TRAFICOM
Liikenne- ja viestintävirasto

Sähköisen tunnistamisen markkinat

Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana

Traficomin tutkimuksia
ja selvityksiä

2/2021

Julkaisupäivämäärä
17.3.2021

Julkaisun nimi
Sähköisen tunnistamisen markkinat — Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana

Tekijät
Liikenne- ja viestintävirasto Traficom, Kilpailu- ja kuluttajavirasto

Toimeksiantaja ja asettamispäivämäärä
Valtiovarainministeriön asettama Digitaalisen henkilöllisyyden kehittämishanke, 8.10.2020

Julkaisusarjan nimi ja numero
Traficomin tutkimuksia ja selvityksiä 2/2021

ISSN(verkkojulkaisu) 2669-8781
ISBN(verkkojulkaisu) 978-952-311-749-5
URN http://urn.fi/URN:ISBN:978-952-311-749-5

Asiasanat
digitalisaatio, sähköinen asiointi, sähköinen tunnistaminen, sääntely, kilpailu, verkkopankkitunniste, mobiilivarmenne, kansalaisvarmenne, organisaatiovarmenne, eIDAS, luottamusverkosto, tunnistusvälitys

Tiivistelmä

Kansalaisten ja yritysten sähköinen asiointi on kasvanut voimakkaasti sekä julkisen että yksityisen sektorin palveluissa. Sähköiset asiointipalvelut nopeuttavat, helpottavat ja monipuolistavat palvelujen saatavuutta ja säästävät kustannuksia verrattuna fyysiseen tiskiasiointiin.

Tietoturvallisuuden ja tietosuojan näkökulmasta on tärkeää suojata sähköisissä asiointipalveluissa oleva tieto ja mahdollistaa näiden tietojen käsittely vain sellaisille henkilöille, joilla on oikeus tietojen käsittelyyn. Tunnistaminen on tässä olennaisessa osassa ja sähköisten asiointipalvelujen asiakkaiden tunnistamisessa tulisi käyttää vain turvallisia ja luotettavia menetelmiä. Tämä korostuu sellaisissa sähköisissä asiointipalveluissa, joissa käsitellään luottamuksellisia tietoja tai henkilötietoja tai tehdään oikeustoimia. Vahva sähköinen tunnistaminen on turvallinen ja luotettava menetelmä sähköisten asiointipalvelujen asiakkaiden henkilöllisyyden varmistamisessa ja siksi on tärkeää, että vahvan sähköisen tunnistamisen palveluja on kattavasti tarjolla, palvelut ovat laadukkaita ja edullisia käyttää. Tämä voidaan taata vain sillä, että vahvan sähköisen tunnistamisen markkina toimivat ja ovat kilpaillut.

Tässä selvityksessä kuvataan sähköisen tunnistamisen yleinen sääntely-ympäristö ja erityisesti vahvan sähköisen tunnistamisen tarjonnan sääntelyn yleispiirteet. Selvityksessä kuvataan tunnistuspalvelujen tarjonnan ja kysynnän tilannetta yksityisellä ja julkisella sektorilla. Selvityksessä esitetyt arviot perustuvat valtiovarainministeriön joulukuussa 2020 teettämien yritys- ja kuluttajakyselyjen tuloksiin, Liikenne- ja viestintäviraston ja Kilpailu- ja kuluttajaviraston tiedonkeruisiin, Liikenne- ja viestintäviraston havaintoihin valvontaviranomaisena sekä julkisista lähteistä saatavaan tietoon. Selvityksessä on ollut käytössä myös valtiovarainministeriön toimintarajoitteisille henkilöille kohdistetun kyselyn tulokset.

Markkinaselvityksen perusteella vahvan sähköisen tunnistamisen markkinat toimivat pääasiassa hyvin ja viimevuosina tehdyt lainsäädäntömuutokset ja sääntely ovat avanneet markkinaa entistä enemmän kilpailulle ja merkittäviä kilpailun esteitä on saatu purettua. Tehtyjen lainsäädäntömuutosten ja sääntelyn vaikutukset ovat kuitenkin vielä osin realisoitumatta ja on todennäköistä, että kilpailu kehittyy edelleen myönteiseen suuntaan ja muun muassa markkinan hintatason odotetaan laskevan erityisesti yksityisen ja kolmannen sektorin sähköisten asiointipalvelujen maksamien hintojen osalta. Vahvan sähköisen tunnistamisen markkinalla on myös tilaa kasvaa merkittävästi nykyisestään, mikä osaltaan voi houkutella markkinalle uusia toimijoita, jotka lisäävät edelleen kilpailua markkinalla.

Suurin osa kansalaisista käyttäisi vahvaa sähköistä tunnistusvälinettä sähköisiin asiointipalveluihin tunnistamisessa, jos vain sähköisten asiointipalvelujen tarjoajat mahdollistaisivat sen palveluissaan. Suurimmalla osalla kansalaisista on jo käytössään vähintään yksi vahva sähköinen tunnistusväline ja he kokevat niiden käytön olevan pääosin helppoa. Vahvan sähköisen tunnistusvälineen käytöstä käyttäjille eli kansalaisille koituvat kustannukset ovat kohtuullisia.

Kansalaiset ovat tyytyväisiä nykyisin tarjolla oleviin vahvoihin sähköisiin tunnistusvälineisiin eikä valtion mahdolliselle uudelle tunnistusvälineelle nähdä ehdotonta tarvetta. Merkittävä osa kansalaisista olisi kuitenkin valmis ottamaan mahdollisen uuden vahvan sähköisen tunnistusvälineen käyttöönsä, mikäli väline täyttäisi tietyt ominaisuudet. Kansalaiset kuitenkin pitävät tärkeänä, että julkisen hallinnon sähköisiin asiointipalveluihin voi jatkossakin tunnistautua nykyisillä tunnistusvälineillä eli verkkopankkitunnuksilla ja mobiilivarmenteilla.

Suomessa on erityisryhmiä, joilla ei ole mahdollisuutta saada käyttöönsä vahvaa sähköistä tunnistusvälinettä tai joilla on muutoin haasteita ottaa käyttöönsä ja käyttää tietoteknisiä laitteita, sähköisiä asiointipalveluja ja vahvaa sähköistä tunnistusvälinettä. Näiden henkilöiden mahdollisuuksiin käyttää sähköisiä asiointipalveluja, mukaan lukien vahvaa sähköistä tunnistamista, tulisi kiinnittää erityistä huomioita. Esteiden poistaminen vaatii useita erilaisia toimenpiteitä, ja on tärkeää, että valitut toimenpiteet ovat optimaalisia koko yhteiskunnan kannalta. Pääosin nämä haasteet ovat ratkaistavissa kehittämällä lainsäädäntöä, sähköisiä asiointipalveluja ja vahvoja sähköisiä tunnistusvälineitä.

Yhteyshenkilö
Jukka-Pekka Juutinen

Raportin kieli
Suomi

Luottamuksellisuus
Julkinen

Kokonaissivumäärä
86

Jakaja

Kustantaja
Liikenne- ja viestintävirasto Traficom

Transport- och kommunikationsverket

Utgivningsdatum
17.3.2021

Publikation
Marknaden för elektronisk identifiering — Elektronisk identifiering möjliggör trygg användning av elektroniska tjänster

Författare
Transport- och kommunikationsverket Traficom, Konkurrens- och konsumentverket

Tillsatt av och datum
Projektet för att utveckla den digitala identiteten, tillsatt av finansministeriet 8.10.2020

Publikationsseriens namn och nummer
Traficoms forskningsrapporter och utredningar 2/2021

ISSN (webbpublikation) 2669-8781
ISBN (webbpublikation) 978-952-311-749-5
URN http://urn.fi/URN:ISBN: 978-952-311-749-5

Ämnesord
Digitalisering, elektroniska tjänster (e-tjänster), reglering, konkurrens, nätbankskoder, mobilcertifikat, medborgarcertifikat, organisationscertifikat, eIDAS, förtroendenät, identifieringsförmedling

Sammandrag

Medborgare och företag har kraftigt ökat användningen av både den offentliga och den privata sektorns elektroniska tjänster. Elektroniska tjänster blir mer lättillgängliga, snabbare och mångsidigare för alla och sparar kostnader jämfört med fysiska tjänster på plats.

Med tanke på informationssäkerhet och dataskydd är det viktigt att skydda uppgifter i elektroniska tjänster och möjliggöra behandlingen av dessa uppgifter bara för de personer som har rätt att behandla uppgifterna. Identifiering spelar en viktig roll här och man borde endast använda trygga och tillförlitliga metoder för att identifiera kunder som använder elektroniska tjänster. Detta betonas i sådana elektroniska tjänster där man behandlar konfidentiella uppgifter eller personuppgifter eller företar rättshandlingar. Stark autentisering är en trygg och tillförlitlig metod för att kontrollera identiteten hos kunder som använder elektroniska tjänster och därför är det viktigt att tjänster för stark autentisering finns tillgängliga till alla delar för användare, att tjänsterna är av god kvalitet och förmånliga att använda. Detta kan garanteras enbart med det att marknaden för elektronisk identifiering fungerar och att det finns konkurrens på marknaden.

I denna utredning beskrivs den allmänna regleringsmiljön för elektronisk identifiering och speciellt de allmänna inslagen i regleringen av tillhandahållandet av stark autentisering. I utredningen beskrivs utbuds- och efterfrågeläget i fråga om identifieringstjänster på den privata och den offentliga sektorn. De uppskattningar som presenteras i utredningen baserar sig på resultaten av förfrågningar till företag och konsumenter som finansministeriet låtit göra i december 2020, på Transport- och kommunikationsverkets och Konkurrens- och konsumentverkets datainsamlingar, på Transport- och kommunikationsverkets observationer i egenskap av tillsynsmyndighet samt på uppgifter från offentliga källor. I utredningen har även använts resultaten från finansministeriets enkät till personer med funktionshinder.

På basis av marknadsutredningen fungerar marknaden för stark autentisering i regel bra och de lagändringar som gjorts under de senaste åren jämte reglering har öppnat marknaden för konkurrens och det har varit möjligt att undanröja betydande hinder för konkurrens. Lagändringarnas och regleringens konsekvenser har dock ännu inte realiserats och det är sannolikt att konkurrensen fortsätter att utvecklas positivt och bland annat prisnivån på marknaden förväntas sjunka speciellt för priser som den privata och den tredje sektorn betalar för elektroniska tjänster. Marknaden för stark autentisering har också rum att växa avsevärt, vilket för sin del kan locka nya aktörer som ytterligare ökar konkurrensen på marknaden.

Största delen av medborgarna skulle använda ett starkt elektroniskt identifieringsverktyg för att identifiera sig i elektroniska tjänster om bara leverantörer av elektroniska tjänster möjliggör det i sina tjänster. Största delen av medborgarna har redan åtminstone ett starkt identifieringsverktyg och de upplever att det i regel är lätt att använda dem. Kostnaderna för användningen av ett starkt elektroniskt identifieringsverktyg är skäliga för användare, m.a.o. för medborgare.

Medborgarna är nöjda med nuvarande tillgängliga identifieringsverktyg för stark autentisering och man ser inte något absolut behov för ett eventuellt nytt statens identifieringsverktyg. En stor del av medborgarna skulle dock vara beredda att börja använda ett eventuellt nytt identifieringsverktyg för stark autentisering om verktyget skulle uppfylla vissa egenskaper. Medborgarna anser dock att det är viktigt att de även i framtiden ska kunna identifiera sig i den offentliga förvaltningens elektroniska tjänster med nuvarande identifieringsverktyg, dvs. med nätbankskoder och mobilcertifikat.

I Finland finns grupper med särskilda behov som inte har möjlighet att börja använda ett starkt elektroniskt identifieringsverktyg eller som annars har utmaningar med att börja använda och använda IT-utrustning, elektroniska tjänster och ett starkt elektroniskt identifieringsverktyg. Man bör fästa särskild uppmärksamhet vid dessa personers möjligheter att använda elektroniska tjänster, inbegripet stark autentisering. Det krävs flera olika åtgärder för att undanröja hinder, och det är viktigt att de valda åtgärderna är optimala för hela samhället. Dessa utmaningar kan i regel avgöras genom att man utvecklar lagstiftningen, elektroniska tjänster och starka elektroniska identifieringsverktyg.

Kontaktperson
Jukka-Pekka Juutinen

Språk	Sekretessgrad	Sidoantal
Finska	Offentlig	86

Distribution

Förlag
Transport- och kommunikationsverket Traficom

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
17 March 2021

Title of publication
The Market on Electronic Identification — Electronic Identification as an Enabler of Secure Use of Electronic Services

Author(s)
Finnish Transport and Communications Agency Traficom, Finnish Competition and Consumer Authority

Commissioned by, date
Digital identity development project launched by the Ministry of Finance, 8 October 2020

Publication series and number
Traficom Research Reports 2/2021

ISSN (online) 2669-8781
ISBN (online) 978-952-311-749-5
URN http://urn.fi/URN:ISBN: 978-952-311-749-5

Keywords
digitalisation, electronic services, electronic identification, regulation, competition, online banking credentials, mobile certificate, citizen certificate, certificate for organisations, eIDAS, trust network, identification broker services

Abstract

Citizens' and companies' use of public and private-sector electronic services has seen a significant increase. Electronic services make accessing services easier and faster, result in the availability of a more diverse range of services, and provide a cost-effective alternative to traditional in-person services.

From the viewpoint of information security and data protection, it is important to ensure the adequate protection of the data processed in electronic services and to limit access to the data as appropriate. As identification plays a crucial role in this context, all methods used to identify electronic service users should be secure and reliable. This is particularly important for those services that are used to process personal data or other confidential information, or to carry out legal transactions. Given that strong electronic identification is a secure and reliable method of verifying the identity of electronic service users, it should be widely available, high quality and inexpensive to use. This, in turn, requires a well-functioning, competitive market for strong electronic identification services.

This publication describes the general regulatory environment for electronic identification, with a particular focus on the general features of the regulations governing the provision of strong electronic identification services. The report examines the current situation as regards the supply of and demand for identification services in the private and public sectors. The assessments presented as part of the report are based on the results of business and consumer surveys conducted by the Ministry of Finance in December 2020, data gathered by the Finnish Transport and Communications Agency and the Finnish Competition and Consumer Authority, observations made by the Finnish Transport and Communications Agency in its role as a supervisory authority, and publicly available sources. The report also drew on the results of a Ministry of Finance survey of people with disabilities.

A study of the strong electronic identification services market showed that the market mainly functions well, and legislative and regulatory changes implemented in recent years have further opened it up to competition while dismantling significant obstacles to competition. While the full effects of the legislative and regulatory changes are not yet observable, it is probable that the competitive environment will continue to develop in a positive direction. The prices paid by private and third-sector actors are expected to fall, for example. The substantial growth potential that the strong electronic identification services market has may also serve to increase competition as new providers seek to enter the market.

Most citizens would use strong electronic identification means when logging in to electronic services if electronic service providers offered this as an option. Strong electronic identification means are already prevalent among the population, and their use is generally considered to be easy. The costs incurred by users as a result of using strong electronic identification means are reasonable.

Citizens are satisfied with the strong electronic identification means currently available, and a possible state-provided identification means is thus not seen as absolutely necessary. A significant share of the population would, however, be willing to adopt a new strong electronic identification means, if it met certain criteria. Users nevertheless consider it important that electronic services provided by public administrative bodies continue to allow identification using currently available identification means, i.e. online banking credentials and mobile certificates.

Meanwhile, certain subsets of the Finnish population do not have access to strong electronic identification means or otherwise experience difficulties when attempting to adopt and use information technology devices, electronic services and strong electronic identification means. Particular attention should be paid to the opportunities afforded to these individuals to use electronic services and strong electronic identification means. Removing the obstacles they face requires a range of measures, which should be selected so as to ensure an outcome that is optimal for society at large. These challenges can be solved by improving the legislation, electronic services and strong electronic identification means.

Contact person	Language	Confidence status	Pages, total
Jukka-Pekka Juutinen	Finnish	Public	86

Distributed by	Published by
	Finnish Transport and Communications Agency Traficom

ALKUSANAT

Tämä markkinaselvitys on tehty osana valtiovarainministeriön asettamaa Digitaalisen henkilöllisyyden kehittäminen -hanketta. Markkinaselvityksen laatimiseen ovat osallistuneet Liikenne- ja viestintävirasto ja Kilpailu- ja kuluttajavirasto. Selvityksessä esitetyt arviot perustuvat valtiovarainministeriön joulukuussa 2020 teettämien yritys- ja kuluttajakyselyjen tuloksiin, Liikenne- ja viestintäviraston ja Kilpailu- ja kuluttajaviraston tiedonkeruisiin, Liikenne- ja viestintäviraston havaintoihin valvontaviranomaisena sekä julkisista lähteistä saatavaan tietoon. Selvityksessä on ollut käytössä myös valtiovarainministeriön toimintarajoitteisille henkilöille kohdistetun kyselyn tulokset.

Markkinaselvityksen tavoitteena on selvittää muun muassa tunnistuspalvelujen ja ennen kaikkea vahvan sähköisen tunnistamisen markkinan nykytilaa, eri käyttäjäryhmien tarpeita tunnistuspalveluille ja vahvan sähköisen tunnistamisen mahdollisuuksia vastata näihin tarpeisiin. Markkinaselvityksessä tarkastellaan myös tunnistuspalvelujen tarjontaa, saavutettavuutta ja esteettömyyttä erityisryhmien näkökulmasta sekä vahvan sähköisen tunnistamisen markkinalle kohdistetun sääntelyn vaikutuksia markkinakilpailuun ja hintatasoon markkinalla.

Markkinaselvityksen tarkoituksena on tukea Digitaalisen henkilöllisyyden kehittäminen -hankkeessa vaihtoehtoisten ratkaisujen löytämistä hankkeessa esille nostettuihin kysymyksiin ja haasteisiin sekä näiden vaihtoehtoisten ratkaisujen arviointia ja vertailua.

Tärkeää on, että esille nostetut kysymykset ja haasteet ratkaistaan koko yhteiskunnan kannalta optimaalisella tavalla. Toivottavasti tämä selvitys osaltaan auttaa tällaisten ratkaisujen löytämisessä.

Helsingissä, 17. maalisuuta 2021

Jukka-Pekka Juutinen
Johtaja
Liikenne- ja viestintävirasto Traficom

Sisällysluettelo

1 Selvityksen tarkoitus

Tässä markkinaselvityksessä tarkastellaan kokemuksia tunnistuspalvelujen käyttämisestä ja käytettävyydestä sekä tarpeita, joita tunnistuspalvelujen käyttämiseen ja käytettävyyteen kohdistuu. Asiaa tarkastellaan tunnistusvälineiden ja sähköisten asiointipalvelujen käyttäjien sekä sähköisiä asiointipalveluja tarjoavien toimijoiden kannalta. Markkinaselvityksen pohjana on käytetty valtiovarainministeriön Taloustutkimuksella teettämien kuluttaja- ja yrityskyselyjen tuloksia.

Markkinaselvityksessä arvioidaan myös vahvojen sähköisten tunnistuspalvelujen markkinan tilannetta, kilpailun kehittymistä ja sitä, miten hyvin markkina onnistuu vastaamaan tunnistuspalvelujen käyttäjien ja niitä ostavien sähköisten asiointipalvelujen tarjoajien tarpeisiin. Selvityksessä tarkastellaan lisäksi sääntelyn vaikutuksia markkinan toimivuuteen, kilpailuun ja hinnoitteluun.

Markkinaselvityksen tarkoituksena on tukea valtiovarainministeriön asettaman Digitaalisen henkilöllisyyden kehittämishanketta ja tuottaa tietoa hankkeessa valmisteltavien toimenpide-ehdotusten kartoittamiseksi ja ennen kaikkea niiden vertailemiseksi ja arvioimiseksi. Markkinaselvityksessä selvitettävät asiat ovat perusasioita, joita tällaisissa kehittämishankkeissa on ensi sijaisen tärkeää selvittää ennen mahdollisten toimenpide-ehdotusten valmistelua ja niistä päättämistä.

Markkinaselvityksen luvussa 2 käydään läpi yleisesti tunnistamista ja tunnistuspalveluja koskevat määritelmät ja säädökset. Luvussa 3 tarkastellaan yleisesti sähköisiä tunnistus- ja identiteettipalveluja tarjonnan ekosysteemin, tietoturvallisuuden ja kuluttajan oikeuksien kannalta ja luvussa 4 kilpailun edistämistä ja kilpailuneutraliteettia. Luvussa 5 tarkastellaan tunnistus- ja identiteettipalveluihin kohdistuvia tarpeita, mukaan lukien tunnistuspalvelujen käytettävyys ja saavutettavuus, sekä näiden palvelujen käyttöä. Luvussa 6 tarkastellaan vahvan sähköisen tunnistamisen markkinaa, markkinalle kohdistetun sääntelyn toimivuutta ja vaikutuksia kilpailutilanteeseen sekä markkinalla tarjottujen palvelujen kykyä vastata tunnistuspalvelujen käyttäjien ja ostajien tarpeisiin. Luvussa 7 tehdään yhteenveto sähköisen tunnistamisen markkinan tilanteesta.

2 Määritelmät ja säädökset

2.1 Määritelmät

2.1.1 Sähköisen tunnistamisen osapuolet

Vahva sähköinen tunnistuspalvelu*[1] tarkoittaa tunnistuslain mukaisesti rekisteröityä tunnistuspalvelua.

Vahva sähköinen tunnistaminen* tarkoittaa sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset.

Heikko tunnistuspalvelu tai tunnistusmenetelmä tarkoittaa tässä selvityksessä sähköistä tunnistuspalvelua, jota ei ole ilmoitettu tunnistuslain mukaiseen rekisteriin. Heikon tunnistuspalvelun luotettavuutta ei ole arvioitu eikä sitä valvota jonkin lainsäädännön mukaisesti.[2] Termin heikko sijaan voidaan käyttää myös termiä **rekisteröimätön tunnistuspalvelu** tai **tunnistusmenetelmä**.

Tunnistuspalvelu* tarkoittaa tunnistusvälineen tarjoamista käyttäjille, tunnistusvälinettä käyttävien tunnistamisen tarjoamista sähköisille asiointipalveluille tai tunnistusvälityspalvelun tarjoamista sähköisille asiointipalveluille.

Tunnistusvälineen tarjoaja* tarkoittaa toimijaa, joka tarjoaa tunnistusvälinettään yleisölle eli käyttäjille, sen käyttäjille tarjoamien tunnistusvälinettä käyttävien tunnistamisen tarjoamista sähköisille asiointipalveluille ja/tai tunnistusvälinettään tunnistusvälityspalvelun tarjoajalle välitettäväksi. Markkinaselvitystä laadittaessa vahvan sähköisen tunnistusvälineen tarjoajia olivat pankit, matkaviestinverkkoyritykset ja Digi- ja väestötietovirasto. Tunnistusvälineen tarjoajasta käytetään usein myös englanninkielistä lyhennettä **IdP** (Identity Provider).

Tunnistusvälineen haltija* tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolle tunnistusvälineen tarjoaja on sopimukseen perustuen antanut tunnistusvälineen käytettäväksi. Haltijasta käytettään tässä selvityksessä myös termiä **käyttäjä**. Ennen ensitunnistamista ja tunnistusvälineen myöntämistä kysymyksessä on tunnistusvälineen **hakija**.

Tunnistusvälityspalvelun tarjoaja* tarkoittaa tunnistustapahtumia luottaville osapuolille eli sähköisten asiointipalvelujen tarjoajille välittävää toimijaa. Markkinaselvitystä laadittaessa pelkästään vahvan sähköisen tunnistusvälityspalvelun tarjoajia olivat Nets Branch Norway (jatkossa NETS) ja Signicat AS (jatkossa Signicat). Vahvaa sähköistä tunnistusvälinettä ja vahvojen sähköisten tunnistusvälityspalvelua tarjosivat Danske Bank A/S (jatkossa Danske Bank), DNA Oyj (jatkossa DNA), Elisa Oyj (jatkossa Elisa), Nordea Bank Oyj (jatkossa Nordea), OP-Palvelut Oy (jatkossa OP-Palvelut) ja Telia Finland Oy (jatkossa Telia). Tunnistusvälityspalvelun tarjoajasta käytetään usein myös englanninkielistä termiä **broker**.

Luottamusverkosto* tarkoittaa Liikenne- ja viestintävirastoon lakisääteisen ilmoituksen tehneiden vahvan sähköisen tunnistuspalvelun tarjoajien verkostoa.

[1] Tähdellä merkittyjen termien määritelmästä on säädetty vahvan sähköisen tunnistamisen osalta erikseen vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa.

[2] Hallituksen esityksessä 272/2014 todetaan 12 a §:n perusteluissa seuraavaa:
Tunnistuspalvelua on mahdollista tarjota myös ilmoittautumatta Viestintävirastoon, mutta tällöin tunnistuspalvelun tarjoajalla ei ole vahvan sähköisen tunnistuspalvelun tarjoajan asemaa. Luottamusverkostossa toimivaa tunnistuspalvelun tarjoajaa velvoittavat ne säädökset, joista laissa vahvasta sähköisestä tunnistamisesta ja [sähköisistä allekirjoituksista] on säädetty, kuten tunnistuspalvelun tarjoajan yleiset velvollisuudet.

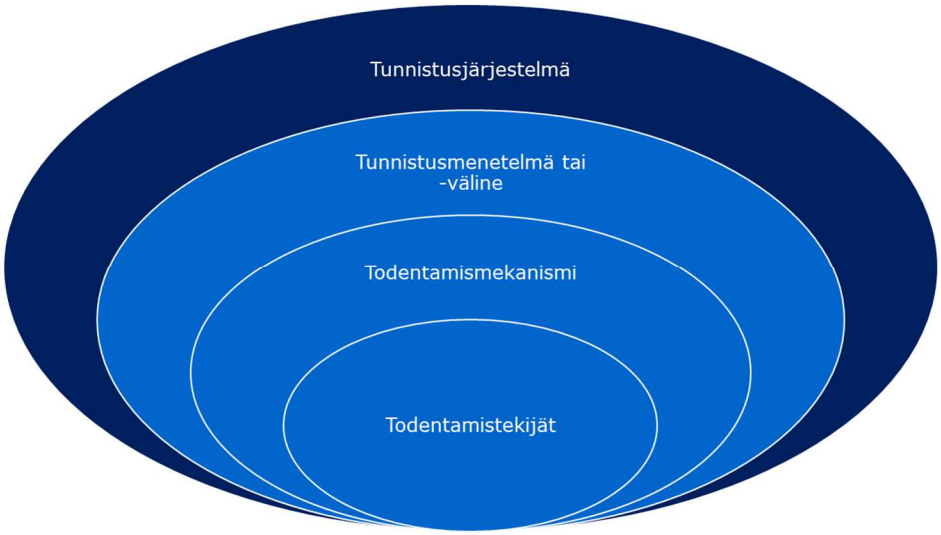
Verkoston perusta on vahvan sähköisen tunnistusvälineen tarjoajan velvollisuus tarjota tunnistuspalvelunsa käyttöoikeutta vahvan sähköisen tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle eli **sähköisille asiointipalveluille**.

Sähköinen asiointipalvelu tarkoittaa sähköisen järjestelmän ja käyttäjärajapinnan kautta tarjottua palvelua, jossa käyttäjä voi lukea ja/tai muokata, lähettää ja/tai vastaanottaa tietoja sähköisesti sekä tehdä muita erikseen määriteltyjä toimenpiteitä. Tunnistuspalvelujen koskevassa lainsäädännössä sähköisestä asiointipalvelusta käytetään termiä **luottava osapuoli** kuin myös **palveluntarjoaja**. Laissa digitaalisten palvelujen tarjoamisesta (306/2019) käytetään termiä **digitaalinen palvelu**. Se on kyseisen lain velvoitteiden kannalta osittain päällekkäinen tunnistuspalvelun määritelmän kanssa.

Luottava osapuoli* tarkoittaa on luonnollista henkilöä tai oikeushenkilöä, joka luottaa sähköiseen tunnistamiseen. Luottavia osapuolia ovat **sähköiset asiointipalvelut**, jotka hankkivat asiakkaidensa vahvan sähköisen tunnistuksen tunnistuspalvelun tarjoajalta. Luottavasta osapuolesta käytetään usein myös englanninkielistä termiä **relying party**.

2.1.2 Vahva sähköinen tunnistus

Tunnistusjärjestelmä* tarkoittaa järjestelmää, jonka puitteissa vahvan sähköisen tunnistamisen menetelmiä myönnetään ja tuotetaan käyttäjille. Tunnistusjärjestelmä kattaa vahvan sähköisen tunnistuspalvelun tarjoajan tekniset järjestelmät, tietoturvallisuuden hallinnan ja muut säädetyt luotettavuusvaatimukset. Tunnistusjärjestelmä kattaa myös kaikki alihankitut osat ja toiminnot, jotka liittyvät tunnistuspalvelun tuottamiseen. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa tunnistusjärjestelmästä käytetään termiä **sähköisen tunnistamisen järjestelmä.** Tunnistusjärjestelmästä käytetään usein myös englanninkielistä termiä **eID scheme.**



Kuva 1: Tunnistusjärjestelmän osakokonaisuudet.

Tunnistusväline tai tunnistusmenetelmä* tarkoittaa aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään sähköiseen asiointipalveluun liittyvään todentamiseen. Tunnistusmenetelmä perustuu **todentamistekijöihin,** jotka liittyvät käyttäjän tietoon, ominaisuuteen tai hallussapitoon sekä **dynaamiseen todentamismekanismiin**, jolla taataan jokaisen tunnistustapahtuman ainutkertaisuus. Tunnistusvälineestä tai tunnistusmenetelmästä käytetään usein myös englanninkielistä termiä **eID means**.

Autentikointi* eli todentaminen tarkoittaa sähköistä prosessia, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön vahvan sähköisen tunnistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen. **Kun käyttäjä** käyttää vahvaa sähköistä tunnistusvälinettä tunnistautuakseen sähköiseen asiointipalveluun, vahvan sähköisen tunnistuspalvelun todentamismekanismilla todennetaan eli autentikoidaan, että käyttäjä on vahvan sähköisen tunnistusvälineen oikea haltija eli se henkilö, joka väittää olevansa.

(Henkilön) Tunnistetiedot* tarkoittaa tietoja, jotka mahdollistavat luonnollisen henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden toteamisen. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa[3] noudatetaan eIDAS-asetusta tarkentavan komission yhteentoimivuusasetuksen määrityksiä vähimmäistiedoista ja lisämääreistä eli valinnaisista tiedoista[4]. Vähimmäistietojen tarkoitus ja määritelmä vastaa valtiovarainministeriön Digitaalinen henkilöllisyyden hankkeessa[5] käytetyn termin **ydinidentiteetti** tarkoitusta. Vahvalla sähköisellä tunnistamisella voidaan todentaa luotettavasti myös jokin niukempi tieto, kuten ikä (lain mukaan *tunnistusvälineen haltijan salanimi tai ainoastaan rajoitettu määrä henkilötietoja[6]).* Tunnistetiedoista käytetään usein myös englanninkielistä termiä **person identification data**.

Ensitunnistaminen* tarkoittaa vahvan sähköisen tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä. Ensitunnistaminen

[3] Ks. tunnistus- ja luottamuspalvelulain 12 b § 1) *kuvaus tunnistusvälineestä mukaan lukien tieto saatavilla olevista yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti annetun komission täytäntöönpanoasetuksen (EU) 2015/1501 liitteen mukaisista **henkilön tunnistetiedoista**;*

[4] Ks. (EU) 2015/1501 *11 artikla Henkilön tunnistetiedot* ja liite *Luonnollista tai oikeushenkilöä yksilöivästi edustavien henkilön tunnistetietojen vähimmäisvaatimukset*

1. Luonnollisen henkilön tunnistetietoja koskevat vähimmäisvaatimukset

*Luonnollisen henkilön **vähimmäistietojen** on sisällettävä kaikki seuraavat pakolliset määreet:*
a) nykyinen sukunimi (-nimet);
b) nykyinen etunimi (-nimet);
c) syntymäaika;
d) yksilöllinen tunniste, jonka lähettävä jäsenvaltio on luonut noudattaen teknisiä eritelmiä rajat ylittävää tunnistamista varten ja joka on mahdollisimman pitkäkestoinen.

*Luonnollisen henkilön vähimmäistiedot voivat sisältää yhden tai useamman seuraavista **lisämääreistä**:*
a) etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä;
b) syntymäpaikka;
c) nykyinen osoite;
d) sukupuoli.

*2. Oikeushenkilön tunnistetietoja koskevat **vähimmäisvaatimukset***

Oikeushenkilön vähimmäistietojen on sisällettävä kaikki seuraavat pakolliset määreet:
a) nykyinen virallinen nimi;
b) yksilöllinen tunniste, jonka lähettävä jäsenvaltio on luonut noudattaen teknisiä eritelmiä rajat ylittävää tunnistamista varten ja joka on mahdollisimman pitkäkestoinen.

*Oikeushenkilön vähimmäistiedot voivat sisältää yhden tai useamman seuraavista **lisämääreistä**:*
a) nykyinen osoite;
b) arvonlisäverotunniste;
c) verorekisterinumero;
d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY (1) 3 artiklan 1 kohdassa tarkoitettu tunniste;
e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012 (2) tarkoitettu oikeushenkilötunnus (LEI);
f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013 (3) tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero);
g) neuvoston asetuksen N:o 389/2012 (4) 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

[5] https://vm.fi/digitaalisen-henkilollisyyden-hanke

[6] Tunnistus- ja luottamuspalvelulain 8 § 2 momentti: *Mitä 1 momentissa säädetään, ei estä palvelun tarjoamista palvelukohtaisesti siten, että tunnistuspalvelun tarjoaja ilmoittaa tunnistuspalvelua käytävälle palveluntarjoajalle tunnistusvälineen haltijan salanimen tai ainoastaan rajoitetun määrän henkilötietoja.*

voidaan jakaa kahteen pääasialliseen vaihtoehtoon: fyysinen ensitunnistaminen ja sähköinen ensitunnistaminen. **Fyysinen ensitunnistaminen** tehdään kasvotusten paikan päällä tarkistamalla ensiksi henkilön esittämän virallisen asiakirjan, eli passin tai henkilökortin, aitous ja sen jälkeen vertaamalla esittäjän ulkoisia ominaispiirteitä viralliseen asiakirjaan. **Sähköinen ensitunnistaminen** tehdään etämenettelyllä esimerkiksi vahvalla sähköisellä tunnistusvälineellä (niin kutsuttu ensitunnistamisen ketjutus). Vahvan sähköisen tunnistusvälineen tarjoajan on mahdollistettava se, että toinen vahvan sähköisen tunnistusvälineen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Sähköinen ensitunnistaminen voi perustua myös etäyhteydellä esitetyn passin tai henkilökortin aitouden tarkistamiseen ja henkilön ominaisuuksien ja asiakirjan vertailuun (*remote identification*). Tämän menettelyn luotettavuusvaatimukset ovat vasta kehittymässä Euroopassa.

Luotettu lähde* (eIDAS varmuustasoasetuksessa 'luotettava lähde', englanniksi authoritative source) tarkoittaa mitä tahansa sellaista lähdettä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen. eIDAS-sääntelyyn nähden nämä ovat kansallisesti säädettävissä. Ensitunnistamisessa henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Vahvan sähköisen tunnistusvälineen myöntäminen edellyttää lisäksi tietojen varmistamista väestötietojärjestelmästä (jatkossa myös VTJ).

2.1.3 Omadata ja SSI

Itsehallittava identiteetti (engl. Self-Sovereign Identity, SSI) tarkoittaa henkilötietojen käsittelyn mallia, jossa henkilö voi itse hallinnoida joko itseltään tai luotettavalta kolmannelta taholta lähtöisin olevien henkilötietojensa antamista asiointipalvelulle, jossa henkilötietoja tarvitaan. SSI-termiä käytetään yleensä malleissa, joissa luotettavuus itsehallittaviin tietoihin on toteutettu lohkoketjuteknologialla ja henkilöllä on hallussaan väline (lupalompakko), jolla hän pystyy teknisesti vahvistamaan saajataholle oikeuden käsitellä henkilötietoaan.[7] Henkilötietoja ei talleteta lohkoketjuun, vaan lohkoketjua ja krytografisia tunnisteita käytetään siihen, että tiedon vastaanottaja voi varmistaa muuta kautta lähetetyn tiedon paikkansapitävyyden ja voimassaolon.[8] SSI-mallit ovat vasta kehittymässä, joten edellä kuvattu ei välttämättä kuvaa kaikkia kehitteillä olevia malleja.

Lupalompakko, identiteettilompakko tarkoittaa käyttäjän hallussa olevaa sovellusta, jolla hän voi hallinnoida henkilötietojensa luovutusta. Teknisesti lompakko on turvattu moduuli (tyypillisesti laitteiston ja ohjelmiston yhdistelmä), missä on tallennettuna identiteetin haltijan yksityiset kryptoavaimet.[9] Mobiiliisovellukseen perustuva vahva sähköinen tunnistusmenetelmä on tyyppiesimerkki tällaisesta teknisestä toteutuksesta.

Omadata (engl. MyData) tarkoittaa henkilötietojen käsittelytapaa, joka toteuttaa seuraavat periaatteet: 1. yksilöiden oikeus ja mahdollisuus hallita omaa dataansa,

[7] Ks. ***Itsehallittavan identiteetin sääntely EU:n yleisessä tietosuoja-asetuksessa**, Pitkänen Jyrki, Notaaritutkielma kevät 2018, Lapin yliopisto Oikeustieteiden tiedekunta* https://lauda.ulapland.fi/bitstream/handle/10024/63735/Notaaritutkimus.Pitka%20nen.Jyrki.pdf?sequence=1
Ks. Myös ***SSI eIDAS Legal Report**, April 2020* https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf
[8] *Ks. **My data - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen**, Poikola, Kuikkaniemi, Kuittinen, Honko, Knuutila **2018** s. 43* https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160954/MyData%202018.pdf?sequence=4&isAllowed=y
[9] Ks. edellisen viitteen lähde, s. 38

2. henkilötiedon kattava ja käytännöllinen saatavuus sekä 3. henkilötiedon hallinnan hajauttaminen ja yhteentoimivuus.[10]

2.1.4 Sähköinen allekirjoitus ja sähköinen leima

Sähköinen allekirjoitus* tarkoittaa sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon ja jota allekirjoittaja käyttää allekirjoittamiseen. **Allekirjoittaja** tarkoittaa luonnollista henkilöä, joka luo sähköisen allekirjoituksen.

Sähköinen leima* tarkoittaa sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon viimeksi mainitun tiedon alkuperän ja eheyden varmistamiseksi. **Leiman luoja** tarkoittaa oikeushenkilöä, joka luo sähköisen leiman.

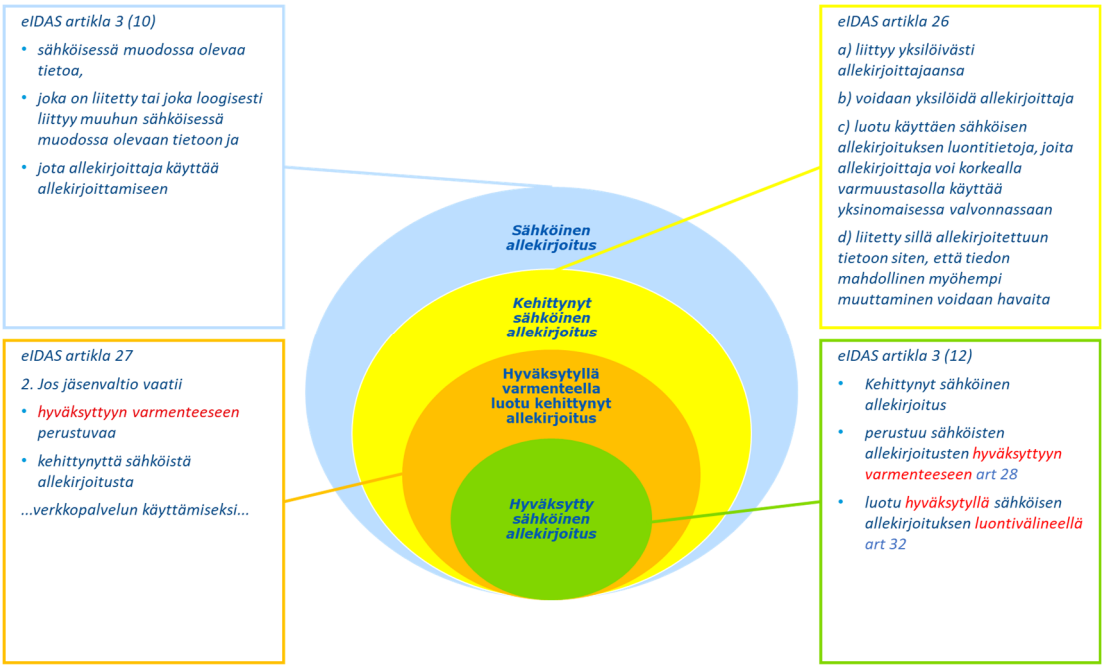
Kehittynyt sähköinen allekirjoitus* tarkoittaa sähköistä allekirjoitusta, joka a) liittyy yksilöivästi allekirjoittajaansa; b) jolla voidaan yksilöidä allekirjoittaja; c) joka on luotu käyttäen sähköisen allekirjoituksen luontitietoja, joita allekirjoittaja voi korkealla varmuustasolla käyttää yksinomaisessa valvonnassaan; ja d) joka on liitetty sillä allekirjoitettuun tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

Kehittynyt sähköinen leima* tarkoittaa sähköistä leimaa, joka a) liittyy yksilöivästi leiman luojaan; b) jolla voidaan yksilöidä leiman luoja; c) joka on luotu käyttäen sähköisen leiman luontitietoja, joita leiman luoja voi korkealla varmuustasolla käyttää valvonnassaan sähköisen leiman luomiseen; ja d) joka on liitetty kohteenaan olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

Hyväksytty sähköinen allekirjoitus* tarkoittaa kehittynyttä sähköistä allekirjoitusta, joka on luotu hyväksytyllä sähköisen allekirjoituksen luontivälineellä ja joka perustuu sähköisten allekirjoitusten hyväksyttyyn varmenteeseen. eIDAS-asetuksen 25 artiklan nojalla (Sähköisten allekirjoitusten oikeusvaikutukset) hyväksytyllä sähköisellä allekirjoituksella on oltava samanlaiset oikeusvaikutukset kuin käsin kirjoitetulla allekirjoituksella.

Hyväksytty sähköinen leima* tarkoittaa kehittynyttä sähköistä leimaa, joka on luotu hyväksytyllä sähköisen leiman luontivälineellä ja joka perustuu sähköisen leiman hyväksyttyyn varmenteeseen. eIDAS-asetuksen 35 artiklan nojalla (Sähköisten leimojen oikeusvaikutukset) hyväksyttyyn sähköiseen leimaan liitetään oletettama tietojen eheydestä ja niiden tietojen alkuperän oikeellisuudesta, joihin hyväksytty sähköinen leima on liitetty.

[10] Ks. ***My data - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen**, Poikola, Kuikkaniemi, Kuittinen,* ***2014***, s. 19 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/77875/My_data_-_johdatus_ihmiskeskeiseen_henkilotiedon_hyodyntamiseen.pdf?sequence=1&isAllowed=y



Kuva 2: eIDAS-asetuksessa sähköiselle allekirjoitukselle määritellyt tasot.

2.2 Säädökset

Sähköiseen tunnistamiseen liittyy useita säädöksiä, joista alla on mainittu olennaisimmat. On hyvä huomata, että kyseisissä säädöksissä käytetään jossain määrin eri terminologiaa, ja esimerkiksi viitatessa sähköiseen tunnistamiseen toimialakohtaisessa maksupalvelulaissa on valittu termi *vahva tunnistus* erotuksena lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, jossa käytetään termiä *vahva sähköinen tunnistus*. Osin nämä erot johtuvat siitä, että niillä tarkoitetaan hieman eri asioita. Tässä markkinaselvityksessä käytetään termiä vahva sähköinen tunnistaminen kuvaamaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaista vahvaa sähköistä tunnistamista ja tunnistuspalvelujen tarjoamista.

2.2.1 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista

Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, jatkossa myös tunnistuslaki) säädetään vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille. Lisäksi laissa säädetään sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (jäljempänä eIDAS) säännösten noudattamisen valvonnasta ja annetaan mainittua asetusta täydentäviä säännöksiä. Tässä laissa säädetään lisäksi tunnistus- ja luottamuspalvelujen vaatimustenmukaisuuden arvioinnista.

Euroopan komissiolle ilmoitettaviin rajat ylittäviin tunnistusjärjestelmiin sovelletaan tätä lakia vain, jollei sähköisestä tunnistamisesta ja luottamuspalveluista annetusta EU:n asetuksesta muuta johdu.

Lakia ei sovelleta yhteisön sisäiseen tunnistamiseen käytettävien palvelujen tarjontaan. Lakia ei sovelleta myöskään yhteisöön, joka käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan.

Lain keskeisenä tavoitteena on edistää sähköistä tunnistamista ja lisätä kuluttajalle turvallisten ja luotettavien sähköisten palvelujen tarjontaa. Laissa säädetään tunnistuspalvelujen yhtenäisistä vaatimuksista sekä tunnistuspalvelujen viranomaisvalvonnasta. Toisaalta lain tavoitteena on myös kehittää sähköisen tunnistamisen markkinoita ja mahdollistaa kilpailua siten, että palveluntarjoajien keskinäinen hinnoittelu pysyy kuluttajalle kohtuullisena.

Tunnistuspalvelun tarjoajan on ennen toimintansa aloittamista tehtävä kirjallinen ilmoitus Liikenne- ja viestintävirastolle. Ilmoituksen voi tehdä Suomeen tai ETA-maahan sijoittautunut tunnistuspalvelun tarjoaja. Liikenne- ja viestintävirasto ylläpitää julkista rekisteriä tunnistuspalveluista, jotka vaatimustenmukaisuuden arvioinnin perusteella täyttävät säädetyt vaatimukset.

Lain olennaisin sisältö käsittelee sähköistä tunnistamista. Sähköisellä tunnistamisella tarkoitetaan luonnollisen henkilön tai oikeushenkilön henkilöllisyyden todentamista sähköisesti. Laki asettaa useita luotettavuus - ja tietoturvallisuusvaatimuksia sähköisen tunnistamisen järjestelmälle, tunnistusmenetelmälle sekä tunnistuspalvelun tarjoajalle. Laissa säädetään mm. tunnistusvälineen myöntämisen edellytyksistä eli ensitunnistamisesta ja siinä sallituista luotettavista lähteistä sekä tunnistusvälineen uusimisesta, sulkemisesta ja muusta elinkaaren hallinnasta. Laissa säädetään tunnistuspalvelun säännöllisestä vaatimustenmukaisuuden arvioinnista ja arviointielinten pätevyydestä ja riippumattomuudesta.

Suomen lainsäädännön vaatimukset vahvalle sähköiselle tunnistamiselle on yhdenmukaistettu eIDAS-asetuksen kanssa. Liikenne- ja viestintävirasto osallistuu aktiivisesti eIDAS-asetuksen mukaisiin vertaisarviointeihin, jotta sääntelyn soveltaminen on mahdollisimman yhdenmukaista muiden EU-jäsenmaiden ja ETA-maiden kanssa. Lainsäädännön vaatimusten yhdenmukaistaminen mahdollistaa sen, että Suomessa vahvaksi sähköiseksi tunnistusvälineeksi hyväksytty korotetun tai korkean varmuustason tunnistusväline tulisi voida sellaisenaan hyväksyä myös eIDAS-asetuksen mukaisena korotetun tai korkean varmuustason tunnistusvälineenä, jotta sitä on mahdollisuutta käyttää rajat ylittävästi muiden EU-jäsenmaiden julkisten hallintojen tarjoamissa sähköisissä asiointipalveluissa.

Laissa säädetään myös pakottavasti käyttäjän oikeuksista, velvollisuuksista ja vastuuvapauksista.

Ilmoituksen yhteydessä tunnistuspalvelun tarjoaja liittyy osaksi luottamusverkostoa. Luottamusverkoston tavoitteena on helpottaa vahvan sähköisen tunnistamisen käyttöä sähköisissä asiointipalveluissa, sillä sähköiset asiointipalvelut voivat hankkia eri tunnistusvälineiden käyttäjien tunnistuksen omaan sähköiseen asiointipalveluunsa luottamusverkoston tunnistusvälityspalvelulta tekemättä sopimuksia kaikkien välineen tarjoajien kanssa erikseen. Tunnistusvälineen tarjoajan on annettava rekisteröidylle tunnistusvälityspalvelulle käyttöoikeus tunnistuspalveluunsa laissa säädetyillä ehdoilla. Laki asettaa tunnistuspalvelun käyttöoikeudesta suoritettavalle korvaukselle enimmäisrajan. Tunnistusvälineen tarjoajan on myös sallittava toiselle tunnistusvälineen tarjoajalle oman tunnistusvälineensä käyttö ensitunnistamisessa laissa säädetyillä ehdoilla. Ensitunnistamisen ketjuttamiselle on säädetty määräaikaisesti enimmäishinta.

Liikenne- ja viestintä*ministeriölle* kuuluu sähköisen tunnistamisen ja sähköisten luottamuspalveluiden yleinen ohjaus, valvonta ja kehittäminen.

Liikenne- ja viestintä*virasto* voi antaa lakia tarkentavia määräyksiä ja valvoo lain noudattamista. Lakia tai sen nojalla annettuja määräyksiä rikkoneeseen voidaan kohdistaa hallintopakkokeinoja Liikenne- ja viestintäviraston päätöksellä.

2.2.2 Valtioneuvoston asetus 169/2016 vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta ja asetus 1212/2018 asetuksen 3 §:n muuttamisesta

Asetuksessa tarkennetaan sitä, mitkä tekniset rajapinnat ovat tunnistuslain yhteentoimivuus- ja turvallisuussääntelyn piirissä ja säädetään tunnistuspalvelun tarjoajien neuvottelu- ja sopimisvelvoitteista luottamusverkostossa. Asetuksessa tarkennetaan luottamusverkoston hallinnollisia vastuita ja säädetään luottamusverkoston yhteistoimintaryhmästä, jonka liikenne- ja viestintävirasto voi asettaa.

2.2.3 Määräys 72 sähköisistä tunnistus- ja luottamuspalveluista

Viestintäviraston Määräyksessä 72A/2018 M sähköisistä tunnistus- ja luottamuspalveluista annetaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 42 §:n nojalla tarkempia määräyksiä

- vahvojen sähköisten tunnistuspalvelujen tietoturvallisuudesta ja yhteentoimivuudesta,
- vahvan sähköisen tunnistamisen palvelujen vaatimustenmukaisuuden arvioinnin kriteereistä ja
- tunnistuspalvelujen arviointielinten riippumattomuus- ja pätevyyskriteereistä,
- hyväksyttyjen sähköisten luottamuspalvelujen vaatimuksista,
- hyväksyttyjen luottamuspalvelujen vaatimustenmukaisuuden arvioinnin riippumattomuus- ja pätevyyskriteereistä siltä osin, kun näistä ei ole säädetty Euroopan Unionin lainsäädännössä, sekä
- sähköisen allekirjoituksen tai sähköisen leiman luontivälineen sertifiointilaitoksen nimeämisen kriteereistä siltä osin, kun näistä ei ole säädetty Euroopan unionin lainsäädännössä.

Määräys on alemman asteista lainsäädäntöä suhteessa lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista sekä eIDAS-asetukseen.

Määräystä sovelletaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain tarkoittamien Viestintävirastolle (nykyisin Liikenne- ja viestintävirasto) ilmoitettujen vahvan sähköisen tunnistamisen tunnistusvälineiden ja tunnistusvälityspalvelujen tarjontaan sekä näiden vaatimustenmukaisuuden arviointiin.

Määräystä sovelletaan myös eIDAS-asetuksessa tarkoitettuihin hyväksyttyihin sähköisiin luottamuspalveluihin ja näiden vaatimustenmukaisuuden arviointiin sekä sähköisen allekirjoituksen tai leiman luontivälineiden sertifiointilaitoksen nimeämiseen.

Määräystä sovelletaan Euroopan komissiolle ilmoitettaviin vahvan sähköisen tunnistamisen järjestelmiin tai 2 edellä momentissa tarkoitettuihin luottamuspalveluihin ja näiden vaatimustenmukaisuuden arviointiin sekä sähköisen allekirjoituksen tai leiman luontivälineiden sertifiointiin vain, jollei eIDAS-asetuksesta tai sen nojalla annetuista komission täytäntöönpanosäädöksistä muuta johdu.

Määräyksen tavoitteena on selkeyttää toimijoille ja vaatimustenmukaisuuden arviointilaitoksille luottamuspalvelujen vaatimuksia siltä osin, kun komissio ei ole käyttänyt luottamuspalveluihin liittyvää säädäntötoimivaltaansa ja antanut täytäntöönpanosäädöksiä, joissa viitattaisiin tarpeellisiin standardeihin.

Määräyksen valmistelussa on pyritty hyödyntämään mahdollisimman laajasti kansainvälisiä standardeja, vaatimusmäärittelyjä ja ilmoittamistapoja. Ratkaisulla pyritään helpottamaan rajat ylittävää palveluntarjontaa ja välttämään kansallisesti räätälöityjä vaatimuksia. Määräyksen tavoitteena on selkeyttää hyväksyttyjen luot-

tamuspalvelujen eIDAS-asetuksessa säädettyjä vaatimuksia viittaamalla EU:n valmistelutyössä viitoittamiin kansainvälisiin standardeihin siltä osin, kun niihin ei ole ainakaan toistaiseksi tehty viittauksia komission täytäntöönpanosäädöksillä, vaikka siihen olisi eIDAS-asetuksessa toimivalta.

Tunnistuspalvelujen arvioinnin osalta määräyksen tavoitteena on selkeyttää toimijoille, millä perusteella niiden käyttämät auditoijat ovat päteviä tekemään tunnistusjärjestelmän arviointeja. Tunnistuspalveluntarjoajan arviointielimen ei tarvitse hakea erikseen hyväksyntää, ellei se ole vaatimustenmukaisuuden arviointilaitos. Määräyksen tavoitteena on, että toimijat voisivat mahdollisimman paljon hyödyntää auditointeja, joita ne tekevät tai teettävät jo ennestään.

Määräys on valittu ohjauskeinoksi niissä tilanteissa, joissa on nähtävissä, että muut keinot eivät ole toimijoiden kannalta riittävän ennakoitavia ja tasapuolisia tai palvelujen käyttäjien ja niihin luottavien tahojen kannalta riittävän tehokkaita sääntelyn tavoitteiden saavuttamiseksi. Määräyksen, ohjeiden ja suositusten laatimisessa on joka tapauksessa vahvoja yhteissääntelyn piirteitä, koska ne laaditaan avoimessa työryhmäyhteistyössä toimijoiden kanssa.

2.2.4 eIDAS-asetus

Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta eli niin sanotussa eIDAS-asetuksessa säädetään sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla.

eIDAS-asetus sääntelee rajat ylittävää sähköistä tunnistamista. Asetuksen keskeisenä tavoitteena on tarjota sähköisiä tunnistusvälineitä, joilla on mahdollista tunnistautua julkisen hallinnon palveluissa koko EU:ssa. Notifioidun rajat ylittävän tunnistamisen tunnustamisvelvoite eIDAS-asetuksessa koskee korotettua ja korkeaa varmuustasoa.

eIDAS-asetus tuli voimaan 1.7.2016 ja se toi muutoksia myös kansalliseen sähköiseen tunnistamiseen. Tunnistus- ja luottamuspalvelulain vaatimuksia muutettiin vastaamaan EU-sääntelyä.

eIDAS-asetuksen uudelleenarviointi on parhaillaan käynnissä ja komissiolta odotetaan muutettua asetusehdotusta kevään 2021 aikana. Arvioinnissa painotetaan sähköisen tunnistamisen tarjontaa ja käyttöä yksityisellä sektorilla, mikä on Suomessa ollut tunnistuslain lainsäädäntöpoliittinen päämäärä jo vuodesta 2009.

2.2.5 Komission varmuustasoasetus (EU) 2015/1502 ja tunnistuslaki

Komissio on antanut eIDAS-asetuksen 8 artiklan nojalla täytäntöönpanoasetuksen, jossa tarkennetaan komissiolle notifioitavan vahvan sähköisen tunnistusjärjestelmän ja sen puitteissa käyttäjälle myönnettävän tunnistusmenetelmän (eli tunnistusvälineen) tekniset vaatimukset kolmella eri varmuustasolla: matala, korotettu ja korkea.

Tunnistuslaissa viitataan useassa kohdassa komission varmuustasoasetuksen vaatimuksiin. Suomessa on käytössä kaksi eIDAS-asetuksen mukaista tunnistuksen varmuustasoa: korotettu ja korkea. Käytännössä kansallinen laki velvoittaa Suomessa toimivat vahvan sähköisen tunnistamisen järjestelmät täyttämään vähintään samat luotettavuutta ja tietoturvaa koskevat vaatimukset kuin mitä Euroopan unionin lainsäädännössä vaaditaan unionin rajat ylittäviltä sähköisen tunnistamisen järjestelmiltä.

Korotetun ja korkean tason tunnistuspalvelun tarjoajat voivat halutessaan hakea EU-notifiointia missä tahansa vaiheessa, kun ne täyttävät kansallisesti asetetut vaatimukset. Tunnistuspalvelun tarjoajien ei tarvitse laatia erillistä tunnistusratkaisua rajat ylittäviä tilanteita ja kansallista tunnistamista varten. Jos kansallinen tunnistusmenetelmä läpäisee jäsenvaltioiden vertaisarvioinnin, tunnistusvälineellä voi tunnistautua julkisen hallinnon palveluissa EU:n jäsenvaltioissa.

Kansallisesti vaatimukset täyttävän vahvan sähköisen tunnistuspalvelun tunnistaa siitä, että se löytyy Liikenne- ja viestintäviraston rekisteristä.[11] Notifioinnissa ja siihen liittyvässä jäsenvaltioiden tekemässä vertaisarvioinnissa sovelletaan eIDAS-asetusta ja EU:n komission täytäntöönpanosäädöksiä.

2.2.6 (Toinen) Maksupalveludirektiivi (PSD2)

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/1001/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta eli niin sanotussa PSD2-direktiivissä säädetään maksupalveluista ja muun muassa maksupalveluissa käytettävistä tunnistusjärjestelmistä ja -menetelmistä.

Maksupalveludirektiivin eli PSD2 (Payments Services Directive 2) tavoitteena on yhdistää erilaiset maksupalvelut laajemmin sääntelyn piiriin sekä samalla päivittää maksupalvelujen sääntelyä vastaamaan markkinoilla tapahtunutta kehitystä.

Suomessa direktiivin määräykset toteutettiin kahdessa osassa muuttamalla maksupalvelulakia ja maksulaitoslakia. Muutokset tulivat voimaan pääosin määräpäivään 13.1.2018 mennessä.

Direktiivin I osan säännökset koskevat maksupalveluntarjoajia ja maksulaitostoimiluvan hakemisen vaatimuksia, osan II säännökset tietojen jakamista ja avoimuutta ja osan IV osaston säännökset maksupalvelujen tarjoamiseen ja käyttöön liittyviä oikeuksia ja velvollisuuksia.

Direktiivin artiklassa 97 säädetään tunnistamisesta ja tilanteista, joissa on käytettävä vahvaa tunnistamista. Säännöksen perusteella esimerkiksi maksutilin käyttö verkon kautta ja maksaminen verkossa vaatii lähtökohtaisesti aina asiakkaan vahvan tunnistamisen. Pelkästään maksukortin tiedot antamalla ei enää pysty maksamaan verkossa kuin poikkeustilanteissa.[12] Artiklassa 98 säädetään todentamista ja viestintää koskevista teknisistä sääntelystandardeista ja komission toimivallasta hyväksyä tekniset sääntelystandardit.

2.2.7 Komission delegoitu asetus (EU) 2018/389 asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevista teknisillä sääntelystandardeista (niin kutsuttu RTS SCA & CSC)

Komissio on antanut maksupalveludirektiivin 98 artiklan nojalla delegoidun asetuksen, jossa tarkennetaan vahvan tunnistamisen vaatimukset maksupalveludirektiivin soveltamisalalla. Asetuksen II luvussa säädetään asiakkaan vahvan tunnistamisen soveltamista koskevat turvatoimenpiteet ja esimerkiksi tietoon, hallussapitoon ja ominaisuuksiin perustuvien todentamistekijöiden vaatimuksista ja niiden riippumattomuudesta toisistaan. Asetuksessa säädetään myös poikkeuksista eli tilanteista, joissa vahvaa tunnistamista ei tarvitse käyttää.

[11] Liikenne- ja viestintävirasto ylläpitää verkkosivustollaan rekisteriä lainsäädännön vaatimukset täyttävistä vahvan sähköisen tunnistuspalvelun tarjoajista. Rekisterissä on myös tiedot toimijoista, jotka ovat tehneet virastolle ilmoituksen vahvan sähköisen tunnistuspalvelun tarjoamisen aloittamisesta, mutta joiden vaatimustenmukaisuuden arviointi on vielä kesken. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

[12] Vahvasta tunnistamisesta maksamisen yhteydessä katso tarkemmin jäljempänä luku 6.2.

2.2.8 Maksupalvelulaki

Maksupalvelulaissa (290/2010) säädetään maksupalveluja koskevasta tiedonantovelvollisuudesta ja sopimusehdoista sekä maksupalvelujen toteuttamisesta.

Maksupalvelulakia sovelletaan käteispanoihin ja nostoihin sekä maksutilin hoitoon, maksutapahtuman toteuttamiseen, maksuvälineen liikkeeseenlaskuun, maksutapahtumien hyväksymiseen, rahanvälitykseen, maksutoimeksiantoihin sekä tilitietopalveluihin. Maksupalvelulain sisältö noudattaa EU:n maksupalveludirektiivin sisältöä ja laajentaa lain soveltamisalaa aiempaan lakiin verrattuna, johtuen erilaisten maksutapojen ja vaihtoehtojen lisääntymisestä markkinoilla.

Maksupalvelulaissa (290/2010) on vahvan sähköisen tunnistamisen käyttöä edellyttävää sääntelyä, joka liittyy maksutapahtumien toteuttamiseen. Maksupalvelulain 85 c §:n mukaan vahvaa tunnistamista on käytettävä muun muassa, jos maksaja käyttää maksutiliään tietoverkon välityksellä tai käynnistää sähköisen maksutapahtuman.

Maksupalvelulain säännökset avaavat kuluttajan tilitiedot tietyin rajoituksin myös muiden palveluntarjoajien käyttöön. Maksupalvelut eivät näin ollen ole enää sidoksissa kuluttajan käyttämään yksittäiseen pankkiin, vaan tili- ja maksutapahtumia on mahdollista käsitellä useiden eri palvelujen kautta. Myös kuluttajan omaa vastuuta huolimattomuudesta aiheutuvissa väärinkäytöstapauksissa on lakimuutoksin lievennetty. Toisaalta maksupalvelulaki lisää vahvan sähköisen tunnistamisen merkitystä asioinnissa, sillä turvallisuuden vaatimus tulee korostumaan entisestään palveluvalikoiman laajentuessa.

2.2.9 Tunnistuslain ja maksupalvelulain vaatimusten yhteensopivuus

Komission eIDAS-asetuksen nojalla antamaa sähköisen tunnistamisen varmuustasoasetusta ja PSD2-direktiivin nojalla antamaa maksupalvelualan delegoitua asetusta vahvasta tunnistamisesta ei ole EU-tasolla yhdenmukaistettu.

Maksupalvelulaissa käytetään termiä vahva tunnistus, kun tunnistuslaissa käytetään termiä vahva sähköinen tunnistus. Nämä voivat poiketa jossain määrin toisistaan ja vahvan tunnistuksen ja vahvan sähköisen tunnistuksen välille ei voida laittaa suoraan yhtäläisyysmerkkiä.

Liikenne- ja viestintävirasto ja Finanssivalvonta ovat vuonna 2018 tarkastelleet yleisen vahvan sähköisen tunnistamisen ja finanssialan toimialakohtaisen vahvan tunnistamisen vaatimusten yhteensopivuutta ja pyytäneet arviosta lausuntoja toimialalta. Johtopäätös oli, että samaa käyttäjälle tarjottavaa sähköistä tunnistusmenetelmää on mahdollista käyttää molempien sääntelyjen mukaisesti, kunhan eräissä yksityiskohdissa täyttää kulloinkin tarkemman tai tiukemman sääntelyn vaatimukset.

Liikenne- ja viestintävirasto on 2020-2021 käynnissä olevan määräysuudistuksensa yhteydessä tarkastellut maksupalvelusääntelyn toimialakohtaisen soveltamiskäytännön tarkentumista ja vertaillut sitä tunnistuslain mukaiseen yleiseen vahvaan sähköiseen tunnistamiseen.

Vuoden 2018 ja 2020 tarkastelut on julkaistu Liikenne- ja viestintäviraston verkkosivulla.[13]

[13] 1) Kalvot 10102018 PSD2-seurantaryhmä eIDAS- ja PSD2-RTS-vaatimusten vertailu https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kalvot%2010102018%20PSD2-seurantaryhm%C3%A4%20eIDAS-%20ja%20PSD2-RTS-vaatimusten%20vertailu.pdf
2) Lausuntoversio 10102018 Vivin ja Fivan eIDAS-PSD2-RTS-vertailu (excel) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lausuntoversio%2010102018%20Vivin%20ja%20Fivan%20eIDAS-PSD2-RTS-vertailu.XLSX

2.2.10 Laki digitaalisten palvelujen tarjoamisesta (306/2019)

Laissa digitaalisten palvelujen tarjoamisesta säädetään julkisen sektorin elinten verkkosivujen ja mobiilisovellusten saavutettavuuden vähimmäisvaatimuksista ja saavutettavuuden valvonnasta ja viranomaisten velvoitteista digitaalisten palvelujen järjestämisessä yleisölle.

Suomessa lain soveltamisalaa on laajennettu direktiivistä ja laki koskee tunnistuslain mukaisia vahvan sähköisen tunnistuspalvelun tarjoajia. Lailla ei säädetä yleistä velvollisuutta tuottaa sähköiset tunnistuspalvelut esteettömästi, vaan se koskee tunnistuspalveluja verkkosivujen ja mobiilisovellusten saavutettavuuden osalta. Tunnistuspalveluja valvoo tältä osin Etelä-Suomen aluehallintovirasto.

Digi- ja väestötietovirasto tuottaa ohjeistuksia ja muuta tukimateriaalia digitaalisten palvelujen järjestämiseen liittyen.

Laki tuli voimaan 1.4.2019 ja sillä toimeenpannaan saavutettavuusdirektiivi Suomessa.

2.2.11 Yleinen tietosuoja-asetus (GDPR)

Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta eli niin sanotussa yleisessä tietosuoja-asetuksessa (GDPR-asetus) säädetään henkilötietojen käsittelystä. Lain tavoitteena on yhdenmukaistaa henkilötietoja koskevaa sääntelyä koko EU:n alueella ja parantaa yksityishenkilöiden yksityisuudensuojaa.

Tietosuoja-asetusta sovelletaan kaikissa viranomaisissa, organisaatioissa ja yrityksissä, jotka keräävät, käsittelevät tai säilyttävät henkilötietoja. Henkilötiedon käsite on laaja. Henkilötiedoiksi määritellään kaikki sellainen tieto, joista yksilö on tunnistettavissa. Henkilörekisteri muodostuu henkilötietoja sisältävästä tietomassasta, josta yksittäinen henkilötieto on haettavissa. Rekisterinpitäjällä tarkoitetaan mitä tahansa organisaatiota, luonnollista henkilöä, viranomaista tai oikeushenkilöä, joka käsittelee henkilötietoja sisältävää rekisteriä.

Tietosuoja-asetus asettaa vaatimuksia rekisterinpitäjille ja sen tavoitteena on henkilötietojen käsittelyn läpinäkyvyys, hallittavuus ja tietoturvallisuus. Lähtökohtaisesti henkilötietojen tulisi olla asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Myös tietoturvaan ja sen ylläpitoon kuuluvat toimenpiteet on huomioitu tietoturvaasetuksessa. Tietoturvakäytäntöjen on oltava ajantasaisia ja dokumentoituja. Mikäli henkilötietoja käsittelee julkinen hallintoon kuuluva toimija tai viranomainen, on tietosuojavastaavan nimeäminen pakollista. Tietosuojavastaava on nimitettävä myös siinä tapauksessa, jos organisaation ydintoimintoihin kuuluu arkojen henkilötietojen tai laajojen henkilötietorekistereiden käsittely. Tapahtuneesta tietoturvaloukkauksesta on ilmoitettava tietosuojaviranomaiselle ja asianosaselle mahdollisimman pian.

Asetus antaa yksityishenkilölle laajat oikeudet pyytää rekisterinpitäjältä selvitystä siitä, mitä tietoja hänestä on tallennettu ja missä rekisterissä tietoja säilytetään.

3) Traficomin kysely 04082020 tunnistus- ja luottamuspalvelumääräyksen muutostarpeista, kohta 3.3 PSD2:sta tai muusta lainsäädännöstä tulevat rinnakkaiset tekniset vaatimukset https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficomin%20kysely%2004082020%20tunnistus-%20ja%20luottamuspalvelum%C3%A4%C3%A4r%C3%A4yksen%2072%20muutostarpeista.pdf

Tietoja on oikeus vaatia korjattavaksi tai poistettavaksi. Mikäli kyseessä ei ole lakisääteisen velvoitteen noudattamiseksi kerättävä henkilötieto, on henkilöltä saatava suostumus henkilötietojen käsittelyyn ja suostumus on oltava tarvittaessa myös peruutettavissa. Asetuksen noudattamatta jättäminen voi johtaa sakkorangaistukseen, jonka summa määräytyy pääsääntöisesti yrityksen tai organisaation liikevaihdon perusteella.

Tunnistuslain muutosesityksessä hallituksen esityksessä HE 237/2020[14] arvioidaan tunnistuslain ja yleisen tietosuoja-asetuksen suhdetta.

2.2.12 Tietosuojalaki

Tietosuojalaissa säädetään eräistä henkilötietojen käsittelyyn liittyvistä asioista, joista yleisen tietosuoja-asetuksen nojalla voidaan säätää kansallisesti. Lain 29 §:ssä säädetään henkilötunnuksen käsittelystä.

2.2.13 Esteettömyysdirektiivi

Euroopan parlamentin ja neuvoston direktiiviin (EU) 2019/882, annettu 17 päivänä huhtikuuta 2019, tuotteiden ja palvelujen esteettömyysvaatimuksista eli niin sanotussa esteettömyysdirektiiviin päätavoitteena on vammaisten ja muiden toimintarajoitteisten henkilöiden täysimääräinen ja tehokas osallistuminen ja itsenäisen elämän helpottuminen YK:n vammaisyleissopimuksen tavoitteiden mukaisesti. Direktiivin tavoitteena on edistää esteettömien tuotteiden ja palvelujen saatavuutta ja liikkuvuutta yhdenmukaistamalla niitä koskevia vaatimuksia jäsenvaltioissa. Direktiivillä helpotetaan jäsenmaiden YK:n vammaisyleissopimuksen täytäntöönpanoa ja sopimuksen velvoitteiden toteuttamista säätämällä yhteisistä säännöistä. Direktiiviä sovelletaan muun muassa kuluttajapankkipalvelujen ja verkkokaupan tunnistustapoihin ja sähköiseen allekirjoittamiseen.

Direktiiviä ollaan parhaillaan implementoimassa kansalliseen lainsäädäntöön Suomessa. Siten tässä markkinaselvityksessä ei ole tarkemmin arvioitu direktiivin ja sen myötä kansalliseen lainsäädäntöön tehtyjen muutoksien vaikutuksia tunnistuspalveluihin ja identiteettipalveluihin.

[14] HE 237/2020 vp https://www.eduskunta.fi/valtiopaivaasiakirjat/HE+237/2020

3 Sähköiset tunnistus- ja identiteettipalvelut yleisesti

Sähköiset tunnistus- ja identiteettipalvelut ovat osa laaja-alaisempaa sähköisen asioinnin kokonaisuutta eli sähköisen asioinnin ekosysteemiä. Sähköisiä tunnistus- ja identiteettipalveluja voidaan myös hyödyntää puhelinasioinnissa ja fyysisessä käyntiasioinnissa, vaikkei niitä alun perin ole suunniteltu niitä varten. Tunnistus- ja identiteettipalvelut mahdollistavat osaltaan sähköisten palvelujen tarjoamisen ja sähköisen asioinnin. Tunnistuspalvelujen ja -identiteettipalvelujen tarkoituksena on yksilöidä sähköistä asiointipalvelua käyttävä asiakas, jotta hänelle voidaan antaa yksilöityjä oikeuksia käsitellä itseään ja/tai muita henkilöitä sekä organisaatioita koskevia tietoja (lukea, muokata, poistaa) ja tehdä muita erikseen määriteltyjä toimenpiteitä.

3.1 Sähköinen tunnistaminen ja sähköisen asioinnin ekosysteemi

3.1.1 Sähköinen tunnistaminen ja MyData tai Self-Sovereign Identity

Sähköistä tunnistamista ja sen roolia sähköisen asioinnin ekosysteemissä voi kuvata esimerkiksi Omadata -tutkimuksessa hahmotetuilla malleilla. Liikenne- ja viestintäministeriö julkaisi vuonna 2014 selvityksen *MyData - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen*. Selvitystä päivitettiin vuonna 2018.[15] MyData -selvitys soveltuu hyvin pohjaksi myös itsehallittavan identiteetin (SSI, Self-Sovereign Identity) roolien ja toimintojen tarkasteluun.

Seuraavassa on vertailtu sähköistä tunnistamista, erityisesti vahvaa sähköistä tunnistamista, MyData-selvityksessä omaksuttuun henkilötiedon jakamisen ekosysteemin roolien ryhmittelyyn (selvitys 2018 s. 40).

Tunnistamisen roolit	MyData -ekosysteemin roolit
Luonnollinen tai oikeushenkilö, jonka henkilötiedoista tai tiedoista on kysymys. Oikeushenkilön tunnistusvälineeseen on aina kytkettävä luonnollisen henkilön tunnistusväline. Luonnollisella henkilöllä tai oikeushenkilöllä on hallinnassaan vahva sähköinen tunnistusväline. Tunnistusvälineellä sen haltija voi osoittaa henkilöllisyytensä ja tunnistuspalvelun mahdollistamat tietonsa luottavalle osapuolelle eli sähköiselle asiointipalvelulle.	**Ihminen** on verkostossa identiteetin haltija ja se henkilö, jonka datasta on kyse. Ihminen hallinnoi, mitkä tahot saavat hänen dataansa ja mihin käyttötarkoituksiin. Datan välittämisen verkostossa voidaan henkilötiedon lisäksi välittää myös esimerkiksi yrityksiin tai esineisiin liittyvää tietoa. Teknisesti ei ole merkittävää eroa, onko dataa hallinnoiva taho ihminen vai esimerkiksi organisaatio, mutta lainsäädäntö on erilainen silloin, jos käsitellään henkilötietietoa.
Luotettu lähde on eIDAS-asetuksen valossa kansallisesti määritelty lähde, johon tunnistusvälineen tarjoaja voi luottaa varmistaessaan tunnistusvälineen hakijan henkilöllisyyden. Tunnistuslain mukaan luotettuja lähteitä ovat väestötietojärjestelmä, pa-	**Datan lähde** kerää, käsittelee ja mahdollistaa henkilötiedon jakelun muille toimijoille verkostossa. Datan välittämisen verkostossa voidaan henkilötiedon lisäksi välittää myös esimerkiksi yrityksiin tai esineisiin liittyvää tietoa.

[15] *MyData - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen,* 2018 (Antti Poikola, Kai Kuikkaniemi, Ossi Kuittinen, Harri Honko, Aleksi Knuutila), https://julkaisut.valtioneuvosto.fi/handle/10024/77875

tentti- ja rekisterihallituksen yhteisörekisterit ja viranomaisen myöntämät passit ja henkilökortit. Tunnistussääntelyn tietovalikoima on rajattu ja jakautuu vähimmäistietoihin (kuten henkilön nimi ja syntymäaika) ja lisätietoihin (kuten henkilön osoite). eIDAS-asetuksen uudistamisen yksi olennainen muutoskohde on luotettavien lähteiden sääntelymalli ja tietovalikoiman (attribuuttien) lisääminen vahva sähköisen tunnistamisen/autentikoinnin yhteydessä.	Toimijat voivat olla samanaikaisesti useammissa rooleissa. Esimerkiksi yritykset ovat tyypillisesti sekä datan lähteitä että dataa hyödyntävien palvelujen tarjoajia
Tunnistamiseen **luottava osapuoli** eli sähköinen **asiointipalvelu**, johon tunnistusvälineen haltija tunnistautuu. Perustoteutuksessa tunnistuspalvelu välittää sähköiselle asiointipalvelulle vähimmäishenkilötiedot. Tunnistuspalvelu voi myös rikastaa henkilötietoja ja toimittaa niitä luottavalle osapuolelle. Yleisen tietosuoja-asetuksen edellytysten on tällöin täytyttävä. Tunnistuslain mukaan tunnistuspalvelu voi toimittaa luottavalle osapuolelle myös vain köyhdytetyn tiedon eli esimerkiksi vahvasti autentikoidun ikätiedon. Vahvaan tunnistamiseen ei ole määritelty MyData- mallin mukaista luvitustoimintoa oletusarvoisesti, vaan sellainen olisi luottavalle osapuolelle rakennettu lisätoiminto.	**Dataa käyttävä palvelu** voi henkilön valtuuttamana hakea ja käyttää henkilötietoa yhdestä tai useammasta datan lähteestä.
Tunnistusvälineen tarjoaja mahdollistaa tunnistusvälineen haltijalle ja **tunnistusvälityspalvelu** sähköiselle asiointipalvelulle henkilöllisyyden varmentamisen osapuolelle. Vahvaan tunnistamiseen ei ole määritelty MyData- mallin mukaista luvitustoimintoa oletusarvoisesti, vaan sellainen olisi luottavalle osapuolelle rakennettu lisätoiminto. Tunnistusvälineitä tarjoavat pankit toimivat sikäli kaksoisroolissa, että niiden tunnistusmenetelmät ovat käytössä	**Operaattori** mahdollistaa henkilötiedon käyttölupien digitaalisen hallinnan ja varmentamisen tarjoamalla MyData-tilipalveluja. Myös muissa rooleissa olevat toimijat voivat ottaa lisäksi operaattorin roolin ja ylläpitää itse MyData-tiliä, jota kautta ne kytkeytyvät verkostoon.

myös niiden omissa pankki- ja maksupalveluissa eli niiden omissa sähköisissä asiointipalveluissa. eIDAS-asetuksessa säädetyt sähköiset allekirjoitukset ja sähköiset leimat ovat teknisesti menetelmiä, joita voidaan käyttää luonnollisen tai oikeushenkilön tahdonilmaisun vahvistamisessa ja validoinnissa.	

Taulukko 1: Sähköinen tunnistamisen roolit suhteessa MyData -ekosysteemin rooleihin.

3.1.2 Sähköinen asiointi, puhelinasiointi ja käyntiasiointi

Edellä esitetyn taulukon 1 rooleja voi käytännössä tarkastella ensinnäkin siltä kannalta, millaisia tarpeita sähköisillä asiointipalveluilla on varmistaa asiakkaansa henkilöllisyys asiointitilanteissa. Kysymys on tällöin pohjimmiltaan siitä, millaisia ICT-palveluita asiointipalvelu tarvitsee rakentaessaan sähköisiä asiointipalvelujaan.

Sähköisessä asiointipalvelussa voidaan käyttää vahvaa sähköistä tunnistamista tai jotain muuta seuraavassa kohdassa (3.2) kuvattuja tapoja. Vahvan sähköisen tunnistamisen voi hankkia luottamusverkoston tunnistusvälityspalvelulta sopimuksella ja parhaassa tapauksessa riittää, että toteuttaa yhden rajapintaintegraation tunnistusvälityspalvelun kanssa. Muita tunnistustapoja voi joko toteuttaa itse tai hankkia toteutuksia erilaisilta ICT-palveluilta.

Sähköisen tunnistamisen integrointiin puhelinasioinnissa ei ole vielä laajalti levinneitä vakioratkaisuja. Siitä syystä sähköisissä asiointipalveluissa yhä edelleen saatetaan "tunnistaa" asiakas kysymällä tältä tietoja, joiden ei pitäisi olla muiden kuin oikean asiakkaan tiedossa. Tähän toimintamalliin liittyy myös yleinen epävarma ja tietosuojan kannalta ei-hyväksyttävä tapa kysyä henkilötunnusta. Sähköisen tunnistamisen yhdistäminen puhelinasiointiin edellyttää, että sähköisen asiointipalvelun ICT-järjestelmissä rakennetaan tekninen ratkaisu tunnistamisen yhdistämiseksi puhelinpalveluihin. Esimerkiksi pankit ovat toteuttaneet omissa pankkipalveluissaan tällaisia ratkaisuja.

Käyntiasioinnissa asiointipalvelu yleensä tarkistaa asiakkaan henkilöllisyyden fyysisestä asiakirjasta. Asiakirja voi olla viranomaisen myöntämä virallinen asiakirja, eli passi tai henkilökortti, tai ei-virallinen asiakirja, esimerkiksi jäsenkortti, johon asiointipalvelu katsoo voivansa luottaa. Käyntiasioinnissa voitaisiin kuitenkin hyödyntää myös sähköistä tunnistamista - kirjastokorttia voisi pitää tästä eräänlaisena esimerkkinä. Valtiovarainministeriön käynnissä olevan Digitaalisen henkilöllisyyden hankkeen tarkoituksena on tarjota taustajärjestelmäpohjainen mobiilihenkilökortti, jolla henkilö voisi käyntiasioinnissa osoittaa henkilöllisyytensä ja muita viranomaisen hänelle myöntämiä lupia. Asiointipalvelujen täytynee tällaista palvelua käyttääkseen integroitua viranomaisen järjestelmään voidakseen validoida asiakkaan esittämän mobiilihenkilökortin.

3.1.3 Tunnistuspalvelut ja muut sähköisen asioinnin mahdollistajapalvelut

Edellä esitetyn taulukon 1 operaattoriroolia voinee luonnehtia niin, että se kattaa kaikki palvelut, jotka kolmansina osapuolina yhdistävät henkilön ja tämän henkilötiedot käytettäväksi sähköisessä asioinnissa. Koska kysymyksessä on kolmas osapuoli, johon kaikkien muiden tulee voida luottaa, keskeinen kysymys on, mihin luottamus perustuu. Se voi perustua toimijoiden viranomaisvalvontaan ja säänneltyyn rooliin, kuten vahvassa sähköisessä tunnistamisessa. Tai se voi perustua ekosysteemin osapuolten keskinäisiin sopimuksiin ja sitoutumiseen tiettyjen toimintamallien, standardien ja sääntöjen noudattamiseen. Tämän selvityksen kan-

nalta olennaisia ovat vahvan sähköisen tunnistusvälineen ja tunnistusvälityspalvelun tarjoajat. Myös muun tunnistuksen kuin vahvan sähköisen tunnistuksen tarjoajat kuuluvat tähän ryhmään.

Itsehallittavan identiteetin eli Omadata-malleissa käyttäjällä on mobiilisovellus, jolla hän hallinnoi ja luvittaa tietojaan. Sovellus on yhdistelmä henkilöllisyyden autentikointia eli tunnistamista ja sähköistä allekirjoitusta. Sovelluksen tarjoajan rooli on keskeinen ekosysteemissä, sillä tämän vastuulla on taata se, että sovellus on oikean henkilön hallussa ja että se on turvallinen.

Sähköiseen asiointiin liittyviä lisätoimintoja tai pääasiallisia toimintoja ovat maksut ja sähköiset allekirjoitukset. Maksupalveluja tarjoavat maksupalvelulain mukaiset toimijat. Sähköisiä allekirjoituksia ja leimoja säännellään eIDAS-asetuksessa. eIDAS-asetuksessa säännellään myös monia muita sähköisiä luottamuspalveluja, kuten aikaleimoja ja verkkosivuvarmenteita, joita tarvitaan sähköisen asiointipalvelun rakentamisessa.

3.1.4 Henkilötiedon lähteet

Tiedonlähteitä sähköisessä asioinnissa voi kuvata käytännönläheisesti henkilörekistereinä. Ne voivat olla julkisen tai yksityisen tahon ylläpitämiä ja niiden tiedon luotettavuuden taso voi vaihdella. Väestötietojärjestelmä ja patentti- ja rekisterihallituksen kaupparekisteri ovat esimerkkejä rekistereistä, joihin liittyy vahva lakiin perustuva luotettavuus ja joiden tietojen käyttöön saamiselle on määritelty valmiit käyttöehdot ja tekniset rajapinnat.

Ekosysteemin kehittämisen kannalta on ilmeistä, että rekistereiden luotettavuuden määrittelyyn ja tekniseen käyttöön tarvitaan laajemmin ratkaisuja, joiden avulla niiden tiedot saadaan käyttöön sähköisessä asioinnissa.

Julkisen hallinnon ja yksityisen sektorin sähköisten asiointipalvelujen käyttötarpeet eivät rajoitu yhteen maahan, vaan sähköisen asioinnin on oltava mahdollista myös toisessa valtiossa. Kun eri lähteistä peräisin olevien tietojen yhdistämistä yhteen henkilöön ei voida rajat ylittävässä asioinnissa sitoa kansalliseen henkilötunnukseen, tähän tarvitaan muita ratkaisuja *(identity matching, record matching*).

Eri toimialoilla on lukuisia esimerkkejä hankkeista, joissa on suunniteltu tai toteutettu tiettyyn toimintaympäristöön tapoja jakaa tietoja eri lähteistä. Esimerkiksi EU:n tukemassa MyAcademicID -hankkeessa[16] selvitetään tapoja yhdistää tiedot opiskelijan kotiyliopistosta attribuutteina eIDAS-asetuksen mukaiseen notifioituun tunnistusvälineeseen ja välittää näitä tietoja eIDAS-yhteentoimivuusjärjestelmässä. Toimialakohtaisena yksityisen sektorin toteutuksena voi mainita Vastuu Group Oy:n sähköiset palvelut, joita tarjotaan muun muassa rakennustöiden tilaajille helpottamaan tilaajavastuuseen, verotukseen ja työturvallisuuteen liittyvien tietojen hallinnoimista ja rakennustyömailla työskentelevien tunnistamiseen ja pätevyyksien todentamiseen.

3.1.5 Yhteentoimivuus edellyttää yhteisiä standardeja

Sähköisen tunnistamisen tai henkilötietojen jakelun ekosysteemi tarvitsee toimiakseen teknisen arkkitehtuurin ja yhteisiä standardeja.

My Data -selvityksessä yhteentoimivuuden viitekehys ryhmitellään neljään eri tasoon

- luottamusverkostot
- käyttölupien hallinta
- henkilökohtaiset data-alustat ja
- tietomallit.

[16] https://myacademic-id.eu/the-project/about-ok

Ekosysteemin osapuolten yhteenliittämistapa puolestaan ryhmitellään MyData -selvityksessä kolmeen eri malliin

- API-ekosysteemi, jossa verkoston toimijat käyttävät toistensa rajapintoja (tunnistamisen luottamusverkosto ja eIDAS-solmupistejärjestelmä ovat esimerkkejä tästä mallista)
- organisaatiokohtainen alusta, jossa yksittäinen toimija kerää ja harmonisoi dataa useasta lähteestä ja jakelee sitä eteenpäin. Esimerkkeinä on esitetty Google, Facebook, Alibaba ja Amazon.
- MyData -malli, jossa selvityksen vision mukaan henkilötiedon hallinnan palveluja tarjoavat toimijat ovat keskenään kilpailevia, mutta muodostavat yhteentoimivan verkoston ja yhdessä tarjoavat infrastruktuurin henkilötiedon välittämiseen.

Itsehallittava identiteetin (SSI) malli toteuttaa omadatan periaatteita. Teknisesti mallissa selvitetään lohkoketjuteknologian käyttämistä.

Seuraavassa on lainattu Lapin yliopistoon tehtyä oikeusinformatiikan opinnäytetyötä (*Itsehallittavan identiteetin sääntely EU:n yleisessä tietosuoja-asetuksessa*, Jyrki Pitkänen, Kevät 2018)[17]. Tutkielmassa analysoidaan Sovrin Foundationin SSI-mallia EU:n yleisen tietosuoja-asetuksen kannalta ja arvioidaan muun ohessa lohkoketjun roolia.

> *2 Itsehallittava identiteetti, 2.1 Määritelmä* (s. 3, alleviivaukset lisätty tässä)
>
> *Itsehallittavan identiteetin mallissa luonnollinen henkilö omistaa ja hallinnoi itse omia henkilötietojaan…*
>
> *…Henkilöä koskevat tiedot itsehallittavan identiteetin järjestelmään tulevat joko käyttäjältä itseltään tai joltakin luotettavalta kolmannelta taholta. Tietojen luotettavuuden vuoksi käyttäjän itsensä lisäämät tiedot, eli väitteet, ovat yksinkertaisia, kuten vaikkapa osoite tai puhelinnumero. Kolmansilta tahoilta tulevat varmenteet luovat pohjan varmennetuille väitteille, joiden avulla henkilötiedon vastaanottaja voi olla varma merkittävän henkilötiedon totuudenmukaisuudesta. Tällaisia tietoja voisi Suomessa olla esimerkiksi Väestörekisterikeskuksen antama henkilötunnus, yliopiston antama todistus koulutuksesta tai Poliisin antama tieto ajo-oikeudesta. Näitä tietoja yhdistelemällä tai rajaamalla voidaan luoda kulloinkin tarpeellisia mutta rajattuja henkilötietoja, eli julkituonteja. Edellä mainituilla tiedoilla voidaan esittää muun muassa tieto täysi-ikäisyydestä ja sukupuolesta paljastamatta henkilötunnusta tai edes tarkkaa ikää.*
>
> *Luotettavuus itsehallittaviin henkilötietoihin on toteutettu lohkoketjuteknologialla. Henkilötietoja ei talleta lohkoketjuun, vaan lohkoketjun kautta varmennetaan lähetetty kryptografinen tunniste, jolla sen vastaanottaja voi varmistaa lähetetyn tiedon paikkansapitävyyden ja voimassaolon. Tämä varmentaminen tapahtuu hajautetun julkisen avaimen menetelmällä.*
>
> *…*

Ekosysteemin kehittyminen ja kehittäminen riippuu olennaisesti siitä, mikä tekninen malli ja mitkä standardit saavat laajimman suosion. Standardien ja mallien käyttöönotto voi laajeta sääntelyn tuella tai markkinoiden valintojen perusteella.

[17] https://lauda.ulapland.fi/bitstream/handle/10024/63735/Notaaritutkimus.Pitka%20nen.Jyrki.pdf?sequence=1

3.2 Tietoturvallisuus ja tietosuoja sähköisessä asioinnissa

3.2.1 Tietosuoja rakentuu tietoturvallisuudesta

Sähköisen asiointipalvelun tietoturvallisuus on monen tekijän summa. Turvallisuus rakentuu sähköisessä asiointipalvelussa käytettyjen tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta. Tietosuoja eli henkilötietojen asianmukainen käsittely edellyttää sisällön ja osallisten määrittelyn lisäksi käsittelyn tietoturvallisuutta. Tietosuoja sähköisessä henkilötietojen käsittelyssä edellyttää tietoturvallisuutta. Sähköisen asiointipalvelun asiakkaan sähköisen tunnistamisen luotettavuus vaikuttaa suoraan siihen, kuinka hyvin palveluntarjoaja pystyy huolehtimaan asiakkaansa tietosuojasta.

Sähköisen tunnistamisen turvallisuus vaikuttaa suoraan siihen riskiin, että sähköiseen asiointipalveluun annetaan vääriä tietoja tai että järjestelmässä olevat tiedot altistuvat oikeudettomalle paljastumiselle, muuttamiselle tai muulle käsittelylle. Epäluotettavasta tunnistamisesta voi seurata henkilötiedon päätyminen vääriin käsiin, identiteettivarkaus eli toisen henkilön henkilötietojen käyttäminen erilaisissa taloudelliseen hyötyyn tähtäävissä rikoksissa tai organisaation salassa pidettävän tiedon paljastuminen tai oikeudeton muuttaminen tai tuhoaminen. Sähköisen tunnistamisen turvallisuus voi vaikuttaa luonnollisen henkilön tietosuojan toteutumisen lisäksi oikeushenkilön tietoihin ja liikesalaisuuksiin.

Sähköiseen tunnistamisratkaisuun on syytä kiinnittää erityistä huomioita, kun sähköistä asiointipalvelua suunnitellaan ja toteutetaan. Edellä mainituista syistä on perusteltua suositella mahdollisimman laajalti vahvan sähköisen tunnistamisen käyttöä sähköisissä asiointipalveluissa ja välttää tarpeettomat riskit.

3.2.2 Muut kuin vahvat sähköiset tunnistusmenetelmät

Alla on käyty läpi yleisimmin käytössä olevia tunnistusratkaisuja, jotka eivät täytä lainsäädännön asettamia vaatimuksia vahvalle sähköiselle tunnistusmenetelmälle ja -välineelle. Yleisesti näistä käytetään nimitystä heikko tunnistusmenetelmä tai -väline, vaikka turvallisuuden kannalta näissä menetelmissä käytetään monia vahvalle sähköiselle tunnistamisellekin tuttuja ratkaisuja.

Käyttäjätunnus-salasana -tunnistus

Sähköisissä asiointipalveluissa on usein edelleenkin käytössä käyttäjätunnus-salasana -yhdistelmä, joilla asiointipalvelun käyttäjän tunnistus tehdään. Käyttäjätunnuksena voidaan käyttää esimerkiksi sähköpostiosoitetta, puhelinnumeroa, käyttäjän nimeä tai mitä tahansa muuta keksittyä merkkijonoa.

Käyttäjätunnukseen liitettävän salasanan määrittelee asiakas tai sähköisen asiointipalvelun tarjoaja. Silloinkin, kun salasanan antaa palveluntarjoaja, asiakkaalla on yleensä mahdollisuus vaihtaa salasana itse valitsemaansa, ei kuitenkaan aina. Salasanan muodon ja vaihtamissyklin vaatimukset määrittelee sähköisen asiointipalvelun tarjoaja.

Salasanan suojaus salauksella ja säilyttämiseen käytettävän tietojärjestelmän turvatoimenpiteillä sähköisessä asiointipalvelussa voidaan vaikuttaa siihen, kuinka helposti käyttäjätunnukset ja salasanat voivat päätyä vääriin käsiin teknisen virheen tai tietomurron seurauksena. Salasanan muoto vaikuttaa suoraan siihen, kuinka helppoa hyökkääjän on murtaa se vaihtoehtoja kokeilemalla sähköisen asiointipalvelun rajapinnassa tai muuttaessaan oikeudettomasti haltuunsa saamiaan salattuja salasanoja selkokielisiksi[18].

[18] Ks. esim. Visman esitys tietomurrosta Tietoturva 2019 -seminaarissa, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/visman-joakim-tauren-hakkerien-varkausyritys-pakotti-laittamaan-tietoturvan-kuntoon

Myös asiakkaan toiminta vaikuttaa käyttäjätunnus-salasana -parin luotettavuuteen. Jos asiakas tallentaa ne selaimeen, tunnisteita voi käyttää kuka tahansa selaimen käyttäjä. Käyttäjätunnus-salasana -parit ovat myös alttiita kalastelulle.

Käyttäjätunnus-salasana -pari on luotettavuudeltaan lähtökohtaisesti heikko ratkaisu. Sen haltija voidaan käyttäjätunnus-salasanaparia luotaessa tunnistaa vahvasti ja siten varmistaa luomisvaiheessa, että henkilö on se, joka väittää olevansa. Tämä ei kuitenkaan poista menetelmän edellä kuvattuja riskejä.

Kaksivaiheinen tunnistus (2FA, MFA)

Kaksivaiheinen tunnistus (2FA, two-factor-authentication tai MFA, multi-factor-authentication) perustuu siihen, että asiakkaan tiliin sähköisessä asiointipalvelussa liitetään jokin selaimesta tai sovelluksesta riippumaton yhteystieto, yleensä puhelinnumero tai sähköposti. Kaksivaiheisessa tunnistamisessa käytetään käyttäjätunnuksen ja salasanan lisäksi tällä toisella yhteydellä toimitettavaa vahvistusta, kuten puhelimeen lähetettyä kertakäyttöistä koodia, joka varmistaa sitä, että asiakas on käyttäjätunnukseen liitetyn puhelinnumeron haltija, tai sähköpostiin lähetettyä vahvistuspyyntöä, joka puolestaan varmistaa asiakkaan olevan käyttäjätunnukseen liitetyn sähköpostin haltija.

Asiakkaan kannattaa ottaa kaksivaiheinen tunnistus käyttöön aina, kun se on mahdollista sähköisessä asiointipalvelussa[19].

Kaksivaiheinen tunnistus ei kuitenkaan ole sähköisen asiointipalvelun tarjoajan kannalta kokonaisuutena vahva menetelmä, koska sähköpostin ja tekstiviestin väärentäminen ei edellytä kovinkaan kehittynyttä hyökkäyskykyä. Kaksivaiheisen tunnistamisen käyttöönotto omassa asiointipalvelussa edellyttää myös määrittely- ja ylläpitotyötä, jonka hyötysuhdetta verrattuna vahvan tunnistuspalvelun hankintaan kannattaa arvioida huomioiden sähköisen asiointipalvelussa käsiteltävä tieto ja käyttäjien tarpeet asiointipalvelulle.

Kansainvälisten alustapalvelujen tunnistusratkaisut

Sähköisen asiointipalvelun tarjoaja voi ottaa käyttöön ja tarjota asiakkailleen tunnistautumisen kansainvälisten alustapalvelujen tarjoamilla tunnuksilla. Esimerkiksi Applen, Googlen tai Facebookin tunnistusratkaisu näkyy monissa kansainvälisissä sähköisissä asiointipalveluissa kirjautumisen vaihtoehtona.[20] Näitä tunnuksia käytettäessä turvallisuus riippuu muun muassa siitä, onko asiakkaalla käytössä kyseisessä tunnuksessaan kaksivaiheinen tunnistus. Sähköisen asiointipalvelun tarjoajan kannalta merkityksellistä voi olla myös se, että asiakkaan henkilöllisyyden varmentaminen näissä palveluissa perustuu toissijaisiin lähteisiin kuten puhelinnumeroihin.

Tietosuojan kannalta kansainvälisten alustapalvelujen heikkoutena on se, että käyttäjällä ei ole todellista mahdollisuutta kieltää henkilötietojensa käyttämistä muihin kuin kulloistakin sähköistä asiointia koskeviin tarkoituksiin. Komissio on erityisesti kiinnittänyt eIDAS-asetuksen uudelleenarvioinnissa huomiota tähän epäkohtaan ja arvioi, että käyttäjille on saatava Euroopan laajuisesti käyttöön sähköisiä tunnistusmenetelmiä, joissa suojataan yksityisyyttä. Komission kyselyssä eIDAS-asetuksen muutostarpeista myös valtaosa käyttäjistä toivoi läpinäkyvyyttä ja vaikutusmahdollisuuksia henkilötietojensa käyttöön.

[19] Ks. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus Tietoturva Nyt! 4.9.2020 Nasevia neuvoja tiliesti turvaamiseksi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

[20] Ks. Esim. https://www.booking.com/

3.2.3 Vahva sähköinen tunnistus

Tunnistuslain mukaisessa tai EU:n eIDAS-asetuksen mukaisessa vahvassa sähköisessä tunnistamisessa tunnistusmenetelmän luotettavuus perustuu kokonaisvaltaisiin vaatimuksiin:

- Uuden tunnistusvälineen hakijan henkilöllisyys tarkistetaan huolellisesti.
- Tunnistusväline toimitetaan haltijalle turvallisesti ja uusitaan turvallisesti.
- Tunnistusvälineen voi sulkea nopeasti ja varmasti, jos se katoaa tai joutuu vääriin käsiin. Käyttäjän ilmoitus sulkemisesta siirtää vastuun oikeudettomasta käytöstä tunnistuspalvelulle.
- Tunnistusväline muodostuu aina vähintään kahdesta erityyppisestä todentamistekijästä, jotka ovat toisistaan riippumattomia. Todentamistekijät perustuvat tietoon, hallussapitoon tai ihmisen ominaispiirteisiin. Todentamistekijöissä voi olla esimerkiksi seuraavia yhdistelmiä:
    - hallussa on mobiililiittymä eli SIM-kortti ja tiedossa PIN-koodi
    - hallussa on mobiilisovellus ja tiedossa on PIN-koodi
    - hallussa on mobiilisovellus ja ominaisuutena sormenjälki
    - hallussa on tunnuslukulista ja tiedossa erillinen PIN-koodi tai salasana tai
    - hallussa on henkilökortin siru ja tiedossa PIN-koodi.
- Tunnistuspalvelu kytkee tunnistusvälineen tekijät henkilöön omassa taustajärjestelmässään. Näin varmistetaan, että käyttäjä on todella se, jolle tunnistusväline on myönnetty.
- Taustajärjestelmässä tunnistustapahtuman dynaaminen todentamismekanismi ja salausmenetelmät varmistavat sen, että jokainen tunnistustapahtuma on teknisesti uniikki, eikä sitä voi kopioida tai väärentää.

Vahvan sähköisen tunnistuspalvelun tarjoajan luotettavuus perustuu niin ikään kokonaisvaltaisiin vaatimuksiin ja vaatimustenmukaisuuden varmistamiseen arvioinnilla ja valvonnalla:

- Vaatimukset koskevat yhtä lailla tunnistusvälineen tarjoajia ja tunnistusvälityspalveluita huomioiden kuitenkin niiden toiminnan erilaiset näkökulmat:
    - tunnistusvälineen tarjoaja tarjoaa välineitä käyttäjille ja
    - tunnistusvälityspalvelu tarjoaa asiakkaiden tunnistusta sähköisille asiointipalveluille.
- Tunnistuspalvelurekisteriin hyväksyminen ja siellä pysyminen edellyttää turvallisuuden riippumatonta auditointia kahden vuoden välein.
- Kaikki tunnistusjärjestelmän kannalta merkityksellinen alihankinta kuuluu arvioinnin piiriin. Viranomainen tarkistaa auditoinnit ja päättää tarvittaessa korjausvelvoitteista.
- Häiriöt ilmoitetaan viranomaiselle.
- Luottamusverkoston yhteistoimintaryhmässä keskenään kilpailevat tunnistuspalvelut voivat tehdä yhteistyötä turvallisuusasioissa.

Käyttäjien yksityisyydensuojan näkökulmasta rekisteröidyt vahvan sähköisen tunnistuspalvelun tarjoajat käsittelevät henkilötietoja sääntelyn mukaisesti vain tunnistukseen eivätkä muihin tarkoituksiin. Vahvan sähköisen tunnistusvälityspalvelun tarjoajat varmistuvat myös sähköisen asiointipalvelun oikeudesta käsitellä henkilötietoja, kun osapuolet tekevät sopimuksen tunnistuspalvelun toimittamisesta.

3.2.4 Jatkuvuudenhallinta ja resilienssi

Edellä on käsitelty henkilötietojen luottamuksellisuuden eheyden turvaamista sähköisellä tunnistamisella. Tietoturvallisuus ja tietosuoja edellyttävät myös tietojen saatavuutta. Sähköisen asiointipalvelun tunnistamisratkaisussa on hyvä mahdollistaa tunnistautuminen useammalla eri tunnistusvälineellä, jolloin yhden tunnistuspalvelun häiriö ei estä sähköisen asiointipalvelun käyttöä.

Vahvassa sähköisessä tunnistuspalvelussakin voi olla huoltokatkoksia tai toimivuushäiriöitä. Tunnistusväline voi myös mennä rikki tai kadota, ja silloin on hyvä, jos käyttäjällä on olemassa toinen vahva sähköinen tunnistusväline, jolla sähköiseen asiointipalveluun voi edelleen tunnistautua. Monella onkin jo käytössä sekä verkkopankkitunnukset että mobiilivarmenne. Myös henkilökortilla oleva kansalaisvarmenne löytyy yli miljoonalta suomalaiselta, mutta harvat käyttävät sitä, koska sen käyttöönotto vaatii erillisen kortinlukijan hankkimista ja erillisen ohjelmiston lataamista.

Sähköisen asiointipalvelun on mahdollista hankkia luottamusverkostosta vahva sähköinen tunnistusvälityspalvelu, jolla sähköisen asiointipalvelun käyttäjien on mahdollista tunnistautua vahvasti sekä pankkitunnuksilla että mobiilivarmenteilla. Vahvat sähköiset tunnistuspalvelut voi hankkia kattavasti vain yhdeltä tunnistusvälityspalvelulta, mutta jatkuvuudenhallinnan kannalta asiointipalvelu voi arvioida, onko sillä tarvetta varmistaa tunnistuspalvelujen saatavuus tunnistusvälityspalvelun häiriötilanteissa käyttämällä useampaa tunnistusvälityspalvelua yhden sijasta.

Käyttäjät puolestaan voivat varautua tunnistuspalvelun häiriöihin ottamalla käyttöön useamman kuin yhden vahvan sähköisen tunnistusvälineen, kuten verkkopankkitunnukset ja mobiilivarmenteen.

Esimerkiksi Virossa vuonna 2017 henkilökorttien varmenteeseen liittyvän tietoturvauhan seurauksena arviolta noin 760 000, eli yli puolella virolaisella, sähköisen henkilökortin käyttäjällä ei ollut mahdollisuutta kirjautua Viron valtion sähköisiin asiointipalveluihin ennen kuin kortin varmenne uusittiin[21]. Varmenteiden uusimisen arvioitiin kestävän noin viikon, mikä on pitkä aika digitalisoituneessa maailmassa. Tuolloin Viron valtion sähköisiin asiointipalveluihin oli mahdollista kuitenkin tunnistautua myös mobiilivarmenteella, mikä helpotti tilannetta.

3.2.5 Luotetut identiteetin lähteet

Vahvan sähköisen tunnistusvälineen myöntämisessä käyttäjästä on varmistettava välinettä hakevan henkilöllisyys, henkilöllisyyden voimassaolo ja se, että välineen hakija on se, joka väittää olevansa. Henkilöllisyyden olemassaolon luotetut lähteet ovat eIDAS-asetuksen kannalta kansallisesti säädettävissä.

Tunnistuslain mukaan vahvan sähköisessä tunnistuksessa luonnollisen henkilön identiteetin luotettuja lähteitä ovat väestötietojärjestelmä ja viranomaisen myöntämät passit ja henkilökortit. Vahvan sähköisen tunnistusvälineen haltijan henkilöllisyyden olemassaolo on aina tarkistettava väestötietojärjestelmästä ja tietoja on myös ylläpidettävä ajantasaisena. Suomen viranomaisen myöntämien passien ja henkilökorttien lisäksi oletusarvoisesti luotettuja identiteetin lähteitä ovat Euroopan talousalueen jäsenvaltioiden, Sveitsin ja San Marinon viranomaisten myöntämät passit tai henkilökortit. Halutessaan vahvan sähköisen tunnistusvälineen tarjoaja voi myös käyttää henkilöllisyyden varmentamisessa luotettuna identiteetin lähteenä myös muun valtion viranomaisen myöntämää voimassa olevaa passia, mikä edellyttää muun muassa henkilökunnan koulutusta näiden aitouden arvioinnista.

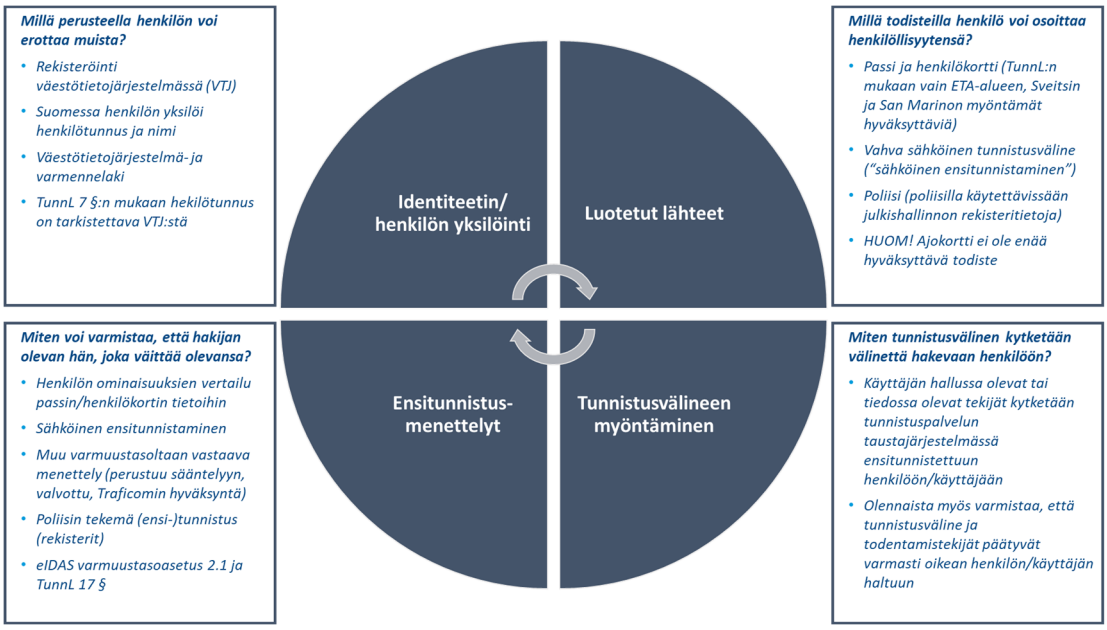
Lisäksi luotettavana identiteetin lähteenä voidaan pitää poliisin rekisteriä passien ja henkilökortin voimassaolosta. Vahvan sähköisen tunnistuspalvelun tarjoajille on myös tunnistuslaissa säädetty oikeus käyttää tätä rekisteriä.

Väestötietojärjestelmässä on nykyisellään vain yksi luotetun identiteetin lähteen luotettavuustaso. Myös ulkomaisen passin tai henkilökortin haltijoilla voi olla henkilötunnus väestötietojärjestelmässä ja tällöin väestötietojärjestelmän henkilölle antamaa identiteettiä luotettavana lähteenä pidetään tunnistuslain kannalta oletusarvoisesti yhtä luotettuna kuin suomalaisille annettua ja väestötietojärjestelmään

[21] https://yle.fi/uutiset/3-9916528

kirjattua identiteettiä.[22] Valtiovarainministeriön asettamassa henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskevassa hankkeessa pohditaan varmuustasojen luomista väestötietojärjestelmän identiteetteihin ja tällöin niiden status suhteessa tunnistuslakiin ja eri varmuustason tunnistusvälineisiin tulee mietittäväksi.[23]

Oikeushenkilön identiteetin luotetut lähteet ovat tunnistuslain mukaan patentti- ja rekisterihallituksen yritys- ja yhteisörekisterit. Oikeushenkilön vahvaan sähköiseen tunnistusvälineeseen olisi aina kytkettävä myös luonnollisen henkilön vahva sähköinen tunnistusväline. Suomessa ei ole syntynyt oikeushenkilön vahvan sähköisen tunnistusvälineen tarjontaa, mutta Suomi.fi -valtuudet palvelu kattaa osittain samoja tarpeita. eIDAS-asetuksen mukainen oikeushenkilön sähköinen leima olisi myös varteenotettava välinen oikeushenkilöiden sähköisten oikeustoimien tarpeisiin.



Kuva 3: Ensitunnistaminen vahvaa sähköisen tunnistusvälinettä haettaessa ja siinä käytettävät luotetut identiteetin lähteet ja todisteet sekä niiden verifiointimenettely

3.2.6 Vahvat identiteetin verifiointitavat (ensitunnistus)

Identiteetin luotetut lähteet ja vahvan sähköisen tunnistusvälineen hakijan henkilöllisyyden verifiointimenettelyt ovat käytännössä sidoksissa toisiinsa ja luokittelu on siksi osittain keinotekoinen. Passeja, henkilökortteja ja vahvoja sähköisiä tunnistusvälineitä voi pitää sekä luotettuina identiteetin lähteinä että henkilöllisyyden verifiointitapoina.

Ensitunnistamisella tarkoitetaan vahvan sähköisen tunnistusvälineen hakijan henkilöllisyyden todentamista tunnistusvälineen hakemisen yhteydessä. Ensitunnistusmenettelyistä vahvaa sähköistä tunnistusvälinettä haettaessa on säädetty eIDAS-asetuksessa. Suomessa tunnistuslaissa on mahdollistettu kaikki eIDAS-asetuksen mukaiset menettelyt.

Ensitunnistamismenettelyt voidaan jakaa viiteen eri tapaan:

1) Henkilöllisyys tarkistetaan käyntiasioinnissa henkilön esittämästä viranomaisen asiakirjasta eli yleensä passista tai henkilökortista ja erikseen vielä väestötieto-

[22] *Toisin Ruotsissa, missä tietyn tason tunnistusvälineen saaminen edellyttää, että henkilöllä on asiakirja, josta näkyy ruotsalainen henkilötunnus.*
[23] https://vm.fi/hanke?tunnus=VM183:00/2020

järjestelmästä. Käytännössä näissä tilanteissa ensiksi tarkistetaan asiakirjan aitous ja sen jälkeen henkilön ominaisuuksia verrataan tähän asiakirjaan, eli yleensä henkilön ulkonäköä verrataan asiakirjassa olevaan kuvaan. Lisäksi on mahdollista tarkistaa poliisin rekisteristä, onko viranomaisen myöntämä asiakirja voimassa, mutta tämän tekemistä ei ole säädetty pakolliseksi.

2) Henkilöllisyys tarkistetaan etäyhteydellä henkilön esittämästä viranomaisen asiakirjasta eli yleensä passista tai henkilökortista (niin kutsuttu etäidentifiointi, *remote identification*) ja erikseen vielä väestötietojärjestelmästä. Viranomaisen asiakirjan esittämisessä on voitava varmistua siitä, että asiakirja on aito ja että asiakirja on esittäjän oma. Asiakirjan aitous on siis jollain keinoin tarkistettava ja henkilön ominaisuuksia verratta asiakirjan tietoihin. Näiden varmistamiseen liittyy useita luotettavuuskysymyksiä, joiden takia tällaisia menettelyjä on vasta tulossa käyttöön ja vaatimusten tulkinta tai arviointikriteerit ovat vasta muotoutumassa. Esimerkiksi viranomaisen myöntämän asiakirjan aitouden todentamisessa luotettavuuden edellytyksenä on pidetty asiakirjan sähköisen sirun lukemista. Tuoreinta yhteiseurooppalaista näkemystä asiasta löytyy komission varmuustasoasetuksen soveltamisohjeesta (niin kutsuttu LOA-guidance, jossa asiaa käsitellä termillä *videoidentification*).[24] Jäsenvaltiokohtaisia menettelyitä on tuotteistettu ja hyväksytty, ja ne perustuvat varsin usein eIDAS-asetuksen sähköisen allekirjoitusvarmenteen myöntämismenettelyihin tai finanssisektorin sääntelyyn.

3) Henkilöllisyys tarkistetaan toisella vahvalla sähköisellä tunnistusvälineellä (niin kutsuttu *ensitunnistamisen ketjuttaminen*), jonka varmuustaso on vähintään sama kuin haetun vahvan sähköisen tunnistusvälineen, ja erikseen vielä väestötietojärjestelmästä. Sen lisäksi, että tunnistuslaissa säädetään sähköisen ensitunnistus päteväksi menettelyksi tunnistaa vahvan sähköisen tunnistusvälineen hakija, laissa säädetään vahvan sähköisen tunnistusvälineen tarjoajalle velvollisuus mahdollistaa toiselle vahvan sähköisen tunnistusvälineen tarjoajalle tunnistusvälineen käyttö ensitunnistamisessa säännellyillä ehdoilla. Säänneltyiin ehtoihin kuuluu myös ensitunnistamien ketjuttamisesta perittävä enimmäishinta.

4) Henkilöllisyys tarkistetaan tai on tarkistettu muita menettelyjä vastaavan varmuuden takaavalla menettelyllä, josta on säädetty, jota valvontaan ja jonka Liikenne- ja viestintävirasto on hyväksynyt (niin kutsuttu *aikaisempi tai muu asiakkuus*). Se, että kansalaisvarmenteen, vahvana sähköisenä tunnistusvälineenä, myöntämisessä ensitunnistus perustuu samaan prosessiin, jolla poliisi myöntää henkilökortin, kuuluu menettelynä tähän kategoriaan.

5) Poliisi tarkistaa henkilöllisyyden ja antaa siitä todistuksen.

3.3 Kuluttajan oikeudet

Vahvaa sähköistä tunnistamista on tässä tarkasteltu niiden oikeuksien ja velvoitteiden näkökulmasta, jotka liittyvät yksityishenkilöiden asemaan kaupallisten palvelujen asiakkaina ja ovat keskeisimpiä markkinaselvityksen kannalta. Tarkastelua on tehty vain vahvan sähköisen tunnistamisen näkökulmasta, koska heikkoon tunnistamiseen ei liity vastaavia oikeuksia ja velvoitteita.

3.3.1 Tunnistusvälineen saatavuus ja sopimusvapaus

Kuluttajille eli käyttäjille kysymys vahvan sähköisen tunnistusvälineen saamisesta on perustavanlaatuinen ja tärkeä, sillä vahva sähköinen tunnistusväline on välttämätön monien muiden digitaalisten palvelujen tosiasialliselle saatavuudelle ja sähköiselle asioinnille. Kuluttajille suosituimmat ja käytetyimmät vahvan sähköisen

[24] TULOSSA

tunnistamisen välineet ovat jo pitkään olleet yksityisten palveluntarjoajien tarjoamat verkkopankkitunnukset ja mobiilivarmenteet, ja lähes kaikilla suomalaisilla on käytössään joko verkkopankkitunnukset ja/tai mobiilivarmenne. Suomessa on kuitenkin ryhmiä, joilla ei tällä hetkellä ole vahvaa sähköistä tunnistusvälinettä käytössään eikä heillä välttämättä ole edes mahdollista saada sellaista käyttöönsä.

Nykyinen tunnistuslaki ei sisällä säännöksiä, joiden perusteella kuluttajilla olisi oikeus saada vahva sähköinen tunnistusväline. Tällöin lähtökohtana yksityisten välisissä suhteissa on sopimusvapaus, johon kuuluu vapaus valita sopimuskumppani. Sopimusvapaudesta poikkeaminen on mahdollista vain säätämällä sopimuspakosta lain tasolla.

Vahva sähköinen tunnistusväline ja sen taustalla oleva lainsäädäntö on myös sidottu suomalaiseen henkilötunnukseen ja sen olemassa olemiseen. Ilman henkilötunnusta henkilöllä ei ole mahdollisuutta saada vahvaa sähköistä tunnistusvälinettä käyttöönsä.

Vahvan sähköisen tunnistamisen palveluja voidaan nykyään pitää tietoyhteiskunnan peruspalveluina. Toisin kuin joidenkin niin sanottujen välttämättömyyspalvelujen kohdalla, tunnistuspalveluille ei kuitenkaan ole säädetty esimerkiksi yleispalveluvelvoitetta, jolla turvattaisiin kuluttajille vahvan sähköisen tunnistuspalvelun saatavuus.

Vahvan sähköisen tunnistusvälineen tarjoamiseen liittyviä velvoitteita on asetettu luottolaitoslain 15 luvun 6 §:ssä, jossa on luotu kytkös peruspankkipalvelujen ja tunnistusvälineiden tarjonnan välille. Nykyisin peruspankkipalvelu sisältää myös verkkopankin ja -pankkitunnukset. Peruspankkipalvelun yhteydessä vahvan sähköisen tunnistuspalvelun tarjonnasta voi kieltäytyä vain lakiin perustuvin objektiivisin perustein, esimerkiksi jos asiakkaalla ei ole henkilötunnusta tai häntä ei ole merkitty väestötietojärjestelmään. Perusmaksutiliä, siihen liittyviä palveluja ja sähköisen tunnistamisen palveluja, mukaan lukien vahvan sähköisen tunnistamisen palvelut, tarjotessaan talletuspankin tulee kohdella kaikkia asiakkaita yhdenvertaisesti ja syrjimättömästi.

3.3.2 Tunnistusvälineen käytettävyys ja esteettömyys

Kuluttajien näkökulmasta tunnistuspalvelujen ja -välineiden käytettävyyteen vaikuttavat keskeisesti sekä digiosaaminen että esteettömyys.

Yhdenvertaisuus edellyttää, että tunnistautuminen ja pääsy palveluihin on mahdollistettava niillekin, joille syystä tai toisesta on vaikeaa sähköisten välineiden käyttö. Yhdenvertaisuuslain (1325/2014) 8 §:n syrjinnän kielto velvoittaa sekä julkisia että yksityisiä toimijoita. Yhdenvertaisuuslain ja sen edellyttämien kohtuullisten mukautuksien noudattamista valvoo yhdenvertaisuusvaltuutettu.

Yhdenvertaisuutta ja syrjimättömyyttä edistäviä säännöksiä on myös erityislainsäädännössä. Vahvan sähköisen tunnistamisen yhteydessä merkityksellinen on luottolaitoslain 15 luvun 6 §:n peruspankkipalvelusääntelyssä oleva vaatimus mukauttamisesta ja asiakkaiden yhdenvertaisesta kohtelusta, joka koskee myös verkkopankkitunnuksia.

Laki digitaalisten palvelujen tarjoamisesta (306/2019) toimeenpanee saavutettavuusdirektiivin Suomessa. Lain yhtenä tavoitteena on parantaa yhteiskunnan erityisryhmien edellytyksiä selvitä omatoimisesti julkisen sektorin digitaalisten palvelujen käytöstä. Lain 3 §:n 4 kohdan mukaan lakia sovelletaan myös vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 12 §:ssä tarkoitettuun rekisteriin merkittyjen tunnistuspalvelun tarjoajien tunnistuspalveluihin, mutta vain siten, että vahvojen sähköisten tunnistuspalvelujen osakokonaisuudet tulevat vain osittain kyseessä olevalla lainsäädännöllä katetuiksi.

3.3.3 Tunnistusvälineeseen ja sen käyttöön liittyvät vastuukysymykset

Digitalisaation edetessä kuluttajat tekevät verkossa yhä merkittävämpiä oikeustoimia, esimerkiksi asunto- ja kiinteistökauppoja sekä terveyspalveluihin liittyviä valintoja. Digitaalisessa prosessissa kuluttajan on ennen asiointia tunnistauduttava onnistuneesti, jolloin viiveet tai virheet tunnistautumisessa voivat estää asioinnin tai jopa koko oikeustoimen.

Nykyinen laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ei sisällä kattavia vastuusäännöksiä vahvojen sähköisten tunnistuspalvelujen osalta. Lain tasolla olisi huomioitava vahvan sähköisen tunnistusvälineen käyttöön liittyvät vastuukysymykset ja riittävät seuraamukset ainakin tilanteissa, joissa

- tunnistusvälineen käyttäjän pyyntö/toimeksianto jää toteuttamatta tai se toteutetaan virheellisesti,
- välinettä käytetään ja toimeksianto tehdään oikeudettomasti (esim. kadonneella tai varastetulla välineellä taikka tietojärjestelmiin murtautumalla).

Samalla olisi varmistettava se, että kuluttajaan päin toimeksiannon hoitamisesta vastaa aina selkeästi yksi vastuutaho. Varsinkin vahvaan sähköiseen tunnistamiseen liittyvän luottamusverkoston kaltaisissa olosuhteissa tunnistustapahtuman toteuttaminen on luonteeltaan ketjuuntuvaa toimintaa. Vahvan sähköisen tunnistuspalvelujen käyttäjänä kuluttajan olisi kuitenkin voitava luottaa siihen, että yksi vastuutaho on hänelle vastuussa tunnistus- tai allekirjoitustapahtuman[25] toteuttamisesta ja tiedon välittymisestä tietoverkossa eri järjestelmien rajapinnat ylittäen.

Ilman lain tasoisia vastuusäännöksiä vastuukysymykset ja riskinjako jäävät sopimuskäytännön varaan. Kuluttajien saama suojan taso vaihtelee tällöin sen mukaan, millaiset ehdot sopijakumppani tarjoaa. Vahvan sähköisen tunnistuspalvelun tarjoajat voivat muotoilla sopimusehtonsa niin, että heidän vastuunsa jää rajalliseksi. Kuluttajat eivät heikompana osapuolena pääse neuvottelemaan palvelun ehdoista vaan voivat ainoastaan hyväksyä tai hylätä vakiomuotoisen sopimuksen.

3.3.4 Tunnistamista edellyttävä asiointi

Velvoitteet vahvan sähköisen tunnistamisen käyttämiseen

Tietyissä tilanteissa laki edellyttää, että sähköisen asiointipalvelun tarjoajan on varmistuttava vahvan sähköisen tunnistamisen avulla asiakkaan henkilöllisyydestä ennen kuin se voi ottaa henkilön asiakkaakseen taikka toteuttaa asiakkaan pyynnön tai toimeksiannon. Silloin, kun kyse on lakisääteisestä velvoitteesta, sähköisen asiointipalvelun on edellytettävä kuluttajilta vahvaa sähköistä tunnistamista, sillä laiminlyönnistä voi seurata sanktio elinkeinonharjoittajalle.

Digitaalisten palvelujen tarjoamisesta annetun lain 6 §:n mukaan *viranomainen voi vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi. Jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi, palvelun käyttäjä on tunnistettava hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:n 1 momentin 4 kohdassa tarkoitettua luonnollisen henkilön tunnistuspalvelua, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 momentin 1 kohdassa tarkoitettua vahvaa sähköistä tunnistamista tai painavasta perustellusta syystä muuta vastaavaa tietoturvallista tunnistuspalvelua käyttämällä*.

[25] On hyvä huomata, että tunnistus- ja luottamuspalveluissa ei kuitenkaan säädetä sähköisistä allekirjoituspalveluista. Allekirjoituspalvelun tarjoaja voi myös olla eri taho kuin tunnistuspalvelun tarjoaja.

Kuluttajansuojalaissa (38/1978) on asetettu henkilöllisyyden todentamista koskevia velvoitteita kuluttajaluottosopimusten osalta. Kuluttajansuojalain 7 luvun 15 §:n mukaan luotonantajan on ennen kuluttajaluottosopimuksen tekemistä todennettava luottoa hakevan henkilöllisyys huolellisesti. Jos henkilöllisyys todennetaan sähköisesti, luotonantajan on ensitunnistamisvaiheessa käytettävä tunnistusmenetelmää, joka täyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 8 §:ssä säädetyt vaatimukset.

Kuluttajansuojalain 7 luvun säännökset vahvan sähköisen tunnistamisen käyttämisestä eivät koske hyödykesidonnaisia kertaluottoja tai laskutuspalveluja, joita tarjotaan monesti yhtenä rahoitusvaihtoehtona verkossa ostoksia maksettaessa. Keväällä 2021 käynnistettävän kuluttajaluottosäännösten uudistamista koskevan oikeusministeriön lainsäädäntöhankkeen yhteydessä arvioidaan, tuleeko kuluttajansuojalain 7 luvun lainanhakijan henkilöllisyyden todentamisesta sääntelyä tiukentaa laajentamalla se koskemaan kaikkien kuluttajaluottosopimusten tekemistä.

Maksupalvelulaissa (290/2010) on vahvan sähköisen tunnistamisen käyttöä edellyttävää sääntelyä, joka liittyy maksutapahtumien toteuttamiseen. Maksupalvelulain 85 c §:n mukaan vahvaa tunnistamista[26] on käytettävä muun muassa, jos maksaja käyttää maksutiliään tietoverkon välityksellä tai käynnistää sähköisen maksutapahtuman. Maksupalvelulain vaatimukset tulee toteutua myös maksullisissa viranomaispalveluissa maksettaessa käyttäen esimerkiksi maksajan maksutiliä tietoverkon välityksellä.

Velvoitteet asiakkaan todennettuun tunnistamiseen

Erityislainsäädännössä on useita asiakkaan tunnistamiseen velvoittavia säädöksiä, joiden taustalla on esimerkiksi ns. tunne asiakkaasi (know your customer) -periaate. Lisäksi salassa pidettävään tietoon, kuten terveystietoon tai muuhun arkaluonteiseen henkilötietoon, liittyy velvoitteita sekä yleisen henkilötietolainsäädännön perusteella että erityislainsäädännössä. Näissä tilanteissa lain tasolla ei aina viitata nimenomaisesti vahvan sähköisen tunnistamisen käyttämiseen tai siitä annettuun lakiin (617/2009). Silloin kun laki edellyttää todennettua tunnistamista, vahvan sähköisen tunnistamisen välineet ovat kuitenkin toimiva tapa tunnistusvelvoitteiden täyttämiseen.

Esimerkiksi rahanpesun estämistä koskeva sääntely vaikuttaa laajasti eri toimialoilla, kuten finanssialalla, tilintarkastuksessa ja kiinteistönvälityksessä. Laki rahanpesun ja terrorismin rahoittamisen estämisestä edellyttää, että ilmoitusvelvollisen on tunnistettava asiakkaansa ja todennettava tämän henkilöllisyys sekä vakituista asiakassuhdetta perustettaessa että lain 3 luvun 2 §:ssä määritellyissä tilanteissa.

Esimerkiksi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 8 § edellyttää, että asiakastietojen sähköisessä käsittelyssä asiakas, sosiaalihuollon ja terveydenhuollon palvelujen antaja, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet tulee tunnistaa luotettavasti. Potilastietoja käsittelevien henkilöiden, palvelujen antajien, tietoteknisten laitteiden sekä valtakunnallisten tietojärjestelmäpalvelujen tunnistaminen edellyttää lisäksi todentamista.

Tunnistaminen sopimuksia solmittaessa

Suomen sopimusoikeuden yleisten periaatteiden mukaan sopimukseen vetoavan on tarvittaessa voitava näyttää toteen se, kenen kanssa sopimus on solmittu ja että sopimus on syntynyt sitovalla tavalla. Tästä seuraa, että on sähköisen asiointipalvelun omassa intressissä, että se varmistuu riittävän luotettavasti sopimuskumppaninsa henkilöllisyydestä ja tarvittaessa todentaa sen tarpeelliseksi katsomallaan tavalla. Vastaavasti kuluttajalla on tarve saada luotettava tieto siitä, kenen kanssa

[26] Katso kohta 2.2.9 Tunnistuslain ja maksupalvelulain vaatimusten yhteensopivuus.

hän on solmimassa sopimusta. Tunnistusprosessin aikana annettu ilmoitus siitä, kuka on pyytänyt kuluttajan tietoja, voi osaltaan tukea tätä.

Sopimusvapauteen kuuluu myös muotovapaus. Jollei sääntelystä muuta johdu, sopimus voidaan solmia kirjallisesti, suullisesti tai konkludenttisesti osapuolten tosiasiallisen käyttäytymisen perusteella. Esimerkiksi verkkokaupoissa sopimukset syntyvät digitaalisella ostopolulla, jossa tunnistautumisen ja maksamisen lisäksi ei yleensä edellytetä erillistä allekirjoitusta.

4 Kilpailun edistäminen ja kilpailuneutraliteetti

Kilpailupolitiikalla pyritään turvaamaan, että kilpailu markkinoilla toimii ja kuluttajat hyötyvät kilpailusta. Tavoitteena on luoda ja ylläpitää sellainen toimintaympäristö, jossa yrityksillä on tasapuoliset toimintaedellytykset ja mahdollisuus menestyä osaamisensa avulla. Kilpailu edistää yrittäjyyttä ja tehokkuutta, ja sen ansiosta asiakkailla on enemmän valinnanvaraa, hinnat ovat edullisempia ja laatu parempaa.

Kilpailuilla avoimilla markkinoilla hinnat ovat edulliset, mikä hyödyttää sekä kuluttajia että yrityksiä. Kilpailulliset hinnat kasvattavat kysyntää ja sitä kautta tuotantoa ja talouskasvua. Kilpailu kannustaa yrityksiä tarjoamaan parempia vaihtoehtoja kuin kilpailijansa, tehostamaan toimintatapojaan sekä kehittämään asiakkaiden tarpeita vastaavia tuotteita ja palveluja. Näin ne voivat kasvattaa asiakaspohjaansa ja kasvattaa markkinaosuuttaan. Tuotteita ja palveluja ostaville kilpailun lisääntyminen näkyy muun muassa edullisempina hintoina ja laadukkaampina tuotteina ja palveluina. Laadulla voidaan tarkoittaa monenlaisia asioita, kuten tuotteita, jotka kestävät pitempään tai toimivat paremmin, parempaa myynninjälkeistä tai teknistä tukea taikka parempaa palvelua. Kilpailu näkyy asiakkaille myös laajempana valikoimana: kilpailulle avoimilla markkinoilla yritykset pyrkivät erottautumaan kilpailijoistaan, mistä syystä valikoima kasvaa ja asiakkaat voivat valita tuotteen, joka on hinnaltaan ja laadultaan heille sopivin.

Kilpailullisilla markkinoilla yritysten on oltava innovatiivisia tuotekehityksessään, suunnittelussaan, tuotantomenetelmissään ja palveluissaan. Vastaavasti markkinoilla, joilla on kilpailun esteitä, on vähemmän innovaatioita. Kilpailu kotimarkkinoilla tekee yrityksistä vahvempia: näin ne pystyvät kilpailemaan kansainvälisiä kilpailijoitaan vastaan ja myös laajentumaan oman kotimarkkinansa ulkopuolelle.

Kilpailu ja markkinamekanismi eivät kuitenkaan aina tuota yhteiskunnan kannalta optimaalista tuotantomäärän ja hinnan yhdistelmää kyseisen hyödykkeen osalta: erilaiset markkinahäiriöt voivat johtaa siihen, että tuotteen tai palvelun tarjonta voi jäädä puutteelliseksi, hinnat voivat nousta korkeiksi tai toiminnan mahdolliset haitalliset ulkoisvaikutukset voivat jäädä huomiotta. Julkinen sektori voi pyrkiä korjaamaan markkinamekanismin häiriöitä sääntelyllä ja muilla politiikkatoimilla. Näin on myös tehty vahvan sähköisen tunnistamisen markkinalla, kun on katsottu, ettei vallalla oleva markkinamekanismi ole tuottanut yhteiskunnan kannalta optimaalista lopputulosta. Markkinapuutteella viitataan usein tilanteeseen, jossa yksityistä markkinaehtoista tarjontaa tietystä hyödykkeestä ei ole eikä sellaista ole myöskään näköpiirissä. Tällöin julkisen sektorin voi olla perusteltua tuottaa hyödykettä, ainakin jos kysymys on asiakkaiden kannalta välttämättömyystuotteesta tai -palvelusta.

Erilaiset alalle tulon esteet voivat heikentää kilpailua ja markkinoiden toimivuutta. Potentiaalisten uusien toimijoiden epävarmuus tulevasta kehityksestä ja sääntelystä voi hidastaa alalle tuloa ja vähentää tuotekehitykseen sijoitettua pääomaa. Ylimääräinen epävarmuus heikentää yritysten näkymää sen suhteen, tulevatko tehdyt investoinnit maksamaan itsensä takaisin. Mitä tulee vahvaan sähköiseen tunnistamiseen, sääntelyllä ja julkisen sektorin muilla toimenpiteillä on keskeinen vaikutus nykyisten markkinatoimijoiden ja mahdollisten uusien alalle tulijoiden kannustimiin. Valtion nykyinen rooli tärkeänä tunnistuspalvelujen asiakkaana ja tähän kohdistuvat muutospaineet kuten myös mahdollinen valtion toteuttama uusi tunnistusväline ja identiteettipalvelujen kokonaisuus sekä mahdolliset muut julkisen sektorin hankkeet aiheuttavat epävarmuutta ja ovat omiaan vähentämään investointihalukkuutta.

Julkisten toimijoiden taloudellista toimintaa tunnistuspalvelujen markkinoilla ohjaa kilpailuneutraliteettisääntely. Kilpailuneutraliteetista säädetään kilpailulain (948/2011) 4 a luvussa. Kilpailuneutraliteetti tarkoittaa sitä, että julkisella ja yksityisellä elinkeinotoiminnalla on tasapuoliset toimintaedellytykset. Julkisyhteisöt voi-

vat harjoittaa taloudellista toimintaa ja kilpailla yksityisten yritysten kanssa samoilla markkinoilla. Kilpailuneutraliteettisäännösten tavoitteena on varmistaa, että julkiset toimijat eivät saa kilpailuetuja, joita yksityiset toimijat eivät voi saada ja jotka voivat vääristää kilpailua.

Kilpailu- ja kuluttajavirasto (KKV) voi puuttua julkisyhteisön menettelyyn tai toiminnan rakenteeseen, jolla on tai voi olla kilpailua vääristäviä tai estäviä vaikutuksia markkinoilla. KKV ei voi kieltää lainsäädäntöön perustuvaa toimintaa, mutta siihen voidaan puuttua kilpailuneutraliteettisäännöksien nojalla. KKV:lla ei kuitenkaan ole toimivaltaa, jos kilpailuneutraliteettiongelma johtuu väistämättä lainsäädännöstä. Kilpailuneutraliteettisääntelyn perusteella ei siis voida muuttaa tai oikaista voimassa olevaa lainsäädäntöä. Kilpailulain 4 a lukua ei myöskään sovelleta, jos soveltaminen estäisi merkittävään yleiseen etuun liittyvän palvelun toteuttamisen.

Kilpailuneutraliteettisääntely velvoittaa julkisyhteisöjä pitämään erillistä kirjanpitoa markkinoilla harjoittamastaan toiminnasta. Julkisyhteisön tulee laatia tästä toiminnasta tuottoja ja kuluja koskeva tuloslaskelma, joka on esitettävä julkisyhteisön tilinpäätöksessä. Tavoitteena on lisätä julkisyhteisöjen toiminnan läpinäkyvyyttä ja tehostaa kilpailuneutraliteetin valvontaa.

Kilpailulain 4 a luvun säännökset koskevat ainoastaan julkisyhteisöjen tai niiden määräysvallassa olevien yhteisöjen harjoittamaa taloudellista toimintaa. Toiminta, joka ei ole luonteeltaan taloudellista jää lain soveltamisalan ulkopuolelle. Sääntely ei siten koske tilanteita, joissa julkisyhteisö toimii julkisen vallan käyttäjänä tai viranomaisen ominaisuudessa harjoittaen viranomaistoimintaa. Taloudellisen toiminnan käsite on yhdenmukainen EU-oikeuden kanssa. Toiminnan taloudellinen luonne ratkaistaan tapauskohtaisesti. Ratkaisevaa taloudellisen ja ei-taloudellisen toiminnan erottamisessa on toiminnan harjoittaminen markkinaympäristössä.

5 Tarpeet tunnistus- ja identiteettipalveluille

5.1 Kuluttajien eli käyttäjien tarpeet

5.1.1 Tunnistustavan valintaperusteet

Lähtökohtaisesti kuluttajan eli tunnistusvälineen käyttäjän on tyydyttävä siihen tunnistusratkaisuun tai -ratkaisuihin, mitä sähköisen asiointipalvelun tarjoaja tarjoaa käytettäväksi. Siten kuluttajan mahdollisuudet vaikuttaa siihen, mitä tunnistusratkaisua hän käyttää sähköiseen asiointipalveluun tunnistautuessa ovat hyvin rajalliset, jopa vain teoreettiset. Käytännössä kuluttajat voivat vaikuttaa vain vaihtamalla kokonaan (sähköisen) asiointipalvelun tarjoajaa tai lopettamalla sen asiointipalvelujen käyttämisen. Jossain määrin kuluttajat voivat pyrki vaikuttamaan myös antamansa kuluttajapalautteen kautta.

Julkisen hallinnon sähköisissä asiointipalveluissa tarjotaan yleisesti vahvaa sähköistä tunnistusta. Sen sijaan yksityisen ja kolmannen sektorin sähköisissä asiointipalveluissa suurelta osin tarjotaan kuluttajille ainoastaan rekisteröimätöntä tunnistusta asiointipalveluun tunnistautumiseksi. Yksityisen ja kolmannen sektorin sisällä tilanteet kuitenkin poikkeavat merkittävästi ja esimerkiksi finanssisektorilla tarjotaan laaja-alaisesti vahvaa sähköistä tunnistamista sähköisiin asiointipalveluihin, kuten verkkopankkiin, tunnistautumiseksi. Yksityisen ja kolmannen sektorin sähköisissä asiointipalveluissa on kuitenkin viime vuosina otettu entistä laajemmin käyttöön vahva sähköinen tunnistus joko ainoana tai rinnakkaisena vaihtoehtona jollekin rekisteröimättömälle tunnistusratkaisulle. Pääasiallinen syy tähän on lainsäädäntö, joka vaatii sähköisen asiointipalvelun tarjoajaa tekemään asiakkaan tunnistamisen vahvalla sähköisellä tunnistuksella, mutta myös viime vuosina esille tulleet tietomurrot ja tietosuojaloukkaukset ovat lisänneet vahvan sähköisen tunnistuksen käyttöönottamista. Myös yleisen tietosuoja-asetuksen voimaantulo on todennäköisesti lisännyt vahvan sähköisen tunnistamisen käyttöä sähköisissä asiointipalveluissa.

Tilastokeskuksen Väestön tieto- ja viestintätekniikan käyttö -tutkimus 2020 mukaan vuonna 2020 68 prosenttia kyselytutkimukseen vastanneista oli viimeisen 12 kuukauden aikana kirjautunut sähköisiin asiointipalveluihin käyttäjätunnuksella ja salasanalla, 64 prosenttia avaintunnuslukulistalla (verkkopankkitunnisteella), 54 prosenttia mobiilivarmenteella, 31 prosenttia yhteisöpalvelun (esimerkiksi Facebookin) käyttäjätunnuksilla, 8 prosenttia sähköisellä toimikortilla (organisaatiovarmenne), 3 prosenttia sähköisellä henkilökortilla (kansalaisvarmenne) ja 4 prosenttia jollain muulla tavoin.[27] 10 prosenttia ei ollut tunnistautunut lainkaan sähköisiin asiointipalveluihin viimeisen 12 kuukauden aikana.

Valtiovarainministeriön teettämän kyselytutkimuksen[28] mukaan 88 prosenttia vastanneista käyttäisi nykyistä vahvaa sähköistä tunnistusvälinettä sähköiseen asiointipalveluun tunnistautuessa, jos heillä olisi mahdollisuus valita käytettävä tunnistusmenetelmä.[29] Ennen kaikkea vastaajat perustelivat vahvan sähköisen tunnistusvälineen käyttämistä sillä, että se on turvallinen käyttää (60 %), sitä on helpompi käyttää (29 %) ja heidän ei tarvitse muistaa kuin yksi käyttäjätunnus ja salasana tunnistautuessaan eri palveluihin (19 %).

[27] Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. ISSN=2341-8699. 2020, Liitetaulukko 30. Verkkopalveluihin kirjautumistapa 2020, %-osuus väestöstä. Helsinki: Tilastokeskus [viitattu: 5.1.2021]. Saantitapa: http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tau_030_fi.html

[28] Valtiovarainministeriön syksyllä 2020 teettämällä kyselytutkimuksella on pyritty kartoittamaan sähköisen tunnistamisen nykytilaa ja tarpeita kuluttajien näkökulmasta. Tutkimuksen kohderyhmä oli 15 vuotta täyttäneet Suomen kansalaiset ja se suoritettiin puhelinhaastatteluina, jotka toteutti Taloustutkimus 30.10.-9.12.2020 välisenä aikana. Tutkimukseen poimitut haastateltavat poimittiin valtion tietojärjestelmästä. Tiedonkeruussa käytettiin kiintiöintiä väestöedustavuuden varmistamiseksi ja aineisto on painotettu iän, sukupuolen ja suuralueen mukaan väestöä vastaavaksi. Tutkimukseen osallistui 2003 henkilöä.

[29] Kyselytutkimus tehtiin 30.10.-9.12.2020 välisenä aikana ja sen otos oli 2003 haastattelua.

Vastanneista 7 prosenttia taas käyttäisi muuta kuin vahvaa sähköistä tunnistusvälinettä eli rekisteröimätöntä tunnistusvälinettä, ja 4 prosenttia ei osannut sanoa käyttäisikö vahvaa vai rekisteröimätöntä sähköistä tunnistusvälinettä. Vastanneista rekisteröimätöntä tunnistusvälinettä mieluummin käyttävät perustelivat valintaansa ennen kaikkea sillä, että rekisteröimätöntä tunnistusvälinettä on helpompi (52 %) ja nopeampi (16 %) käyttää ja että se on turvallisempi käyttää (16 %). Perusteina olivat myös se, että tarvitsee muistaa vain yksi käyttäjätunnus ja salasana (9 %) ja että välinettä voi käyttää ilman tunnuslukulistaa, -sovellusta tai laitetta tai matkapuhelinta (8%). Vastausten osalta on syytä huomioida, että vastaajajoukko, joka käyttäisi mieluummin rekisteröimätöntä tunnistusvälinettä, oli pieni, jolloin vastausten perusteella ei voida tehdä kaikkia kansalaisia koskevia johtopäätöksiä perusteista rekisteröimättömän tunnistusvälineen käyttämiseksi. Vastauksista voidaan kuitenkin saada jonkinlaista osviittaa niistä perusteista, miksi osa kansalaisista valitsisi mieluiten rekisteröimättömän tunnistusvälineen.

Kysyttäessä, mikä olisi mieluisin tunnistuksessa käytettävä tunnistusväline, 34 prosenttia vastanneista piti älypuhelimeen tai tablettiin asetettavaan tunnuslukusovellukseen, 22 prosenttia tunnuslukulistaan, 22 prosenttia älypuhelimen tai tabletin sormenjälkitunnistukseen, 6 prosenttia tunnuslukulaitteeseen, 5 prosenttia käyttäjätunnukseen ja salasanaan, 4 prosenttia älypuhelimen tai tabletin kasvojentunnistukseen ja 3 prosenttia fyysisesti paikanpäällä tehtävään tunnistukseen perustuvaa todentamismekanismia mieluisampana. Loput 5 prosenttia vastaajista ilmoittavat jonkin muun tavan tai eivät osanneet sanoa. Myös näiden tulosten perusteella näyttää siltä, että vahvassa sähköisessä tunnistamisessa käytössä olevat (esimerkiksi tunnuslukusovellus ja -tunnuslukulista) tai mobiililaitteen mahdollistamat (esimerkiksi sormenjälkitunnistus) tunnistusvälineet ovat käyttäjien näkökulmasta mieluisia. Näitä ominaisuuksia käytetään rekisteröimättömissä sähköisissä tunnistusvälineissä, jolloin siirtymä rekisteröimättömän tunnistusvälineen käyttämisestä vahvan sähköisen tunnistusvälineen käyttämiseen on helpompaa.

Vastanneista, joilla oli käytössään vahva sähköinen tunnistusväline, 95 prosenttia piti sen käyttämistä vähintäänkin helppona, vaikka osa (15 %) olikin kokenut joitakin haasteita sen käyttämisessä. 5 prosenttia piti vahvan sähköisen tunnistusvälineen käyttämistä haastavana. Kysyttäessä, mitä ongelmia vastaajat kokivat vahvan sähköisen tunnistusvälineen käyttämisessä, korostuivat vastauksessa lähinnä muut kuin itse tunnistusvälineeseen liittyvät ongelmat, kuten sähköisen asiointipalvelun käyttöön liittyvät yhteysongelmat ja -häiriöt (12 %) sekä yleinen tietoteknisten laitteiden hankala käytettävyys (8%). Jossain määrin koetut ongelmat liittyivät myös itse tunnistusvälineen käyttämiseen ja häiriöihin niissä sekä annettuihin ohjeisiin välineen käyttämiseksi.

Kyselytutkimuksen perusteella suurin osa käyttäjistä selkeästi käyttäisi vahvaa sähköistä tunnistusvälinettä tunnistautumisessa, jos vain sähköisten asiointipalvelujen tarjoajat mahdollistaisi sen palveluissaan. Kansalaisten näkökulmasta vahvalle sähköiselle tunnistukselle sähköisissä asiointipalveluissa on selkeää kysyntää eivätkä nykyiset käyttömahdollisuudet vastaa tätä tarvetta. Rekisteröimättömiä tunnistusvälineitä käytetään ennen kaikkea siitä syystä, ettei vahvaa sähköistä tunnistusvälinettä ole mahdollista käyttää laaja-alaisesti sähköisissä asiointipalveluissa. Kyselytutkimuksen perusteella ei ole selkeästi osoitettavissa, että kansalaiset pitäisivät nykyisiä vahvoja sähköisiä tunnistusvälineitä suuressa määrin hankalana käyttää, vaan ennemminkin päinvastoin, helppona käyttää. Samoja mobiililaitteiden ominaisuuksia kuin rekisteröimättömissä eli heikoissa tunnistusvälineissä käytetään myös vahvoissa sähköisissä tunnistusvälineissä, jolloin myös siirtyminen rekisteröimättömän tunnistusvälineen käyttämisestä vahvaan sähköiseen tunnistusvälineeseen on helppoa käyttökokemuksen kannalta.

Kyselytutkimuksen mukaan 98 prosentilla vastanneista oli käytössään verkkopankkitunnukset, 22 prosentilla mobiilivarmenne, 7 prosentilla organisaatiovarmenne ja 6 prosentilla kansalaisvarmenne. Vastaajista 90 prosenttia ilmoitti käyttävänsä ylei-

simmin verkkopankkitunnusta. Verkkopankkitunnusten merkittävä käyttö yleisimpänä vahvana sähköisenä tunnistusvälineenä selittynee sillä, että 87 prosenttia ilmoitti tunnistautuneensa viimeisen kuuden kuukauden aikana kaikkein yleisimmin verkkopankkiin, jonne tällä hetkellä ei ole mahdollisuutta tunnistautua muulla välineellä kuin kyseisen verkkopankkipalvelun tarjoavan pankin verkkopankkitunnisteella. Kun vastaajilta myös kysyttiin, missä palveluissa vahvaa sähköistä tunnistusvälinettä on viimeisten kuuden kuukauden aikana käyttänyt, korostuu vastauksissa palvelut, joissa voi käyttää vain pankin myöntämää verkkopankkitunnusta. Vastaajista 8 prosenttia ilmoitti käyttävänsä yleisimmin mobiilivarmennetta ja 1 prosentti organisaatiovarmennetta. Kyselytutkimuksesta saadut tulokset näyttävät olevan hyvin linjassa tunnistustapahtumien määristä kerättyjen vahvojen sähköisten tunnistusvälinekohtaisten markkinaosuustietojen kanssa.

Vastaajista 6 prosenttia ilmoitti viimeisen vuoden aikana ottaneensa käyttöön mobiilivarmenteen ja 5 prosenttia verkkopankkitunnuksen käytössä olleen vahvan sähköisen tunnistusvälineen rinnalle. 8 prosenttia vastanneista on suunnitellut ottavansa mobiilivarmenteen, 3 prosenttia kansalaisvarmenteen ja 1 prosentti verkkopankkitunnusten käyttöönsä nykyisen vahvan sähköisen tunnistusvälineen rinnalle.

Kyselytutkimuksen perusteella suurin osa kansalaisista käyttää verkkopankkitunnusta johtuen muun muassa siitä, ettei verkkopankkiin tunnistautuessa heillä ole mahdollisuutta käyttää muita vahvoja sähköisiä tunnistusvälineitä. Verkko-ostoksia maksaessa maksun vahvistamisessa ja tunnistautumisessa pankit myös ohjaavat käytännössä aina käyttämään pankin tarjoamaa vahvaa sähköistä tunnistusvälinettä tai pankin tarjoamaa vahvaa tunnistusta. Lähes noin neljänneksellä kansalaisista on kuitenkin käytössään myös mobiilivarmenne, jota he voivat käyttää verkkopankkitunnusten rinnalla, mutta muissa kuin verkkopankkiin tunnistautumisessa tai maksujen vahvistamisessa. Muiden tietojen perusteella mobiilivarmenteen käyttöönottaminen ja käyttö on muiden vahvojen tunnistusvälineiden käytöstä poiketen myös selkeästi kasvanut viimeisten vuosien aikana, vaikkakin kasvuvauhti on ollut maltillista. Osaltaan sähköisen ensitunnistamisen hintasääntelyllä on ollut vaikutusta tähän kehitykseen. Kyselytutkimuksen perusteella merkittävällä määrällä kansalaisista on kiinnostusta ottaa käyttöönsä mobiilivarmenne. Kiinnostus kansalaisvarmenteen käyttämiseen tai kansalaisvarmenteen käyttöönottamiseksi on vähäisempää muihin vahvoihin sähköisiin tunnistusvälineisiin nähden, vaikka noin 1,3 miljoonalla henkilöllä on jo käytössään henkilökortti, johon kansalaisvarmenteen käyttämisessä tarvittava mikrosiru on integroitu. Vahvojen sähköisten tunnistusvälineiden käyttömäärätiedot tukevat näitä kyselytutkimuksen perusteella tehtyjä johtopäätöksiä. Samanlaisia johtopäätöksiä voidaan tehdä organisaatiovarmenteesta, mutta organisaatiovarmenteen käyttötapaus ja käyttöönotto poikkeavat muista vahvoista sähköisistä tunnistusvälineistä siinä, että varmenteen yleensä hankkii työnantaja työntekijälle käyttöön ja sen käyttö liittyy ensi sijaisesti työtehtävien hoitamiseen.

Kyselytutkimuksessa ei erikseen kysytty syitä, miksi vastaaja ei ole ottanut käyttöönsä vahvaa sähköistä tunnistusvälinettä, vaikka on suunnitellut sen käyttöönottamista. Kyselytutkimuksessa ei myöskään tarkemmin kysytty ovatko vastaajat miten hyvin tietoisia tarjolla olevista vahvoista sähköisistä tunnistusvälineistä, jotta olisi saatu tarkemmin tietoa siitä, onko tunnistusvälineen tunnettavuudella vaikutusta vahvojen sähköisten tunnistusvälineiden hankintaan. Voidaan kuitenkin olettaa, että verkkopankkitunnukset ovat kansalisille tutuimpia johtuen siitä, että ne ovat olleet vuosikymmenien ajan käytössä ja jokaisella kansalaisella on käytännössä sellainen, jos heillä on pankkitili pankissa. Pankkiasiointi verkossa edellyttää verkkopankkitunnusten käyttöönottoa, kun taas mobiililiittymän käyttö ei edellytä mobiilivarmenteen käyttöä. Mobiilivarmenteet sekä kansalais- ja organisaatiovarmenteet näyttävät olevan huomattavasti vieraampia eikä niiden käyttäminen ole tullut luonnolliseksi osaksi käyttötottumuksia vuosikymmenien aikana, mikä osaltaan selittää niiden vähäisempää käyttöä.

Mikäli muiden kuin verkkopankkitunnusten käyttöä haluttaisiin edistää merkittävästi nykyistä nopeammin, yhtenä keinona voitaisiin harkita niiden käytön mahdollistamista jollain tavoin verkkopankkiin tunnistautumisessa ja nykyistä laajemmin verkko-ostoksia maksaessa. Tämä kuitenkin vaatisi tarkempaa selvittämistä muun muassa sen suhteen, missä määrin pankkitoimintaa koskeva lainsäädäntö mahdollistaisi tämän. Toinen keino edistää kaikkien vahvojen sähköisten tunnistusvälineiden käyttöä, on edistää ylipäätään vahvan sähköisen tunnistamisen käyttöönottoa sähköisissä asiointipalveluissa. Julkisen hallinnon sähköisissä asiointipalveluissa vahva sähköinen tunnistus on laaja-alaisesti käytössä eli mahdolliset edistämistoimet on syytä keskittää ennen kaikkea yksityiselle ja kolmannelle sektorille. Nämä samat edellä mainitut haasteet koskevat myös uusia mahdollisesti markkinoille tuotavia vahvoja sähköisiä tunnistusvälineitä.

Kyselytutkimuksen perusteella 49 prosenttia vastaajista ei nähnyt tarvetta uudelle valtion tarjoamalle tunnistusvälineelle ja 5 prosenttia ilmoitti, etteivät käytä sähköisiä asiointipalveluja ja ei siten tarvitse uutta valtion tunnistusvälinettä. Vastaajista 42 prosenttia sen sijaan olisi kiinnostunut käyttämään valtion tarjoamaa älypuhelimella ja/tai muistitikulla käytettävää vahvaa sähköistä tunnistusvälinettä, jos sen käyttö on ilmaista (32 %), käyttö olisi helppoa (30 %), sitä voisi käyttää muissa kuin julkisen hallinnon asiointipalveluissa (23 %) ja/tai sitä voisi käyttää työtehtävien hoitamisessa (9 %). Näistä, jotka olivat kiinnostuneita valtion tarjoamasta tunnistusvälineestä, 87 prosenttia olisi kiinnostunut käyttämään uutta valtion tarjoamaa tunnistusvälinettä myös muissa kuin julkisen hallinnon asiointipalveluissa.

Vastaajista, joilla on jo käytössään verkkopankkitunnukset ja/tai mobiilivarmenne, 91 prosenttia piti melko (32 %) tai erittäin (59 %) tärkeänä sitä, että verkkopankkitunnuksilla ja/tai mobiilivarmenteella olisi mahdollista tunnistautua julkisen hallinnon sähköisiin asiointipalveluihin myös jatkossa. 7 prosenttia vastanneista ei pitänyt tätä kovin tai lainkaan tärkeänä.

Vastaajista ainoastaan 4 prosentilla oli tarve tunnistautua muiden EU-maiden viranomaisten sähköisiin asiointipalveluihin, kun 97 prosenttia ei nähnyt tällaiselle tarvetta. Vastaajista 2 prosenttia oli jo tunnistautunut muiden EU-maiden viranomaisten sähköisiin asiointipalveluihin.

Kyselytutkimuksen perusteella voidaan todeta, että kansalaiset ovat pääosin tyytyväisiä nykyisin tarjolla oleviin vahvoihin sähköisiin tunnistusvälineisiin eikä valtion uudelle tunnistusvälineelle sähköisiin asiointipalveluihin tunnistautumiseksi nähdä erityistä tarvetta. Merkittävä osa kansalaisista olisi kuitenkin valmis ottamaan valtion uuden vahan sähköisen tunnistusvälineen käyttöönsä, mikäli väline täyttäisi tietyt ominaisuudet. Kansalaiset pitävät tärkeänä, että julkisen hallinnon sähköisiin asiointipalveluihin voi jatkossakin tunnistautua nykyisillä verkkopankkitunnuksilla ja/tai mobiilivarmenteilla. Sen sijaan kansalaisilla ei ole suurta tarvetta tunnistautua muiden EU-maiden viranomaisten sähköisiin asiointipalveluihin. Kansalaisten joukossa on kuitenkin erityisryhmiä, joilla ei tällä hetkellä ole käytössään vahvaa sähköistä tunnistusvälinettä ja jotka toivovat erityisominaisuuksia tunnistusvälineeltä, kuten mahdollisuutta tunnistautua muiden EU-maiden viranomaisten sähköisiin asiointipalveluihin.

5.1.2 Kannustimet, edellytykset ja esteet vahvan tunnistusvälineen käyttöönotolle

Kyselytutkimuksen mukaan 98 prosentilla vastaajista oli käytössään tietokone (91 %), tabletti (59 %) ja/tai älypuhelin (93 %) ja 96 prosentilla internet-yhteys joko kotona tai julkisessa paikassa käytettävissä, millä voi selata verkkosivuja tai käyttää sähköisiä asiointipalveluja. Ainoastaan 2 prosentilla vastaajista ei ollut käytössään tietokonetta, tablettia tai älypuhelinta ja 3 prosentilla internetyhteyttä. Tietokone, tabletti, älypuhelin ja/tai internetyhteys puuttuivat erityisesti 75-80 -vuotiailta.

Kyselytutkimuksen mukaan 99 prosentilla vastaajista oli käytössään vahva sähköinen tunnistusväline eli verkkopankkitunnukset, mobiilivarmenne tai kansalais- tai organisaatiovarmenne. 99 prosenttia näistä ilmoitti käyttävänsä vahvaa sähköistä tunnistusvälinettä vähintään kerran kuukaudessa ja 90 prosenttia vähintään kerran viikossa. Yhdellä prosentilta ei ollut käytössään mitään näistä tunnistusvälineistä ja erityisesti tämä koski 65-80 -vuotiaita, vaikka myös 15-24 ja 45-64 -vuotiaista löytyi henkilöitä, joilla ei ollut vahvaa sähköistä tunnistusvälinettä käytössään. Kyselytutkimuksen perusteella näyttää siltä, että pääsääntöisesti niillä kansalaisilla, joilla ei ole käytössään internetyhteyttä ei myöskään ole käytössään vahvaa sähköistä tunnistusvälinettä, mikä on hyvin yhdenmukaista sen kanssa, että henkilö, joka ei käytä internetyhteyttä ja sitä kautta sähköisiä asiointipalveluja, ei tarvitse myöskään vahvaa sähköistä tunnistusvälinettä.

Kyselytutkimuksessa myös kysyttiin, miksi vastaaja ei ole hankkinut vahvaa sähköistä tunnistusvälinettä, mutta niiden vastaajien määrä, joilla ei ole vahvaa sähköistä tunnistusvälinettä, jäi sen verran pieneksi, ettei tulosten perusteella voida tehdä kaikkia kansalaisia koskevia johtopäätöksiä. Jotain osviittaa mahdollisista syistä vastauksista voidaan kuitenkin saada ja niiden perusteella näyttäisi siltä, että vastaajat eivät ole hankkineet vahvaa sähköistä tunnistusvälinettä johtuen siitä, että joku toinen hoitaa hänen puolestaan asioista tai vastaaja hoitaa asiat fyysisesti toimipisteissä asioimalla tai muilla kuin sähköisillä viestintävälineillä. Nämä havainnot vaikuttavat yhdenmukaisilta sen havainnon kanssa, että vahva sähköinen tunnistusväline puuttuu erityisesti vanhempien ikäluokkien edustajilta. Yleisesti on kuitenkin tiedossa, ettei kaikilla ole mahdollisuutta saada vahvaa sähköistä tunnistusvälinettä käyttöönsä, vaikka he haluaisivatkin. Tällainen erityisryhmä on muun muassa alaikäiset.

Vastaajista 86 prosenttia ilmoitti, etteivät he ole tarvinneet muilta apua vahvan sähköisen tunnistusvälineen käyttämisessä viimeisten kuuden kuukauden aikana. Vastaavasti 14 prosentti ilmoitti tarvinneensa apua läheiseltään tai muulta henkilöltä vahvan sähköisen tunnistusvälineen käyttämisessä. Erityisesti apua tarvinneiden vastaajajoukko painottuu vanhimpiin ikäluokkiin, 55-80 -vuotiaisiin, ja mitä vanhemmasta ikäluokasta on kyse, sitä enemmän on vastaajia, jotka ovat ilmoittaneet tarvitsevansa apua. Poikkeuksena ovat 15-24 -vuotiaiden vastaajien joukko, jossa on enemmän vastaajia ilmoittanut tarvitsevansa apua kuin 25-34 tai 35-44 -vuotiaiden joukossa. Tämä selittynee pitkälti sillä, että 15-24 -vuotiaiden joukossa on alaikäisiä vastaajia, joille tunnistusvälineen käyttäminen ei vielä ole arkipäiväistä. Kuten edellä todettiin, kyselytutkimuksen perusteella haasteita vahvan sähköisen tunnistamisen käyttämiselle luovat muut kuin itse tunnistusvälineeseen liittyvät haasteet, kuten asiointipalvelun käyttöön liittyvät yhteysongelmat ja -häiriöt sekä yleinen tietoteknisten laitteiden hankala käytettävyys.

Tunnistuspalvelun ja -välineen käyttäjiltä perittävät kuukausimaksut vaihtelevat 1,99-4 euron välillä. Usealla toimijalla ja erityisesti pankkien tarjoamien tunnistuspalvelujen ja -välineiden käyttö ovat osa palvelupaketteja ja niistä perittäviä maksuja (esim. verkkopankkipalvelu sisältää tunnistuspalvelun lisäksi useita muita palveluja), jolloin eri tunnistuspalvelujen kuukausimaksuja ei voida suoraan verrata toisiinsa. DNA ja Elisa perivät kuukausimaksun lisäksi myös mobiilivarmenteen avausmaksun kuluttajaliittymäasiakkailtaan. Telialla mobiilivarmenteen käyttö kuuluu osaksi matkapuhelinliittymäpalvelu eikä mobiilivarmenteen käytöstä periä erillistä maksua.

Tunnistusvälineen tarjoaja	Avausmaksu	Kuukausimaksu	Lisätiedot
Aktia Pankki Oyj	- €	2,00 €	
Danske Bank A/S Suomen sivuliike	- €	3,00 €	Etuohjelmaan kuuluville ilmainen.
DNA Oyj	3,90 €	1,99 €	Yritysliittymissä mobiilivarmenne on maksuton.
Elisa Oyj	3,90 €	1,99 €	Yritysliittymissä mobiilivarmenne on maksuton.
Nordea Bank Oyj	- €	3,00 €	
Oma Säästöpankki Oyj	- €	2,00 €	Verkkopankin kuukausimaksu sisätäen viestinvälityksen omaan pankkiin, tili-, rahasto- ja lainatiedot, omien tilien väliset siirrot, rahastomerkinnät, vaihdot ja lunastukset, 15 minuuttia viivästetty markkinainformaatio ja OmaMobiili-palvelun.
OP Ryhmä	- €	3,00 €	Alle 26-vuotiaille maksuton.
POP-Ppankki -ryhmä	- €	4,00 €	Verkkopankin kuukausimaksu. Kuukausimaksu jäsenille 3 €/kk.
S-Pankki Oyj	- €	2,50 €	Pankkitunnussopimuksen kuukausimaksu 2,50 euroa sisältäen asioinnin verkkopankissa, S-mobiilissa ja S-Pankin asiakaspalvelussa sekä tunnistautumisen ja maksaminen muissa verkkopalveluissa. Kuukausimaksu asiakasomistajille 0 €/kk.
Svenska Handelsbanken AB	- €	3,00 €	Verkkopankin kuukausimaksu sisältäen mobiilipankin, verkkomaksun ja tunnistuspalvelun sekä pankin puhelinpalveluun tunnistautumisen. Alle 27-vuotiaille maksuton.
Säästöpankkiryhmä	- €	2,50 €	Verkkopalveluiden kuukausimaksu toimipaikasta riippuen 2,50 tai 3 €/kk. Kuukausimaksu sisältää mobiilisovelluksen, verkkopankin, verkkopalvelutunnukset, viestinvälitystoiminnon omaan pankkiin, tili-, rahasto- ja lainatiedot, omien tilien väliset siirrot, rahastomerkinnät, vaihdot ja lunastukset ja markkinainformaation.
Telia Finland Oyj	- €	- €	Mobiilivarmenne on maksuton matkapuhelinliittymän lisäpalvelu.

Taulukko 2: Tunnistuspalvelun/-välineen käytöstä käyttäjiltä perittävät maksut 1.2.2021. Hintatiedot on kerätty vahvan sähköisen tunnistusvälineen tarjoajien verkkosivuilta.

Lähtökohtaisesti voidaan katsoa, että tunnistuspalvelun ja välineen käytöstä käyttäjiltä perittävät maksut ovat kohtuullisia eikä niiden voida katsoa muodostavan merkittävää estettä vahvan sähköisen tunnistusvälineen käyttämiselle. Puhelinliittymä katsotaan kuuluvan osaksi Kelan myöntämää perustoimeentulon perusosaa ja jokapäiväisiä elämän välttämättömiä menoja, jolloin myös yhteiskunnan vähävaraisimmilla on mahdollisuus saada puhelinliittymä ja sitä kautta vahva sähköinen tunnistusväline käyttöönsä yhteiskunnan tukemana.

Kannustimista, edellytyksistä ja esteistä käyttää vahvaa sähköistä tunnistusta voidaan todeta, että kansalaisilla on käytössään vahva sähköinen tunnistusväline, jos ne haluavat käyttää sähköisiä asiointipalveluja tai yleensäkin tietoteknisiä laitteita. Mikäli vahva sähköinen tunnistusväline halutaan saada laajempaa käyttöön, tulisi ensisijaisesti tehdä toimenpiteitä, joilla loputkin kansalaisista saadaan käyttämään sähköisiä asiointipalveluja ja yleensäkin tietoteknisiä laitteita. Erityisesti tämä koskee vanhempien ikäluokkien edustajia. Kyselytutkimuksen perusteella ei ole viitteitä siitä, että itse vahvojen sähköisten tunnistusvälineiden käyttö olisi esteenä vahvan sähköisen tunnistusvälineen hankkimiselle ja käyttämiselle. Käyttäjiltä perittävien maksujenkaan ei voida katsoa muodostavan estettä vahvan sähköisen tunnistuksen käyttämiselle. Poikkeuksen edellä mainittuihin tekevät ne henkilöt, jotka eivät syystä tai toisesta saa vahvaa sähköistä tunnistusvälinettä, vaikka haluaisivatkin. Näiden henkilöiden kannalta tulisikin miettiä mahdollisia toimenpiteitä, joilla heille mahdollistettaisiin vahva sähköinen tunnistusväline. Asettaako esimerkiksi lainsäädäntö heille esteitä saada vahvaa sähköistä tunnistusvälinettä ja onko tarpeen säätää erillinen yleispalveluvelvoite tarjota vahvaa sähköistä tunnistusvälinettä näille henkilöille.

Myös sähköiset asiointipalvelut tulisi saada kattavammin ja laaja-alaisemmin tarjoamaan mahdollisuutta tunnistautua käyttäen vahvaa sähköistä tunnistusvälinettä, mikäli vahva sähköinen tunnistusväline halutaan saada laajempaan käyttöön.

5.1.3 Erityisryhmien erityistarpeet tunnistuspalveluille

Erityisryhmät muodostavat hyvin toisistaan poikkeavia ryhmiä. Erityisryhmiin kuuluu arviolta reilut 1,6 miljoonaa henkilöä. Vahvan sähköisen tunnistamiseen liittyvien tarpeiden ja käyttöön liittyvien haasteiden ratkaisutoimenpiteiden näkökulmasta nämä erilaiset ryhmät voidaan jakaa neljään joukkoon. Näihin jokaiseen joukkoon ja jokaisen joukon sisällä jokaiseen ryhmään kuuluvien henkilöiden haasteet vaativat jokainen hieman erilaista ratkaisua eikä kaikkien näiden henkilöiden haasteita voida ratkaista yhdellä toimenpiteellä.[30] Alla on esitetty vain karkea arvioi

[30] Ratkaisut ovat lähtökohtaisesti järkevä toteuttaa siten, että ne hyödyttävät kaikkia eikä vain tiettyä ryhmää, mutta jossain tapauksissa voi olla myös järkevää toteuttaa vain tietylle ryhmälle kohdistettuja ratkaisuja.

näistä asioista. Olisi hyvä, että nämä erityisryhmät ja niiden tarpeet kartoitettaisiin vielä erikseen sekä se, mihin eritysryhmien haasteet kohdistuvat eli kohdistuvatko haasteet esimerkiksi käytössä oleviin tunnistusvälineisiin, lainsäädäntöön vai sähköisiin asiointipalveluihin. Erikseen tehtävässä kartoitustyössä olisi tärkeää ottaa myös nykyiset ja potentiaaliset tunnistuspalvelun tarjoajat mukaan arvioimaan tilannetta sekä keinoja ratkaista kartoituksessa esille tulevia haasteita. Erityisryhmien tarpeiden huomioinen ja palvelujen kehittäminen siten, että jokainen voi niitä käyttää, parantaa lähtökohtaiseesti myös erityisryhmän ulkopuolelle kuuluvien henkilöiden mahdollisuuksia käyttää palveluja.

Suurimman joukon muodostavat henkilöt, jotka eivät syystä tai toisesta saa käyttöönsä suomalaista vahvaa sähköistä tunnistusvälinettä. Tähän joukkoon kuuluvat muun muassa alle 15-vuotiaat suomalaiset, ulkomaalaiset opiskelijat ja tutkijat, ulkomaalaisten yritysten edustajat, ulkomaalaiset yrityksen perustajat, ulkomailta Suomeen töihin tulevat ja ulkomailta Suomeen muuttavat. Tämän joukon voi myös jakaa henkilöihin, joilla on oikeus saada suomalainen henkilötunnus, sekä henkilöihin, joilla ei ole oikeutta saada suomalaista henkilötunnusta. Näiden henkilöiden kannalta haaste käyttää vahvaa sähköistä tunnistusvälinettä liittyy lähes poikkeuksetta muihin seikkoihin kuin vahvan sähköisen tunnistusvälineen käytettävyyteen tai hinnoitteluun. Pääasiallisena syynä on kansallinen lainsäädäntö, joka estää näitä henkilöitä saamasta henkilötunnusta, jolloin heille ei voida myöskään myöntää vahvaa sähköistä tunnistusvälinettä, tai alle 15-vuotiasta[31] suomalaista tekemästä häntä koskevia oikeudellisia päätöksiä. Tähän joukkoon kuuluu arviolta reilut 1,1 miljoonaa henkilöä.[32] Tähän joukkoon kuuluvien kannalta olennaista on ennen kaikkea arvioida lainsäädännön tai sähköisten asiointipalvelujen muutostarpeet ja tehdä sellaisia muutoksia, jotka mahdollistavat turvallisen sähköisen asioinnin esimerkiksi henkilön ikä huomioiden ja vahvan sähköisen tunnistusvälineen myöntämisen joukkoon kuuluville henkilöille. Myös mahdollisen yleispalvelulainsäädännön, jolla vahvan sähköisen tunnistuspalvelun tarjoajat tai osa niistä velvoitettaisiin tarjoamaan vahvaa sähköistä tunnistusvälinettä tietyin ehdoin, tarpeellisuutta voisi arvioida.[33]

Toisen joukon muodostavat henkilöt, joille syystä tai toisesta tietoteknisten laitteiden ja sitä kautta myös sähköisten asiointipalvelujen, mukaan lukien vahvan sähköisen tunnistusvälineen käyttö, on hankalaa. Tähän joukkoon kuuluu arviolta 170 000 henkilöä.[34] Näiden henkilöiden kannalta ensisijainen haaste on tietoteknisten laitteiden ja sähköisten asiointipalvelujen käyttäminen. Näiden henkilöiden haasteita voidaan madaltaa tukemalla, kouluttamalla ja opastamalla heitä tietoteknisten laitteiden ja sähköisten asiointipalvelujen käyttämisessä sekä tekemällä laitteista, sähköisistä asiointipalveluista ja vahvoista sähköisistä tunnistusvälineistä helpommin käytettäviä ja saavutettavimpia. Esimerkiksi julkinen hallinto ja kolmannen sektorin toimijat voisivat tarjota kyseisiä tuki- ja koulutuspalveluja. Julkinen hallinto voisi myös kilpailuttaa, ostaa ja tarjota näille erityisryhmien henkilöille vahvan sähköisen tunnistuspalveluja, jotka ovat yleisesti tarjolla olevia tunnistuspalveluja helpommin käytettäviä ja saavutettavimpia sekä jotka täyttävät vaaditut saavutettavuusvaatimukset. Lainsäädännöllä ja sääntelyllä voitaisiin myös osaltaan ohjata,

[31] Suomessa alle 18-vuotiaan katsotaan olevan alaikäinen ja hänellä ei ole lainsäädännön mukaan oikeutta itse määrätä omaisuudestaan, tehdä tärkeitä sopimuksia tai muita merkittäviä toimenpiteitä. Alaikäinen voi kuitenkin tehdä olosuhteisiin nähden tavanomaisia ja merkitykseltään vähäisiä toimenpiteitä. Alaikäinen, joka on täyttänyt 15 vuotta, voi itse määrätä siitä omaisuudesta, jonka hän on omalla työllään ansainnut. Tunnistuslaissa ei ole säädetty alaikärajaa vahvan sähköisen tunnistamisen myöntämiselle, vaan vahvaa sähköistä tunnistusvälinettä myönnettäessä olennaisena asiana on oletettu kyky huolehtia välineestä vastuullisesti ja mahdollisesti tehdä oikeustoimia sähköisissä asiointipalveluissa. Alaikäisten kannalta asiaa tulisikin tarkastella ensisijaisesti sähköisten asiointipalvelujen näkökulmasta siltä kannalta, mitä alaikäinen voi niissä tehdä pätevästi.

[32] Tilastokeskuksen Väestörakenne-tilaston mukaan vuonna 2019 alle 20-vuotiaita oli noin 1 168 000, joista 15-19-vuotiaita noin 297 000, 10-14-vuotiaita noin 309 000, 5-9-vuotiaita noin 306 000 ja 0-4-vuotiaita 256 000. Väestörakenne-tilaston mukaan vuonna 2019 Suomessa asui noin 268 000 ulkomaalaista, joilla ei ollut Suomen kansalaisuutta.

[33] Yleispalveluvelvoitteen asettamisen sijaan valtiohallinto voisi myös kilpailuttaa niin sanotun yleispalvelun tarjoajan/-t, jotka saisivat erityisaseman tarjota vahvoja sähköisiä tunnistuspalveluja kilpailutuksen kautta.

[34] Arvio on laskettu perustuen valtiovarainministeriön teettämän kyselytutkimuksesta saatuihin vastauksiin kysymykseen siitä, kuinka monella ei ollut käytettävissään internetyhteyttä joko kotona tai jossain julkisessa paikassa.

ja jopa velvoittaa, tekemään sähköisistä asiointipalveluista saavutettavia ja tuomaan tarjolle myös esteettömiä sähköisiä tunnistusvälineitä.[35] Näiden henkilöiden kannalta tarvitaan useita erilaisia toimenpiteitä eivätkä haasteet ole ratkaistavissa jollain yksittäisellä toimenpiteellä, kuten vain tarjoamalla esteetöntä vahvaa sähköistä tunnistusvälinettä.

Kolmantena joukkona ovat henkilöt, joilla on vahva sähköinen tunnistusväline käytössään, mutta joille tietoteknisten laitteiden, sähköisten asiointipalvelujen ja vahvan sähköisen tunnistusvälineen käyttö on hankalaa. Tähän joukkoon kuuluvat niin sanotusti toimintarajoitteiset henkilöt (esimerkiksi sokeat ja muutoin henkilöt, joiden näkökyky on merkittävästi heikentynyt, sekä henkilöt, joiden motoriikka ja motoristiset taidot ovat merkittävästi heikentyneet esimerkiksi normaalin ikääntymisen seurauksena). Moni joukkoon kuuluva henkilöä tarvitsee yleensä erillisiä apuvälineitä (suurennuslasi, pistekirjoitus, ruudunlukuohjelma, jne.) tai avustavaa henkilöä käyttääkseen tietoteknisiä laitteita, sähköisiä asiointipalveluja ja vahvaa sähköistä tunnistusvälinettä. Tähän joukkoon kuuluu arviolta reilut 270 000 henkilöä aina iäkkäistä ihmisistä näkö- ja kehitysvammaisiin. Näkövammaisten liiton mukaan Suomessa on arviolta 55 000 näkövammaista, joista noin 10 000 on sokeita. Näkövammaisista yli 80 % on yli 65-vuotiaita ja alle 18-vuotiaita vain noin 2 %.[36] Vastaavasti kehitysvammaisia arvioidaan olevan noin 50 000 ihmistä.[37] Haasteista ja rajoitteista huolimatta pääosa tähän joukkoon kuuluvista henkilöistä kykenee käyttämään vahvaa sähköistä tunnistusvälinettä. Heidän kannaltaan tarpeet ennen kaikkea kohdistuvat siihen, että sähköiset asiointipalvelut ja käytössä olevat tunnistusvälineet ovat helppokäyttöisiä ja saavutettavia (esim. riittävän suuren tekstin käyttäminen sähköisissä asiointipalveluissa) ja että ne tukevat esteettömästi erilaisia teknisiä apuvälineitä. Kuten edellä olevan joukon osalta, myös tähän joukkoon kuuluvien henkilöiden osalta vahvan sähköisen tunnistusvälineen käyttämiseen, ja yleensäkin sähköisten asiointipalvelujen käyttämiseen, liittyviä haasteita voitaisiin alentaa esimerkiksi kilpailuttamalla, ostamalla ja tarjoamalla julkisen hallinnon toimesta vahvan sähköisen tunnistamisen palveluja, jotka ovat tarjolla olevia tunnistuspalveluja helpommin käytettäviä ja saavutettavimpia sekä jotka täyttävät vaaditut saavutettavuusvaatimukset. Samoin lainsäädännöllä voitaisiin myös osaltaan ohjata, ja jopa velvoittaa, tekemään sähköisistä asiointipalveluista saavutettavia ja tuomaan tarjolle myös esteettömiä sähköisiä tunnistusvälineitä.

Neljännen joukon muodostavat henkilöt, jotka eivät syystä tai toisesta halua käyttää tietoteknisiä laitteita ja sähköisiä asiointipalveluja, vaikka mahdollisesti kykenisivätkin niitä muutoin käyttämään. Tähän joukkoon kuuluu arviolta reilut 50 000 henkilöä. Lähtökohtaisesti tähän joukkoon kuuluvien henkilöiden kannalta tulee varmistaa mahdollisuus hoitaa asiansa käyntiasiointina eri toimipisteissä. Ei ole todennäköistä, että tähän joukkoon kuuluvia henkilöitä saataisiin suuressa määrin käyttämään tietoteknisiä laitteita ja sähköisiä asiointipalveluja mukaan lukien vahvaa sähköistä tunnistusta.

[35] Esimerkiksi niin sanottu saavutettavuusdirektiivi ((EU) 2016/2102)) ja sitä seuraava kansallinen lainsäädäntö (Laki digitaalisten palvelujen tarjoamisesta) vaativat viranomaisia tekemään digitaaliset palvelut saavutettaviksi. Saavutettavuudella tarkoitetaan, että verkkosivut ja mobiilisovellukset sekä niiden sisällöt ovat sellaisia, että kuka tahansa voisi niitä käyttää ja ymmärtää mitä niissä sanotaan. Saavutettavuusdirektiivin tavoite on edistää kaikkien mahdollisuutta toimia täysivertaisesti digitaalisessa yhteiskunnassa, luoda Euroopan laajuiset yhdenmukaiset minimitason vaatimukset julkisen sektorin verkkosivustojen ja mobiilisovellusten saavutettavuudelle, parantaa digitaalisten palveluiden laatua ja parantaa Euroopan unionin saavutettavuuden toteuttamisen sisämarkkinoita. Lähde: https://vm.fi/saavutettavuusdirektiivi.

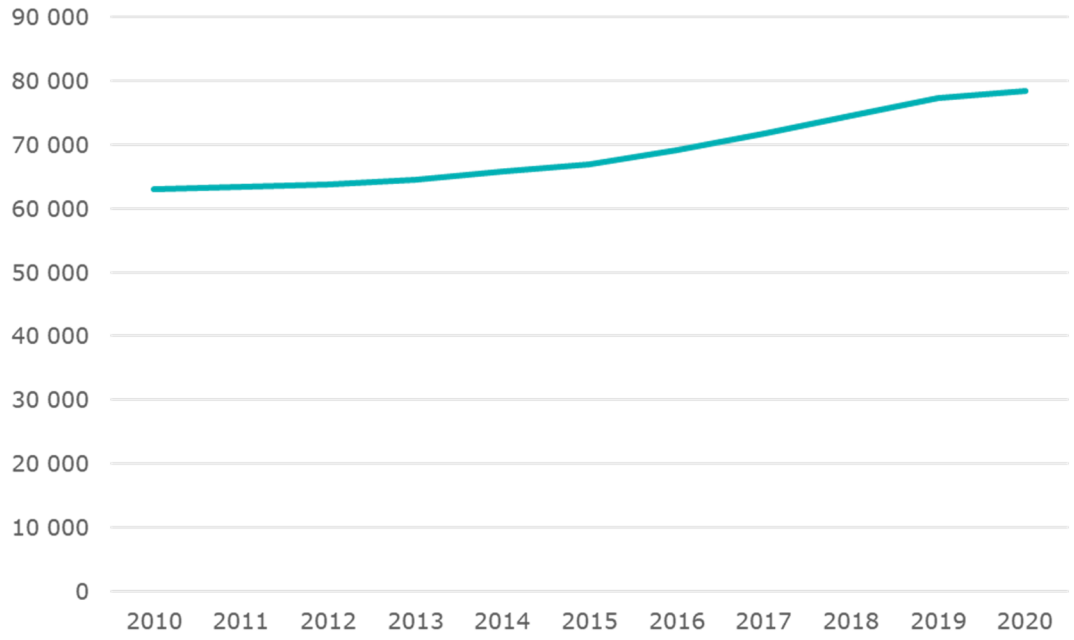
[36] Lähde: Näkövammaisten liiton verkkosivusto https://www.nkl.fi/fi/nakovammaisuus (Tieto haettu 28.1.2021). *Näkövammaiseksi määritellään henkilö, jonka paremman silmän laseilla korjattu näöntarkkuus on heikompi kuin 0.3, ja sokeaksi henkilö, jonka paremman silmän laseilla korjattu näöntarkkuus on alle 0.05 tai näkökenttä supistunut halkaisijaltaan alle 20 asteeseen, tai jos toiminnallinen näkö on jostain muusta syystä vastaavalla tavalla heikentynyt.*

[37] Lähde: Kehitysvammaliiton verkkosivut https://www.kehitysvammaliitto.fi/kehitysvammaisuus/ (Tieto haettu 28.1.2021). *Kehitysvammaisuus tarkoittaa vaikeutta oppia ja ymmärtää uusia asioita. Kehitysvammaisuuden vaikutus yksilön elämään vaihtelee paljon. Kehitysvamma voi olla lievä, jolloin henkilö tulee toimeen melko itsenäisesti ja tarvitsee tukea vain joillakin elämänalueilla. Vaikeasti kehitysvammainen ihminen tarvitsee jatkuvaa tukea.*

Edunvalvottavien ja edunvalvontavaltuuden alaisten henkilöiden voidaan myös katsoa muodostavan oman joukkonsa, vaikka he kuuluvatkin jo johonkin tai joihinkin edellä mainituista joukoista. Myös tulevaisuudessa on joukko henkilöitä, jotka eivät tule itsenäisesti toimeen ja kykene kaikilta osin hoitamaan omia asioitaan. Sähköinen valtuuttaminen on jatkossa yksi merkittävimmistä keinoista hoitaa tähän joukkoon kuuluvien henkilöiden asioita.

Digi- ja väestötietoviraston tilastojen mukaan vuonna 2020 oli noin 78 000 edunvalvonnan ja edunvalvontavaltuutuksen alaista henkilöä. Edunvalvojan määrääminen on viimesijainen keino järjestää tietyn henkilön asioiden hoito. Edunvalvojan määrääminen edellyttää, että apua tarvitsevan henkilön asiat eivät tule asianmukaisesti hoidetuiksi muilla tavoin. Edunvalvottaviin kuuluvat myös alaikäiset lapset, joiden huoltajat toimivat heidän edunvalvojinaan. Huoltajien on hoidettava alaikäisen omaisuutta huolellisesti ja suunnitelmallisesti. Alaikäisen omaisuutta voidaan käyttää vain hänen omaksi hyödykseen ja hänen henkilökohtaisiin tarpeisiinsa huomioiden kuitenkin vanhempien elatusvastuu. Alaikäisen edunvalvonta päättyy, kun hän täyttää 18 vuotta. Edunvalvoja yleensä hoitaa edunvalvottavan asioita ja edunvalvottavalla ei välttämättä ole tarvetta vahvalle sähköiselle tunnistusvälineelle. Alaikäisillä on kuitenkin terveystietoihinsa liittyviä oikeuksia, jotka ovat lisänneet vahvan sähköisen tunnistusvälineen tarvetta olennaisesti.

Edunvalvontavaltuutus on edunvalvontaa joustavampi tapa järjestää asioiden hoito. Edunvalvontavaltuutuksella henkilö voi itse etukäteen järjestää asioidensa hoidon sen varalta, että hän tulee myöhemmin kykenemättömäksi hoitamaan asioitaan. Edunvalvontavaltakirjassa henkilö (valtuuttaja) nimeää valtuutetun hoitamaan asioitaan. Edunvalvontavaltuutus tulee voimaan, kun holhousviranomainen on sen vahvistanut.



Kuva 4: Voimassaolevien edunvalvontojen ja edunvalvontavaltuutusten kehittyminen vuosittain. (Lähde: Digi- ja väestötietovirasto)

Edunvalvonnan ja edunvalvontavaltuuden lisäksi toisen puolesta asiointi ja sähköinen valtuuttaminen voivat olla ratkaisu joidenkin henkilöiden osalta, joille tietoteknisten laitteiden ja sähköisten asiointipalvelujen, mukaan lukien vahvan sähköisen tunnistusvälineen käyttäminen, ovat haasteellisia tai jotka eivät halua käyttää näitä palveluja. Toisen puolesta asiointia ja sähköistä valtuuttamista käsitellään alla omassa luvussa 5.1.4. Voitaisiin myös harkita olisiko joissain tilanteissa mahdollista hyväksyä avustajan käyttäminen vahvan sähköisen tunnistamisen käyttämisessä.

Valtiovarainministeriö teki kyselyn toimintarajoitteisille niitä edustavien vammaisjärjestöjen kautta erityisryhmiin kuuluvien kokemista haasteista tunnistuspalvelujen käytössä. Kyselyyn vastasi 98 henkilöä. Kyselyn otos ei ole edustava eikä vastauksia ole mahdollista yleistää koskemaan kaikkia erityisryhmiin kuuluvia suomalaisia ja Suomessa asuvia ulkomaalaisia. Vastauksien perusteella saadaan kutienkin osviittaa mahdollisista haasteista, joita erityisryhmiin kuuluvat kokevat tunnistuspalvelujen käytössä.

Yleisesti voidaan todeta, etteivät vastausten perusteella valmiudet käyttää vahvaa sähköistä tunnistusta ja sen käyttö merkittävästi poikenneet valtaväestöstä.[38] Vaihtoehtoiset vahvat sähköiset tunnistusvälineet saattavat myös jopa edesauttaa ja helpottaa vahvan sähköisen tunnistamisen käyttämistä. Esimerkiksi eräs vastaaja perusteli uuden tunnistusvälineen käyttöönottamista tai vaihtamista avoimeen tekstikenttään annetussa vastauksessa sillä, että "*mobiilivarmenne toimii myös vanhemmilla puhelimilla ja sokeiden ruudunlukuohjelmilla*". Vastaajista 89 prosenttia ilmoittikin tunnistusvälineen käyttämisen olevan helppoa, vaikka osa olikin kokenut haasteita sen käyttämisessä. Vastaajista 11 prosenttia ilmoitti käyttämisen olevan haastavaa.

Haasteita koettiin erityisesti siinä, että sähköinen asiointipalvelu oli itsessään hankala käyttää (51 %), tunnistautumisvaiheessa tarjotut ohjeet olivat epäselvät (32 %), tunnistautumisvaiheessa ruudulla näkyvä teksti oli liian pientä (20 %), tunnistusvälineen tarjoajalta saadut käyttöohjeet olivat epäselvät (17 %), käyttäjätunnuksen ja salasanan muistaminen oli hankalaa (15 %), tunnuslukulistan numerot ovat liian pienellä (15 %), asiointipalvelu ei ollut tukenut oman vahvan sähköisen tunnistusvälineen käyttämistä (15 %), tarvitsi avustajaa tunnuksilla kirjautuakseen (15 %), käytetty apulaite ei osannut lukea tunnuslukulistaa (15 %), käytetty tietotekninen laite oli hankala käyttää (12 %), tunnuslukulaitetta oli hankala käyttää (10 %), tunnuslukusovellusta oli hankala käyttää (10%), tunnuslukulista oli kadoksissa (7 %) ja kansalaisvarmenteen lukemiseen tarvittava kortinlukulaite ei ollut aina käytettävissä (5 %). Muissa koetuissa ongelmissa (13 %) korostuivat myös näkemiseen ja näkemistä tukevien apulaitteiden (esim. ruudunlukuohjelmat sekä pistekirjoitussovellukset ja -laitteet) tuen puute asiointipalveluissa.

Pääosa näistä erityisryhmissä koetuista haasteista on helposti ratkaistavissa kehittämällä sähköisiä asiointipalveluja ja vahvoja sähköisiä tunnistusvälineitä huomioimalla entistä paremmin erityisryhmien tarpeet niille. Jos sähköisten asiointipalvelujen ja tunnistuspalvelujen suunnittelussa otetaan jo suunnitteluvaiheessa huomioon saavutettavuutta ja esteettömyyttä tukevat ominaisuudet, ne eivät välttämättä lisää normaaleja palvelujen kehityskustannuksia.

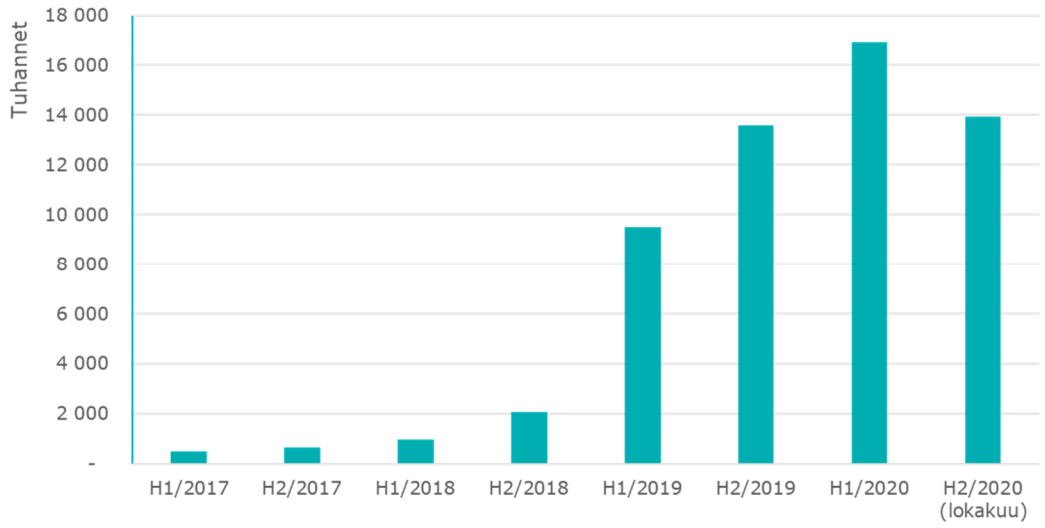
5.1.4 Toisen puolesta asiointi ja sähköinen valtuuttaminen

Kyselytutkimuksen perusteella 44 prosenttia vastanneista oli hoitanut jonkun toisen henkilön asioita omaa vahvaa tunnistusvälinettä käyttäen. Eniten vastaajat olivat hoitaneet oman lapsensa (20 %), yrityksen (13 %), oman puolison (11 %) ja oman vanhemman (8 %) asioita. Hoitaessaan toisen henkilön asioita 78 prosenttia ei ollut kokenut haasteita asioiden hoitamisessa, kun 21 prosenttia oli kokenut jotain haasteita. Ennen kaikkea vastaajat ovat kokeneet haasteita siinä, ettei heillä ole ollut oikeuksia toisen tietoihin ja/tai mahdollisuutta hoitaa toista tai jotain organisaatiota koskevia asioita. Muut haasteet liittyivät lähinnä tieto- ja tietoliikenneteknisiin ongelmiin ja joidenkin vastaajien osalta myös vahvan sähköisen tunnistusvälineen käyttämiseen ja mahdollisiin häiriöihin välineen käytössä.

[38] Vastaajista 99 prosentilla oli käytössään tietokone, tabletti, älypuhelin ja/tai puhelin sekä internet-yhteys, jolla esimerkiksi selata verkkosivuja ja käyttää sähköisiä palveluja. 94 prosentilla oli käytössään verkkopankkitunnukset, 20 prosentilla mobiilivarmenne, 9 prosentilla kansalaisvarmenne ja 2 prosentilla organisaatiovarmenne. Kolmella prosentilla vastanneista ei ollut vahvaa sähköistä tunnistusvälinettä käytössään. Vastaajat, joilla oli käytössään vahva sähköinen tunnistusväline, 90 prosenttia ilmoitti käyttävänsä tunnistusvälinettä vähintään kerran viikossa ja 98 prosenttia vähintään kerran kuukaudessa.

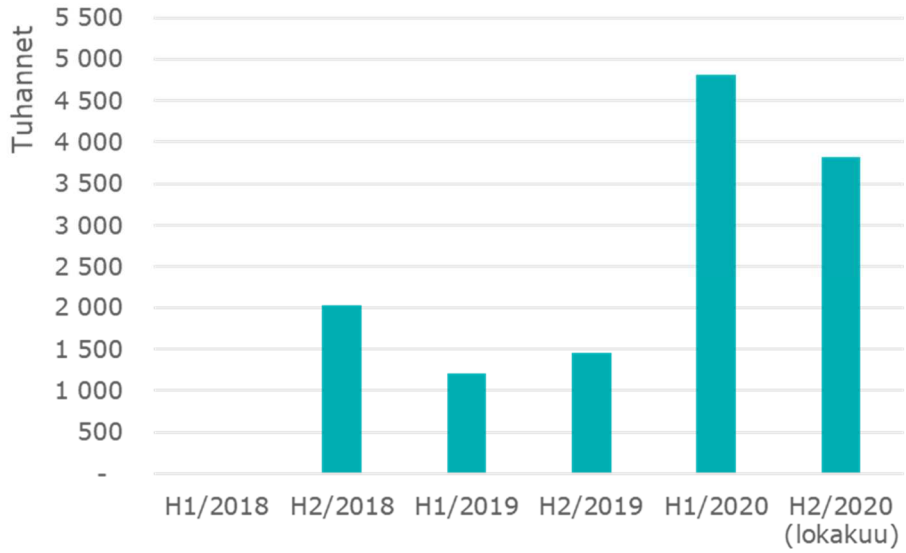
Julkisen hallinnon asiointipalveluihin on mahdollisuus antaa toiselle henkilölle valtuutus eli oikeudet päästä käsiksi tietoihin ja hoitaa asioita yrityksen tai itsensä puolesta. Valtuutus on mahdollista antaa vahvasti tunnistautuneena Suomi.fi -palvelussa tai erillisellä Digi- ja väestötietovirastolle toimitettavalla kirjallisella hakemuksella. Valtuutta on mahdollista käyttää julkisen hallinnon sähköisissä asiointipalveluissa vain vahvasti tunnistautuneena vahvalla sähköisellä tunnistusvälineellä. Valtuutus mahdollistaa muun muassa erityisryhmiin kuuluvien, kuten alaikäisten, asioiden hoitamisen heidän puolestaan, mikäli lainsäädäntö muutoin mahdollistaa tämän. Yksityisellä ja kolmannella sektorilla ei ole vastaavanlaista keskitettyä palvelua tarjolla, vaikkakin osa sähköisten palvelujen tarjoajista ovat mahdollistaneet toisen puolesta asioinnin omissa palveluissaan. Suomi.fi:n valtuutuspalvelu on kuitenkin myös yksityisen ja kolmannen sektorin käyttävissä.

Julkisen hallinnon sähköisessä asiointipalvelussa valtuutusta käytettäessä palvelu tarkistaa valtuutuksen Suomi.fi -palvelusta tekemällä niin sanotun valtuuskyselyn valtuusrekisteistä. Valtuuksien antaminen ja käyttäminen ovat kasvaneet merkittävästi viimeisten vuosien aikana ja kasvu näyttää jatkuvan vahvana. Vuoden 2017 ensimmäisen vuosipuoliskon aikana valtuuskyselyitä tehtiin noin 0,5 miljoonaa, kun vuoden 2020 ensimmäisellä vuosipuoliskolla määrä oli jo lähes 17 miljoonaa kyselyä.



Kuva 5: Suomi.fi -palvelussa tehdyt valtuuskysely henkilön ja yrityksen puolesta asiointiin. Vuoden 2020 toisen vuosipuoliskon tiedot sisältävät vain valtuuskyselyjen määrän lokakuun loppuun saakka. (Lähde: Digi- ja väestötietovirasto)

Myös Suomi.fi -palvelussa vahvistettujen valtuuksien ja valtuuspyyntöjen määrät ovat kasvaneet merkittävästi viime vuosina ja myös näiden osalta kasvu näyttää jatkuvan seuraavat vuodet. Vuoden 2018 ensimmäisen vuosipuoliskon aikana tehtiin noin 20 000 vahvistettua valtuutta ja valtuuspyyntöä, kun vuoden 2020 ensimmäisellä vuosipuoliskolla määrä oli jo noin 4,8 miljoonaa.



Kuva 6: Suomi.fi -palvelussa vahvistettujen valtuuksien ja valtuuspyyntöjen lukumäärä. Vuoden 2020 toisen vuosipuoliskon tiedot sisältävät vain valtuuskyselyjen määrän lokakuun loppuun saakka. (Lähde: Digi- ja väestötietovirasto)

Valtuutuksen mahdollistaminen ja hyödyntäminen ovat avainasemassa, kun etsitään erilaisia keinoja mahdollistaa erityisryhmien asioiden hoitaminen sähköisesti niissä tilanteissa, joissa erityisryhmään kuuluva henkilö ei itse kykene käyttämään tietoteknisiä laitteita, sähköisiä asiointipalveluja ja/tai vahvaa sähköistä tunnistusvälinettä. Valtuutuksien mahdollistamisella ja hyödyntämisellä voidaan myös saavuttaa kustannussäästöjä, kun sähköisä asiointipalveluja käytetään entistä enemmän korvaamaan fyysistä asiointia.

5.1.5 Sähköinen allekirjoittaminen

Asiakirjojen sähköinen allekirjoittaminen on yksi käyttökohde, mihin vahvaa sähköistä tunnistusvälinettä usein käytetään osana allekirjoituksen toteuttamista. Ennen allekirjoittamista asiakirjaa allekirjoittava henkilö tunnistetaan vahvalla sähköisellä tunnistusvälineellä. Fyysisessä maailmassa tätä voi verrata siihen tilanteeseen, missä allekirjoittava henkilö tunnistetaan esimerkiksi passin tai henkilökortin kuvaa vertaamalla fyysisesti paikalla olevaan allekirjoittavan henkilöön enenen kuin henkilö allekirjoittaa asiakirjan. Fyysisen tunnistamisen jälkeen henkilö allekirjoittaa asiakirjan yleensä vähintäänkin kahtena kappaleena, jolloin asiakirjasta jää vähintäänkin molemmille asiakirjan kohteena olevalle taholle omat allekirjoitetut kappaleet. Tällä varmistetaan se, että allekirjoitettua asiakirjaa ei voida muuttaa ilman, ettei asiakirjaa allekirjoiteta vähintään kahtena kappaleena uudelleen.

eIDAS-asetuksen mukaisissa hyväksytyissä ja lähtökohtaisesti myös kehittyneissä sähköisissä allekirjoituksissa allekirjoitukseen käytetään erillistä allekirjoitusvarmennetta, joka varmentaa paitsi haltijansa henkilöllisyyden, myös liittää allekirjoituksen muuhun sähköiseen tietoon, kuten esimerkiksi sähköpostiviestiin, siten, että tiedon mahdolliset muutokset voidaan havaita. Jos sähköistä asiakirjaa muutetaan jälkikäteen, aiemmin tehty allekirjoitus ei täsmää muutetun asiakirjan sisällön kanssa. Fyysisessä maailmassa tätä voidaan verrata siihen, että asiakirja allekirjoitetaan vähintään kahtena kappaleena. Markkinoilla on kuitenkin myös tarjolla sähköisiä allekirjoituspalveluita, joissa vahvaa sähköistä tunnistusvälinettä käytetään myös allekirjoituksen tekemiseen. Näissä palveluissa yleensä allekirjoitetun asiakirjan muuttamattomuutta ei voida taata tai se perustuu luottamukseen allekirjoituspalveluun ja tämän järjestelmiin.

Valtiovarainministeriön teettämän kyselytutkimuksen mukaan 51 prosenttia niistä vastaajista, joilla oli käytössään jokin vahva sähköinen tunnistusväline, olivat käyttäneet vahvaa sähköistä tunnistusvälinettä allekirjoittaakseen sähköisesti jonkin

asiakirjan liittyen omiin, läheisten, yrityksen tai jonkin järjestön asioihin. 48 prosenttia vastanneista ei ollut käyttänyt vahvaa sähköistä tunnistusvälinettä asiakirjojen allekirjoittamiseen ja 1 prosentti ei osannut sanoa. Kyselytutkimuksessa ei kysytty tarkemmin, minkä tasoista sähköistä allekirjoitusta vastaajat olivat käyttäneet. Kyselytutkimuksessa ei myöskään kysytty tarkemmin mahdollisista esteistä sähköisen allekirjoituksen käyttämisessä tai syistä, miksi sitä ei mahdollisesti oltu käytetty.

KKV:n tunnistusvälineen tarjoajilta saamien selvitysten perusteella sähköinen allekirjoituspalvelu oli vuoden 2020 ensimmäisellä vuosipuoliskolla kolmanneksi käytetyin yksityisen sektorin sähköinen asiointipalvelu vakuutus- ja terveyspalvelujen jälkeen. Sähköiseen allekirjoitukseen liittyviä tunnistustapahtumia oli kyseisellä ajanjaksolla yli kolme miljoonaa kappaletta.[39]

Voidaan todeta, että sähköinen allekirjoitus on yksi merkittävä vahvan sähköisen tunnistusvälineen käyttökohteista, vaikka edelleen suuri osa suomalaisista ei ollut käyttänyt sitä sähköisten allekirjoitusten tekemiseen. Sähköisen allekirjoittamisen edistämisellä on mahdollisuus edelleen lisätä asioiden hoitamista sähköisesti ja vastaavasti vähentää tarvetta fyysiseen asiointiin julkisen hallinnon, yksityisen sektorin ja kolmannen sektorin toimipisteissä. Sähköisen allekirjoittamisen edistäminen edistää myös vahvan sähköisen tunnistamisen käyttöä, mutta tähän vaikuttaa paljon se, minkä tasoisiin sähköisiin allekirjoituksiin oikeustoimissa eri yhteyksissä luotetaan.

5.2 Yritysten tarpeet

Sähköisten asiointipalvelujen tarpeet asiakkaiden tunnistamisen osalta vaihtelevat riippuen toimialasta ja sähköisen asiointipalvelun sisällöstä. Julkisen sektorin sähköisten asiointipalvelujen ohella asiakkaan vahvaa sähköistä tunnistamista käytetään laajasti yksityisellä sektorilla muun muassa finanssi-, terveydenhuolto- ja vakuutusaloilla. Muita yksityisen sektorin toimijoita, joilla vahva sähköinen tunnistus on nykyisin laajasti käytössä, ovat muun muassa tele-, sähkö- ja kuljetusyritykset sekä monet matkustuspalveluja tarjoavat yritykset. Vahvaa sähköistä tunnistamista käytetään myös sähköiseen allekirjoittamiseen liittyvien palvelujen osana. Edelleen kuitenkin monet yksityisen sektorin toimijat tukeutuvat sähköisissä asiointipalveluissaan asiakkaiden tunnistamisessa rekisteröimättömään tunnistusmenetelmään (heikko tunnistus). Verkkokaupan maksutapahtuman yhteydessä asiakas kuitenkin tunnistetaan pääsääntöisesti vahvasti.[40]

Valtiovarainministeriön syksyllä 2020 teettämällä yrityskyselyllä on pyritty kartoittamaan sähköisen asioinnin sekä sähköisen tunnistamisen nykytilaa ja tarpeita yritysten ja yhteisöjen näkökulmasta. Tutkimuksen sisällön suunnittelivat valtiovarainministeriö, Kilpailu- ja kuluttajavirasto sekä Liikenne- ja viestintävirasto. Tutkimuksen kohderyhmänä olivat Suomessa toimivat yritykset ja se suoritettiin puhelinhaastatteluina, jotka toteutti Taloustutkimus 11.11.-2.12.2020 välisenä aikana. Tiedonkeruussa käytettiin kiintiöintiä, jotta aineistoon saatiin yrityksiä eri kokoluokista ja toimialoilta. Kyselytutkimukseen vastasi kaikkiaan 501 organisaatiota.

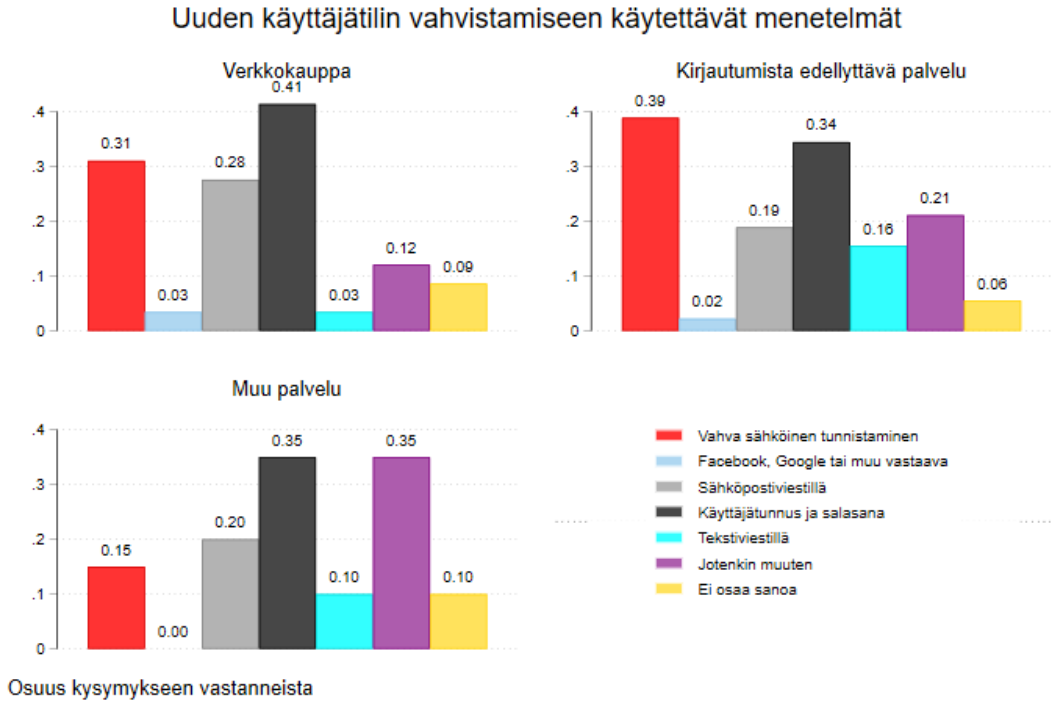
Kyselyyn vastanneista yrityksistä 61 prosentilla ei ole käytössään sähköisiä asiointipalveluja. Alhaisin sähköisten palvelujen käyttöönottoaste on rakennuspalveluja tuottavien organisaatioiden keskuudessa: näistä 86 prosentilla ei ole käytössään kyselyssä tarkoitettuja sähköisiä palveluja. Vaikuttaakin siltä, että osa toimialoista ja yritysten tarjoamista tuotteista ja palveluista on sen tyyppisiä, että sähköiselle asiointipalvelulle ei välttämättä ole suurta tarvetta. Kyselyyn vastanneista yrityksistä verkkokauppa on käytössään 15 prosentilla ja kirjautumista edellyttävä asiointipalvelu 21 prosentilla. Jokin muu digitaalinen palvelu, jonka kautta voi asioida

[39] Tunnistusvälineen tarjoajien sekä tunnistusvälityspalvelujen tarjoajien myynti sähköistä allekirjoitusta tarjoaville asiointipalveluille.

[40] Vahvasta tunnistamisesta maksamisen yhteydessä tarkemmin jaksossa 6.2.

tai ostaa tuotteita tai palveluja löytyy 14 prosentilta vastaajayrityksistä. Joillakin vastaajilla on käytössään näistä vaihtoehdoista samanaikaisesti useampi. Tulosten perusteella sähköisten asiointipalvelujen tarjoamisen todennäköisyys on korkeampaa henkilöstön määrällä ja liikevaihdolla mitattuna suurempien organisaatioiden keskuudessa. Toisaalta on kuitenkin havaittavissa, että koronaepidemian myötä monet pienetkin toimijat ovat katsoneet verkkokaupan perustamisen tarpeelliseksi, minkä myötä sähköinen asiointi on lisääntymässä.

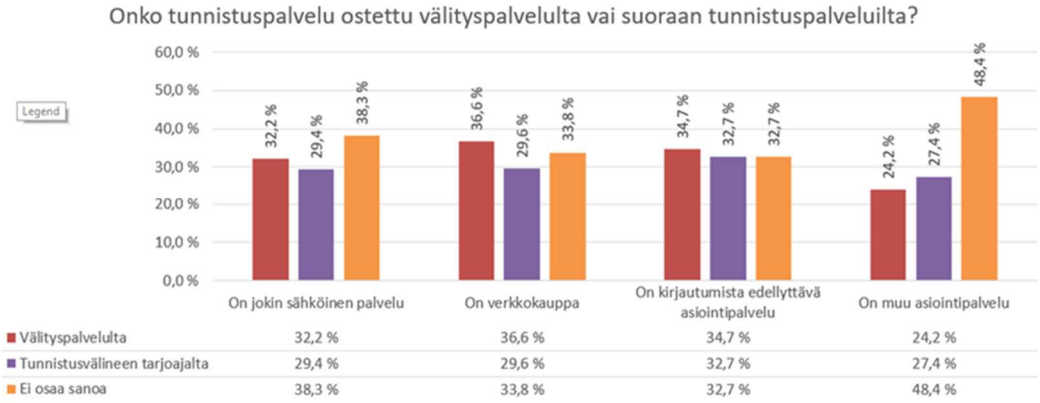
Yrityskyselyllä kartoitettiin myös sitä, millä menetelmillä yritykset ja yhteisöt tunnistavat asiakkaitaan sähköisissä palveluissa. Tavoitteena oli selvittää sekä vahvojen että heikkojen tunnistusmenetelmien käyttöä. Kaikista sähköisiä asiointipalveluja tarjoavista yrityksistä 78 prosenttia ilmoitti varmistavansa asiakkaan henkilöllisyyden tai yksilöivänsä tämän ensimmäisellä käyttökerralla eli käyttäjää rekisteröitäessä. Loppuosa vastaajista ei näin ollen tunnista tai yksilöi asiakkaitaan sähköisissä asiointipalveluissaan. *Verkkokauppatoimijoista* 31 prosenttia ilmoitti käyttävänsä vahvoja tunnistusmenetelmiä (pankkitunniste tai mobiilivarmenne) asiakkaidensa tunnistuksessa. Heikoista tunnistusmenetelmistä verkkokaupoissa ovat laajasti käytössä esimerkiksi sähköpostiin lähetettävä kirjautumislinkki taikka käyttäjätunnukseen ja salasanaan perustuvat kirjautumismenetelmät. Kirjautumista edellyttäviä sähköisiä asiointipalveluja (muu kuin verkkokauppa) tarjoavien toimijoiden osalta asiakkaan vahvaa tunnistusta käyttää 39 prosenttia vastaajista. Vastaavasti kuin verkkokauppojen osalta kirjautumista edellyttävissä sähköisissä asiointipalveluissa on myös laajalti käytössä heikkoja tunnistusmenetelmiä: sähköpostivarmistuksen ja käyttäjätunnus-salasana-yhdistelmien lisäksi melko yleisessä käytössä on myös vahvistuskoodi asiakkaalle tekstiviestillä.



Kuva 7: Uuden käyttäjätilin vahvistamiseen käytettävät tunnistusmenetelmät.

Yrityskyselyllä selvitettiin myös sitä, miten sähköisten asiointipalvelujen tunnistuspalveluhankinnat jakautuvat tunnistusvälityspalvelun tarjoajien ja vahvoilta sähköisiltä tunnistusvälineen tarjoajilta tehtyjen suorien ostojen välillä. Kyselyyn vastanneista sähköisiä asiointi palveluja tarjoavista yrityksistä 32,2 prosenttia kertoi hankkivansa vahvat sähköiset tunnistuspalvelut tunnistusvälityspalvelun tarjoajilta. Vastaavasti 29,4 prosenttia ilmoitti asioivansa suoraan tunnistusvälineen tarjoajien kanssa. Kun asiointipalvelujen vastauksia tarkastellaan segmenteittäin *verkkokauppaa* käyvistä yrityksistä 36,6 prosenttia asioi tunnistusvälityspalvelujen

kanssa ja 29,6 prosenttia kertoi asioivansa tunnistusvälineen tarjoajien kanssa. Kirjautumista edellyttäviä sähköisiä asiointipalveluita tarjoavista yrityksistä välityspalvelun kautta tunnistustapahtumat hankki 34,7 prosenttia ja vastaavasti suoraan välineen tarjoajalta 32,7 prosenttia.



Kuva 8: Sähköisten asiointipalvelujen tunnistuspalveluhankintojen jakautuminen vahvan sähköisen tunnistusvälityspalvelujen ja vahvan sähköisen tunnistusvälineen tarjoajien välillä.

Monet sähköiset asiointipalvelut eivät osanneet sanoa, hankkivatko ne tunnistuspalvelunsa tunnistusvälityspalvelun tarjoajalta vai suoraan tunnistusvälineen tarjoajilta. Kysymykseen vastaamista on saattanut hankaloittaa se, että osa vahvan sähköisen tunnistusvälineen tarjoajista toimii myös välityspalvelun roolissa. Kysymykseen tunnistustapahtumien määrästä vastanneista vahvaa sähköistä tunnistusta sähköisissä asiointipalveluissaan käyttävistä yrityksistä 30 prosenttia ilmoitti tunnistustapahtumiensa määrän jääneen alle viidensadan vuonna 2019. Kyselyyn vastanneiden yritysten raportoimat vahvojen sähköisten tunnistustapahtumien lukumäärät niiden sähköisissä asiointipalveluissa ovat siten olleet verrattain alhaisia.

Yritysten oma sähköinen asiointi

Kyselytutkimuksessa tiedusteltiin myös yritysten oman sähköisen asioinnin toteuttamista suhteessa viranomaisiin – kuten Verohallintoon ja Kelaan – sekä muihin yrityksiin. Vastausten perusteella yrityksillä on tyypillisesti samanaikaisesti useita sähköisen tunnistuksen tapoja ja välineitä rinnakkain käytössään. Peräti 62 prosenttia vastaajayrityksistä hoitaa oman organisaationsa asiointia siten, että sen työntekijä käyttää asioinnissa omia henkilökohtaisia verkkopankkitunnuksiaan. Yrityksen nimissä olevia verkkopankkitunnuksia käytetään 35 prosentissa ja mobiilivarmennetta 37 prosentissa vastaajayrityksistä. Käytöstä poistuva ja monelta osin jo poistunut Katso-tunniste on ollut käytössä 25 prosentilla ja suomi.fi-tunnistus 10 prosentilla vastaajista. Organisaatiovarmennetta ilmoitti käyttävänsä 11 prosenttia yrityksistä.

Erilaisten vahvojen sähköisten tunnistusmenetelmien käytön yleisyydessä ei kyselyn mukaan näyttäisi olevan merkittäviä eroavaisuuksia toimialojen kesken. Vastaavasti henkilöstön suuruusluokkakohtainen tarkastelu ei paljastanut merkittäviä eroavaisuuksia yritysten välillä. Kyselyn otos on kuitenkin suomalaiseen yrityskenttään nähden verrattain pieni ja kattavammat otokset saattaisivat nostaa lähemmässä tarkastelussa esiin joitakin toimialaan tai yrityksen kokoon liittyviä eroja vahvojen sähköisten tunnistusmenetelmien käyttöasteissa.

Tunnistuspalvelujen hinnoittelu ja kustannukset yrityksille

Yrityskyselyyn vastanneista vahvaa sähköistä tunnistamista hyödyntävistä yrityksistä 17 prosenttia kertoi vahvan sähköisen tunnistamisen kustannusten kasvaneen viimeisen vuoden aikana. Valtaosa eli 64 prosenttia vastaajista kertoi kustannusten kuitenkin pysyneen samana. Sähköisten asiointipalvelujen osalta vahvojen sähköisten tunnistuspalvelujen käytöstä koituviin kustannuksiin vaikuttaa muun muassa

toteutuneiden tunnistustapahtumien määrä ja yksittäisestä tunnistustapahtumasta laskutettu tapahtumakohtainen hinta. Palvelujen käytön kasvun ja vastaajien ilmoittamien kustannusten muutosten vertailu antaa viitteitä keskimääräisen tapahtumakohtaisen hinnan alenemisesta kuluneen vuoden aikana. Osa kysymykseen vastanneista yrityksistä ei tarjonnut itse sähköisiä asiointipalveluja: tunnistuspalvelujen kustannuksilla nämä yritykset viittaavat niiden omaan sähköiseen asiointiin hankittujen tunnistusvälineiden kustannuksia. Yrityksen tarvitessa omaan sähköiseen asiointiinsa vahvaa sähköistä tunnistusvälinettä se hankkii käytännössä joko pankkitunnisteet, mobiilivarmenteen ja/tai organisaatiovarmenteen. Kustannus on tällöin kiinteä, mutta maksu yleensä kasvaa yrityksen lisätessä tunnistusvälineen käyttäjien määrää organisaatiossaan. Sen sijaan tapahtumakohtaista lisämaksua ei tässä tilanteessa peritä.

Hinnoittelun osalta 34 prosenttia vastaajista kertoi, että niiden vahvan sähköisen tunnistuspalvelun käyttöön liittyy kiinteä kuukausi- tai vuosimaksu. Tämän kiinteän kuukausi- tai vuosimaksun lisäksi palvelun käytöstä peritään aina myös tapahtumaperusteinen hinta. Tunnistustapahtumamäärän jäädessä alhaiseksi saattaa kiinteä kuukausimaksu nostaa keskimääräistä tapahtumakohtaista kokonaiskustannusta merkittävästi. Kyselyn tulokset näyttävät tältä osin olevan linjassa KKV:n suoraan vahvan sähköisen tunnistusvälineen ja tunnistusvälityspalvelun tarjoajilta saamien selvitysten kanssa: hinnoittelu tyypillisesti muodostuu yhdistelmästä kiinteitä maksuja ja tapahtumakohtaisia maksuja, jolloin lopullisen tapahtumakohtaisen hinnan kokonaismäärä riippuu siitä, mille tasolle tunnistustapahtumien määrä asettuu.

Sähköisten asiointipalvelujen näkemyksiä tulevaisuuden tarpeista

Kyselytutkimuksen yhteydessä yrityksiltä tiedusteltiin myös niiden näkemystä vahvan sähköisen tunnistamisen yhteydessä välittyvien tietojen riittävyydestä heidän tarjoamiensa palvelujen kannalta. Lähes kaikki eli 98 prosenttia näkemyksensä antaneista vastaajista pitää vahvan sähköisen tunnistamisen yhteydessä saatavia tietoja riittävinä. Nykyisellään vahvan sähköisen tunnistamisen yhteydessä välitettävän tiedon lisäksi joissakin vastauksissa toivottiin tietoa tunnistautuvan henkilön täysi-ikäisyydestä sekä tietoa tunnistautuvan henkilön äidinkielestä. Toisaalta neljä prosenttia kysymykseen vastanneista kertoi jättäneensä jonkin osan digitaalista palveluaan toteuttamatta vahvan sähköisen tunnistuksen yhteydessä välitettävän tiedon niukkuuden takia. Vastauksien välinen epäjohdonmukaisuus indikoi kysymysten tai asiakokonaisuuksien vaikeaselkoisuudesta.

Vahvan sähköisen tunnistamisen lisäksi vastaajilta kysyttiin tarvetta erilliselle lupalompakolle ja laajennetulle sähköiselle valtuuttamiselle. 18 prosenttia kysymykseen vastanneista indikoi tarvetta erilliselle vahvalle sähköiselle tunnistusvälineelle, jolla työntekijöiden olisi mahdollista tunnistautua yrityksen nimissä verkkopalveluihin. Erityisesti tarve erilliselle vahvalle sähköiselle tunnistusvälineelle näkyi henkilömäärältään ja liikevaihdoltaan suurempien yritysten keskuudessa.

Niin kutsuttujen lupalompakoiden käyttö on vielä alhaista. Nykyisellään vain yhdellä prosentilla vastanneista yrityksistä on käytössään lupalompakko, kun taas esimerkiksi työtekijöiden sähköinen valtuuttaminen on käytössä 60 prosentilla vastaajista ja sähköinen allekirjoitus 30 prosentilla vastaajista. 16 prosenttia vastaajista piti kuitenkin lupalompakkoa tarpeellisena edustamallensa organisaatiolle.

Koronaepidemia - poikkeusajan vaikutukset palvelujen käyttämisessä

Tutkimuksen perusteella iso osa yrityskenttää kokee koronaepidemian lisänneen sähköisten asiointipalvelujen käyttöä: vastaajista 42 prosenttia ilmoittaa käyttäjämäärien kasvaneen epidemian seurauksena. Toisaalta 48 prosenttia kyselyyn vastanneista organisaatioista ei ole kokenut epidemian lisänneen sähköisten asiointipalvelujen käyttöä. Yhdeksän prosenttia vastanneista jopa kertoo sähköisten asiointipalvelujen käyttäjämäärien laskeneen epidemian seurauksena. Vastausten

perusteella ei kuitenkaan voida varmuudella todeta, kuinka suuri osa havaituista käyttäjämäärien muutoksista johtuu tavallisesta satunnais- ja kausivaihtelusta. Epidemian seurauksena käyttäjämäärien kasvua havainneet yritykset raportoivat epidemian kasvattaneen kävijämääriä keskimäärin 41 prosentilla. Suurinta sähköisten asiointipalvelujen käytön kasvu oli kaupan alalla, kyselyyn saatujen vastausten osalta peräti 91 prosenttia. Kaupan alalla sähköisten asiointipalvelujen kasvun taustalla näkyy ruoan ja muiden tuotteiden verkkomyynnin merkittävä lisääntyminen. Palvelualoilla sähköisten asiointipalvelujen kasvua voi selittää muun muassa kasvu ravintoloiden ulosmyynnissä, mikä usein toteutuu sähköisten alustojen kautta.

Sähköisiä asiointipalveluja tarjonneista yrityksistä 14 prosenttia ilmoitti nostaneensa sähköisen asiointipalvelunsa kapasiteettia tartuntaepidemian seurauksena. Samoin 14 prosenttia kertoi parantaneensa sähköisen asiointipalvelun toimivuutta ja 20 prosenttia kasvattaneensa etätyöskentelyn ja muiden etänä tapahtuvien toimenpiteiden osuutta. Kysymykseen vastanneista yrityksistä 47 prosenttia ei sen sijaan ole tehnyt muutoksia toimintatapoihinsa epidemian seurauksena.

Yrityskyselyn tulokset ja johtopäätökset

Yrityksille suunnatun kyselytutkimuksen perusteella vahvan sähköisen tunnistamisen markkina näyttäisi toimivan: vahvan sähköisen tunnistusvälineen tarjoajien ja pelkästään vahvan sähköisen tunnistusvälityspalvelun tarjoajien mahdollisuus välittää toisten vahvan sähköisen tunnistusvälineen tarjoajien tunnistustapahtumia on lisännyt kilpailua markkinoilla. Tunnistustapahtumista sähköisiltä asiointipalveluilta perittävät tapahtumakohtaiset hinnat ovat laskeneet tukkumarkkinoiden hintasääntelyn myötä. Sähköisten asiointipalvelujen tunnistustapahtumien hinnoittelun perustuessa tyypillisesti kaksiosaiseen hinnoittelumalliin (kiinteä kuukusimaksu ja tapahtumakohtainen maksu) keskimääräinen tapahtumakohtainen tunnistuspalvelun ostajan maksama hinta saattaa muodostua korkeaksi kiinteän kuukausimaksun kohdentuessa pieneen tunnistustapahtumien lukumäärään. Kokonaiskustannukset ovat kuitenkin keskimäärin maltillisia.

Vahvan sähköisen tunnistamisen yhteydessä välitettävissä tiedoissa haastatellut yritykset eivät havainneet suuria puutteita. Lähes kaikki kysymykseen vastanneista yrityksistä piti vahvan sähköisen tunnistamisen yhteydessä välitettäviä tietoja riittävinä.

Yrityskyselyllä pyrittiin kartoittamaan myös organisaation puolesta asioimiseen liittyviä tarpeita ja halukkuutta yksityishenkilöön liittyvien erilaisten lupa-asiakirjojen keskittämiseen jonkinlaisen lupalompakkosovelluksen alle. Kyselyyn vastanneista 18 prosenttia kannatti ajatusta erillisestä organisaation puolesta asioinnin mahdollistavasta vahvasta sähköisestä tunnistusvälineestä. Lupalompakkoa tarpeellisena piti 16 prosenttia vastanneista. Vastauksien tulkinta ei ole kuitenkaan yksiselitteistä. Organisaation puolesta asioiminen sähköisesti on jo mahdollista. Vastaavasti markkinoilla toimii jo lupalompakko-sovellusta kehittäviä ja tarjoavia yrityksiä. Kyselytutkimuksella saaduista vastauksista ei käy suoraan ilmi sitä, miksi olemassa olevat ratkaisut koetaan puutteellisina, vaan sitä tulisi selvittää esimerkiksi erillisillä kohdennetuilla haastatteluilla.

5.3 Julkisen sektorin tarpeet

Valtiovarainministeriön asettaman Digitaalinen henkilöllisyyden kehittäminen -hankkeen asettamiskirjeessä listataan hankkeelle seuraavat tavoitteet, joiden voidaan myös katsoa kuvastavan julkisen sektorin tarpeita tunnistuspalveluille ja laajemmin henkilöä koskevien tietojen käsittelyn mahdollistamiselle:

- *tuottaa yhdenvertaiset edellytykset ja mahdollisuudet jokaiselle hyödyntää digitaalista henkilöllisyyttä yhteiskunnan palveluissa ja luoda mahdollisuuksia laajentaa viranomaisen vahvistamien henkilötietojen joukkoa, joka asioinnissa voidaan välittää toiselle osapuolelle.*

- *varmistaa edellytykset yksilökeskeisesti ihmiseen itseensä liittyvien henkilötietojen jakamisen (Self Sovereign Identity) syntymiselle ja kehitykselle tulevaisuudessa siten, että digitaalisen henkilöllisyyden ratkaisujen perustana voisi toimia valtion takaama ydinidentiteetti*

- *mahdollistaa jokaiselle tarvitsevalle tunnistautuminen julkishallinnon palveluihin sähköisesti myös työtehtävien hoitamista varten*

- *varmistaa julkisen hallinnon vahvan sähköisen tunnistamisen kustannusten hallittavuus ja ennakoitavuus sekä*

- *tuottaa edellytykset ulkomaalaisen henkilön rekisteröinnille ja sähköiselle tunnistautumiselle Suomeen ja mahdollistaa Suomesta rajat ylittävä sähköinen tunnistaminen Euroopan parlamentin ja neuvoston sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista annetun asetuksen (EU) N:o 910/2014 mukaisesti huomioiden Euroopan Unionin regulaatioon kohdistuvat muutokset.*

Pääosin edellä esitetyt tavoitteet liittyvät väestötietojärjestelmän kehittämiseen ja sen tietojen hyödyntämiseen entistä tehokkaammin sekä fyysiseen tunnistamiseen ja sähköiseen ensitunnistamiseen ja niissä käytettäviin passin ja henkilökortin kuin myös toisella vahvalla sähköisellä tunnistusvälineellä tehtävän sähköisen ensitunnistamisen korvaaviin sähköisiin menetelmiin.

Suoraan tunnistuspalveluja koskevina tavoitteina on käytännössä mahdollistaa kaikille suomalaisille, Suomessa asuville ja Suomeen asumaan, opiskelemaan tai työskentelemään pyrkiville mahdollisuus tunnistautua asiointipalveluihin eli saada käyttöönsä vahva sähköinen tunnistusväline tai sitä vastaava tunnistusväline. Kuten edellä on todettu, Suomessa on noin 1,6 miljoonan henkilön joukko, joihin kuuluvilla henkilöryhmillä jokaisella on vähän erilaisensa haaste ja ongelma käyttää tunnistuspalveluja tai yleensäkin tietoteknisiä laitteita ja sähköisiä asiointipalveluja. Tavoitteena voidaankin katsoa olevan löytää jokaiselle tähän joukkoon kuuluvalle henkilöryhmälle oikeanlainen ratkaisu ratkaista ne ongelmat, joita he kokevat jokapäiväisessä tietoteknisten laitteiden, sähköisten asiointipalvelujen että vahvojen sähköisten tunnistusvälineiden käyttöönottamisessa ja käyttämisessä.

Lisäksi tavoitteena on mahdollistaa se, että käytettävällä (vahvalla sähköisellä) tunnistusvälineellä on mahdollisuus tunnistautua myös muiden EU-jäsenmaiden julkisen hallinnon sähköisiin asiointipalveluihin. Valtiovarainministeriön kyselytutkimuksen mukaan vain 4 prosentilla oli tarve tunnistautua, ja 2 prosenttia vastanneista oli tunnistautunut muiden EU-maiden julkinen hallintojen sähköisiin asiointipalveluihin, mutta voidaan kuitenkin katsoa, että tarve rajat ylittävälle tunnistamiselle tulee tulevaisuudessa kasvamaan ja osaltaan rajat ylittävä tunnistaminen omalla käytössä olevalla tunnistusvälineellä lisää merkittävästi kansalaisten mahdollisuuksia asioida myös muiden viranomaisten kanssa. Myös EU-sääntely osaltaan ohjaa voimakkaasti tämän mahdollistamiseen.

Tavoitteena on myös hillitä vahvasta sähköisen tunnistamisesta julkisen hallinnon sähköisiin asiointipalveluihin julkiselle hallinnolle koituvia kustannuksia, jotka ovat kasvaneet siitä johtuen, että julkisen hallinnon tarjoaminen sähköisten asiointipalvelujen käyttö ja sitä myöden myös vahvan sähköisen tunnistamisen käyttö näissä sähköisissä asiointipalveluissa on kasvanut nopeasti ja nopeammin kuin vahvan sähköisen tunnistuspalvelun tarjoajien tunnnistustapahtumista perimät yksikköhinnat ovat alentuneet. Julkisen hallinnon vahvojen sähköisten tunnistuspalvelujen kustannukset ovat kasvaneet kasvaneen käytön vuoksi, vaikka tunnistuspalveluista

maksetut hinnat ovat samaan aikaan laskeneet. Vastavuoroisesti voitaisiin olettaa, että julkisen hallinnon tarjoaman sähköisen asiointipalvelun kokonaiskustannukset olisivat laskeneet, kun entistä suurempi osa niiden asiakkaista on siirtynyt hoitamaan asiansa sähköisten asiointipalvelujen kautta fyysisen asioinnin sijasta joko kokonaan tai osittain. On myös todennäköistä, että myös julkisen hallinnon sähköisiä asiointipalveluja käyttävät asiakkaat ovat hyötyneet muun muassa taloudellisesti siitä, että ne ovat voineet hoitaa asioitaan sähköisesti käyntiasioinnin sijaan.

Edellä esitetyt tavoitteet on mahdollista ratkaista hyvin moninaisin keinoin ja toimenpitein ja yhteiskunnan kannalta on tärkeintä, että esitetyt tavoitteet saavutetaan ja niihin liittyvät haasteet ratkaistaan yhteiskunnan näkökulmasta mahdollisimman kustannustehokkaasti.

6 Vahvan sähköisen tunnistamisen markkina

Tässä luvussa tarkastellaan vahvan sähköisen tunnistamispalvelujen kysyntää ja tarjontaa, markkinoilla toimivien toimijoiden markkinavoimaa, markkinoiden sääntelyä ja sen toimivuutta kuin myös hintatasoa. Luvussa tarkastellaan myös ensitunnistamista vahvan sähköisen tunnistusvälineen hakemisessa ja siihen liittyvää sääntelyä omana kokonaisuutenaan.

6.1 Vahvan sähköinen tunnistamisen kysyntä tunnistusvälineen käyttäjien näkökulmasta

Käyttäjille on tällä hetkellä tarjolla kolmenlaisia vahvoja sähköisiä tunnistusvälineitä:

- pankkien tarjoamat verkkopankkitunnisteet,
- matkaviestinverkkoyritysten tarjoamat mobiilivarmenteet ja
- Digi- ja väestötietoviraston tarjoamat henkilö- ja organisaatiovarmenteet.

Pankkien tarjoamien verkkopankkitunnuksien käyttämiseen käyttäjä tarvitsee normaalisti käyttäjätunnuksen, salasanan ja tunnuslukulistan/-laitteen tai käyttäjätunnuksen ja matkaviestinlaitteeseen, vähintään älypuhelimeen asennettavan tunnuslukusovelluksen. Pankkien tarjoamien verkkopankkitunnusten todentamistekijät poikkeavat jossain määrin toisistaan ja kehittyvät jatkuvasti.

Matkaviestinverkkoyritysten tarjoamien mobiilivarmenteiden käyttämiseen käyttäjä tarvitsee matkapuhelinliittymän (SIM-kortti), liittymänsä puhelinnumeron käyttäjätunnukseksi ja salasanan. Mobiilivarmenne toimii myös muissa kuin älypuhelimissa toisin kuin verkkopankkitunnisteet. Matkaviestinverkkoyritysten tarjoamat mobiilivarmenteet on toteutettu hyvin samalla tavoin ja niissä on käytössä käytännössä samat todentamistekijät ja -mekanismit. Matkaviestinverkkoyritykset myös kehittävät yhdessä mobiilivarmenteitaan, jolloin on odotettavaa, että myös jatkossa niiden toteutus ei poikkea merkittävästi toisistaan.

Digi- ja väestötietoviraston tarjoamien henkilö- ja organisaatiovarmenteiden käyttämiseen käyttäjä tarvitsee henkilö- tai organisaatiokortin, jossa henkilö- tai organisaatiovarmenne on aktivoitu, kortinlukulaitteen, salasanan ja ilmaiseksi tietotekniselle laitteelle ladattavan ohjelmiston. Henkilö- ja organisaatiovarmenne vaativat aina erillistä kortinlukulaitetta eikä niitä ole tällä hetkellä mahdollista käyttää esimerkiksi älypuhelimen avulla.

Verkkopankkitunnisteet ovat sidottuja pankkien tiliasiakkuuteen ja ilman asiakkuutta käyttäjällä ei ole mahdollisuutta saada verkkopankkitunnistetta käyttöönsä. Vastaavasti mobiilivarmenne on sidottu matkaviestinliittymäasiakkuuteen ja ilman asiakkuutta käyttäjällä ei ole mahdollisuutta saada mobiilivarmennetta käyttöönsä.[41] Myös henkilö- ja organisaatiovarmenteet ovat sidottuja tunnistuspalvelun ulkopuoliseen asiakkuuteen ja ilman näitä asiakkuuksia ei käyttäjällä ole mahdollisuutta saada käyttöönsä henkilö- tai organisaatiovarmennetta. Kansalaisvarmenteen saadakseen käyttäjä tarvitsee poliisin myöntämän henkilökortin (poliisi ylläpitää rekisteriä henkilön henkilöllisyyden osoittavista tiedoista, joita käytetään muun muassa henkilökortin myöntämisessä ja voimassa olon valvomisessa) ja organisaatiovarmenteen saadakseen käyttäjä tarvitsee organisaatiokortin ja työ- tai virkasuhteen työnantajaan.

Tällä hetkellä tarjolla olevat vahvat sähköiset tunnistusvälineet ovat siis sidottuja toisen palvelun käyttämiseksi tarvittavaan asiakkuuteen, eikä markkinalla ole tarjolla vahvaa sähköistä tunnistuspalvelua, jossa asiakas voisi ottaa käyttöönsä ja

[41] Mobiilivarmennetta ei ole mahdollista saada käyttöön prepaid-liittymissä.

tehdä sopimuksen palvelun tarjoajan kanssa pelkästään vahvasta sähköisestä tunnistusvälineestä. Markkinalla ei siten ole vain vahvaa sähköistä tunnistusvälinettä tarjoavaa palvelun tarjoajaa.

Maailmanpankin The Global Findex:in mukaan vuonna 2017 99,8 prosentilla yli 15-vuotiaasta suomalaisesta oli käytössään pankkitili.[42] Monelta osin tämä johtunee siitä, ettei Suomessa palkkaa, palkkioita tai etuutta makseta käteisenä ja näiden maksamiseen maksun kohde tarvitsee pankkitilin. Valtiovarainministeriön teettämän kyselytutkimuksen mukaan vuonna 2020 noin 98 prosentilla oli käytössään verkkopankkitunnukset. Tilastokeskuksen Väestön tieto- ja viestintätekniikan käyttö -tutkimus 2020 mukaan vuonna 2020 verkkopankkia viimeisen kolmen kuukauden aikana oli käyttänyt noin 87 prosenttia vastanneista.[43] Näiden lukujen perusteella voidaan todeta, että käytännössä kaikilla yli 15-vuotiailla suomalaisilla on pankkitili ja mahdollisuus sitä kautta ottaa käyttöönsä verkkopankkitunnukset ja suurimmalta osin suomalaiset ovatkin ottaneet verkkopankkitunnukset käyttöönsä ja käyttävät niitä.

Liikenne- ja viestintäviraston Viestintäpalvelujen käyttö -tutkimuksen mukaan vuonna 2020 hieman yli 99 prosentilla vastanneista oli käytössään matkapuhelinliittymä. Valtiovarainministeriön teettämän kyselytutkimuksen mukaan vuonna 2020 noin 22 prosentilla oli käytössään mobiilivarmenne ja 8 prosenttia oli kiinnostunut hankkimaan sen nykyisen tunnistusvälineen rinnalle. Näiden lukujen perusteella voidaan todeta, että lähes kaikilla suomalaisilla on käytössään matkapuhelinliittymä ja siten mahdollisuus ottaa käyttöönsä mobiilivarmenne. Mobiilivarmenteen tarjoajilla on valmis asiakassuhde potentiaalisiin mobiilivarmenteen käyttäjiin ja potentiaalisten käyttäjien määrä on todella suuri. Merkittävä määrä käyttäjistä on myös kiinnostunut hankkimaan mobiilivarmenteen nykyisen tunnistusvälineen rinnalle, vaikka määrä voisi olla tätä merkittävästi suurempikin huomioiden uusien potentiaalisten käyttäjien suuren määrän. Osa matkaviestinverkkoyrityksistä tarjoaa mobiilivarmennetta kuluttaja-asiakkailleen veloituksetta, toisilla palvelusta veloitetaan tietty kuukausimaksu. On todennäköistä, että kynnys ottaa mobiilivarmenne käyttöön on matalampi tilanteessa, jossa palvelu tarjotaan veloituksetta matkapuhelinliittymän kylkiäisenä.

Poliisihallituksen tilastojen mukaan vuoden 2021 alkupuolella voimassa oli noin 1,3 miljoonaa henkilökorttia. Valtiovarainministeriön teettämän kyselytutkimuksen mukaan vuonna 2020 kansalaisvarmenne oli noin 6 prosentilla suomalaisista käytössä ja 3 prosenttia oli kiinnostunut hankkimaan sen nykyisen tunnistusvälineen rinnalle. Näiden lukujen perusteella voidaan todeta, että merkittävällä osalla suomalaisista on käytössään henkilökortti ja siten mahdollisuus ottaa käyttöönsä kansalaisvarmenne. Potentiaalisten kansalaisvarmenteen käyttäjien määrä on suuri. Jossain määrin käyttäjät ovat myös kiinnostunut hankkimaan kansalaisvarmenteen nykyisen tunnistusvälineen rinnalle, vaikka määrä voisi olla tätä merkittävästi suurempikin huomioiden uusien potentiaalisten käyttäjien suuren määrän.

Valtiovarainministeriön teettämän kyselytutkimuksen mukaan suurin osa kansalaisista käyttäisi ensi sijaisesti vahvaa sähköistä tunnistusta tunnistautumisessa (88 %), jos sähköisen asiointipalvelun tarjoaja olisi mahdollistanut sen käyttämisen palveluunsa kirjautumisessa. Käyttäjien näkökulmasta vahvoille sähköisille tunnistusvälineille ja niiden käyttämiselle on siis suuri kysyntä. Markkinoiden kannalta tällä hetkellä haaste on enemmän tarjonnassa eli kansalaisille ei ole tarjolla mahdollisuuksia hyödyntää käytössään olevia vahvoja sähköisiä tunnistusvälineitä siinä määrin kuin he haluaisivat. On todennäköistä, että vahvojen sähköisten tunnistusvälineiden käyttö kasvaisi, jos entistä suuremmassa osassa sähköisistä asiointipalveluista olisi käyttäjille tarjolla mahdollisuus tunnistautua vahvalla sähköisellä tunnistusvälineellä. On myös todennäköistä, että vahvan sähköisen tunnistusvälineen

[42] https://globalfindex.worldbank.org/node
[43] http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tie_001_fi.html

käyttö lisäisi käyttäjien mielenkiintoa vertailla ja kilpailuttaa eri tunnistusvälineitä ja niiden tarjoajia.

6.1.1 Tunnistuspalvelun hinnoittelu ja vaihtaminen käyttäjän näkökulmasta

Käyttäjiltä tunnistuspalvelujen käyttämisestä perittävät maksut vaihtelevat tunnistusvälineen tarjoajittain. Osa tunnistuspalvelun tarjoajista ei peri käyttäjiltä tunnistuspalvelujen käyttämisestä maksua lainkaan (esim. Telian mobiilivarmenne ja Digi- ja väestötietoviraston kansalaisvarmenne[44]), osa perii maksun osana muita maksuja (esim. verkkopankkitunnisteiden käytöstä voidaan periä maksu osana pankkitilin hoitomaksua) ja osa perii maksun selkeästi erillään muista maksuista (esim. DNA:n ja Elisan mobiilivarmenteet). Jos tunnistuspalvelun tarjoaja perii maksua käyttäjältä, peritään käytöstä normaalisti ainoastaan kuukausimaksua ja maksu on yleensä muutaman euron suuruinen. Maksut ovat riippumattomia tunnistuspalvelun käyttömääristä. Elisa ja DNA perivät kuukausimaksujen lisäksi avausmaksun niiden tarjoamien mobiilivarmenteiden käyttöönottamisesta.

Kuukausimaksujen ja mahdollisten avausmaksujen lisäksi käyttäjät joutuvat joissain tapauksissa hankkimaan erikseen muita palveluja tai ostamaan laitteita tunnistusvälinettä käyttääkseen. Näitä kustannuksia muassa syntyy henkilö-/organisaatiokortin ja kortinlukulaitteen hankkimisesta käytettäessä henkilö- tai organisaatiovarmennetta, matkaviestinliittymän tai pankkitilin hankkimisesta (liittymän tai tilin avausmaksut) käytettäessä mobiilivarmennetta tai verkkopankkitunnistetta kuin myös mahdollisen tietokoneen, puhelimen tai tabletin hankkimisesta käytettäessä mitä tahansa edellä mainituista tunnistusvälineistä. Ottaen huomioon, että suurimmalla osalla suomalaisista on jo käytössään matkaviestinlaite, tabletti ja/tai tietokone, käyttäjälle selkeästi kalleimmaksi tulee kansalaisvarmenteen käyttöönottaminen. Nämä kustannukset osaltaan ohjaavat käyttäjiä tunnistuspalvelun valinnassa, vaikkei kyse ole suurista euromääristä.

Käyttäjien mahdollisuutta kilpailuttaa tunnistusvälineitä rajoittaa se, että nykyiset tunnistusvälineet ovat kaikki liitettyinä johonkin toiseen palveluun, jolloin kilpailuttamisen seurauksena käyttäjän tulisi vaihtaa myös tämän toisen palvelun tarjoaja vahvan tunnistusvälineen tarjoajan lisäksi. Käyttäjien mahdollisuutta kilpailuttaa tunnistusvälineitä rajoittaa myös merkittävästi se, ettei verkkopankkien ja verkkoostosten tekemiseen tarvittavassa tunnistamisessa ole mahdollisuutta käyttää kuin käyttäjän oman pankin myöntämää verkkopankkitunnusta.[45] Hinnoittelu tulee käyttäjille monelta osin annettuna eikä käyttäjillä ole juurikaan mahdollisuutta kilpailuttaa tunnistuspalveluja. Toisaalta tunnistuspalveluista käyttäjiltä perittävät maksut ovat olleet ja ovat tällä hetkellä kohtuulliset ja sen verran alhaiset, etteivät käyttäjät välttämättä koe suurta tarvetta kilpailuttaa palvelujen tarjoajia hinnan suhteen. Käyttäjillä voisi kuitenkin olla jatkossa tarvetta kilpailuttaa tunnistuspalveluja muiden ominaisuuksien suhteen (esim. käytettävyys), jos vahva sähköinen tunnistaminen olisi nykyistä laaja-alaisemmin käytössä erilaisissa sähköisissä asiointipalveluissa.

6.1.2 Kilpailu tunnistusvälineen käyttäjistä

Tällä hetkellä pääasiassa matkaviestinverkkoyritykset markkinoivat ja myyvät aktiivisesti mobiilivarmennetta käyttäjille. Usein kuitenkin markkinointi tapahtuu matkaviestinliittymän myynnin yhteydessä tai markkinointia tehdään yhdessä markkinoiden mobiilivarmennetta yleisesti esimerkiksi mobiilivarmenne.fi -sivuston

[44] Digi- ja väestötietoviraton kansalaisvarmenteesta käytännössä peritään maksu siinä yhteydessä, kun henkilö hankkii henkilökortin kansalaisvarmennetta käyttääkseen.

[45] Maksukortilla verkko-ostoksia maksettaessa tunnistusvaatimuksista säädetään maksupalvelusääntelyssä. Maksukortit eivät myöskään ole välttämättä sidottuja pankin tiliasiakkuuteen eli maksukortti on mahdollista saada ilman pankin tiliasiakkuuttakin. Pankkitililtä maksettaessa tarvitaan kuitenkin aina tunnistautumista kyseisen pankin verkkopankkiin käyttäen pankin verkkopankkitunnuksia.

kautta. Verkkopankkitunnuksia pankit tarjoavat lähinnä pankkipalveluja markkinoidessaan ja tarjotessaan ja ne ovat yleensä sivuroolissa. Verkkopankkitunnuksia ei markkinoida tai tarjota käyttäjille erillään pankkipalveluista. Myöskään henkilö- ja organisaatiovarmennetta ei markkinoida ja myydä aktiivisesti käyttäjille, vaan niistä vain mainitaan käyttäjille esimerkiksi henkilökorttia hankittaessa.

Markkinoilla ei ole havaittavissa selkeää kilpailua käyttäjistä tunnistusvälineen tarjoajien kesken siten, että käyttäjiä yritettäisiin saada oman tunnistusvälineen käyttäjäksi. Enemmän markkinoilla on näkyvissä tunnistusvälineiden ja -tekniikoiden välistä kilpailua, missä mobiilivarmenteita tarjoavat matkaviestinyritykset pyrkivät markkinoimaan mobiilivarmennetta vaihtoehtona pankkien tarjoamille verkkopankkitunnuksille. Markkinoilla ei ole myöskään selkeästi nähtävissä olevaa hintakilpailua tunnistuspalvelujen tarjoajien kesken.

Monelta osin nämä edellä mainitut asiat johtuvat siitä, ettei tunnistuspalvelujen tarjoaminen ole tunnistusvälineen tarjoajien pääasiallinen palvelu, jota ne tarjoavat, vaan se on poikkeuksetta lisäpalvelu. Siten myös markkinointi ja myynti kohdistuvat ensisijaisesti pääasiallisten palvelujen markkinointiin ja myyntiin, joiden rinnalla markkinoidaan ja myydään tunnistuspalveluja. Markkinalla ei ole toimijaa, joka ensisijaisesti markkinoisi ja myisi käyttäjille ja myös sähköisille asiointipalveluille tunnistusvälinettään pääasiallisena palvelunaan.[46]

Tunnistusvälineiden tarjoajien mahdollisuutta kilpailla käyttäjistä myös rajoittaa se, ettei verkkopankkien ja verkko-ostosten tekemiseen tarvittavassa tunnistamisessa ole lähtökohtaisesti mahdollisuutta käyttää kuin käyttäjän oman pankin myöntämää verkkopankkitunnusta ja etteivät kaikki tunnistusvälineen tarjoajat siten voi tarjota tunnistusvälinettä, jota olisi mahdollista käyttää asiointipalveluissa, joihin käyttäjät tunnistautuvat kaikkein eniten. Osin nämä rajoitukset voivat johtua erilaisista verkkopankkien ja verkkomaksujärjestelmien teknisistä toteutustavoista, jolloin muiden kuin pankin omien tarjoaminen vahvojen sähköisten tunnistusvälineiden käyttäminen ei ole mahdollista ilman järjestelmämuutoksia.[47] Myös pankkitoimintaa koskeva lainsäädäntö muun muassa asiakkaan tuntemista koskevien velvoitteiden kannalta voi rajoittaa muiden kuin pankin oman vahvan sähköisen tunnistuksen käyttämistä näissä pankin omissa palveluissa.[48] Toisaalta osin pankkien tarjoamissa sähköisissä asiointipalveluissa tunnistautumisessa voi jo käyttää myös mobiilivarmennetta, jolloin muutos ei välttämättä olisi suuri, ainakaan kaikilla pankeilla.

6.1.3 Saatavuus

Vahvaa sähköistä tunnistamista koskevassa lainsäädännössä ei ole säädetty erikseen velvoitetta tarjota vahvaa sähköistä tunnistusvälinettä käyttäjille samalla tavoin kuin esimerkiksi telesääntelyssä säädetään internetyhteyden tarjontavelvoitteista eli niin sanotuista yleispalveluvelvoitteista.[49] Luottolaitostoiminnasta annetun lain (610/2014) mukaan kuitenkin maksupalveluita tarjoavan talletuspankin on tarjottava euromääräistä perusmaksutiliä mukaan lukien siihen liittyviä maksupalve-

[46] Jossain määrin voitaisiin katsoa, että Digi- ja väestötietovirato markkinoisi ja myisi kansalaisvarmennetta pääasiallisena palveluna, mutta kun asiaa tarkastellaan näkökulmasta, jossa valtiohallinto on palvelun tarjoa, voidaan katsoa, että pääasiallinen markkinoitu ja myyty tuote on henkilökortti.

[47] Verkkopankkipalvelujen ja verkkomaksupalvelujen tunnistusratkaisuissa käytetään pääasiassa yleisesti standardoituja ratkaisuja ja teknisiä rajapintoja, kuten SAML- ja OpenID-rajapintoja, jotka ovat yleisesti käytössä myös vahvan sähköisen tunnistuspalvelujen järjestelmissä. Tämä helpottaa muiden kuin pankin oman vahvan sähköisen tunnistuspalvelun liittämistä verkkopankkiin ja verkkomaksujärjestelmiin.

[48] Laki rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017) ja Laki eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä (659/1967) asetettavat pankeille erinäisiä velvoitteita muun muassa tuntea asiakkaansa.

[49] Liikenne- ja viestintävirasto on nimennyt DNA Oy:n, Elisa Oyj:n ja TeliaSonera Finland Oyj:n sähköisen viestinnän palveluista annetun lain (917/2014) 87 §:ssä säädetyn yleispalveluun kuuluvan internetyhteyden tarjontaan velvollisiksi yleispalveluyrityksiksi. Kullekin yritykselle on nimetty erilliset postinumeroalueet, joilla ne ovat velvollisia toimimaan yleispalveluyrityksenä.

luita ja sähköisen tunnistamisen palveluita Euroopan talousalueella laillisesti asuville asiakkaille.[50] Tässä sähköisen tunnistamisen palveluilla tarkoitetaan käytännössä verkkopankkitunnuksien tarjoamista pankin asiakkaille.

Voidaan todeta, lähtökohtaisesti kaikilla Suomessa asuvilla on mahdollisuus saada käyttöönsä vahva sähköinen tunnistusväline pois lukien Euroopan talousalueella laittomasti asuvat henkilöt sekä henkilöt, joiden mahdollisuus saada perusmaksutili ja sitä kautta vahva sähköinen tunnistusväline evätään asiakkaan tunnistamiseen liittyvien esteiden tai rahanpesuun tai terrorismin rahoittamiseen liittyvien seikkojen nojalla[51]. Näyttäisikin siltä, etteivät kaikki Suomessa asuvat ole hankkineet ja saaneet käyttöönsä perusmaksutiliä ja sitä kautta vahvaa sähköistä tunnistusvälinettä, vaikka heillä on tähän lainsäädännön tuoma mahdollisuus. Tätä osaltaan tukee myös valtiovarainministeriön kyselytutkimukseen saadut vastaukset.

Voidaan myös todeta, että velvoitteesta tarjota vahvaa sähköistä tunnistusvälinettä säädetään epäsuorasti ja säädökset koskevat vain osaa tunnistuspalvelujen tarjoajia eli pankkeja. Velvollisuus tarjota vahvaa sähköistä tunnistusvälinettä on myös sidottu perusmaksutilin tarjoamiseen eikä vahvaa sähköistä tunnistusvälinettä ole velvoitetta tarjota ja mahdollista saada ilman perusmaksutilin avaamista. Tämä epäsuora velvoite tarjota vahvaa sähköistä tunnistusvälinettä omalta osaltaan ohjaa käyttäjiä käyttämään verkkopankkitunnisteita.

6.1.4 Saavutettavuus ja esteettömyys

Vahvan sähköisen tunnistuspalvelun saavutettavuudesta ja esteettömyydestä ei ole suoraan ja kattavasti säädetty lainsäädännössä. Vahvan sähköisen tunnistuspalvelun saavutettavuuteen kohdistuu kuitenkin epäsuoria, tunnistuspalveluja sivuavia vaatimuksia, joista säädetään laissa digitaalisten palvelujen tarjoamisesta (306/2019). Kyseisessä laissa säädetään mobiilisovellusten ja verkkosivujen saavutettavuudesta julkisen hallinnon sähköisissä palveluissa. Säädös kohdistuu ennen kaikkea julkisen hallinnon toimijaan ja sen tarjoamiin mobiilisovelluksiin ja verkkosivuihin näiden toteuttajana. Saavutettavuusvelvoitteet koskevat lain mukaan myös vahvoja sähköisiä tunnistuspalveluja, mutta itse tunnistusväline ei kuitenkaan kuulu kyseessä olevan lain soveltamisalaan. [52]

Valtiovarainministeriön teettämän kyselytutkimuksen ja erityisryhmille teetetyn kyselyn perusteella nykyiset vahvat sähköiset tunnistusvälineet eivät ole kaikilta osin saavutettavia ja esteettömiä. Pääosin esille tulleet saavutettavuus- ja esteettömyyshaasteet ovat ratkaistavissa kehittämällä vahvoja sähköisiä tunnistusvälineitä huomioimalla entistä paremmin erityisryhmien tarpeet niille. Huomiota tulisi kiinnittää erityisesti siihen, että tunnistusvälineiden käyttöohjeet ja tunnistustapahtumassa annetut ohjeet ovat selkeitä, helppolukuisia ja ymmärrettäviä, tunnistustapahtumassa ja tunnuslukulistoissa käytetty tekstifontinkoko on mahdollisimman

[50] Luottotoiminnasta annetun lain 15 luvun 6 §:n mukaan *Talletuspankki saa kieltäytyä tavanomaisen talletustilin avaamisesta ja tilin käyttöön tarkoitetun välineen myöntämisestä taikka maksupalvelua koskevan toimeksiannon hoitamisesta ETA-valtiossa laillisesti oleskelevalle luonnolliselle henkilölle vain, jos kieltäytymiselle on painava peruste. Perusteen tulee liittyä asiakkaaseen tai hänen aiempaan käyttäytymiseensä taikka siihen, ettei asiakassuhteelle ilmeisesti ole todellista tarvetta. Kieltäytymisen peruste on ilmoitettava asiakkaalle.*

[51] Luottotoiminnasta annetun lain 15 luvun 6 §:n mukaan pykälässä säädettyä ei sovelleta, *jos 18 §:stä tai rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetusta laista (503/2008) johtuu muuta*.

[52] *Ehdotettavan lain 3 §:n 1 momentin 4 kohdassa ehdotetaan saavutettavuusdirektiivin nähden soveltamisalan laajentamista vahvoihin sähköisiin tunnistuspalveluihin ja julkisen hallinnon palveluihin liittyvien verkkomaksamisen mahdollistamiin digitaalisiin palveluihin. Ehdotettavan lain 3 §:n 1 momentin 4 kohdan mukaan lakia sovellettaisiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 12 §:ssä tarkoitettuun rekisteriin merkittyihin tunnistuspalvelun tarjoajien tunnistuspalveluihin liittyviin digitaalisiin palveluihin.* ***Soveltamisalaan ei siten kuuluisi varsinaiset tunnistusvälineet, vaan tunnistustapahtumaan liittyvien verkkosivustojen tai mobiilisovellusten sisällöt****.* (HE 60/2018 vp). Lakia digitaalisten palvelujen tarjoamisesta valvoo Etelä-Suomen Aluehallintovirasto. Aluehallintovirastolta ei ole tämän markkinaselvityksen kirjoittamisen aikana antanut tarkempaa tulkintaa kyseessä olevasta laista ja sen soveltamisalasta.

suuri, tunnuslukulaitteen näppäimet ovat riittävän suuret sekä tunnistusmenetelmät tukevat erilaisia, vähintäänkin yleisiin standardeihin perustuvia apulaitteita (esim. ruudunlukuohjelmat sekä pistekirjoitussovellukset ja -laitteet).

Yhdenvertaisuuslain (1325/2014) 15 §:ssä säädetään kohtuullisista mukautuksista, mutta laki ei velvoita tuotteistamaan palveluita säännönmukaisesti esteettömiksi.[53] Pitkäaikainen ruumiillinen, henkinen, älyllinen tai aisteihin liittyvä vamma vaatii jokainen vähintäänkin jossain määrin ja monilta osin täysin erilaista ratkaisu tunnistuspalvelun saavutettavuuden ja esteettömyyden takaamiseksi. Ottaen huomioon myös tunnistusmenetelmien monimuotoisuuden ja teknologianeutraalisuuden, kaikkien tunnistuspalvelujen tuotteistaminen säännönmukaisesti saavutettavaksi ja esteettömäksi on haasteellista. Olisikin tarpeen varmistaa tunnistuspalvelujen yleinen saavutettavuus ja esteettömyys sekä tarjota erikseen yksityiskohtaisempia ratkaisuja edellä mainituille erityisryhmille niissä tapauksissa, joissa yleisesti saavutettava ja esteetön tunnistuspalvelu ei ole saavutettavissa ja esteetön.

Tunnistuspalvelujen yleinen saavutettavuus ja esteettömyys voitaneen monelta osin taata tarjoamalla tunnistuspalvelun tarjoajille tietoa ja osaamista koetuista esteistä ja haasteista sekä tekemällä yhteistyötä tunnistuspalvelujen kehittämisessä vapaaehtoisuuteen perustuen, jolloin mahdolliset saavutettavuutta ja esteettömyyttä koskevat kehitystoimet tehdään normaalin kehitystyön yhteydessä. Julkinen hallinto voi myös tarvittaessa ohjata tunnistuspalvelujen tarjontaa ostamalla erityispalveluja yleisesti saavutettavien ja esteettömien tunnistuspalvelujen ulkopuolille jääville henkilöille. Viime kädessä julkisella hallinnolla on myös mahdollisuus säätää yleisistä tunnistuspalvelujen saavutettavuus ja esteettömyysvaatimuksista.

6.1.5 Puolesta-asiointi ja avustajan käyttö

Esteellisellä käyttäjällä voi olla tarve käyttää sähköisessä asioinnissa ja tunnistautumisessa avustajaa, jos tunnistusmenetelmä ei ole esteetön siten, että hän voi käyttää sitä itsenäisesti. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista sekä eIDAS-varmuustasoasetus edellyttävät kuitenkin, että tunnistusmenetelmä saa olla vain haltijansa käytettävissä.[54] Esteellisten henkilöiden avustajat voivat saada avustaessaan tietoonsa tunnistusmenetelmän salaisia tekijöitä. Lainsäädäntöä voitaisiin kuitenkin selkeyttää avustamisen osalta. Lainsäädännössä voisi esimerkiksi varmistaa avustajan erityiset hyödyntämiskiellot, vastuut ja muut sellaiset asiat, joiden tarkoituksena on estää tunnistusvälineen luvaton käyttö avustajan toimesta. Vertailun vuoksi voi todeta, että maksupalvelulain muutoksessa esimerkiksi todettiin perusteluissa, että vahvan tunnistusmenetelmän käyttö tilitieto- tai maksutoimeksiantopalvelussa ei ole tunnistuslain 23 §:ään nähden luvatonta luovuttamista, vaikka palvelu saakin tietoon todentamistietoja. Erityiset rajoitukset tietojen käyttämiselle tilitieto- tai maksutoimeksiantopalvelussa on säädetty.

Puolesta asioinnissa olennaista on, että sähköisessä tunnistautumisessa tunnistaudutaan aina omalla tunnistusvälineellä ja edustusoikeus tarkistetaan jostain muusta

---

[53] Yhdenvertaisuuslain 15 §:n mukaan "*Viranomaisen, koulutuksen järjestäjän, työnantajan sekä tavaroiden tai **palvelujen tarjoajan on tehtävä asianmukaiset ja kulloisessakin tilanteessa tarvittavat kohtuulliset mukautukset, jotta vammainen henkilö voi yhdenvertaisesti muiden kanssa** asioida viranomaisissa sekä **saada** koulutusta, työtä ja **yleisesti tarjolla olevia** tavaroita ja **palveluita** samoin kuin suoriutua työtehtävistä ja edetä työuralla.*

Mukautusten kohtuullisuutta arvioitaessa otetaan huomioon vammaisen ihmisen tarpeiden lisäksi 1 momentissa tarkoitetun toimijan koko, taloudellinen asema, toiminnan luonne ja laajuus sekä mukautusten arvioidut kustannukset ja mukautuksia varten saatavissa oleva tuki."

HE 19/2014 vp 15 §:n perustelut, s. 79: *Kohtuulliset mukautukset on käsitteellisesti erotettava yleis- ja pysyväisluonteisista esteettömyystoimenpiteistä. Tällaisista toimenpiteistä säädetään muualla lainsäädännössä…*

[54] Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 23 §:n 2 momentin mukaan *Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön*.

lähteestä. Vertailukohtana voi käyttää fyysistä puolesta asiointia, jossa esitetään oma viranomaisen myöntämä henkilöllisyystodistus edustettavalta henkilön allekirjoittaman ja siltä saadun valtakirjan lisäksi.

6.2 Vahvan sähköisen tunnistamisen markkina sähköisten asiointipalvelujen näkökulmasta

Tällä hetkellä merkittävin yksittäinen tunnistuspalvelujen ostaja on Digi- ja väestötietovirasto, joka välittää keskitetysti tunnistuspalveluja julkiselle hallinnolle Suomi.fi-tunnistuksen kautta.[55] Arviolta noin 60-75 prosenttia tunnistustapahtumista kohdistuu julkisen hallinnon palveluihin Suomi.fi-tunnistuksen kautta. Digi- ja väestötietovirasto onkin todella merkittävä asiakas tunnistuspalvelujen tarjoajille. Loput, arviolta noin 25-40 prosenttia tunnistustapahtumista kohdistuu yksityisen sektorin ja kolmannen sektorin toimijoiden tarjoamiin sähköisiin asiointipalveluihin.

Julkisen sektorin toimijat ovat velvoitettuja käyttämään Suomi.fi-tunnistusta eli ne eivät voi itse hankkia vahvan sähköisen tunnistamisen palveluja markkinoilta. Suurimmaksi osaksi julkisen sektorin toimijat ovat myös lainsäädännöllä velvoitettuja käyttämään vahvaa sähköistä tunnistamista sähköisissä asiointipalveluissaan, joissa käsitellään henkilötietoja tai muutoin salassa pidettävää tietoa.

Useaan yksityisen sektorin toimijaan kohdistuu myös velvoite tunnistaa asiakkaansa vahvasti, minkä seurauksena ne ovat ottaneet vahvan sähköisen tunnistamisen käyttöön tarjoamissaan sähköisissä asiointipalveluissa. Tämä näkyy myös Esimerkiksi kuluttajansuojalain (38/1978) mukaan luotonantajan on ennen kuluttajaluottosopimuksen tekemistä todennettava luottoa hakevan henkilöllisyys huolellisesti ja, jos henkilöllisyys todennetaan sähköisesti, luotonantajan on käytettävä vahvaa sähköistä tunnistuspalvelua asiakkaittensa tunnistamiseksi. Vastaavasti sähköisestä lääkemääräyksestä annetun lain (61/2007) mukaan sähköinen lääkemääräys tulee toteuttaa siten, että reseptikeskuksessa olevien tietojen katselu, tallettaminen ja muu käsittely edellyttävät käsittelijän yksilöivää vahvaa tunnistusmenetelmää eli vahvan sähköisen tunnistusvälineen käyttämistä.

Merkittävin vahvan sähköisen tunnistamisen käyttöalue liittyy verkkopankissa asiointiin ja maksamiseen. Muualla yksityisellä sektorilla asiakkaiden tunnistamisessa vahvaa sähköistä tunnistamista käyttävät muun muassa apteekit, lääkäriasemat ja muut terveydenhuoltopalveluja tarjoavat yritykset, vakuutusyhtiöt, teleyritykset, sähköyritykset, postipalveluyritykset ja matkustuspalveluja tarjoavat yritykset. Myös erilaisten asiakirjojen sähköisessä allekirjoittamisessa yritykset käyttävät allekirjoituspalveluja, joiden osana käytetään vahvaa sähköistä tunnistamista. Edelleen kuitenkin usea yksityisen sektorin toimija tukeutuu asiointipalvelussaan asiakkaiden tunnistamisessa heikkoon tunnistusmenetelmään, vaikka palvelussa käsitellään henkilötietoja tai muita salassa pidettäviä tietoja. KKV:n tekemien selvitysten yhteydessä eräät verkkokauppa-alustoja tarjoavat toimijat ovat nostaneet esille, että apteekkisektorin ulkopuolella verkkokauppojen kysyntä asiakkaan vahvalle sähköiselle tunnistukselle on vähäistä. Verkkokaupan maksutapahtuman yhteydessä asiakas kuitenkin tunnistetaan pääsääntöisesti vahvasti maksupalvelusääntelyn säädettyjen vaatimusten takia.[56] Aiemmin monessa verkkokaupassa on ollut mahdollista maksaa syöttämällä palveluun maksukortin tiedot. PSD2-direktiivin mukaisesti 14.9.2019 alkaen pelkästään maksukortin tiedot verkkokauppaan

[55] Tässä ei ole huomioitu tunnistusvälineen tarjoajan välineen käyttöä sen omissa palveluissa, mikä ei lukeudu vahvan sähköisen tunnistamisen lainsäädännön piiriin ja soveltamisalaan. Esimerkiksi pankkiasioinnissa muutamia poikkeuksia lukuun ottamatta asiakkaalla on mahdollisuus tunnistautua pankin sähköisiin asiointipalveluihin vain pankin kehittämällä ja asiakkaalle tarjoamalla tunnistusvälineellä.

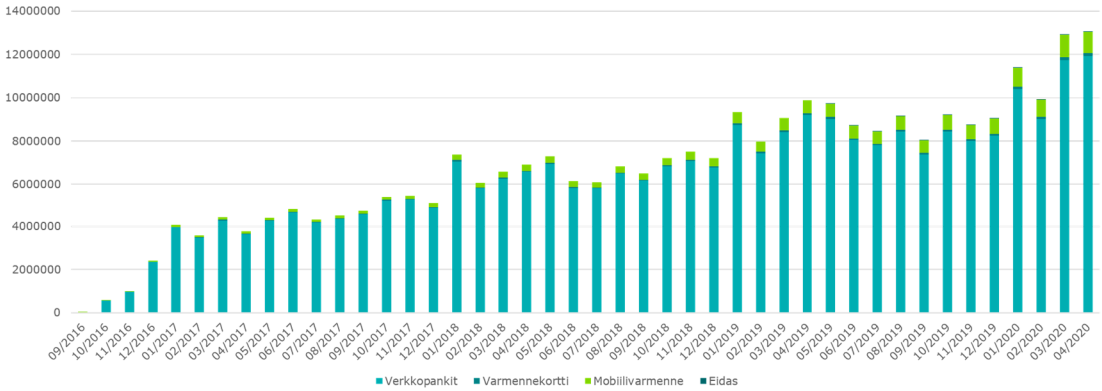
[56] Lisätietoja esimerkiksi Finanssivalvonnan internet-sivulta: https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/maksupalvelut/psd2--toinen-maksupalveludirektiivi/

syöttämällä ei ole voinut enää maksaa, vaan asiakas on tullut myös tunnistaa vahvasti maksun yhteydessä.[57] Tietyissä poikkeustapauksissa, kuten pienissä enintään 30 euron ostoksissa, vahvaa tunnistusta ei välttämättä vaadita. Pienissäkin verkkomaksuissa vahva tunnistaminen vaaditaan kuitenkin, kun ostokerroille tai ostojen yhteismäärälle asetetut turvarajat tulevat täyteen.

Yksityisen ja kolmannen sektorin toimijoille vahva sähköinen tunnistaminen on yksi keino tunnistaa niiden tarjoamien sähköisten asiointipalvelujen asiakkaat. Pääsääntöisesti yksityisen ja kolmannen sektorin toimijat käyttävät vahvaa sähköistä tunnistamista, koska ne ovat velvoitettuja siihen tai kokevat muutoin tarpeelliseksi tunnistaa asiakkaansa vahvasti ja huolehtia asiakkaidensa tietoturvallisuudesta ja -suojasta kuin myös oman toimintaansa kohdistuvista liiketaloudellisista riskeistä.

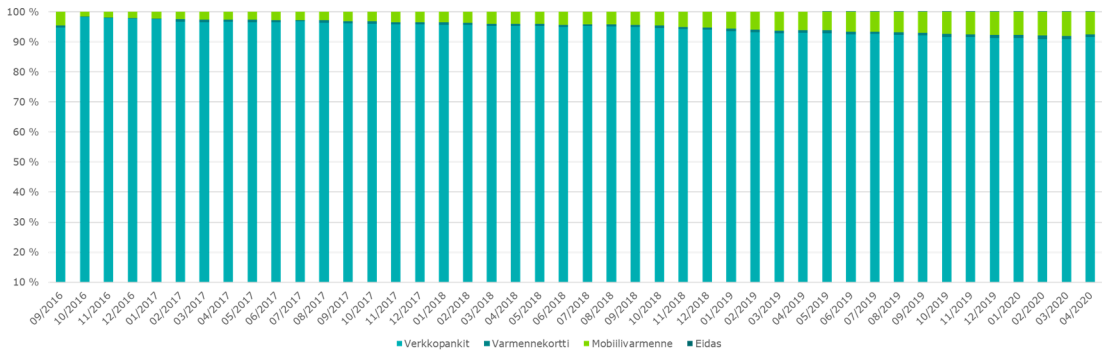
6.2.1 *Julkisen hallinnon sähköiset asiointipalvelut (julkisen hallinnon yhteinen välityspalvelu Suomi.fi-tunnistus)*

Digi- ja väestötietovirasto on suurin vahvoja sähköisiä tunnistuspalveluja ostava asiakas eli sähköinen asiointipalvelu. Digi- ja väestötietovirasto hankkii ja kilpailuttaa julkisen hallinnon toimijoiden puolesta niiden sähköisissä asiointipalveluissa käytössä olevat vahvan sähköisen tunnistamisen palvelut ja tarjoaa sen jälkeen näitä tunnistuspalveluja Suomi.fi-tunnistuksen kautta. Suomi.fi-tunnistuksen käyttäminen on julkisen hallinnon toimijoille ilmaista eli Digi- ja väestötietoviraston huolehtii kustannuksista, joita vahvan sähköisen tunnistuspalvelujen käytöstä julkiselle hallinnolle koituu, ja maksaa tunnistuspalvelujen käytöstä yksityisille tunnistuspalvelujen tarjoajille.



Kuva 9: Suomi.fi -tunnistustapahtumamäärien kehittyminen 9/2016-4/2020. (Lähde: Digi- ja väestötietovirasto)

[57] Finanssivalvonta salli velvoitteeseen tilapäisiä helpotuksia vuoden 2020 loppuun asti: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2019/finanssivalvonta-sallii-tilapaisia-helpotuksia-vahvan-tunnistamisen-toteuttamiseen-verkkokaupan-korttimaksamisessa/
https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2020/lisaaikaa-verkkokaupan-korttitapahtumien-tilastotietojen-seurantaraportoinnille/



Kuva 10: Suomi.fi -tunnistustapahtumamäärien osuudet tunnistusmenetelmittäin 9/2016 - 4/2020. (Lähde: Digi- ja väestötietovirasto)

Kuva 11: Suomi.fi -tunnistustapahtumamäärien kehitys ja ennuste kehityksestä vuosille 2021-2025 (miljoonaa tunnistustapahtumaa). (Lähde: Digi- ja väestötietovirasto)

Suomi.fi -tunnistamisen kautta vahvalla sähköisellä tunnistusvälineellä tehtyjen tunnistustapahtumien määrä on kasvanut nopeasti. Vuonna 2017 Suomi.fi -tunnistamisen kautta tunnistauduttiin noin 55 miljoonaa kertaa, kun vuonna 2018 tunnistauduttiin jo noin 82 miljoonaa ja vuonna 2019 107 miljoonaa kertaa julkisen hallinnon sähköisiin palveluihin. Nopeaa kehitystä selittää se, että julkisenhallinnon palveluita on siirretty vuosina 2017-2019 nopeaa vauhtia sähköisesti saatavilla ja palveluiden käyttämisessä on vaadittu asiakkaan vahvaa sähköistä tunnistamista. Nopea kasvuvauhti on kuitenkin tasaantunut ja, kun vuonna 2018 vuotuinen tunnistustapahtumamäärän kasvu oli noin 50 prosenttia edellisvuoteen verrattuna, vuonna 2019 kasvu oli enää 31 prosenttia.

Digi- ja väestötietovirasto myös odottaa, että tunnistustapahtumamäärien kasvu tulee edelleen tasaantumaan ja vuosina 2021 ja 2022 vuotuinen kasvu tulisi olemaan noin 20 prosenttia vuosittain. Tämän jälkeen kasvun oletetaan tasaantuvan. Korona toi vuonna 2020 odotettua suuremman hyppäyksen, noin 36 prosentin lisäys edelliseen vuoteen, mutta vuoden 2020 tapahtumamäärien oletetaan määrittelevän tapahtumille uuden tason tulevina vuosina. Suurimmat julkisen sektorin toimijat ovat pääosin sähköistäneet palvelunsa, joten merkittäviä hyppäyksiä ei ole enää odotettavissa, mutta käyttäjien siirtymä tuo kasvua vielä muutaman vuoden. Tämän jälkeen tunnistustapahtumamäärien odotetaan tasaantuvan noin 10 prosentin vuosikasvuvauhdin tasolle.

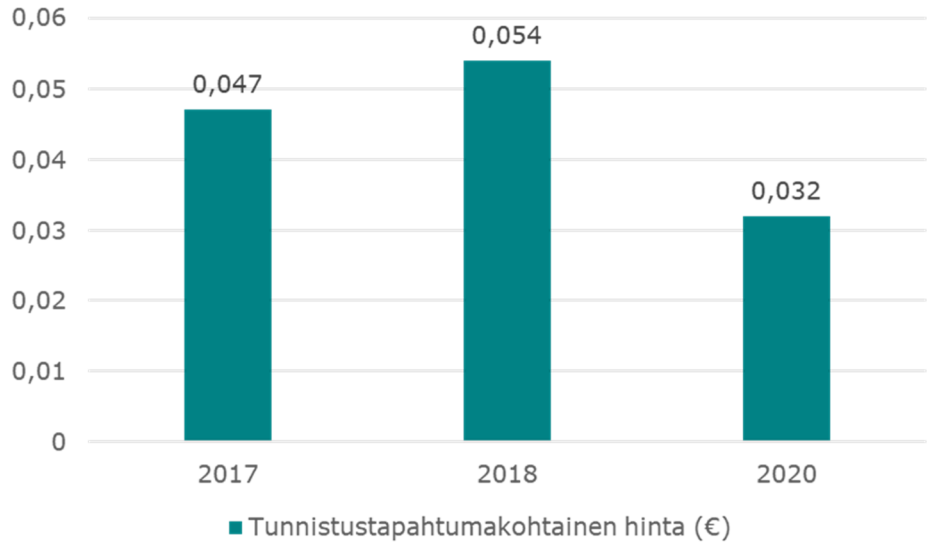
6.2.2 Ostajan eli sähköisten asiointipalvelujen markkinavoima

Digi- ja väestötietovirastolla suurimpana yksittäisenä vahvojen sähköisten tunnistuspalvelujen ostajana voidaan katsoa olevan merkittävää markkinavoimaa, mitä se pystyy muun muassa hyödyntämään kilpailuttaessaan tunnistusvälityspalveluja. Sen vahvoista sähköisistä tunnistuspalveluista maksama tapahtumakohtainen hinta on hyvin lähellä tunnistuspalvelun tarjoajien toisiltaan tunnistustapahtuman välittämisestä perimää säänneltyä enimmäishinta. Digi- ja väestötietoviraston markkinavoimaa rajoittaa se, että sen on lainsäädännön mukaan tarjottava kaikille kansalaisille yhtäläiset mahdollisuudet käyttää julkisenhallinnon palveluja eikä se siten voi helposti jättää joitakin tunnistusvälineen tarjoajaa Suomi.fi -tunnistuksen ulkopuolelle siten, ettei näiden tunnistusvälineillä voisi tunnistautua julkisen hallinnon sähköisiin palveluihin.

Yksityisen ja kolmannen sektoreiden sähköisten palvelujen tarjoajien ostajan markkinavoima sen sijaan voidaan katsoa olevan heikompi eivätkä ne välttämättä kykene Digi- ja väestötietoviraston tavoin yhtä tehokkaasti kilpailuttamaan tunnistuspalvelujen tarjoajia ja painamaan hintoja alas. Tässäkin palveluja ostavan yrityksen koolla näyttäisi olevan merkitystä ja esimerkiksi KKV:n selvitysten perusteella etenkin suurilla yrityksillä on ostaja- ja neuvotteluvoimaa, kun ne ostavat välityspalvelun tarjoajilta tunnistuspalveluja: isot yritykset näyttävät ostavan tunnistuspalvelunsa selvästi pieniä yrityksiä edullisemmilla hinnoilla. Tunnistusvälityspalvelujen tarjoajien markkinoille tulo on kuitenkin helpottanut huomattavasti niiden tilannetta ja lisännyt markkinavoimaa kilpailuttaa ja neuvotella tunnistuspalveluista perityistä hinnoista. Ennen tunnistusvälityspalvelujen tarjoajien markkinoille tuloa jokainen tunnistusvälineen tarjoaja toimi niiden näkökulmasta käytännössä monopolina. Ainoa vaihtoehto vaikuttaa tunnistuspalvelujen perimiin hintoihin oli uhata jättää tunnistuspalvelun tarjoaja sähköisen palvelun ulkopuolelle siten, ettei kyseisen tunnistuspalvelun tarjoajan välineellä ollut mahdollista tunnistautua sähköiseen palveluun. Sähköisen palvelun tarjoajalle tämä kuitenkin tarkoitti pahimmillaan oman ja potentiaalisen asiakaskunnan rajaamista omien sähköisten palvelujensa ulkopuolelle eikä siten uhkavaikutus ole ollut merkittävä.

Digi- ja väestötietovirasto ja sitä edeltänyt Väestötietovirasto on kilpailuttanut tunnistuspalvelun tarjoajat vuosina 2020, 2018 ja 2017. Kilpailutusten myötä Digi- ja väestötietoviraston tunnistuspalvelun tarjoajille maksamat hinnat ovat laskeneet vuoden 2017 kilpailutuksen tuloksena saadusta hinnasta 0,047 €/tunnistustapahtuma vuoden 2020 kilpailutuksen tuloksena saatuun hintaan 0,032 €/tunnistustapahtuma, vaikka vuoden 2018 kilpailutuksen jälkeen hinnat nousivatkin.[58]

[58] Tunnistustapahtumakohtainen hinta on laskettu toteutuneen laskutuksen ja tunnistustapahtumamäärien perusteella pois lukien vuoden 2020 hinta, joka on laskettu kilpailutuksessa käytetyn hintojen vertailuun käytetyn tapahtumamäärän mukaan.



Kuva 12: Tunnistustapahtumakohtainen hinta laskettuna toteutuneen laskutuksen ja tunnistustapahtumamäärien perusteella.

Tunnistuspalvelujen kilpailutusmenetelmä on vaihdellut vuosittain. Vuonna 2017 Väestörekisterikeskus kilpailutti ensimmäistä kertaa vahvan sähköisen tunnistamisen välityspalvelujen tarjoajia, kun aikaisemmin palvelut oli kilpailutettu ja ostettu suoraan tunnistusvälineen tarjoajilta. Vuonna 2017 Väestörekisterikeskus haki kilpailutuksessa tunnistuspalveluille kiinteää hintaa tunnistustapahtumakohtaisten hintojen sijasta. Tuolloin kilpailutus jouduttiin osittain keskeyttämään, koska saatujen tarjousten perusteella valtion maksamien tunnistamismaksujen kustannustaso olisi noussut merkittävästi. Ainoastaan mobiilivarmenteiden tunnistuspalvelut hankittiin kilpailutuksen perusteella syntyneen sopimuksen kautta. Muut tunnistusvälineet hankittiin aiemmin tehtyjen sopimusten kautta suoraan tunnistusvälineen tarjoajilta. Hinnat vaihtelivat tunnistusvälineittäin. Käytännössä vuonna 2018 toteutuneen laskutuksen perusteella laskettu keskimääräinen hinta per tunnistustapahtuma oli 0,047 €/tunnistustapahtuma. Vuoden 2017 aikana markkinoilla ei vielä ollut tunnistusvälityspalvelun tarjoajia, joilla olisi ollut sopimukset laaja-alaisesti tunnistusvälineen tarjoajien kanssa ja jotka olisivat voineet tarjota kattavasti eri tunnistuspalveluja sähköisille asiointipalveluille.

Vuonna 2018 toteutetussa tunnistusvälityspalveluiden kilpailutuksessa välityspalvelun kautta saatiin mobiilivarmenteiden tunnistuspalvelujen ohella yhden pankin verkkopankkitunnistuspalvelu. Muiden välineiden kohdalla nojauduttiin suoriin sopimusneuvotteluihin ja sopimuksiin kestävän hintatason saavuttamiseksi. Vuonna 2019 toteutuneen laskutuksen perusteella laskettu keskimääräinen hinta per tunnistustapahtuma oli 0,054 €/tunnistustapahtuma. Vuoden 2017 tavoin vuonna 2018 ei myöskään ollut tunnistusvälityspalvelun tarjoajia, jotka olisivat voineet tarjota kattavasti eri tunnistuspalveluja sähköisille asiointipalveluille ja joita olisi ollut mahdollista kilpailuttaa keskenään sähköisen asiointipalvelun toimesta. Vasta vuonna 2019 markkinoilla oli useampia tunnistusvälityspalvelun tarjoajia, jotka kykenivät tarjoamaan kattavasti eri tunnistuspalveluja sähköisille asiointipalveluille ja sähköisille asiointipalveluille oli todellinen mahdollisuus kilpailuttaa niitä.

Vuonna 2020 toteutetussa välityspalveluiden kilpailutuksessa valittiin aiemmista kilpailutuksista poiketen vain yksi välityspalvelu, jonka edellytettiin tarjoavan kaikki nykyisin käytössä olevat vahvan sähköisen tunnistamisen välineet. Tämä oli ensimmäinen kerta, kun luottamusverkostossa oli välityspalveluita, joilla oli kaikki tunnistusvälineet välitettävänään. Kilpailutuksessa oli edelleen mahdollista hinnoitella eri tunnistusvälineet erikseen ja välineet painotettiin aiemmin toteutuneiden jakaumien perusteella. Vertailuhinta laskettiin 170 miljoonan tunnistustapahtuman perusteella. Kilpailutuksen voittaneen tarjoajan vertailuhinta oli 5 440 000 €, jolloin

yksittäisen tapahtuman laskennallinen kustannus on 0,032 €. Viimeisimmässä kilpailutuksessa Digi- ja väestötietovirasto pystyi hyödyntämään ison asiakkaan asemaansa verraten hyvin edellyttämällä yhden välityspalvelun tarjoavan kaikki välineet. Hinta on lähellä säänneltyä enimmäishintaa (0,03 €/tunnistustapahtuma), jonka tunnistusvälineen tarjoaja saa enimmillään periä tunnistusvälityspalvelulta yhden tunnistustapahtuman välittämisestä. Kilpailutuksessa jätetyissä tarjouksissa yhdenkään välitettäväksi tarjotun tunnistuspalvelun tapahtumakohtainen hinta ei alittanut tätä säänneltyä enimmäishintaa, mikä viittaisi siihen, että tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä hinnoittelussa sovelletaan säänneltyä enimmäishintaa eikä yksikään tunnistusvälineen tarjoaja ole hinnoitellut tunnistustapahtuman hintaa enimmäishintaa alemmaksi. Tämä on varsin normaali ilmiö markkinoilla, joissa sovelletaan markkinatoimijoiden hinnoitteluun niin sanottuja enimmäistukkuhintoja. Luottamusverkostossa asiaan vaikuttavat myös tunnistuslain säännökset, jotka edellyttävät vahvan sähköisen tunnistusvälineen tarjoajien toimitusehdoilta syrjimättömyyttä.[59] Tunnistusvälityspalvelun tarjoajalla ei ole tällaisissa tilanteissa käytännössä mahdollisuutta myydä tunnistuspalveluaan alle säännellyn enimmäishinnan tekemättä tappiota.

Vahvoille sähköisille tunnistuspalveluille ei ole suoraan verrannollisia palveluja, joiden hintatasoon tunnistuspalvelujen hintoja ja hintataso olisi verrattavissa. Jotain osviitta kuitenkin saadaan, kun hintoja ja hintatasoa verrataan esimerkiksi Digi- ja väestötietoviraston maksullisiin julkisoikeudellisten suoritteiden hintoihin. Digi- ja väestötietoviraston julkisoikeudelliset suoritteet muodostavat myös yhden tunnistuspalvelujen kustannuskomponentin, joten siten niillä on myös yhteys vahvojen sähköisten tunnistuspalvelujen tarjoamiseen. Tunnistuslain 7 §:n 1 momentin mukaan tunnistusvälineen tarjoajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa. Lain perusteluissa (HE 74/2016) kyseistä lainkohtaa tarkennetaan seuraavasti: "*Tiedot tulisi päivittää niin usein, että voidaan riittävällä tavalla varmistua siitä, etteivät tiedot ole vanhentuneita.*". Tunnistuspalvelun tarjoajien ei siis tarvitse tarkastaa rekistereissään olevia tietoja väestötietojärjestelmästä jokaisen tunnistustapahtuman osalta eivätkä ne myöskään näin tee, vaan tarkastuksia tehdään esimerkiksi viikoittain.

Tunnistuslain 7 §:n 2 momentin mukaan väestötietojärjestelmästä luovutettava momentin 1 mukainen tieto on julkisoikeudellinen suorite. Suoritteen maksullisuudesta säädetään valtion maksuperustelaissa (150/1992). Julkisoikeudellisissa suoritteissa edellytetään omakustannushintojen käyttöä eli tietojen päivittämisestä väestötietojärjestelmästä saatavalla tiedosta perittävien maksujen tulisi kattaa vain Digi- ja väestötietovirastolle niiden tarjoamisesta koituvat kustannukset.[60] Maksuperustelain nojalla annetussa Valtiovarainministeriön asetuksessa Digi- ja väestötietoviraston suoritteiden maksuista vuonna 2020 (1304/2019) on VTJ-kyselyn hinnaksi kyselyrajapinnan kautta tehtynä määritelty 0,074 euroa/peruskysely. Tähän suhteutettuna vahvan sähköisen tunnistuspalveluista esimerkiksi Digi- ja väestötietoviraston maksama hinta vahvoista sähköisistä tunnistuspalveluista ei ole kohtuuton. On myös todennäköistä, että säänneltyä tunnistustapahtuman enimmäistukkuhintaa (0,03 €/tunnistustapahtuma) voidaan jatkossa laskea tunnistusmäärien kasvaessa, tekniikan kehittyessä ja yksikkökustannusten laskiessa, mikä vastaavasti mahdollistaa tunnistuspalvelujen tarjoamisen nykyistä alhaisemmilla vähittäishinnoilla.

[59] Tunnistuslain 12 a §:n 2 momentti.

[60] Digi- ja väestötietoviraston liiketaloudellisin perustein perimät hinnat sen tarjoamista palveluista ovat moninkertaiset suhteessa vastaaviin julkisoikeudellisina suoritteina eli omakustannehinnoin tarjottujen palvelujen hintoihin. Esimerkiksi VTJ-kyselyrajapinnan kautta tehtävä peruskyselyn liiketaloudellinen hinta on 0,27 €/kysely (Lähde: https://dvv.fi/documents/16079645/17333102/VTJrajapinnan-liiketaloudellinen-hinnasto.pdf/06915187-a623-a8d4-065a-98cdf64d484d/VTJrajapinnan-liiketaloudellinen-hinnasto.pdf).

Kilpailutusten kautta Digi- ja väestötietovirasto on saanut hillittyä sille vahvan sähköisen tunnistamispalvelujen ostamisesta aiheutuneita kustannuksia, mutta tunnistustapahtumamäärien oletettu kasvu luo paineita kustannusten nousulle. Toisaalta siirtämällä käyttäjiä käyttämään sähköisiä palveluja julkisella hallinnolla on mahdollisuus alentaa muualla ja erityisesti fyysisestä asioimisesta ja sen järjestämisestä aiheutuvia kustannuksia. Näistä mahdollista kustannushyödyistä ja -vaikutuksista ei ole tehty laskelmia eikä niitä ole arvioitu. Näitä mahdollisia kustannushyötyjä voitaisiin mitata ja arvioida esimerkiksi valtioneuvoston julkaiseman Julkisen hallinnon digitalisaatio – tuottavuus ja hyötyjen mittaaminen -tutkimuksessa esitetyillä menetelmillä.[61]

Myöskään suomalaisten siirtymisestä käynti tai paperiasioinnista julkisen hallinnon sähköisten palvelujen käyttäjiksi ei ole tarkempaa tietoa tai arvioita saatavilla.

Digi- ja väestötietoviraston tehtävänä on mahdollistaa osaltaan julkisen hallinnon palvelujen tarjoaminen kaikille kansalaisille, joten sillä on rajoitetut mahdollisuudet jättää jokin tunnistusväline kilpailutuksen ulkopuolelle ja siten käyttää ostajanvoimaansa ja lisätä kilpailupainetta tunnistusvälineen tarjoajia kohtaan. Tämä lähtökohtaisesti koskee myös muita sähköisten palvelujen tarjoajia, vaikkakin osa niistä on jättänyt joitakin tunnistusvälineitä palvelunsa ulkopuolelle, jolloin kyseisillä tunnistusvälineillä ei ole mahdollisuutta tunnistautua kyseisiin palveluihin. Kuitenkin, mitä enemmän tunnistusvälineiden välille saadaan kilpailua ja käyttäjien kokemat tunnistusvälineen vaihtamisen esteet poistettua, sitä suurempi mahdollisuus ja paremmat perusteet Digi- ja väestötietovirastolla olisi jättää jokin tai jotkin tunnistusvälineet Suomi.fi-tunnistuksen ulkopuolelle.

Tunnistusvälityspalvelujen markkina on tällä hetkellä rajautunut vain korotetun varmuustason välineisiin. Markkinalla toimii kuitenkin yksi tunnistusvälityspalvelun tarjoaja, joka täyttää korkean tason tunnistusvälityspalvelulle asetetut vaatimukset (Nets). Toisaalta tällä hetkellä tunnistuspalvelujen markkinalla ei ole tarjolla kuin kansalais- ja organisaatiovarmenne, jotka täyttävät korkean varmuustason tason vaatimukset tunnistusvälineelle ja olisivat siten myös välitettävissä korkealla tasolla. Korkean tason tunnistusvälityspalvelulle asetetut vaatimukset täyttävät välityspalvelu ei ole tähän mennessä nähnyt tarvetta tai muutoin kaupallisesti järkeväksi (syynä voi olla esimerkiksi se, etteivät sähköisen asiointipalvelun tarjoajat ole nähneet tarvetta korkean tason tunnistuspalvelulle) alkaa välittää kansalais- ja organisaatiovarmenteita korkealla tasolla.

6.3 Vahvan sähköisen tunnistuspalvelun tarjonta

Vahvan sähköisen tunnistuspalvelujen vähittäismarkkinoilla toimii sekä tunnistusvälineiden että tunnistusvälityspalvelujen tarjoajia, jotka tarjoavat tunnistuspalveluja sähköisille asiointipalveluille. Sama yritys voi toimia molemmissa rooleissa. Kaiken kaikkiaan Liikenne- ja viestintäviraston rekisterissä on tällä hetkellä 16 vahvan sähköisen tunnistuspalvelun tarjoajaa. Näistä omaa vahvaa sähköistä tunnistusvälinettä tarjoaa 14 toimijaa[62] ja muidenkin kuin oman vahvan sähköisen tunnistusvälineen käyttäjien tunnistusta välittäviä tunnistuspalveluja on kahdeksan.[63] Tunnistusvälityspalvelun tarjoajista kaksi tarjoaa pelkästään välityspalvelua eli niillä ei ole omaa vahvaa sähköistä tunnistusvälinettä tarjottavana sähköisille asiointipalveluille.

[61] Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 3/2017 (https://valtioneuvosto.fi/documents/10616/3866814/3_Julkisen hallinnon+digitalisaatio+%E2%80%93+tuottavuus+ja+hy%C3%B6tyjen+mittaaminen/49e6b987-6d37-44dd-a86e-cc548fc66760?version=1.0)

[62] Aktia Pankki Oyj, Danske Bank A/S, Digi- ja väestötietovirasto, DNA Oyj, Elisa Oyj, Nordea Bank Oyj, Oma Säästöpankki Oyj, OP-Palvelut Oy, POP-Pankki -ryhmä, S-Pankki Oy, Svenska Handelsbanken Ab, Säästöpankkiryhmä, Telia Finland Oyj ja Ålandsbanken AbP

[63] Danske Bank A/S, DNA Oyj, Elisa Oyj, NETS Branch Norway, Nordea Bank Oyj, OP-Palvelut Oy, Signicat AS ja Telia Finland Oy.

Vahvan sähköisen tunnistusvälityspalvelun tarjoajista kuusi välittää sähköisille asiointipalveluille kaikkia Suomessa käytössä olevia tunnistusvälineitä pois lukien Digi- ja väestötietoviraston henkilö- ja organisaatiovarmenteita. Tilanne on tältä osin parantunut huomattavasti parin vuoden takaisesta tilanteessa, jolloin tällaisia tunnistusvälityspalvelun tarjoajia oli vain muutama tai ei ollenkaan.

Vahvojen sähköisten tunnistuspalvelujen käyttöoikeuden myynnistä välityspalveluille kertynyt liikevaihto oli vuonna 2019 arviolta noin 5-8 miljoonaa euroa. Tämä liikevaihto ei sisällä välityspalvelun tarjoajien sähköisiltä asiointipalveluilta perimiä maksuja, eli tunnistuspalvelujen käyttöoikeuden ostamisesta koituvien kustannusten päälle laskettavia välityspalvelun omia kustannuksia ja myyntikatetta, eikä tunnistusvälineen tarjoajien suoraan sähköisille asiointipalveluille myymien tunnistuspalvelujen liikevaihtoa. Huomioiden näistä tuleva liikevaihto oli vahvan sähköisen tunnistuspalvelujen kokonaisliikevaihto vähintäänkin kaksinkertainen käyttöoikeuden myynnistä saatuun liikevaihtoon suhteutettuna, eli arviolta vähintään noin 10-16 miljoonaa euroa.[64] Tämä liikevaihto ei sisällä vahvan sähköisen tunnistusvälineen tarjoajien omissa sähköisissä palveluissa käytetyistä vahvoista sähköisistä tunnistuspalveluista mahdollisesti kertyvää liikevaihtoa.

Vahvojen sähköisten tunnistuspalvelujen käyttöoikeuden myynnin kautta vuonna 2019 välitettiin arviolta noin 40-80 miljoonaa tunnistustapahtumaa, kun kokonaisuudessaan sähköisissä asiointipalveluissa tehtiin arviolta noin 130-170 miljoonaa tunnistustapahtumaa. Luku ei sisällä vahvan sähköisen tunnistusvälineen tarjoajien omissa sähköisissä palveluissa käytetyistä vahvoista sähköisistä tunnistuspalveluista kertyviä tunnistustapahtumia.[65]

Vahvojen sähköisten tunnistuspalvelujen käyttöoikeuden tunnistustapahtuma- ja euromääräistämyyntiä tarkasteltaessa erottuu kolme suurinta käyttöoikeuden myyjää, Nordea, OP-Palvelut ja S-pankki Oy, selkeästi muista käyttöoikeuden myyjistä. Tämä selittyy yksinomaan sillä, että suurin osa suomalaisista ja Suomessa asuvista ovat kyseisten pankkien pankkiasiakkaina kuin myös niiden tarjoamien verkkopankkitunnusten käyttäjiä.

Tarkasteltaessa vahvan sähköisen tunnistuspalvelujen markkinaa kokonaisuudessaan järjestys on täysin toinen. Telia on tunnistustapahtuma- ja euromääräistämyyntiä tarkasteltaessa selkeästi suurin markkinatoimija ja myös Signicat ohittaa selkeästi edellä mainitut pankit pois lukien Nordeaa, joka on toiseksi suurin vahvan sähköisen tunnistuspalvelujen tarjoaja. Telian asemaa selitti monelta osin se, että Digi- ja väestötietoviraston oli sen asiakas ja suurelta osin Suomi.fi-tunnistuspalvelussa tehdyt tunnistustapahtumat välitettiin Telian toimesta. Kun huomioidaan myös Signicatin asema markkinoilla, voidaan todeta, että tunnistusvälityspalvelun tarjoajien tulo markkinoille on merkittävästi muuttanut markkina-asetelmia vahvan sähköisen tunnistuspalvelun markkinalla.

Tarkasteltaessa vahvan sähköisen tunnistuspalvelun käyttöoikeuden myyntiä tunnistuspalvelujen pääasiallisen toimialan mukaan vuonna 2019 noin 87-90 prosenttia käyttöoikeuden myynnistä kohdistui verkkopankkitunnisteilla ja noin 10-13 prosenttia mobiilivarmenteilla tehtävien tunnistustapahtumien välittämistä. Nämä luvut ovat linjassa Digi- ja väestötietoviraston julkaisemien tunnistusmenetelmiä koskevien osuuslukujen kanssa kuin myös sen kanssa kuinka paljon eri tunnistusvälineitä suomalaisilla ja Suomessa asuvilla on käytössä.

[64] Vahvan sähköisen tunnistuspalvelun tarjoajilta ei ole saatu kattavasti ja tarkempia tietoja liikevaihdon laskemiseksi ja siten markkinaselvityksessä liikevaihdon suuruus on jouduttu arvioimaan saatujen ja muiden julkisesti saatavilla olevien tietojen pohjalta.

[65] Suomen pankin tilastojen mukaan yksistään pankkien omiin sähköisiin asiointipalveluihin tehtiin vuonna 2019 noin 150 miljoonaa tunnistustapahtumaa. Vuoteen 2018 kasvua on lähes 25 miljoonaa tunnistustapahtumaa. Lähde: https://www.suomenpankki.fi/fi/Tilastot/maksuliiketilastot/taulukot/

6.3.1 Tunnistuspalvelun tarjoajien markkinavoima

Tällä hetkellä vahvojen sähköisten tunnistuspalvelujen markkinalla tunnistusvälineiden kesken käytävä kilpailu on vähäistä. Syy on varsin luonnollinen, sillä esimerkiksi verkkopankkitunnuksia tarjoavat pankit kilpailevat keskenään pankkipalvelujen kokonaisasiakkuuksista, eivät erikseen vahvan sähköisen tunnistusvälineen tarjoamisesta ja siihen liittyvistä asiakkuuksista. Samoin mobiilioperaattorit kilpailevat keskenään matkaviestinliittymissä.

Kokonaisasiakkuuksista kilpailu on johtanut siihen, ettei vahvan sähköisen tunnistusvälineen käyttäjällä ole todellista mahdollisuutta saada käyttöönsä vahvaa sähköistä tunnistusvälinettä ilman toista tunnistuspalvelun saamiseksi vaadittua palvelua ja asiakkuutta. Saadakseen käyttöönsä vahvan sähköisen tunnistusvälineen, esimerkiksi verkkopankkitunnukset, käyttäjän tulee olla jonkin pankin tiliasiakas ja mobiilivarmenteen saadakseen käyttäjällä on oltava matkaviestinverkkoyrityksen liittymäasiakkuus. Valtion kansalaisvarmenteen saamiseksi käyttäjällä tulee olla henkilökortti ja organisaatiovarmennetta varten työsuhde. Jos käyttäjä haluaa kilpailuttaa vahvan sähköisen tunnistusvälineen tarjoajia, hän voi lähinnä ottaa käyttöön rinnakkain tilipankkinsa verkkopankkitunnukset ja matkaviestinyrityksensä mobiilivarmenteen, mikä on nykyisin varsin helppoa. Digi- ja väestötietoviraston kansalaisvarmenne tai työnantajan kautta käytössä oleva organisaatiovarmenne eivät näytä olevan todellinen vaihtoehto käyttäjien näkökulmasta vaihtoehtoiskustannusten ja käyttöönoton teknisten esteiden takia. Myös rajalliset käyttömahdollisuudet eri sähköisissä asiointipalveluissa vaikuttanevat kansalais- ja organisaatiovarmenteen suosioon.

Vahvaa sähköistä tunnistamista käyttävien sähköisten asiointipalvelujen kannattaa sisällyttää kattavasti tunnistusvälineen tarjoajien välineitä palveluihinsa, jotta ne palvelevat mahdollisimman hyvin asiakkaitaan. Laajasti käytössä olevien välineiden jättäminen tunnistusvalikoiman ulkopuolelle johtaisi käytännössä aina merkittävän loppuasiakaskunnan ja siten myös potentiaalisen tulonlähteen ulkopuolelle jättämistä. Vahvan sähköisen tunnistusvälineen tarjoajia, erityisesti verkkopankkitunnisteita tarjoavia pankkeja, onkin voitu pitää sähköisille asiointipalveluille käytännössä pakollisina kauppakumppaneina. Tämä tekee vahan sähköisen tunnistusvälineen tarjoajista vähintään heikosti monopolistisia yrityksiä sähköisiin asiointipalveluihin nähden.

Vahvan sähköisen tunnistamisen tukkumarkkinan enimmäishinta ja muu luottamusverkostosääntely mahdollistavat nykyisin vahvan sähköisen tunnistusvälityspalvelun tarjoamisen ja uusien toimijoiden markkinoille tulon. Tunnistusvälityspalvelun tarjoajien tulo markkinoille on vähentänyt vahvan sähköisen tunnistusvälineiden tarjoajien markkinavoimaa suhteessa sähköisiin asiointipalveluihin. Ennen kaikkea vahvat sähköiset tunnistusvälityspalvelut ovat mahdollistaneet sähköisille asiointipalveluille tunnistuspalvelujen hintojen kilpailuttamisen. Jossain määrin sähköisille asiointipalveluille on tullut myös mahdolliseksi kilpailuttaa muitakin tunnistuspalvelun ominaisuuksia. Tunnistusvälityspalvelujen toiminnan mahdollistaminen on kuitenkin vaatinut ja vaatii edelleen tukkumarkkinoiden sääntelyä, mukaan lukien sopimus- ja hintasääntelyä.[66] Ilman sääntelyä tunnistusvälityspalvelun tarjoajilla ei olisi tosiasiallisia mahdollisuuksia välittää tunnistustapahtumia ja tarjota vahvoja sähköisiä tunnistuspalveluja sähköisille asiointipalveluille, koska tunnistusvälineen tarjoaja kykenisi markkinavoimansa avulla hinnoittelemaan sähköiselle asiointipalvelulle tarjoamansa oman tunnistuspalvelunsa hinnan alle välityspalvelun sille tunnistustapahtuman välittämisestä maksaman tukkuhinnan. Vahvojen sähköisten tunnistuspalvelujen markkinalla vallitsi

[66] Vastaavanlaista hintasääntelyä on kohdistettu vuosikymmenien ajan esimerkiksi matkaviestinverkkoyritysten toisiltaan ja kiinteän verkon yrityksiltä perimiin laskevan puheliikenteen hintoihin eli niin sanottuihin terminointihintoihin. Hintasääntely on ollut merkittävässä asemassa matkaviestinpalvelumarkkinoiden avaamisessa kilpailulle ja sille, että Suomessa matkaviestinpuhepalveluiden hinnat ovat Euroopan halvimpia ja käyttö suurinta

pääosin tällainen tilanne ennen kuin vahvojen sähköisten tunnistuspalvelujen tukkumarkkinoille kohdistettiin hintasääntelyä.

Verkkopankkitunnukset ovat syntyneet alun perin, jotta pankit voivat tunnistaa verkkopankissa omat asiakkaansa. Pankit ovat toistaiseksi muun muassa finanssialan tietoturvasyistä halunneet pitää omiin verkkopankkeihinsa tunnistautumisen omissa käsissään, mutta ensimmäiset askeleet tunnistusvälineiden laajemman käytettävyyden suuntaan ovat jo nähtävissä verkkopankeissa. Pankkien verkkosivuilta huhtikuussa 2020 selvitettyjen tietojen perusteella yksi vahvaa sähköistä tunnistusvälinettä tarjoava pankki, Danske Bank, hyväksyi verkkopankkiasioinnissa tunnistautumisen myös muidenkin pankkien vahvoilla sähköisillä tunnistusvälineillä kuin vain sen itse tarjoamilla tunnistusvälineillä. Yhdeksässä pankissa tai pankkiryhmässä verkkopankkiin oli kuitenkin mahdollista tunnistautua vain pankin omalla vahvalla sähköisellä tunnistusvälineellä.[67] OP-Palvelut hyväksyi muiden pankkien verkkopankkitunnukset tilitietopalveluihin ja vakuutusasioissa tunnistautuessa. Mikään pankki ei hyväksynyt matkaviestinverkkoyritysten tarjoamia mobiilivarmenteita pankin palveluihin tunnistautumisessa. Sen sijaan Telian ja Elisan omissa sähköisissä asiointipalveluissa oli mahdollisuus tunnistautua kaikilla mobiilivarmenteilla ja kaikilla verkkopankkitunnuksilla.

Vahvan sähköisen tunnistusvälineen tarjoajilla on jokaisella markkinavoimaa suhteessa sähköisiin asiointipalveluihin, joiden mahdollisuudet rajata jokin tunnistusväline sähköisen asiointipalvelunsa ulkopuolelle ovat hyvin rajoitetut. Ilman luottamusverkostosääntelyä vahvan sähköisen tunnistusvälineen tarjoajilla olisi nykyistä huomattavasti vahvempi markkina-asema käyttää markkinavoimaansa neuvotellessaan tunnistuspalvelusopimuksia sähköisten asiointipalvelujen kanssa. Paitsi tunnistusvälineiden välisen kilpailun toimivuuden myös erilaisten häiriötilanteiden ja palvelukatkojen kannalta olisi toivottavaa, että mobiilivarmenne ja mahdolliset tulevaisuudessa nähtävät uudet vahvan tunnistuksen välineet saisivat laajempaa jalansijaa markkinoilla.

6.3.2 Markkinoiden kasvupotentiaali

Vahva sähköinen tunnistaminen on jo laaja-alaisesti käytössä julkisen hallinnon sähköisissä palveluissa, vaikka edelleen useita julkisen hallinnon palveluja on vielä sähköistämättä. Myös olemassa olevien sähköisten asiointipalvelujen käyttö tulee kasvamaan entisestään. Digi- ja väestötietovirasto on arvioinut, että julkisen hallinnon sähköisiin asiointipalveluihin tehdyt tunnistustapahtumat tulevat vielä kaksinkertaistumaan seuraavan viiden vuoden aikana vuoden 2020 noin 150 miljoonasta vuoden 2025 yli 300 miljoonaa tunnistustapahtumaan. Jo siis yksistään julkisen hallinnon tunnistuspalvelujen käyttö tulee kasvamaan merkittävästi ja mahdollistamaan merkittävän liiketoiminnan kasvattamisen vahvojen sähköisten tunnistuspalvelujen tarjoajille. Toisaalta julkinen hallinto pyrkii omilla toimillaan hillitsemään tunnistuspalvelujen käytöstä koituvia kustannuksia, mikä voi osaltaan jarruttaa liiketoiminnan kasvamista.

Sen sijaan yksityisen sektorin ja kolmannen sektorin sähköisissä asiointipalveluissa vahvan sähköisen tunnistamisen käyttö on vielä kehitysvaiheessa ja suurimmassa osassa palveluja ei ole käytössä vahvaa sähköistä tunnistusta. Vahvojen sähköisten tunnistuspalvelujen kasvupotentiaali yksityisten ja kolmannen sektorin sähköisissä asiointipalveluissa on siten valtava. Jo maltillisestikin laskettuna yksityisen ja kolmannen sektorin sähköisissä asiointipalveluissa tehtyjen tunnistustapahtumien määrä voi seuraavien viiden vuoden aikana kasvaa yli 100 miljoonaan tunnistustapahtumaan vuodessa. Kokonaisuutena, julkisen sektorin tunnistustapahtumamäärien kehitys huomioiden, tämä tarkoittaisi yli 400 miljoonaan tunnistustapahtumaa

[67] Aktia Pankki Oyj, Svenska Handelsbanken An, Nordea Bank Oyj, Oma Säästöpankki Oyj, OP-Palvelut Oy, POP-pankki -ryhmä, S-Pankki Oy, Säästöpankkiryhmä, Ålandsbanken AbP.

vuodessa ja sitä, että vahvojen sähköisten tunnistuspalvelujen markkinan koko tunnistustapahtumien määrällä mitattuna yli 2,5-kertaistuisi viiden vuoden aikana.

Liikevaihdolla mitattu markkinan koko ei kuitenkaan tulenne kasvamaan samaa vauhtia, koska sääntelyn seurauksena edelleen vahvistuva kilpailu ja tekniikoiden kehittyminen tulevat todennäköisesti alentamaan tunnistustapahtumasta perittävää hintaa. Karkeasti voidaan kuitenkin arvioida, että vahvojen sähköisten tunnistuspalvelujen markkinan liikevaihto tulee viiden vuoden aikana kasvamaan yli kaksinkertaiseksi siitä, mikä se on ollut vuonna 2020.

Vahvojen sähköisten tunnistuspalvelujen markkinan kasvupotentiaalin voidaan katsoa olevan todella merkittävä seuraavien viiden vuoden aikana. Markkinan voidaan myös ennakoida kasvavan merkittävästi tämänkin jälkeen.

6.3.3 Markkinalle tulon esteet ja uudet tunnistuspalvelujen tarjoajat

Potentiaalinen vahvan sähköisen tunnistuspalvelun tarjoaja voi tulla markkinalle tarjoamaan uutta tunnistusvälinettä ja/tai tunnistusvälityspalvelua. Markkinalle tulon esteet vahvan sähköisen tunnistusvälineen tarjonnan aloittamiselle ja vahvan sähköisen tunnistusvälityspalvelun tarjonnan aloittamiselle poikkeavat jossain määrin toisistaan muun muassa sen osalta, missä määrin markkinalle tulo vaatii teknistä järjestelmä- ja palvelukehittämistä ja erilaisten sopimusten solmimista markkinalla jo toimivien toimijoiden kanssa. Yleisesti voidaan katsoa, että markkinalle tulo tunnistusvälityspalvelun tarjoajan roolissa on helpompaa kuin markkinalle tulo tunnistusvälineen tarjoajan roolissa. Tämä on myös näkynyt markkinalle tulleissa ja kiinnostuksensa ilmaisseissa toimijoissa, joista suurempi osa on tullut ja on ollut kiinnostunut tulemaan tarjoamaan tunnistusvälityspalveluja. Alla näitä markkinoille tulon esteitä on kuitenkin käsitelty yhtenä kokonaisuutena.

Lähtökohtaisesti markkinalle tulolle ainoan kynnyksen muodostavat lainsäädännössä asetetut vaatimukset tunnistusvälineen ja/tai tunnistusvälityspalvelun tarjoamiselle ja markkinalle tulijan vakavaraisuudelle[68], mitkä sen tulee täyttää ennen kuin se voi aloittaa tarjoamaan vahvoja sähköisiä tunnistuspalveluja. Vaatimusten mukaisen tunnistuspalvelun kehittäminen vaatii investointeja muun muassa tietojärjestelmiin ja tietoliikenneyhteyksiin sekä tunnistuspalvelujen asiakaspalvelu- ja myyntiverkostoon. Uuden tunnistusvälineen tarjoajalle näiden lisäksi investointikustannuksia muodostuu muun muassa itse tunnistusvälineen, mahdollisen oman ensitunnistamisen ja tunnistusvälineen sulkupalvelun kehittämisestä ja järjestämisestä.

[68] Toimijoilta odotetaan riittäviä taloudellisia resursseja tarjota tunnistuspalveluita ja huolehtia ja ylläpitää riittävästä palveluiden turvallisuudesta ja jatkuvuudesta.

Tunnistuspalvelun tarjoajan luotettavuus	Tunnistusjärjestelmän ja -menetelmän luotettavuus ja tietoturvallisuus	Vaatimustenmukaisuuden arviointi
Oma selvitys mm. seuraavista:	**Riippumaton ja pätevä arviointi mm. seuraavista**	**Tunnistuslaissa säädetyt arvioinnin vaatimukset, arviointielimet ja kriteerit**
• Oikeushenkilön ja vastuuhenkilöiden oikeustoimi- ja liiketoimintakelpoisuus • Taloudelliset resurssit ja vahinkovastuun kantokyky • Henkilöstöresurssit (24/7 valvonta, tekninen ja oikeudellinen osaaminen) • Vastuut alihankkijoista • Käyttäjäehdot ja tietosuojaperiaatteet	• Tietoturvallisuuden hallinta (esim. ISO 27001) • Tietojärjestelmien ja tietoliikennejärjestelyiden ml. käyttöturvallisuus ja tilaturvallisuus (ts. tunnistusmenetelmän taustajärjestelmät) • Tunnistusmenetelmä ja todentamismekanismi • Poikkeamien havainnointi ja hallinta ➢ Tunnistusjärjestelmän ja menetelmän varmuustason mukainen sietokyky tietoturvauhkia ja -loukkauksia vastaan	• Arviointi ennen aloitusilmoituksen tekemistä • Arviointi toiminnan aikana vähintään kahden vuoden välein • Korotetulla varmuustasolla sisäinen tarkastuslaitos tai ulkoinen arviointielin • Korkealla varmuustasolla ulkoinen arviointielin • Arviointikriteerit tarkennettu määräyksellä ja ohjeella

Taulukko 3: Tunnistusjärjestelmän ja -menetelmän luotettavuus ja sen osoittaminen.

Uuden tunnistusvälineen kehittämisessä markkinalle tulija voi hyödyntää jo olemassa olevia ja yleisesti saatavilla olevia standardeja ja tekniikoita. Tunnistusvälineen kehittämisessä markkinalle tulija voi myös hyödyntää valmiiksi kehitettyjä sovelluksia ja järjestelmiä ja siten vähentää tutkimus- ja investointikustannuksia. Pääosin vahvan sähköisen tunnistamisen markkinalla tarjotut tunnistusvälineet pohjautuvatkin yleisesti saatavilla oleviin standardeihin ja tekniikoihin ja niissä hyödynnetään valmiiksi kehitettyjä sovelluksia ja järjestelmiä.

Vaikka markkinalle tulolle on olemassa esteitä ja markkinalle tulo vaatii pääomia ja investointeja, ei esteiden voida katsoa olevan sellaisia, että ne estäisivät kokonaan markkinalle tulon. Tätä näkemystä tukee myös se, että markkinoille on tullut vahvan sähköisen tunnistusvälityspalvelun tarjoajia ja markkinoille tulo on kiinnostanut hyvin eri kokoisia toimijoita.

Näiden edellä mainittujen investointikustannusten lisäksi markkinoille tulevalle tunnistuspalvelun tarjoajalle aiheutuu kustannuksia muun muassa vahvan sähköisen tunnistuspalvelun tarjontaan kohdistuvasta sääntelystä. Vahvan sähköisen tunnistuspalvelun tarjoajien tulee muun muassa aloittaessaan ja siitä joka toisena vuonna auditoida tunnistuspalvelunsa ja siinä käytettävät järjestelmät riippumattomalla arvioitsijalla. Aloittaessaan palvelun tarjoajan tulee myös tehdä Liikenne- ja viestintävirastolle aloitusilmoitus ja maksaa erikseen laissa määritelty rekisteröintimaksu, kun palvelun tarjoaja on merkitty tunnistuspalvelurekisteriin. Tunnistuspalvelurekisteriin merkityn palvelun tarjoajan on myös maksettava vuotuinen valvontamaksu, josta säädetään laissa.[69]

Sen jälkeen, kun markkinoille tulija on saanut kehitettyä ja rekisteröityä vaatimukset täyttävän tunnistuspalvelun, tulee sen kyetä myymään tunnistuspalvelujaan ja tekemään sopimuksia tunnistusvälineen tarjoajien, tunnistusvälityspalvelujen ja/tai sähköisten asiointipalvelujen kanssa, mistä aiheutuu erinäisiä kustannuksia mukaan lukien muun muassa markkinointi- ja sopimuskustannukset. Esimerkiksi tunnistusvälityspalvelun tarjoajaksi aikovan tulee saada aikaan sopimuksia tunnistusvälineiden tarjoajien kanssa ennen kuin se voi alkaa tarjota, ainakaan kattavasti

[69] Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 47 §:n mukaan, *Kun 10 §:ssä tarkoitetun ilmoituksen tehnyt tunnistuspalvelun tarjoaja tai palveluntarjoajien yhteenliittymä rekisteröidään ensimmäisen kerran, sen on suoritettava Liikenne- ja viestintävirastolle 5 000 euron rekisteröimismaksu. Lisäksi tunnistuspalvelun tarjoajan tai yhteenliittymän on suoritettava Liikenne- ja viestintävirastolle vuosittain yhteensä 14 000 euron valvontamaksu kaikkien tarjoamiensa tunnistuspalveluiden valvonnasta.*

tunnistuspalveluja sähköisille asiointipalveluille. Vastaavasti tunnistusvälineen tarjoajaksi aikovan tulee ennen kaikkea saada loppukäyttäjät käyttämään sen tunnistusvälinettä sen lisäksi, että sen tulisi saada aikaiseksi tunnistusvälityssopimuksia tunnistusvälityspalvelujen ja/tai tunnistuspalvelujen myyntisopimuksia suoraan sähköisten asiointipalvelujen tarjoajien kanssa.

Liikenne- ja viestintävirasto on saanut viimeisten vuosien aikana useita yhteydenottoja vahvan sähköisen tunnistamisen markkinoille tulosta niin uutena tunnistusvälineen tarjoajana ja/tai tunnistusvälityspalvelun tarjoajana. Kiinnostuksensa markkinoille tulolle ovat ilmaisseet niin toimijat, jotka ovat vasta kehittämässä tunnistusvälinettä[70] tai välityspalvelua, mutta etenkin toimijat, jotka jo tarjoavat jossain muussa maassa vastaavanlaisia tunnistuspalveluja ja joilla on jo monelta osin olemassa vaadittavat tietojärjestelmät ja toimintaedellytykset tulla Suomen vahvan sähköisen tunnistamisen markkinalle.

Uusien toimijoiden tulo markkinoille on myös realisoitunut, kun sekä NETS Branch Norway että Signicat AS tulivat luottamusverkoston perustamisen yhteydessä markkinoille ja alkoivat tarjota tunnistusvälityspalveluja. Näiden toimijoiden markkinoille tulon jälkeen lainsäädäntöön ja sääntelyyn on tehty useita muutoksia, jotka ovat helpottaneet markkinoille tuloa muun muassa helpottaen välityspalvelusopimusten tekemistä tunnistusvälineen tarjoajien kanssa. Lainsäädäntöön ja sen tulkitsemiseen liittyvät epäselvyydet on myös pääosin saatu ratkaistua, jolloin lainsäädännön ennakoitavuus on parantunut. Myös toimintatavat mukaan lukien tunnistuspalvelun tarjoajien väliset sopimusmallit ja tekniset järjestelmärakenteet ovat vakiintuneet näiden toimijoiden markkinoille tulon jälkeen. Sähköisten asiointipalvelujen tietoisuus tunnistusvälityspalveluiden olemasta olosta ja mahdollisuudesta ostaa tunnistusvälineet keskistetysti käyttöönsä on myös lisääntynyt. Tietoisuuteen vaikutti osaltaan tekniseen sääntelyyn ja salausvaatimuksiin liittyvä muutos, jonka takia tunnistuspalvelut luopuivat Tupas-protokollasta ja siirtyivät käyttämään uusia rajapintoja, mikä edellytti viimeistään syksyllä 2019 muutoksia myös sähköisille asiointipalveluille.

6.4 Vahvan sähköisen tunnistamisen hinnoittelu

Vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinalla hinnoittelu tapahtuu markkinaehtoisesti ja hinnoitteluun ei ole kohdistettu sääntelyä. Vahvan sähköisen tunnistuspalvelujen tarjoajien sähköisiltä asiointipalveluilta ja tunnistusvälineen käyttäjiltä perimiin hintoihin vaikuttaa siten lähtökohtaisesti tunnistuspalvelun tarjoajan palvelun tarjoamisesta aiheutuvat kustannukset ja markkinan kilpailutilanne, joka säätelee tunnistuspalvelun mahdollisuuksia tehdä voittoa tunnistuspalvelujen tarjoamisella. Myös vahvoja sähköisiä tunnistuspalveluja ostavan sähköisen asiointipalvelun markkinavoimalla on merkittävä vaikutus vahvan sähköisen tunnistuspalvelun tarjoajien mahdollisuuksiin hinnoitella palvelujansa ja esimerkiksi Digi- ja väestötietovirasto tunnistuspalvelujen ostajana on kyennyt käyttämään tehokkaasti markkinavoimaansa vahvoja sähköisiä tunnistuspalveluja ostaessaan.

Vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinalla hinnoittelu sähköisten asiointipalvelujen osalta on sopimusperusteista eikä yhdelläkään vahvan sähköisen tunnistuspalvelun tarjoajalla ole julkista tunnistuspalvelujen hinnastoa saatavilla. Vahvasta sähköisestä tunnistuspalvelusta sähköisen asiointipalvelun maksama hinta voi vaihdella merkittävästikin palvelua kysyvän sähköisen asiointipalvelun tarjoajan mukaan ja vaikuttaisi siltä, että mitä enemmän tunnistuspalveluja sähköinen asiointipalvelu kysyy ja käyttää sitä vähemmän se maksaa tunnistuspalvelusta per tunnistustapahtuma. Toisin sanoen sopimushinnoittelussa on käytössä paljousalennukset.

[70] Esimerkiksi SisuID- hanke on kertonut julkisesti kehittävänsä uudenlaista tunnistusvälinettä tavoitteenaan myös rekisteröidä se vahvaksi sähköiseksi tunnistusvälineeksi.

Vahvojen sähköisten tunnistusvälineen tarjoajien tunnistusvälineen käyttäjiin kohdistuva hinnoittelu perustuu listahinnoitteluun, vaikka osin palveluja myydään myös sopimusperusteisesti osana muita palveluja.

Vahvojen sähköisten tunnistuspalvelujen vähittäismarkkinoilla tällä hetkellä yleisin ja lähtökohtaisesti ainut sähköisiin asiointipalveluihin sovellettava hinnoittelumalli on tapahtumaperusteinen hinnoittelu, jossa tunnistustapahtumalle on annettu yksikköhinta ja palvelun käytöstä laskutetaan tunnistustapahtumamäärien mukaan. Lisäksi saatetaan periä erilaisia avaus- ja käyttöönottomaksuja ja kiinteitä kuukausimaksuja. Tapahtumaperusteisella hinnoittelulla on pitkä historia ja sitä on muun muassa sovellettu jo ennen kuin vahvan sähköisen tunnistamisen markkinalle on kohdistettu hintasääntelyä. Käyttöönotettu tapahtumaperusteinen tukkuhintasääntely on myös omalta osaltaan tukenut tämän hinnoittelumallin säilymistä, vaikkei hintasääntely estä vähittäismarkkinalla käyttämästä myös kiinteään kuukausihintaa perustuvaa hinnoittelumallia. KKV:n selvitysten perusteella vaikuttaa myös siltä, että tällä hetkellä sähköiset asiointipalvelut pääasiassa itsekin odottavat vahvan sähköisen tunnistusvälityspalveluilta tapahtumaperusteista hinnoittelua. Kiinteä hinta voisi tuoda sähköisten asiointipalvelujen tarjoajille ennustettavuutta, mutta ainakin nykyisessä markkinatilanteessa tämä olisi todennäköisesti kalliimpi vaihtoehto, koska kiinteää vähittäishinnoittelua sovellettaessa vahvan sähköisen tunnistuspalvelun tarjoajan olisi todennäköisesti liiketoiminnallisista syistä sisällytettävä tapahtumamäärien vaihteluun liittyvä riskilisä hintoihinsa.

Esimerkiksi matkaviestinverkon puhelinpalveluihin on kohdistunut puheluminuuttiperusteista tukkuenimmäishintasääntelyä ja siitä huolimatta matkaviestinpalveluja tarjoavat teleyritykset ovat vähitellen siirtyneet tarjoamaan lähes pelkästään kuukausihinnoitteluun ja käytännössä lähes rajattomaan käyttöön perustuvia palveluja. Siirtymän taustalla ja mahdollistajana on ollut se, että käyttömäärien kasvaessa ja matkaviestinverkkotekniikan tehostuessa matkapuheluminuutin yksikkötuotantokustannukset ja sitä myöden yksikkötukkuenimmäishinta ovat alentuneet siinä määrin, että riski asiakkaiden suurien käyttömäärien aiheuttamista kustannuksista on lähes merkityksetön ja lähes poikkeuksetta teleyritykset kykenevät kattamaan matkapuhelupalvelujen käyttäjien aiheuttamat kustannukset niiltä perittävillä kuukausimaksuilla. Matkaviestinverkon puhelupalvelujen tarjoaminen on monelta osin samanlaista liiketoimintaa kuin vahvojen sähköisten tunnistuspalvelujen tarjoaminen, missä yksikkötuotantokustannukset palvelun tarjoamisesta alenevat sitä enemmän mitä enemmän palvelua käytetään. Siten vastaavanlainen hinnoittelumallien muutos on mahdollinen myös vahvan sähköisen tunnistamisen markkinalla, kun tunnistuspalvelujen käyttö yleistyy ja kasvaa nykyisestä sekä vahvan sähköisen tunnistuspalvelun tarjoajan riski mahdollisista alihinnoittelun aiheuttamista tappioista pienenee merkittävästi.

Sähköisiltä asiointipalveluilta perittäviin maksuihin voi myös kuulua niin vahvan sähköisen tunnistuspalvelun käyttöönottomaksuja kuin kiinteitä kuukausimaksuja tunnistuspalvelujen tapahtumakohtaisten maksujen lisäksi.

Vahvojen sähköisten tunnistusvälineen tarjoajien tunnistusvälineen käyttäjiin kohdistuva hinnoittelu perustuu kiinteisiin kuukausimaksuihin. Pari vahvan sähköisen tunnistusvälineen tarjoajista perii käyttäjiltä myös tunnistusvälineen käyttöönottomaksun.

Vahvan sähköisen tunnistusvälineen käyttäjiltä perittäviä maksuja voidaan pitää kohtuullisina ja jopa siinä määrin alhaisina, etteivät hinnat saa käyttäjiä suuremmassa määrin kilpailuttamaan vahvan sähköisen tunnistusvälineen tarjoajia. Kilpailuttamista myös rajoittaa merkittävästi se, että vahva sähköinen tunnistusväline on sidottu tiiviisti toiseen ja käyttäjän kannalta pääasialliseen palveluun vahvan sähköisen tunnistuspalvelun ollessa liitännäispalvelu. Vahvan sähköisen tunnistusvälineen käyttämisestä perittäviä maksuja on käsitelty tarkemmin luvussa 5.1.2.

KKV:n vahvan sähköisen tunnistusvälityspalvelun tarjoajilta saamien selvitysten perusteella sähköisten asiointipalvelujen kanssa sovituissa hinnoissa on suuret vaihteluvälit riippuen muun muassa asiakkaan koosta. Suuret sähköisten asiointipalvelujen tarjoajat pystyvät neuvottelemaan merkittävästi edullisempia tapahtumakohtaisia hintoja kuin pienet. Halvimmillaan tapahtumakohtaiset hinnat ovat lähellä tunnistustapahtumien välittämisen enimmäistukkuhintaa eli kolmea eurosenttiä. Pienimpien sähköisten asiointipalvelujen tarjoajien osalta tapahtumakohtaiset hinnat saattavat kuitenkin olla moninkertaiset. Tapahtumakohtaisen hinnan lisäksi vahvan sähköisen tunnistusvälityspalvelun tarjoajat saattavat periä erilaisia kertaluonteisia avaus- tai käyttöönottomaksuja sekä kiinteitä kuukausimaksuja, mutta tältäkin osin hajonta on suurta.

6.5 Luottamusverkosto: vahvan sähköisen tunnistamisen kilpailusääntely

Luottamusverkostolla tarkoitetaan Liikenne- ja viestintävirastolle ilmoituksen tehneiden vahvan sähköisen tunnistuspalvelun tarjoajien eli tunnistusvälineen tarjoajien ja tunnistusvälityspalvelun tarjoajien verkostoa. Luottamusverkostosta säädetään tunnistuslain 12 a-d §:ssä. Vahvan sähköisen tunnistuspalvelun tarjoaja liittyy automaattisesti osaksi luottamusverkostoa tehdessään tunnistuslain 10 §:n mukaisen ilmoituksen Traficomille, ja siihen aletaan soveltaa tunnistuslain 12 a-d §:ssä säädettyjä vaatimuksia ja velvoitteita. Luottamusverkoston perustana on vahvan sähköisen tunnistusvälineen tarjoajan velvollisuus tarjota tunnistuspalvelunsa käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että tunnistusvälityspalvelun tarjoajat voivat välittää tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle eli sähköisille asiointipalveluille. Kyse on niin sanotusta tukkumarkkinasääntelystä, joka kohdistuu vain ja ainoastaan vahvan sähköisen tunnistamisen markkinalla tunnistuspalveluja tarjoavien tarjoajien väliseen liiketoimintaan.

Luottamusverkoston ja siihen liittyvän sääntelyn kautta on mahdollistettu ja mahdollistetaan vahvan sähköisen tunnistusmarkkinan kilpailua parantavien ja edistävien tunnistusvälityspalvelujen syntyminen. Luottamusverkosto myös mahdollistaa parhaimmillaan sähköisille asiointipalveluille sen, että ne voivat hankkia kaikkien eri vahvoja sähköisiä tunnistusvälineitä käyttävien käyttäjien ja siten myös asiakkaidensa tunnistamisen yhdeltä tunnistusvälityspalvelulta. Tällöin sähköisen asiointipalvelun ei tarvitse tehdä erikseen sopimusta jokaisen vahvan sähköisen tunnistusvälineen tarjoajan kanssa ja erillisiä teknisiä järjestelyitä, mitkä myös alentavat sähköisille asiointipalveluille aiheutuvia sopimus- ja käyttöönottokustannuksia. Ilman luottamusverkoston tukkumarkkinasääntelyä sähköinen asiointipalvelu joutuisi tekemään sopimukset kaikkien vahvan sähköisen tunnistusvälineen tarjoajien kanssa saadakseen tunnistettua kaikki asiakkaansa. Tämä oli tilanne vielä vuonna 2019, ennen luottamusverkostoa ja tukkumarkkinasääntelyn toimeenpanoa sekä tunnistusvälityspalvelujen markkinoille tuloa.

Erikseen vahvan sähköisen tunnistamisen markkinalle kohdistetun tukkumarkkinasääntelyn lisäksi markkinaan sovelletaan myös yleistä kilpailulainsäädäntöä ja sen valvontaa. Yleisen kilpailulainsäädännön ja sen valvonnan tavoitteena on ennen kaikkea estää markkinavoiman väärinkäyttö markkinalla.

6.5.1 Luottamusverkoston historia ja kehitys

Vahvasta sähköisestä tunnistamisesta säädettiin ensimmäistä kertaa vuonna 2009 annetussa laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi (617/2009). Kyseinen laki tuli voimaan 1.9.2009. Tuolloin laissa ei vielä puhuttu luottamusverkostosta, mutta laissa sallittiin ensitunnistamisen ketjuttaminen kahden tunnistuspalvelun välillä nimenomaisella sopimuksella siitä. Hintaa ei säännelty.

Vasta vuonna 2015 tunnistuslain muutoksella (laki 139/2015, HE 272/2014) lakiin lisättiin uusi luottamusverkostosääntely ja ensitunnistamisen ketjuttamisen mahdollisuutta laajennettiin. Laki tuli voimaan pääosin 1.6.2016, mutta luottamusverkostosääntely tuli sovellettavaksi vasta 1.5.2017. Lain 12 a §:ssä määriteltiin yleisellä tasolla tunnistuspalvelujen hallinnollisia käytäntöjä, jotka *luovat edellytykset tunnistuspalveluita tarjoavien ja niitä hyödyntävien toimijoiden väliselle toiminnalle*. Tunnistustapahtuman enimmäishinnaksi säädettiin 10 eurosenttiä. Ensitunnistamisen ketjuttamisen rajoittuminen kahden toimijan väliseen sopimukseen poistettiin eli sallittiin rajoitukseton ketjuttaminen. Ensitunnistamisen ketjuttamisen hintaa ei kuitenkaan vieläkään säännelty. Ennen tätä ja pitkään tämänkin lakimuutoksen jälkeen vahvan sähköisen tunnistuspalvelun tarjoajat toimivat käytännössä vähintäänkin heikon monopolin asemassa suhteessa oman tunnistusvälineensä käyttämiseen sähköisissä asiointipalveluissa.

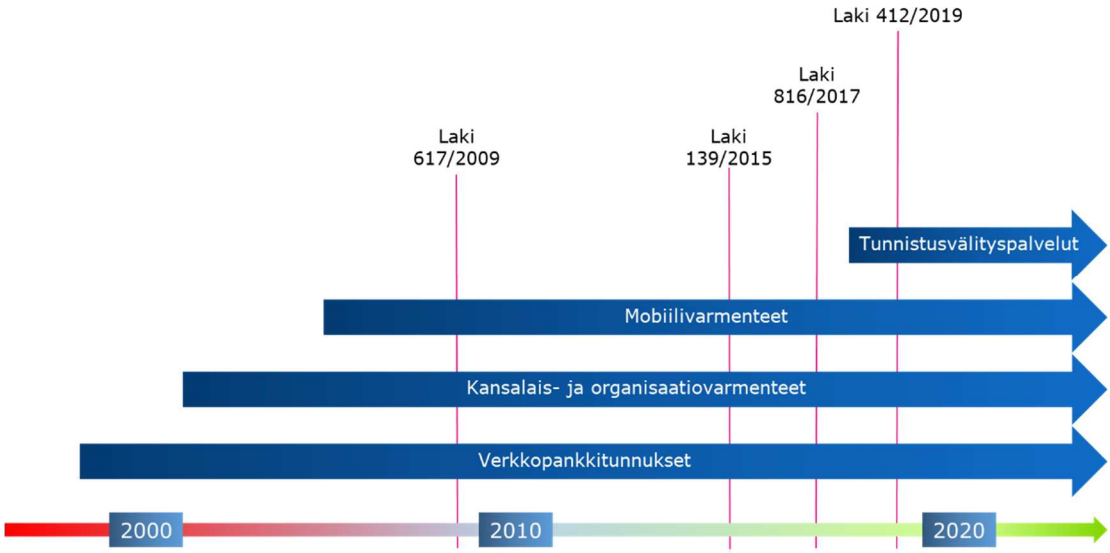
Vuonna 2017 tunnistuslain muutoksella (laki 816/2017, HE 82/2017) säänneltiin ensimmäisen kerran ensitunnistamisen hintaa. Laki tuli voimaan 15.12.2017. Hintasääntely säädettiin määräaikaiseksi viideksi vuodeksi lain voimaantulosta. Ensitunnistamisen ketjuttamisen hintasääntelyn perusteeksi säädettiin *Suomessa toimivien tunnistusvälineen tarjoajien perimien ensitunnistamistietojen hintojen mediaani.* Enimmäishinnan tuli lain mukana laskea vuosittain *siten, että se laskee vuosittain 25 prosenttia mutta on kuitenkin vähintään 35 senttiä ja enintään 5 euroa.* Viestintäviraston tuli lain mukaan antaa päätös korvauksen enimmäistasosta sentin tarkkuudella. Enimmäishinta asetettiinkin erillisellä Viestintäviraston (nykyisin Liikenne- ja viestintävirasto) päätöksellä ja annetun päätöksen enimmäishinta tuli voimaan 1.6.2018. Päätös kuvataan jäljempänä kuvassa 16.

Vuonna 2019 tunnistuslain muutoksella (laki 412/2019, HE 264/2018) luottamusverkostoa koskeviin säännöksiin tehtiin useita tarkennuksia. Laki tuli voimaan 1.4.2019 ja siinä oli 2 kuukauden siirtymäaika toimitusehtojen julkaisemiselle ja 3 kuukauden siirtymäaika vanhojen sopimusten saattamiselle uusien ehtojen mukaiseksi. Ensitunnistamisen ketjuttamisen sääntely säädettiin määräaikaisena kahdeksi vuodeksi lain voimaantulosta. Lain 12 a § - 12 d §:issä säädettiin tarkasti tunnistusvälineen tarjoajan käyttöoikeuden luovutusvelvollisuudesta, käyttöoikeuden toimitusehdoista, sopimuksen tekemisen määräajasta ja vahingonkorvausvelvollisuudesta käyttöoikeuden luovutuksen säännöksen tahallisen tai tuottamuksellisen rikkomisen aiheuttamasta vahingosta. Tunnistustapahtuman enimmäishintaa laskettiin 10 sentistä 3 senttiin. Sopimusehtojen ja enimmäishinnan sääntely ulotettiin koskemaan myös ensitunnistamisen ketjuttamista. Näiden muutosten seurauksena luottamusverkoston velvoitteista saatiin vihdoin toimivat ja tunnistusvälityspalvelut saivat tehtyä sopimukset tunnistusvälineen tarjoajien kanssa eli kattavien tunnistusvälityspalvelujen tarjoaminen tosiallisesti mahdollistui. Kehityksen vaikutti samanaikaisesti käynnissä ollut teknisten rajapintojen salausvaatimusten jatketun siirtymäajan voimaantulo ja valvonta, jonka takia vanhat TUPAS-integraatiot asiointipalvelujen kanssa oli päivitettävä viimeistään lokakuussa 2019.

Vuosi 2020 oli käytännössä ensimmäinen täysi vuosi, jonka aikana tunnistusvälityspalveluja tarjottiin kattavasti tunnistuspalvelujen markkinalla ja sähköisillä asiointipalveluilla oli tosiasialliset mahdollisuudet kilpailuttaa vahvojen sähköisten tunnistuspalvelujen tarjoajia. Kilpailun avaamisen vaikutukset ovat nyt alkaneet näkyä muun muassa vahvojen sähköisten tunnistuspalvelujen kasvaneena käyttämisenä ja sähköisille asiointipalveluille alentuneina tunnistuspalvelujen hintoina.

Tunnistuslain muutosehdotus (HE 237/2020) on parhaillaan eduskunnassa[71]. Lainmuutoksella jatketaan kahdella vuodella ensitunnistamisen ketjuttamisen enimmäishinnan sääntelyä.

[71] Muutos on hyväksytty eduskunnassa 11.3.2021.



Kuva 13: Luottamusverkoston ja kilpailun kehittyminen vahvojen sähköisten tunnistuspalvelujen markkinalla sekä luottamusverkoston kannalta merkittävimmät hallituksen esitykset vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalvelusta annetun lain antamiseksi ja muuttamiseksi.

6.5.2 Tunnistustapahtumien välittäminen luottamusverkostossa

Vahvan sähköisen tunnistuspalvelun tarjoajilta ei ole ollut saatavilla kattavasti tietoja tunnistuspalveluiden käyttöoikeuden eli tunnistustapahtumien välittämisen myyntimääristä aikaisempien vuosien osalta. Siten tätä markkinaselvitystä tehtäessä ei ole ollut mahdollisuutta tarkastella välitettyjen tunnistustapahtumien määrän kehittymistä useamman vuoden aikajaksolta. Vahvan sähköisen tunnistuspalvelun tarjoajilla on ollut myös vaikeuksia tarjota tarkkoja lukuja tunnistustapahtumien määristä ja erotella esimerkiksi sähköisille asiointipalveluille tarjottujen tunnistuspalvelujen tunnistustapahtumia välitettäväksi tarjottujen tunnistustapahtumien määristä.

Välitettyjen vahvojen sähköisten tunnistusvälineiden tunnistustapahtumien määrän voidaan katsoa selkeästi kasvaneen vuoden 2020 ensimmäisellä vuosipuoliskolla suhteessa vuoden 2019 jälkimmäisen vuosipuoliskoon. Vuoden 2019 jälkimmäisen vuosipuoliskon aikana välitettiin arviolta noin 20 miljoonaa tunnistustapahtumaa, kun vuoden 2020 ensimmäisellä vuosipuoliskolla välitettyjen tunnistustapahtumien määrä oli lähes kolminkertaistunut arviolta noin 60 miljoonaan tunnistustapahtumaan. Arviot perustuvat tunnistuspalvelun tarjoajilta saatuihin tietoihin. Lukujen osalta on syytä huomioida, että osa tunnistuspalvelun tarjoajista ei kyennyt erottelemaan niiden omissa palveluissa tehtyjä tunnistustapahtumia ja niiden suoraan sähköisille asiointipalveluille myymiä tunnistustapahtumia tunnistuspalveluille välitettävien tunnistustapahtumien määristä. Tämä koskee erityisesti vuoden 2019 lukuja. Karkeasti voidaan kuitenkin arvioida, että luottamusverkoston koko vuotuisena tunnistustapahtumamäärinä mitattuna on vuonna 2019 ollut noin 40-80 miljoonaa tunnistustapahtumaa.

Suhteutettuna kaikkiin vahvan sähköisen tunnistuspalvelujen markkinalla vahvalla sähköisellä tunnistusvälineellä tehtyihin tunnistustapahtumiin vuoden 2020 ensimmäisellä vuosipuoliskolla noin puolet tunnistustapahtumista välitettiin tunnistusvälityspalvelun kautta, kun vielä vuoden jälkimmäisellä vuosipuoliskolla alle 30 prosenttia välitettiin tunnistusvälityspalvelun kautta.

Vuoden 2019 jälkimmäisellä vuosipuoliskolla arviolta noin 85-90 prosenttia välitetyistä tunnistustapahtumista koski verkkopankkitunnisteilla ja noin 10-15 prosenttia mobiilivarmenteilla tehtyjen tunnistustapahtumien välittämistä. Vuoden 2020 ensimmäisen vuosipuoliskon vastaavat luvut olivat arviolta noin 75-80 ja 20-25

prosenttia. Mobiilivarmenteilla tehtyjen tunnistustapahtumien välittämisen suhteellinen osuus oli siten kasvanut puolessa vuodessa noin 10 prosenttiyksikköä.

Välitettyjen tunnistustapahtumien määrän kasvun vastaisesti, tunnistustapahtumien välittämisestä saadut tulot laskivat jossain määrin vuoden 2020 ensimmäisellä vuosipuoliskolla. Vuoden 2019 jälkimmäisellä vuosipuoliskolla tunnistustapahtumien välittämisestä saadut tulot olivat arviolta noin 4,1 miljoonaa euroa, kun vuoden 2020 ensimmäisellä vuosipuoliskolle ne olivat noin 3,7 miljoonaa euroa. Arviot perustuvat tunnistuspalvelun tarjoajilta saatuihin tietoihin. Myös näiden lukujen osalta on syytä huomioida, että osa tunnistuspalvelun tarjoajista eivät kyenneet tarjoamaan tarkkoja eurosummia eikä erottelemaan sähköisiltä asiointipalveluilta saatuja tuloja tunnistustapahtumien välittämisestä saaduista tuloista. Karkeasti voidaan kuitenkin arvioida, että luottamusverkoston koko vuotuisena liikevaihdolla mitattuna oli vuonna 2019 noin 5-8 miljoonaa euroa.

6.5.3 Luottamusverkoston sopimussuhteet ja enimmäishintasääntely

Tunnistuslaissa (12 c §) on säädetty enimmäistukkuhinnasta, jonka tunnistusvälineen tarjoaja voi enintään periä tunnistusvälityspalvelun tarjoajalta tunnistuspalvelun käyttöoikeudesta eli yhden tunnistustapahtuman välittämisestä. Voimassa olevan lain mukaan tämä enimmäishinta saa olla enintään 3 senttiä per välitettävä tunnistustapahtuma. Hinnan tulee kattaa kaikki sähköiseen tunnistusvälineeseen liittyvät henkilön tunnistetiedot. Tunnistuspalvelun käyttöoikeudesta ei myöskään saa periä muuta korvausta. Laskutuksen sekä kaikkien sellaisten tunnistusvälineen tarjoajan rajapintojen, toimintojen, palvelujen, ohjelmistojen ja tietojärjestelmien käyttöoikeudet, joita tarvitaan tunnistuksen välittämiseen luottavalle osapuolelle, tulee myös sisältyä edellä mainittuun enimmäishintaan. Uusissa sopimuksissa vielä 1.4.2019 ja vanhoissa sopimuksissa 1.7.2019 asti säännelty enimmäishinta sai olla enintään 10 senttiä ja hintaan kuuluvia palveluita, toiminteita, jne. ei oltu tarkemmin määritelty.

Vahvan sähköisen tunnistuspalvelun tarjoajilta saatujen tietojen mukaan vuonna 2020 kaikki tunnistusvälineen tarjoajat perivät välityspalvelun tarjoajilta enimmäishinnan mukaisen hinnan eli 3 senttiä per välitettävä tunnistustapahtuma pois lukien yksi tunnistusvälineen tarjoaja, joka ei perinyt lainkaan maksua tunnistustapahtuman välittämisestä. Tunnistustapahtumasta perittävän tapahtumakohtaisen hinnan lisäksi lainsäädännön mukaisesti tunnistusvälineen tarjoajat eivät perineet muita toistuvaluonteisia maksuja.

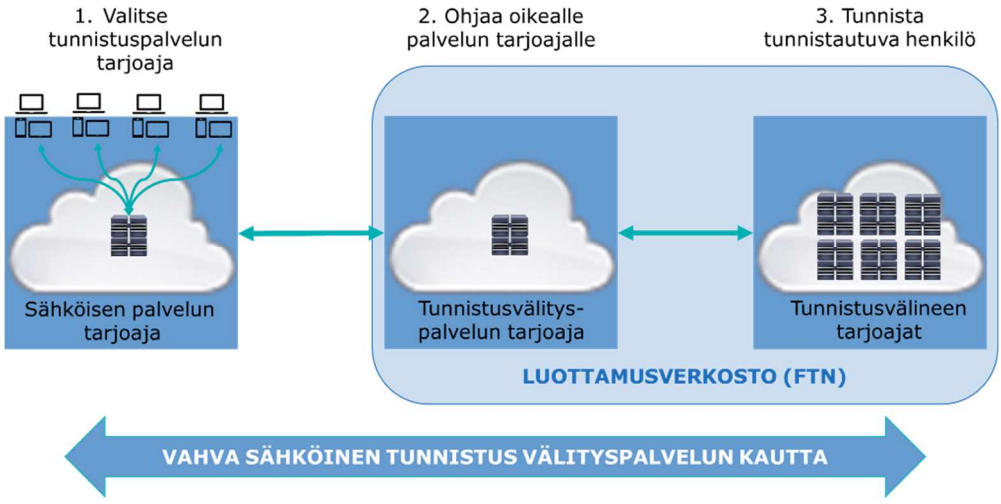
Tunnistusmarkkinaselvitystä tehtäessä ei ole ollut käytössä tarkempaa ja ajantasaista tietoa eri vahvan sähköisen tunnistusvälineen tarjoajien todellisista kustannuksista, joita niille syntyy tunnistustapahtuman välittämisestä, ja niiden suuruudesta. Siten ei ole ollut mahdollista tarkemmin selvittää näiden kustannusten suhdetta välitettävän tunnistustapahtuman hintaan, kuten ei myöskään esimerkiksi sitä, onko tunnistustapahtuman määrällä vaikutusta yksittäisen tunnistustapahtumasta syntyvään kustannukseen.

KKV:n selvitysten perusteella voidaan todeta yleisellä tasolla, että vahvan sähköisen tunnistusvälineen tarjoamisen kustannuksia – oli kyse kiinteistä tai muuttuvista kustannuksista – ei ole yksinkertaista selvittää tai vertailla. Mobiilivarmenteita tarjoavien matkaviestinverkkoyritysten osalta kustannukset liittyvät pitkälti luottamusverkostossa toimimiseen. Sen sijaan verkkopankkitunnuksia tarjoavilla pankeilla vahvan sähköisen tunnistusvälineen pääpaino on yleensä oman verkkopankin toiminnassa ja maksamisessa, joskin on huomattava, että pankeissakin vahvan sähköisen tunnistuksen välityspalvelut on kehitetty luottamusverkostossa toimimista varten. Osa vahvan sähköisen tunnistusvälineen tarjoajista on päätynyt yhteisiin järjestelmiin, jolloin kustannukset ovat suhteessa alhaisemmat, mutta näiden toimijoiden volyymit ovat myös pienemmät kuin suurilla toimijoilla. Kustannusten arvioinnin kannalta merkitystä on silläkin, että osa toimijoista on ulkoistanut järjestelmien kehitystyön, kun taas osalla on kyse omista järjestelmistä.

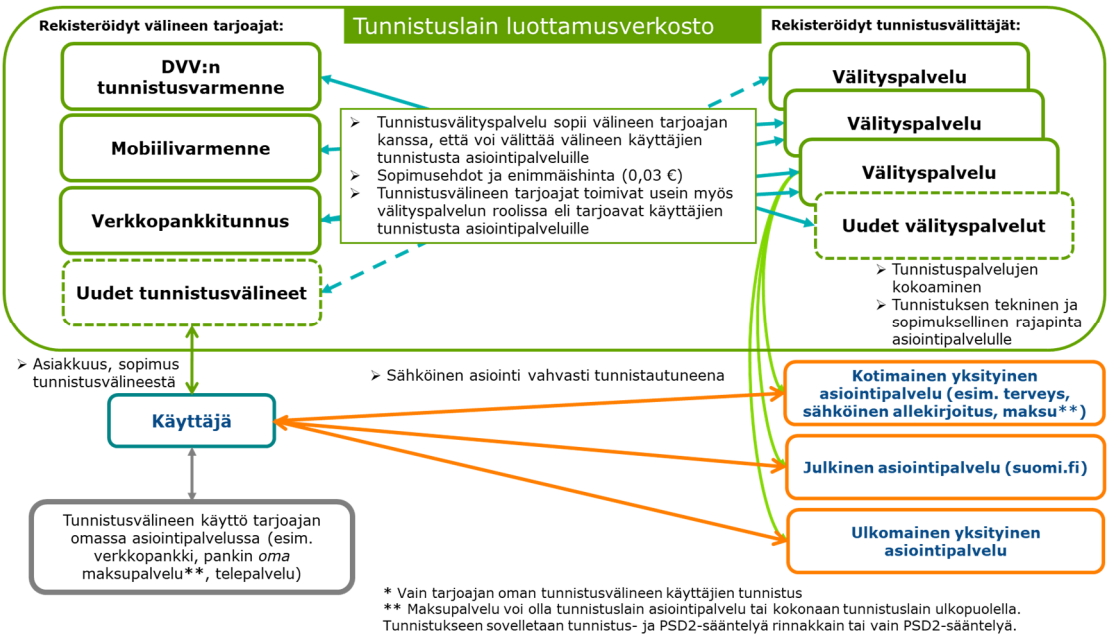
KKV:n vahvan sähköisen tunnistusvälineen tarjoajilta saamat arviot volyymin eli tapahtumamäärien muutosten vaikutuksista kustannuksiin vaihtelivat huomattavasti. Merkittävä tapahtumamäärien kasvu on kuitenkin omiaan kasvattamaan vahvan sähköisen tunnistuspalvelun ylläpitokustannuksia.

6.5.4 *Luottamusverkoston vaikutukset vahvan sähköisen tunnistamisen markkinalla*

Luottamusverkostossa vahvan sähköisen tunnistusvälityspalvelun tarjoaja käytännössä myy sähköiselle asiointipalvelulle tunnistustapahtuman välittämistä tunnistusvälineille. Välityspalvelun tarjoaja huolehtii sähköisen asiointipalvelun puolesta tarvittavien sopimusten laatimisesta ja teknisten järjestelmärajapintojen rakentamisesta tunnistusvälineen tarjoajien kanssa, jolloin sähköisen asiointipalvelun tarvitsee parhaimmillaan tehdä vain yksi sopimus ja toteuttaa yksi tekninen rajapinta välityspalvelun tarjoajan kanssa ostaakseen ja saadakseen käyttöönsä kaikki vahvan sähköisen tunnistamisen markkinalla olevat tunnistusvälineet. Tämä luo sähköiselle asiointipalvelulle mahdollisuuden kilpailuttaa tunnistusvälityspalvelun tarjoajia. Luottamusverkostolla ja siihen kohdistetulla tukkumarkkinasääntelyllä siis mahdollistetaan kilpailu vähittäismarkkinoilla. Vastaavanlaista sääntelyä toteutetaan esimerkiksi viestintäpalvelujen markkinoilla.



Kuva 14: Luottamusverkoston yleinen toimintaperiaate



Kuva 15: Luottamusverkoston sopimussuhteet ja tunnistusjärjestelmien yhteenliitokset.

Vahvojen sähköisten tunnistuspalvelujen tukkuhintasääntelyllä on vastaavanlaisesti ollut vaikutuksia vähittäismarkkinakilpailun mahdollistamiseen ja sitä kautta vähittäismarkkinoiden tunnistuspalveluista maksettuun hintatasoon. Erityisesti vuonna 2019 tehdyillä muutoksilla (muun muassa enimmäishinnan alentaminen ja hinnan sisältämien palvelujen tarkentaminen sekä sopimusehtojen ja sopimuksen tekemisen määräajan sääntely) on ollut merkittävä vaikutus tunnistusvälityspalvelun tarjoajien toimintaan ja toimintaedellytyksiin. Käytännössä ennen vuonna 2019 tehtyä enimmäishinnan alentamista 3 senttiin tunnistustapahtumalta vahvan sähköisen tunnistusvälineen tarjoajat tarjosivat vähittäismarkkinoilla tunnistuspalveluja alle säädetyn 10 sentin enimmäistukkuhinnan, jolloin tunnistusvälityspalvelun tarjoajilla ei ollut mitään mahdollisuutta kilpailla tunnistusvälineen tarjoajien kanssa sähköisiltä asiointipalveluilta tunnistustapahtumasta perittävällä hinnalla.[72] Sähköisille asiointipalveluille oli käytännössä aina taloudellisesti kannattavampaa ostaa vahvat sähköiset tunnistuspalvelut suoraan tunnistusvälineen tarjoajilta kuin tunnistusvälityspalveluiden tarjoajilta. Nämä tapaukset myös osoittivat, että jopa yksittäisillä vahvan sähköisen tunnistusvälineen tarjoajilla oli merkittävästi markkinavoimaa hinnoitella vahvat sähköiset tunnistuspalvelunsa riippumatta muista tunnistusvälineen tarjoajista, välityspalvelun tarjoajista ja sähköisistä asiointipalveluista. Säännellyn enimmäishinnan alentamisen seurauksena tunnistusvälityspalvelun tarjoajille muodostui todellinen mahdollisuus kilpailla tunnistusvälineen tarjoajien kanssa myös sähköisiltä asiointipalveluilta tunnistustapahtumasta perittävällä hinnalla.

Kilpailu kannustaa yrityksiä tarjoamaan parempia vaihtoehtoja kuin kilpailijansa, tehostamaan toimintatapojaan sekä innovoimaan asiakkaiden tarpeita vastaavia tuotteita ja palveluja. Asiakkaille toimiva kilpailu näkyy edullisempina hintoina, parempina tuotteina ja palveluina sekä laajempana valikoimana, mikä lisää kysyntää ja kasvua. Tunnistusmarkkinoilla lisääntyvä kilpailu omiaan lisäämään käytettävyyttä ja turvallisuudeltaan entistä parempia ja laajemmassa käytössä olevia ratkaisuja.

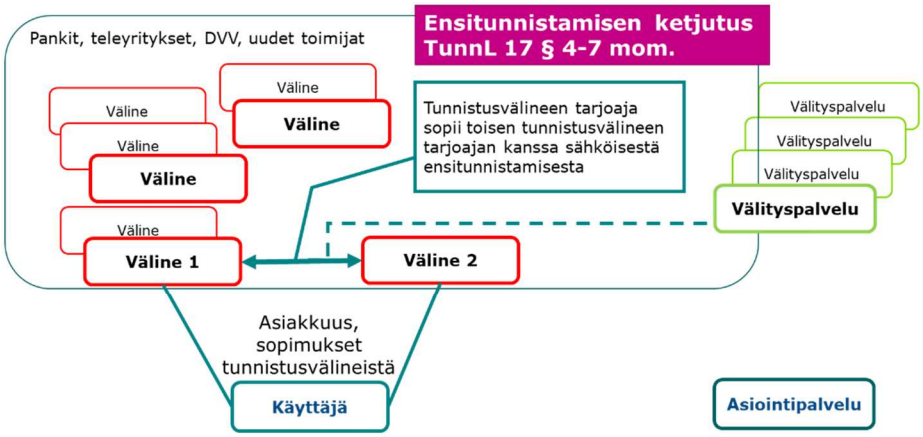
[72] Esimerkiksi pankit tarjosivat vuonna 2018 Väestörekisterikeskukselle toistaiseksi voimassa olevalla sopimuksella tunnistuspalvelua yksikköhintaan 6 senttiä per tunnitustapahtuma siihen saakka, kunnes pankkitunnistusten kokonaismäärä ylittää kalenterivuonna 40 000 000 tapahtumaa, jolloin yksikköhinta laski vielä kalenterivuoden loppuun saakka 4,5 senttiin per tunnistustapahtuma. Vuodelle 2019 Väestörekisterikeskus oli tehnyt tunnistusvälineen tarjoajien kanssa hankintasopimuksia, joissa yksikkökohtainen hinta vaihteli pyöristettynä 3,4 sentistä 6,8 senttiin. (Lähde: HE 264/2018).

Digi- ja väestötietoviraston henkilö- ja organisaatiovarmenteita ei tällä hetkellä välitä yksikään välityspalvelun tarjoaja. Tämä todennäköisemmin johtuu siitä, että henkilö- ja organisaatiovarmenteiden käyttö on yleisesti vähäistä kansalaisten keskuudessa eikä monessakaan sähköisessä asiointipalvelussa ole nähty tarpeelliseksi mahdollistaa asiakkaidensa tunnistautumista näillä varmenteilla, koska asiakkailla on käytössään jokin toinen ja yleisesti käyttämä tunnistusväline. Henkilö- ja organisaatiovarmenteiden välittäminen vaatii myös aina niin sanotun satu-hetu-kyselyn, koska varmennekortilla on vain tieto satusta eli sähköisestä asiointitunnuksesta ja hetua eli henkilötunnusta sähköisessä asiointipalvelussa tarvittaessa ei henkilötunnustieto siirry palveluun ilman satu-hetu-kyselyä.

6.6 Sähköinen ensitunnistaminen vahvan sähköisen tunnistusvälineen hakemisessa ja myöntämisessä

Tunnistuslain 17 §:n mukaan vahvan sähköisen tunnistusvälineen tarjoajan on mahdollistettava se, että toinen tunnistusvälineen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä sähköiseen ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä.

Vahvan sähköisen tunnistuspalvelujen tarjoajien tarkastuskertomusten mukaan tällä hetkellä 9 tunnistusvälineen tarjoajaa on mahdollistanut niiden tarjoaman vahvan sähköisen tunnistusvälineen hakemisen käyttämällä sähköistä ensitunnistamista. Vastaavasti viisi tunnistusvälineen tarjoajaa ei ole tätä mahdollistanut ja niiden vahva sähköinen tunnistusväline on mahdollista ottaa käyttöön vain asioimalla fyysisesti tunnistusvälineen tarjoajan toimipisteessä. Digi- ja väestötietoviraston tarjoamien kansalais- ja organisaatiovarmenteiden osalta sähköinen ensitunnistus ei ole ollut mahdollista, koska muiden vahan sähköisen tunnistusvälineen tarjoajien tunnistusvälineet ovat korotetun varmuustason tunnistusvälineitä, jolloin ne eivät ole riittäviä korkean varmuustason kansalais- ja organisaatiovarmenteiden hakemisessa.



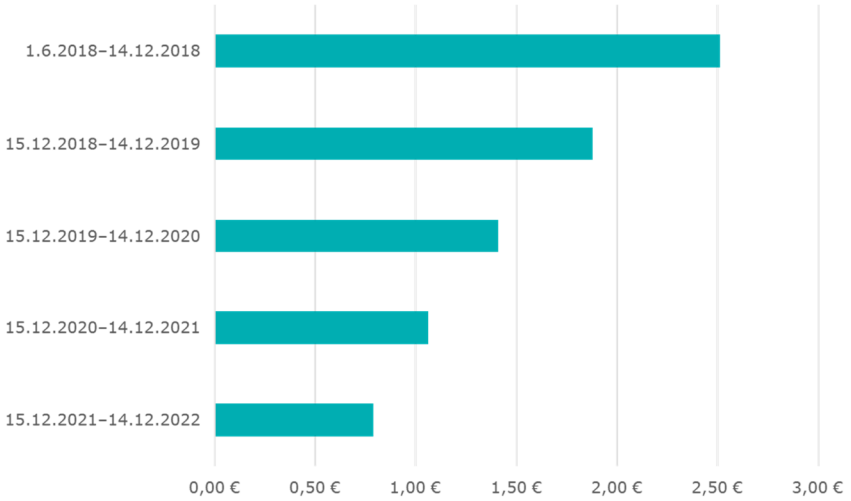
- **Tarjontavelvollisuus:** mahdollistettava ensitunnistus toiselle tunnistusvälineen tarjoajalle
- **Sopimusehdot:** laadittava ja julkaistava (TunnL 12 a-b § soveltuvat myös tähän)
- **Hinta:** enimmäishinta myös ensitunnistamisesta 0,03 € (TunnL 12 c § soveltuu *2 v*)
- Tunnistusvälineen tarjoajat voivat *halutessaan* yhdistää ensitunnistussopimuksen välityspalvelusopimukseen – käyttötarkoitus ensitunnistukseen huomioitava

Kuva 16: Sähköinen ensitunnistaminen, siitä sopiminen ja sen hinnoittelu.

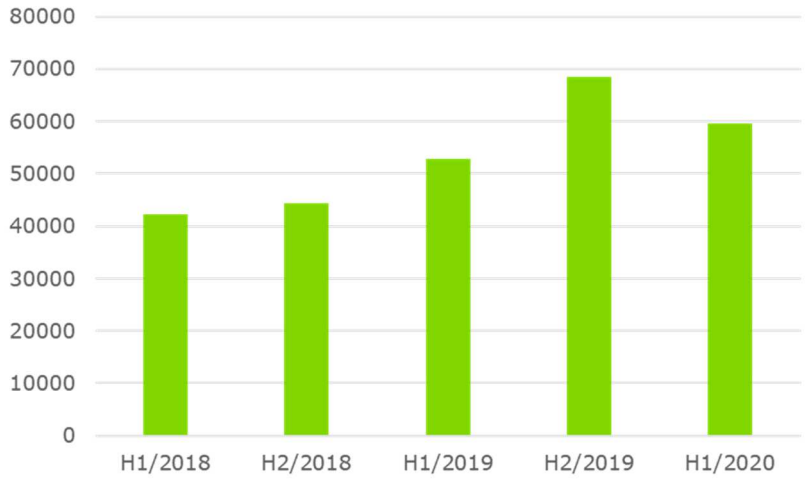
Tunnistuslain 17 §:ssä on säädetty sähköisen tunnistamisesta eli ensitunnistamisen ketjuttamisesta enimmäishinnasta eli hinnasta, jonka toinen vahvan sähköisen tunnistusvälineen tarjoaja saa periä toiselta vahvan sähköisen tunnistusvälineen tarjoajalta ensitunnistamisen ketjuttamisesta. Enimmäishinta saa tällä hetkellä olla enintään 3 senttiä per ensitunnistamisen ketjuttaminen. Asetettu enimmäishinta on väliaikaisesti voimassa 1.4.2019–31.3.2021 ja sääntelyn voimassaoloa jatketaan

lainmuutoksella kahdella vuodella. Hallituksen esityksessä on esitetty, että enimmäishinta olisi edelleen edellä mainittu 3 senttiä per ensitunnistamisen ketjuttaminen.

Ennen vuonna 2019 tehtyä lainmuutosta enimmäishintaan sovellettiin silloisen Viestintäviraston (nykyisin Liikenne- ja viestintävirasto) 23.4.2018 antamaa päästöstä (dnro 23/620/2018) korvauksen enimmäistasosta, missä enimmäishinta oli määritelty vuonna 2017 lakiin lisättyjen ja laissa asetettujen periaatteiden mukaisesti. Päätöksessä asetettu enimmäishinta laski portaittain vuoden 2018 kesäkuun 2,51 eurosta vuoden 2021 joulukuun 0,79 euroon. Ensitunnistamisen ketjuttamisen määristä nähdään, että vuonna 2019 lainmuutoksen myötä voimaan tullut 3 sentin enimmäishinta ja sen myötä tehty merkittävä enimmäishinnan lasku kasvatti merkittävästi ensitunnistamisen ketjuttamisen määriä. Vuonna 2019 tehtyä lainmuutosta voidaan ensitunnistamisen ketjuttamisen määrin näkökulmasta pitää siten onnistuneena eli lainmuutoksella saatiin aikaan muutos, jota sillä tavoiteltiin. Ennen kesäkuuta 2018 ensitunnistamisen ketjuttamisen hintoihin ei kohdistettu hintasääntelyä ja hintojen annettiin määräytyä markkinaehtoisesti.



Kuva 17: Viestintäviraston päätöksessä dnro 23/620/2018 asetetut ensitunnistamisen ketjuttamisen enimmäishinnat ajanjaksolle 1.6.2018 - 14.12.2022.



Kuva 18: Ensitunnistamisen ketjuttamisen määrät.

Liikenne- ja viestintävirasto Traficom

PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978-952-311-749-5
ISSN 2669-8781 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto