuvat konsortiot	53

ESIPUHE

Suomeen on rakennettu viimeisten kahdenkymmenen vuoden ajan vauhdilla sähköisiä palveluita sekä julkishallintoon että muualle yhteiskuntaan. Eräs julkishallinnon tavoitteista on saada siirrettyä asiointin painopistettä käynti- ja puhelinasiointista sähköiseen asiointikanavaan. Kaikki kansalaiset eivät pysty sähköiseen asiointiin esimerkiksi laitteiden puuttumisen tai fyysisten rajoitteiden vuoksi ja heille on jatkossakin turvattava muita asiointimuotoja. Muille kansalaisille sähköiset palvelut voisivat olla lähtökohtainen valinta – onhan sähköinen palvelukanava avoinna kellon ympäri vuoden jokaisena päivänä, juuri silloin kun asiointi sopii parhaiten kansalaiselle itselleen.

Kaikessa asiointissa keskeistä on se, että voidaan luotettavasti tunnistaa, kuka asioiva kansalainen on. Asiointipisteessä tunnistaminen tapahtuu henkilöllisyystodistuksella ja sähköisessä palvelussa sähköisellä tunnistusvälineellä. Julkishallinnon palveluiden tulee olla kaikille kansalaisille saatavilla yhdenvertaisesti ja ketään syrjimättä. Jotta kaikki kansalaiset olisivat julkisten digipalveluiden edessä tasaveroisessa asemassa, jokaiselle kansalaiselle ikään, varallisuuteen, terveydentilaan ja asuinpaikkaan katsomatta tulisi taata sujuva, helppokäyttöinen, turvallinen ja maksuton tunnistamistapa julkisiin palveluihin.

Julkishallinnon palveluiden tulee olla kaikille kansalaisille saatavilla yhdenvertaisesti ja ketään syrjimättä.

Valtiovarainministeriö pyysi elokuussa 2018 Väestörekisterikeskusta selvittämään vaihtoehtoja, kuinka tunnistautuminen julkishallinnon sähköisiin palveluihin olisi tarkoituksenmukaisinta järjestää. Selvityksen tavoitteena on löytää toimintamalli, jossa sähköinen tunnistaminen julkisen hallinnon palveluihin on mahdollisimman laajasti koko väestön saatavilla syrjimättömästi henkilön iästä tai fyysisistä rajoitteista huolimatta. Selvityksessä otetaan myös kantaa Suomessa asioivien ulkomaalaisten henkilöiden tunnistamiseen. Selvitystyön käynnistymisen jälkeen on samaan

aihepiiriin liittyen myös tullut vireille hallituksen esitys (264/2018 vp) laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta.

Väestörekisterikeskus on työn aikana selvittänyt asiaa laajalti ja eri tulokulmista. Esitettävissä vaihtoehdoissa on pidetty keskeisenä periaatteena, että kansalaisten asiointiin sähköisissä palveluissa tulee olla helppoa ja vaivatonta. Helppo asiointi tarkoittaa, että tunnistusvälineet ovat helposti saatavilla, ja että niiden käyttäminen palveluihin kirjautumiseen on helppoa erilaisissa asiointitilanteissa mukaan luettuna mobiiliasioinnissa. Selvitystyön tukena on ollut valtiovarainministeriön asettama ohjausryhmä ja työn aikana on kuultu laajalti vahvan sähköisen tunnistamisen toimijoita niin yksityiseltä sektorilta, julkishallinnosta kuin etujärjestöistäkin. Työn aikana kartoitettujen eri teknologioiden osalta on pyritty rajaamaan esitettävät vaihtoehdot sellaisiin, joiden kustannukset on arvioitu kokonaistaloudellisesti kestäviksi.

Väestörekisterikeskuksen puolesta kiitän valtiovarainministeriötä mahdollisuudesta kartoittaa vaihtoehtoja sähköisen tunnistamisen järjestämiseksi sekä hyvästä yhteistyöstä ja tuesta selvitystyön aikana. Kiitän myös selvitystyön aikana kuultuja sidosryhmiä aktiivisuudesta, ratkaisuhakuisista ehdotuksista ja rakentavasta kommentoinnista sekä saamastamme tuesta selvitystyötä kohtaan. Kiitos myös kaikille selvitystyöhön osallistuneille Väestörekisterikeskuksen virkamiehille. Erityiskiitokset ansaitsevat pääosan selvitystyöstä ja sidosryhmien haastatteluista tehnyt kehityspäällikkö Juha Mitrunen sekä työtä Väestörekisterikeskuksessa ohjannut johtaja Timo Salovaara. Uskon, että selvitystyömme antaa hyvän pohjan jatkokeskustelulle ja päätöksenteolle, jotta sähköiset tunnistusvälineet saataisiin syrjimättömästi kaikkien kansalaisten saataville, niiden käyttäminen helpommaksi ja julkishallinnon tunnistuskustannukset ennustettavammiksi.

Väestörekisterikeskuksen ylijohtaja

Janne Viskari

1 Selvityksen tarkoitus ja toimeksianto

Vahva sähköinen tunnistaminen tapahtuu Suomessa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009; ”tunnistuslaki”) mukaisessa luottamusverkostossa. Lain mukaan kaikkien vahvaa tunnistamista tarjoavien tai välittävien toimijoiden on kuuluttava luottamusverkostoon. Luottamusverkoston jäsenten on annettava tunnistusvälineensä luottamusverkostossa edelleen välitettäväksi. Lisäksi laissa säädetään enimmäishinnat yhdelle tunnistustapahtumalle sekä tunnistusvälineiden ketjuttamiselle. Ketjuttaminen tarkoittaa sitä, että kansalainen käyttää tunnistusvälinettä jonkin toisen tunnistusvälineen hankkimiseen. Ketjuttamisesta käytetään myös nimitystä sähköinen ensitunnistaminen.

Ensitunnistamisella tarkoitetaan prosessia, jolla kansalainen tunnistetaan luotettavasti ensimmäisen kerran, kun hänelle myönnetään uusi tunnistusväline, kuten pankkitunnukset, mobiilivarmenne tai henkilökortin kansalaisvarmenne. Ensitunnistaminen voi tapahtua asiointipisteessä virallisesta viranomaisen myöntämästä henkilöllisyystodistuksesta tai ketjuttamalla sähköisesti olemassa olevasta tunnistusvälineestä. Ensitunnistamisen luotettava järjestäminen on tärkeää, jotta yleinen luottamus sähköiseen asiointiin käytettäviä välineitä kohtaan ei vaarannu.

Laissa hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) säädetään, että kaikki julkishallinnon toimijat ovat velvoitettuja käyttämään Väestörekisterikeskuksen ylläpitämää Suomi.fi-tunnistusta asiointipalveluissaan, joissa vaaditaan kansalaisten vahvaa tunnistamista. Lain mukaan tunnistustapahtumien vastaanottaminen Suomi.fi-tunnistuksesta on asiointipalveluille maksutonta ja valtio kattaa vahvan tunnistamisen kulut keskitetysti.

Sähköisten tunnistustapahtumien määrän ennakoitaan kasvavan hyvin voimakkaasti lähivuosina.

Tunnistamisen volyymit julkishallinnon palveluissa ovat olleet viime vuosina voimakkaassa kasvussa. Vuonna 2017 tunnistustapahtumia oli julkishallinnon palveluissa 67,8 miljoonaa ja vuonna 2018 tapahtumien määrä nousi jo 81,7 miljoonaan. Valtiolla on myös tahtotila siirtää edelleen asioinnin painopistettä käynti- ja puhelinpalveluasiointista verkkoasiointiin. Tämän myötä sähköisen tunnistamisen tapahtumamäärien ennakoitaan edelleen kasvavan hyvin voimakkaasti.

Luottamusverkoston käynnistymisen (1.5.2017) myötä Väestörekisterikeskus on kilpailuttanut sopimuskokonaisuuden luottamusverkostosta tavoitteenaan saada kaikki tunnistusvälineet käytettäväksi Suomi.fi-tunnistuksessa. Kilpailutuksen keskeisenä tavoitteena oli, että valtion tunnistamisesta maksama hinta ei nousisi nykyisestä, vaikka volyymit ovat kasvussa. Valtiovarainministeriö on varannut tunnistamisen kuluihin enintään 20 miljoonaa euroa neljälle vuodelle 2018–2021. Ensimmäinen kilpailutus toteutettiin syksyllä 2017 dynaamisena hankintajärjestelyinä, jossa tunnistusvälineille pyydettiin kiinteää hintaa yhden vuoden sopimuskaudeksi. Kilpailutuksen lopputulemana valtion maksama kokonaiskustannus olisi noin kaksinkertaistunut, joten Väestörekisterikeskus keskeytti kilpailutuksen mobiilivarmenteiden hankintaa lukuun ottamatta. Väestörekisterikeskus järjesti uuden kilpailutuksen keväällä 2018, jossa haettiin kappalehintaa yhdelle tunnistustapahtumalle. Myös tämän kilpailutuksen lopputulemana oli, että valtion maksama kokonaiskustannus olisi noin kaksinkertaistunut, mikäli kilpailutuksesta olisi hankittu kaikki Suomessa käytössä olevat vahvat tunnistusvälineet. Näiden kahden eri mekanismeilla läpiviedyn kilpailutuksen johtopäätöksenä on, että haetun sähköisen tunnistamisen kustannustason saavuttaminen ilman nykyisen toimintamallin kehittämistä on haastavaa.

Kansalaisten asiointin sähköisissä palveluissa tulee olla helppoa ja vaivatonta.

Korkean kustannustason lisäksi julkishallinnon kannalta erityishaasteena on, että kaikilla kansalaisilla ei ole sähköisiä tunnistusvälineitä. Ylivoimaisesti käytetyin tunnistusväline julkishallinnon palveluissa on pankkitunnus, joilla tehdään 95 % kaikista tunnistamisista. Kilpailu- ja kuluttajaviraston vuonna 2015 tekemän selvityksen mukaan noin 400 000 suomalaisella ei ole pankkitunnuksia. Selvityksen mukaan eri väestöryhmistä eniten pankkitunnuksia on työmarkkinoilla olevilla korkeasti koulutetuilla. Vähiten niitä on iäkkäillä, eläkeläisillä, työttömillä, matalasti koulutetuilla sekä pienituloisilla. Monella näihin väestöryhmiin kuuluvilla on jatkuvaa asiointitarvetta julkishallinnon kanssa. Myös alaikäisillä on itsenäistä asiointitarvetta julkishallinnon kanssa. Julkishallinnon palveluiden tulee kuitenkin olla kaikille kansalaisille saatavilla yhdenvertaisesti ja ketään syrjimättä, mukaan lukien myös ulkomailla pysyvästi tai pitkään asuvat suomalaiset. Kun asiointin painopistettä halutaan siirtää sähköisiin palveluihin, on myös kansalaisten yhdenvertaisuuden toteutumiseen kiinnitettävä entistä enemmän huomiota. Jotta kaikki kansalaiset olisivat julkisten digipalveluiden edessä tasaveroisessa asemassa, jokaiselle kansalaiselle ikään, varallisuuteen, terveydentilaan ja asuinpaikkaan katsomatta tulisi taata sujuva, helppokäyttöinen, turvallinen ja maksuton tunnistamistapa julkisiin palveluihin.

Edellä mainittujen haasteiden ratkaisemiseksi ja mahdollisten vaihtoehtojen kartoittamiseksi valtiovarainministeriö pyysi elokuussa 2018 Väestörekisterikeskusta selvittämään, kuinka tunnistautuminen julkishallinnon sähköisiin palveluihin olisi tarkoituksenmukaisinta järjestää. Selvityksen tavoitteena on ollut sellaisen toimintamallin löytäminen, jossa sähköinen tunnistaminen julkisen hallinnon palveluihin on mahdollisimman laajasti koko väestön saatavilla syrjimättömästi henkilön iästä tai fyysisistä rajoitteista huolimatta. Kansalaisten lisäksi myös Suomessa asioivien ulkomaalaisten henkilöiden tunnistamisen tulisi olla mahdollista. Suomessa asioivien ulkomaalaisten osalta selvitystyö on kytketty Väestörekisterikeskuksen ylläpitämän Katso-palvelun elinkaareen. Tavoitteena on ollut löytää toimintamalli, joka olisi kokonaistaloudellisesti toimivin ja mahdollistaisi yhteneväisen konseptin niin suomalaisten kuin Suomessa asioivien ulkomaalaistenkin tunnistamiseen sekä Katso-palvelun alasajon.

Selvitystyön aikana asiaa on tarkasteltu laajalti. Esitettävissä vaihtoehdoissa on pidetty keskeisenä periaatteena, että kansalaisten asiointiin sähköisissä palveluissa tulee olla helppoa ja vaivatonta. Helppo asiointi tarkoittaa, että tunnistusvälineet ovat paitsi helposti saatavilla, myös että niiden käyttäminen palveluihin kirjautumiseen on helppoa erilaisissa asiointitilanteissa mukaan luettuna mobiiliasioinnissa. Selvitystyön tukena on ollut valtiovarainministeriön asettama ohjausryhmä ja työn aikana on kuultu laajalti vahvan sähköisen tunnistamisen toimijoita yksityiseltä sektorilta, julkishallinnosta ja etujärjestöistä. Selvityksessä esitettävät vaihtoehdot on teknologioiden osalta pyritty rajaamaan sellaisiin, joiden kustannukset on arvioitu kokonaistaloudellisesti kestäviksi.

2 Yhteenvedo kehittämissuhteista

Sähköisen tunnistamisen kokonaisuus jakautuu tunnistusvälinettä hankkivan henkilön ensitunnistamiseen sekä tunnistusvälineen käyttämiseen asiointipalveluun kirjautumisessa. Ensitunnistaminen tapahtuu joko asiointipisteessä, jossa virkailija tarkastaa henkilöllisyyden virallisesta henkilöllisyystodistuksesta, tai sähköisesti, kun kansalainen käyttää jo olemassa olevaa sähköistä tunnistusvälinettään jonkin toisen sähköisen tunnistusvälineen hankkimiseen.

Selvitystyön aikana keskeisimmäksi kehityssuhteeksi nousi ensitunnistamisen uudelleenorganisointi. Useat haastatellut tunnistuspalvelujen tarjoajat esittivät, että kansalaisten ensitunnistaminen voisi kuulua valtion ylläpitämään yhteiskunnan digitaaliseen perusinfrastruktuuriin eli valtio voisi järjestää sen peruspalveluna ja tarjota muun yhteiskunnan hyödynnettäväksi, mikä edistäisi vahvan sähköisen tunnistamisen hyödyntämistä laajemminkin kuin vain julkishallinnon palveluissa. Tämä selvitys käsittää kolme vaihtoehtoa sähköisen tunnistamisen toimintamalleiksi sekä ehdotuksen valtion tuottamiseksi tunnistamisen peruspalveluiksi.

2.1 Ehdotus valtion tuottamiseksi tunnistamisen peruspalveluiksi

Suomen kansalaisille myönnettävien vahvan sähköisen tunnistamisen välineiden ensitunnistaminen pohjautuu poliisin tekemään tunnistamiseen passia tai henkilökorttia myönnettäessä. Väestörekisterikeskus ehdottaa, että jatkossa kansalaisen henkilöllisyys kiinnitettäisiin samassa yhteydessä automaattisesti kyseisen kansalaisen sähköiseen identiteettiin, eli häntä koskeviin mm. väestötietojärjestelmässä oleviin henkilötietoihin. Kansalaiselle luovutettaisiin tällöin passin tai henkilökortin ohella automaattisesti valtion tuottama sähköinen tunnistusväline. Tämä uusi väline olisi ensisijaisesti älypuhelinsovellus. Niille kansalaisille, joilla ei ole älypuhelin, tarjottaisiin samaa taustajärjestelmää hyödyntäen vaihtoehtoinen väline, joka olisi tietokoneen oheislaitteporttiin (USB) liitettävä tunnistustikku. Uusi väline korvaisi nykyisen kansalaisvarmenteen, mikä keventäisi henkilökortin tuotantokustannuksia ja laskisi henkilökortin hintaa Väestörekisterikeskuksen arvion mukaan 5–10 eurolla.



Uutta välinettä voisi käyttää kaikkiin julkishallinnon asiointipalveluihin tunnistamiseen sekä sähköiseen ensitunnistamiseen eli henkilöllisyyden luotettavaan todentamiseen verkon välityksellä jotakin toista tunnistusvälinettä haettaessa. Väestörekisterikeskus ehdottaa, että sähköisen asioinnin vauhdittamiseksi väline olisi budjettirahoitteinen eli kansalaisille sen hakeminen ja käyttäminen olisi maksutonta.

Kansalaisten kannalta tämä helpottaisi sähköisissä palveluissa asiointia usealla tavalla. Sähköisen tunnistusvälineen saisi jatkossa automaattisesti henkilöllisyystodistuksen myöntämisen yhteydessä ilman erillistä hakemusta ja erillistä kustannusta. Julkishallinnon palveluihin tunnistautuminen voitaisiin toteuttaa suoraan kaikkien asiointipalveluiden käyttämään Suomi.fi-tunnistukseen. Tällöin kirjautumisesta saataisiin helpompaa, sillä nykyisessä toimintamallissa olevia ja tarpeettomaksi jääviä välivaiheita poistuisi. Koska uusi tunnistusväline ei pohjautuisi nykyisiin välineisiin, joista monet ovat olleet käytössä jo pitkään, sen kehittämistyössä voitaisiin huomioida nykypäivän vaatimustaso muun muassa mobiiliasioinnille, helppokäyttöisyydelle ja saavutettavuudelle. Kansalaisten asiointi myös yksityisten palveluntarjoajien kanssa helpottuisi. Tällaisella toimintamallilla kansalainen voitaisiin luotettavasti tunnistaa verkon välityksellä ilman, että hänet olisi tarpeen pyytää käymään tunnistautumassa palveluntarjoajan konttorissa esimerkiksi asiakassuhteen avaamista varten.

Kansalainen saisi sähköisen tunnistusvälineen automaattisesti muun asioinnin yhteydessä.

Uuden tunnistusvälineen käyttöönoton nopeuttamiseksi Väestörekisterikeskus ehdottaa harkittavaksi, että siirtymäkauden ajan ensitunnistaminen ja uuden tunnistusvälineen myöntäminen voitaisiin tehdä poliisin lupahallinnon lisäksi sopimusperusteisesti myös muiden valtion virastojen asiointipisteissä, kuten esimerkiksi maistraateissa sekä Verohallinnon, Kelan, Maahanmuuttoviraston ja ulkoasiainhallinnon asiointipis-

teissä. Tämä laajentaisi siirtymäkauden ajaksi asiointipisteverkoston ja lisäisi kansalaisten mahdollisuuksia hankkia uusi maksuton tunnistusväline. Passin ja henkilökortin myöntämisen yhteydessä ensitunnistamisen tekisi kuitenkin aina poliisi.

Nykyisiä luottamusverkossa olevia tunnistusvälineitä, kuten pankkitunnisteita ja mobiilivarmennetta, on siirtymävaiheessa myös mahdollista hyödyntää uuden välineen käyttöönottoisissa ilman tarvetta käydä asiointipisteessä. Lisäksi Väestörekisterikeskus ehdottaa harkittavaksi, voisiko ensitunnistamisen asiointipisteverkoston laajentaa edelleen sopimus pohjaisesti myös yksityisten toimijoiden asiointipisteverkoston. On myös mahdollista, että valtion kannattaisi kilpailuttaa ja hankkia oman välineensä tekninen tuotanto, ylläpito ja käyttäjätuki yksityisiltä toimijoilta. Valtio vastaisi tässäkin tapauksessa tunnistusjärjestelmän kokonaisuudesta mm. lakisääteisten luottavuusvaatimusten toteuttamisen osalta.

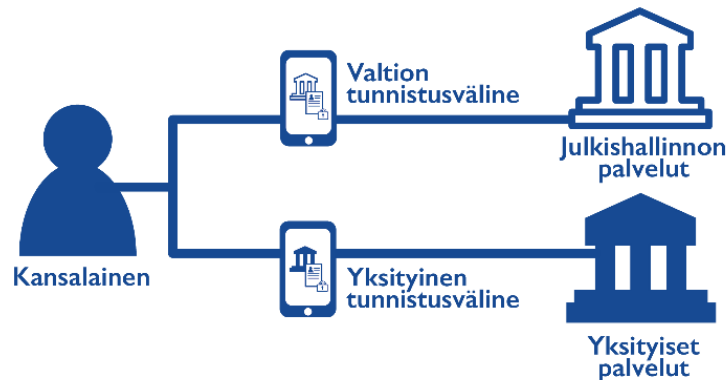
Käyttömahdollisuuksien laajentamiseksi Väestörekisterikeskus ehdottaa lisäksi, että uuteen välineeseen kytkettäisiin saumattomasti ja mahdollisimman helpokäyttöisellä tavalla myös Suomi.fi-valtuuksien kautta saatavat puolesta asioinnin tiedot. Tällä hetkellä palvelusta on saatavilla tieto oikeudesta asioida alaikäisen huollettavan puolesta tai yrityksen puolesta nimenkirjoittajana. Kaikki puolesta asioinnin tiedot ovat saatavilla maksutta. Käyttömahdollisuuksien laajentaminen puolesta asioinnin tiedoilla tarkoittaisi, että kansalainen voisi tunnistusvälineellään automaattisesti hoitaa sähköisesti alaikäisen lapsensa tai yrityksensä asioita niissä asiointipalveluissa, jotka tätä puolesta asioinnin tietoa hyödyntäisivät. Palveluntarjoajien kannalta puolesta asioinnin tiedot olisivat entistä helpommin hyödynnettävissä, mikä saattaisi lisätä puolesta asiointia hyödyntävien asiointipalveluiden määrää.

Valtion tuottamat tunnistamisen peruspalvelut käsittäisivät myös EU:n eIDAS-asetuksen mukaisen vahvojen tunnisteiden välittämisen muiden EU-maiden kanssa. Tällöin Suomen kansalainen voisi käyttää uutta välinettä sellaisenaan myös joissakin muiden EU-maiden sähköisissä palveluissa. Tunnisteiden välittäminen vastaavalla tavalla on myös tarvittaessa mahdollista järjestää sopimus pohjaisesti kahdenvälisesti EU/ETA:n ulkopuolisten maiden kanssa.

Suomessa asioiville ulkomaalaisille sekä ulkosuomalaisille olisi mahdollista rakentaa kokonaan etänä tapahtuva sähköinen ensitunnistaminen (etätodentaminen), jonka avulla uusi väline voitaisiin myöntää automatisoidusti, ja joka ei edellyttäisi käyntiä esimerkiksi Suomen edustustossa. Etätodentaminen ei kuitenkaan olisi yhtä luotettavaa kuin asiointipisteessä tapahtuva ensitunnistaminen, joten etätodentamisen perusteella myönnettävällä tunnistusvälineellä pääsisi ainoastaan joihinkin asiointipalveluihin, kuten esimerkiksi antamaan ulkomaankauppaan liittyviä ilmoituksia Suomen viranomaisille.

2.2 Esitettävät vaihtoehdot tunnistamisen toimintamalleiksi

Vaihtoehdossa 1 valtion tunnistusväline tarjottaisiin vain julkishallinnon omaan käyttöön. Kansalaisen kannalta tämä vaihtoehto tarkoittaisi, että julkishallinnon palveluihin käytettäisiin eri tunnistusvälinettä kuin yksityisiin palveluihin. Jokaisella kansalaisella tulisi tällöin käytännössä olla hallussaan vähintään kaksi eri tunnistusvälinettä. Tässä vaihtoehdossa nykyinen luottamusverkosto säilyisi, mutta valtio poistuisi sieltä väliin tarjoajana ja jättäisi luottamusverkoston toiminnan kokonaisuudessaan yksityisille toimijoille.



Vaihtoehdossa 2 valtion tunnistusvälinettä tarjottaisiin myös yksityisten asiointipalveluiden käyttöön. Kansalaisen kannalta samalla tunnistusvälineellä voisi kirjautua sekä kaikkiin julkishallinnon palveluihin, että todennäköisesti ainakin osaan yksityisistä palveluista. On huomattava, että yksityiset asiointipalvelut voivat itse harkita mitkä tunnistusvälineet ne hyväksyvät omaan palveluunsa eikä niitä voi pakottaa hyväksymään valtion tunnistusvälinettä. Tässä vaihtoehdossa nykyinen luottamusverkosto säilyisi ja sen toiminta painottuisi erityisesti tunnistamisen välityspalveluihin. Valtio ei kuitenkaan välittäisi yksityisiin asiointipalveluihin muita tunnistusvälineitä kuin omaansa. Jos valtion välineen käyttämisestä yksityisissä asiointipalveluissa perittäisiin maksu, sen tulisi olla sidoksissa tuotantokustannuksiin ja sen suuruutta säänneltäisiin maksuasetuksella.



Vaihtoehdossa 3 tunnistusväline laajennettaisiin nykymuotoisen tunnistamisen lisäksi kansalaisen identiteetilompakoksi. Tässä vaihtoehdossa on kuitenkin huomattava, että sen toteuttamisessa on vaihtoehtoja 1 ja 2 enemmän muita, varsinaisten tunnistuspalveluiden ulkopuolella olevia kehittämistarpeita. Tämän vaihtoehdon realistiset toteutumismahdollisuudet ovat siten selvästi pidemmällä aikavälillä. Vaihtoehto 3 ei kuitenkaan ole muita vaihtoehtoja poissulkeva, ja niin haluttaessa se on mahdollista nähdä myös vaihtoehtoa 1 tai 2 jatkokehittävänä pidemmän aikavälin kehityspolkena.



Tässä vaihtoehdossa esitettävä identiteetilompakko voisi sisältää nykyisin henkilön tunnistamiseen käytettävän henkilötunnuksen lisäksi useita erilaisia todentamistietoja ja lupia kuten esimerkiksi ajo- tai aseluvat. Todentamistietoja voisivat olla esimerkiksi, onko henkilö tunnistautunut, onko henkilö täysi-ikäinen, missä henkilö asuu tai onko henkilöllä luottotietomerkintä. Laajempi kirjo todentamistietoja toisi lisää vaihtoehtoja henkilön tunnistamiseen. Joillekin asiointipalveluille voitaisiin esimerkiksi välittää pelkästään tieto, onko henkilö täysi-ikäinen. Henkilötunnuksen väärinkäytösten mahdollisuuden vähenisivät, kun asiointipalveluille toimitettaisiin ainoastaan niiden tarvitsemat todentamistiedot.

Tämä vaihtoehto muuttaisi sähköisen tunnistamisen monimuotoisemmaksi henkilötietojen hallinnaksi ja edellyttäisi OmaData-suostumuksen hallinnan mekanismien rakentamista. Kansalaisen kannalta tämä vaihtoehto tarkoittaisi, että hänen oma päätösvaltansa kasvaisi omien henkilötietojensa luovuttamisesta asiointipalveluiden käyttöön. Palveluihin tunnistautuminen ei tarkoittaisi enää pelkästään henkilön identiteetin todentamista, vaan sen yhteydessä kansalainen voisi itse antaa asiointipalvelulle luvan hyödyntää laajemmin hänen tietojansa ja saisi vastineeksi parempia ja pidemmälle vietyjä palveluita. OmaData-mekanismi takaisi, että halutessaan kansalainen voisi myös peruuttaa antamansa suostumuksen ja voisi olla varma siitä, että asiointipalvelun pääsy hänen tietoihinsa silloin lakkaisi.

Tässä vaihtoehdossa nykymuotoinen luottamusverkosto voisi kehittyä OmaData-opeeraattoriverkostoksi, jonka toiminta keskittyisi erilaisten datapakettien välittämiseen kansalaisen omalla suostumuksella. Valtion roolina olisi luovuttaa julkishallinnon rekistereissä olevaa dataa mukaan luettuna henkilötunnus tai sitä tulevaisuudessa vastaava yksilöivä identiteettitieto.

Tämän vaihtoehdon edellytyksenä on laajamittaisempi rajapintojen rakentaminen erilaisiin julkisen ja yksityisen sektorin henkilötietovarantoihin.

3 Sähköisen tunnistamisen perusteita ja käsitteitä

3.1 Henkilön identiteetti ja tiedot

Vahvan sähköisen tunnistamisen perustana on valtion virallisessa väestörekisterissä, väestötietojärjestelmässä, digitaalisessa muodossa ylläpidettävät henkilön identiteettiä koskevat tiedot, joista myös tunnistamisen kannalta oleellinen on henkilön yksilöivä henkilötunnus. Asiointipalveluille tarjottavassa tunnistuspalvelussa on käytännössä ja yksinkertaistetusti kysymys siitä, että tunnistuspalvelu ilmoittaa käyttäjällä olevaa tunnistusvälinettä hyödyntäen asiointipalvelulle käyttäjän henkilötunnuksen. Henkilön sähköiseen identiteettiin voidaan sähköisesti ja henkilötunnusta yhdistämisen avaimena käyttäen liittää selkeästi todennettavissa olevaa, muista lähteistä peräisin olevaa tietoa.

3.2 Tunnistaminen ja tunnistusväline

Vahvalla sähköisellä tunnistamisella tarkoitetaan luonnollisen henkilön yksilöimistä ja tälle annettun tunnisteiden aitouden ja oikeellisuuden todentamista sähköisellä menetelmällä eli tunnistusvälineellä, joka täyttää sähköistä tunnistamista ja luottamuspalveluja koskevassa EU-säätelyssä määritellyt korotetun tai korkean varmuustason vaatimukset.

Tunnistusvälineen luotettavuuteen liittyy useita eri osatekijöitä, kuten itse tunnistusväline teknisine ja turvaominaisuuksineen, välineen rekisteröintiprosessi ja ensitunnistamisen tapa sekä tunnistuksen välityskerroksen ominaisuudet. Tunnistusvälineen luotettavuuden taso määräytyy varmuustasoltaan heikoimman osatekijän mukaiseksi. On siis mahdollista, että kaksi samalla teknisellä ratkaisulla toteutettua tunnistusvälinettä ovat varmuustasoltaan erilaisia.

3.3 Ensitunnistaminen

Ensitunnistamisella tarkoitetaan tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä. Vahvasta sähköisestä tunnistamisesta ja

sähköisistä luottamuspalveluista annetuin lain (617/2009; ”tunnistuslaki”) mukaan ensitunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Tunnistusvälineen hakijan henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, joita ovat valtion myöntämä passi tai henkilökortti, tai toiseen, henkilön käytössä jo olevaan vahvaan sähköiseen tunnistusvälineeseen. Käytännön sovellutuksena viime mainittu tarkoittaa, että esim. mobiilivarmenteen luomisen ja myöntämisen yhteydessä ensitunnistaminen voidaan tehdä sähköisessä palvelussa käyttäen pankkitunnuksia. Tätä sähköisen tunnistusvälineen hyödyntämistä toisen sähköisen tunnistusvälineen luomisessa sanotaan ensitunnistamisen ketjuttamiseksi.

Suomessa hyväksytään tunnistautumisen välineeksi fyysisessä tunnistamistilanteessa passi ja henkilökortti, joista molemmat myöntää poliisi. Prosessissa poliisi varmistaa väestötietojärjestelmästä, että kyseinen henkilö on olemassa ja elossa, sekä hakee järjestelmästä passiin tai henkilökorttiin merkittävät tiedot kuten henkilön etu- ja sukunimen. Mikäli henkilö ei aikaisemmin ole saanut passia tai henkilökorttia, tai edellisestä sormenjälkien ottamisesta on enemmän kuin kuusi vuotta, hänen on tultava asiomaan henkilökohtaisesti poliisin lupapalvelupisteeseen, missä häneltä otetaan sormenjäljet. Lisäksi henkilön on käytävä valokuvaamossa, joka lähettää passikuvan sähköisesti poliisille. Liittämällä henkilön kuva passiin tai henkilökorttiin, mahdollistetaan henkilön tunnistus toisaalla tätä dokumenttia käyttäen. Henkilökortin tapauksessa luodaan lisäksi digitaaliset varmenteet, joiden avulla henkilö voi tunnistautua sähköisesti ja luoda sähköisiä allekirjoituksia.



Passia tai henkilökorttia käyttämällä voidaan tunnistaa henkilö asiointipisteessä ja myöntää hänelle jokin sähköinen tunnistusväline, esimerkiksi pankkitunnuksset.

3.4 Varmuustaso

Tunnistuslaissa määritellyt vahvan sähköisen tunnistamisen menetelmien luokittelut korotettu ja korkea varmuustaso perustuvat EU:n ns. eIDAS-asetuksen täytäntöönpanosäädöstöön, joka luokittelee sähköisen tunnistamisen menetelmät kolmelle eri varmuustasolle:

- matala
- korotettu
- korkea

Julkishallinnon sähköisten asiointipalveluiden tunnistaminen on keskitetty Väestörekisterikeskuksen tuottamaan Suomi.fi-tunnistukseen. Suomi.fi-tunnistuksen käyttövolyymista 99,4 % perustuu korotetulle tasolle rekisteröityihin tunnisteisiin (pankkitunnukset 95,3 %, mobiilivarmenteet 4,1 %). Korkealle tasolle rekisteröityjen Väestörekisterikeskuksen myöntämien varmenteiden, eli henkilökortin kansalaisvarmenteen sekä terveydenhuollon ammattikorttien ja muiden viranomaisten käyttämien organisaatiokorttien varmenteiden, osuus käyttövolyymista on 0,6 %.

Valtion myöntämiä korkean varmuustason tunnistusvälineitä voidaan käyttää Suomi.fi-tunnistuksen välityksellä sähköisessä asiointissa pankkien ja operaattorien tarjoamien tunnistusvälineiden rinnalla kaikissa julkisen hallinnon sähköisissä asiointipalveluissa. Mikäli sähköiseen asiointipalveluun edellytetään korkean tason tunnistusvälineitä, ovat valtion tarjoamat varmenteet toistaiseksi ainoita välineitä Suomessa, jotka täyttävät korkean varmuustason vaatimukset. Lisäksi useissa julkishallinnon sisäisissä tietojärjestelmissä hyödynnetään tai edellytetään korkean tason välineellä tehtyä tunnistamista sekä allekirjoitusta.

Kaikissa kansalaisille suunnatuissa asiointipalveluissa riittää korotetun varmuustason vaatimukset täyttävät tunnistusvälineet, jotka ovat myös kustannustehokkaampia tuottaa ja ylläpitää. Johtopäätös edellä todetusta on, että mahdollinen valtion uusi tunnistusväline kannattaisi toteuttaa korotetun varmuustason vaatimusten mukaisesti.

Valtion myöntämiä sosiaali- ja terveydenhuollon ammattihenkilöiden toimikortille asennettuja varmenteita hyödynnetään laajasti terveydenhuollon järjestelmissä, joissa varmennekortille myönnetyllä varmenneparilla ratkaistaan sekä vahva tunnistaminen että sähköisen reseptin myöntämiseen ja osaan potilasasiakirjamerkinnöistä lakisääteisesti vaadittava kehittynyt sähköinen allekirjoitus. Mahdollisella henkilökortin kansalaisvarmenteesta hallitusti luopumisella ei saa olla mitään negatiivisia vaikutuksia virka- ja ammattivarmenteiden tuotannolle ja jatkuvalla tuelle.

Väestörekisterikeskuksen myöntämiä sähköiseen asiointiin soveltuvia tunnistusvälineitä oli 31.1.2019 voimassa yhteensä 1 050 850 kpl. Näillä välineillä tunnistauduttiin julkisen hallinnon sähköisiin asiointipalveluihin vuoden 2018 aikana Suomi.fi-tunnistuksen kautta 548 376 kertaa, eli noin 0,5 kertaa välinettä kohden. Osa näistä tunnistuksista on tehty henkilökortin kansalaisvarmenteella ja osa terveydenhuollon ammatilaisen tai viranomaisen organisaatiokortin varmenteella.

Varmuustasojen määrittelyn ja soveltamisen taustalla on ajatus siitä, että myös ”täydellisen” turvallisen menetelmän lisäksi joissakin käyttötarkoituksissa hyväksyttäviä ovat vähemmän turvalliset menetelmät, mikäli riski on kohtuullinen ja oikeasuhtainen verrattuna menetelmän käytöstä saatavaan hyötyyn.

Mikäli tunnistusvälineellä voi olla erilaisia varmuustasoja, voivat myös tunnistusvälineen haltijan sähköisten palvelujen käytön mahdollisuudet olla vaihteittain vahvistettavissa. Tunnistusväline voidaan myöntää ensin heikommalla varmuustasolla ja vahvistaa myöhemmin pelkästään uusimalla välineen niin sanottu rekisteröintiprosessi, eli tekemällä haltijan ensitunnistaminen uudelleen, mutta vahvemmallalla menetelmällä. Käytännössä kysymyksessä voisi olla esimerkiksi tilanne, jossa myönnetty tunnistusväline on saavuttanut korotetun varmuustason etäpalveluna. Kun tunnistusvälineen haltija käy ensitunnistautumassa välineen tarjoajan toimipisteessä kasvotusten, tunnistusvälineen varmuustaso voidaan ao. vaatimukset täyttäviä menettelyjä soveltaen nostaa korkealle tasolle. Itse tunnistusvälinettä ei tarvitse uusia.

3.5 Luottamusverkosto

Suomen kansallisen vahvan tunnistamisen palveluntarjoajien muodostaman luottamusverkoston perusteista on säädetty toukokuun 2017 alussa voimaan tulleilla vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009; ”tunnistuslaki”) muutoksilla.

Tunnistuslain mukaan kaikkien markkinaehtoisesti vahvaa tunnistamista tarjoavien (”tunnistusvälineen tarjoajat”) tai välittävien (”tunnistusvälityspalvelun tarjoajat”) toimijoiden on kuuluttava luottamusverkostoon. Luottamusverkoston jäsenten on annettava liikkeelle laskemansa tunnistusväline luottamusverkostossa edelleen välitettäväksi. Laissa määritellään myös yksittäisen tunnistustapahtuman kattohinta, joka on tällä hetkellä 0,10 euroa. Eduskunnassa on käsiteltävänä tunnistuslain muutos (HE 264/2018 vp), jonka mukaan kattohinta laskettaisiin 0,03 euroon ja se laajennettaisiin koskemaan myös sähköistä ensitunnistamista eli olemassa olevaan vahvaan sähköiseen tunnistusvälineeseen perustuvan tunnistusvälineiden ketjuttamisen hintaa.

Tunnistuslain mukaan kaikkien markkinaehtoisesti vahvaa tunnistamista tarjoavien ("tunnistusvälineen tarjoajat") tai välittävien ("tunnistusvälityspalvelun tarjoajat") toimijoiden on kuuluttava luottamusverkostoon. Luottamusverkoston jäsenten on annettava liikkeelle laskemansa tunnistusväline luottamusverkostossa edelleen välitettäväksi. Laissa määritellään myös yksittäisen tunnistustapahtuman kattohinta, joka on tällä hetkellä 0,10 euroa. Eduskunnassa on käsiteltävänä tunnistuslain muutos (HE 264/2018 vp), jonka mukaan kattohinta laskettaisiin 0,03 euroon ja se laajennettaisiin koskemaan myös sähköistä ensitunnistamista eli olemassa olevaan vahvaan sähköiseen tunnistusvälineeseen perustuvan tunnistusvälineiden ketjuttamisen hintaa.



Luottamusverkostolle asetettuja tavoitteita kuten kilpailun lisääntymistä, uusien tunnistusratkaisujen saataville tuloa sekä kustannussäästöjä ei ole vielä saavutettu. Sopimusneuvottelut tunnistuspalveluita tarjoavien osapuolten välillä ovat olleet käynnissä huomattavan pitkään, eivätkä luottamusverkoston rakenteille asetetut odotukset tunnistuspalvelujen hankkimiseen ja kilpailuttamiseen helpottumisesta ole vielä toteutuneet. Vireillä olevalla tunnistuslain muutoksella onkin hintasääntelyn muutosten lisäksi tarkoitus selkeyttää luottamusverkostoon kuuluvien palveluntarjoajien sopimusketjovelvoitteita sekä ensitunnistamisen ketjuttamiseen liittyvää vastuusääntelyä.¹

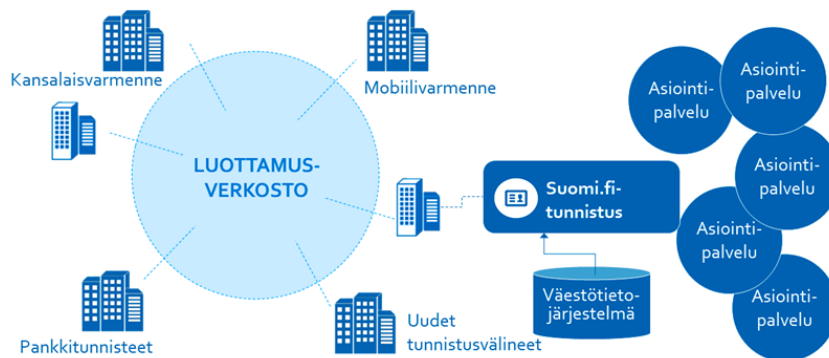
¹ Perusteellisempi ja täsmällisempi selvitys luottamusverkostosta löytyy mainitun hallituksen esityksen (HE 264/2018 vp) perusteluista.

4 Sähköisen tunnistamisen nykytila Suomessa julkisen hallinnon tarpeiden näkökulmasta

4.1 Yleiset huomiot

Suomen valtio on suurin ja ainoa volyymillisesti merkittävä vahvan sähköisen tunnistamisen palvelun tarjoajien asiakas. Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016) nojalla julkishallinnon sähköisiin asiointipalveluihin tunnistautumiseen on käytettävä Suomi.fi-tunnistusta.

Vuonna 2018 Suomi.fi-tunnistuksen kautta välitettiin 81,7 miljoonaa tunnistustapahtumaa julkisen hallinnon asiointipalveluille, mistä VRK maksoi tunnistuspalvelujen tuottajille yhteensä noin 4,1 miljoonaa euroa. Vuonna 2017 palvelun kautta välitettyjen tunnistustapahtumien kokonaismäärä oli 67,8 miljoonaa. Tunnistustapahtumien määrä on ollut nopeassa kasvussa julkishallinnon toimijoiden laajentaessa sähköisten asiointipalvelujen tarjontaa ja kasvun oletetaan jatkuvan myös tulevana vuosina voimakkaana, erityisesti mikäli sähköisen viestinvälityksen palvelun hyödyntämistä koskevat tavoitteet toteutuvat.



Vahvan sähköisen tunnistamisen palvelujen hyödyntäminen muissa yksityisen sektorin asiointipalveluissa kuin verkkopankki- ja sähköisen maksamisen palvelussa on Suomessa kehittynyt heikosti. Tunnistustlain muuttamista koskevan hallituksen esityk-

sen (HE 264/2018 vp) eduskuntakäsittelyn puitteissa annetussa asiantuntijalausunnossa² on esitetty arvio, jonka mukaan vahvan tunnistamisen palvelun käytön volyymi on näissä muissa yksityissektorin palveluissa alle viisi miljoonaa tapahtumaa vuodessa. Tätä voidaan pitää yhtenä keskeisenä suomalaisen vahvan tunnistamisen palvelujen ekosysteemin epäkohtana. Myös yritykset sekä niiden asiakkaat hyötyisivät oleellisesti turvallisten sähköisten asiointipalvelujen käytön yleistymisestä. Pidättäytyminen vahvan tunnistuksen käyttämisestä johtuu tyypillisesti kustannussyistä. Samalla pidättäytyminen kuitenkin lisää identiteettivarkauksien sekä petosten riskiä, mikä toteutuessaan aiheuttaa taloudellisia menetyksiä ja sähköisten palvelujen käytön edellytyksenä olevan kuluttaja-asiakkaiden luottamuksen rapautumista.

4.2 Kansalaisten yhdenvertaisuus julkisissa palveluissa

Yhdenvertaisuus on perusoikeus, josta on säädetty Suomen perustuslaissa: ihmiset ovat yhdenvertaisia lain edessä, eikä ketään saa ilman hyväksyttävää perustetta asettaa eri asemaan sukupuolen, iän, alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella.

Yhdenvertaisuuslaki (1325/2014) velvoittaa viranomaisia ryhtymään tarvittaviin toimenpiteisiin yhdenvertaisuuden toteutumisen edistämiseksi. Viranomaisen on tehtävä asianmukaiset ja kulloisessakin tilanteessa tarvittavat kohtuulliset mukautukset, jotta vammainen tai muuten toimintarjoitteinen henkilö voi mm. asioida yhdenvertaisesti muiden kanssa viranomaispalveluissa. Lain noudattamista valvova yhdenvertaisuusvaltuutettu on toimivaltansa puitteissa kiinnittänyt huomiota mm. sähköisen tunnistamisen välineiden saatavuuteen sekä saavutettavuuteen (maahanmuuttajat, näkövammaiset henkilöt).

Kaikilla kansalaisilla tulee olla tasavertaiset mahdollisuudet käyttää digitaalisia palveluja.

Viranomaisten ja muiden toimijoiden tarjoamien palvelujen saavutettavuus on osa perustuslaissa säädetyn yhdenvertaisuuden toteuttamista³. Digitaalisten palvelujen saa-

² FISC ry:n asiantuntijalausunto Eduskunnan talousvaliokunnalle 14.12.2019. Asiantuntijalausunto on julkinen valiokunnan annettua lausuntonsa.

³ Perusteellisempi ja täsmällisempi katsaus saavutettavuuden tavoitteiden ja keinojen kannalta relevanttiin lainsäädäntöön sisältyy HE 60/2018 vp yleisperusteluihin.

vutettavuudesta annettu EU:n direktiivi on tarkoitus toimeenpanna Suomessa lailla digitaalisten palvelujen tarjoamisesta, jota koskeva hallituksen esitys on eduskunnan käsiteltävänä (HE 60/2018 vp). Uudella lailla pyritään varmistamaan kaikille tasaveritaiset mahdollisuudet käyttää digitaalisia palveluja riippumatta kuulo- tai näkökyvystä, motorisista vaikeuksista tai muista toimintarajoituksista. Lakisääteisten saavutettavuusvaatimusten noudattaminen mahdollistaa ja helpottaa lain esitöiden mukaan 5–10 prosenttia väestöstä tuloa digitaalisten palvelujen käyttäjiksi. Laki sisältää EU-sääntelyyn perustuvien saavutettavuusvaatimusten lisäksi myös muita digitaalisten palvelujen mm. tietoturvallisuuteen ja yleiseen helppokäyttöisyyteen liittyviä vaatimuksia, joita sovelletaan viranomaisten digitaalisten palvelujen lisäksi myös luottamusverkostossa tarjottaviin vahvan sähköisen tunnistamisen palveluihin.

Oleellinen viranomaistoimintaa koskeva vaatimus on hallintolaissa (434/2003) säädetty palveluperiaate. Verkkosivut ja digitaaliset asiointipalvelut ovat osa viranomaisien palvelujen kokonaisuutta, jota järjestettäessä tulee kiinnittää huomiota palvelujen riittävyteen ja saatavuuteen sekä hallinnossa asioivan valinnanvapauteen. Palvelujen saatavuutta ei tulisi rajoittaa ilman asiallisesti hyväksyttäviä perusteita. Kaikille palveluja tarvitseville, myös erityisryhmille, olisi pyrittävä turvaamaan yhtäläinen mahdollisuus asioidensa hoitamiseen palvelutarpeesta riippumatta.

4.2.1 Saavutettavuus sähköisen tunnistamisen käytötapauksessa

Tunnistuspalvelua tulee tarkastella kokonaisuutena, jonka saavutettavuuteen vaikuttaa tunnistusvälineen ja sen käyttöliittymän lisäksi mm. ensitunnistamisen prosessin toteutus, mahdollisesti tarvittavien sovellusasennusten sujuvuus, käyttäjätuki ja neuvonta sekä toimiminen poikkeustilanteissa (esimerkkinä tunnistusvälineen kadottaminen). Puhelintuki näkövammaiselle, selkeät toimintaohjeet ja palvelukanavat verkkopalvelussa puhelinpalvelun lisäksi kuulovammaiselle, sekä tarvittavien tietojen toimitaminen esteettömässä muodossa ovat muutamia esimerkkejä tunnistuksen kokonaispalvelussa huomioitavista saavutettavuusasioista.

Digitaalisten asiointipalveluiden käytössä saavutettavuutta voidaan osaltaan edistää myös Suomi.fin Valtuudet-palvelun avulla, joka mahdollistaa toisen henkilön puolesta asioimisen.

4.3 Eräiden erityisryhmien sähköinen tunnistaminen

Mahdollisuus vahvan sähköisen tunnistamisen käyttöön avaa mahdollisuudet hyödyntää viranomaisten ja muiden toimijoiden tarjoamia digitaalisia asiointipalveluja. Tunnistusvälineen saatavuudella sekä saavutettavuudella on merkitystä hallinnon asiakkaiden yhdenvertaisuuden sekä palveluperiaatteen käytännön toteutumisen kannalta. Oleellista on sekä tunnistusvälineen että siihen liittyvän kokonaispalvelun toteutus saavutettavasti. Ilman saavutettavia tunnistusvälineitä potentiaaliset ja halukkaat asiakkaat eivät pysty käyttämään digitaalisia palveluja.

Seuraavaksi eritellään muutamia selvityksessä tunnistettuja henkilöryhmiä, joiden saatavilla ei ole vahvan sähköisen tunnistamisen välineitä, tai välineiden käytännön saatavuudessa tai saavutettavuudessa on merkittäviä haasteita.

4.3.1 Näkö- ja kuulovammaiset sekä kognitiivisista ongelmista kärsivät käyttäjät

Nykytilassa vahvan tunnistuksen välineiden saatavuus ja käyttömahdollisuus näkö- ja kuulovammaisille sekä kognitiivisista ongelmista kärsiville käyttäjille vaihtelee tunnistusvälineen tarjoajasta riippuen erityisesti kun tarkastellaan tunnistusta kokonaispalveluna.

Sokealle tai heikkonäköiselle käyttäjälle itse tunnistusväline ja siihen liittyvät tiedot, kuten henkilökohtainen PIN-koodi tai asennettava sovellus, voivat olla vaikeita tai jopa mahdottomia käyttää. Tunnistusvälineet ja tunnistuspalveluiden käyttöliittymät eivät välttämättä tue teknisesti saavutettavuutta kuten toimivuutta ruudunlukuhjelmilla sokeille käyttäjille. Palveluiden käytön ohjeet, tuki ja käyttöönotto voivat olla vaikeaselkoisia tai tietoja ei ole tarjolla selkokielellä. Lisäksi itse tunnistusväline tai siihen liittyvät tiedot voidaan toimittaa esteellisellä tavalla, kuten PIN-koodin toimittaminen paperikirjeellä sokealle asiakkaalle, ja toimimiseen poikkeustilanteissa ei välttämättä ole tarjolla esteetöntä palvelukanavaa. Esimerkiksi tuki voi olla tarjolla vain puhelinpalveluna, jota kuuro ei voi käyttää.

Riippumatta valittavasta etenemistavasta tulee tunnistuspalvelun toteutuksessa kiinnittää erityistä huomiota kokonaispalvelun saavutettavuuteen kaikkien esteellisten käyttäjien näkökulmasta. Saavutettavuusdirektiivi ja sen kansallinen toimeenpano tuovat osaltaan sääntelyä sähköisten palveluiden ja mm. tunnistusvälineiden käyttöliittymien toteuttamiseen saavutettaviksi, mutta eivät yksinään takaa tunnistamisen kokonaispalvelun saavutettavuutta.

Tunnistuspalvelun toteutuksessa tulee kiinnittää erityistä huomiota kokonaispalvelun saavutettavuuteen kaikkien esteellisten käyttäjien näkökulmasta.

Lähtökohtaisesti tunnistuspalvelun tulee olla kokonaisuudessaan tarjolla kaikille käyttäjille ja poikkeustilanteissa digitaalisten palveluiden käyttö voidaan mahdollistaa Suomi.fi-valtuuksien avulla (sähköinen puolesta asiointi).

4.3.2 Alaikäiset

Täysi oikeustoimikelpoisuus on vain 18 vuotta täyttäneillä. Rajoitettu oikeustoimikelpoisuus on alle 18-vuotiailla ns. oman omaisuuden suhteen. Vahvan sähköisen tunnistuspalvelun tarjoajat ovat lähestyneet tätä haastetta hieman erilaisilla riskiarvioilla ja esim. määrittämällä alaikärajoja, jota nuoremmille lapsille ei anneta vahvan tunnistuksen välinettä edes huoltajien suostumuksella. Henkilökortti on huoltajien suostumuksella kaikenikäisten lasten saatavilla, mutta sen käyttöön sähköisenä tunnistusvälineenä liittyvät käytännön haasteet korostuvat tässä käyttäjäryhmässä.

Pääsääntöisesti vahvaa sähköistä tunnistamista edellyttävissä asioissa alaikäistä edustaa eli digitaalista palvelua käyttää tämän puolesta huoltaja. Ongelmia syntyy niissä palveluissa, joissa tietosuojasyistä on rajattu huollettavan puolesta asioinnin tai tietojen katselun oikeuksia. Paljon huomiota saanut käyttötapaus on valtakunnallinen terveystietojen verkkopalvelu Omakanta, jossa huoltaja ei voi katsoa 10 vuotta täyttäneen huollettavansa tietoja, tai tehdä tämän puolesta suostumuksia terveystietojen jakamisesta. Kun 10 vuotta täyttäneellä huollettavalla ei kuitenkaan yleisesti ottaen ole palvelun käytön edellyttämää vahvan sähköisen tunnistamisen välinettä, estyy digitaalisen palvelun käyttö kokonaisuudessaan ja saatavilla oleva palvelu on fyysinen asiointi terveydenhuollon toimintayksikössä.

Alaikäisen helppokäyttöiselle, älypuhelimessa toimivalle vahvan sähköisen tunnistamisen välineelle on todennäköistä käyttöpotentiaalia, mikäli tällainen väline olisi saatavilla. Esimerkki kohtuullisen luotettavaa tunnistamista edellyttävästä lapsille ja nuorille tarkoitettusta digitaalisesta palvelusta on koulujen oppilastietojärjestelmä. Yleiskäyttöisen tunnisteen hyödyntäminen helpottaisi ja suoraviivaistaisi käyttäjä- ja pääsynhallinnan toimintoja, kun esimerkiksi koulun tai paikkakunnan vaihto ei edellyttäisi uusien tunnisteen luomista ja toimittamista lapsen sekä tämän huoltajien tietoon paperikirjeenä.

Lasten ja nuorten kohdalla tunnistusvälineen varmuustason vaiheittainen nostaminen saattaisi olla hyödyllinen ominaisuus. Välineen voisi esimerkiksi luoda aluksi matalalle

tasolle huoltajan tunnistusvälinettä hyödyntäen ja nostaa myöhemmin korotetulle tasolle, kun lapselle haetaan passia tai henkilökorttia.

4.3.3 Ulkosuomalaiset

Ulkosuomalaiset eli ulkomailla asuvat Suomen kansalaiset rekisteröidään väestötietojärjestelmään. Siten heillä on suomalainen henkilötunnus ja mahdollisuus saada Suomen passi tai henkilökortti, joita hyödyntämällä heillä on mahdollisuus saada myös sähköinen tunnistusväline. Ulkosuomalaisilla ei kuitenkaan aina ole ulkomailla asumisen kestosta ja muusta henkilöhistoriastaan riippuen asiakassuhdetta suomalaiseen pankkiin tai teleoperaattoriin, jotka tarjoavat tunnistusvälineitä. Tällaisten henkilöiden saatavilla olevana vaihtoehtona tunnistusvälineeksi on vain henkilökortti. Ulkosuomalaisten erityishaasteena saattaa kuitenkin olla pääsy Suomen ulkoasiainhallinnon asiointipisteeseen, josta henkilökorttia voi hakea.

Väestörekisterikeskus toteuttaa kuluvan vuoden 2019 aikana järjestelmän henkilötunnuksettomien ulkomaalaisten sähköistä tunnistamista varten. Tämä etänä tapahtuvan ensitunnistamiseen tukeutuva järjestelmä voisi olla laajennettavissa käytettäväksi myös ulkosuomalaisten sähköisen tunnistamisen ratkaisuna.

4.3.4 Suomen viranomaisten kanssa asioivat ulkomaalaiset

Suomalaisissa julkisen hallinnon sähköisissä asiointipalveluissa asioi myös ulkomailla asuvia ulkomaiden kansalaisia sellaisten yritysten puolesta, joita ei ole rekisteröity Suomessa. Erityisesti Verohallinnolla ja Tullilla on tähän erityisryhmään kuuluvia asiakkaita, ja hoidettavissa asioissa saattaa olla kysymys suuristakin taloudellisista arvoista.

Tähän ryhmään kuuluville henkilöille ei ole tarjolla luottamusverkoston tunnistusvälineisiin perustuvaa tapaa tunnistautua, koska heillä ei ole suomalaista henkilötunnusta eikä suomalaisen pankin tai mobiilioperaattorin asiakkuutta, eikä heille myöskään voi myöntää suomalaista henkilökorttia.

Puuttuvan tunnistusvälineen ja sähköisen identiteetin eli väestötietojärjestelmästä annetun henkilötunnuksen sekä siihen liitettyjen henkilön ominaisuustietojen puuttumisen vuoksi Suomi.fi-valtuudet ei myöskään voi valtuuttaa henkilöä asioimaan jonkun yrityksen puolesta, koska henkilöllä tosiasiallisesti olevaa valtuutusta ei voida liittää mihinkään Suomessa hyväksyttävään sähköiseen identiteettiin.

EU/ETA-alueen kansalaisille tarjottava eIDAS-tunnistuksen välitys ratkaisee osan tästä ongelmasta tulevien vuosien aikana, mutta järjestelyn kehitys on osoittautunut hitaaksi ja sen edetessäkin Euroopan ulkopuoliset alueet jäävät edelleen vaille ratkaisua.

4.3.5 Maahanmuuttajat

Maahanmuuttajat ovat sähköisen tunnistamisen kannalta haasteellinen erityisryhmä Suomeen tulon ja Suomeen asettumisen elämäntilanteessa. Maahanmuuttajat voivat saada vahvan sähköisen tunnistusvälineen vasta, kun henkilölle on myönnetty suomalainen henkilötunnus.

Väestörekisterikeskuksessa toteutettavana oleva ulkomaalaisten erillinen tunnistusjärjestelmä voisi soveltua myös maahanmuuttajien ja näille tarkoitettuja palveluja tuottavien viranomaisten tarpeisiin. Suomeen muuttamassa oleva henkilö voisi saada tunnistusvälineen jo ulkomailla ollessaan ja jatkaa sen käyttöä saumattomasti Suomeen muutettuaan. Myös maahanmuuttajien tapauksessa etätodentamiseen perustuvaa ensitunnistusta hyödyntävä sähköisen tunnistamisen järjestelmä olisi erityisen käyttökelpoinen.

Erityisesti maahanmuuttajille tarkoitetun tunnistusratkaisun yhteyttä ja integroitumista väestötietojärjestelmään tulisi selvittää tarkemmin, koska samat henkilöt saavat myöhemmässä vaiheessa henkilötunnuksen ja voivat tällöin saada myös sähköisen tunnistusvälineen.

4.4 Julkishallinnon yhteinen välityspalvelu Suomi.fi-tunnistus

Vahvojen tunnistustapahtumien välittämisestä julkisen hallinnon asiointipalveluihin säädetään laissa hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016), jonka mukaan kaikki julkishallinnon toimijat ovat veloitettuja käyttämään Väestörekisterikeskuksen tuottamaa Suomi.fi-tunnistusta niissä asiointipalveluissaan, joissa vaaditaan kansalaisten vahvaa tunnistamista.

Lain mukaan tunnistustapahtumien vastaanottaminen Suomi.fi-tunnistuksesta on asiointipalveluille maksutonta ja valtio maksaa vahvan tunnistamisen palvelujen käytön maksut keskitetysti. Hallinnollisesti tämä on järjestetty niin, että Väestörekisterikeskukselle on myönnetty käyttö- ja kirjausoikeus valtion talousarvion momentille, jolta

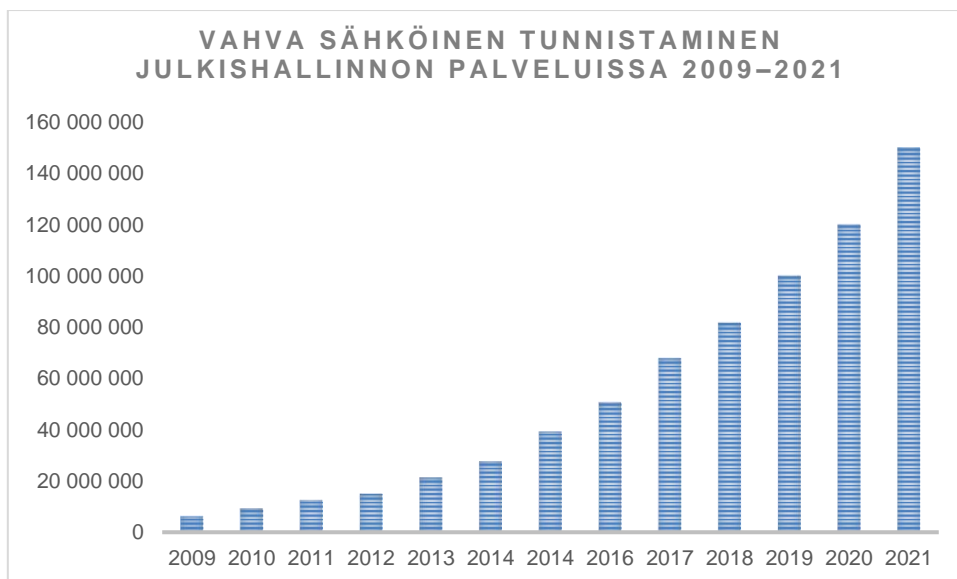
suoritetaan tunnistuspalvelujen ja tunnistusvälityspalvelujen käytön maksut. Tunnistuspalvelujen keskitetty hankinta on tuottanut huomattavia tehokkuushyötyjä julkishallinnon tunnistuspalvelujen sopimus- ja maksuliikennehallinnassa: Väestörekisterikeskuksella on tällä hetkellä sopimus noin kymmenen palveluntarjoajan kanssa, kun aikaisemmin tarvittiin yli 1 000 yksittäisen asiointipalvelun ja tunnistuspalvelun tuottajan välistä sopimusta.

4.4.1 Suomi.fi-tunnistuksen transaktiomäärät, volyyymiennusteet ja kustannukset

Tunnistamisen volyymit julkishallinnon palveluissa ovat olleet viime vuosina voimakkaassa kasvussa, minkä taustalla on valtion pyrkimys kasvattaa sähköisen asioinnin osuutta kaikesta asioinnista. Myös yleinen datatalouden ja digitalisaation aiheuttama muutos vaikuttaa asiointipalveluiden kehittämiseen tunnistuksen tapahtumamääriä kasvattavaan suuntaan.

Vuonna 2018 Suomi.fi-tunnistus välitti 81,7 miljoonaa tunnistustapahtumaa julkishallinnon asiointipalveluihin. Tunnistustapahtumista 95,3 % tehtiin pankkitunnuksilla, 4,1 % teleoperaattorien mobiilivarmenteilla ja 0,6 % henkilökortin kansalaisvarmenteella tai terveydenhuollon ammattikorttien ja muiden viranomaisten käyttämien organisaatiokorttien varmenteilla.

Tällä hetkellä voimassa olevien tunnistuspalvelujen hankintasopimusten yksikköhintojen (painottamaton) keskiarvo on 5,7 senttiä. Eri välineiden toteutuneilla käyttöosuuksilla painotettuna ja ennakoituilla käytön volyyymeilla tunnistuspalvelujen käytön kustannukset olisivat vuonna 2019 kokonaisuudessaan 5,3 miljoonaa euroa, eli tarkoitukseen osoitettu käyttö- ja kirjausoikeus on lähitulevaisuudessa osoittautumassa liian niukaksi.



5 Yksilökeskeisen tiedonhallinnan kehitysnäkymiä

Tunnistetun henkilön sähköiseen identiteettiin voidaan liittää muista lähteistä peräisin olevaa tietoa. Sähköisen tunnistamisen lisäpalvelujen asiayhteydessä henkilöön liitettävissä olevaa ja todennettavaa tietoa kutsutaan usein attribuutiksi. Muuttumattomia tai lähes muuttumattomia attribuutteja ovat esimerkiksi henkilön syntymäaika tai sormenjäljet. Muutettavissa olevia ovat esimerkiksi asuinpaikka, puhelinnumero tai luotokortin numero.

Organisaatioilla on hallussaan erilaista informaatiota samasta henkilöstä. Siten sähköinen identiteetti vaikkapa pankin, vakuutusyhtiön tai verotoimiston asiointipalvelun näkökulmasta on erilainen osajoukko tietoja samasta henkilöstä. Organisaation keräämät ja todentamat henkilötiedot eivät useinkaan ole käytettävissä ulkopuolisille tahoille, jotka voisivat ja haluaisivat hyödyntää omassa liiketoiminnassaan näitä tietoja, vaikka kyseinen henkilö itsekin niin haluaisi.

Kansalaisella tulisi olla mahdollisuuksia hallita henkilötietojensa liikuttamista sekä seurata ja kontrolloida tiedon elinkaarta.

Datatalouden kehitys perustuu osittain erilaisiin tekoälyn avulla tuotettaviin palveluihin. Mitä enemmän tekoälyllä on käytettävissään tarkkaa, laadukasta dataa, sen laadukkaampaa palvelua sen avulla pystyy tuottamaan. Erityisesti todennetun tiedon saatavuuden edistymisen voi olettaa vauhdittavan digitalisaatiota sekä mahdollisuuksia innovoida uudenlaisia digitaalisia palveluita.

Koska henkilön identiteettiä määrittävä tieto on myös henkilön tietoa, henkilöllä tulisi olla mahdollisuuksia hallita tuon tiedon liikuttamista sekä seurata ja kontrolloida tiedon elinkaarta. Kansalainen ei enää ole vain jonkun sähköisen tiedonkäsittelyprosessin kohde, vaan prosessin sisällä toimiva tiedontuottaja. Kansalaisen mahdollisuuksia päättää omien tietojensa jakamisesta tulisi vahvistaa.

Henkilöä koskeviin tietoihin perustuvan digitalisaation kiihtyminen sekä tarve lisätä kansalaisen hallintaa omaan sähköiseen identiteettiinsä ohjaavat sähköisen tunnistamisen liiketoimintamallien, tunnistusvälineen toiminnallisuuksien ja tunnistuspalveluun liittyvien taustajärjestelmien kehittymistä. Liiketoimintamallit sähköisessä tunnistamisessa muuttuvat samalla, koska niiden puitteissa syntyvä lisäarvo on erilaista kuin ennen.

Keskitetyn sähköisen tunnistamisen ja rakentumassa olevan ohjelmointirajapintojen laajaan hyödyntämiseen perustuvan ns. API-talouden yhteensovittaminen vaatii tunnistusratkaisulta ja tunnistusekosysteemiltä muutoksia. Attribuuttien jakajan on myös tunnistettava loppukäyttäjä ja loppukäyttäjän tulee luvittaa attribuuttien jako.

Attribuuttien välittämiseen tulisi kiinnittää samalla tavoin huomiota kuin tunnistuksen välittämiseen. Myös attribuuttien välittämisessä tulisi huomioida attribuuttien hinnoittelu, välitysprotokollat ja käyttäjän oikeudet hallinnoida henkilökohtaisten attribuuttien välittämistä. Attribuuttien välittämisen ekosysteemi ei ole erillinen, tunnistamisesta irrotettavissa oleva ekosysteemi.

World Economy Forumin pankeille tekemä laaja selvitys (Blueprint for Digital Identity, 2016) pyrki osoittamaan, että attribuuttien välittäminen ja tunnistaminen ovat tulevaisuudessa käytännössä sama asia. Keskitetystä tunnistuspalvelun hallinnoimasta identiteettimallista siirrytään World Economy Forumin mukaan tulevaisuudessa käyttäjän itsensä hallinnoimaan hajautettuun identiteettimalliin.

5.1 Käyttäjän kontrolloima identiteetti

Sähköiset tunnistusjärjestelmät olivat aluksi keskitettyjä, luotetun myöntäjän hallinnoimia järjestelmiä. Vuoteen 2005 tullessa käyttäjälle pyrittiin antamaan tunnistus-ekosysteemeissä enemmän vaikutusvaltaa sähköisen tunnistusvälineensä hallinnassa ja siirryttiin yhden myöntäjän mallista kohti avoimempia ekosysteemejä. Tunnistusväline on yhä useammin käyttäjän kontrolloima, mutta edelleen keskitetyn tunnistusvälineen myöntäjän myöntämä. Käyttäjän suostumus, avoimet rajapinnat ja attribuutit ovat tulleet osaksi uusia teknologioita ja metodeja, kuten OpenID (2005), OpenID 2.0 (2006), OpenID Connect (2014), OAuth (2010) ja FIDO (2013).

Käyttäjän kontrolloima identiteetti on kehityksen valtavirtaa maailmalla, joista esimerkkejä ovat FacebookID ja GoogleID. Facebook ja Google ovat identiteetin myöntäjiä, jotka tarjoavat käyttäjille käyttäjähallintaa myöntämäänsä identiteettiin. Tunnistusta pahtumalla ei ole välttämättä hintaa, koska käyttäjä ”maksaa” tunnisteensa ylläpidon ja käytön omalla attribuuttidatallaan, jota tunnisteiden myöntäjä saa vapaasti hyödyntää. Toteutusten läpinäkymättömyys ja käyttäjän tosiasiallisen kontrollin puute on herättänyt voimakastakin kritiikkiä.

Myös sähköistä identiteettiä kuluttajille maakohtaisesti ylläpitävissä konsortioissa, kuten Verimi Saksassa, on yleistymässä käyttäjän kontrolloiman identiteetin malli. Ve-

rimi tarjoaa konsortion jäsenille keskitettyjä alustapalveluita sähköiseen tunnistamiseen, henkilön todentamiseen ja attribuuttien jaon luvittamiseen ja suostumuksenhallintaan.

5.2 Hajautettu itsehallittava identiteetti

Itsehallittavan identiteetin (engl. self-sovereign identity, SSI) mallissa luonnollinen henkilö omistaa ja hallinnoi itse omia henkilötietojaan OmaData-periaatteen mukaisesti. Hänellä on käytettävissään omia henkilötietoja sisältävä rekisteri, josta voidaan hakea tiettyjä seikkoja taikka esittää väitteitä tai varmennettavia väitteitä käyttäjän identiteetistä. Käyttäjällä on omien tietojensa osalta nykyistä suurempi vapaus ja vastuu.

Tiedon vastaanottaja voi olla varma käyttäjän toimittaman henkilötiedon totuudenmukaisuudesta ja luotettavuudesta siinä tapauksessa, että ne pohjautuisivat luotettujen kolmansien tahojen varmennettuihin väitteisiin. Tällaisia tietoja voisivat Suomessa olla esimerkiksi henkilötunnus ja muut henkilöä koskevat väestötietojärjestelmän tiedot, yliopiston tutkintotodistus, yksityisen koulutustoimijan pätevyyssodistus tai ajo-oikeuden voimassaolo. Käyttäjä voisi myös itse lisätä yksinkertaisia, käyttäjän itsensä parhaiten varmennettavissa olevia tietoja kuten sähköpostiosoitteen tai puhelinnumeron. Identiteettiin liitetyt eri tavoin varmennetut attribuutit ovat tallessa henkilön omassa suojatussa identiteetilompakossa (engl. identity wallet).

Tunnistamisen toimintamallit ja ekosysteemi muuttuvat, kun identiteetin hallintamalli muuttuu. Attribuutteja hallinnoivat tai todentavat tahot korvaavat tunnistusvälineitä myöntäneet tahot.

5.3 Yksilökeskeisen tiedonhallinnan ja tunnistamisen yhteensovittamisen haaste

Oleellinen osa identiteettiattribuutteja rajautuu pois ekosysteemin käytöstä, jos datatalouden rakennusmateriaalina käytettävissä olevat kansalaisen todennetut attribuutit rajoittuvat pelkästään tunnistuspalvelun tarjoajalla oleviin attribuutteihin.

Attribuuttien jakoa ja suostumuksenhallintaa tulisi tarkastella tekoälyä, riskienhallintaa ja alustataloutta mahdollistavana toimintona siten, että attribuuttien jako olisi mahdollista muillekin ekosysteemin toimijoille kuin pelkästään tunnistusvälineen tarjoajalle. Lopullisena tavoitteena olisi sitten käyttäjän itsehallittava identiteetti.

5.4 Periaatteet datatalouden ja sähköisen tunnistamisen yhteen sovittamiseen

- Kansalaisen näkökulmasta olisi sujuvaa hallita suostumuksia OmaDataan keskitetyn portaalin kautta. Hallintaportaali voi toimia joko ainoastaan valtionhallinnossa välitettävien attribuuttien suostumuksenhallintaan tai kaikkeen kansalaisen luvittamaan attribuuttidatan välittämiseen.
- Käytettävän teknologian olisi tuettava OmaDatan suostumuksenhallintaa sekä standardeja API-rajapintoja ja välitysprotokollia, jotka mahdollistavat myös mobiilisovellusten suoraviivaisen käyttöönoton asiointipalvelun sovelluksissa.

Kansallisen sähköisen tunnistusratkaisun tulisi olla ominaisuuksiltaan sellainen, että se siirtyy saumattomasti vaihe vaiheelta uuteen malliin. Arkkitehtuuri, ekosysteemi, teknologia ja näitä ohjaava sääntely tulisi rakentaa siten, että ne tukevat vaiheittaista siirtymistä tulevaisuudessa hajautettuun identiteetin hallintaan.

6 Kehittämiss ehdotukset

6.1 Ehdotus valtion tuottamiksi maksuttomiksi tunnistamisen peruspalveluiksi

6.1.1 Ehdotus valtion mahdollistamaksi ensitunnistamiseksi

Suomen kansalaisille myönnettävien vahvan sähköisen tunnistamisen välineiden ensitunnistaminen pohjautuu poliisin tekemään tunnistamiseen passia tai henkilökorttia myönnettäessä. Väestörekisterikeskus ehdottaa, että jatkossa kansalaisen henkilöllisyys kiinnitettäisiin samassa yhteydessä automaattisesti kyseisen kansalaisen sähköiseen identiteettiin. Kansalaiselle luovutettaisiin tällöin passin tai henkilökortin ohella automaattisesti valtion tuottama käyttövalmis sähköinen tunnistusväline. Tämä uusi väline olisi ensisijaisesti älypuhelinsovellus. Niille kansalaisille, joilla ei ole älypuhelinlaite, tarjottaisiin samaa taustajärjestelmää hyödyntäen vaihtoehtoinen väline, joka olisi tietokoneen oheislaiteporttiin (USB) liitettävä tunnistustikku.

Uutta välinettä voisi käyttää kaikkiin julkishallinnon asiointipalveluihin tunnistamiseen sekä sähköiseen ensitunnistamiseen eli henkilöllisyyden luotettavaan todentamiseen verkon välityksellä jotakin toista tunnistusvälinettä haettaessa. Väestörekisterikeskus ehdottaa, että sähköisen asiointin vauhdittamiseksi väline olisi budjettirahoitteinen eli kansalaisille sen hakeminen ja käyttäminen olisi maksutonta.

Valtion tarjoama tunnistuspalvelu olisi yksityissektorille mahdollistava peruspalvelu.

Kansalaisten kannalta tämä helpottaisi sähköisissä palveluissa asiointia usealla tavalla. Sähköisen tunnistusvälineen saisi jatkossa automaattisesti passin tai henkilökortin myöntämisen yhteydessä ilman erillistä hakemusta ja erillistä kustannusta. Julkishallinnon palveluihin tunnistaminen voitaisiin toteuttaa suoraan kaikkien asiointipalveluiden käyttämään Suomi.fi-tunnistukseen, jolloin kirjautumisesta saataisiin poistettua nykyisessä toimintamallissa olevia ja tarpeettomaksi jääviä välivaiheita. Koska väline ei pohjautuisi nykyisiin välineisiin, joista monet ovat olleet käytössä jo pitkään, sen

kehittämistyössä voitaisiin huomioida nykypäivän vaatimustaso muun muassa mobiili-asiointille, helppokäyttöisyydelle ja saavutettavuudelle. Kansalaisten asiointi myös yksityisten palveluntarjoajien kanssa helpottuisi. Tällaisella toimintamallilla kansalainen voitaisiin luotettavasti tunnistaa verkon välityksellä ilman, että kansalainen olisi tarpeen pyytää käymään tunnistautumassa palveluntarjoajan konttorissa esimerkiksi asiakassuhteen avaamista varten.

Uuden tunnistusvälineen käyttöönoton nopeuttamiseksi Väestörekisterikeskus ehdottaa harkittavaksi, että siirtymäkauden ajan ensitunnistaminen ja uuden tunnistusvälineen myöntäminen voitaisiin tehdä poliisin lupahallinnon lisäksi sopimusperusteisesti myös muiden valtion virastojen asiointipisteissä, kuten esimerkiksi maistraateissa sekä Verohallinnon, Kelan, Maahanmuuttoviraston ja ulkoasiainhallinnon asiointipisteissä. Tämä laajentaisi siirtymäkauden ajaksi asiointipisteverkostoa ja lisäisi kansalaisten mahdollisuuksia hankkia uusi maksuton tunnistusväline. Passin ja henkilökortin myöntämisen yhteydessä ensitunnistamisen tekisi kuitenkin aina poliisi.

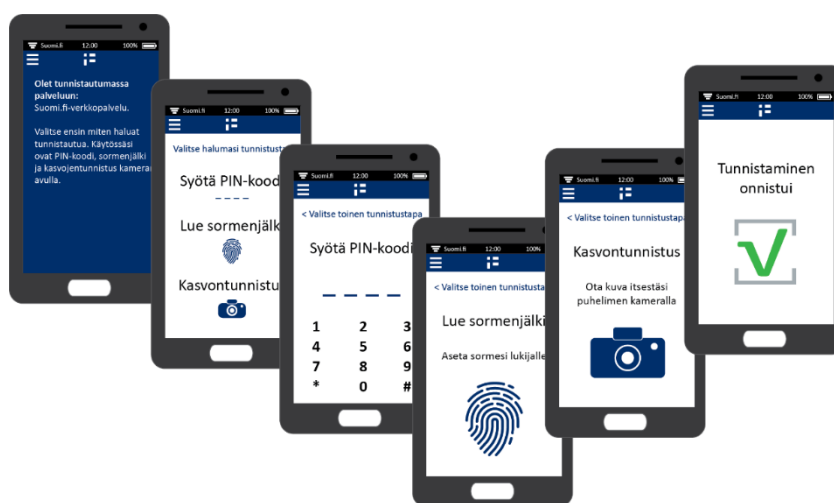
Nykyisiä luottamusverkossa olevia tunnistusvälineitä, kuten pankkitunnisteita ja mobiilivarmennetta, on siirtymävaiheessa myös mahdollista hyödyntää uuden välineen käyttöönottamisessa ilman tarvetta käydä asiointipisteessä. Lisäksi Väestörekisterikeskus ehdottaa harkittavaksi, voisiko ensitunnistamisen asiointipisteverkostoa laajentaa edelleen sopimus pohjaisesti myös yksityisten toimijoiden asiointipisteverkoston. On myös mahdollista, että valtion kannattaisi kilpailuttaa ja hankkia oman välineensä tekninen tuotanto, ylläpito ja käyttäjätuki yksityisiltä toimijoilta.

Palveluun olisi myös mahdollista rakentaa kokonaan etänä tapahtuva sähköinen ensitunnistaminen (etätodentaminen), jonka avulla uusi väline voitaisiin myöntää automatisoidusti, ja joka ei edellyttäisi henkilökohtaista käyntiä asiointipisteessä. Etätodentaminen ei kuitenkaan olisi yhtä luotettavaa kuin asiointipisteessä tapahtuva ensitunnistaminen, joten etätodentamisen perusteella myönnettävällä tunnistusvälineellä pääsisi ainoastaan joihinkin asiointipalveluihin, kuten esimerkiksi ilmoittamaan ulkomaankauppaan liittyviä ilmoituksia Suomen viranomaisille. Etätodentaminen olisi hyödyllistä erityisesti Suomessa asioiville muiden maiden kansalaisille, joille voitaisiin myöntää automatisoidusti tunnistusväline, jolla pääsisi joihinkin suomalaisiin viranomaispalveluihin. Korkeampaa varmuustasoa vaativiin palveluihin ei kuitenkaan pääsisi ennen kuin henkilö olisi korottanut ensitunnistamisensa varmuustasoa esimerkiksi käymällä Suomen ulkoasiainhallinnon asiointipisteessä.

6.1.2 Ehdotus valtion uudeksi tunnistusvälineeksi

Julkishallinnon palveluiden tulee olla kaikille kansalaisille saatavilla yhdenvertaisesti ja ketään syrjimättä. Kun asioinnin painopistettä halutaan siirtää sähköisiin palveluihin,

myös kansalaisten yhdenvertaisuuden toteutumiseen sähköisissä palvelukanavissa tulee kiinnittää entistä enemmän huomiota. Jotta voidaan varmistaa, että julkishallinnon erityispiirteitä vastaavat tunnistusvälineen ominaisuudet ja käyttökokemus voidaan tuottaa, välineen ominaisuuksien määrittely ja tiekartta tulisi olla valtion omassa hallinnassa. Välineen taustajärjestelmän teknistä tuotantoa sen sijaan ei olisi välttämätöntä hoitaa valtion toimesta, vaan se olisi mahdollista hankkia kilpailutettunakin.



Tilastokeskuksen vuonna 2017 tekemän tutkimuksen mukaan jo 71 % kaikesta netti-asiointista tapahtui älypuhelimilla ja tableteilla. Siten uuden välineen suunnittelun lähtökohtana on, että se on suunniteltu ensisijaisesti mobiililaitteilla käytettäväksi. Käytännössä tämä tarkoittaa, että välineen käyttämisen tulee olla sujuvaa älypuhelimilla ja tableteilla.

Ensisijaisesti uusi väline olisi älypuhelinsovellus, jonka kansalainen voisi ladata maksutta sovelluskaupoista, joita ovat Google Play Android-laitteille sekä App Store iPhoneille ja iPadille. Jotta käyttökokemus julkishallinnon palveluihin kirjautumisessa olisi mahdollisimman sujuvaa, olisi selvitettävä kannattaisiko uusi tunnistusväline kehittää ominaisuudeksi jo olemassa olevaan Suomi.fi-mobiilisovellukseen. Tällöin kansalaisen ei tarvitsisi ladata sovelluskaupasta yhtä sovellusta tunnistamiseen ja toista viestinvälitykseen viranomaisten kanssa.

Älypuhelinsovellukseen olisi myös mahdollista kehittää erilaisia viranomaisten yhteistyössä kehitettäviä lisäominaisuuksia. Se voisi esimerkiksi toimia myös mobiilihenkilökorttina, jossa olisi sähköisen ajokortin tapaisia fyysisessä maailmassa tapahtuvan tunnistamisen ja henkilöllisyyden todentamisen toiminnallisuuksia.

Niille kansalaisille, joilla ei ole älypuhelinlaite, tarjottaisiin samaa taustajärjestelmää hyödyntäen vaihtoehtoinen väline, joka olisi tietokoneen oheislaitteporttiin (USB) liitettävä

tunnistustikku. Tämä toteutettaisiin selainkäyttöisenä ja käyttövalmiina siten, että välineen käyttäminen ei edellyttäisi kansalaiselta ajureiden tai ohjelmistojen asennusta ja se toimisi sellaisenaan myös julkisissa tiloissa olevissa tietokoneissa kuten esimerkiksi kirjastoissa. On kuitenkin huomattava, että julkisissa tiloissa olevissa tietokoneissa ei välttämättä ole näkyvillä USB-porttia. Julkisia tiloja varten olisi myös mahdollista tuottaa erillinen, ulkoasultaan tunnistustikun kanssa yhteneväinen ulkoinen lukijalaite, mikä auttaisi kansalaista hahmottamaan, että tunnistustikku on tarkoitettu käytettäväksi sen kanssa.



Tavoitteena on helppokäyttöinen, turvallinen ja helposti käyttöön otettava tunnistusratkaisu jokaiselle kansalaiselle. Välineen ja sen palvelukonseptin suunnittelun perusteina tulisi olla:

- Käyntiasiointina tapahtuvan ensitunnistamisen asiointipisteverkosto olisi oltava mahdollisimman laaja ja koko maan kattava.
- Välineen hakemisen, jakelun, ensitunnistamisen ja käyttöönoton olisi oltava mahdollista myös sähköisesti ja paikkariippumattomasti.
- Välineen käyttämisen tulisi olla mahdollista ilman, että päätelaitteisiin tarvitsee tehdä mitään käyttäjälle monimutkaisia tai totutuista poikkeavia toimenpiteitä, kuten luotettujen varmenteiden määrittelyä tai lisälaitteiden tai niitä ohjaavien sovellusten asentamista.
- Välineen käyttöönoton ja käytön olisi oltava kaikilta osiltaan helppoa ja intuitiivista.
- Tarvittavaa tukea välineen käyttöön mahdollisten ongelmien ilmetessä olisi oltava saatavilla sekä verkon välityksellä että käyntiasiointina.
- Välineen tulisi toimia saumattomasti mobiililaitteen kanssa, jolla käytetään vahvaa tunnistusta edellyttävää asiointipalvelua.
- Välineen tulisi täyttää saavutettavuuteen liittyvien EU:n ja kansallisen sääntelyn vaatimukset ja sen kielivaihtoehtoina tarjotaan suomi, ruotsi ja englanti.

- Välineen tulisi toimia saumattomasti yhteen Suomi.fi-tunnistuksen kanssa.
- Välineen hankkimisen ja käyttämisen tulisi olla kansalaiselle maksutonta, jotta vähäisetkään maksut eivät muodostuisi esteeksi sähköisten palvelujen käytölle.
- Väline tulisi voida antaa myös sellaisten henkilöiden käyttöön, joilla ei ole suomalaista henkilötunnusta, kuten Suomessa asioiville muiden maiden kansalaisille.
- Välineen myöntämisessä tulisi voida soveltaa useita erilaisia ensitunnistamisen menettelyitä. Välineen tulisi ensisijaisesti olla korotetun varmuustason väline, mutta ensitunnistamisessa käytetystä menetelmästä riippuen sen varmuustasona tulisi voida olla korotetun tason sijaan myös joko matala tai korkea.

6.1.3 Ehdotus valtuutustietojen hyödyntämisestä

Käyttömahdollisuuksien laajentamiseksi Väestörekisterikeskus ehdottaa, että uuteen tunnistusvälineeseen kytkettäisiin saumattomasti ja mahdollisimman helppokäyttöisellä tavalla myös Suomi.fi-valtuuksien kautta saatavat puolesta asiointin tiedot. Tällä hetkellä palvelusta on saatavilla tieto oikeudesta asioida alaikäisen huollettavan puolesta tai yrityksen puolesta nimenkirjoittajana. Kaikki puolesta asiointin tiedot ovat saatavilla maksutta. Käyttömahdollisuuksien laajentaminen puolesta asiointin tiedoilla tarkoittaisi, että kansalainen voisi tunnistusvälineellään automaattisesti hoitaa sähköisesti alaikäisen lapsensa tai yrityksensä asioita niissä asiointipalveluissa, jotka tätä puolesta asiointin tietoa hyödyntäisivät. Palveluntarjoajien kannalta puolesta asiointin tiedot olisivat entistä helpommin hyödynnettävissä, mikä saattaisi lisätä puolesta asiointia hyödyntävien asiointipalveluiden määrää.

6.1.4 Ehdotus portaittain vahvistuvasta identiteetistä

Portaittain vahvistuva identiteetti tarkoittaa, että samaa tunnistusvälinettä voidaan käyttää eri varmuustasoisena. Tällöin käyttäjän identiteetti ja asiointihistoria eri palveluissa pysyvät linkitetynä samaan tunnistusvälineeseen. Jos välineen hankinnassa on hyödynnetty matalan varmuustason ensitunnistusta, kuten etätodentamista, välineellä pääsisi ainoastaan sellaisiin palveluihin, jotka eivät vaadi korkeampaa varmuustasoa. Esimerkiksi kunnallisen tenniskentän varaamiseen voisi riittää matalan varmuustason väline, mutta sillä ei pääsisi vaikkapa hakemaan Kelalta etuuksia. Matalalle varmuustasolle haetun välineen voisi halutessaan myöhemmin korottaa korkeammalle varmuustasolle, kunhan huolehditaan eri tasoisten välineiden riittävästä eriyttämisestä niin, että niiden käyttöön liittyvät erilaiset vastuut ja ehdot ovat selkeät ja läpinäkyvät niin välineen haltijalle kuin sitä käyttäen tehtyyn tunnistukseen luottavalle osapuolelle.

Vahvistuva identiteetti hyödyttäisi erityisesti ryhmiä, jotka nykyjärjestelmässä eivät välttämättä saa sähköisiä tunnistusvälineitä lainkaan. Tällaisia ryhmiä ovat muun muassa alaikäiset, Suomessa asioivat muiden maiden kansalaiset sekä henkilöt, joiden iästä, nimestä ja syntymäpaikasta ei ole täyttä varmuutta.

6.1.5 Ehdotus rajat ylittäväksi tunnistamiseksi

Valtion tuottamat tunnistamisen peruspalvelut käsittäisivät myös EU:n eIDAS-asetuksen mukaisen vahvojen tunnisteiden välittämisen muiden EU-maiden kanssa. Tällöin Suomen kansalainen voisi käyttää uutta välinettä sellaisenaan myös joissakin muiden EU-maiden sähköisissä palveluissa. Tunnisteiden välittäminen vastaavalla tavalla on myös tarvittaessa mahdollista järjestää sopimus pohjaisesti kahdenvälisesti EU/ETA -alueen ulkopuolisten maiden kanssa.

EU:n sisällä rajat ylittävän tunnistamisen mahdollistaja on solmupisteverkosto. Jokaisessa EU-maassa on tunnistamisen solmupiste, jonka kautta välitetään muiden maiden vahvoja tunnistamistapahtumia. Suomen solmupistettä ylläpitää Väestörekisterikeskus ja se on toteutettu Suomi.fi-tunnistuksen yhteyteen. Uusi tunnistusväline suunniteltaisiin solmupisteverkostossa välitettäväksi, jolloin kansalaiset voisivat käyttää sitä myös joissakin muiden EU-maiden palveluissa. On kuitenkin huomattava, että solmupisteverkostosta huolimatta tulee vielä kestävänsä vuosia ennen kuin eri EU-maiden tunnistusvälineet toimivat kattavasti myös muiden maiden asiointipalveluissa.

EU:n solmupisteverkosta täydentävä ratkaisumalli olisi tehdä maiden välisiä luottamus sopimuksia, jotka mahdollistaisivat tunnistusvälineiden rajat ylittävän käytön. Tämä voisi tulla kyseeseen erityisesti Pohjoismaiden ja Baltian maiden välisinä sopimuksina. Toisin kuin laajassa solmupisteverkostossa, kahdenvälisessä tunnistusvälineiden välittämisessä voisi olla mahdollista rakentaa muunnospalvelu, joka muuttaisi esimerkiksi Ruotsissa käytettävän henkilön yksilöivän tunnisteiden muotoseikoiltaan suomalaista henkilötunnusta vastaavaksi ja päinvastoin. Muunnoksen ansiosta kaikki suomalaiset asiointipalvelut pystyisivät käsittelemään myös ruotsalaisia tunnisteita samaan tapaan kuin suomalaista henkilötunnusta.

6.1.6 Ehdotuksen kustannukset

Ehdotuksen kustannukset jakautuvat teknisen tunnistusinfrastruktuurin kustannuksiin sekä hallinnollisen operoinnin kustannuksiin. Teknisen infrastruktuurin kulut jakautuvat edelleen rakentamisen investointikustannuksiin sekä jatkuvan palvelun kustannuksiin. Hallinnollisen operoinnin kustannuksia ovat ensitunnistamisen kustannukset, tunnistusvälineen jakelun, peruuttamisen ja uusimisen kustannukset sekä asiakas palvelun, käyttäjätuen ja muiden taustapalvelujen kustannukset.

Tässä esitettävät arviot pohjautuvat Väestörekisterikeskuksen kokemukseen valtion varmennepalveluiden tuottajana sekä tätä selvitystä varten tehtyihin markkinakartoituksiin.

Väestörekisterikeskus arvioi, että teknisen infrastruktuurin kertaluonteinen investointikustannus olisi noin 3–4 miljoonaa euroa sisältäen sekä palvelinympäristön rakentamisen että kansalaisille jaeltavan älypuhelinsovelluksen kehittämiskustannukset. Vaihtoehtoiseksi tunnistusvälineeksi tarjottavan tunnistustikun varmenteet tuotettaisiin samassa taustajärjestelmässä ja niiden osuus sisältyy investointiin. Itse fyysisten tunnistustikkujen kustannus riippuu siitä, kuinka monelle kansalaiselle se jaeltaisiin. Väestörekisterikeskuksen arvion mukaan yhden tunnistustikun hinta olisi korkeintaan 10–15 euroa. Mikäli vaihtoehtoista välinettä käyttäisi 100 000 kansalaista, niiden kustannus olisi siten 1–1,5 miljoonaa euroa. Teknisen infrastruktuurin jatkuvan palvelun kustannuksiksi arvioidaan noin 2,5 miljoonaa euroa vuodessa.

Pysyvät lisäkustannukset jäisivät vähäisiksi, sillä siirtymäajan jälkeen tunnistusvälineet myönnettäisiin passin ja henkilökortin myöntämisen yhteydessä.

Ensitunnistamisen hallinnolliset kustannukset jakautuvat käytettävän ensitunnistamisen menetelmän mukaisesti. Uuden välineen ottaminen käyttöön olemassa olevalla sähköisellä tunnisteella, kuten pankkitunnuksilla tai mobiilivarmenteella, maksaisi viireillä olevan hallituksen esityksen mukaisesti 0,03 euroa ensitunnistustapahtumalta. Siten esimerkiksi 1,5 miljoonan kansalaisen ensitunnistautuminen olemassa olevalla välineellä maksaisi kertaluonteisesti 45 000 euroa. Ensitunnistaminen etätodentamalla ilman olemassa olevaa sähköistä tunnistusvälinettä maksaisi tehdyn markkinakartoituksen mukaan noin 2–3 euroa ensitunnistustapahtumalta. Siten esimerkiksi 50 000 käyttäjän ensitunnistaminen etätodentamalla maksaisi noin 100 000–150 000 euroa. Valtion asiointipisteissä tapahtuva ensitunnistaminen tehtäisiin virkatyönä. Arvion mukaan poliisin passien ja henkilökorttien myöntämisprosessin ulkopuolella tehdyn virkatyön määrä asiointipisteissä olisi 15 minuuttia ensitunnistustapahtumaa kohden. Mikäli 100 000 kansalaista ensitunnistettaisiin poliisihallinnon ulkopuolella asiointipisteessä, virkatyön määrä lisääntyisi määräaikaisesti noin kolmen vuoden siirtymäajan ajalle yhteensä noin 20 henkilötyövuotta, mikä vastaisi hieman yli miljoonan euron kustannuksia. Henkilötyövuosien lisäresursointi jaettaisiin asiointipisteissä ensitunnistamista tekevien virastojen kesken käyntivolyyymien suhteessa. Kun siirtymäajan jälkeen uudet välineet myönnettäisiin passin ja henkilökortin myöntämisen yhteydessä, jäisivät ensitunnistamisen pysyvät lisäkustannukset varsin vähäisiksi.

Käyttäjätuki hoidettaisiin asiointipisteissä samalla henkilöstöllä kuin ensitunnistaminenkin. Käyttäjätukea tarjottaisiin myös puhelin- ja chat-palveluna Väestöketerikeskuksen ylläpitämässä Kansalaisneuvonnassa, jonne lisäresurssitarve olisi kolmen vuoden siirtymäaikana 10 henkilötyövuotta/vuosi, jonka jälkeen pysyvästi 5 henkilötyövuotta. Vastaavat kustannukset olisivat siten kolmen vuoden siirtymäaikana noin 650 000 euroa vuodessa ja sen jälkeen pysyvästi noin 325 000 euroa vuodessa.

Teknisen infrastruktuurin investointi- ja jatkuvan palvelun kustannukset perustuvat arvioon valtion itse rakentamasta ja hallinnoimasta teknisestä infrastruktuurista. Tekninen tuotanto olisi kuitenkin myös mahdollista kilpailuttaa, jolloin tarjottavien palveluiden kustannusten suuruusluokkaa tulisi verrata tähän vaihtoehtoon, jossa tuotanto hoidettaisiin valtion omana toimintana.

Arvio valtion uuden tunnistusratkaisun perustamisen ja jatkuvan tuotannon kustannuksista:

Perustamisvaiheen (vuodet 1–3) kustannukset yhteensä	
Teknisen infrastruktuurin rakentaminen	3 500 000
Tekniset käyttö- ja ylläpitokustannukset, 3 vuotta (à 2 500 000)	7 500 000
Vaihtoehtoinen väline (tunnistustikku), 100 000 kpl (à 15,00)	1 500 000
Poliisin suorittama ensitunnistaminen passin tai henkilökortin myöntämisen yhteydessä, 1 500 000 kpl	
Ensitunnistaminen (muun) viranomaisen tai yhteistyökumppanin asiointipisteessä, 100 000 kpl (20 htv à 65 000 tai 13,00 / kpl)	1 300 000
Ensitunnistaminen toisella tunnistusvälineellä, 1 500 000 kpl (à 0,03)	45 000
Ensitunnistaminen etätodennusratkaisulla, 50 000 kpl (à 2,50)	125 000
Käyttäjätuki, (30 htv, à 65 000)	1 950 000
3 VUODEN AIKANA YHTEENSÄ	15 920 000

Vuotuiset käyttö- ja ylläpitokustannukset, vuosi 4–	
Tekniset käyttö- ja ylläpitokustannukset	2 500 000
Vaihtoehtoinen väline (tunnistustikku), 10 000 kpl (à 15,00)	150 000
Poliisin suorittama ensitunnistaminen passin tai henkilökortin myöntämisen yhteydessä	
Ensitunnistaminen toisella tunnistusvälineellä, 50 000 kpl (à 0,03)	15 000
Ensitunnistaminen etätodennusratkaisulla, 10 000 kpl (à 2,50)	25 000
Käyttäjätuki (5 htv à 65 000)	325 000
VUODESSA YHTEENSÄ	3 015 000

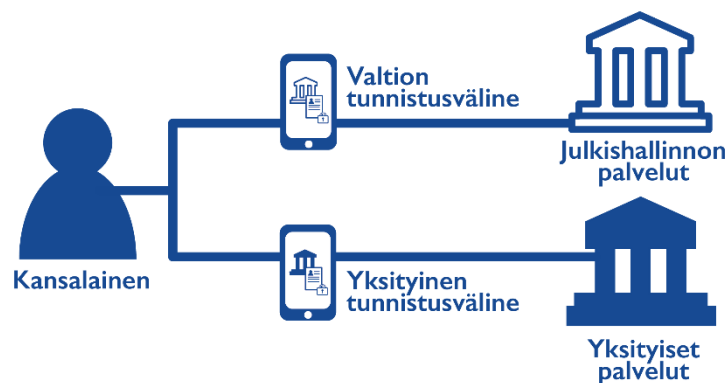
Kustannusarvion osalta on huomioitava, että siinä oletetaan tunnistustikkuja jaettavan maksutta esim. viranomaisissa käyntiasioinnin yhteydessä. Toinen vaihtoehto olisi, että väline jäisi käyttäjän maksettavaksi, jolloin perustamisvaiheen arvioidut kustannukset jäisivät 1,5 miljoonaa euroa yllä esitettyä pienemmiksi.

6.2 Ehdotukset kolmeksi vaihtoehtoiseksi tunnistamisen toimintamalliksi

Tässä selvityksessä esitellään kolme toimintamallia, joissa kaikissa hyödynnetään niiden omien piirteidensä lisäksi edellä ehdotettuja valtion tunnistamisen peruspalveluita. Jokainen ehdotettu toimintamalli tuo uusia hyödyllisiä ominaisuuksia kansalaisten, viranomaisten, luottamusverkoston toimijoiden ja asiointipalveluiden hyödynnettäväksi. Oleelliset erot eri vaihtoehdoissa syntyvät siitä, millaisia vaikutuksia niillä on vahvan sähköisen tunnistamisen kansalliseen ekosysteemiin ja millaisella siirtymäajalla ne olisivat toteutettavissa.

6.2.1 Vaihtoehto 1: Valtio tarjoaisi tunnistusvälineen vain julkishallinnon käyttöön

Vaihtoehdossa 1 valtion tunnistusväline tarjottaisiin vain julkishallinnon omaan käyttöön. Kansalaisen kannalta tämä vaihtoehto tarkoittaisi, että julkishallinnon palveluihin käytettäisiin eri tunnistusvälinettä kuin yksityisiin palveluihin. Jokaisella kansalaisella tulisi tällöin käytännössä väistämättä olla hallussaan vähintään kaksi eri tunnistusvälinettä. Tässä vaihtoehdossa nykyinen luottamusverkosto säilyisi, mutta valtio poistuisi sieltä välineen tarjoajana ja jättäisi luottamusverkoston toiminnan kokonaisuudessaan yksityisille toimijoille.



Yksityiset toimijat saisivat kuitenkin tässä vaihtoehdossa hyödyntää valtion välinettä maksutta kansalaisen sähköiseen ensitunnistamiseen, eli välineen ketjuttamiseen. Kansalaiselle olisi siten mahdollista hankkia valtion tunnistusvälineen avulla sähköisesti muita tunnistusvälineitä ilman tarvetta käydä palveluntarjoajan asiointipisteessä. Valtion välineen eräs keskeinen käyttötarkoitus olisikin sen maksuton hyödynnettävyys muiden tunnistusvälineiden hankkimiseen.

Kuten nykyäänkin, luottamusverkoston toimijoita olisi myös jatkossa kahdenlaisia: tunnistusvälineen tarjoajia sekä tunnistusvälityspalvelujen tarjoajia. Tunnistusvälineen tarjoajat tarjoavat välineitä käyttäjille ja tunnistusvälityspalvelujen tarjoajat puolestaan käyttäjien tunnistusta asiointipalveluille. Tunnistusvälineen tarjoajat voivat toimia myös välityspalvelun tarjoajina. Luottamusverkostoon kuuluu myös puhtaita välityspalveluita, joilla ei ole tarjolla omaa tunnistusvälinettä käyttäjille. Välityspalvelut voivat tarjota tunnistusta asiointipalveluille vain omalla välineellään, tai koota useampia luottamusverkostossa olevia tunnistusvälineitä sopimusteknisesti yhteen, jolloin asiointipalveluiden on mahdollista hankkia useita markkinoilla olevia tunnistusvälineitä, tai jopa kaikki, yhdellä sopimuksella.

Alan terminologiassa tunnistuspalvelu tarkoittaa tunnistusvälineen eli tunnistusmenetelmän, sen taustajärjestelmän sekä tunnistusvälineen myöntämisen ja elinkaaren hallinnan muodostamaa kokonaisuutta. Tässä vaihtoehdossa valtion tunnistuspalvelu olisi luottamusverkoston jäsen ja se välittäisi tunnistusvälinettä luottamusverkostossa vain ensitunnistamiseen.

Vaihtoehdon 1 kustannukset valtiontaloudelle ovat käytännössä samat kuin kappalessa 6.1.6 eritellyt kustannukset.

6.2.2 Vaihtoehto 2: Valtio tarjoaisi tunnistusvälineen myös markkinatoimijoiden edelleen välitettäväksi luottamusverkostossa

Vaihtoehdossa 2 valtion tunnistusväline tarjottaisiin myös yksityisten asiointipalveluiden käyttöön. Kansalaisen kannalta samalla tunnistusvälineellä voisi kirjautua sekä kaikkiin julkishallinnon palveluihin, että todennäköisesti ainakin osaan yksityisistä palveluista. On huomattava, että yksityiset asiointipalvelut voivat itse harkita mitkä tunnistusvälineet ne hyväksyvät omaan palveluunsa eikä niitä voi pakottaa hyväksymään valtion tunnistusvälinettä. Tässä vaihtoehdossa nykyinen luottamusverkosto säilyisi ja sen toiminta painottuisi erityisesti tunnistamisen välityspalveluihin. Valtio ei kuitenkaan välittäisi yksityisiin asiointipalveluihin muita tunnistusvälineitä kuin omaansa. Jos valtion välineen käyttämisestä yksityisissä asiointipalveluissa perittäisiin maksu, sen tulisi olla valtion maksuperustelain periaatteiden mukaisesti sidoksissa tuotantokustannuksiin ja sen suuruutta säänneltäisiin maksuasetuksella. Luottamusverkoston puitteissa toisille tunnistuspalvelun tarjoajille välitettävän tapahtuman hinta olisi kuitenkin ao. erityislainsäädännön eli tunnistuslain säätelyn mukainen.

Valtion tarjoama tunnistuspalvelu olisi yksityissektorille ensisijaisesti mahdollistava peruspalvelu.

Finanssialan tiettyjä käyttötapauksia lukuun ottamatta tunnistusvälineen ja todentamisen teknologian vaatimukset ovat yksityissektorilla samankaltaiset kuin julkisellakin sektorilla. Tavoiteltavat varmuustasot ovat kaikilla toimialoilla, finanssiala mukaan luettuna, samat. Edellä kuvattu valtion oma tunnistusväline voidaan teknologiansa ja varmuustasonsa puolesta jakaa myös yksityisten asiointipalveluiden hyödynnettäväksi. Tämä vaihtoehto olisi tekniseltä toteutukseltaan lähes sama kuin vaihtoehto 1: erona olisi, että tunnistusväline tarjottaisiin välitettäväksi luottamusverkostoon, jolloin valtion välineellä voisi tunnistautua myös yksityisissä asiointipalveluissa.

Alan terminologiassa tunnistuspalvelu tarkoittaa tunnistusvälineen ja sen taustajärjestelmän muodostamaa kokonaisuutta. Tässä vaihtoehdossa valtion tunnistuspalvelu olisi luottamusverkoston jäsen ja se välittäisi tunnistusvälinettä luottamusverkostossa sekä ensitunnistamiseen että kansalaisten tunnistautumiseen asiointipalveluissa.



Valtion tarjoaman tunnistuspalvelun avaamista yksityissektorin palvelujen käyttöön olisi kuitenkin tässäkin vaihtoehdossa tarkasteltava ensisijaisesti mahdollistavana peruspalveluna, jota hyödyntäen muut toimijat voisivat luoda oman kerroksensa liiketoimintatarpeisiinsa. Valtio tuottaisi tunnistamisen perustoiminnallisuudet siinäkin tapauksessa, että markkinatoimijat ylläpitävät edelleen omia tunnistuspalveluitaan. Vainnanvapauden näkökulmasta vaihtoehto 2 tarkoittaisi, että kansalaisten saatavilla olisi minkään yrityksen asiakkuudesta riippumaton, viranomaisvastuulla ylläpidetty tunnistuspalvelu.

Valtion tunnistusvälineen hyödyntäminen myös yksityisissä asiointipalveluissa lisäisi tunnistustapahtumien määrää, mutta ei käyttäjämäärää, koska käytännössä kaikilla kansalaisilla on asiointitarvetta sekä julkishallinnon että yksityisen sektorin palveluissa. Koska tunnistuspalvelun tuotantokustannukset ovat sidoksissa ennen kaikkea käyttäjämäärään, ei niinkään tunnistustapahtumisen määrään, myös vaihtoehdon 2

kustannukset valtiontaloudelle ovat käytännössä samat kuin kappaleessa 6.1.6 eriteltyt ehdotettujen tunnistamisen peruspalveluiden kustannukset.

6.2.3 Vaihtoehto 3: Käyttäjän hallinnoima identiteettilompakko

Vaihtoehdossa 3 ehdotettava toimintamalli on enemmän skenaarioluontoinen kuin edellä esitetyt kaksi konkreettisempaa mallia. Tämän toimintamallin taustalla on edellä luvussa 5 esitetyt yksilökeskeisen tiedonhallinnan kehittymistä koskevat arviot, joiden mukaan kansalaisten todentamistietojen jakaminen ja suostumuksenhallinnan ratkaisujen kehittäminen vauhdittaisivat datataloutta. Näihin tarvittavat uudet palvelut ominaisuuksineen voisi olla tarkoituksenmukaista toteuttaa tunnistuspalvelujen yhteyteen.

Tässä vaihtoehdossa tunnistusväline laajennettaisiin nykymuotoisen tunnistamisen lisäksi kansalaisen identiteettilompakoksi. Tässä vaihtoehdossa on kuitenkin huomattava, että sen toteuttamisessa on vaihtoehtoja 1 ja 2 enemmän muita, varsinaisten tunnistuspalveluiden ulkopuolella olevia kehittämistarpeita. Tämän vaihtoehdon realistiset toteutumismahdollisuudet ovat siten selvästi pidemmällä aikavälillä. Vaihtoehto 3 ei kuitenkaan ole muita vaihtoehtoja poissulkeva, ja niin haluttaessa se on mahdollista nähdä myös vaihtoehtoa 1 tai 2 jatkokehittävänä pidemmän aikavälin kehityspolkuna.

Tässä vaihtoehdossa esitettävä identiteettilompakko voisi sisältää nykyisin henkilön tunnistamiseen käytettävän henkilötunnuksen lisäksi useita erilaisia todentamistietoja ja lupia kuten esimerkiksi ajo- tai aseluvat. Todentamistietoja voisivat olla esimerkiksi: onko henkilö tunnistautunut, onko henkilö täysi-ikäinen, missä henkilö asuu tai onko henkilöllä luottotietomerkintä. Laajempi kirjo todentamistietoja toisi lisää vaihtoehtoja henkilön tunnistamiseen. Joillekin asiointipalveluille voitaisiin esimerkiksi välittää pelkästään tieto, onko henkilö täysi-ikäinen. Henkilötunnuksen väärinkäytösten mahdollisuuden vähenisivät, kun asiointipalveluille toimitettaisiin ainoastaan niiden tarvitsemat todentamistiedot.



Tämä vaihtoehto muuttaisi sähköisen tunnistamisen monimuotoisemmaksi henkilötietojen hallinnaksi ja edellyttäisi OmaData-suostumuksenhallinnan mekanismien rakentamista. Kansalaisen kannalta tämä vaihtoehto tarkoittaisi, että hänen oma päätösvaltansa kasvaisi omien henkilötietojensa luovuttamisesta asiointipalveluiden käyttöön. Palveluihin tunnistautumisen ei tarkoittaisi enää pelkästään henkilön identiteetin todentamista, vaan sen yhteydessä kansalainen voisi itse antaa asiointipalvelulle luvan hyödyntää laajemmin hänen tietojensa ja saisi vastineeksi parempia ja pidemmälle vieviä palveluita. OmaData-mekanismi takaisi, että halutessaan kansalainen voisi myös peruuttaa antamansa suostumuksen ja voisi luottaa, että asiointipalvelun pääsy hänen tietoihinsa silloin lakkaisi. Tässä vaihtoehdossa nykymuotoinen luottamusverkosto voisi kehittyä esimerkiksi OmaData-operaattoriverkostoksi, jonka toiminta keskittyisi erilaisten datapakettien välittämiseen kansalaisen omalla suostumuksella. Valtion roolina olisi luovuttaa julkishallinnon rekistereissä olevaa dataa mukaan luettuna henkilötunnus, tai sitä tulevaisuudessa vastaava yksilöivä identiteettitieto. Valtion rekistereistä liiketoiminnan harjoittamistarkoituksiin luovutettavan datan hinnoittelua säänneltäisiin maksuasetuksilla, jolloin taattaisiin myös datan korkean laadun ylläpitäminen ja kehittäminen.

Tämän vaihtoehdon edellytyksenä onkin laajamittaisempi rajapintojen rakentaminen erilaisiin julkisen ja yksityisen sektorin henkilötietovarantoihin.

Kansalaisen todentamistietoja ja suostumuksenhallintaa voisi tarkastella tekoälyä, riskienhallintaa ja alustataloutta mahdollistavana toimintona siten, että kansalaisen todentamistietojen jakaminen kansalaisen omalla suostumuksella olisi mahdollista:

- Kansalaisen kannalta olisi toimivinta, mikäli hän voisi hallinnoida kaikkia omien tietojensa jakamiseen antamia suostumuksia yhdestä paikasta.

- Tunnistamisen ratkaisuihin ja toimintamalleihin tulisi suosia standardeja ja yleisesti käytettyjä ohjelmistorajapintoja (API) ja välitysprotokollia, jotka mahdollistaisivat myös mobiilisovellusten suoraviivaisen käyttöönoton asiointipalveluissa.
- Käytettävän identiteettihallinta (IDP) -teknologian olisi tuettava myös suostumuksenhallintaa ja todentamistietojen jakamista.

Sähköisenä mobiilisovelluksena toteutettuun tunnistusvälineeseen tulisi pystyä liittämään mobiilijokortin tapaiset luvan osoittamisen tai todentamistietojen osoittamisen toiminnallisuudet kuten iän todistaminen. Lisäksi lupia ja todentamistietoja tulisi voida osoittaa ja hallinnoida useasta eri taustajärjestelmästä samalla mobiilisovelluksella. Tällöin yksi ja sama mobiilisovellus voisi toimia sekä etätunnistusvälineenä että lupien ja muiden todentamistietojen hallinnointivälineenä – kansalaisen mobiilina identiteettilompakkona.

Valtion rooli datatalouden murroksessa olisi tuottaa ne peruspalvelut, jotka mahdollistaisivat hallitun siirtymisen myöntäjäkeskeisestä käyttäjäkeskeiseen ja kansalaisen itsehallittavaan malliin. Sähköisen tunnistamisen ekosysteemissä tämä tapahtuisi vaiheittain. Siirtymävaiheessa keskitetty ja hajautettu malli olisivat samanaikaisesti käytössä.

Kansalaisten OmaDataan perustuvan digitalisaation kiihtyminen sekä tarve kehittää kansalaisen hallintamahdollisuuksia oman sähköisen identiteettinsä muodostumisesta voisivat kannustaa toimijoita kehittämään sähköisen tunnistamisen liiketoimintamalleja pelkästä sähköisestä tunnistamisesta enemmän lisäarvoa tuottavaksi datan hyödyntämiseksi – kansalaisen omalla suostumuksella.

Tämän vaihtoehdon kustannukset ovat suuremmat kuin kahden muun ehdotetun vaihtoehdon ja niihin liittyy enemmän valintoja ja siten myös epävarmuuksia. Valtion tuottamisen tunnistamisen peruspalveluiden kustannukset ovat tässäkin mallissa samat. Niiden lisäksi tulisi kehittää valtion hallinnoimien datavarantojen rajapintoja ja rajapintojen hallintaa, rakentaa lakisääteisenä tiedonsiirtokerroksena toimivaan Suomi.fi-palveluväylään geneerinen OmaData-suostumuksenhallintamekanismi sekä rakentaa kansalaiselle käyttöliittymä omien suostumustensa hallintaan. Kustannukset riippuvat muun muassa mitä ja missä rekistereissä sijaitsevia henkilötietoja mallin piiriin päätettäisiin ottaa ja kuinka paljon rajapintojen rakentamistyötä vaadittaisiin. Arviolta tämän vaihtoehdon tekniset rakentamiskustannukset asettaisivat 10–20 miljoonan euron haarukkaan. Tässä mallissa on kuitenkin myös huomattava, että kaikella toimintamallin piirissä olevalla sekä julkishallinnon että yksityisen sektorin hallinnoimalla datalla olisi todennäköisesti jokin dataa hyödyntävän asiointipalvelun maksama hinta, joten tästä toimintamallista koituisi julkishallinnolle myös tuloja.

LIITE Mobiilin sähköisen tunnistamisen ratkaisumalleja maailmalla

1. Keskitetyt valtion tuottamat sähköisen tunnistamisen järjestelmät

1.1. Singapore

<https://www.singpass.gov.sg/myinfo/intro>

Singaporen valtion keskitetty tunnistusjärjestelmä perustui kertakäyttöisiin SMS-tunnisteisiin ja se uusittiin nykyaikaiseksi mobiilisovellusta hyödyntäväksi järjestelmäksi vuosi sitten. Singapore on myös keskittänyt kansalaisen attribuuttien hallinnan yhteen palveluun (Myinfo), jolloin on syntynyt keskitetty piste, josta kansalainen voi halutesaan jakaa tietojaan kolmansille osapuolille. Samaan järjestelmään on keskitetty esimerkiksi ajoneuvojen hallintatiedot, opintosuoritukset ja muuta kansalaisista erilaisiin hallinnon rekistereihin kerättyä tietoa. Tietojen jakoa hallitsee kansalainen itse vahvan sähköisen mobiilitunnistusvälineen, Singpassin, avulla.

1.2. Viro

<https://e-estonia.com/solutions/e-identity/smart-id>

Viron henkilökorttiin ja sillä olevaan varmenteeseen perustuvan järjestelmän rinnalle on kehitetty mobiilisovellukseen perustuva Smart-ID, joka ainoastaan ensitunnistetaan henkilökortilla ja tämän jälkeen tunnistautumiseen käytetään mobiilisovellusta. Valtion palveluissa Smart-ID ja henkilökortti ovat saman arvoisia tunnistus- ja allekirjoitusvälineitä.

2. BankID-mallit

2.1. Norja

<https://www.bankid.no/en/company/>

BankID-malleissa pankit ovat keskittäneet tunnistuspalvelunsa ja valtio on sitten hyväksynyt pankkien yhteisesti toteuttaman tunnistuspalvelun myös julkishallinnon käyt-

töön. Norjan BankID (Vipps AS) toimii kaikkien pankkien keskitettynä tunnistusratkaisun tuottajana, mutta itse välineitä on useita. Norjan BankIDtä voisi kuvata pankkien tunnistuksen välityspalveluksi. Käytössä on mobiilisovelluksia, salasanoja generoivia erillisiä laitteita ja Suomessakin käytettäviä mobiilivarmenteita. Norjassa BankID toimii mobiilivarmenteen ainoana asiakkaana, jolloin sitä ei tulkita pankin tunnistusvälineen kilpailijaksi, vaan pankkien yhdessä lanseeraamaksi vaihtoehtoiseksi tunnistusvälineeksi.

Norjan BankID:n taustajärjestelmä perustuu julkisen avaimen järjestelmään (PKI). Vaikka käyttäjän näkemä laite olisi tunnuslukuja generoiva tunnistusväline, taustajärjestelmässä luodaan aina allekirjoitus jokaisesta transaktiosta käyttäjän pankin varmenteilla.

2.2. Ruotsi

<https://www.bankid.com/en/>

Ruotsin BankID on keskitetty loppukäyttäjän tunnistusvälineeseen asti toisin kuin Norjan vastaava. Samalla mobiilisovelluksella tunnistaudutaan jokaisen pankin verkkopalveluihin. Käyttäjät erotellaan pankkikohtaisesti taustajärjestelmän tasolla. Voimakkaasti keskitetty järjestelmä takaa yhtenäisen käyttökokemuksen koko kansalle. Palveluntuottajat hyötyvät kehitystyön ja ylläpidon jaettujen kulujen ekonomiasta.

3. Valtion ja pankkien konsortiot

3.1. Belgia

<https://www.itsme.be/en/>

Belgia uusi sirulliseen henkilökorttiin perustuvan kansalaisen sähköisen tunnistamisen muutama vuosi sitten. Mobiilisovellukseen perustuva uusi tunnistusjärjestelmä luotiin pankkien ja valtion yhteistyöhankkeena. Mobiilioperaattorit tulivat mukaan konsortioon tuottamalla attribuuttitiedon käytetystä puhelinliittymästä. Tämän tiedon avulla mobiilisovellus pystytään rajaamaan yhteen ainoaan välineeseen eikä kahta tunnistetta samalle henkilölle sallita.

3.2. Tanska

<https://en.digst.dk/digitisation/eid/next-generation-nemid/>

Tanskan hallinnon digitalisaatiosta vastaava virasto kilpailuttaa parhaillaan Tanskan seuraavan sukupolven sähköistä tunnistusratkaisua. Tarkoitus on tuottaa pankkien ja julkishallinnon yhteiskäyttöinen uusi tunnistusjärjestelmä, jossa nykyinen salasanalistoihin perustuva NemID korvataan mobiilisovellukseen perustuvalla ratkaisulla. Samalla palvelun taustajärjestelmää uusitaan sähköisen identiteetin ja attribuuttien hallinnan tulevaisuuden vaatimuksia paremmin vastaavaksi.

4. Attribuuttien jakoon perustuvat konsortiot

4.1. Saksa

<https://verimi.de/en>

Attribuuttien jakamiseen perustuvat konsortiot poikkeavat perinteisistä tunnistuspalvelun järjestämisen malleista siten, että sähköisen identiteetin takaajaksi ei niinkään haeta luotettua yhtä osapuolta, vaan identiteetti muodostuu konsortion keskenään jakamasta ja verifioimasta asiakasdatasta, jonka hyödyntämistä kansalainen hallinnoi mobiilisovelluksellaan. Tällaisen konsortion jäseniksi soveltuvat kaikki sellaiset tahot, joilla on runsaasti asiakasdataa sekä omia sähköisen tunnistuksen tarpeita.

Saksan virallinen sähköinen identiteetti nojaa edelleen vahvasti korkean eIDAS-tason henkilökorttiin. Verimi on uuden tyyppinen konsortio, joka tarjoaa jäsenilleen keskitettyjä alustapalveluita sähköiseen mobiiliin tunnistautumiseen, henkilön todentamiseen ja suostumuksenhallintaan. Konsortion jäsenet tuovat samasta käyttäjästä verifioimansa attribuutit konsortion muodostaman identiteetin pohjaksi. Verimin sähköinen tunniste on varmuustasoltaan astetta matalammalla tasolla kuin Saksan valtion henkilökortti.

4.2. Kanada

Kanadan vielä vain suunnittelun asteella olevassa tulevaisuuden mallissa identiteetin hallinta on täysin kansalaisella. Identiteetin myöntäjät tarjoavat todennettuja attribuutteja käyttäjistä niitä tarvitseville tahoille. Työkaluna tälle on identiteetin omistajan sähköinen lompakko, johon on keskitetty todennettujen attribuuttien rekisteri ja attribuuttien hallinta. Singaporen attribuuttirekisterin ollessa keskitetty, Kanada pyrkii toteuttamaan ratkaisun hajautetusti, mm. lohkoketjuteknologiaa hyödyntämällä.

Kirjoittajat:
Juha Mitrunen
Timo Salovaara
Janne Viskari



VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIOEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-251-000-6 (pdf)

Maaliskuu 2019